



TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Auditoría con ISO 27001 para
cumplimiento normativo de la
empresa SayNet Soluciones Integrales
S.A. de C.V.

Informe técnico de Residencias
Profesionales

Para obtener el título de
INGENIERO EN SISTEMAS COMPUTACIONALES

Con especialidad
Auditoría en Seguridad Informática

Presenta:
Gante Sánchez Brenda Itzel
Gutiérrez Guerra Lizeth Viridiana

RESUMEN

El presente informe constituye un análisis detallado del cumplimiento normativo de la empresa SayNet Soluciones Integrales S.A. de C.V. con el estándar internacional ISO 27001:2015 en el ámbito de la seguridad de la información. A lo largo del estudio, se ha llevado a cabo una exhaustiva auditoría con el objetivo de evaluar el nivel de conformidad de la empresa con los requisitos establecidos por la normativa ISO 27001 y proporcionar recomendaciones concretas para fortalecer su sistema de gestión integral.

La importancia estratégica de este trabajo radica en el contexto empresarial actual, donde la seguridad de la información se ha convertido en un factor crítico y la protección de los intereses. En un entorno caracterizado por la creciente digitalización y las amenazas cibernéticas, el cumplimiento de estándares reconocidos internacionalmente como ISO 27001 se presenta como una estrategia clave para mitigar riesgos y demostrar el compromiso de la empresa con la seguridad de la información.

Se presentan las generalidades del proyecto, contextualizando la situación de la empresa y delineando los objetivos específicos de la auditoría. Se ofrece un marco teórico que comprende conceptos fundamentales sobre seguridad de la información, los principios de la norma ISO 27001 y las metodologías de auditoría de cumplimiento. También se detalla el proceso de auditoría, describiendo con detalle la metodología empleada, que incluye listas de cotejo, entrevistas Y cuestionarios. Por último, se presentan los resultados obtenidos de la auditoría, resaltando los hallazgos más relevantes en los informes y las recomendaciones para la mejora continua del sistema de gestión integral.

ÍNDICE DE CONTENIDOS

GENERALIDADES DEL PROYECTO	15
1.1 INTRODUCCIÓN	16
1.2 DESCRIPCIÓN DE LA EMPRESA	18
1.2.1 Nombre, razón social	18
1.2.2 Ubicación	18
1.2.3 Organigrama.....	18
1.2.4 Sector productivo de la empresa	19
1.2.5 Misión, Visión, Filosofía y/o Valores	19
1.2.5.1 Misión.....	19
1.2.5.2 Visión	19
1.2.5.3 Filosofía y/o Valores	20
1.2.6 Breve historia de la empresa.....	20
1.3 PROBLEMA A RESOLVER.....	22
1.4 OBJETIVOS	23
1.4.1 Objetivo general	23
1.4.2 Objetivos específicos.....	23
1.5 JUSTIFICACIÓN.....	25
MARCO TEÓRICO	27
2.1 Estado del arte	28
2.2 Marco conceptual	32
2.3 Marco metodológico	34
ISO/IEC 27001.....	34
2.4 Estructura de ISO 27001.....	37
DESARROLLO	40
Objetivo 3 Planificar la Auditoria	41
3.1.1 Actividades	41
3.1.1.1 Actividad: Definir el alcance de la auditoría, identificando los controles de seguridad informática a evaluar.	41
3.1.1.1.1 Descripción de la actividad	41
3.1.1.1.2 Resultado de la actividad	41
3.1.1.1.2.1 Alcance	41

3.1.1.2 Actividad 1.2 Elaborar un plan de auditoría detallado, que incluya los objetivos, el alcance, los criterios de evaluación, el cronograma y los recursos necesarios.	42
3.1.1.2.1 Descripción de la actividad.....	42
3.1.1.2.2 Resultado de la actividad	43
3.1.1.2.2.1 Plan de auditoria	43
3.1.1.3 Actividad 1.3 Preparar los cuestionarios, listas de verificación y otros instrumentos necesarios para la recolección de datos durante la auditoría.	49
3.1.1.3.1 Descripción de la actividad.....	49
3.1.1.3.2 Resultado.....	50
3.1.1.3.2.1 Cuestionario día 1 de auditoria	50
3.1.1.3.2.2 Cuestionario día 2 de auditoria	53
3.1.1.3.2.3 Cuestionario día 3 de auditoria	55
3.1.1.3.2.4 Formato de revisión documental	63
3.1.1.3.2.5 Formato de lista de verificación	64
3.1.1.3.2.6 Formato de pruebas	100
3.1.1.3.2.7 Formato de remediación de hallazgos	101
3.1.1.3.2.8 Formato de informe de auditoria.....	101
3.1.1.3.2.9 Formato de informe de recomendación de remediación de hallazgos	103
3.1.1.3.2.10 Formato plan de acción.....	105
3.2 Objetivo 2 Ejecutar la Auditoria	107
3.2.1 Actividades	107
3.2.1.1 Actividad 2.1 Recolectar información y evidencias relevantes mediante entrevistas con el personal.....	107
3.2.1.1.1 Descripción de la actividad.....	107
3.2.1.1.2 Resultado de la actividad	108
3.2.1.1.2.1 Cuestionario día 1 de auditoria	108
3.2.1.1.2.2 Cuestionario día 2 de auditoria	117
3.2.1.1.2.3 Cuestionario día 3 de auditoria	123
3.2.1.2 Actividad 2.2 Revisar la documentación pertinente, como políticas de seguridad, procedimientos de gestión y registros de incidentes.	144
3.2.1.2.1 Descripción de la actividad.....	144
3.2.1.2.2 Resultado de la actividad	144
3.2.1.2.2.1 Revisión documental	144

3.2.1.3 Actividad 2.3 Analizar la relación entre la evidencia objetiva recopilada y los criterios establecidos, determinando el grado de conformidad o desviación respecto a los estándares y requerimientos predefinidos.	152
3.2.1.3.1 Descripción de la actividad.....	153
3.2.1.3.2 Resultado de la actividad	153
3.2.1.3.2.1 Lista de verificación	153
3.2.1.4 Actividad 2.4 Realizar pruebas con base en la información recabada en las entrevistas y la revisión documental, llevando a cabo un análisis más detallado al incumplimiento de los requisitos y/o controles.	252
3.2.1.4.1 Descripción de la actividad.....	253
3.2.1.4.2 Resultado de la actividad	253
3.2.1.4.2.1 Prueba: Partes interesadas	253
3.2.1.4.2.2 Prueba: Contacto con autoridades	255
3.2.1.4.2.3 Prueba: Seguridad en los proyectos	258
3.2.1.4.2.4 Prueba: Derechos ARCO	260
3.2.1.4.2.5 Prueba: Croquis de la organización	266
3.2.1.4.2.6 Prueba: Gestión del cambio	268
3.2.1.4.2.7 Prueba: Respaldos	272
3.2.1.4.2.8 Prueba: Transferencia de datos	274
3.2.1.4.2.9 Prueba: Seguridad de la información	278
3.2.1.4.2.10 Prueba: Requisitos contractuales	281
3.2.1.5 Actividad 2.5 Generar recomendaciones para abordar y remediar los hallazgos identificados durante la auditoría que no cumplan o cumplan parcialmente con los requisitos y controles predefinidos.	283
3.2.1.5.1 Descripción de la actividad.....	284
3.2.1.5.2 Resultado de la actividad	284
3.2.1.5.2.1 Recomendaciones de remediaciones	284
RESULTADOS	296
4.1 Objetivo 3 Entregar Resultados.....	297
4.1.1 Actividades	297
4.1.1.1 Actividad 3.1 Analizar y sintetizar los hallazgos de la auditoría en un informe final.....	297
4.1.1.1.1 Descripción de la actividad.....	297
4.1.1.1.2 Resultado de la actividad	297
4.1.1.1.2.1 Informe de auditoría	297

4.1.1.2 Actividad 3.2 Elaborar recomendaciones específicas sobre los hallazgos y mejorar las áreas identificadas.	307
4.1.1.2.1 Descripción de la actividad.....	307
4.1.1.2.2 Resultado de la actividad	308
4.1.1.2.2.1 Informe de recomendación de remediación de hallazgos.....	308
4.1.1.3 Actividad 3.3 Elaborar los planes de acción basados en los hallazgos y recomendaciones.	320
4.1.1.3.1 Descripción de la actividad.....	320
4.1.1.3.2 Resultado de la actividad	321
4.1.1.3.2.1 Plan de acción: Partes interesadas.....	321
4.1.1.3.2.2 Plan de acción: Contacto con autoridades.....	328
4.1.1.3.2.3 Plan de acción: Seguridad en los proyectos.....	332
4.1.1.3.2.4 Plan de acción: Derechos ARCO	337
4.1.1.3.2.5 Plan de acción: Croquis de la organización	341
4.1.1.3.2.6 Plan de acción: Gestión del cambio	347
4.1.1.3.2.7 Plan de acción: Respaldos	353
4.1.1.3.2.8 Plan de acción: Transferencia de información	359
4.1.1.3.2.9 Plan de acción: Seguridad de la información	366
4.1.1.3.2.10 Plan de acción: Requisitos contractuales.....	372
CONCLUSIONES	376
COMPETENCIAS DESARROLLADAS	378
FUENTES DE INFORMACIÓN.....	381
ANEXOS	382
Anexo 1: Carta de autorización del proyecto.....	382
Anexo 2: Contrato de confidencialidad.....	0

ÍNDICE DE TABLAS

Tabla 1 Aplicación ISO 27001 en las diferentes empresas	28
Tabla 1 Aplicación ISO 27001 en las diferentes empresas	29
Tabla 1 Aplicación ISO 27001 en las diferentes empresas	30
Tabla 2 Criterios de calificación de hallazgos	44
Tabla 3 Agenda del día 1 de auditoría	44
Tabla 4 Agenda del día 2 de auditoría	46
Tabla 5 Agenda del día 3 de auditoría	46
Tabla 6 Equipo auditor	47
Tabla 7 Formato de revisión documental	63
Tabla 8 Formato de Lista de verificación ISO/IEC 27001:2013	64
Tabla 8 (Continuación)	65
Tabla 8 (Continuación)	66
Tabla 8 (Continuación)	67
Tabla 8 (Continuación)	68
Tabla 8 (Continuación)	70
Tabla 8 (Continuación)	71
Tabla 8 (Continuación)	71
Tabla 8 (Continuación)	73
Tabla 8 (Continuación)	74
Tabla 8 (Continuación)	75
Tabla 8 (Continuación)	75
Tabla 8 (Continuación)	76
Tabla 8 (Continuación)	77
Tabla 8 (Continuación)	78
Tabla 8 (Continuación)	80
Tabla 8 (Continuación)	80
Tabla 8 (Continuación)	81
Tabla 8 (Continuación)	82
Tabla 8 (Continuación)	83
Tabla 8 (Continuación)	84
Tabla 8 (Continuación)	85
Tabla 8 (Continuación)	86
Tabla 8 (Continuación)	88
Tabla 8 (Continuación)	88
Tabla 8 (Continuación)	89
Tabla 8 (Continuación)	90
Tabla 8 (Continuación)	91
Tabla 8 (Continuación)	92
Tabla 8 (Continuación)	93
Tabla 8 (Continuación)	94
Tabla 8 (Continuación)	95
Tabla 8 (Continuación)	96

Tabla 8 (Continuación)	97
Tabla 8 (Continuación)	98
Tabla 8 (Continuación)	99
Tabla 9 Formato de pruebas	100
Tabla 9 Formato de pruebas(continuación)	100
Tabla 10 Formato de remediación de hallazgos	101
Tabla 11 Equipo auditor	102
Tabla 12 Hallazgos de la auditoria.....	102
Tabla 13 Resultados de la evaluación	102
Tabla 14 Autorización del informe	103
Tabla 15 Equipo auditor	104
Tabla 16 Recomendación de remediación de hallazgos de auditoria.....	104
Tabla 17 Autorización del informe	105
Tabla 18 Datos generales plan de acción	105
Tabla 19 Descripción del hallazgo plan de acción	106
Tabla 20 Plan de acción.....	106
Tabla 21 Evaluación del plan de acción.....	106
Tabla 22 Eficacia del plan de acción.....	107
Tabla 23 Revisión documental	144
Tabla 23 (Continuación)	145
Tabla 23 (Continuación)	146
Tabla 23 (Continuación)	147
Tabla 23 (Continuación)	148
Tabla 23 (Continuación)	149
Tabla 23 (Continuación)	150
Tabla 23 (Continuación)	151
Tabla 24 Lista de verificación ISO27001:2015.....	153
Tabla 24 (Continuación)	155
Tabla 24 (Continuación)	155
Tabla 24 (Continuación)	158
Tabla 24 (Continuación)	159
Tabla 24 (Continuación)	160
Tabla 24 (Continuación)	161
Tabla 24 (Continuación)	163
Tabla 24 (Continuación)	165
Tabla 24 (Continuación)	166
Tabla 24 (Continuación)	168
Tabla 24 (Continuación)	170
Tabla 24 (Continuación)	171
Tabla 24 (Continuación)	173
Tabla 24 (Continuación)	174
Tabla 24 (Continuación)	176
Tabla 24 (Continuación)	177
Tabla 24 (Continuación)	179

Tabla 24 (Continuación)	180
Tabla 24 (Continuación)	181
Tabla 24 (Continuación)	182
Tabla 24 (Continuación)	183
Tabla 24 (Continuación)	184
Tabla 24 (Continuación)	184
Tabla 24 (Continuación)	186
Tabla 24 (Continuación)	186
Tabla 24 (Continuación)	187
Tabla 24 (Continuación)	189
Tabla 24 (Continuación)	190
Tabla 24 (Continuación)	191
Tabla 24 (Continuación)	192
Tabla 24 (Continuación)	193
Tabla 24 (Continuación)	195
Tabla 24 (Continuación)	197
Tabla 24 (Continuación)	197
Tabla 24 (Continuación)	198
Tabla 24 (Continuación)	199
Tabla 24 (Continuación)	200
Tabla 24 (Continuación)	202
Tabla 24 (Continuación)	202
Tabla 24 (Continuación)	203
Tabla 24 (Continuación)	204
Tabla 24 (Continuación)	205
Tabla 24 (Continuación)	206
Tabla 24 (Continuación)	207
Tabla 24 (Continuación)	209
Tabla 24 (Continuación)	210
Tabla 24 (Continuación)	211
Tabla 24 (Continuación)	212
Tabla 24 (Continuación)	213
Tabla 24 (Continuación)	215
Tabla 24 (Continuación)	215
Tabla 24 (Continuación)	216
Tabla 24 (Continuación)	217
Tabla 24 (Continuación)	218
Tabla 24 (Continuación)	219
Tabla 24 (Continuación)	220
Tabla 24 (Continuación)	221
Tabla 24 (Continuación)	222
Tabla 24 (Continuación)	223
Tabla 24 (Continuación)	224
Tabla 24 (Continuación)	225

Tabla 24 (Continuación)	226
Tabla 24 (Continuación)	227
Tabla 24 (Continuación)	228
Tabla 24 (Continuación)	229
Tabla 24 (Continuación)	230
Tabla 24 (Continuación)	231
Tabla 24 (Continuación)	232
Tabla 24 (Continuación)	232
Tabla 24 (Continuación)	233
Tabla 24 (Continuación)	235
Tabla 24 (Continuación)	235
Tabla 24 (Continuación)	237
Tabla 24 (Continuación)	238
Tabla 24 (Continuación)	240
Tabla 24 (Continuación)	242
Tabla 24 (Continuación)	242
Tabla 24 (Continuación)	243
Tabla 24 (Continuación)	244
Tabla 24 (Continuación)	246
Tabla 24 (Continuación)	247
Tabla 24 (Continuación)	247
Tabla 24 (Continuación)	248
Tabla 24 (Continuación)	251
Tabla 24 (Continuación)	252
Tabla 25 Prueba partes interesadas.....	253
Tabla 26 Prueba contacto con autoridades	255
Tabla 27 Prueba seguridad en los proyectos	258
Tabla 28 Prueba derechos ARCO.....	260
Tabla 29 Prueba croquis de la organización.....	266
Tabla 30 Prueba gestión del cambio	268
Tabla 31 Prueba respaldos.....	272
Tabla 32 Prueba Transferencia de datos.....	274
Tabla 33 Prueba transferencia de información.....	278
Tabla 34 Prueba Requisitos contractuales	281
Tabla 35 Remediación de hallazgos	284
Tabla 35 (Continuación)	285
Tabla 35 (Continuación)	286
Tabla 35 (Continuación)	288
Tabla 35 (Continuación)	289
Tabla 35 (Continuación)	291
Tabla 35 (Continuación)	292
Tabla 35 (Continuación)	293
Tabla 35 (Continuación)	295
Tabla 36 Equipo auditor	298

Tabla 37 Hallazgos de la auditoria.....	298
Tabla 37 (Continuación)	299
Tabla 37 (Continuación)	300
Tabla 37 (Continuación)	301
Tabla 37 (Continuación)	302
Tabla 37 (Continuación)	303
Tabla 37 (Continuación)	304
Tabla 37 (Continuación)	305
Tabla 38 Resultados de la evaluación	306
Tabla 39 Autorización del informe	307
Tabla 40 Equipo auditor	308
Tabla 41 Recomendación de remediación de hallazgos de auditoria.....	309
Tabla 41 (Continuación)	310
Tabla 41 (Continuación)	312
Tabla 41 (Continuación)	313
Tabla 41 (Continuación)	314
Tabla 41 (Continuación)	316
Tabla 41 (Continuación)	317
Tabla 41 (Continuación)	319
Tabla 42 Autorización del informe	320
Tabla 43 Datos generales plan de acción 160	321
Tabla 44 Descripción del hallazgo plan de acción 160	321
Tabla 45 Plan de acción 160	322
Tabla 46 Evaluación del plan de acción 160.....	323
Tabla 47 Eficacia del plan de acción 160.....	323
Tabla 48 Datos generales plan de acción 161	328
Tabla 49 Descripción del hallazgo plan de acción 161	329
Tabla 50 Plan de acción 161	329
Tabla 51 Evaluación del plan de acción 161.....	330
Tabla 52 Eficacia del plan de acción 161.....	330
Tabla 53 Datos generales plan de acción 162	332
Tabla 54 Descripción del hallazgo plan de acción 162	333
Tabla 55 Plan de acción 162	334
Tabla 56 Eficacia del plan de acción 162.....	334
Tabla 57 Eficacia del plan de acción 162.....	334
Tabla 58 Datos generales plan de acción 163	338
Tabla 59 Descripción del hallazgo plan de acción 163	338
Tabla 60 Plan de acción 163	339
Tabla 61 Evaluación del plan de acción 163.....	339
Tabla 62 Evaluación del plan de acción 163.....	339
Tabla 63 Datos generales plan de acción 164	342
Tabla 64 Descripción del hallazgo plan de acción 164	342
Tabla 65 Plan de acción 164	343
Tabla 66 Evaluación del plan de acción 164.....	343

Tabla 67 Eficacia del plan de acción 164.....	343
Tabla 68 Datos generales plan de acción 165.....	347
Tabla 69 Descripción del hallazgo plan de acción 165.....	347
Tabla 70 Plan de acción 165.....	349
Tabla 71 Evaluación del plan de acción 165.....	350
Tabla 72 Eficacia del plan de acción 165.....	350
Tabla 73 Datos generales plan de acción 166.....	353
Tabla 74 Descripción del hallazgo plan de acción 166.....	354
Tabla 75 Plan de acción 166.....	355
Tabla 76 Evaluación del plan de acción 166.....	356
Tabla 77 Eficacia del plan de acción 166.....	356
Tabla 78 Datos generales plan de acción 167.....	359
Tabla 79 Descripción del hallazgo plan de acción 167.....	360
Tabla 80 Plan de acción 167.....	360
Tabla 81 Evaluación del plan de acción 167.....	362
Tabla 82 Eficacia del plan de acción 167.....	362
Tabla 83 Datos generales plan de acción 168.....	366
Tabla 84 Descripción del hallazgo plan de acción 168.....	367
Tabla 85 Plan de acción 168.....	368
Tabla 86 Evaluación del plan de acción 168.....	369
Tabla 87 Eficacia del plan de acción 168.....	369
Tabla 88 Datos generales plan de acción 169.....	372
Tabla 89 Descripción del hallazgo plan de acción 169.....	372
Tabla 90 Plan de acción 169.....	373
Tabla 91 Evaluación del plan de acción 169.....	374
Tabla 92 Eficacia del plan de acción 169.....	374
Tabla 93 Competencias.....	378

ÍNDICE DE FIGURAS

Figura 1 Ubicación de la empresa Soluciones Integrales SAYNET S.A. de C.V.	18
Figura 2 Organigrama Soluciones Integrales SAYNET S.A. de C.V.	19
Figura 3 Gestión de seguridad de la información	37
Figura 4 Portada manual de sistema de gestión integral.....	254
Figura 5 Formato de partes interesadas en el manual de sistema de gestión integral	255
Figura 6 Pestañas del registro matriz contacto autoridades	256
Figura 7 Portada del registro matriz de contacto con autoridades	257
Figura 8 Matriz de contactos de grupos especiales	257
Figura 9 Portada del formato evaluación de nuevos proyectos	259
Figura 10 Evaluación del proyecto "Instalación de memorias RAM y discos duros en servidores"	260
Figura 11 Carta de renuncia de Gabriel Arcega Soto	262
Figura 12 Solicitud de baja del biométrico de Gabriel Arcega Soto.....	263
Figura 13 Solicitud de baja de activos físicos y lógicos de Gabriel Arcega Soto.....	264
Figura 14 Aviso de privacidad firmado por Gabriel Arcega Soto	265
Figura 15 Portada del manual de sistema de gestión integral.....	267
Figura 16 Croquis oficina 13	268
Figura 17 Croquis oficina 11	268
Figura 18 Portada del procedimiento gestión del cambio	270
Figura 19 Información principal del cambio.....	271
Figura 20 Plan de implementación.....	271
Figura 21 Seguimiento y la evaluación que se llevara a cabo	271
Figura 22 Bitácora de respaldos	274
Figura 23 Datos de respaldo.....	274
Figura 24 Portada de Política convenio de confidencialidad	276
Figura 25 Índice de Política convenio de confidencialidad	276
Figura 26 Descripción de información confidencial en distintos niveles.	277
Figura 27 Información confidencial en distintos niveles.....	277
Figura 28 Riesgos y sanciones	277
Figura 29 Portada del plan de continuidad	280
Figura 30 Plan de continuidad.....	280
Figura 31 Procedimientos de respuesta.....	280
Figura 32 Plan de continuidad.....	281
Figura 33 Matriz de cumplimiento	283
Figura 34 Contenido matriz de cumplimiento	283
Figura 35 Portada del manual del sistema de gestión integral	324
Figura 36 Matriz de partes interesadas del manual del sistema integral	325
Figura 37 Matriz de partes interesadas del manual del sistema integral	326
Figura 38 Matriz de partes interesadas del manual del sistema integral	327
Figura 39 Política de partes interesadas del manual del sistema integral.....	328
Figura 40 Portada del registro matriz de contacto con autoridades	331
Figura 41 Pestañas del registro matriz de contacto con autoridades.....	331
Figura 42 Matriz de contacto con autoridades	332
Figura 43 Portada del documento evaluación de nuevos proyectos.....	335

Figura 44 Formato actualizado de evaluación de nuevos proyectos.....	336
Figura 45 Evaluación del proyecto "Instalación de memorias RAM y discos duros en servidores".....	337
Figura 46 Formato de carta de derechos ARCO.....	341
Figura 47 Portada del manual de sistema de gestión integral.....	345
Figura 48 Croquis oficina 11 actualizado.....	346
Figura 49 Croquis oficina 13 actualizado.....	347
Figura 50 Portada procedimiento gestión del cambio.....	351
Figura 51 Procedimiento gestión del cambio.....	352
Figura 52 Procedimiento gestión del cambio.....	353
Figura 53 Procedimiento gestión del cambio.....	353
Figura 54 Portada bitácora de respaldos	357
Figura 55 Bitácora de respaldos.....	358
Figura 56 Bitácora de respaldos.....	359
Figura 57 Portada del convenio de confidencialidad	363
Figura 58 índice convenio de confidencialidad	364
Figura 59 Convenio de confidencialidad	365
Figura 60 Convenio de confidencialidad	366
Figura 61 Convenio de confidencialidad	366
Figura 62 Portada plan de continuidad	370
Figura 63 Plan de continuidad.....	371
Figura 64 Plan de continuidad.....	371
Figura 65 Plan de continuidad.....	372
Figura 66 Portada matriz de cumplimiento	375
Figura 67 Matriz de cumplimiento	376
Figura 68 Carta de autorización del proyecto	382
Figura 69 Convenio de confidencialidad declaraciones	0
Figura 70 Declaraciones	1
Figura 71 Clausulas.....	2
Figura 72 Clausulas segunda parte.....	3
Figura 73 Clausulas Ultima Parte	4
Figura 74 Firmas Contrato de confidencialidad	5

CAPÍTULO I

GENERALIDADES DEL PROYECTO

1.1 INTRODUCCIÓN

El presente informe se centra en un análisis exhaustivo del cumplimiento normativo de la empresa SayNet Soluciones Integrales S.A. de C.V. en relación con el estándar internacional ISO 27001:2015, específicamente en el ámbito de la seguridad de la información. En un mundo empresarial caracterizado por la rápida evolución tecnológica y la creciente interconexión digital, la protección de la información se erige como uno de los pilares fundamentales para la continuidad y el éxito de las organizaciones. En este contexto, cumplir estándares ISO 27001 es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información y mitigar los riesgos asociados a la seguridad cibernética y preservar la confianza de los clientes. Este informe se propone evaluar el grado de adhesión de SayNet Soluciones Integrales S.A. de C.V. a los requisitos establecidos por la normativa ISO 27001, a través de un análisis riguroso y detallado de su sistema de gestión integral en relación con los principios y mejores prácticas establecidos por dicho estándar internacional.

La relevancia de este estudio radica en la importancia estratégica que posee la seguridad de la información en el contexto empresarial actual, donde la protección de los activos de información es crucial para salvaguardar la confianza de los clientes y preservar la reputación de la organización. En este sentido, el cumplimiento de estándares internacionales como ISO 27001 se presenta como un factor determinante para garantizar la seguridad y la confidencialidad de la información en las empresas.

El informe se organiza en cuatro capítulos que abarcan distintos aspectos relacionados con la auditoría de cumplimiento normativo. En primer lugar, se exponen las generalidades del proyecto, proporcionando un contexto sobre la empresa y delineando los objetivos específicos de la auditoría. Posteriormente, se ofrece un marco teórico que comprende conceptos fundamentales sobre seguridad de la información, los principios de la norma ISO 27001 y las metodologías de auditoría de cumplimiento. En el tercer capítulo, se detalla el proceso de auditoría, describiendo con detalle la metodología empleada, que incluye listas de cotejo, entrevistas, cuestionarios. Por último, se presentan los resultados obtenidos de la auditoría, destacando los hallazgos más relevantes, las áreas de conformidad y las recomendaciones para la mejora continua del sistema de gestión integral.

Hay limitaciones identificadas en el proceso de auditoría, como el conocimiento limitado de los nuevos colaboradores respecto al sistema de gestión integral, lo que puede haber impactado en la evaluación exhaustiva de ciertas áreas. No obstante, se confía en que este informe contribuirá significativamente a fortalecer el compromiso de la empresa con la seguridad de la información y a orientar acciones concretas para alcanzar un mayor nivel de cumplimiento normativo.

1.2 DESCRIPCIÓN DE LA EMPRESA

1.2.1 Nombre, razón social

Soluciones Integrales SAYNET S.A. de C.V.

1.2.2 Ubicación

Cto Dramaturgos 47, Cd. Satélite, 53100 Naucalpan de Juárez, Méx.

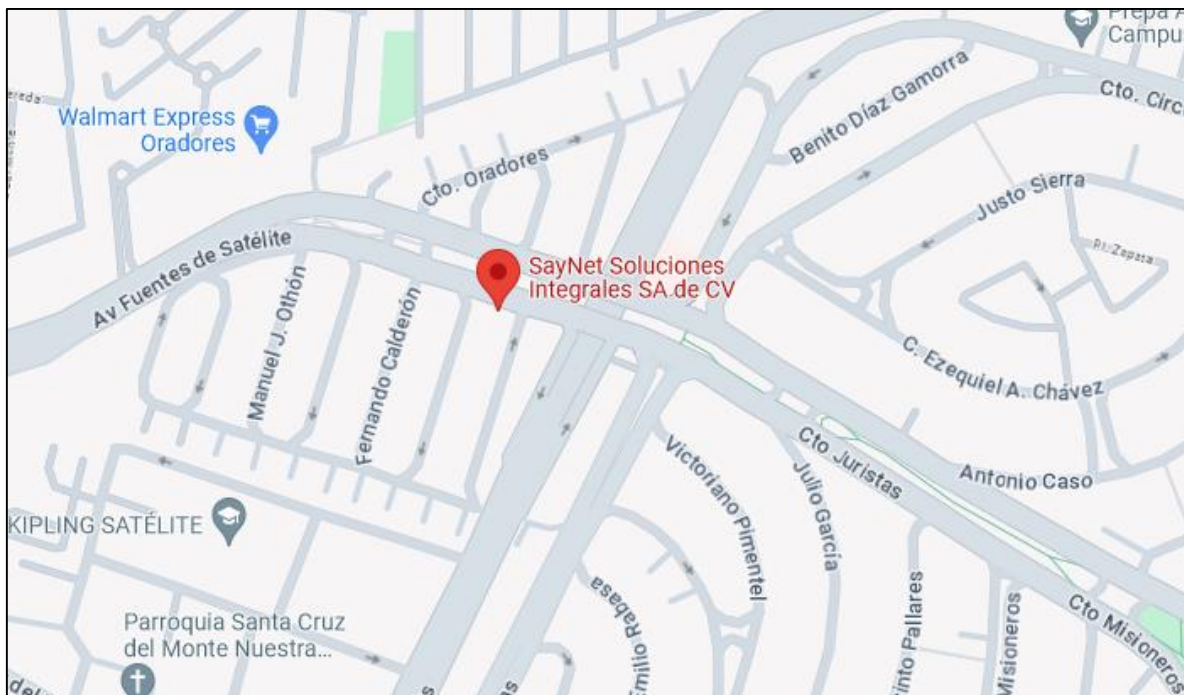


Figura 1 Ubicación de la empresa Soluciones Integrales SAYNET S.A. de C.V.

1.2.3 Organigrama

AVISO DE CONFIDENCIALIDAD y TRATAMIENTO DE LA INFORMACIÓN

La información que a continuación se muestra puede ser utilizada por las interesadas únicamente para complementar las evidencias de residencias profesionales, ningún nombre de persona ni empresa que no sea de la unidad de negocio (Trezentos) puede ser referida en este documento.

El punto de contacto de la unidad económica (Trezentos) para fin de aclaraciones es vania.carvalho@trezentos.mx / director de Implementación de la organización para la que las estudiantes Brenda Itzel Gante Sánchez y Lizeth Viridiana Gutiérrez Guerra ejecutan sus prácticas profesionales.

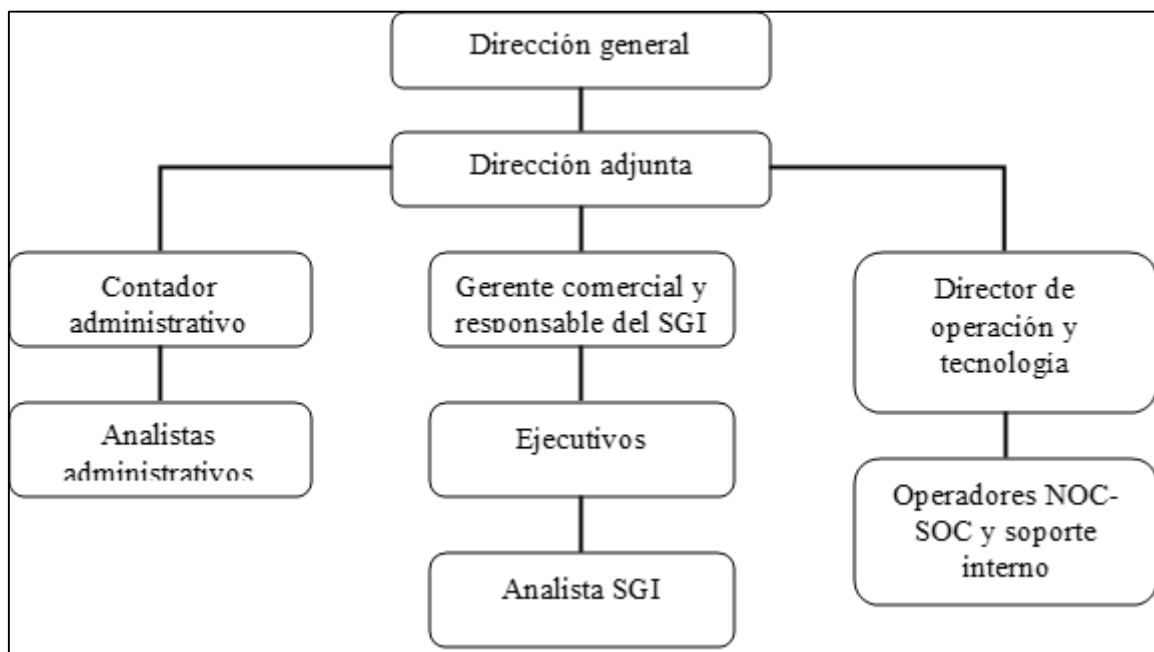


Figura 2 Organigrama Soluciones Integrales SAYNET S.A. de C.V.

1.2.4 Sector productivo de la empresa

Ejecutar servicios de SOC (Centro de Operaciones de Seguridad) - NOC (Centro de Operaciones de Red) a gobierno y empresas privadas.

1.2.5 Misión, Visión, Filosofía y/o Valores

1.2.5.1 Misión

Soluciones integrales de TI, confiables e innovadoras hechas a tu medida.

1.2.5.2 Visión

Ser una institución consolidada y reconocida con colaboradores apasionados por su trabajo que logren un equilibrio en el ámbito personal y profesional que permita a la institución un crecimiento sostenido e innovador como asociado estratégico de negocio.

1.2.5.3 Filosofía y/o Valores

- Lealtad
- Honorabilidad y palabra
- Agradecimiento y empatía
- Pasión y compromiso
- Sinergia
- Confianza
- Innovación
- Resiliencia
- Desarrollar a otros / liderar

1.2.6 Breve historia de la empresa.

Sayten es una empresa 100% mexicana, integradora de servicios administrados de TI que cuenta con personal altamente capacitado y tecnologías de vanguardia, con una trayectoria y experiencia de más de 19 años en el mercado, otorgando servicios a clientes del sector gubernamental y empresas AAA de iniciativa privada.

Fue creada en 2004 y empezó operaciones en 2005, en este año se enfocaron en la comercialización de consumibles refacciones, computo e impresión donde su primer cliente de gobierno fue el Instituto Nacional de Ecología y Cambio Climático.

En el 2007 realizaron una alianza estratégica con Sistemas Especializados Brain y Document Plus, así mismo renovaron la plataforma de cómputo e impresión de CONAFE a nivel Nacional.

En septiembre de 2008 se incorporó el Ing. Adolfo Tolentino López como director general.

Entre el 2009 y 2010 incorporaron una oferta de valor de infraestructura y conectividad para redes de datos, se cambio toda la red de Fibra óptica e infraestructura de la red de Datos de la Dirección General de Televisión Educativa.

En el 2011 incorporaron los servicios administrados de Redes de Datos ala Oferta de valor de Saynet y obtienen su primer cliente en su modalidad por 3 años para la secretaria de Turismo, incorporaron una cartera de clientes a el ISSSTE y renovaron su imagen corporativa.

En el 2012 realizaron una alianza estratégica con Alestra de grupo ALFA, incorporaron servicios administradores de seguridad informática y redes de datos, dirección general y televisión educativa.

En el 2013 y 2014 adquirieron oficinas en Ciudad Satélite, ganaron una licitación en lotería nacional, en el municipio de Atizapán y por último en seguridad informática y switching en OPMA.

En el 2016 y 2017 realizaron una alianza estratégica con tecnologías de la información América, así mismo construyeron e implementaron SOC-NOC HOURS, incorporaron su cartera de clientes a SEMARNAT y SEP por último duplicaron la facturación y pasaron la barrera de los 5MDD anuales de facturación.

En el 2018 y 2019 realizaron una alianza estratégica con Bestel de Grupo TELEVISA, así mismo incorporaron su cartera de clientes a Pemex, gobierno de Tamaulipas Michoacán, Nissan y Toyota por último certificaron el SOC-NOC HOURS en ISO 2000 y 27001.

En el 2020 incorporaron su cartera de clientes a INFONAVIT, IMSS y Corporativo Hospital Satélite e implementaron una nueva mesa de ayuda y un SIEM de nueva generación en el SOC-NOC HOURS. (Desconocido, 2021)^[BG4]

1.3 PROBLEMA A RESOLVER

En un mundo cada vez más digitalizado, la seguridad de la información se ha convertido en una prioridad crítica para las organizaciones de todos los tamaños y sectores. La gestión adecuada de la información no solo protege los datos sensibles, sino que también preserva la integridad y la reputación de la empresa. Las brechas de seguridad, los ataques cibernéticos y la gestión inadecuada de datos pueden resultar en pérdidas financieras significativas, daños a la reputación y la pérdida de confianza de los clientes.

Las organizaciones enfrentan diversos riesgos, incluyendo:

- **Amenazas Internas y Externas:** Los empleados pueden representar un riesgo tanto intencionado como accidental, y las amenazas externas, como los ciberataques, son cada vez más sofisticadas.
- **Cumplimiento Normativo:** Las empresas deben cumplir con diversas regulaciones y normativas que exigen la protección de datos, lo que hace necesario implementar un sistema robusto de gestión de la seguridad de la información.
- **Confianza del Cliente:** Los clientes son cada vez más conscientes de la importancia de la privacidad de sus datos. La confianza en la capacidad de una organización para proteger su información es un factor determinante en la decisión de hacer negocios.

A pesar de la creciente importancia de la seguridad de la información, muchas empresas, incluyendo SayNet Soluciones Integrales S.A. de C.V., aún enfrentan desafíos significativos en este ámbito. La empresa maneja información sensible y valiosa, lo que la expone a diversos riesgos de seguridad cibernética. La falta de un sistema de gestión de seguridad de la información robusto podría resultar en consecuencias graves, tales como:

- **Riesgo de Brechas de Seguridad:** Sin controles adecuados, la empresa está en una posición vulnerable ante posibles brechas, lo que podría resultar en la pérdida de datos críticos y un daño irreversible a su reputación.
- **Pérdida de Clientes y Oportunidades de Negocio:** La falta de una certificación reconocida, como la ISO 27001, podría llevar a la desconfianza por parte de los

clientes actuales y potenciales, lo que podría traducirse en pérdida de oportunidades de negocio.

- **Sanciones Legales y Multas:** No cumplir con regulaciones y leyes relacionadas con la seguridad de la información puede acarrear sanciones y multas que afectarían tanto la situación financiera como la imagen de la empresa.

Dada la necesidad de una sólida gestión de la seguridad de la información, se propone llevar a cabo una auditoría interna en SayNet Soluciones Integrales S.A. de C.V. con el objetivo de evaluar y certificar el cumplimiento de la norma ISO 27001. Esta norma proporciona un marco estructurado que permite a las organizaciones establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI).

La implementación de ISO 27001 no solo protegerá los activos de información de la empresa, sino que también fortalecerá su credibilidad y confianza ante los clientes, asegurará el cumplimiento de requisitos legales y normativos, y facilitará una gestión eficiente de los riesgos. A largo plazo, esto permitirá a SayNet posicionarse como un líder en la industria, comprometido con la seguridad y la confianza de sus clientes.^[BG5]

1.4 OBJETIVOS

1.4.1 Objetivo general

Realizar una Auditoría con ISO 27001 para cumplimiento normativo en la empresa SayNet Soluciones Integrales S.A. de C.V.

1.4.2 Objetivos específicos

1. Planificar la Auditoría

- ✓ Definir el alcance de la auditoría, identificando los controles de seguridad informática a evaluar.

- ✓ Elaborar un plan de auditoría detallado, que incluya los objetivos, el alcance, los criterios de evaluación, el cronograma y los recursos necesarios.
- ✓ Preparar los cuestionarios, listas de verificación y otros instrumentos necesarios para la recolección de datos durante la auditoría.

2. Ejecutar la Auditoria

- ✓ Recolectar información y evidencias relevantes mediante entrevistas con el personal y revisión de documentación.
- ✓ Revisar la documentación pertinente, como políticas de seguridad, procedimientos de gestión y registros de incidentes.
- ✓ Analizar la relación entre la evidencia objetiva recopilada y los criterios establecidos, determinando el grado de conformidad o desviación respecto a los estándares y requerimientos predefinidos.
- ✓ Realizar pruebas con base en la información recabada en las entrevistas y la revisión documental, llevando a cabo un análisis más detallado al incumplimiento de los requisitos y/o controles.
- ✓ Generar recomendaciones para abordar y remediar los hallazgos identificados durante la auditoría que no cumplan o cumplan parcialmente con los requisitos y controles predefinidos.

3. Entregar Resultados

- ✓ Analizar y sintetizar los hallazgos de la auditoría en un informe final.
- ✓ Elaborar recomendaciones específicas sobre los hallazgos y mejorar las áreas identificadas.
- ✓ Elaborar los planes de acción basados en los hallazgos y recomendaciones.

1.5 JUSTIFICACIÓN

La necesidad de llevar a cabo una auditoría interna en SayNet Soluciones Integrales S.A. de C.V. para evaluar y certificar el cumplimiento de la norma ISO 27001 se sustenta en diversos factores críticos que impactan directamente en la seguridad de la información. Los puntos más importantes por los cuales se realiza esta auditoría son:

Protección de Activos de Información:

La empresa maneja información confidencial tanto propia como de sus clientes. La implementación de ISO 27001 garantiza la aplicación de controles adecuados para proteger estos activos de información. La auditoría permitirá identificar áreas de vulnerabilidad y asegurar la implementación efectiva de medidas de seguridad.

Credibilidad y Confianza del Cliente:

La certificación ISO 27001 es un indicador clave de compromiso con la seguridad de la información. Contar con esta certificación mejora la credibilidad y confianza de los clientes al demostrar que SayNet Soluciones Integrales S.A. de C.V. toma en serio la protección de la información que maneja. La auditoría contribuirá a garantizar que los controles implementados cumplan con los estándares requeridos.

Cumplimiento Legal y Normativo:

En un entorno regulatorio en constante evolución, cumplir con requisitos legales y normativos relacionados con la seguridad de la información es crucial. La ISO 27001 proporciona un marco que ayuda a la empresa a adaptarse y cumplir con estas regulaciones. La auditoría asegurará que los controles estén alineados con los requisitos específicos del entorno legal y normativo.

Gestión Eficiente de Riesgos:

La norma ISO 27001 proporciona un marco estructurado para la identificación y gestión de riesgos de seguridad de la información. La auditoría permitirá evaluar la efectividad de la gestión de riesgos existente y propondrá mejoras para anticipar y mitigar posibles amenazas.

Consecuencias de la Falta de Implementación:

La falta de un sistema de gestión de seguridad de la información robusto aumenta el riesgo de brechas de seguridad. La auditoría, al identificar posibles deficiencias, contribuirá a evitar pérdidas de datos y daños a la reputación que podrían surgir de posibles violaciones de seguridad.

Pérdida de Clientes y Oportunidades de Negocio:

La certificación ISO 27001 se ha convertido en un requisito fundamental para muchos clientes que buscan socios comerciales confiables. La falta de certificación podría disuadir a los clientes potenciales y afectar las oportunidades de negocio. La auditoría permitirá abordar estas preocupaciones y fortalecer la posición competitiva de la empresa.

Sanciones Legales y Multas:

La no conformidad con regulaciones y leyes relacionadas con la seguridad de la información puede resultar en sanciones legales y multas significativas. La auditoría, al identificar áreas de no conformidad, ayudará a evitar estas consecuencias negativas, protegiendo así la situación financiera y la imagen de la empresa.

La auditoría propuesta es esencial para garantizar que SayNet Soluciones Integrales S.A. de C.V. no solo cumpla con los requisitos de la norma ISO 27001, sino que también fortalezca su postura en términos de seguridad de la información, ganando la confianza de los clientes y asegurando el cumplimiento continuo de las obligaciones legales y normativas.

CAPÍTULO II

MARCO TEÓRICO

2.1 Estado del arte

Tabla 1 Aplicación ISO 27001 en las diferentes empresas

Empresa	Sector	Estrategias/Técnicas	Resultados Obtenidos
AWS (Amazon Web Services)	Implementación en productos y servicios en la nube	Desarrollo de medidas de seguridad a nivel de infraestructura y aplicaciones específicamente diseñadas para proteger los servicios en la nube, cumpliendo con los estándares de seguridad de la ISO 27001 y otras certificaciones relevantes. Auditorías externas e internas para garantizar la conformidad con los estándares de seguridad.	Garantía de la seguridad y privacidad de los datos de los clientes que utilizan los servicios en la nube de AWS. Cumplimiento de estándares de seguridad globales. Confianza del cliente en la plataforma de servicios en la nube de AWS. (Desconocido, AWS, 2011)
Google Cloud Platform	Certificación para Google Cloud Platform	Implementación de medidas de seguridad específicas para la infraestructura de la Google Cloud Platform, cumpliendo con los requisitos de la ISO 27001 y otras certificaciones relevantes.	Protección efectiva de la información y datos de los clientes alojados en la Google Cloud Platform. Cumplimiento de estándares de seguridad reconocidos internacionalmente. Fortalecimiento de la confianza del cliente en la

	Participación en programas de divulgación de vulnerabilidades y auditorías de seguridad independientes.	plataforma de Google Cloud. (Desconocido, Google, 2014)
--	---	--

Tabla 2 Aplicación ISO 27001 en las diferentes empresas

(Continuación)

Empresa	Sector	Estrategias/Técnicas	Resultados Obtenidos
IBM	Aplicación en diversos servicios y soluciones.	Desarrollo de un enfoque integral de seguridad de la información basado en la ISO 27001, adaptado a una amplia gama de servicios y soluciones de IBM. Implementación de controles de seguridad avanzados y evaluación continua de riesgos y vulnerabilidades. Participación en estándares de la industria y grupos de trabajo relacionados con la seguridad.	Reducción de riesgos de seguridad en una amplia variedad de servicios y soluciones de IBM. Protección de la información y propiedad intelectual de los clientes. Cumplimiento de estándares y regulaciones de seguridad relevantes. (Desconocido, IBM, 2015)
AWS (Amazon)	Certificación para varios	Implementación de medidas de seguridad específicas para varios	Garantía de la seguridad y privacidad de los datos de los clientes que utilizan una

servicios en la nube.	servicios en la nube de AWS, cumpliendo con los requisitos de la ISO 27001 y otras certificaciones relevantes. Auditorías externas e internas para garantizar la conformidad con los estándares de seguridad.	variedad de servicios en la nube de AWS. Cumplimiento de estándares de seguridad globales. Confianza del cliente en la seguridad de los servicios en la nube de AWS. (Desconocido, AWS, 2011)
-----------------------	---	---

Tabla 3 Aplicación ISO 27001 en las diferentes empresas

(Continuación)

Empresa	Sector	Estrategias/Técnicas	Resultados Obtenidos
Banco Santander	Implementación en el sector financiero.	Desarrollo de un sistema de gestión de seguridad de la información (SGSI) basado en la ISO 27001, adaptado a las necesidades y regulaciones específicas del sector financiero. Implementación de controles de seguridad específicos para proteger la información financiera confidencial. Capacitación del personal en prácticas de	Protección efectiva de la información financiera confidencial de los clientes. Cumplimiento de regulaciones bancarias y estándares de seguridad. Reducción de riesgos de fraude y violación de datos. Fortalecimiento de la confianza del cliente y la reputación de la marca en el sector financiero. (Desconocido, Banco Santander, 2017)

		seguridad. Monitoreo continuo y auditorías internas y externas.	
--	--	---	--

[BG6] 2.2 Marco conceptual

La planificación y ejecución de una Auditoría ISO 27001 en SayNet Soluciones Integrales S.A. de C.V. implican una serie de términos interconectados, cada uno esencial para alcanzar el objetivo general de cumplimiento normativo en seguridad informática.

En este contexto, el **cumplimiento normativo** se refiere al conjunto de acciones y medidas que una organización toma para asegurar que sus prácticas y operaciones cumplan con las normas y regulaciones establecidas, específicamente en el ámbito de la seguridad informática. (Estevez, 2024)

Durante la fase de **planificación de la auditoría**, se define el alcance y los objetivos específicos. Aquí, el alcance aborda la extensión de la evaluación, identificando los controles de seguridad informática a examinar. Los objetivos establecen metas claras, y la revisión de documentación, como políticas de seguridad y procedimientos, proporciona un contexto normativo y operativo. (Gironzini, 2016)

La elaboración de un **plan de auditoría** detallado incluye la definición de objetivos, alcance, cronograma y recursos necesarios. Se preparan cuestionarios, listas de verificación y otros instrumentos para garantizar una recolección eficiente de datos durante la auditoría. (Ramirez, 2021)

Durante la fase de ejecución de la auditoría, se procede con la implementación de una **lista de verificación** para recopilar información y evidencia relevante. Esta **lista de verificación** comprende puntos específicos que deben ser corroborados y cumplidos durante el proceso de auditoría. Se realiza una revisión exhaustiva del cumplimiento de cada uno de los elementos enlistados en la lista mediante inspecciones visuales, verificación de documentación y entrevistas con el personal pertinente. (Melo, 2021) Además, se utiliza la **lista de verificación** para identificar áreas de cumplimiento satisfactorio y posibles áreas de mejora o no conformidad. Este enfoque sistemático asegura que ningún aspecto crítico sea pasado por alto durante la auditoría y facilita la posterior evaluación de riesgos y formulación de recomendaciones para mejorar el desempeño organizacional.

La evaluación de **pruebas**, se abordan aspectos relacionados con el acceso físico, acceso lógico y protección de datos. Este proceso implica realizar pruebas directas sobre dispositivos

y procedimientos para salvaguardar el acceso físico y digital y aplicar medidas que garanticen la confidencialidad, integridad y disponibilidad de los datos. Este enfoque de pruebas directas permite identificar posibles vulnerabilidades y evaluar la efectividad de los sistemas de seguridad implementados. (Desconocido, pmg-ssi, 2018)

La verificación del **cumplimiento de políticas** de seguridad se extiende a políticas y procedimientos, como políticas de control de acceso, normativas de seguridad, políticas de contraseñas y directrices de autenticación. (Desconocido, Linked in, 2023)

La fase final, para entregar resultados, consiste en **analizar y sintetizar hallazgos**, dando una visión de la situación. Se elaboran recomendaciones específicas destacando áreas de mejora y proponiendo soluciones concretas para garantizar un adecuado cumplimiento normativo en seguridad informática. (Desconocido, Red Hat, 2023)

Dentro de este proceso, se integra la fase de **plan de acción**, que se desarrolla posteriormente a la fase de evaluación y entrega de resultados. Esta etapa se enfoca en priorizar, definir, implementar, monitorear y ajustar acciones correctivas y preventivas para abordar los hallazgos identificados durante la auditoría, garantizando así una mejora continua en el cumplimiento normativo en seguridad informática. (Deming, 2014)^[BG7]

2.3 Marco metodológico

ISO/IEC 27001

Es una norma internacional creada por la Organización Internacional de Normalización (ISO) para garantizar buenas prácticas de seguridad de la información. Además, la norma ISO 27001 brinda herramientas que permiten a las empresas gestionar su información de manera segura.

Este estándar internacional se creó, entre otras razones, para proporcionar a las organizaciones un modelo consistente que permita establecer, implementar, monitorear, revisar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).

En 2005 fue publicada su primera versión, enfocada en la norma británica BS 7799-2, y en 2013 fue actualizada ajustándose a las novedades tecnológicas del mercado y basándose en normas como ISO/IEC 17799:2005, ISO 13335, ISO/IEC TR 18044:2004 y las directrices de la Organización para la Cooperación y el Desarrollo Económico (Ocde) para la seguridad de sistemas y redes de información. Esta norma puede aplicarse a cualquier tipo de empresa, sin importar su industria o tamaño. (Limited, 2011)

¿Qué temas aborda?

Objeto y campo de la aplicación: brinda las herramientas para saber cómo es el uso de la norma, qué beneficios trae y cómo debes aplicarla.

Referencias normativas: son los documentos que debes tener en cuenta para aplicar las recomendaciones de la norma.

Términos y definiciones: es un glosario que te permite entender las palabras claves de lo que está descrito allí.

Contexto de la organización: es uno de los requisitos fundamentales de la norma. Busca entender el contexto de la empresa y sus necesidades para verificar el alcance del Sistema de Gestión de Seguridad de la Información que se pondrá en marcha.

Liderazgo: es importante generar una cultura en la compañía alrededor de la seguridad de la información, por eso, todos los empleados deben saber los planes de acción que se llevarán a cabo y de qué manera contribuyen a su cumplimiento. Por eso, es clave que los líderes de la empresa nombren responsables y den a conocer oportunamente las políticas establecidas

Planificación: aquí debes establecer los objetivos y el camino para lograrlos, cómo será la implementación del Sistema de Gestión de Seguridad de la Información considerando los riesgos identificados.

Soporte: para el adecuado funcionamiento del sistema debes contar con los recursos necesarios que les permitan ser competentes, contar con una óptima comunicación y documentar la información requerida para cada caso.

Operación: para tener una gestión eficaz debes planificar, implementar, monitorear y controlar cada proceso, valorar cada riesgo y crear una solución para cada uno.

Evaluación de desempeño: debes realizar el seguimiento, la medición, el análisis y la evaluación del sistema implementado para verificar que se cumple con lo establecido.

Mejora: Se trata de identificar qué aspectos no están funcionando correctamente para poder ajustarlos y cumplir con su objetivo final. (Limited, 2011)

¿Qué temas resuelve?

- Obtener un diagnóstico mediante entrevistas.
- Realizar un análisis exhaustivo de todos los riesgos que se puedan presentar.
- Crear un plan de acción acorde a las necesidades puntuales de la empresa.
- Diseñar procedimientos.
- Entender los requerimientos de seguridad de la información y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.

- Monitorear y revisar el desempeño y la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI).
- Favorecer el mejoramiento continuo según la medición del objetivo.

Principales ventajas al implementar ISO 27001

Las ventajas que proporciona implementar ISO 27001 son muchas, sin embargo, existen 4 ventajas comerciales esenciales en la seguridad de la información:

Cumplir con los requisitos legales: Con el creciente número de leyes, regulaciones y requisitos contractuales relacionados con la seguridad de la información, implementar ISO 27001 proporciona una metodología efectiva para cumplir con estos requisitos, simplificando la gestión y garantizando el cumplimiento normativo.

Ventaja competitiva: Obtener la certificación puede conferir una ventaja comercial significativa. Si su empresa cuenta con la certificación ISO 27001 y sus competidores no, es probable que obtenga una posición favorable ante los clientes preocupados por mantener segura su información.

Reducción de costos: La filosofía central de ISO 27001 se centra en prevenir incidentes de seguridad. Cada incidente, ya sea grande o pequeño, implica costos. Al evitar estos incidentes, la empresa logra ahorros sustanciales. Además, la inversión en la implementación de ISO 27001 suele ser considerablemente menor que los costos asociados con los incidentes de seguridad.

Mejora de la organización: La implementación de ISO 27001 no solo se trata de seguridad de la información, sino que también fomenta la documentación y definición de procesos y procedimientos, incluso aquellos no directamente relacionados con la seguridad. Esto contribuye a una mejor organización interna, reduce la incertidumbre entre los empleados y optimiza la eficiencia al reducir el tiempo perdido. (Desconocido, GlobalSuite, 2023)

Intervención a la gestión de seguridad de la información

La seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información (Deming, 2014):



Figura 3 Gestión de seguridad de la información[BG8]

2.4 Estructura de ISO 27001

ISO/IEC 27001 se estructura en 11 secciones, además del Anexo A. Las secciones 0 a 3 son introductorias y no son obligatorias para la implementación, mientras que las secciones 4 a 10 son obligatorias. Esto implica que una organización debe implementar todos los requisitos de las secciones 4 a 10 para cumplir con la norma. Los controles del Anexo A solo deben implementarse si se determina que son aplicables en la Declaración de Aplicabilidad.

La estructura de las secciones de ISO 27001 sigue los principios del Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización. Esto significa que los títulos de las secciones son los mismos que los de otras normas de gestión, como ISO 22301:2012 y la nueva ISO 9001:2015. Esta alineación facilita la integración de estas normas, lo que puede simplificar el proceso para las organizaciones que buscan implementar varios sistemas de gestión.

Sección 0 – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.

Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.

Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 – Términos y definiciones – de nuevo, hace referencia a la norma ISO/IEC 27000.

Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.

Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Anexo A – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18). (Limited, 2011)^[BG9]

CAPÍTULO III

DESARROLLO

Objetivo 3 Planificar la Auditoria

El objetivo de planificar la auditoría es diseñar y organizar un marco de trabajo que permita llevar a cabo una revisión integral y efectiva de la evidencia. La planificación asegura que la auditoría se realice de manera estructurada, en línea con la norma ISO 27001 que se enfoque en áreas de riesgo significativo.

3.1.1 Actividades

3.1.1.1 Actividad: Definir el alcance de la auditoría, identificando los controles de seguridad informática a evaluar.

Determinar qué aspectos o áreas específicas del departamento se van a evaluar, identificando los controles que serán objeto de revisión.

3.1.1.1.1 Descripción de la actividad

En el alcance de la auditoria se considera la definición con el sistema cuando trabajan con varias normas ISO se implementa un sistema de gestión integral y, si trabajamos con una norma, implementamos un sistema de gestión, se considera el área donde se realizará la auditoria, la empresa debe definirse considerando el nombre de lugar y ubicación real de esta área, así como las políticas y documentos implementados durante el proceso por medio de una entrevista.

3.1.1.1.2 Resultado de la actividad

3.1.1.1.2.1 Alcance

Revisar y evaluar el Sistema de Gestión Integral implementado en el SOC-NOC HORUS, incluyendo los procedimientos, políticas, manuales, anexos, formatos declarados e implementados en los servicios de mesa de ayuda, monitoreo, en sus procesos de atención de incidentes y solicitudes de servicio, atención de problemas, niveles de servicio, procesos de servicios nuevos o modificados, y en todos sus procesos de gestión del servicio y seguridad

de la información, ofrecidos por su SOC-NOC Horus, así como, la protección de recursos, servicios y partes interesadas.

3.1.1.2 Actividad 1.2 Elaborar un plan de auditoría detallado, que incluya los objetivos, el alcance, los criterios de evaluación, el cronograma y los recursos necesarios.

3.1.1.2.1 Descripción de la actividad

Implica la creación de un plan completo que establezca los objetivos de la auditoría, el alcance, los criterios de evaluación, el cronograma y los recursos necesarios para llevar a cabo la auditoría de manera eficiente.

Para realizar un plan de auditoría se considera lo que es un criterio de auditoría, este debe contener con que norma ISO se trabajará como lo menciona dentro del plan la norma ISO 27001:2015, después lo que vamos a considerar es el alcance algo que tenemos que considerar, cuando se trabaja con más de una norma implementamos un sistema de gestión integral cuando es una sola norma solo es un sistema de gestión, así como el área donde se implementará debe definirse por la propia empresa.

Dando continuidad para los requisitos se debe considerar el anexo SL este anexo es una estructura de alto nivel de las normas ISO que estos manejan requisitos en general como los son:

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación

9. Evaluación de rendimiento

10. Mejora

Este anexo SL es más conocido como cláusulas, complementando con los otros requisitos que son parte del sistema gestión, para finalizar solo se consideran los auditores encargados los días en los que se llevara a cabo dicha auditoría y los horarios.

3.1.1.2.2 Resultado de la actividad

3.1.1.2.2.1 Plan de auditoria

1. Alcance

Revisar y evaluar el Sistema de Gestión Integral implementado en el SOC-NOC HORUS, incluyendo los procedimientos, políticas, manuales, anexos, formatos declarados e implementados en los servicios de mesa de ayuda, monitoreo, en sus procesos de atención de incidentes y solicitudes de servicio, atención de problemas, niveles de servicio, procesos de servicios nuevos o modificados, y en todos sus procesos de gestión del servicio y seguridad de la información, ofrecidos por su SOC-NOC Horus, así como, la protección de recursos, servicios y partes interesadas.

2. Objetivo

Verificar si el Sistema de Gestión Integral implementado en la organización es conforme a los requisitos de las normas ISO/IEC 27001:2013 y Anexo A.

3. Criterios

El presente plan de auditoría toma como criterio principal, los requisitos de la norma ISO/IEC 27001:2013 y Anexo A, mismos que se detallan en el punto 6 (agenda) de este documento.

4. Criterios de calificación de hallazgos

Los criterios que se emplearán para la calificación de los hallazgos identificados durante el proceso de auditoría son:

Tabla 4 Criterios de calificación de hallazgos[BG10]

Criterio	Descripción
Conforme	El auditado presenta evidencia correspondiente para sustentar el cumplimiento de algún requisito estipulado por los criterios de referencia.
No Conforme	El auditado no presenta evidencia de cumplimiento contra los requisitos estipulados por los criterios de referencia. La desviación identificada representa un riesgo alto para la organización. La desviación identificada es igual o mayor al 26 % de la muestra solicitada.
Observación	El auditado presenta evidencia parcial de cumplimiento contra los requisitos estipulados por los criterios de referencias. La desviación identificada NO representa un riesgo alto para la organización. La desviación identificada es menor o igual al 25 % de la muestra solicitada.
No Revisado	Aplica cuando, en el ejercicio de auditoría no se tiene planificada la revisión de algún requisito proceso o documento del SG.

5. Área(s) a auditar

Todas las áreas involucradas en el alcance del Sistema de Gestión Integral, incluyendo todas las políticas, procesos, formatos, registros y demás documentos declarados e implementados como parte del sistema de gestión.

6. Agenda

Tabla 5 Agenda del día 1 de auditoría

Horario	Procesos	Auditor(s)	Responsable(s)
---------	----------	------------	----------------

09:00 - 09:30	Reunión de apertura	BIGS LVGG	Todos los involucrados
09:30 - 10:30	Comprensión de la organización (4.1) Partes interesadas (4.2)	BIGS LVGG	Todos los involucrados
10:30 - 11:30	Alcance del SGI (4.3) Sistema de Gestión Integral (4.4)	BIGS LVGG	Todos los involucrados
11:30 - 12:30	Liderazgo (5.1) Política (5.2) Roles responsabilidades y autoridades (5.3)	BIGS LVGG	Todos los involucrados
12:30 - 13:30	Acciones para tratar riesgos y oportunidades (6.1) Evaluación de Riesgos de seguridad de la información (8.2) Tratamiento de riesgos de seguridad de la información (8.3)	BIGS LVGG	Todos los involucrados
13:30 - 14:30	Planificación de los objetivos (6.2) Planificación del SGI (6.3) Monitoreo, medición, análisis y evaluación (9.1) Revisión por dirección (9.3) Auditoría Interna (9.2) No conformidad y acción correctiva (10.1) Mejora continua (10.2)	BIGS LVGG	Todos los involucrados
Alimentos			
15:30 - 16:30	Recursos (7.1) Concientización (7.3) Comunicación (7.4)	BIGS LVGG	Todos los involucrados
16:30 - 17:30	Información documentada (7.5) Conocimiento (7.6)	BIGS LVGG	Todos los involucrados

17:30 - 18:30	Competencia (7.2)	BIGS	Todos los involucrados
	A.7 Seguridad en los recursos humanos	LVGG	

Tabla 6 Agenda del día 2 de auditoría

Horario	Procesos	Auditor(s)	Responsable(s)
09:00 - 10:30	Planificación y control operacional (8.1)	BIGS	Todos los
		LVGG	involucrados
10:30 - 12:00	A.15 Relación con proveedores	BIGS	Todos los
		LVGG	involucrados
ALIMENTOS			
16:30 - 17:30	Políticas de seguridad de la información (A.5, A.6, A.16)	BIGS	Todos los
		LVGG	involucrados

Tabla 7 Agenda del día 3 de auditoría

Horario	Procesos	Auditor(s)	Responsable(s)
9:00 - 10:30	A.17 Seguridad de la información en la continuidad del negocio	BIGS	Todos los
		LVGG	involucrados
10:30 - 11:30	Seguridad en las operaciones (A.12)	BIGS	Todos los
		LVGG	involucrados
11:30 - 12:30	Seguridad en las comunicaciones (A.13)	BIGS	Todos los
		LVGG	involucrados
ALIMENTOS			
13:30 - 14:30	Adquisición, desarrollo y mantenimiento de sistemas (A.14)	BIGS	Todos los
		LVGG	involucrados
16:00 - 16:30	Seguridad física y ambiental (A.11)	BIGS	Todos los
		LVGG	involucrados
16:30 - 17:00	Gestión de activos (A.8)	BIGS	Todos los
	Control de accesos (A.9)	LVGG	involucrados

17:00 - 17:30	Cumplimiento (A.18)	BIGS LVGG	Todos los involucrados
17:30 - 18:00	Cifrado (A.10)	BIGS LVGG	Todos los involucrados
18:00 - 18:30	Reunión de cierre entrega del informe	BIGS LVGG	Todos los involucrados

7. Equipo auditor

Para la presente auditoría, el equipo auditor estará conformado por:

Tabla 8 Equipo auditor

Nombre	Iniciales	Rol
Brenda Itzel Gante Sánchez	BIGS	Auditor en entrenamiento
Lizeth Viridiana Gutiérrez Guerra	LVGG	Auditor en entrenamiento

8. Método de auditoría

Los métodos que el equipo auditor podrá utilizar para la recopilación de información son:

- a) Entrevistas.
- b) Observaciones.
- c) Revisión de la información documentada.
- d) Resumen de datos, análisis e indicadores de desempeño.

Los métodos se aplicarán de forma remota en su totalidad.

9. Recursos

Para la correcta realización del ejercicio de auditoría conforme a lo planificado en la agenda es necesario que:

Para cada actividad programada se encuentre el personal responsable asignado formalmente dentro del SGSI.

La liga de acceso para la conexión será prevista por el responsable del sistema de gestión de seguridad de la información a través de correo electrónico.

Que cada persona asignada para participar en cada actividad planificada en la agenda deberá asegurarse de contar con conexión a internet estable, energía eléctrica de fácil acceso, batería al 100 %, acceso a la información que presentará de acuerdo a la actividad programada y un espacio libre de interrupciones.

Todos los recursos que el auditado determine necesarios para realizar las actividades planificadas en la agenda, sin interrupciones.

10. Informe de auditoría

Una vez finalizado el ejercicio de auditoría, el equipo auditor elaborará el informe de auditoría correspondiente, mismo que deberá contener los hallazgos, recomendaciones y conclusiones de la auditoría, será firmado y entregado por el auditor líder al responsable del SGSI o a la lista de distribución que proporcione este último.

11. Observaciones

Idioma de trabajo y del informe: El proceso de auditoría será llevado a cabo en su totalidad en español.

Si existen observadores deberán notificarse su participación al equipo auditor a más tardar al inicio de la auditoría interna.

A fin de proteger la confidencialidad de la información, las sesiones de auditoría no podrán ser grabadas bajo ninguna circunstancia, por ninguna de las partes involucradas (auditor ni auditado).

3.1.1.3 Actividad 1.3 Preparar los cuestionarios, listas de verificación y otros instrumentos necesarios para la recolección de datos durante la auditoría.

3.1.1.3.1 Descripción de la actividad

Esto incluye la preparación de cuestionarios, listas de verificación y otros instrumentos que serán utilizados para recopilar datos y evidencias durante la auditoría.

La preparación de cuestionarios, listas de verificación y otros instrumentos para la recolección de datos durante una auditoría es un paso crítico que garantiza el proceso de auditoría. Esta actividad implica varios pasos importantes:

1. **Identificación de requisitos de información:** Comprender los objetivos y el alcance de la auditoría es fundamental para determinar qué información es necesaria recopilar. Esto implica definir claramente los criterios de evaluación, las áreas de enfoque y las preguntas clave que deben responderse durante la auditoría.
2. **Diseño de cuestionarios y listas de verificación:** Una vez que se han identificado los requisitos de información, se procede al diseño de los instrumentos de recolección de datos. Los cuestionarios consisten en una serie de preguntas estructuradas que se utilizan para recopilar información de manera sistemática, mientras que las listas de verificación enumeran los elementos específicos que deben verificarse o evaluarse durante la auditoría.
3. **Selección de formatos y métodos:** Es importante elegir los formatos adecuados para los cuestionarios y listas de verificación, teniendo en cuenta factores como la facilidad de uso, la claridad de las instrucciones y la capacidad de capturar la información requerida de manera precisa. Además, se decide si estos instrumentos se administrarán de forma física o electrónica, dependiendo de la naturaleza de la auditoría y los recursos disponibles.
4. **Elaboración de preguntas y elementos de verificación:** Se redactan las preguntas de los cuestionarios y se definen los elementos que deben incluirse en las listas de verificación. Es esencial que las preguntas sean claras, concisas y pertinentes para los

objetivos de la auditoría, mientras que los elementos de verificación deben ser específicos y medibles para facilitar la evaluación de cumplimiento, mediante el alcance de la auditoria que se va a implementar.

3.1.1.3.2 Resultado

3.1.1.3.2.1 Cuestionario día 1 de auditoria

1. ¿De qué manera identifican las cuestiones internas y externas pertinentes para el SGI?
2. ¿Qué acciones toman para las Fortalezas, Debilidades, Oportunidades y Amenazas identificadas por la organización?
3. ¿Cómo se identifican a las partes interesadas y dónde se documenta este proceso?
4. ¿Cuál es el alcance del Sistema de Gestión Integrado?
5. ¿Qué servicios ofrece la organización?
6. ¿Cómo se define y documenta el sistema de gestión integral?
7. ¿De qué manera la alta dirección muestra el liderazgo ante la organización y su sistema de gestión integral?
8. ¿En dónde se encuentra documentada la política de seguridad de la información?
9. ¿Como se autorizó la política?
10. ¿Como aseguran que los colaboradores conocen esta política?
11. ¿Dónde se encuentran documentadas los roles y responsabilidades del comité?
12. ¿Como se dan a conocer los roles y responsabilidades?
13. ¿Qué documento utilizan para abordar riesgos y oportunidades?
14. ¿Cuentan con algún proceso de valoración de riesgos de seguridad de la información?
15. ¿Se tiene algún riesgo detectado actualmente?
16. ¿Como evalúan los riesgos de seguridad de la información?

17. ¿Qué roles están asignados para la gestión de riesgos en la organización?
18. ¿Cómo están definidas las responsabilidades del propietario de la gestión de riesgos?
19. ¿Dónde se localizan los objetivos documentados?
20. ¿Cuántos objetivos tienen registrados?
21. ¿Qué abarcan los objetivos registrados?
22. ¿Qué documentos se muestran en relación con la gestión de mejora continua?
23. ¿Cuál es la deficiencia identificada en los informes?
24. ¿Quién lleva a cabo revisiones del sistema de gestión de la calidad de la organización?
25. ¿Con qué objetivo se realizan estas revisiones del sistema de gestión de la calidad?
26. ¿Se cuenta con un documento donde alta dirección haga la revisión del SGI?
27. ¿Se cuenta con un calendario de auditoria?
28. ¿Se tiene un plan de auditoria previsto para algún ejercicio?
29. ¿Los auditores tienen las competencias necesarias para realizar el ejercicio?
30. Cuando existe un hallazgo calificado como OM o NC ¿Tienen algún plan de acción?
31. ¿Cuentan con un plan de acción de su último ejercicio de auditoria?
32. ¿Cuentan con un documento en relación con la mejora del servicio de mesa de ayuda?
33. ¿Qué documentos evidencian el respaldo de los recursos necesarios para las operaciones de la organización?
34. ¿Qué información proporciona el registro Organigrama?
35. ¿Qué información detalla el registro Presupuesto?
36. ¿Qué establece el registro Plan de Capacidad?
37. ¿Qué documentos se muestran en relación con la concientización del personal?

38. ¿Cuáles son los aspectos abordados en los comunicados dirigidos a la concientización del personal?
39. ¿Tienen algún documento donde se declare el procedimiento del control documental de la organización?
40. ¿Qué documentos se muestran en relación con el control de documentos?
41. ¿Dónde se encuentran los procedimientos, manuales, políticas, anexos, registros, constancias y todo lo documental?
42. ¿Cómo ha establecido la organización las competencias necesarias para los colaboradores que participan en la prestación de servicios?
43. ¿Cuentan con algún perfil de puesto evaluado?
44. ¿Cómo ha sido la evaluación del puesto en términos de cumplimiento?
45. ¿Qué tipo de evaluaciones y verificaciones aplican a los candidatos que están considerando contratar?
46. ¿Estás verificaciones o evaluaciones de las que hablamos, aplican a todos los candidatos sin importar el puesto para el que estén siendo considerados o solamente se les aplican a ciertos puestos?
47. En el contrato laboral que se firma con los colaboradores, ¿se les especifica sus responsabilidades incluyendo las responsabilidades relacionadas con seguridad y con el sistema de gestión?
48. ¿Cuentan con evidencia que demuestre que la alta dirección exige a todos los colaboradores el cumplir sus responsabilidades?
49. ¿Cuentan con alguna política, proceso y/o planes en dónde aborden los temas de concientización y capacitación de todo el personal en materia de seguridad de la información, privacidad de datos y otros temas relevantes para que desempeñen sus funciones?
50. ¿En el año 2023 se ha aplicado algún proceso disciplinario?

51. ¿Se tienen algún caso en los últimos 12 meses, de alguien que hayan promovido o cambiado de puesto?
52. ¿Qué documentos tiene para evidenciar el cambio de puesto?
53. En caso de que finalice una relación laboral ¿Como recuerdan las responsabilidades que tienen en relación con la seguridad de la información o derechos ARCO?

NOTA: Durante la auditoría ISO 27001, se aplicaron cuestionarios a través de la herramienta de videoconferencia Meet Y Microsoft Teams. La sesión fue grabada para garantizar la correcta documentación del proceso. Sin embargo, por razones de confidencialidad de la empresa, no es posible mostrar ni compartir la grabación.

3.1.1.3.2.2 Cuestionario día 2 de auditoria

1. ¿Como mantienen el control de los procesos para la seguridad de la información?
2. ¿Como mantienen controlados los cambios que sufre la organización?
3. ¿Cuál es el proceso mediante el cual los requisitos de seguridad de la información se establecen y documentan en colaboración con los proveedores para mitigar los riesgos asociados con su acceso a los activos de la organización?
4. ¿Cómo se asegura la organización de que todos los requisitos de seguridad de la información relevantes se establezcan y acuerden con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de la infraestructura de TI de la información de la organización?
5. ¿Qué requisitos se incluyen en los acuerdos con proveedores para abordar los riesgos de seguridad de la información asociados con la información y los servicios de tecnología de las comunicaciones y la cadena de suministro de productos?
6. ¿Cómo garantizan las organizaciones el monitoreo, revisión y auditoría regular de la entrega del servicio por parte de los proveedores?

7. ¿Cómo se administran los cambios en la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados, y la revaloración de los riesgos?
8. ¿Cuentan con una política de seguridad de la información en dónde se establezcan todos los lineamientos de seguridad que se deben seguir internamente?
9. ¿Cuándo fue la última vez que se revisó este documento?
10. ¿Tienen documentado en algún lugar, cada cuándo se deben revisar las políticas de seguridad para ver si se requieren hacer actualizaciones?
11. ¿Cuentan con roles definidos?
12. ¿Quiénes conforman el comité del Sistema de Gestión Integral?
13. ¿Cómo determinan cuáles son las tareas o actividades que deben segregarse para evitar riesgos?
14. ¿Cuentan con algún documento en donde tengan un listado de las autoridades relevantes en materia de seguridad con las que requieran mantener contacto?
15. ¿Quiénes forman parte de la lista de contacto?
16. ¿Cuentan con algún documento en donde tengan
17. ¿Quiénes forman parte de la lista de contacto?
18. ¿Cuentan con un proceso o documento en dónde se hable sobre seguridad en los proyectos?
19. ¿Cuentan con algún proyecto en curso?
20. ¿Qué políticas o lineamientos internos tienen documentados acerca del uso de dispositivos móviles dentro de la organización?
21. ¿Se tiene permitido el trabajo remoto?

22. ¿Cuentan con una política documentada en dónde se determina si se permite o no, o en casos si y en qué casos no?
23. ¿Cómo establecen las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?
24. ¿Cuál es el proceso para reportar eventos de seguridad de la información a través de los canales de gestión adecuados de manera rápida?
25. ¿Qué medidas se implementan para asegurar que tanto empleados como contratistas anoten e informen cualquier debilidad de seguridad de la información en los sistemas y servicios de la organización?
26. ¿Cómo se determina si los eventos de seguridad de la información deben ser clasificados como incidentes de seguridad de la información?
27. ¿Cuáles son los procedimientos documentados que se deben seguir al responder a los incidentes de seguridad de la información?
28. ¿De qué manera se utiliza el conocimiento adquirido del análisis y resolución de incidentes de seguridad de la información para reducir la probabilidad o impacto de futuros incidentes?
29. ¿Qué procedimientos ha establecido la organización para la identificación, recopilación, adquisición y preservación de la información que podría ser utilizada como evidencia en casos de seguridad de la información?

NOTA: Durante la auditoría ISO 27001, se aplicaron cuestionarios a través de la herramienta de videoconferencia Meet Y Microsoft Teams. La sesión fue grabada para garantizar la correcta documentación del proceso. Sin embargo, por razones de confidencialidad de la empresa, no es posible mostrar ni compartir la grabación.

3.1.1.3.2.3 Cuestionario día 3 de auditoria

1. ¿Cómo determinan sus requisitos de seguridad de la información y gestionar la continuidad de la seguridad de la información durante situaciones adversas, como crisis o desastres?
2. ¿Qué procesos, procedimientos y controles debe establecer, documentar, implementar y mantener una organización para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa?
3. ¿Con qué frecuencia la organización debe verificar los controles de continuidad de seguridad de la información para asegurar su validez y eficacia durante situaciones adversas?
4. ¿Cómo se garantiza que las instalaciones de procesamiento de la información estén implementadas con suficiente redundancia para cumplir con los requisitos de disponibilidad dentro de la organización?
5. ¿Cómo se asegura la documentación y disponibilidad de los procedimientos operativos para todos los usuarios que los requieran?
6. ¿Cuentan con un proceso que permita controlar los cambios a sistemas e infraestructura?
7. ¿En dónde llevan el registro de los cambios que van haciendo, es decir utilizan una herramienta de tickets o algo similar?
8. ¿Cuentan con un proceso o lineamiento en dónde se especifique cómo llevan a cabo la gestión de la capacidad?
9. ¿Podemos ver cómo monitorean el ambiente productivo en dónde está la aplicación obtén más o la que es utilizada para brindar los servicios de Saynet?
10. ¿Cuentan con un diagrama de su infraestructura en dónde podamos ver cómo es que tienen separados los ambientes de pruebas, desarrollo y productivos?
11. ¿Cómo se asegura la implementación de controles de detección, prevención y recuperación para protegerse contra el malware, y cómo se combinan estos controles con una adecuada concientización a los usuarios dentro de la organización?

12. ¿Cómo garantizan que las copias de respaldo de la información, software e imágenes de sistemas se realicen y prueben regularmente de acuerdo con la política de respaldos acordada?
13. ¿Cómo generan, mantienen y revisan regularmente los registros de eventos de las actividades de usuarios, excepciones, fallas y eventos de seguridad de la información?
14. ¿Cómo protegen el acceso no autorizado y la manipulación de la información en las instalaciones/infraestructura del registro?
15. ¿Cómo registran, protegen y revisan los eventos de las actividades del administrador y del operador de sistemas?
16. ¿Cómo garantizan que los relojes de todos los sistemas de procesamiento de la información relevantes dentro de la organización o dominio de seguridad estén sincronizados con una sola fuente de tiempo de referencia?
17. ¿Cómo implementan procedimientos para controlar la instalación de software en sistemas operacionales?
18. ¿Cómo obtienen información acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados de manera oportuna, evalúa la exposición de la organización a tales vulnerabilidades y toma medidas apropiadas para tratar los riesgos asociados?
19. ¿Cómo establecen e implementan reglas que gobiernan la instalación de software por los usuarios?
20. ¿Cómo planifican y acuerdan los requisitos de la auditoría y las actividades de verificación de los sistemas operativos para minimizar las interrupciones a los procesos del negocio?
21. ¿Cómo garantiza la organización la protección de la información en las redes e infraestructura de apoyo para el procesamiento de información?
22. ¿Cómo gestionan y controlan las redes para proteger la información en los sistemas y aplicaciones?

23. ¿Qué medidas toma la organización para identificar y incluir los mecanismos de seguridad, niveles de servicio y requisitos de gestión en los acuerdos de servicios de red, ya sea que estos servicios sean provistos internamente o subcontratados?
24. ¿Cómo se aseguran de que los grupos de servicios de información, usuarios y sistemas de información estén segregados en las redes?
25. ¿Cómo protege la organización la transferencia de información a través del uso de cualquier tipo de medio de comunicación?
26. ¿Cómo se aseguran de que los acuerdos aborden la transferencia segura de la información del negocio entre la organización y partes externas?
27. ¿Qué medidas toma la organización para garantizar que la información involucrada en mensajes electrónicos esté protegida adecuadamente?
28. ¿Cómo se aseguran de que los requisitos para los acuerdos de confidencialidad o no divulgación se identifiquen, revisen regularmente y documenten, reflejando adecuadamente las necesidades de la organización para la protección de la información?
29. ¿Cómo aseguran que los requisitos relacionados con la seguridad de la información estén integrados en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes?
30. ¿Cómo protegen la información involucrada en servicios de aplicaciones que pasan sobre redes públicas de actividades fraudulentas, disputas contractuales y exposición no autorizada y modificación?
31. ¿Qué medidas toma la organización para asegurar que la información involucrada en transacciones de servicios de aplicación esté protegida contra transmisión incompleta, errores de enrutamiento, alteración de mensajes no autorizados, divulgación no autorizada, duplicación del mensaje no autorizado o reproducción?
32. ¿Cómo establece y aplica la organización reglas para el desarrollo de software y sistemas si no se dedica al desarrollo de software?

33. ¿Cuál es el proceso utilizado por la organización para controlar los cambios a los sistemas dentro del ciclo de vida del desarrollo, si no se dedica al desarrollo de software?
34. ¿Cómo revisa y prueba la organización las aplicaciones críticas del negocio cuando cambian las plataformas operativas, si no se dedica al desarrollo de software?
35. ¿Qué medidas toma la organización para disuadir las modificaciones a los paquetes de software y controlar estrictamente los cambios, si no se dedica al desarrollo de software?
36. ¿Cómo establece y aplica la organización principios de ingeniería para sistemas seguros si no se dedica al desarrollo de software?
37. ¿Qué medidas toma la organización para establecer y proteger los entornos de desarrollo seguro si no se dedica al desarrollo de software?
38. ¿Cómo supervisa y monitorea la organización la actividad del desarrollo de sistemas subcontratados (outsourcing)?
39. ¿Qué procedimientos se implementan para llevar a cabo pruebas de la funcionalidad de seguridad durante el desarrollo?
40. ¿Cómo establece la organización programas de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones?
41. ¿Cuáles son los métodos utilizados por la organización para seleccionar, proteger y controlar cuidadosamente los datos de prueba?
42. ¿Cómo se asegura la protección de las áreas que albergan información sensible o crítica, así como las instalaciones de procesamiento de la información, mediante la definición y utilización de perímetros de seguridad?
43. ¿Cómo se asegura que las áreas estén debidamente protegidas, garantizando que únicamente el personal autorizado tenga acceso mediante la implementación de controles de entrada apropiados?
44. ¿Cómo se lleva a cabo el diseño y la implementación de medidas de seguridad física para garantizar la protección de oficinas, salas e instalaciones dentro de la organización?

45. ¿Cómo se lleva a cabo el diseño e implementación de medidas de protección física para mitigar los riesgos asociados a desastres naturales, ataques maliciosos o accidentes dentro de las instalaciones de la organización?
46. ¿Cómo se desarrollan y ejecutan los procedimientos destinados a operar en áreas seguras dentro de las instalaciones de la organización?
47. ¿Cómo se gestionan los puntos de acceso, como las zonas de carga y descarga, así como otros puntos potenciales de entrada para personas no autorizadas, con el fin de controlarlos y, en la medida de lo posible, aislarlos de las áreas de procesamiento de la información para prevenir accesos no autorizados?
48. ¿Cómo garantizan que el equipo esté ubicado y protegido de manera adecuada para reducir los riesgos de amenazas ambientales y peligros, así como las oportunidades para el acceso no autorizado?
49. ¿Cómo se protegen sus equipos contra las fallas de energía y otras interrupciones ocasionadas por problemas en los servicios públicos para garantizar la continuidad operativa y la integridad de los sistemas?
50. ¿Cómo aseguran la protección del cableado de energía y telecomunicaciones que transporta datos o soporta los servicios de información, con el fin de prevenir interceptaciones, interferencias y daños que puedan afectar la integridad y seguridad de los sistemas de la organización?
51. ¿Cómo se garantiza el mantenimiento adecuado del equipo para asegurar su continua disponibilidad e integridad?
52. ¿Cómo se asegura de que el equipo, la información o el software no sean sacados del sitio sin autorización previa?
53. ¿Cómo se implementa la seguridad en los activos fuera de las instalaciones, considerando los variados riesgos asociados con el trabajo fuera de los límites físicos de la organización?
54. ¿Cómo se verifica que todos los elementos del equipo que contienen medios de almacenamiento hayan sido eliminados o sobrescritos de manera segura?

55. ¿Qué medidas se implementan para garantizar la eliminación de cualquier dato sensible y software licenciado antes de la disposición o reutilización del equipo?
56. ¿Cómo garantizan los usuarios que el equipo desatendido cuente con la protección adecuada?
57. ¿Cómo implementan y adoptan las políticas de escritorio limpio, que prohíben papeles y medios de almacenamiento removibles, y de pantalla limpia en las instalaciones de procesamiento de la información?
58. ¿Cuentan con uno o varios inventarios de activos?
59. ¿Cuentan con algún lineamiento interno documentado en dónde describan la forma en la que clasifican la información, dependiendo de su nivel de confidencialidad?
60. ¿Como etiquetan la información dependiendo de su clasificación?
61. ¿Cuentan con algún proceso documentado para administrar todos los activos, en dónde se incluya el decir cómo es que van a cuidar los activos dependiendo del tipo de información que procesen, transmitan o resguarden?
62. Tratándose de medios removibles (p. ej. usb, discos duros, tarjetas de memoria extraíbles, etc.), ¿cómo se protegen?
63. ¿Como destruyen la información física?
64. ¿Como destruyen la información lógica?
65. ¿Tienen algún registro de borrado?
66. ¿Por necesidad de algún proyecto o por cuestiones internas, tienen o han tenido la necesidad de transportar información a través de medios físicos?
67. ¿Cuentan con una política documentada para la gestión de los accesos lógicos?
68. ¿Tratándose de brindar acceso a servicios de red tienen un listado de las áreas o los puestos que están autorizados para tener acceso a dichos servicios?
69. ¿Cuándo existe una solicitud de acceso que deben hacer?

70. Siguiendo con el tema de accesos, una vez que ya fué creado el usuario, ¿en dónde tienen documentado el cómo se le deben entregar las credenciales de acceso al usuario?
71. ¿Tienen alguna matriz o lista en dónde tengan documentado quienes son las personas que pueden tener accesos privilegiados? Si no, ¿cómo saben quién si puede tener acceso privilegiados?
72. ¿Como controlan la información secreta como usuarios y contraseñas?
73. ¿Los administradores de los sistemas, realizan revisiones cada determinado tiempo para asegurar que todos los usuarios tengan el estatus que deberían tener?
74. ¿Cómo se aseguran de que los colaboradores salvaguardan la información?
75. ¿Dé que manera previenen el acceso no autorizado?
76. Actualmente, para acceder a cualquier activo crítico, ¿se tiene implementado algún método de inicio de sesión seguro?
77. ¿Como aseguran que las contraseñas sean de calidad?
78. Los usuarios, es decir todos los colaboradores que son usuarios de algún equipo de cómputo, ya sea lap top o de escritorio, ¿tienen permiso para alguna de las siguientes: cambiar configuración de inicio de sesión, bloqueo de pantalla automático, deshabilitar antivirus, ¿instalar software?
79. ¿De qué manera restringen el acceso al código fuente?
80. ¿Cómo se identifican, documentan y mantienen actualizados todos los requisitos legislativos, regulatorios, contractuales relevantes, así como el enfoque de la organización para cumplir con estos requisitos, para cada sistema de información y para la organización en su conjunto?
81. ¿Qué medidas se han implementado para asegurar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentado dentro de la organización?

82. ¿De qué manera se implementan medidas para proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, en conformidad con los requisitos legales, regulatorios, contractuales y de negocios?
83. ¿Cómo garantizan la privacidad y protección de la información de identificación personal conforme a lo requerido por la legislación y regulación relevante aplicable dentro de la organización?
84. ¿Cómo se garantiza que los controles criptográficos sean utilizados en cumplimiento con todos los acuerdos, legislación y regulaciones relevantes dentro de la organización?
85. ¿Cómo se lleva a cabo la revisión independiente del enfoque de la organización para la gestión de la seguridad de la información y su implementación, incluyendo objetivos de control, controles, políticas, procesos y procedimientos, en intervalos planificados o cuando ocurran cambios significativos?
86. ¿Cómo llevan a cabo las revisiones periódicas de los sistemas de información para garantizar su conformidad con las políticas y normas de seguridad de la información establecidas por la organización?
87. ¿Cuentan con una política documentada sobre el uso de controles criptográficos?
88. ¿Cuentan con un procedimiento para gestión de llaves de cifrado?

NOTA: Durante la auditoría ISO 27001, se aplicaron cuestionarios a través de la herramienta de videoconferencia Meet Y Microsoft Teams. La sesión fue grabada para garantizar la correcta documentación del proceso. Sin embargo, por razones de confidencialidad de la empresa, no es posible mostrar ni compartir la grabación. [BG11]

3.1.1.3.2.4 Formato de revisión documental

Tabla 9 Formato de revisión documental

Requisito / Control	Tipo de documento	Nombre	Versión	Fecha entrada en vigor

--	--	--	--	--

3.1.1.3.2.5 Formato de lista de verificación

Tabla 10 Formato de Lista de verificación ISO/IEC 27001:2013

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
4. Contexto de la organización			
4.1 Comprensión de la organización y de su contexto	La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y su dirección estratégica, y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la calidad. La organización debe realizar el seguimiento y la revisión de la información sobre estas cuestiones externas e internas.		
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Debido a su efecto o efecto potencial en la capacidad de la organización de proporcionar regularmente productos y servicios que satisfagan los requisitos del cliente y los legales y reglamentarios aplicables, la organización debe determinar: a) las partes interesadas que son pertinentes al sistema de gestión de la calidad; b) los requisitos pertinentes de estas partes interesadas para el sistema de gestión de la calidad.		

	La organización debe realizar el seguimiento y la revisión de la información sobre estas partes interesadas y sus requisitos pertinentes.		
--	---	--	--

Tabla 11 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
4.3 Determinación del alcance del sistema de gestión de la calidad	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la calidad para establecer su alcance. Cuando se determina este alcance, la organización debe considerar: a) las cuestiones externas e internas indicadas en el apartado 4.1; b) los requisitos de las partes interesadas pertinentes indicados en el apartado 4.2; c) los productos y servicios de la organización. La organización debe aplicar todos los requisitos de esta Norma Internacional si son aplicables en el alcance determinado de su sistema de gestión de la calidad. El alcance del sistema de gestión de la calidad de la organización debe estar disponible y mantenerse como información documentada. El alcance debe establecer los tipos de productos y servicios cubiertos, y proporcionar la justificación para cualquier requisito de esta Norma Internacional que la organización determine que no es aplicable para el alcance de su sistema de gestión de la		

	calidad. La conformidad con esta Norma Internacional sólo se puede declarar si los requisitos determinados como no aplicables no afectan a la capacidad o a la responsabilidad de la organización de asegurarse de la conformidad de sus productos y servicios y del aumento de la satisfacción del cliente.		
--	--	--	--

Tabla 12 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
4.4 Sistema de gestión de Seguridad de la Información	La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información		
5 Liderazgo			
5.1 Compromiso y liderazgo	La alta dirección debe demostrar su liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información		
5.2 Política	La alta dirección debe establecer una política de seguridad de la información		
5.3 Roles, responsabilidades y autoridades en la organización	La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen, se comuniquen y se entiendan en toda la organización.		
6 Planificación			
6.1 Acciones para abordar riesgos y oportunidades			

6.1.1	Al planificar el sistema de gestión de seguridad de la información la organización debe considerar las cuestiones referidas en el apartado 4.1 y los requisitos referidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario abordar con el fin de: a) asegurar que el sistema de gestión de SGSI pueda lograr sus resultados previstos; b) aumentar los efectos deseables; c) prevenir o reducir efectos no deseados; d) lograr la mejora.		
-------	---	--	--

Tabla 13 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
6.1.2	La organización debe definir y aplicar un proceso de valoración de riesgos de seguridad de la información para: a) establecer y mantener los criterios de riesgo de seguridad de la información que incluya: El criterio de aceptación del riesgo y los criterios para realizar las valoraciones de riesgos de seguridad de la información. b) Asegurar de que al repetir las valoraciones de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables; c) identificar los riesgos de seguridad de la información: aplicar el proceso de valoración de riesgos		

	de seguridad de la información para identificar riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del SGSI. identificar a los propietarios de los riesgos. d) Analizar los riesgos de seguridad de la información: Valorar las consecuencias potenciales que se derivan si los riesgos identificados llegan a materializarse; valorar la probabilidad realista de la ocurrencia de los riesgos identificados y determinar los niveles de riesgo. e) Evaluar los riesgos de seguridad de la información: Comparar los resultados del análisis de riesgo con los criterios de riesgo establecidos en el inciso a). priorizar los riesgos analizados para el tratamiento de riesgo. La organización debe conservar información documentada sobre el proceso de valoración de riesgos de seguridad de la información.		
--	---	--	--

Tabla 14 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

6.1.3	La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para: a) Seleccionar opciones apropiadas de tratamiento de riesgos de seguridad de la información, tomando en cuenta los resultados de la valoración de riesgos; b) Determinar todos los controles que sean necesarios para implementar las opciones de tratamiento de riesgos de seguridad de la información elegidas. c) Comparar los controles determinados con los descritos en el apéndice "A" y verificar que no se hayan omitido controles necesarios; d) Producir una declaración de aplicabilidad que contenga los controles necesarios (véase el inciso 6.1.3 subinciso b) y c)) y la justificación de las inclusiones, si están implementadas o no, y la justificación de la exclusión de controles del apéndice "A".		
6.2 Objetivos de la calidad y planificación para lograrlos	La organización debe establecer los objetivos de seguridad de la información en funciones y niveles pertinentes		
7 Apoyo			
7.1 Recursos	La organización debe determinar y proveer los recursos necesarios para el establecimiento, implementación,		

	mantenimiento y mejora continua del SGSI.		
--	---	--	--

Tabla 15 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
7.2 Competencia	La organización debe: a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al desempeño y eficacia del sistema de gestión de la calidad; b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia apropiadas; c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; d) conservar la información documentada apropiada como evidencia de la competencia.		
7.3 Concientización	La organización debe asegurarse de que las personas que realizan el trabajo bajo el control de la organización tomen conciencia de: a) la política de la calidad; b) los objetivos de la calidad pertinentes; c) su contribución a la eficacia del sistema de gestión de la calidad, incluidos los beneficios de una mejora del desempeño;		

	d) las implicaciones del incumplimiento de los requisitos del sistema de gestión de la calidad.		
--	---	--	--

Tabla 16 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
7.4 Comunicación	La organización debe determinar las comunicaciones internas y externas pertinentes al sistema de gestión de la calidad, que incluyan: a) qué comunicar; b) cuándo comunicar; c) a quién comunicar; d) cómo comunicar; e) quién comunica.		
7.5 Información documentada			
7.5.1 Generalidades	El sistema de gestión de la calidad de la organización debe incluir: a) la información documentada requerida por esta Norma Internacional; b) la información documentada que la organización determina como necesaria para la eficacia del sistema de gestión de seguridad de la información.		

Tabla 17 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

7.5.2 Creación y actualización	Al crear y actualizar la información documentada, la organización debe asegurarse de que lo siguiente sea apropiado: a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia); b) el formato (por ejemplo, idioma, versión del software, gráficos) y los medios de soporte (por ejemplo, papel, electrónico); c) la revisión y aprobación con respecto a la conveniencia y adecuación		
7.5.3 Control de la información documentada			
7.5.3	La información documentada requerida por el sistema de gestión de la calidad y por esta Norma Internacional se debe controlar para asegurarse de que: a) esté disponible y sea idónea para su uso, donde y cuando se necesite; b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado o pérdida de integridad).		
8 Operación			
8.1 Planificación y control operacional	La organización debe planear, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información, y para implementar las acciones determinadas en el inciso 6.1 La organización debe también		

	implementar planes para lograr los objetivos de seguridad de la información determinados en el inciso 6.2 La organización debe mantener la información documentada en la medida necesaria para tener certeza de que los procesos se han llevado a cabo según lo planeado. La organización debe controlar los cambios planeados y revisar las consecuencias de los cambios no deseados, tomando acciones para mitigar efectos adversos, según sea necesario. La organización debe asegurarse de que los procesos de desarrollo de sistemas sean determinados y controlados.		
--	--	--	--

Tabla 18 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
8.2 Evaluación de riesgos y de seguridad de la información	La organización debe llevar a cabo las evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se proponen o se producen cambios significativos, teniendo en cuenta los criterios establecidos en el inciso 6.1.2 inciso a).		
8.3 Tratamiento de riesgos de seguridad de la información	La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información. La organización debe conservar la información documentada de los resultados del tratamiento de riesgos de seguridad de la información.		

Tabla 19 (Continuación)

9 Evaluación del desempeño			
9.1 Seguimiento, medición, análisis y evaluación			
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
9.1 Monitoreo, medición, análisis y evaluación	La organización debe determinar: a) qué necesita seguimiento y medición; b) los métodos de seguimiento, medición, análisis y evaluación necesarios para asegurar resultados válidos; c) cuándo se deben llevar a cabo el seguimiento y la medición; d) cuándo se deben analizar y evaluar los resultados del seguimiento y la medición. La organización debe evaluar el desempeño y la eficacia del sistema de gestión de la calidad. La organización debe conservar la información documentada apropiada como evidencia de los resultados		
9.2 Auditoría interna	La organización debe llevar a cabo auditorías internas a intervalos planificados para proporcionar información acerca de si el sistema de gestión de la calidad: a) es conforme con: 1) los requisitos propios de la organización para su sistema de gestión de la calidad; 2) los requisitos de esta Norma Internacional; b) se implementa y mantiene eficazmente.		

Tabla 20 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
9.3 Revisión por la dirección	La alta dirección debe revisar el sistema de gestión de la calidad de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación, eficacia y alineación continuas con la dirección estratégica de la organización.		
10 Mejora			
10.1 No conformidad y acción correctiva	Cuando ocurre una no conformidad, la organización debe reaccionar a la inconformidad según sea el caso.		
10.2 Mejora continua	La organización debe mejorar continuamente la idoneidad, la adecuación y la eficacia del SGSI.		
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
A.5.1 Gestión de la Dirección para la Seguridad de la Información	Proporcionar dirección general y apoyo para la seguridad de la información de acuerdo con los requisitos del negocio y las leyes y regulaciones relevantes.		
A.5.1.1 Políticas para la Seguridad de la Información	Se debe definir, aprobar por la dirección, publicar y comunicar a todos los empleados y partes externas relevantes u conjunto de políticas para la seguridad de la información.		

Tabla 21 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.5.1.2 Revisión de Políticas de Seguridad de la Información	Las políticas para la seguridad de la información deben revisarse a intervalos planeados o si ocurren cambios significativos para garantizar su continua idoneidad, adecuación y eficacia.		
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1 Organización Interna	Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		
A.6.1.1 Roles y Responsabilidades para la Seguridad de la Información	Todas las responsabilidades de la seguridad de la información deben definirse y asignarse.		
A.6.1.2 Segregación de Tareas	Las tareas en conflicto y áreas de responsabilidad deben segregarse para reducir las oportunidades de modificación no autorizada, no intencional o mal uso de los activos de la organización.		
A.6.1.3 Contacto con Autoridad	Se deben mantener contactos apropiados con las autoridades relevantes		
A.6.1.4 Contacto con Grupos de Especial Interés	Se deben mantener contactos apropiados con grupos especiales de interés u otros foros de seguridad especializados y asociaciones profesionales.		

Tabla 22 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.6.1.5 Seguridad de la Información en la Administración de Proyectos	La seguridad de la información debe incluirse en la administración de proyectos independientemente del tipo de proyecto.		
A.6.2 Dispositivos móviles y teletrabajo	Garantizar la Seguridad del Teletrabajo y el uso de dispositivos móviles.		
A.6.2.1 Política de Dispositivos Móvil	Se debe adoptar una política y medidas de seguridad de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles.		
A.6.2.2 Teletrabajo	Se debe implementar una política y medidas de seguridad de soporte para proteger el acceso, proceso o almacenamiento de la información en los sitios de trabajo a distancia.		
A.7 SEGURIDAD EN LOS RECURSOS HUMANOS			
A.7.1 Previo al Empleo	Asegurar que los empleados y contratistas entiendan sus responsabilidades y son adecuados para los roles para los cuales son considerados		
A.7.1.1 Investigación	Se deben llevar a cabo verificaciones de antecedentes a todos los candidatos al empleo de acuerdo con las leyes, regulaciones relevantes y la ética, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.		

Tabla 23 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.7.1.2 Términos y Condiciones del Empleo	Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de la organización para la seguridad de la información.		
A.7.2 Durante el Empleo	Asegurar que los empleados y contratistas estén conscientes de que cumplen con sus responsabilidades de la seguridad de la información.		
A.7.2.1 Responsabilidades de la Dirección	La dirección debe exigir a todos los empleados y contratistas aplicar la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.		
A.7.2.2 Concientización, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando sea relevante, contratistas deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y procedimientos organizacionales, cuando sea relevante para sus funciones de trabajo.		
A.7.2.3 Proceso Disciplinario	Debe haber y comunicarse un proceso disciplinario formal para tomar acciones contra empleados que hayan cometido una violación a la seguridad de la información.		
A.7.3 Terminación y Cambio de Empleo	Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.		

Tabla 24 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.7.3.1 Responsabilidades en la terminación o cambio de empleo	Las responsabilidades de la seguridad de la información y obligaciones que permanecen validos después de la terminación o el cambio e empleo deben estar definidos, comunicados a los empleados o contratistas y hacerse cumplir.		
A.8 GESTIÓN DE ACTIVOS			
A.8.1 Responsabilidad Sobre los Activos	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		
A.8.1.1 Inventario de Activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información y se debe elaborar y mantener un inventario de estos activos.		
A.8.1.2 Propiedad de los Activos	Los activos incluidos en el inventario deben contar con un propietario.		
A.8.1.3 Uso aceptable de los Activos	Se debe identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos asociados con la información y las instalaciones de procesamiento de la información.		
A.8.1.4 Devolución de Activos	Todos los empleados y los usuarios de partes externas deben devolver todos los activos de la organización en su posesión a la terminación de su empleo, contrato o acuerdo		

Tabla 25 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.8.2 Clasificación de Información	Asegurar que la información reciba un apropiado nivel de protección de acuerdo con su importancia para la organización.		
A.8.2.1 Clasificación de Información	La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad de su divulgación o modificación no autorizada.		
A.8.2.2 Etiquetado de información	Se debe desarrollar e implementar un apropiado conjunto de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización		
A.8.2.3 Manejo de Activos	Se deben desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de la información adoptado por la organización.		
A.8.3 Manejo de Medios	Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de información almacenada en medios.		
A.8.3.1 Gestión de Medios Removibles	Se deben implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la organización.		

Tabla 26 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.8.3.2 Disposición de Medios	Se deben disponer de manera segura los medios cuando ya no se requieran, utilizando procedimientos formales.		
A.8.3.3 Transferencia de Medios Físicos	Se deben proteger los medios que contengan información contra acceso no autorizado, mal uso o corrupción durante la transportación.		
A.9 CONTROL DE ACCESO			
A.9.1 Requisitos del Negocio para el Control de Acceso	Limitar el acceso a la información y a las instalaciones de procesamiento de la información.		
A.9.1.1 Política de Control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de la seguridad de la información.		
A.9.1.2 Acceso a las Redes y los Servicios de la Red	Se debe proporcionar a los usuarios únicamente el acceso a la red y servicios de la red para los que hayan sido específicamente autorizados		
A.9.2 Gestión del Acceso de Usuarios	Garantizar el acceso de usuarios autorizados y prevenir acceso no autorizado a sistemas y servicios.		
A.9.2.1 Registro y Cancelación de Usuarios	Se debe implementar un proceso formal de registro y cancelación de usuarios para permitir la asignación de derechos de acceso.		

Tabla 27 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.9.2.2 Provisión de Acceso de Usuarios	Se debe implementar un proceso formal para la provisión de acceso a usuarios para asignar o revocar derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.		
A.9.2.3 Gestión de Derechos de Acceso Privilegiado	La asignación y uso de los derechos de acceso privilegiado deben restringirse y controlarse.		
A.9.2.4 Gestión de Información Secreta de Autenticación de los Usuarios	La asignación de información secreta de autenticación debe controlarse a través de un proceso de gestión formal.		
A.9.2.5 Revisión de los Derechos de Acceso de Usuario	Los propietarios de activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.		
A.9.2.6 Eliminación o Ajuste de los Derechos de Acceso.	Los derechos de acceso de todos los empleados y usuarios de partes externas a la información e instalaciones de procesamiento de la información deben ser eliminados después de la terminación de su empleo, contrato o acuerdo, o adaptados a los cambios producidos.		
A.9.3 Responsabilidad del Usuario	Hacer responsables a los usuarios de salvaguardar su información de autenticación.		
A.9.3.1 Uso de Información Secreta de Autenticación.	Se debe exigir a los usuarios que sigan las prácticas de la organización en el uso de su información secreta de autenticación.		

Tabla 28 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.9.4 Control de Acceso a Sistemas y Aplicaciones	Prevenir el acceso no autorizado a los sistemas y aplicaciones.		
A.9.4.1 Restricción de Acceso a la Información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones de los sistemas de acuerdo con la política de control de acceso.		
A.9.4.2 Procedimiento de Inicio de Sesión Seguros	Cuando se requiere por la política de control de acceso, el acceso a los sistemas y aplicaciones debe controlarse por un procedimiento de inicio de sesión seguro.		
A.9.4.3 Sistema de Administración de Contraseñas	Los sistemas de administración de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.		
A.9.4.4 Uso de Privilegios de los Programas de Utilidades	El uso de programas de utilidades que puedan ser capaces de anular los controles del sistema y de las aplicaciones deben estar restringidas y estrechamente controladas.		
A.9.4.5 Control de Acceso a Código Fuente del Programa	Se debe restringir el acceso al código fuente del programa.		
A.10 CRIPTOGRAFÍA			
A.10.1 Controles Criptográficos	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información		

Tabla 29 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.10.1.1 Política sobre el Uso de Controles Criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.		
A.10.1.2 Gestión de Llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, a través de todo su ciclo de vida.		
A.11 SEGURIDAD FÍSICA Y AMBIENTAL			
A.11.1 Áreas Seguras	Prevenir el acceso físico no autorizado, daños e interferencia a la información e instalaciones de procesamiento de la información de la organización.		
A.11.1.1 Perímetro de Seguridad Física	Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen información ya sea sensible o crítica y las instalaciones de procesamiento de la información.		
A.11.1.2 Controles Físicos de Entrada	Se deben proteger las áreas seguras mediante controles de entrada apropiados para garantizar que sólo el personal autorizado tenga acceso permitido.		
A.11.1.3 Aseguramiento de Oficinas, Salas e Instalaciones	Se debe diseñar y aplicar seguridad física para oficinas, salas e instalaciones.		

Tabla 30 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.11.1.4 Protección contra Amenazas Externas y Ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.		
A.11.1.5 Trabajo en Áreas Seguras	Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras.		
A.11.1.6 Áreas de Entrega y Carga	Los puntos de acceso, tales como las áreas de entrega y carga y otros puntos en los que personas no autorizadas puedan entrar en las instalaciones deben ser controlados y, si es posible, aislados de las instalaciones de procesamiento de la información para evitar acceso no autorizado.		
A.11.2 Equipo	Prevenir la pérdida, daño, robo o comprometer los activos e interrupción de las operaciones de la organización.		
A.11.2.1 Ubicación y Protección de Equipo	El equipo debe estar situado y protegido para reducir los riesgos de amenazas ambientales y peligros, y las oportunidades para el acceso no autorizado.		
A.11.2.2 Servicios Públicos	El equipo debe estar protegido contra fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.		
A.11.2.3 Seguridad del Cableado	El cableado de energía y telecomunicaciones que transporten datos o soporten los servicios de la información deben protegerse de interceptación, interferencia y daño.		

Tabla 31 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.11.2.4 Mantenimiento de Equipo	El equipo debe mantenerse correctamente para asegurar su continua disponibilidad e integridad.		
A.11.2.5 Retiro de Activos	No se debe sacar del sitio sin autorización previa el equipo, información o software.		
A.11.2.6 Seguridad de los Equipos y Activos fuera de las Instalaciones	Se debe aplicar seguridad a los activos fuera de las instalaciones tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.		
A.11.2.7 Disposición o Reutilización Segura del Equipo	Todos los elementos del equipo que contiene medios de almacenamiento deben ser verificados para garantizar que cualquier dato sensible y software licenciado ha sido eliminado o sobrescrito de manera segura previo a su disposición o reutilización.		
A.11.2.8 Equipo de Usuario Desatendido	Los usuarios deben garantizar que el equipo desatendido tenga la protección adecuada.		
A.11.2.9 Política de Pantalla y Escritorio Limpio	Se debe adoptar una política de escritorio limpio de papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de la información.		
A.12 SEGURIDAD EN OPERACIONES			

Tabla 32 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.12.1 Procedimientos y Responsabilidades Operativas	Garantizar la operación correcta y segura de las instalaciones de procesamiento de la información.		
A.12.1.1 Procedimientos Operativos Documentados	Deben documentarse los procedimientos operativos y estar disponibles para todos los usuarios que los necesiten.		
A.12.1.2 Gestión del Cambio	Se deben controlar los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten a la seguridad de la información.		
A.12.1.3 Gestión de Capacidad	El uso de recursos debe monitorearse, afinarse para realizar proyecciones de los requisitos futuros de la capacidad para garantizar el desempeño requerido de los sistemas.		
A.12.1.4 Separación de Entornos de Desarrollo, Pruebas y Operación.	Se deben separar los entornos de desarrollo, pruebas y operación para reducir los riesgos de acceso no autorizado o cambios al entorno de operación.		
A.12.2 Protección contra Malware	Garantizar que la información y las instalaciones de procesamiento de la información estén protegidas contra malware.		
A.12.2.1 Controles contra Malware	Se deben implementar controles de detección, Prevención y recuperación para protegerse contra malware y combinarse con una apropiada concientización a usuarios.		

Tabla 33 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.12.3 RespalDOS	Proteger contra la pérdida de datos.		
A.12.3.1 RespalDOS de la Información	Copias de respaldos de la información, software e imágenes de sistemas deben realizarse y probarse regularmente de acuerdo con la política de respaldos acordada.		
A.12.4 Registro y Monitoreo	Registrar eventos y generar evidencia.		
A.12.4.1 Registro de Eventos	Se deben generar, mantener y revisar regularmente los registros de eventos de las actividades de usuarios, excepciones, fallas y eventos de seguridad de la información.		
A.12.4.2 Protección de la Información del Registro	Se deben proteger con acceso no autorizado y negación de manipulación de la información en las instalaciones/infraestructura del registro.		
A.12.4.3 Registros del Administrador y Operador	Se deben registrar, proteger y revisar los eventos de las actividades del administrador y del operador de sistemas.		
A.12.4.4 Sincronización del reloj	Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de la organización o dominio de seguridad deben estar sincronizados con una sola fuente de tiempo de referencia.		

Tabla 34 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.12.5 Control del Software Operacional	Garantizar la integridad de los sistemas operacionales.		
A.12.5.1 Instalación de Software en Sistemas Operacionales	Se deben implementar procedimientos para controlar la instalación de software en sistemas operacionales.		
A.12.6 Gestión de Vulnerabilidades Técnicas	Prevenir la explotación de vulnerabilidades técnicas.		
A.12.6.1 Gestión de Vulnerabilidades Técnicas	Se debe obtener información acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados de manera oportuna, evaluar la exposición de la organización a tales vulnerabilidades y tomar medidas apropiadas para tratar los riesgos asociados.		
A.12.6.2 Restricciones en la Instalación de Software	Se debe establecer e implementar reglas que gobiernen la instalación de software por los usuarios.		
A.12.7 Consideraciones de Auditoría a Sistemas de Información	Minimizar el impacto de las actividades de la auditoría en los sistemas operacionales.		
A.12.7.1 Controles de Auditoría a los Sistemas de Información	Los requisitos de la auditoría y las actividades que implican la verificación de los sistemas operacionales deben planearse y acordarse cuidadosamente para minimizar las interrupciones a los procesos del negocio.		

Tabla 35 (Continuación)

A.13 SEGURIDAD EN LAS COMUNICACIONES			
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo

A.13.1 Gestión de Seguridad en la Red	Garantizar la protección de la información en las redes e infraestructura de apoyo para el procesamiento de información.		
A.13.1.1 Controles de Red	Las redes deben gestionarse y controlarse para proteger la información en los sistemas y aplicaciones.		
A.13.1.2 Seguridad en los Servicios de Red	Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión para todos los servicios de la red deben identificarse e incluirse en los acuerdos de servicios de red, ya sea que estos servicios sean provistos internamente o se subcontraten.		
A.13.1.3 Segregación en Redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes.		
A.13.2 Transferencia de Información	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1 Políticas y Procedimientos de Transferencia de Información	Deben existir políticas formales de transferencia, procedimientos y controles para proteger la transferencia de información a través del uso de cualquier tipo de medio de comunicación.		

Tabla 36 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.13.2.2 Acuerdos de Transferencia de Información	Los acuerdos deben abordar la transferencia segura de la información del negocio entre la organización y partes externas.		

A.13.2.3 Mensajería Electrónica	La información involucrada en mensajes electrónicos debe estar protegida apropiadamente.		
A.13.2.4 Acuerdos de Confidencialidad o no Divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación reflejando las necesidades de la organización para la protección de la información.		
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
A.14.1 Requisitos de Seguridad para los Sistemas de Información	Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios sobre redes públicas.		
A.14.1.1 Análisis y Especificación de Requisitos de Seguridad	Los requisitos relacionados con la seguridad de la información deben estar incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.		

Tabla 37 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.14.1.2 Servicios de Aplicaciones Seguras en Redes Públicas	La información involucrada en servicios de aplicaciones que pasan sobre redes públicas debe estar protegida de actividades fraudulentas, disputas contractuales y exposición no autorizada y modificación.		

A.14.1.3 Protección de Aplicaciones de Servicios de Transacciones	La información involucrada en transacciones de servicios de aplicación debe estar protegida para prevenir transmisión incompleta, errores de enrutamiento, alteración de mensajes no autorizados, divulgación no autorizada, duplicación del mensaje no autorizado o reproducción.		
A.14.2 Seguridad en Desarrollo y Procesos de Soporte	Garantizar que la seguridad de la información se diseña e implementa en el ciclo de vida del desarrollo de los sistemas de información.		
A.14.2.1 Política de Desarrollo Seguro	Deben establecerse y aplicarse reglas para el desarrollo de software y sistemas en los desarrollos dentro de la organización.		
A.14.2.2 Procedimientos de Control de Cambios a Sistemas	Los cambios a los sistemas dentro del ciclo de vida del desarrollo deben controlarse mediante el uso de procedimientos formales de control de cambios.		

Tabla 38 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.14.2.3 Revisión Técnica de Aplicaciones después de Cambios en la Plataforma de Operación	Cuando cambian las plataformas operativas, las aplicaciones críticas del negocio deben revisarse y probarse para garantizar que no hay un impacto adverso en las operaciones de la organización o en la seguridad.		
A.14.2.4 Restricciones a los Cambios en los Paquetes de Software	Se deben disuadir las modificaciones a los paquetes de software, limitar a los cambios necesarios y todos los cambios deben estar estrictamente controlados.		

A.14.2.5 Principios de Ingeniería en Sistemas Seguros	Se deben establecer, documentar, mantener y aplicar principios de ingeniería para sistemas seguros a cualquier esfuerzo de implementación de sistemas de información.		
A.14.2.6 Entorno de Desarrollo Seguro	Las organizaciones deben establecer y proteger apropiadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubran todo el ciclo de vida del desarrollo del sistema.		
A.14.2.7 Desarrollo de Sistemas Subcontratado (Outsourcing)	La organización debe supervisar y monitorear la actividad del desarrollo de sistemas sub contratados (outsourcing).		
A.14.2.8 Pruebas de Seguridad a los Sistemas	Se deben llevar a cabo pruebas de la funcionalidad de seguridad durante el desarrollo.		

Tabla 39 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.14.2.9 Pruebas de Aceptación a los Sistemas	Se deben establecer programas de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones.		
A.14.3 Datos de Prueba	Garantizar la protección de los datos usados para las pruebas.		
A.14.3.1 Protección de Datos de Prueba	Los datos de prueba deben seleccionarse, protegerse y controlarse cuidadosamente.		
A.15 RELACIÓN CON PROVEEDORES			

A.15.1 Seguridad de la Información en Relación con Proveedores	Garantizar la protección de los activos de la organización que sea accesible por los proveedores.		
A.15.1.1 Política de Seguridad de la Información para la Relación con Proveedores	Se deben acordar con los proveedores y documentarse los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso de proveedores a los activos de la organización.		
A.15.1.2 Abordar la Seguridad dentro de los Acuerdos con Proveedores	Todos los requisitos de seguridad de la información relevantes deben establecerse y acordarse con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar componentes de la infraestructura de TI de la información de la organización.		

Tabla 40 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.15.1.3 Cadena de Suministro en Tecnologías de la Información y Comunicaciones	Los acuerdos con proveedores deben incluir los requisitos para tratar los riesgos de seguridad de la información asociados con la información y los servicios de tecnología de las comunicaciones y la cadena de suministro de productos.		
A.15.2 Administración de Entrega de Servicios de Proveedores	Mantener un nivel acordado de seguridad de la información y la entrega de servicios alineados con los acuerdos de proveedores.		
A.15.2.1 Monitoreo y Revisión de los	Las organizaciones deben monitorear, revisar y auditar regularmente la entrega del servicio de Proveedores		

Servicios de Proveedores			
A.15.2.2 Gestión de Cambios a los Servicios de Proveedores	Los cambios en la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, deben ser administrados, tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y la revaloración de los riesgos.		
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
A.16.1 Gestión de Incidentes d Seguridad de la Información y Mejoras	Garantizar un enfoque consistente y eficaz para la administración de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.		

Tabla 41 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.16.1.1 Responsabilidades y Procedimientos	Se deben establecer responsabilidades y procedimientos de gestión para garantizar una rápida, eficaz y ordenada respuesta a los incidentes de seguridad de la información.		
A.16.1.2 Reporte de Eventos de Seguridad de la Información	Los eventos de seguridad de la información deben reportarse a través de canales de gestión apropiados tan rápido como sea posible.		

A.16.1.3 Reporte de Debilidades de Seguridad de la Información	Se debe exigir a los empleados y contratistas que utilizan los sistemas y servicios de información de la organización anotar e informar cualquier debilidad de seguridad de la información observada o sospechosa en los sistemas y servicios.		
A.16.1.4 Evaluación y Decisión sobre Eventos de Seguridad de la Información	Los eventos de seguridad de la información deben evaluarse y se debe decidir si son clasificados como incidentes de seguridad de la información.		
A.16.1.5 Respuesta a Incidentes de Seguridad de la Información	Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.		
A.16.1.6 Aprendizaje de Incidentes de Seguridad de la Información	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de futuros incidentes.		

Tabla 42 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.16.1.7 Recopilación de Evidencia	La organización debe definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de la información que puede servir como evidencia.		
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO			

A.17.1 Continuidad de la Seguridad de la Información	Se debe integrar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad del negocio de la organización.		
A.17.1.1 Planeación de la Continuidad de la Seguridad de la Información	La organización debe determinar sus requisitos de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.		
A.17.1.2 Implementando la Continuidad de la Seguridad de la Información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.		
A.17.1.3 Verificación, revisión y evaluación de la Continuidad de la Seguridad de la Información	La organización debe verificar los controles de continuidad de seguridad de la información establecidos e implementados a intervalos regulares con el objetivo de garantizar que son válidos y eficaces durante situaciones adversas.		

Tabla 43 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.17.2 Redundancias	Garantizar la disponibilidad de las instalaciones de procesamiento de la información.		
A.17.2.1 Disponibilidad de las Instalaciones de	Las instalaciones de procesamiento de la información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.		

Procesamiento de la Información			
A.18 CUMPLIMIENTO			
A.18.1 Cumplimiento con Requisitos Legales y Contractuales			
A.18.1.1 Identificación de la Legislación Aplicable y Requisitos Contractuales	Todos los requisitos legislativos, regulatorios, contractuales relevantes y el enfoque de la organización para cumplir con estos requisitos deben estar explícitamente identificados, documentados y mantenerse actualizados para cada sistema de información y la organización.		
A.18.1.2 Derechos de Propiedad Intelectual	Se deben implementar procedimientos apropiados para garantizar el cumplimiento con los requisitos legislativos, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentado.		

Tabla 44 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.18.1.3 Protección de Registros	Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legales, regulatorios, contractuales y de negocios.		
A.18.1.4 Privacidad y Protección de	Se debe asegurar la privacidad y protección de la información de identificación personal conforme sea		

Información de Identificación Personal	requerido en la legislación y regulación relevante aplicable.		
A.18.1.5 Regulación de Controles Criptográficos	Los controles criptográficos deben ser usados en cumplimiento con todos los acuerdos, legislación y regulaciones relevantes.		
A.18.2 Revisión de Seguridad de la Información	Garantizar que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos de la organización.		
A.18.2.1 Revisión Independiente de la Seguridad de la Información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) deben ser revisados independientemente a intervalos planeados o cuando se ocurran cambios significativos.		

Tabla 45 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.18.2.2 Cumplimiento con Políticas y Normas de Seguridad	Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y procedimientos dentro de su área de responsabilidad con las políticas de seguridad apropiadas, normas y cualquier otro requisito de seguridad.		
A.18.2.3 Inspección de Cumplimiento Técnico	Los sistemas de información deben ser revisados regularmente para su cumplimiento con las políticas y normas		

	de seguridad de la información de la organización.		
--	--	--	--

3.1.1.3.2.6 Formato de pruebas

Tabla 46 Formato de pruebas

Desarrollo de prueba “nombre de la prueba”	
Objetivo de prueba	
Descripción de la prueba	
Técnica	Entrevistas, observaciones, revisión de la información documentada, resumen de datos, análisis e indicadores de desempeño.
Requisito / Control	
Calificación del hallazgo	

Tabla 47 Formato de pruebas(continuación)

Desarrollo de prueba “nombre de la prueba”	
Hallazgo	
Interpretación de resultados	
Recomendaciones	

3.1.1.3.2.7 Formato de remediación de hallazgos

Tabla 48 Formato de remediación de hallazgos

Requisito	Descripción	Hallazgo	Acciones de remediación

3.1.1.3.2.8 Formato de informe de auditoria

1. Alcance

Revisar y evaluar el Sistema de Gestión Integral implementado en el SOC-NOC HORUS, incluyendo los procedimientos, políticas, manuales, anexos, formatos declarados e implementados en los servicios de mesa de ayuda, monitoreo, en sus procesos de atención de incidentes y solicitudes de servicio, atención de problemas, niveles de servicio, procesos de servicios nuevos o modificados, y en todos sus procesos de gestión del servicio y seguridad de la información, ofrecidos por su SOC-NOC Horus, así como, la protección de recursos, servicios y partes interesadas.

2. Objetivo

Verificar si el Sistema de Gestión Integral implementado en la organización es conforme a los requisitos de las normas ISO/IEC 27001:2013 y Anexo A.

3. Equipo auditor

Tabla 49 Equipo auditor

Nombre	Iniciales	Rol
Brenda Itzel Gante Sánchez	BIGS	Auditor en entrenamiento
Lizeth Viridiana Gutiérrez Guerra	LVGG	Auditor en entrenamiento

4. Hallazgos de la auditoria

A continuación, se describen los hallazgos de la auditoría que se identificaron

Tabla 50 Hallazgos de la auditoria

Numeral Requisito	Descripción/Requisitos	Tipo de Hallazgo	Descripción del Hallazgo
#	Descripción (Lista de verificación)	C/NC/OB	Descripción

5. Resultados de la evaluación

Tabla 51 Resultados de la evaluación

Nombre	Iniciales	Rol
Brenda Itzel Gante Sánchez	BIGS	Auditor en entrenamiento
Lizeth Viridiana Gutiérrez Guerra	LVGG	Auditor en entrenamiento

6. Conclusiones de auditoria

El ejercicio se realizó de manera satisfactoria y con base en lo planificado.

7. Distribución del informe

Se realiza la entrega del Informe al responsable del SGI.

8. Comentarios generales del equipo auditor

Lista de comentarios

9. Documentos relacionados

- Lista de verificación
- Informe de remediación de hallazgos

Tabla 52 Autorización del informe

Elaborado por:	
Brenda Itzel Gante Sánchez Auditor en entrenamiento	Lizeth Viridiana Gutiérrez Guerra Auditor en entrenamiento

3.1.1.3.2.9 Formato de informe de recomendación de remediación de hallazgos

1. Alcance

Revisar y evaluar el Sistema de Gestión Integral implementado en el SOC-NOC HORUS, incluyendo los procedimientos, políticas, manuales, anexos, formatos declarados e implementados en los servicios de mesa de ayuda, monitoreo, en sus procesos de atención de

incidentes y solicitudes de servicio, atención de problemas, niveles de servicio, procesos de servicios nuevos o modificados, y en todos sus procesos de gestión del servicio y seguridad de la información, ofrecidos por su SOC-NOC Horus, así como, la protección de recursos, servicios y partes interesadas.

2. Objetivo

Verificar si el Sistema de Gestión Integral implementado en la organización es conforme a los requisitos de las normas ISO/IEC 27001:2013 y Anexo A.

3. Equipo auditor

Tabla 53 Equipo auditor

Nombre	Iniciales	Rol
Brenda Itzel Gante Sánchez	BIGS	Auditor en entrenamiento
Lizeth Viridiana Gutiérrez Guerra	LVGG	Auditor en entrenamiento

4. Recomendación de remediación de hallazgos de auditoria

A continuación, se describen los hallazgos de la auditoría que se identificaron y las recomendaciones de remediación.

Tabla 54 Recomendación de remediación de hallazgos de auditoría

Requisito	Descripción	Hallazgo	Acciones de remediación

5. Documentos relacionados

- Lista de verificación
- Informe de auditoría

Tabla 55 Autorización del informe

Elaborado por:	
Brenda Itzel Gante Sánchez Auditor en entrenamiento	Lizeth Viridiana Gutiérrez Guerra Auditor en entrenamiento

3.1.1.3.2.10 Formato plan de acción

1. Datos generales de la acción

Tabla 56 Datos generales plan de acción

Folio		Fecha de registro	
Tipo de Acción	Correctiva ☒ Preventiva ☐ Mejora ☐	Prioridad	Baja ☐ Media ☐ ☐ Alta ☒
Derivada de	Auditoría interna ☒ Auditoría externa ☐ De la operación ☐ Queja ☐ ☐ Problema ☐ Sugerencia ☐ Revisión por la dirección ☐		

2. Descripción del hallazgo

Tabla 57 Descripción del hallazgo plan de acción

Requisito Normativo Documento(s), y/o activo afectado	Descripción del hallazgo o Problema

3. Análisis de causa raíz

^^ Realizar el análisis mediante el uso de alguna metodología con el fin de detectar la causa raíz, ver procedimiento de acciones correctivas para orientarse ^^

^^ En caso de ser una acción de mejora, el análisis debe incluir lo establecido en las políticas del procedimiento de acciones correctivas ^^

4. Plan de acción

Tabla 58 Plan de acción

Descripción breve de la acción a realizar				
Objetivo / Meta				
No.	Actividad	Fecha de compromiso		Responsables (Iniciales)
		Inicio	Fin	

5. Evaluación del plan de acción

Tabla 59 Evaluación del plan de acción

Estatus	Aprobada ☒ Rechazada ☐	La acción fue rechazada por qué:
---------	---	----------------------------------

6. Eficacia de la acción realizada

Tabla 60 Eficacia del plan de acción

La acción realizada se consideró	Eficaz ☒ Ineficaz ☐	¿Por qué?	
El nivel de eficacia de la acción fue	Alto ☒ Medio ☐ Bajo ☐	¿Por qué?	
Grado de cumplimiento contra el objetivo o meta establecida			Alto ☒ Medio ☐ Bajo ☐
Fecha de Cierre			

7. Resultados

^^Agregar la evidencia del resultado de la implementación del plan de acción^^

3.2 Objetivo 2 Ejecutar la Auditoria

3.2.1 Actividades

3.2.1.1 Actividad 2.1 Recolectar información y evidencias relevantes mediante entrevistas con el personal.

3.2.1.1.1 Descripción de la actividad

La actividad de recolectar información y evidencias relevantes mediante entrevistas con el personal y revisión de documentación es un proceso fundamental en diversas áreas, como la investigación, la auditoría, la gestión de proyectos, entre otros,

Entrevistas con el personal: Los entrevistadores se reúnen con los miembros relevantes del personal para obtener información directa sobre el tema en cuestión. Estas entrevistas pueden ser estructuradas o no estructuradas, y su objetivo es obtener detalles específicos,

perspectivas y conocimientos sobre el tema de interés. Es importante hacer preguntas claras y relevantes para garantizar que se obtenga la información necesaria.

3.2.1.1.2 Resultado de la actividad

3.2.1.1.2.1 Cuestionario día 1 de auditoria

1. ¿De qué manera identifican las cuestiones internas y externas pertinentes para el SGI?

En el Manual del Sistema de Gestión Integrado se presenta un Análisis FODA, el cual detalla las Fortalezas, Debilidades, Oportunidades y Amenazas identificadas por la organización. Las más relevantes están ubicadas en la parte superior de cada sección. Las Fortalezas incluyen la iniciativa para implementar el Sistema de Gestión de Calidad (SGC) conforme a la norma ISO 9001:2015. Entre las Debilidades se destaca la necesidad de concientización y motivación del personal. En cuanto a las Oportunidades, se consideran las empresas de consultoría que podrían ayudar a abordar los desafíos internos actuales. Por último, las Amenazas mencionadas son las nuevas reformas fiscales.

2. ¿Qué acciones toman para las Fortalezas, Debilidades, Oportunidades y Amenazas identificadas por la organización?

Cada uno de estos aspectos identificados se acompaña de una estrategia y se realiza un seguimiento para su implementación y mejora continua.

3. ¿Cómo se identifican a las partes interesadas y dónde se documenta este proceso?

Actualmente no se encuentra documentado, se cuenta con el formato vacío pero los colaboradores cuentan con la información necesaria para identificar a las partes interesadas

4. ¿Cuál es el alcance del Sistema de Gestión Integrado?

Los servicios de mesa de ayuda, monitoreo, SOC y NOC en sus procesos de atención de incidentes y solicitudes de servicio, atención de problemas, niveles de servicio, procesos de servicios nuevos o modificados, y en todos sus procesos de gestión del servicio y seguridad de la información, ofrecidos por su SOC-NOC Horus, así como, la protección

de recursos, servicios y partes interesadas, de acuerdo con la declaración de aplicabilidad (SoA) vigente

5. ¿Qué servicios ofrece la organización?

Mesa de servicio, Monitoreo, NOC (Centro de Operaciones de Red), SOC (Centro de Operaciones de Seguridad)

6. ¿Cómo se define y documenta el sistema de gestión integral?

Se dispone de un modelo sistémico meticulosamente diseñado que facilita la identificación y comprensión integral de los procesos que conforman el Sistema de Gestión Integrado (SGI). Este modelo no solo abarca los procesos centrales de entrega y demanda, sino que también incluye los procesos estratégicos y de control, fundamentales para el funcionamiento eficiente y efectivo del SGI. En detalle, el modelo ofrece una visión perteneciente de las interacciones dinámicas entre estos procesos, sus respectivos subprocesos y los individuos o equipos encargados de su ejecución. Esta estructura sistemática proporciona una base sólida para la gestión y optimización continua de los procesos dentro del SGI, asegurando así la alineación con los objetivos organizacionales y la entrega de resultados consistentes y de alta calidad.

7. ¿De qué manera la alta dirección muestra el liderazgo ante la organización y su sistema de gestión integral?

La alta dirección participa activamente en las sesiones de auditoría, asumiendo además la responsabilidad de asignar y supervisar los recursos necesarios. También juega un papel crucial en la toma de decisiones relacionadas con la asignación y apoyo de roles y responsabilidades, con un enfoque especial en la satisfacción del cliente.

8. ¿En dónde se encuentra documentada la política de seguridad de la información?

La política se encuentra debidamente documentada en el Manual del Sistema de Gestión Integrado.

9. ¿Como se autorizó la política?

La alta dirección lleva a cabo la autorización formal.

10. ¿Como aseguran que los colaboradores conocen esta política?

Se emite un comunicado interno y externo sobre el tema, y la política correspondiente está disponible para su consulta en nuestra página web oficial.

11. ¿Dónde se encuentran documentadas los roles y responsabilidades del comité?

Los roles y responsabilidades del comité están debidamente documentados en el Manual del Sistema de Gestión Integrado. Además, en dicho manual se detallan los puestos relacionados con dichas responsabilidades para una clara comprensión y ejecución de las funciones asignadas.

12. ¿Como se dan a conocer los roles y responsabilidades?

Se elabora una minuta con el propósito de documentar la divulgación de roles y responsabilidades, la cual requiere firma para validar su recepción. Además, se emiten comunicados correspondientes para asegurar una adecuada transmisión de información.

13. ¿Qué documento utilizan para abordar riesgos y oportunidades?

Tenemos el registro Matriz de Oportunidades en la versión 1 que se generó el 1 de abril del 2023, se encuentra en el repositorio como Re Matriz de Oportunidades V01 específicamente en la categoría "Elementos del Entorno", se establece una asociación con los elementos identificados en el Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas)

14. ¿Cuentan con algún proceso de valoración de riesgos de seguridad de la información?

Si se tiene el procedimiento que cuenta con las siguientes 9 actividades

Identificación de elementos críticos

Clasificación de elementos

Amenazas

Probabilidad de ocurrencia

Impacto (humano, material, financiero, operativo, imagen

Identificación del riesgo

Tipo de tratamiento (aceptación, mitigación, transferencia, eliminación)

Aceptación de riesgos residuales

Revisar la eficacia de los controles

El procedimiento se encuentra documentado en el documento Re_Valoración, evaluación y tratamiento de riesgos V09

15. ¿Se tiene algún riesgo detectado actualmente?

Se tienen detectados 70 elementos detectados, todos se encuentran en un nivel bajo y se encuentran en el documento Re_Valoración de riesgos 2do semestre 2023 que fue actualizado por última vez el 31 de agosto del 2023

16. ¿Como evalúan los riesgos de seguridad de la información?

La organización cuenta con el procedimiento Valoración, evaluación y tratamiento de riesgos, el cual comprende un total de 9 actividades a desarrollar para el proceso de valoración, evaluación y tratamiento de riesgos: Identificación de elementos críticos, Clasificación de elementos, Identificación de amenazas, Evaluación de la probabilidad de ocurrencia, Evaluación del impacto en aspectos humano, material, financiero, operativo e imagen, Identificación del riesgo resultante, Determinación del tipo de tratamiento del riesgo (aceptación, mitigación, transferencia, eliminación), Aceptación de los riesgos residuales después de aplicar los controles y Revisión de la eficacia de los controles implementados.

Estas actividades proporcionan un marco estructurado para identificar, evaluar y abordar los riesgos en la organización, asegurando así la gestión efectiva de la seguridad y la continuidad del negocio.

17. ¿Qué roles están asignados para la gestión de riesgos en la organización?

Actualmente, no se cuenta con un propietario claramente identificado para gestionar los riesgos.

18. ¿Cómo están definidas las responsabilidades del propietario de la gestión de riesgos?

Aunque hay responsables asignados, las responsabilidades del rol de propietario de la gestión de riesgos no están definidas de manera precisa

19. ¿Dónde se localizan los objetivos documentados?

En el manual del Sistema de Gestión Integrado (SGI) existe un apartado destinado para los objetivos del SGI en el cual incluyen los objetivos, métrica, meta, periodicidad y responsable.

20. ¿Cuántos objetivos tienen registrados?

Actualmente se han registrado 10 objetivos

21. ¿Qué abarcan los objetivos registrados?

Abarcan áreas clave de desempeño, tales como el aumento en el número de servicios contratados (cuatro anuales), la salvaguarda de la confidencialidad de la información de las partes interesadas mediante la prevención de incidentes con impacto (menos de dos), y la satisfacción del cliente, medida en un índice del 88.5%.

22. ¿Qué documentos se muestran en relación con la gestión de mejora continua?

La organización cuenta con el procedimiento de Gestión de mejora continua en la versión número 3 actualizado el 21 de agosto del 2023 y el registro de la Matriz de monitoreo generado el 21 de agosto del 2023 correspondiente.

23. ¿Cuál es la deficiencia identificada en los informes?

Se identificó que los informes de Recursos Humanos proporcionan una verificación adecuada del cumplimiento de los indicadores establecidos.

24. ¿Quién lleva a cabo revisiones del sistema de gestión de la calidad de la organización?

La alta dirección lleva a cabo estas revisiones.

25. ¿Con qué objetivo se realizan estas revisiones del sistema de gestión de la calidad?

Se realizan en intervalos planificados para garantizar la pertinencia, idoneidad, eficacia y continua alineación con la dirección estratégica de la organización.

26. ¿Se cuenta con un documento donde alta dirección haga la revisión del SGI?

Se cuenta con el registro Revisión por Dirección del 3er trimestre del 2023 generado el 1 de septiembre del 2023, este documento documenta los resultados y las acciones derivadas de la revisión por dirección realizada en el tercer trimestre del año 2023.

27. ¿Se cuenta con un calendario de auditoria?

Se tiene el Calendario de Auditoría interna para el 2023 donde se considera el tiempo para la evaluación de los requisitos inherentes al sistema de gestión integral

28. ¿Se tiene un plan de auditoria previsto para algún ejercicio?

Para cumplir con el calendario de auditoria se tiene el plan de auditoría interna que considera todos los requisitos para el SGI

29. ¿Los auditores tienen las competencias necesarias para realizar el ejercicio?

Los auditores que llevan a cabo el ejercicio de auditoria cuentan con la constancia de la competencia adquirida para auditar la norma ISO 27001:2023

30. Cuando existe un hallazgo calificado como OM o NC ¿Tienen algún plan de acción?

Si, para cada hallazgo calificado como OM o NC se genera un plan de acción para mitigarlo

31. ¿Cuentan con un plan de acción de su último ejercicio de auditoria?

En el último ejercicio de auditoria se calificó con una OM el requisito referente a auditoría interna en este momento se encuentra aún en proceso, tiene un folio de identificación con número 146 el cual fue generado el 5 de junio del 2023

32. ¿Cuentan con un documento en relación con la mejora del servicio de mesa de ayuda?

Se cuenta con el registro Plan de Acción con el folio de identificación numero 154 el cual fue generado el 27 de julio de 2023. El propósito es mejorar el servicio de mesa de ayuda en respuesta a las sugerencias recopiladas a través de las encuestas de satisfacción y se encuentra en fase de ejecución.

33. ¿Qué documentos evidencian el respaldo de los recursos necesarios para las operaciones de la organización?

La organización cuenta con los registros Organigrama 2023, Presupuesto 2023 y Plan de Capacidad 2023

34. ¿Qué información proporciona el registro Organigrama?

Proporciona una representación gráfica clara de la estructura jerárquica y funcional de la organización, delineando las relaciones y responsabilidades entre diferentes unidades y roles dentro de la misma.

35. ¿Qué información detalla el registro Presupuesto?

Proporciona una estimación precisa de los recursos monetarios asignados y disponibles para el funcionamiento de la organización, permitiendo una planificación financiera adecuada y una gestión eficiente de los recursos.

36. ¿Qué establece el registro Plan de Capacidad?

Establece proyecciones y estrategias para garantizar que la organización cuente con los recursos humanos, tecnológicos y físicos necesarios para satisfacer la demanda y las expectativas operativas a corto y largo plazo.

37. ¿Qué documentos se muestran en relación con la concientización del personal?

Se cuenta con el registro del Plan de Concientización y el registro Procedimiento de Concientización y Comunicación del SGI.

38. ¿Cuáles son los aspectos abordados en los comunicados dirigidos a la concientización del personal?

Los aspectos clave abordados son: la contribución de los colaboradores a la eficacia del SGI, las consecuencias derivadas del incumplimiento de los requisitos legales y normativos, la política del SGI y los objetivos establecidos por el SGI. donde se reconoce la eficacia de estas comunicaciones como instrumento para fortalecer la comprensión y el compromiso del personal con los principios y objetivos del SGI tambien se recomienda una revisión continua y periódica de estos comunicados para

asegurar su pertinencia y efectividad en la concientización del equipo respecto a la importancia y responsabilidad en la gestión integral de la organización.

39. ¿Tienen algún documento donde se declare el procedimiento del control documental de la organización?

Se tiene el procedimiento Control de documentos en su segunda versión actualizado el 5 de mayo del 2023

40. ¿Qué documentos se muestran en relación con el control de documentos?

Se cuenta con el "Pr_Control de documentos_V02" actualizado el 5 de mayo del 2023 y el "Re_Inventario de documentos_2023" actualizado el 8 de diciembre del 2023.

41. ¿Dónde se encuentran los procedimientos, manuales, políticas, anexos, registros, constancias y todo lo documental?

Toda la documentación de la organización necesario para el SGI se encuentra en el repositorio documental ahí se ubican los editables, respaldos y los documentos obsoletos.

42. ¿Cómo ha establecido la organización las competencias necesarias para los colaboradores que participan en la prestación de servicios?

La organización ha establecido las competencias necesarias a través de perfiles de puestos.

43. ¿Cuentan con algún perfil de puesto evaluado?

Esta el perfil de puesto del coordinador de recursos humanos que corresponde a María Guadalupe Soriano Mejía que se verifico junto a su Curriculum Vitae, constancia de formación de auditores internos, constancia de Auxiliar de Recursos Humanos y su Diplomado en Psicología.

44. ¿Cómo ha sido la evaluación del puesto en términos de cumplimiento?

La evaluación del puesto reveló un cumplimiento del 100% en este aspecto.

45. ¿Qué tipo de evaluaciones y verificaciones aplican a los candidatos que están considerando contratar?

Se realiza un estudio socioeconómico junto con pruebas psicométricas

46. ¿Estás verificaciones o evaluaciones de las que hablamos, aplican a todos los candidatos sin importar el puesto para el que estén siendo considerados o solamente se les aplican a ciertos puestos?

Se aplican a todos por igual evaluar la comprensión de responsabilidades y la idoneidad de los colaboradores para los roles.

47. En el contrato laboral que se firma con los colaboradores, ¿se les especifica sus responsabilidades incluyendo las responsabilidades relacionadas con seguridad y con el sistema de gestión?

Si, en el contrato que se firma al inicio de la relación laboral en el cual se detallan las responsabilidades tanto del individuo como de la organización se incluye en el contrato una cláusula de confidencialidad

48. ¿Cuentan con evidencia que demuestre que la alta dirección exige a todos los colaboradores el cumplir sus responsabilidades?

Se realiza a través de los perfiles de puesto, los cuales cuentan con las firmas de los que cubren el rol

49. ¿Cuentan con alguna política, proceso y/o planes en dónde aborden los temas de concientización y capacitación de todo el personal en materia de seguridad de la información, privacidad de datos y otros temas relevantes para que desempeñen sus funciones?

Se cuenta con el Plan de capacitación incluye temas relacionados a seguridad de la información y al Sistema de Gestión de la Información (SGI), actualmente se encuentra en ejecución

50. ¿En el año 2023 se ha aplicado algún proceso disciplinario?

No se ha aplicado ninguno

51. ¿Se tienen algún caso en los últimos 12 meses, de alguien que hayan promovido o cambiado de puesto?

Si, se realizó el cambio de puesto de Gabriel Arcega Soto

52. ¿Qué documentos tiene para evidenciar el cambio de puesto?

Se realizo un expediente de todas las solicitudes, minuta, cartas necesarias para la gestión del cambio

53. En caso de que finalice una relación laboral ¿Como recuerdan las responsabilidades que tienen en relacion a la seguridad de la información o derechos ARCO?

Actualmente no se hace un recordatorio de las responsabilidades o derechos ARCO al finalizar la relación laboral

NOTA: Durante la auditoría ISO 27001, se aplicaron cuestionarios a través de la herramienta de videoconferencia Meet Y Microsoft Teams. La sesión fue grabada para garantizar la correcta documentación del proceso. Sin embargo, por razones de confidencialidad de la empresa, no es posible mostrar ni compartir la grabación.

3.2.1.1.2.2 Cuestionario día 2 de auditoria

1. ¿Como mantienen el control de los procesos para la seguridad de la información?

La organización ha documentado meticulosamente sus procedimientos, respaldada por un Plan de Aseguramiento del Mantenimiento del Avance (PAMA) de procesos. Cada procedimiento ha sido detallado con el objetivo de garantizar la claridad y consistencia en su ejecución. Además, se han establecido indicadores de desempeño específicos en cada uno de ellos para medir y evaluar el cumplimiento de los objetivos y detectar áreas de mejora continua.

2. ¿Como mantienen controlados los cambios que sufre la organización?

La organización ha implementado un procedimiento dedicado a la gestión del cambio. Este procedimiento facilita una transición suave y efectiva en situaciones donde se requieran modificaciones en los procesos, políticas o infraestructura organizacional. A través de este procedimiento, se establecen pasos y controles específicos para evaluar, aprobar e implementar cambios, minimizando así los riesgos y maximizando el éxito de cualquier modificación realizada.

3. ¿Cuál es el proceso mediante el cual los requisitos de seguridad de la información se establecen y documentan en colaboración con los proveedores para mitigar los riesgos asociados con su acceso a los activos de la organización?

La organización utiliza el proceso identificado como Gestión de compras y proveedores, actualizado el 28 de junio de 2023, para gestionar proveedores externos, lo cual incluye la gestión de disputas contractuales.

Dentro de este proceso, se destaca la sección 2.4.5.3, relacionada con la base de datos de proveedores. Esta base de datos contiene información detallada sobre cada proveedor, incluyendo datos de identificación y contacto. Además, se lleva a cabo un control de documentos que deben formar parte del expediente de cada proveedor, como el CIF, el acta constitutiva, comprobantes de domicilio, entre otros.

Hasta la fecha de la documentación, se han registrado un total de 39 proveedores en la base de datos.

Por lo tanto, la organización gestiona proveedores externos mediante un proceso estructurado que incluye la gestión de disputas contractuales y un control detallado de los documentos relacionados con cada proveedor.

4. ¿Cómo se asegura la organización de que todos los requisitos de seguridad de la información relevantes se establezcan y acuerden con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de la infraestructura de TI de la información de la organización?

La organización registra en su base de datos de proveedores los datos de identificación y contacto de cada uno, así como un control de documentos que deben incluirse en su expediente, como el CIF, el acta constitutiva, comprobantes de domicilio, entre otros. Sin embargo, no se abordan explícitamente los requisitos de seguridad de la información relevantes con cada proveedor, lo que podría ser un área de mejora en la gestión de seguridad de la información.

5. ¿Qué requisitos se incluyen en los acuerdos con proveedores para abordar los riesgos de seguridad de la información asociados con la información y los servicios de tecnología de las comunicaciones y la cadena de suministro de productos?

Aunque se establece un contrato con los proveedores y se comunica las políticas de seguridad de la información mediante una lista de distribución, no se abordan explícitamente los riesgos de seguridad relacionados con los proveedores. Esta falta de enfoque en los riesgos de seguridad podría representar un punto débil en la gestión de seguridad de la información de la organización.

6. ¿Cómo garantizan las organizaciones el monitoreo, revisión y auditoría regular de la entrega del servicio por parte de los proveedores?

El documento Procedimiento Gestión de compras y proveedores, actualizado el 28 de junio de 2023, aborda la gestión de proveedores, incluyendo disputas contractuales. En cuanto a la base de datos de proveedores, se detallan los datos de identificación y contacto, así como los documentos que deben integrar el expediente de cada proveedor. Se menciona que hay 39 proveedores registrados en la base de datos.

Además, el contrato con los proveedores y la evaluación de los mismos son aspectos importantes. Se indica que se ha llevado a cabo una evaluación de proveedores durante el primer semestre, donde se identificaron y evaluaron a 17 proveedores de los 39 registrados. Se aclara que esta evaluación se realizó únicamente a los proveedores a los que se les hizo una compra.

Por otro lado, se comunica las políticas de seguridad de la información a través de una lista de distribución, enviando las políticas pertinentes a los proveedores.

Sin embargo, no se menciona una trazabilidad clara entre la evaluación de proveedores y la base de datos, ya que no se indica en la base de datos qué proveedores están activos. Aunque se afirma que solo se trabajó con 17 proveedores, la base de datos muestra que se tiene contrato con todos los 39 proveedores registrados.

7. ¿Cómo se administran los cambios en la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados, y la revaloración de los riesgos?

La gestión de cambios en la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y la mejora de las políticas de seguridad de la información existentes,

procedimientos y controles, se lleva a cabo según el documento Procedimiento Gestión de compras y proveedores, actualizado el 28 de junio de 2023.

8. ¿Cuentan con una política de seguridad de la información en dónde se establezcan todos los lineamientos de seguridad que se deben seguir internamente?

Se cuenta con la política de Seguridad de la información

9. ¿Cuándo fue la última vez que se revisó este documento?

Se reviso por última vez el 15 de marzo del 2023 generándose la versión vigente, la número 8

10. ¿Tienen documentado en algún lugar, cada cuándo se deben revisar las políticas de seguridad para ver si se requieren hacer actualizaciones?

Según las políticas definidas se debe revisar una vez al año, cuando exista la necesidad de adaptar o existan cambios significativos en la organización.

11. ¿Cuentan con roles definidos?

Si, se cuentan con roles definidos algunos de ellos son el comité del Sistema de Gestión Integral, responsable de la Gestión del Servicio, responsable del Diseño y Despliegue de Servicios.

12. ¿Quiénes conforman el comité del Sistema de Gestión Integral?

El comité del SGI se encuentra conformado por Dirección General Adjunta, responsable del SGI y Responsable de Seguridad de la Información

13. ¿Cómo determinan cuáles son las tareas o actividades que deben segregarse para evitar riesgos?

Se determinan mediante segregación de deberes, ingreso a portales, casos de negocio, aceptación de cambios en la configuración,

14. ¿Cuentan con algún documento en donde tengan un listado de las autoridades relevantes en materia de seguridad con las que requieran mantener contacto?

Se cuenta con el registro matriz contacto autoridades el cual fue actualizado el 23 de agosto del 2023 pero este solo considera a las autoridades especiales

15. ¿Cuentan con algún documento en donde tengan un listado de los grupos de interés en materia de seguridad con las que requieran mantener contacto?

En el mismo registro matriz contacto autoridades hay un apartado destinado a grupos especiales

16. ¿Quiénes forman parte de la lista de contacto?

contactos y boletines para OWASP, UNAM-CERT, SANS y Alienvault OTX

17. ¿Cuentan con un proceso o documento en dónde se hable sobre seguridad en los proyectos?

El formato Implementación de servicio en la versión número 4 actualizado el 25 de mayo del 2023 considera endpoint para infonavit.

18. ¿Cuentan con algún proyecto en curso?

Si, para el seguimiento de este se tiene el registro del plan de trabajo para la instalación de memorias RAM y discos duros en servidores

19. ¿Qué políticas o lineamientos internos tienen documentados acerca del uso de dispositivos móviles dentro de la organización?

Se cuenta con la política de uso de teléfonos inteligentes y cámaras digitales

20. ¿Se tiene permitido el trabajo remoto?

Si

21. ¿Cuentan con una política documentada en dónde se determina si se permite o no, o en casos si y en qué casos no?

Se cuenta con la política de movilidad la cual especifica el uso de VPN y otras medidas de seguridad

22. ¿Cómo establecen las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?

La organización cuenta con un documento llamado Procedimiento Incidentes de seguridad de la información, fechado el 9 de junio del 2023, que establece responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

23. ¿Cuál es el proceso para reportar eventos de seguridad de la información a través de los canales de gestión adecuados de manera rápida?

Durante el año 2023, no se han reportado incidentes de seguridad de la información en la organización, por lo tanto, no ha sido necesario activar el proceso de reporte a través de los canales de gestión.

24. ¿Qué medidas se implementan para asegurar que tanto empleados como contratistas anoten e informen cualquier debilidad de seguridad de la información en los sistemas y servicios de la organización?

A pesar de que no se han reportado incidentes de seguridad de la información en 2023, la organización mantiene la exigencia a empleados y contratistas de anotar e informar cualquier debilidad de seguridad de la información en los sistemas y servicios según los procedimientos establecidos.

25. ¿Cómo se determina si los eventos de seguridad de la información deben ser clasificados como incidentes de seguridad de la información?

Dado que no se han reportado incidentes de seguridad de la información en 2023, no ha sido necesario llevar a cabo evaluaciones para decidir si clasificar eventos como incidentes de seguridad.

26. ¿Cuáles son los procedimientos documentados que se deben seguir al responder a los incidentes de seguridad de la información?

Los procedimientos documentados para responder a los incidentes de seguridad de la información, aunque existen, no han sido activados durante el año 2023 debido a la ausencia de reportes de incidentes.

27. ¿De qué manera se utiliza el conocimiento adquirido del análisis y resolución de incidentes de seguridad de la información para reducir la probabilidad o impacto de futuros incidentes?

A pesar de la ausencia de incidentes reportados en 2023, el conocimiento previo adquirido del análisis y resolución de incidentes en años anteriores puede ser utilizado para fortalecer aún más los controles y procedimientos de seguridad de la información.

28. ¿Qué procedimientos ha establecido la organización para la identificación, recopilación, adquisición y preservación de la información que podría ser utilizada como evidencia en casos de seguridad de la información?

Aunque no se han activado en el año 2023, la organización mantiene los procedimientos establecidos para la identificación, recopilación, adquisición y preservación de la información que podría servir como evidencia en casos de seguridad de la información, según lo establecido en sus políticas y documentos pertinentes.

NOTA: Durante la auditoría ISO 27001, se aplicaron cuestionarios a través de la herramienta de videoconferencia Meet Y Microsoft Teams. La sesión fue grabada para garantizar la correcta documentación del proceso. Sin embargo, por razones de confidencialidad de la empresa, no es posible mostrar ni compartir la grabación.

3.2.1.1.2.3 Cuestionario día 3 de auditoría

1. ¿Cómo determinan sus requisitos de seguridad de la información y gestionar la continuidad de la seguridad de la información durante situaciones adversas, como crisis o desastres?

La organización debe tener un plan de continuidad y disponibilidad que aborde una variedad de situaciones adversas, como cortes de energía eléctrica, cortes de comunicaciones, indisponibilidad de instalaciones, ausentismo, emergencias sanitarias y

situaciones políticas o sociales, como se muestra en el documento Formato Plan de continuidad y disponibilidad fechado el 2 de mayo del 2023.

2. ¿Qué procesos, procedimientos y controles debe establecer, documentar, implementar y mantener una organización para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa?

La organización garantiza el nivel requerido de continuidad para la seguridad de la información durante situaciones adversas, como se detalla en el documento Formato Plan de continuidad y disponibilidad fechado el 2 de mayo del 2023. Esto incluye la realización de pruebas anuales a los planes de continuidad y disponibilidad, con un informe exitoso de las pruebas realizadas en septiembre, según lo establecido en la política de la organización.

3. ¿Con qué frecuencia la organización debe verificar los controles de continuidad de seguridad de la información para asegurar su validez y eficacia durante situaciones adversas?

Los controles de continuidad de seguridad de la información deben ser verificados al menos una vez al año, durante las pruebas de los planes de continuidad y disponibilidad, que se llevan a cabo en septiembre y octubre. Además, se debe considerar el informe de pruebas realizado en septiembre, que resultó exitoso, para asegurar que los controles sean válidos y eficaces durante situaciones adversas.

4. ¿Cómo se garantiza que las instalaciones de procesamiento de la información estén implementadas con suficiente redundancia para cumplir con los requisitos de disponibilidad dentro de la organización?

Se muestra el Registro Diagrama de red fechado el 3 de abril del 2023, donde se identifica la redundancia de los servicios, incluyendo enlaces perimetrales y switches, lo que asegura la disponibilidad adecuada de las instalaciones de procesamiento de la información.

5. ¿Cómo se asegura la documentación y disponibilidad de los procedimientos operativos para todos los usuarios que los requieran?

Se cuenta con los procedimientos operativos de Gestión del cambio, Gestión de la capacidad, Gestión de la disponibilidad, Gestión de la configuración, Diseño y transición de servicios, Respaldo y Control de documentos, continuidad, todos fechados el día 19 de mayo de 2023. Estos procedimientos están disponibles para todos los usuarios que los requieran.

6. ¿Cuentan con un proceso que permita controlar los cambios a sistemas e infraestructura?

La organización cuenta con un proceso para controlar los cambios a sistemas e infraestructura, como se indica en el Procedimiento Gestión del cambio fechado el 19 de mayo del 2023, el cual incluye los elementos solicitados por el requisito.

7. ¿En dónde llevan el registro de los cambios que van haciendo, es decir utilizan una herramienta de tickets o algo similar?

El registro de los cambios se lleva a cabo utilizando la herramienta Aranda, que se utiliza para gestionar los cambios en la infraestructura o en los servicios. Se muestra un caso específico, el Registro Caso no. 63 / CHG8268-1-63 fechado el 17 de marzo del 2023 por Saul Gómez del cliente Secretaría de Turismo, donde se observa que se adjuntan debidamente los requisitos a la solicitud de cambio al caso creado. Sin embargo, se destaca que en los criterios de impacto no existe un criterio compatible con lo configurado en la herramienta Aranda.

8. ¿Cuentan con un proceso o lineamiento en dónde se especifique cómo llevan a cabo la gestión de la capacidad?

La organización cuenta con un proceso o lineamiento que especifica cómo llevan a cabo la gestión de la capacidad. Se presenta el Formato Plan de capacidad correspondiente al día 20 de enero del año 2023, el cual abarca los activos, el período de evaluación, los datos analizados, la audiencia objetivo y los recursos necesarios para garantizar la provisión efectiva de los servicios.

9. ¿Podemos ver cómo monitorean el ambiente productivo en dónde está la aplicación obtén más o la que es utilizada para brindar los servicios de Saynet?

El monitoreo del ambiente productivo donde se encuentra la aplicación "Obtén Más" o la utilizada para brindar los servicios de Saynet se lleva a cabo de forma bimestral. Se constata que este monitoreo contempla los umbrales de los servicios y sus componentes, así como los recursos técnicos y los indicadores clave de rendimiento (KPIs) para el año 2023.

10. ¿Cuentan con un diagrama de su infraestructura en dónde podamos ver cómo es que tienen separados los ambientes de pruebas, desarrollo y productivos?

Específica sobre la existencia de un diagrama de infraestructura que muestre la separación de los ambientes de pruebas, desarrollo y productivos. Sin embargo, se destaca que se ha constatado la existencia de un entorno de desarrollo que cumple con estándares de seguridad adecuados, lo que contribuye a mitigar riesgos y asegurar la integridad de los sistemas durante el proceso de desarrollo de software

11. ¿Cómo se asegura la implementación de controles de detección, prevención y recuperación para protegerse contra el malware, y cómo se combinan estos controles con una adecuada concientización a los usuarios dentro de la organización?

La organización cuenta con un sistema de seguridad informática, específicamente Kaspersky, instalado en todos los equipos utilizados para brindar servicios. Esta medida asegura una protección integral contra amenazas cibernéticas y contribuye a mantener la integridad y confidencialidad de la información.

12. ¿Cómo garantizan que las copias de respaldo de la información, software e imágenes de sistemas se realicen y prueben regularmente de acuerdo con la política de respaldos acordada?

La organización garantiza el cumplimiento de la política de respaldos mediante la implementación del Registro Bitácora de respaldos, fechada el día 8 de febrero del 2023. Esta bitácora muestra la realización regular de respaldos completos e incrementales para los sistemas de ofimática, PRTG, Firewall y switches. Esta práctica asegura la disponibilidad y la integridad de los datos, así como la capacidad de recuperación en caso de incidentes.

13. ¿Cómo generan, mantienen y revisan regularmente los registros de eventos de las actividades de usuarios, excepciones, fallas y eventos de seguridad de la información?

La organización cumple con esta práctica mediante la confirmación de la presencia de la herramienta de Directorio Activo en el sistema dentro de la organización. Esta herramienta es fundamental para la gestión centralizada de usuarios, equipos y recursos dentro del entorno de red, lo que facilita la administración eficiente de los sistemas y contribuye a mantener la seguridad y el orden en el ambiente informático. Además, el Directorio Activo registra eventos de actividad de usuarios, excepciones, fallas y eventos de seguridad de la información, lo que permite mantener un registro completo y actualizado de todas las actividades relevantes.

14. ¿Cómo protegen el acceso no autorizado y la manipulación de la información en las instalaciones/infraestructura del registro?

La organización protege contra el acceso no autorizado y la manipulación de la información en las instalaciones/infraestructura del registro mediante la verificación de la presencia de la herramienta de Directorio Activo en el sistema. Además, se observa que la segregación por perfil de usuario impide la modificación de registros y/o archivos de información, lo que fortalece la seguridad y la integridad de los datos almacenados en el sistema. Este enfoque garantiza que solo usuarios autorizados tengan acceso a la información y evita cualquier intento de manipulación no autorizada.

15. ¿Cómo registran, protegen y revisan los eventos de las actividades del administrador y del operador de sistemas?

La organización registra, protege y revisa los eventos de las actividades del administrador y del operador de sistemas mediante la presencia de la herramienta de Directorio Activo en el sistema. Además, se observa que la segregación por perfil de usuario impide la modificación de registros y/o archivos de información. Se destaca que únicamente el área de Operaciones cuenta con permisos de administración, lo que garantiza un control adecuado sobre los cambios realizados en el sistema y fortalece la seguridad de la información. Esta configuración asegura que las actividades de administradores y

operadores de sistemas sean registradas y monitoreadas de manera efectiva, minimizando los riesgos de manipulación no autorizada de registros y archivos.

16. ¿Cómo garantizan que los relojes de todos los sistemas de procesamiento de la información relevantes dentro de la organización o dominio de seguridad estén sincronizados con una sola fuente de tiempo de referencia?

La organización garantiza la sincronización de los relojes mediante el uso del protocolo NTP (Network Time Protocol) a través del servidor Cronos ubicado en el Centro Nacional de Metrología (CENAM), específicamente en la dirección 1.cronos.cenam.mx. Este enfoque asegura que todos los sistemas de procesamiento de la información utilicen una fuente de tiempo de referencia confiable y precisa, lo que contribuye a la consistencia y precisión en los registros de tiempo en toda la organización.

17. ¿Cómo implementan procedimientos para controlar la instalación de software en sistemas operacionales?

La organización implementa procedimientos para controlar la instalación de software en sistemas operacionales mediante la asignación exclusiva de privilegios de administración al área de operaciones. Esto les otorga la capacidad de instalar software y aplicaciones en los sistemas. Además, se dispone de un listado de software permitido y cualquier adición a este listado debe ser previamente autorizada por la Dirección General. Este enfoque garantiza un control adecuado sobre la instalación de software, minimizando los riesgos asociados con la instalación no autorizada y promoviendo la seguridad y la integridad del sistema.

18. ¿Cómo obtienen información acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados de manera oportuna, evalúa la exposición de la organización a tales vulnerabilidades y toma medidas apropiadas para tratar los riesgos asociados?

La organización obtiene información sobre las vulnerabilidades técnicas de los sistemas de información mediante la realización de análisis de vulnerabilidades de manera anual en el sistema. Se proporciona información sobre el análisis de vulnerabilidades correspondiente al año 2023, el cual arrojó un total de 40 hallazgos críticos y 15 hallazgos

informativos. Esta información permite a la organización evaluar la exposición a tales vulnerabilidades y tomar medidas apropiadas para tratar los riesgos asociados, fortaleciendo así la seguridad de los sistemas de información utilizados.

19. ¿Cómo establecen e implementan reglas que gobiernan la instalación de software por los usuarios?

La organización establece e implementa reglas que gobiernan la instalación de software por los usuarios mediante la asignación exclusiva de privilegios de administración al área de operaciones. Esto les otorga la capacidad de instalar software y aplicaciones en los sistemas. Además, se dispone de un listado de software permitido y cualquier adición a este listado debe ser previamente autorizada por la Dirección General. Este enfoque garantiza un control adecuado sobre la instalación de software, minimizando los riesgos asociados con la instalación no autorizada y promoviendo la seguridad y la integridad del sistema.

20. ¿Cómo planifican y acuerdan los requisitos de la auditoría y las actividades de verificación de los sistemas operativos para minimizar las interrupciones a los procesos del negocio?

La organización planifica y acuerda cuidadosamente los requisitos de la auditoría y las actividades de verificación de los sistemas operativos para minimizar las interrupciones a los procesos del negocio. Esto se evidencia mediante la realización de auditorías periódicas a la Base de Datos de Gestión de Configuración (CMDB), así como análisis de vulnerabilidades y auditorías de registros. Este enfoque ayuda a mantener la integridad y la seguridad de los sistemas operativos mientras se minimizan las interrupciones a las operaciones comerciales.

21. ¿Cómo garantiza la organización la protección de la información en las redes e infraestructura de apoyo para el procesamiento de información?

La organización garantiza la protección de la información en las redes e infraestructura de apoyo para el procesamiento de información mediante la implementación de la Política del Firewall , fechada el día 13 de marzo del 2023. Además, utiliza el Directorio Activo para acceder a los servicios bajo perfiles establecidos.

22. ¿Cómo gestionan y controlan las redes para proteger la información en los sistemas y aplicaciones?

La organización gestiona y controla las redes para proteger la información en los sistemas y aplicaciones mediante la implementación de una segregación de redes dentro de su infraestructura.

23. ¿Qué medidas toma la organización para identificar y incluir los mecanismos de seguridad, niveles de servicio y requisitos de gestión en los acuerdos de servicios de red, ya sea que estos servicios sean provistos internamente o subcontratados?

La organización asegura que los mecanismos de seguridad, niveles de servicio y requisitos de gestión para todos los servicios de red sean identificados e incluidos en los acuerdos de servicios de red mediante la implementación de la Política del Firewall , fechada el día 13 de marzo del 2023. Además, utiliza el Directorio Activo para acceder a los servicios bajo perfiles establecidos.

24. ¿Cómo se aseguran de que los grupos de servicios de información, usuarios y sistemas de información estén segregados en las redes?

La organización se asegura de que los grupos de servicios de información, usuarios y sistemas de información estén segregados en las redes mediante la identificación de un diagrama de red que muestra claramente esta segregación. El diagrama también ilustra la infraestructura del Centro de Operaciones de Seguridad (SOC-NOC) y la red de usuarios de SAYNET, lo que garantiza que cada grupo esté adecuadamente separado en la red para mejorar la seguridad y proteger la integridad de los datos.

25. ¿Cómo protege la organización la transferencia de información a través del uso de cualquier tipo de medio de comunicación?

La organización protege la transferencia de información mediante el uso de la Política de Convenios de confidencialidad, cifrado de seguridad mediante el uso de contraseñas, 7ZIP y VPN, fechada el día 11 de julio del 2023.

26. ¿Cómo se aseguran de que los acuerdos aborden la transferencia segura de la información del negocio entre la organización y partes externas?

La organización se asegura de que los acuerdos aborden la transferencia segura de la información del negocio entre la organización y partes externas mediante la inclusión de cláusulas específicas en los contratos. Se muestra evidencia del contrato con EFD, el cual incluye la cláusula 14 de Confidencialidad y privacidad de datos, firmado de aceptación. Asimismo, se presenta el contrato con Hospital Satélite, que incluye cláusulas de confidencialidad y no divulgación, privacidad de datos y acuerdos de transferencia de información, todos ellos firmados. Estas cláusulas garantizan que la información del negocio se transfiera de manera segura y protegida, cumpliendo así con los requisitos de seguridad y privacidad.

27. ¿Qué medidas toma la organización para garantizar que la información involucrada en mensajes electrónicos esté protegida adecuadamente?

La organización asegura que la información involucrada en mensajes electrónicos esté protegida adecuadamente mediante la implementación de la Política de Convenios de confidencialidad, cifrado de seguridad mediante el uso de contraseñas, 7ZIP y VPN, fechada el día 11 de julio del 2023.

28. ¿Cómo se aseguran de que los requisitos para los acuerdos de confidencialidad o no divulgación se identifiquen, revisen regularmente y documenten, reflejando adecuadamente las necesidades de la organización para la protección de la información?

La organización asegura que los requisitos para los acuerdos de confidencialidad o no divulgación se identifiquen, revisen regularmente y documenten, reflejando adecuadamente las necesidades de la organización para la protección de la información mediante la evidencia de contratos firmados. Por ejemplo, se presenta evidencia del contrato con EFD que incluye la cláusula 14 de Confidencialidad y privacidad de datos, firmado de aceptación. Asimismo, se muestra un contrato con Hospital Satélite que incluye cláusulas de confidencialidad y no divulgación, privacidad de datos y acuerdos de transferencia de información, también firmado. Estas acciones demuestran el compromiso de la organización con la protección de la información a través de acuerdos formales y documentados.

29. ¿Cómo aseguran que los requisitos relacionados con la seguridad de la información estén integrados en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes?

La organización asegura que los requisitos relacionados con la seguridad de la información estén integrados en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes a través de un proceso de minuta para validar la viabilidad de los requisitos. Este proceso implica la revisión y discusión de los requisitos de seguridad de la información por parte de los interesados, con el fin de garantizar su inclusión efectiva en los requisitos del sistema. Para cualquier consulta adicional, la dirección de correo electrónico designada es atencion@noc-soc-horus.com.mx.

30. ¿Cómo protegen la información involucrada en servicios de aplicaciones que pasan sobre redes públicas de actividades fraudulentas, disputas contractuales y exposición no autorizada y modificación?

La organización protege la información mediante el uso de la Política de Convenios de confidencialidad, cifrado de seguridad mediante el uso de contraseñas, 7ZIP y VPN, fechada el día 11 de julio del 2023.

31. ¿Qué medidas toma la organización para asegurar que la información involucrada en transacciones de servicios de aplicación esté protegida contra transmisión incompleta, errores de enrutamiento, alteración de mensajes no autorizados, divulgación no autorizada, duplicación del mensaje no autorizado o reproducción?

La organización implementa medidas de protección como parte de la Política de Convenios de confidencialidad, cifrado de seguridad mediante el uso de contraseñas, 7ZIP y VPN , fechada el día 11 de julio del 2023, para prevenir tales riesgos en las transacciones de servicios de aplicación.

32. ¿Cómo establece y aplica la organización reglas para el desarrollo de software y sistemas si no se dedica al desarrollo de software?

A pesar de contar con la Política Desarrollo seguro fechada el 7 de julio del 2023, la organización no desarrolla software, por lo que no se aplican reglas para el desarrollo de software y sistemas dentro de la organización.

33. ¿Cuál es el proceso utilizado por la organización para controlar los cambios a los sistemas dentro del ciclo de vida del desarrollo, si no se dedica al desarrollo de software?

Dado que la organización no desarrolla software, no se aplican procedimientos formales de control de cambios para gestionar los cambios en el ciclo de vida del desarrollo.

34. ¿Cómo revisa y prueba la organización las aplicaciones críticas del negocio cuando cambian las plataformas operativas, si no se dedica al desarrollo de software?

La organización no revisa ni prueba aplicaciones críticas del negocio cuando cambian las plataformas operativas, ya que no está involucrada en el desarrollo de software.

35. ¿Qué medidas toma la organización para disuadir las modificaciones a los paquetes de software y controlar estrictamente los cambios, si no se dedica al desarrollo de software?

A pesar de tener la Política Desarrollo seguro, la organización no implementa medidas para disuadir modificaciones a los paquetes de software o controlar estrictamente los cambios, ya que no desarrolla software.

36. ¿Cómo establece y aplica la organización principios de ingeniería para sistemas seguros si no se dedica al desarrollo de software?

La organización no establece ni aplica principios de ingeniería para sistemas seguros, ya que no desarrolla software.

37. ¿Qué medidas toma la organización para establecer y proteger los entornos de desarrollo seguro si no se dedica al desarrollo de software?

No se establecen ni protegen entornos de desarrollo seguro, ya que la organización no desarrolla software.

38. ¿Cómo supervisa y monitorea la organización la actividad del desarrollo de sistemas subcontratados (outsourcing)?

A pesar de contar con una Política de Desarrollo seguro V01 fechada el 7 de julio del 2023, la organización no se involucra en el desarrollo de software, por lo que no se lleva a cabo una

39. ¿Qué procedimientos se implementan para llevar a cabo pruebas de la funcionalidad de seguridad durante el desarrollo?

Dado que la organización no desarrolla software, no se implementan procedimientos específicos para llevar a cabo pruebas de la funcionalidad de seguridad durante el desarrollo.

40. ¿Cómo establece la organización programas de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones?

La organización no establece programas de pruebas de aceptación ni criterios relacionados para nuevos sistemas de información, actualizaciones o nuevas versiones, ya que no desarrolla software.

41. ¿Cuáles son los métodos utilizados por la organización para seleccionar, proteger y controlar cuidadosamente los datos de prueba?

Dado que la organización no desarrolla software, no se aplican métodos específicos para seleccionar, proteger y controlar los datos de prueba.

42. ¿Cómo se asegura la protección de las áreas que albergan información sensible o crítica, así como las instalaciones de procesamiento de la información, mediante la definición y utilización de perímetros de seguridad?

En el Manual de Seguridad de la organización se detallan los controles implementados en materia de seguridad. Este manual proporciona una visión exhaustiva de las medidas y procedimientos establecidos para proteger los activos de información de la organización, incluyendo la identificación de áreas críticas, la definición de políticas de seguridad, y la implementación de controles adecuados. Asimismo, sirve como referencia para la evaluación y mejora continua de la postura de seguridad de la organización, garantizando así la protección efectiva de la información sensible y crítica.

43. ¿Cómo se asegura que las áreas estén debidamente protegidas, garantizando que únicamente el personal autorizado tenga acceso mediante la implementación de controles de entrada apropiados?

Mediante controles de acceso biométrico, circuito cerrado de televisión (CCTV), cercado eléctrico perimetral, sistemas de extinción de incendios, registro de ingresos y salidas, dispositivos de detección de humo y de movimiento, así como se cuenta con un área específica designada para operaciones de carga y descarga.

44. ¿Cómo se lleva a cabo el diseño y la implementación de medidas de seguridad física para garantizar la protección de oficinas, salas e instalaciones dentro de la organización?

La organización ha implementado sistemas de seguridad robustos que comprenden una variedad de medidas para proteger sus instalaciones. Estos sistemas incluyen controles de acceso biométrico, que requieren la verificación de la identidad mediante características físicas únicas, como huellas dactilares o reconocimiento facial. Además, se ha instalado un circuito cerrado de televisión (CCTV) para la vigilancia continua de áreas críticas, permitiendo la supervisión en tiempo real y la revisión de grabaciones en caso de incidentes. Asimismo, se han implementado dispositivos de detección de movimiento para alertar sobre intrusiones no autorizadas o actividades sospechosas dentro de las instalaciones, reforzando así la seguridad física de la organización.

45. ¿Cómo se lleva a cabo el diseño e implementación de medidas de protección física para mitigar los riesgos asociados a desastres naturales, ataques maliciosos o accidentes dentro de las instalaciones de la organización?

Se cuenta con una infraestructura completa que asegura tanto la continuidad operativa como la protección del entorno. Esta infraestructura incluye una planta de emergencia, sistemas de alimentación ininterrumpida (UPS), dispositivos de control de acceso, sistemas de alarma y una red de cableado eléctrico instalada adecuadamente.

46. ¿Cómo se desarrollan y ejecutan los procedimientos destinados a operar en áreas seguras dentro de las instalaciones de la organización?

Se ha implementado un conjunto de medidas que incluyen controles de acceso biométrico, circuito cerrado de televisión (CCTV) y detectores de movimiento para

garantizar la seguridad en áreas designadas. Además, se han establecido lineamientos específicos para operar en estas áreas dentro de la organización. Estos incluyen mantener un puesto de trabajo limpio, con pantalla y escritorio despejados de papeles, para garantizar un entorno de trabajo seguro y ordenado.

47. ¿Cómo se gestionan los puntos de acceso, como las zonas de carga y descarga, así como otros puntos potenciales de entrada para personas no autorizadas, con el fin de controlarlos y, en la medida de lo posible, aislarlos de las áreas de procesamiento de la información para prevenir accesos no autorizados?

En el Manual de Seguridad de la organización donde se identifica el estacionamiento como área de carga y descarga

48. ¿Cómo garantizan que el equipo esté ubicado y protegido de manera adecuada para reducir los riesgos de amenazas ambientales y peligros, así como las oportunidades para el acceso no autorizado?

Se asegura la integridad y seguridad de los sistemas mediante una supervisión continua. Donde se utiliza el cifrado de disco para proteger la información sensible. Además, se activan medidas adicionales, como el bloqueo por inactividad, la restricción de puertos USB, el control de acceso y la gestión del retiro de consolas, con el fin de fortalecer la seguridad del entorno.

49. ¿Cómo se protegen sus equipos contra las fallas de energía y otras interrupciones ocasionadas por problemas en los servicios públicos para garantizar la continuidad operativa y la integridad de los sistemas?

La infraestructura está equipada con una planta de emergencia y sistemas de alimentación ininterrumpida (UPS) para proteger el equipo contra las fallas de energía y otras interrupciones causadas por problemas en los servicios públicos, asegurando así la continuidad operativa y la integridad de los sistemas.

50. ¿Cómo aseguran la protección del cableado de energía y telecomunicaciones que transporta datos o soporta los servicios de información, con el fin de prevenir intercepciones, interferencias y daños que puedan afectar la integridad y seguridad de los sistemas de la organización?

El cableado eléctrico ha sido ocultado y canalizado dentro de canaletas para garantizar su seguridad y protegerlo de posibles daños externos.

51. ¿Cómo se garantiza el mantenimiento adecuado del equipo para asegurar su continua disponibilidad e integridad?

Se llevan a cabo mantenimientos a los equipos de manera semestral para garantizar su adecuado funcionamiento y prolongar su vida útil. Se presenta evidencia de estos mantenimientos, incluyendo el Registro de Mantenimiento a equipo de Pedro Hernández y Erika González fechados el 11 de enero y 25 de marzo de 2023 respectivamente, así como el Procedimiento de Mantenimiento a equipos como el electroimán de puertas, extintores y la planta de emergencia, UPS y aire acondicionado, con fechas que van desde el 14 de febrero hasta el 16 de mayo de 2023.

52. ¿Cómo se asegura de que el equipo, la información o el software no sean sacados del sitio sin autorización previa?

Se muestra el Registro Carta de retiro como el Registro Carta de asignación de equipo (servidores), ambas fechadas el 15 de marzo de 2023, como parte del proceso para autorizar la salida o asignación de equipo, información o software del sitio.

53. ¿Cómo se implementa la seguridad en los activos fuera de las instalaciones, considerando los variados riesgos asociados con el trabajo fuera de los límites físicos de la organización?

Se identifica la aplicación de medidas de seguridad, como la supervisión continua, el cifrado de disco, la activación del bloqueo por inactividad, la restricción de puertos USB, el control de acceso y la gestión del retiro de consolas, para proteger los activos fuera de las instalaciones y mitigar los diversos riesgos asociados con el trabajo fuera de los límites físicos de la organización.

54. ¿Cómo se verifica que todos los elementos del equipo que contienen medios de almacenamiento hayan sido eliminados o sobrescritos de manera segura?

Se verifica que todos los elementos del equipo que contienen medios de almacenamiento hayan sido eliminados o sobrescritos de manera segura mediante la aplicación de borrado seguro.

55. ¿Qué medidas se implementan para garantizar la eliminación de cualquier dato sensible y software licenciado antes de la disposición o reutilización del equipo?

Se implementa el borrado seguro como medida para garantizar la eliminación de cualquier dato sensible y software licenciado antes de la disposición o reutilización del equipo. Además, se registran estos procesos en el Registro de Bitácora de borrado seguro, fechada el 21 de marzo de 2023. Se establece que el equipo de Medar se destinará al almacenamiento según lo registrado en dicha bitácora.

56. ¿Cómo garantizan los usuarios que el equipo desatendido cuente con la protección adecuada?

Se establece y se verifica el cumplimiento dentro de una política Puesto de trabajo libre de papeles y escritorio y pantalla limpia, fechada el 5 de enero de 2023, la cual se valida durante las auditorías para garantizar que el equipo desatendido cuente con la protección adecuada

57. ¿Cómo implementan y adoptan las políticas de escritorio limpio, que prohíben papeles y medios de almacenamiento removibles, y de pantalla limpia en las instalaciones de procesamiento de la información?

La Política de Puesto de trabajo libre de papeles y escritorio y pantalla limpia versión 1 fechado 5 de enero del 2023 se valida durante la auditoría.

58. ¿Cuentan con uno o varios inventarios de activos?

Son 2 Aranda y CMDB, Aranda contiene los activos utilizados para la prestación de los servicios de los clientes y de la organización y CMDB se listan los activos, su categoría y responsable.

59. ¿Cuentan con algún lineamiento interno documentado en dónde describan la forma en la que clasifican la información, dependiendo de su nivel de confidencialidad?

Existe un esquema en el cual se encuentra clasificada la información por las categorías confidencial, restringida, interna y pública

60. ¿Como etiquetan la información dependiendo de su clasificación?

En los encabezados de los documentos se coloca la categoría y tambien se coloca una marca de agua

61. ¿Cuentan con algún proceso documentado para administrar todos los activos, en dónde se incluya el decir cómo es que van a cuidar los activos dependiendo del tipo de información que procesen, transmitan o resguarden?

Se tiene el procedimiento de Gestión de activos y su configuración y tambien se han definidos lineamientos para el manejo de información considerando su clasificación, como el uso de canales seguros, cifrados y VPN

62. Tratándose de medios removibles (p. ej. usb, discos duros, tarjetas de memoria extraíbles, etc.), ¿cómo se protegen?

Los puertos USB están bloqueados, salvo directivos y gerentes

63. ¿Como destruyen la información física?

Se utiliza una trituradora de papel

64. ¿Como destruyen la información lógica?

Se realiza el borrado de discos

65. ¿Tienen algún registro de borrado?

Se tiene una bitácora en la cual se registran todos los borrados seguros realizados

66. ¿Por necesidad de algún proyecto o por cuestiones internas, tienen o han tenido la necesidad de transportar información a través de medios físicos?

Si, para ello la organización cuenta con mensajería interna que se encarga de las entregas de manera personal a los clientes o responsables.

67. ¿Cuentan con una política documentada para la gestión de los accesos lógicos?

Se cuenta con la política de control de acceso.

68. ¿Tratándose de brindar acceso a servicios de red tienen un listado de las áreas o los puestos que están autorizados para tener acceso a dichos servicios?

Se define en los perfiles de acceso

69. ¿Cuándo existe una solicitud de acceso que deben hacer?

Se debe enviar una solicitud de acceso la cual se verifica para dar el acceso.

70. Siguiendo con el tema de accesos, una vez que ya fué creado el usuario, ¿en dónde tienen documentado el cómo se le deben entregar las credenciales de acceso al usuario?

Se gestiona un ticket donde se solicita la asignación de accesos

71. ¿Tienen alguna matriz o lista en dónde tengan documentado quienes son las personas que pueden tener accesos privilegiados? Si no, ¿cómo saben quién si puede tener acceso privilegiados?

Solo el área de operaciones tiene acceso privilegiado de nivel administrador.

72. ¿Como controlan la información secreta como usuarios y contraseñas?

Los usuarios y contraseñas se mandan por medios distintos y para generar una nueva contraseña se levanta un nuevo ticket

73. ¿Los administradores de los sistemas, realizan revisiones cada determinado tiempo para asegurar que todos los usuarios tengan el estatus que deberían tener?

Si, se lleva a cabo de manera semestral

74. ¿Cómo se aseguran que los colaboradores salvaguardan la información?

En la carta de asignación de activos se especifican las responsabilidades a los colaboradores y las contraseñas se actualizan cada 90 días

75. ¿Dé que manera previenen el acceso no autorizado?

A través de los perfiles de accesos

76. Actualmente, para acceder a cualquier activo crítico, ¿se tiene implementado algún método de inicio de sesión seguro?

Los equipos de cómputo deben cumplir con los lineamientos establecidos por la política de creación de contraseñas

77. ¿Como aseguran que las contraseñas sean de calidad?

Se cuentan con lineamientos para la creación de las contraseñas

78. Los usuarios, es decir todos los colaboradores que son usuarios de algún equipo de cómputo, ya sea lap top o de escritorio, ¿tienen permiso para alguna de las siguientes: cambiar configuración de inicio de sesión, bloqueo de pantalla automático, deshabilitar antivirus, ¿instalar software?

Los usuarios de la organización no utilizan programas, aplicaciones y/o software de utilidades en su operación

79. ¿De qué manera restringen el acceso al código fuente?

No se realiza debido a que la organización no genera códigos fuente

80. ¿Cómo se identifican, documentan y mantienen actualizados todos los requisitos legislativos, regulatorios, contractuales relevantes, así como el enfoque de la organización para cumplir con estos requisitos, para cada sistema de información y para la organización en su conjunto?

Se muestra el Registro Matriz de cumplimiento fechada el 24 de marzo del 2023, la cual identifica los requisitos normativos/requisitos, la fuente, la evidencia, las revisiones semestrales y las observaciones relacionadas con los requisitos legislativos, regulatorios y contractuales relevantes, así como con el enfoque de la organización para cumplir con estos requisitos.

81. ¿Qué medidas se han implementado para asegurar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentado dentro de la organización?

La organización cumple con los requisitos al disponer de software licenciado y al establecer cláusulas de propiedad intelectual en sus contratos. Estas medidas garantizan la protección adecuada de los activos intangibles de la empresa y promueven el cumplimiento de las regulaciones pertinentes en materia de propiedad intelectual.

82. ¿De qué manera se implementan medidas para proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, en conformidad con los requisitos legales, regulatorios, contractuales y de negocios?

Los registros son almacenados de manera segura durante un período de 10 años, siguiendo los protocolos y controles de seguridad de la información establecidos por la organización para garantizar su protección contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.

83. ¿Cómo garantizan la privacidad y protección de la información de identificación personal conforme a lo requerido por la legislación y regulación relevante aplicable dentro de la organización?

La organización asegura la privacidad y protección de la información de identificación personal mediante la implementación de un Formato Aviso de privacidad integral, el cual está disponible en la página web de la organización y se proporciona a los colaboradores al inicio de su relación laboral, así como se menciona en los contratos con los clientes. Sin embargo, se identifica una inconsistencia, ya que la última actualización del aviso de privacidad mostrado en la página web es el 12 de enero de 2023, mientras que el aviso de privacidad firmado por el colaborador Daniel Olvera García tiene fecha de entrada en vigor el 12 de junio de 2023 y no presenta fecha de última actualización en el cuerpo del aviso. Por lo tanto, es necesario que la organización homologue los avisos de privacidad para corregir esta discrepancia.

84. ¿Cómo se garantiza que los controles criptográficos sean utilizados en cumplimiento con todos los acuerdos, legislación y regulaciones relevantes dentro de la organización?

Se solicita por contrato el envío de información cifrada con contraseña (7Zip), asegurando así el cumplimiento con todos los acuerdos, legislación y regulaciones relevantes en materia de seguridad criptográfica.

85. ¿Cómo se lleva a cabo la revisión independiente del enfoque de la organización para la gestión de la seguridad de la información y su implementación, incluyendo objetivos de control, controles, políticas, procesos y procedimientos, en intervalos planificados o cuando ocurran cambios significativos?

Se realizan mantenimientos semestrales a los equipos, durante los cuales se verifica el cumplimiento y la implementación de los controles de seguridad de la información correspondientes.

86. ¿Cómo llevan a cabo las revisiones periódicas de los sistemas de información para garantizar su conformidad con las políticas y normas de seguridad de la información establecidas por la organización?

Se llevan a cabo análisis de vulnerabilidades de forma anual para asegurar el cumplimiento con las políticas y normas de seguridad de la información establecidas por la organización. Se presenta el análisis de vulnerabilidades del año 2023, el cual reveló un total de 40 hallazgos críticos y 15 hallazgos informativos.

87. ¿Cuentan con una política documentada sobre el uso de controles criptográficos?

La organización ha implementado una política de seguridad que protege los equipos de los colaboradores. Esta incluye el cifrado de disco mediante Bitlocker, la comunicación con clientes mediante 7zip y el cifrado de correos electrónicos para garantizar la confidencialidad de la información. Esta política demuestra el compromiso de la organización con la seguridad de los datos y la privacidad de sus clientes y colaboradores.

88. ¿Cuentan con un procedimiento para gestión de llaves de cifrado?

El tiempo de vida designado para las llaves se establece en un período de 1 a 2 años. Esta medida se fundamenta en la necesidad de mantener un equilibrio entre la seguridad y la eficiencia operativa dentro del entorno organizacional. Al limitar el tiempo de uso de las llaves a este intervalo específico, se busca mitigar los riesgos asociados con la exposición prolongada a potenciales amenazas de seguridad, como la pérdida, el robo o la comprometida integridad de las llaves.

NOTA: Durante la auditoría ISO 27001, se aplicaron cuestionarios a través de la herramienta de videoconferencia Meet Y Microsoft Teams. La sesión fue grabada para garantizar la correcta documentación del proceso. Sin embargo, por razones de confidencialidad de la empresa, no es posible mostrar ni compartir la grabación. [BG12]

3.2.1.2 Actividad 2.2 Revisar la documentación pertinente, como políticas de seguridad, procedimientos de gestión y registros de incidentes.

3.2.1.2.1 Descripción de la actividad

Se examinan documentos relevantes como informes, registros, políticas, procedimientos y correos electrónicos, los cuales sirven como evidencia concreta y verificable del cumplimiento de las normas establecidas por la norma ISO. La revisión de esta documentación proporciona una visión detallada y objetiva de la situación, fundamentada en datos concretos y registros escritos. Además, ayuda a corroborar la información obtenida en las entrevistas con el personal y a identificar posibles discrepancias o inconsistencias que requieran atención.

3.2.1.2.2 Resultado de la actividad

3.2.1.2.2.1 Revisión documental

Tabla 61 Revisión documental

Requisito / Control	Tipo de documento	Nombre del documento	Versión	Fecha entrada en vigor
4. Contexto de la organización	Manual	Sistema de Gestión Integrado (SGI)	1	lunes, 31 de julio de 2023
4. Contexto de la organización	Anexo	Modelo sistémico del SGI	2	jueves, 15 de junio de 2023
5 Liderazgo	Manual	Sistema de Gestión Integrado (SGI)	1	lunes, 31 de julio de 2023

5 Liderazgo	Registro	Minuta de asignación de roles y responsabilidades	NA	miércoles, 30 de noviembre de 2022
5 Liderazgo	Registro	Comunicado roles y responsabilidades del SGI	NA	viernes, 21 de abril de 2023
6 Planificación	Registro	Matriz de Oportunidades	1	lunes, 3 de abril de 2023
6 Planificación	Manual	Sistema de Gestión Integrado (SGI)	1	lunes, 31 de julio de 2023
6 Planificación	Registro	Valoración, evaluación y tratamiento de riesgos	9	viernes, 14 de julio de 2023
6 Planificación	Registro	Valoración de riesgos_2do semestre 2023	NA	jueves, 31 de agosto de 2023
7 Apoyo	Registro	Organigrama	NA	lunes, 2 de enero de 2023
7 Apoyo	Registro	Presupuesto	NA	lunes, 2 de enero de 2023
7 Apoyo	Registro	Plan de Capacidad	NA	lunes, 2 de enero de 2023

Tabla 62 (Continuación)

Requisito / Control	Tipo de documento	Nombre del documento	Versión	Fecha entrada en vigor
7 Apoyo	Formato	Perfil de Puesto_Coordinador de Recursos Humanos	NA	viernes, 7 de abril de 2023
7 Apoyo	Anexo	Curriculum Vitae	NA	NA
7 Apoyo	Constancia	Formación de Auditores Internos	NA	NA
7 Apoyo	Constancia	Auxiliar de Recursos Humanos	NA	NA
7 Apoyo	Constancia	Diplomado en Psicología	NA	NA
7 Apoyo	Registro	Plan de Concientización_2023	NA	lunes, 5 de junio de 2023
7 Apoyo	Procedimiento	Concientización y Comunicación del SGI	3	viernes, 7 de abril de 2023
7 Apoyo	Procedimiento	Control de documentos	2	viernes, 5 de mayo de 2023

7 Apoyo	Registro	Inventario de documentos	NA	viernes, 8 de diciembre de 2023
7 Apoyo	Registro	Bitácora de revisión de documentos externos_2023	NA	viernes, 8 de diciembre de 2023
8 Operación	Procedimiento	Gestión del cambio	1	viernes, 10 de febrero de 2023
8 Operación	Procedimiento	Valoración, evaluación y tratamiento de riesgos	9	lunes, 31 de julio de 2023
8 Operación	Registro	Valoración de riesgos_2do semestre 2023	NA	jueves, 31 de agosto de 2023
9 Evaluación del desempeño	Procedimiento	Gestión de mejora continua	3	lunes, 21 de agosto de 2023
9 Evaluación del desempeño	Registro	Matriz de monitoreo_2023	NA	lunes, 21 de agosto de 2023
9 Evaluación del desempeño	Procedimiento	Recursos Humanos	1	martes, 19 de septiembre de 2023

Tabla 63 (Continuación)

Requisito / Control	Tipo de documento	Nombre del documento	Versión	Fecha entrada en vigor
9 Evaluación del desempeño	Registro	Calendario de Auditoría Interna_2023	NA	lunes, 2 de enero de 2023
9 Evaluación del desempeño	Registro	Plan de Auditoría Interna_2023	NA	lunes, 2 de enero de 2023
9 Evaluación del desempeño	Registro	Revisión por Dirección_3er trimestre 2023	NA	viernes, 1 de septiembre de 2023
9 Evaluación del desempeño	Registro	Informe de Revisión por Dirección_3er trimestre 2023	NA	viernes, 1 de septiembre de 2023
10 Mejora	Registro	Plan de Acción_146	NA	lunes, 5 de junio de 2023

10 Mejora	Registro	Plan de Acción_154	NA	jueves, 27 de julio de 2023
A.5 Políticas de seguridad de la información	Política	Seguridad de la información	8	miércoles, 15 de marzo de 2023
A.6 Organización de la seguridad de la información	Registro	Matriz contacto autoridades_2023	NA	miércoles, 23 de agosto de 2023
A.6 Organización de la seguridad de la información	Formato	Implementación de servicio	4	jueves, 25 de mayo de 2023
A.6 Organización de la seguridad de la información	Registro	Plan de trabajo_Instalación de memorias RAM	NA	martes, 31 de octubre de 2023

Tabla 64 (Continuación)

Requisito / Control	Tipo de documento	Nombre del documento	Versión	Fecha entrada en vigor
A.6 Organización de la seguridad de la información	Política	Uso de teléfonos inteligentes y cámaras digitales	5	miércoles, 14 de junio de 2023
A.6 Organización de la seguridad de la información	Política	Movilidad	3	martes, 4 de julio de 2023

A.7 Seguridad en los recursos humanos	Contrato	Contrato_Renato Figueroa	NA	jueves, 30 de noviembre de 2023
A.7 Seguridad en los recursos humanos	Registro	Perfil de puesto_Responsable de RH	NA	miércoles, 5 de julio de 2023
A.7 Seguridad en los recursos humanos	Registro	Renuncia_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.7 Seguridad en los recursos humanos	Registro	Baja biométrico_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.7 Seguridad en los recursos humanos	Registro	Solicitud de baja (Activos)_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.7 Seguridad en los recursos humanos	Registro	Aviso de privacidad_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.7 Seguridad en los recursos humanos	Registro	Baja acceso físico/lógico_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023

Tabla 65 (Continuación)

Requisito / Control	Tipo de documento	Nombre del documento	Versión	Fecha entrada en vigor
A.7 Seguridad en los recursos humanos	Registro	Carta asignación y devolución de activos_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.7 Seguridad en los recursos humanos	Registro	Minuta de aprobación de cambio de puesto_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.7 Seguridad en los recursos humanos	Registro	Perfil de puesto_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023

A.8 Gestión de activos	Registro	Renuncia_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.8 Gestión de activos	Registro	Baja biométrico_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.8 Gestión de activos	Registro	Solicitud de baja (Activos)_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.8 Gestión de activos	Registro	Aviso de privacidad_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.8 Gestión de activos	Registro	Baja acceso físico/lógico_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.8 Gestión de activos	Registro	Carta asignación y devolución de activos_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.8 Gestión de activos	Registro	Minuta de aprobación de cambio de puesto_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.8 Gestión de activos	Registro	Perfil de puesto_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.8 Gestión de activos	Procedimiento	Gestión de activos y su configuración	2	miércoles, 1 de febrero de 2023

Tabla 66 (Continuación)

Requisito / Control	Tipo de documento	Nombre del documento	Versión	Fecha entrada en vigor
A.8 Gestión de activos	Registro	Bitácora de destrucción y borrado_2023	NA	viernes, 8 de diciembre de 2023
A.8 Gestión de activos	Registro	Acuse de recibo_Infonavit	NA	martes, 15 de agosto de 2023
A.9 Control de acceso	Política	Control de Accesos	6	viernes, 20 de octubre de 2023
A.9 Control de acceso	Registro	Solicitud de Acceso_150823	NA	martes, 15 de agosto de 2023

A.9 Control de acceso	Registro	6566_Gabriel Arcega Soto	NA	miércoles, 25 de octubre de 2023
A.9 Control de acceso	Registro	Carta de asignación de activos_Juan David Mejía Hernández	NA	martes, 7 de noviembre de 2023
A.10 Criptografía	Política	Controles criptográficos	2	viernes, 2 de junio de 2023
A,11 Seguridad Física ambiental	Manual	Seguridad la organización	1	jueves, 25 de mayo de 2023
A,11 Seguridad Física ambiental	Registro	Mantenimiento a equipo	NA	
A,11 Seguridad Física ambiental	Procedimiento	Mantenimiento a electroimán de puertas	1	miércoles, 11 de enero de 2023
A,11 Seguridad Física ambiental	Procedimiento	Mantenimiento de extintores, recarga y mantenimiento	1	martes, 16 de mayo de 2023
A,11 Seguridad Física ambiental	Procedimiento	Mantenimiento de planta de emergencia, UPS, aire acondicionado	1	viernes, 20 de enero de 2023

Tabla 67 (Continuación)

Requisito / Control	Tipo de documento	Nombre del documento	Versión	Fecha entrada en vigor
A,11 Seguridad Física ambiental	Registro	Carta de retiro	NA	miércoles, 15 de marzo de 2023
A,11 Seguridad Física ambiental	Registro	Carta de asignación de equipo	NA	miércoles, 15 de marzo de 2023
A,11 Seguridad Física ambiental	Registro	Bitácora de borrado seguro	NA	martes, 21 de marzo de 2023

A.11 Seguridad Física ambiental	Política	Puesto de trabajo libre de papeles y escritorio y pantalla limpia	1	jueves, 5 de enero de 2023
A.12 Seguridad en operaciones	Procedimiento	Gestión del cambio	1	viernes, 19 de mayo de 2023
A.12 Seguridad en operaciones	Procedimiento	Gestión de la capacidad	1	viernes, 19 de mayo de 2023
A.12 Seguridad en operaciones	Procedimiento	Gestión de la disponibilidad	1	viernes, 19 de mayo de 2023
A.12 Seguridad en operaciones	Procedimiento	Gestión de la configuración	1	viernes, 19 de mayo de 2023
A.12 Seguridad en operaciones	Procedimiento	Diseño y transición de servicios	1	viernes, 19 de mayo de 2023
A.12 Seguridad en operaciones	Procedimiento	Respaldos	1	viernes, 19 de mayo de 2023
A.12 Seguridad en operaciones	Procedimiento	Control de documentos, continuidad	1	viernes, 19 de mayo de 2023
A.12 Seguridad en operaciones	Registro	Caso no. 63 / CHG8268-1-63	NA	viernes, 17 de marzo de 2023
A.12 Seguridad en operaciones	Formato	Plan de capacidad	1	viernes, 20 de enero de 2023
A.12 Seguridad en operaciones	Registro	Bitácora de respaldos	NA	miércoles, 8 de febrero de 2023

Tabla 68 (Continuación)

Requisito / Control	Tipo de documento	Nombre del documento	Versión	Fecha entrada en vigor
A.13 Seguridad en las comunicaciones	Política	Firewall	1	lunes, 13 de marzo de 2023
A.13 Seguridad en las comunicaciones	Política	Convenios de confidencialidad, cifrado de seguridad mediante uso de contraseñas, 7ZIP, VPN	1	martes, 11 de julio de 2023
A.13 Seguridad en las comunicaciones	Contrato	EFD	NA	

A.13 Seguridad en las comunicaciones	Contrato	Hospital Satélite	NA	
A.14 Adquirió, Desarrollo Y Mantenimiento de sistemas	Política	Desarrollo seguro	1	viernes, 7 de julio de 2023
A.15 Relación con proveedores	Procedimiento	Gestión de compras y proveedores	1	miércoles, 28 de junio de 2023
A.16 Gestión de incidentes de seguridad de la información	Procedimiento	Incidentes de seguridad de la información	1	viernes, 9 de junio de 2023
A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio	Formato	Plan de continuidad y disponibilidad	1	martes, 2 de mayo de 2023
A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio	Registro	Diagrama red	NA	lunes, 3 de abril de 2023
A.18 Cumplimiento	Registro	Matriz de cumplimiento	NA	viernes, 24 de marzo de 2023
A.18 Cumplimiento	Formato	Aviso de privacidad	1	jueves, 12 de enero de 2023

3.2.1.3 Actividad 2.3 Analizar la relación entre la evidencia objetiva recopilada y los criterios establecidos, determinando el grado de conformidad o desviación respecto a los estándares y requerimientos predefinidos.

Comparar la evidencia objetiva recopilada durante la auditoría con los criterios establecidos previamente, para determinar si existe conformidad o desviación respecto a los estándares y requerimientos predefinidos

3.2.1.3.1 Descripción de la actividad

Implica un análisis exhaustivo para evaluar la relación entre la evidencia objetiva recopilada durante la auditoría y los criterios establecidos previamente según la norma ISO.

El objetivo principal es determinar el grado de conformidad o desviación respecto a los estándares y requerimientos predefinidos.

En caso de identificar desviaciones, se pueden implementar medidas correctivas para asegurar el cumplimiento de los estándares y satisfacer los requisitos establecidos. Por otro lado, si se verifica la conformidad, se puede proceder con la validación o aprobación de los procesos, productos o servicios evaluados. Se utiliza una lista de verificación que incluye requisitos y controles a evaluar, así como su descripción, y dependiendo de la información recabada, se asignará una calificación según los criterios definidos en el plan de auditoría. Además, se redacta la relación de la evidencia con los requisitos y controles establecidos para documentar adecuadamente el proceso de evaluación conforme a los estándares de la norma ISO.

3.2.1.3.2 Resultado de la actividad

3.2.1.3.2.1 Lista de verificación

Tabla 69 Lista de verificación ISO27001:2015

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
4. Contexto de la organización			
4.1 Comprensión de la organización y de su contexto	La organización debe determinar las cuestiones externas e internas que son	C	Se presenta el documento "Ma_Sistema de

	pertinentes para su propósito y su dirección estratégica, y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la calidad. La organización debe realizar el seguimiento y la revisión de la información sobre estas cuestiones externas e internas.		Gestión Integrado (SGI)_V01", que incluye un análisis FODA fechado el 31 de julio de 2023. Las Fortalezas identificadas incluyen la iniciativa para implementar el Sistema de Gestión de Calidad (SGC) conforme a la norma ISO 9001:2015. Las Debilidades destacadas son la necesidad de concientización y motivación del personal. En cuanto a las Oportunidades, se mencionan las empresas de consultoría que podrían ayudar a abordar los desafíos internos actuales, mientras que las Amenazas son las nuevas reformas fiscales. Se proporciona evidencia del seguimiento de estas estrategias para su
--	---	--	---

			implementación y mejora continua.
--	--	--	-----------------------------------

Tabla 70 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Debido a su efecto o efecto potencial en la capacidad de la organización de proporcionar regularmente productos y servicios que satisfagan los requisitos del cliente y los legales y reglamentarios aplicables, la organización debe determinar: a) las partes interesadas que son pertinentes al sistema de gestión de la calidad; b) los requisitos pertinentes de estas partes interesadas para el sistema de gestión de la calidad. La organización debe realizar el seguimiento y la revisión de la información sobre estas partes interesadas y sus requisitos pertinentes.	NC	No se encuentra documentadas las partes interesadas, los colaboradores saben la información necesaria para el cumplimiento de necesidades y expectativas, cuentan únicamente con la matriz de partes interesadas en el Ma_Sistema de Gestión Integrado (SGI)_V01

Tabla 71 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

4.3 Determinación del alcance del sistema de gestión de la calidad	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la calidad para establecer su alcance. Cuando se determina este alcance, la organización debe considerar: a) las cuestiones externas e internas indicadas en el apartado 4.1; b) los requisitos de las partes interesadas pertinentes indicados en el apartado 4.2; c) los productos y servicios de la organización. La organización debe aplicar todos los requisitos de esta Norma Internacional si son aplicables en el alcance determinado de su sistema de gestión de la calidad. El alcance del sistema de gestión de la calidad de la organización debe estar disponible y mantenerse como información documentada. El alcance debe establecer los tipos de productos y servicios cubiertos, y proporcionar la	C	La organización ha definido el alcance del Sistema de Gestión Integrado (SGI) como: “Los servicios de mesa de ayuda, monitoreo, SOC y NOC en sus procesos de atención de incidentes y solicitudes de servicio, atención de problemas, niveles de servicio, procesos de servicios nuevos o modificados, y en todos sus procesos de gestión del servicio y seguridad de la información, ofrecidos por su SOC-NOC Horus, así como, la protección de recursos, servicios y partes interesadas, de acuerdo con la declaración de aplicabilidad (SoA) vigente" El SOC NOC HORUS de SayNet ofrece los siguientes servicios: *Mesa de servicio *Monitoreo
--	---	---	--

	justificación para cualquier requisito de esta Norma Internacional que la organización determine que no es aplicable para el alcance de su sistema de gestión de la calidad. La conformidad con esta Norma Internacional sólo se puede declarar si los requisitos determinados como no aplicables no afectan a la capacidad o a la responsabilidad de la organización de asegurarse de la conformidad de sus productos y servicios y del aumento de la satisfacción del cliente.		*NOC (Centro de Operaciones de Red) *SOC (Centro de Operaciones de Seguridad) Además, se detalla en el documento 3.1.5.6 Declaración de Aplicabilidad los controles implementados, así como aquellos excluidos y su justificación correspondiente. Las exclusiones de controles son las siguientes: *A.9.4.5 Control de acceso a código fuente Justificación: Este control se excluye porque la organización no desarrolla software, por lo tanto, no maneja ni tiene acceso a código fuente que requiera protección. *A.14.2.6 Entorno de desarrollo seguro Justificación: Dado que
--	---	--	---

			la organización no desarrolla software, no se considera necesario implementar este control para garantizar un entorno de desarrollo seguro.
--	--	--	---

Tabla 72 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
4.4 Sistema de gestión de Seguridad de la Información	La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información	C	Se dispone de un modelo sistémico que permite la identificación de los procesos del Sistema de Gestión Integrado (SGI), así como los procesos clave de entrega y demanda, y los procesos estratégicos y de control. Este modelo detalla las interacciones entre dichos procesos, sus subprocesos y sus responsables. Se adjunta en el "An_ Modelo sistémico del SGI_V02" fechado el 15 de junio del 2023
5 Liderazgo			

5.1 Compromiso y liderazgo	La alta dirección debe demostrar su liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información	C	La organización muestra un liderazgo sólido al participar en auditorías, asignar recursos de manera estratégica y tomar decisiones clave para el SGI. Además, respalda roles y responsabilidades para promover un ambiente de trabajo colaborativo. Prioriza la satisfacción del cliente, lo que fortalece las relaciones comerciales y asegura su competitividad. Esta implicación activa en todas las áreas garantiza la transparencia, la eficiencia operativa y la adaptación continua a las demandas del entorno,
----------------------------	--	---	--

Tabla 73 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
5.2 Política	La alta dirección debe establecer una política de seguridad de la información	C	Se presenta el documento "Ma_Sistema de Gestión Integrado

			(SGI)_V01", que incorpora la política del Sistema de Gestión Integrado (SGI). Esta política ha sido formalmente autorizada por la alta dirección el 28 de febrero de 2023 y se ha comunicado tanto interna como externamente, incluyendo su publicación en la página web de la organización.
--	--	--	--

Tabla 74 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
5.3 Roles, responsabilidades y autoridades en la organización	La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen, se comuniquen y se entiendan en toda la organización.	C	Se presenta el "Ma_Sistema de Gestión Integrado (SGI)_V01", que abarca el Comité del SGI junto con los roles, puestos relacionados y sus respectivas responsabilidades vinculadas al SGI. Se muestra el Re_Minuta de asignación de roles y responsabilidades_2022 generada el 30 de

			noviembre de 2022, así como el Re_Comunicado roles y responsabilidades del SGI con fecha del 21 de abril de 2023.
--	--	--	---

Tabla 75 (Continuación)

6 Planificación			
6.1 Acciones para abordar riesgos y oportunidades			
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
6.1.1	Al planificar el sistema de gestión de seguridad de la información la organización debe considerar las cuestiones referidas en el apartado 4.1 y los requisitos referidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario abordar con el fin de: a) asegurar que el sistema de gestión de SGSI pueda lograr sus resultados previstos; b) aumentar los efectos deseables; c) prevenir o reducir efectos no deseados; d) lograr la mejora.	C	Se muestra el documento "Re_Matriz de Oportunidades_V01" generado el 3 de abril del 2023 en el cual se observa relación con el requisito 4.1 en el análisis de los elementos del entorno, específicamente en la categoría "Elementos del Entorno", se establece una asociación con los elementos identificados en el Análisis FODA (Fortalezas, Oportunidades, Debilidades y

			Amenazas) del documento "Ma_Sistema de Gestión Integrado (SGI)_V01", una herramienta utilizada para el análisis del contexto externo e interno de la organización. Se ha identificado una relación con los requisitos y necesidades de las partes interesadas, según lo estipulado en el requisito 4.2. Durante la revisión del Análisis FODA realizado el 31 de julio del 2023, se identificaron un total de 22 elementos entre Fortalezas, Oportunidades, Debilidades y Amenazas (FODA). Se realiza una evaluación del impacto en la confidencialidad, disponibilidad e integridad de la
--	--	--	--

			información en relación con los hallazgos identificados. Esta evaluación se realizada de manera exhaustiva, considerando los posibles riesgos y vulnerabilidades asociados.
--	--	--	---

Tabla 76 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
6.1.2	La organización debe definir y aplicar un proceso de valoración de riesgos de seguridad de la información para: a) establecer y mantener los criterios de riesgo de seguridad de la información que incluya: El criterio de aceptación del riesgo y los criterios para realizar las valoraciones de riesgos de seguridad de la información. b) Asegurar de que al repetir las valoraciones de riesgos de seguridad de la información produzcan resultados consistentes,	C	Se muestra el documento "Re_Valoración, evaluación y tratamiento de riesgos_V09" actualizado el 14 de julio del 2023 en el cual el proceso se basa en las siguientes actividades: 1. Identificación de elementos críticos 2. Clasificación de elementos 3. Amenazas 4. Probabilidad de ocurrencia 5. Impacto (humano,

	válidos y comparables; c) identificar los riesgos de seguridad de la información: aplicar el proceso de valoración de riesgos de seguridad de la información para identificar riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del SGSI. identificar a los propietarios de los riesgos. d) Analizar los riesgos de seguridad de la información: Valorar las consecuencias potenciales que se derivan si los riesgos identificados llegan a materializarse; valorar la probabilidad realista de la ocurrencia de los riesgos identificados y determinar los niveles de riesgo. e) Evaluar los riesgos de seguridad de la información: Comparar los resultados del		material, financiero, operativo, imagen 6. Identificación del riesgo 7. Tipo de tratamiento (aceptación, mitigación, transferencia, eliminación) 8. Aceptación de riesgos residuales 9. Revisar la eficacia de los controles
--	--	--	---

	análisis de riesgo con los criterios de riesgo establecidos en el inciso a). priorizar los riesgos analizados para el tratamiento de riesgo. La organización debe conservar información documentada sobre el proceso de valoración de riesgos de seguridad de la información.		
--	---	--	--

Tabla 77 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
6.1.3	La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para: a) Seleccionar opciones apropiadas de tratamiento de riesgos de seguridad de la información, tomando en cuenta los resultados de la valoración de riesgos; b) Determinar todos los controles que sean necesarios para implementar las opciones de tratamiento de riesgos de seguridad de la información	C	Se muestra el documento "Re_Valoración de riesgos_2do semestre 2023" actualizado el 31 de agosto del 2023 donde se han identificado un total de 70 elementos durante la valoración de riesgos y todos los elementos evaluados han sido categorizados como riesgos bajos según los criterios establecidos en el proceso de valoración.

	elegidas. c) Comparar los controles determinados con los descritos en el apéndice "A" y verificar que no se hayan omitido controles necesarios; d) Producir una declaración de aplicabilidad que contenga los controles necesarios (véase el inciso 6.1.3 subinciso b) y c)) y la justificación de las inclusiones, si están implementadas o no, y la justificación de la exclusión de controles del apéndice "A".		Se identifica un propietario del riesgo, y las responsabilidades definidas. Se muestra la comparativa de los controles establecidos en el inciso 6.1.3, apartado b), con aquellos descritos en el apéndice "A". La declaración de aplicabilidad carece de justificación fundamentada en los requisitos establecidos en el inciso d) del apartado 6.1.3.
--	---	--	---

Tabla 78 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
6.2 Objetivos de la calidad y planificación para lograrlos	La organización debe establecer los objetivos de seguridad de la información en funciones y niveles pertinentes	C	Se muestra el "Ma_Sistema de Gestión Integrado (SGI)_V01", que incorpora los objetivos del SGI los cuales incluyen objetivo, métrica, meta, periodicidad y responsable,

		Se han registrado un total de diez objetivos, que abarcan áreas clave de desempeño, tales como el aumento en el número de servicios contratados (cuatro anuales), la salvaguarda de la confidencialidad de la información de las partes interesadas mediante la prevención de incidentes con impacto (menos de dos), y la satisfacción del cliente, medida en un índice del 88.5%. Se observa la existencia de un Sistema de Monitoreo y Control de Objetivos del SGI, destinado a supervisar el cumplimiento de dichos objetivos. Se incluye información detallada sobre las acciones planificadas para alcanzar los objetivos establecidos, se identifican los
--	--	--

			recursos necesarios para llevar a cabo dichas acciones.
--	--	--	---

Tabla 79 (Continuación)

7 Apoyo			
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
7.1 Recursos	La organización debe determinar y proveer los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.	C	Se han establecido los recursos necesarios para respaldar eficazmente sus operaciones, este respaldo se evidencia a través de la disponibilidad y utilización mediante los siguientes documentos: Re_Organigrama_2023 actualizado el 1 de enero del 2023: El cual proporciona una representación gráfica clara de la estructura jerárquica y funcional de la organización, delineando las relaciones y

		responsabilidades entre diferentes unidades y roles dentro de la misma. Re_Presupuesto_2023 actualizado el 1 de enero del 2023: Este documento financiero detallado proporciona una estimación precisa de los recursos monetarios asignados y disponibles para el funcionamiento de la organización, permitiendo una planificación financiera adecuada y una gestión eficiente de los recursos. Re_Plan de Capacidad_2023 actualizado el 5 de enero del 2023: El cual establece las proyecciones y estrategias para garantizar que la organización cuente con los recursos humanos, tecnológicos y físicos
--	--	---

			necesarios para satisfacer la demanda y las expectativas operativas a corto y largo plazo.
--	--	--	--

Tabla 80 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
7.2 Competencia	La organización debe: a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al desempeño y eficacia del sistema de gestión de la calidad; b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia apropiadas; c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; d) conservar la	C	La organización ha establecido de manera formal las competencias necesarias para los colaboradores que participan en la prestación de servicios, a través de perfiles de puestos. Se ha proporcionado la Descripción del Perfil de Puesto_Coordinador de Recursos Humanos actualizado el 7 de abril del 2023, correspondiente a María Guadalupe Soriano Mejía. Además, se

	información documentada apropiada como evidencia de la competencia.		evidenció que el perfil de dicho colaborador se alinea con su An_Curriculum Vitae, la constancia de Formación de Auditores Internos, la constancia de Auxiliar de Recursos Humanos y su Diplomado en Psicología, cumpliendo así con los requisitos solicitados por el perfil de puesto establecido. La evaluación del puesto reveló un cumplimiento del 100% en este aspecto.
--	---	--	---

Tabla 81 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
7.3 Concientización	La organización debe asegurarse de que las personas que realizan el trabajo bajo el control de la organización tomen conciencia de: a) la política de la calidad; b) los objetivos de la calidad pertinentes; c) su contribución a la eficacia	C	Se muestra el "Re_Plan de Concientización_2023" generado el 5 de junio del 2023 y "Pr_Concientización y Comunicación del SGI_V03" actualizado el 7 de abril del 2023, se evidencia la adecuada

	del sistema de gestión de la calidad, incluidos los beneficios de una mejora del desempeño; d) las implicaciones del incumplimiento de los requisitos del sistema de gestión de la calidad.		implementación de comunicados dirigidos a la concientización del personal en relación con los siguientes aspectos clave: *La contribución de los colaboradores a la eficacia del SGI. *Las consecuencias derivadas del incumplimiento de los requisitos legales y normativos. *La política del SGI. *Los objetivos establecidos por el SGI. Se reconoce la eficacia de estas comunicaciones como instrumento para fortalecer la comprensión y el compromiso del personal con los principios y objetivos del SGI. Sin embargo, se recomienda una revisión continua y periódica de estos comunicados para
--	--	--	--

			asegurar su pertinencia y efectividad en la concientización del equipo respecto a la importancia y responsabilidad en la gestión integral de la organización.
--	--	--	---

Tabla 82 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
7.4 Comunicación	La organización debe determinar las comunicaciones internas y externas pertinentes al sistema de gestión de la calidad, que incluyan: a) qué comunicar; b) cuándo comunicar; c) a quién comunicar; d) cómo comunicar; e) quién comunica.	C	Se muestra el "Re_Plan de Concientización_2023" generado el 5 de junio del 2023 y "Pr_Concientización y Comunicación del SGI_V03" actualizado el 7 de abril del 2023, se evidencia la adecuada implementación de comunicados dirigidos a la concientización del personal en relación con los siguientes aspectos clave: *La contribución de los colaboradores a la eficacia del SGI. *Las consecuencias derivadas del

			incumplimiento de los requisitos legales y normativos. *La política del SGI. *Los objetivos establecidos por el SGI. Se reconoce la eficacia de estas comunicaciones como instrumento para fortalecer la comprensión y el compromiso del personal con los principios y objetivos del SGI. Sin embargo, se recomienda una revisión continua y periódica de estos comunicados para asegurar su pertinencia y efectividad en la concientización del equipo respecto a la importancia y responsabilidad en la gestión integral de la organización.
--	--	--	--

Tabla 83 (Continuación)

7.5 Información documentada			
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo

7.5.1 Generalidades	El sistema de gestión de la calidad de la organización debe incluir: a) la información documentada requerida por esta Norma Internacional; b) la información documentada que la organización determina como necesaria para la eficacia del sistema de gestión de seguridad de la información.	C	Se muestra el documento "Pr_Control de documentos_V02" actualizado el 5 de mayo del 2023
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
7.5.2 Creación y actualización	Al crear y actualizar la información documentada, la organización debe asegurarse de que lo siguiente sea apropiado: a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia); b) el formato (por ejemplo, idioma, versión del software, gráficos) y los medios de soporte (por ejemplo, papel, electrónico); c) la revisión y aprobación con respecto a la conveniencia y adecuación	C	Se muestra el "Pr_Control de documentos_V02" actualizado el 5 de mayo del 2023, "Re_Inventario de documentos_2023" actualizado el 8 de diciembre del 2023, en el repositorio documental se encuentran los editables, respaldos y los documentos obsoletos que aún se encuentran en resguardo según las políticas de la

			organización, también se muestra el "Re_Bitácora de revisión de documentos externos_2023" actualizado el 8 de diciembre del 2023
--	--	--	--

Tabla 84 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
7.5.3 Control de la información documentada	La información documentada requerida por el sistema de gestión de la calidad y por esta Norma Internacional se debe controlar para asegurarse de que: a) esté disponible y sea idónea para su uso, donde y cuando se necesite; b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado o pérdida de integridad).	C	Se muestra el "Pr_Control de documentos_V02" actualizado el 5 de mayo del 2023, "Re_Inventario de documentos_2023" actualizado el 8 de diciembre del 2023, en el repositorio documental se encuentran los editables, respaldos y los documentos obsoletos que aún se encuentran en resguardo según las políticas de la organización, también se muestra el "Re_Bitácora de revisión de documentos

			externos_2023" actualizado el 8 de diciembre del 2023
--	--	--	---

Tabla 85 (Continuación)

8 Operación			
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
8.1 Planificación y control operacional	La organización debe planear, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información, y para implementar las acciones determinadas en el inciso 6.1 La organización debe también implementar planes para lograr los objetivos de seguridad de la información determinados en el inciso 6.2 La organización debe mantener la información documentada en la medida necesaria para tener certeza de que los procesos se han llevado a cabo según lo planeado. La organización	C	La organización ha documentado meticulosamente sus procedimientos, respaldada por un Plan de Aseguramiento del Mantenimiento del Avance (PAMA) de procesos. Cada procedimiento ha sido detallado con el objetivo de garantizar la claridad y consistencia en su ejecución. Además, se han establecido indicadores de desempeño específicos en cada uno de ellos para medir y evaluar el cumplimiento de los objetivos y

	debe controlar los cambios planeados y revisar las consecuencias de los cambios no deseados, tomando acciones para mitigar efectos adversos, según sea necesario. La organización debe asegurarse de que los procesos de desarrollo de sistemas sean determinados y controlados.		detectar áreas de mejora continua. Asimismo, la organización ha implementado un procedimiento dedicado a la gestión del cambio Pr_Gestión del cambio_V01 publicado el 10 de febrero del 2023. Este procedimiento facilita una transición suave y efectiva en situaciones donde se requieran modificaciones en los procesos, políticas o infraestructura organizacional. A través de este procedimiento, se establecen pasos y controles específicos para evaluar, aprobar e implementar cambios, minimizando así los riesgos y maximizando el éxito de cualquier modificación realizada.
--	---	--	--

Tabla 86 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
8.2 Evaluación de riesgos y de seguridad de la información	La organización debe llevar a cabo las evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se proponen o se producen cambios significativos, teniendo en cuenta los criterios establecidos en el incisos 6.1.2 inciso a).	C	Se muestra el "Pr_valoración, evaluación y tratamiento de riesgos_V09" actualizado el 31 de julio del 2023 el cual cuenta con 9 actividades a desarrollar 1. Identificación de elementos críticos 2. Clasificación de elementos 3. Amenazas 4. Probabilidad de ocurrencia 5. Impacto (humano, material, financiero, operativo, imagen 6. Identificación del riesgo 7. Tipo de tratamiento (aceptación, mitigación, transferencia, eliminación) 8. Aceptación de riesgos residuales

			9. Revisar la eficacia de los controles
--	--	--	---

Tabla 87 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
8.3 Tratamiento de riesgos de seguridad de la información	La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información. La organización debe conservar la información documentada de los resultados del tratamiento de riesgos de seguridad de la información.	C	Se muestra el "Re_valoración de riesgos_2do semestre 2023" con fecha del 31 de agosto del 2023 donde se identificaron 70 elementos y todos son riesgos bajos Se ha observado que se cuenta con un propietario claramente identificado para gestionar los riesgos, aunque hay responsables asignados, las responsabilidades de este rol están definidas de manera precisa. Además, se ha realizado la comparativa de los controles determinados

			en el inciso 6.1.3 inciso b) con los descritos en el apéndice "A". La declaración de aplicabilidad carece de la justificación requerida según lo establecido en el inciso d) del 6.1.3. Se está llevando a cabo la evaluación del riesgo residual.
--	--	--	--

Tabla 88 (Continuación)

9 Evaluación del desempeño				
9.1 Seguimiento, medición, análisis y evaluación				
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo	
9.1 Monitoreo, medición, análisis y evaluación	La organización debe determinar: a) qué necesita seguimiento y medición; b) los métodos de seguimiento, medición, análisis y evaluación necesarios para asegurar resultados válidos; c) cuándo se deben llevar a cabo el seguimiento y la medición; d) cuándo se deben analizar y evaluar los resultados del seguimiento y la medición. La	C	Se muestra el "Pr_Gestión de mejora continua_V03" actualizado el 21 de agosto del 2023 y el "Re_Matriz de monitoreo_2023" generado el 21 de agosto del 2023 correspondiente. Sin embargo, se identificó que los informes de "Pr_Recursos Humanos_V01"	

	organización debe evaluar el desempeño y la eficacia del sistema de gestión de la calidad. La organización debe conservar la información documentada apropiada como evidencia de los resultados		generado el 19 de septiembre del 2023 no proporcionan una verificación adecuada del cumplimiento de los indicadores establecidos. Se recomienda una revisión y actualización de los informes para garantizar una supervisión efectiva de los indicadores pertinentes.
--	---	--	---

Tabla 89 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
9.2 Auditoría interna	La organización debe llevar a cabo auditorías internas a intervalos planificados para proporcionar información acerca de si el sistema de gestión de la calidad: a) es conforme con: 1) los requisitos propios de la organización para su sistema de gestión de la calidad; 2) los requisitos de esta Norma Internacional; b) se implementa y mantiene eficazmente.	C	Se constata que la organización realiza auditorías internas según lo establecido en el "Re_Calendario de Auditoría Interna_2023", creado el 2 de enero del 2023. Dichas auditorías evalúan los requisitos inherentes a su sistema de gestión integral, como se documenta en el "Re_Plan de Auditoría

			Interna_2023" generado el 2 de enero del 2023. Además, se evidencia que el equipo auditor posee competencias conforme a la normativa ISO 27001:2013.
--	--	--	--

Tabla 90 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
9.3 Revisión por la dirección	La alta dirección debe revisar el sistema de gestión de la calidad de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación, eficacia y alineación continuas con la dirección estratégica de la organización.	C	La alta dirección lleva a cabo revisiones del sistema de gestión de la calidad de la organización en intervalos planificados, con el fin de garantizar su pertinencia, idoneidad, eficacia y continua alineación con la dirección estratégica de la misma. Se muestra el documento "Re_Revisión por Dirección_3er trimestre 2023" generado el 1 de septiembre del 2023 como evidencia de esta revisión planificada, así

			como del "Re_Informe de Revisión por Dirección_3er trimestre 2023" generado el 1 de septiembre del 2023 para documentar los resultados y las acciones derivadas de dicha revisión.
--	--	--	--

Tabla 91 (Continuación)

10 Mejora			
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
10.1 No conformidad y acción correctiva	Cuando ocurre una no conformidad, la organización debe reaccionar a la inconformidad según sea el caso.	C	Se muestra el "Re_Plan de Acción_146" identificado bajo el folio 146 generado el 5 de junio del 2023 correspondiente a una Oportunidad de Mejora en el requisito de Auditoría Interna, según el informe de la Auditoría. Se evidencia progreso en la ejecución del mencionado plan, el cual aún se encuentra en curso.

Tabla 92 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

10.2 Mejora continua	La organización debe mejorar continuamente la idoneidad, la adecuación y la eficacia del SGSI.	C	Se muestra el "Re_Plan de Acción_154", generado el 27 de julio de 2023, dirigido a mejorar el servicio de mesa de ayuda en respuesta a las sugerencias recopiladas a través de las encuestas de satisfacción. Se confirma que el plan de acción se encuentra en fase de ejecución.
----------------------	--	---	--

A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A.5.1 Gestión de la Dirección para la Seguridad de la Información	Proporcionar dirección general y apoyo para la seguridad de la información de acuerdo con los requisitos del negocio y las leyes y regulaciones relevantes.		
A.5.1.1 Políticas para la Seguridad de la Información	Se debe definir, aprobar por la dirección, publicar y comunicar a todos los empleados y partes externas relevantes u conjunto de políticas para la seguridad de la información.	C	Se muestran las políticas de seguridad de la información documentadas en "Po_Seguridad de la información _V08" actualizadas el 15 de marzo del 2023 se identificó que las mismas abordan

			aspectos fundamentales como seguridad física, ambiental, gestión de activos y tratamiento de la información.
--	--	--	--

Tabla 93 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.5.1.2 Revisión de Políticas de Seguridad de la Información	Las políticas para la seguridad de la información deben revisarse a intervalos planeados o si ocurren cambios significativos para garantizar su continua idoneidad, adecuación y eficacia.	C	Se verifica que la revisión se realiza mínimo anualmente, o cuando se presenten cambios significativos en la organización, como lo establecen las políticas de la organización.

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A.6.1 Organización Interna	Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.		
----------------------------	---	--	--

Tabla 94 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.6.1.1 Roles y Responsabilidades para la Seguridad de la Información	Todas las responsabilidades de la seguridad de la información deben definirse y asignarse.	C	Se identifica la existencia de un comité del Sistema de Gestión Integral (SGI)

			conformado por roles claramente definidos, tales como: Dirección General Adjunta, Responsable del SGI, Responsable de Seguridad de la Información y otros roles como Responsable de la Gestión del Servicio, Responsable del Diseño y Despliegue de Servicios.
A.6.1.2 Segregación de Tareas	Las tareas en conflicto y áreas de responsabilidad deben segregarse para reducir las oportunidades de modificación no autorizada, no intencional o mal uso de los activos de la organización.	C	Se ha identificado segregación de deberes en el proceso de ingreso a portales y en la aceptación de cambios en la configuración. Se ha evidenciado adecuada segregación en los cambios realizados en la configuración, lo cual es positivo para mantener la integridad y seguridad de los sistemas.

Tabla 95 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.6.1.3 Contacto con Autoridad	Se deben mantener contactos apropiados con las autoridades relevantes	NC	Se muestra el "Re_Matriz contacto autoridades_2023" actualizado el 23 de agosto del 2023 en el cual solo se incluyen a los grupos de interés especiales.
A.6.1.4 Contacto con Grupos de Especial Interés	Se deben mantener contactos apropiados con grupos especiales de interés u otros foros de seguridad especializados y asociaciones profesionales.	C	Se muestra el "Re_Matriz contacto autoridades_2023" actualizado el 23 de agosto del 2023 en el cual se incluyen los grupos especiales donde considera contactos y boletines para OWASP, UNAM-CERT, SANS y Alienvault OTX
A.6.1.5 Seguridad de la Información en la Administración de Proyectos	La seguridad de la información debe incluirse en la administración de proyectos independientemente del tipo de proyecto.	OB	Se muestra el "Fo_Implementación de servicio_V04" actualizado el 25 de mayo del 2023 el cual considera endpoint para infonavit, en el documento se aprecia que se consideran los riesgos del proyecto. Se muestra evidencia del proyecto "Re_plan

			de trabajo_Instalación de memorias RAM y discos duros en servidores" generado el 31 de octubre del 2023, En este caso, la documentación carece de la identificación de riesgos asociados al proyecto, lo cual constituye una deficiencia que requiere atención y corrección inmediata. Es esencial que la organización considere los riesgos en todos sus proyectos, tanto internos como externos. La gestión proactiva de riesgos es fundamental para anticipar obstáculos, tomar medidas preventivas y asegurar el éxito de los proyectos.
--	--	--	--

Tabla 96 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.6.2 Dispositivos móviles y teletrabajo	Garantizar la Seguridad del Teletrabajo y el uso de dispositivos móviles.		

A.6.2.1 Política de Dispositivos Móvil	Se debe adoptar una política y medidas de seguridad de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles.	C	Se muestra la "Po_Uso de teléfonos inteligentes y cámaras digitales_V05" actualizada el 14 de junio del 2023 que se encarga de la seguridad de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2 Teletrabajo	Se debe implementar una política y medidas de seguridad de soporte para proteger el acceso, proceso o almacenamiento de la información en los sitios de trabajo a distancia.	C	Se identificó que en la versión actualizada de la política "Po_Movilidad_V03", fechada el 4 de julio de 2023, se especifica el uso de VPN y enlaces privados para salvaguardar el acceso, así como el cifrado para proteger tanto el proceso como el almacenamiento de datos durante el trabajo remoto.

Tabla 97 (Continuación)

A.7 SEGURIDAD EN LOS RECURSOS HUMANOS			
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo

A.7.1 Previo al Empleo	Asegurar que los empleados y contratistas entiendan sus responsabilidades y son adecuados para los roles para los cuales son considerados	C	Se lleva a cabo un estudio socioeconómico junto con pruebas psicométricas para evaluar la comprensión de responsabilidades y la idoneidad de los colaboradores para los roles asignados.
A.7.1.1 Investigación	Se deben llevar a cabo verificaciones de antecedentes a todos los candidatos al empleo de acuerdo con las leyes, regulaciones relevantes y la ética, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.	C	Se lleva a cabo un estudio socioeconómico junto con pruebas psicométricas para evaluar la comprensión de responsabilidades y la idoneidad de los colaboradores para los roles asignados.

Tabla 98 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.7.1.2 Términos y Condiciones del Empleo	Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de la organización para la seguridad de la información.	C	Los acuerdos contractuales con colaboradores, como el contrato firmado por Renato Figueroa firmado el 30 de noviembre del 2023,

			contienen disposiciones detalladas sobre las responsabilidades tanto del individuo como de la organización. Se destaca la inclusión de cláusulas de confidencialidad de la información en dichos contratos, para la protección de los datos sensibles y la mitigación de riesgos relacionados con la divulgación no autorizada.
--	--	--	--

Tabla 99 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.7.2 Durante el Empleo	Asegurar que los empleados y contratistas estén conscientes de que cumplen con sus responsabilidades de la seguridad de la información.		
A.7.2.1 Responsabilidades de la Dirección	La dirección debe exigir a todos los empleados y contratistas aplicar la seguridad de la información de acuerdo con las políticas	C	La Dirección ha establecido la exigencia de cumplimiento de las responsabilidades de Seguridad de la

	y procedimientos establecidos en la organización.		Información mediante la definición de perfiles de puesto, incluyendo actividades específicas que resaltan dichas responsabilidades. Se muestra el "Re_Perfil de puesto_Responsable de RH" actualizado el 5 de Julio del 2023
A.7.2.2 Concientización, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando sea relevante, contratistas deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y procedimientos organizacionales, cuando sea relevante para sus funciones de trabajo.	C	Se muestra el "Re_Plan de capacitación_2023" actualizado el 20 de julio del 2023 el cual se encuentra en ejecución, incluye temas relacionados a seguridad de la información y al Sistema de Gestión de la Información (SGI).

Tabla 100 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.7.2.3 Proceso Disciplinario	Debe haber y comunicarse un proceso disciplinario formal para tomar acciones contra empleados que hayan cometido una violación a la seguridad de la información.	C	Durante el año 2023 la organización no ha aplicado ningún proceso disciplinario.

A.7.3 Terminación y Cambio de Empleo	Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.		
A.7.3.1 Responsabilidades en la terminación o cambio de empleo	Las responsabilidades de la seguridad de la información y obligaciones que permanecen validos después de la terminación o el cambio e empleo deben estar definidos, comunicados a los empleados o contratistas y hacerse cumplir.	OB	Se evidencia la baja de Gabriel Arcega Soto, documentada con la conformación del expediente de baja, el cual incluye diversos elementos como renuncia, baja del biométrico, solicitud de baja de activos, accesos físicos y lógicos, carta de asignación y devolución de activos, y aviso de privacidad. Asimismo, se presenta evidencia del cambio de puesto de Gabriel Arcega Soto, respaldado por la minuta de aprobación del cambio y el perfil de puestos firmado por la parte involucrada generados el 25 de octubre de 2023. Sin embargo, no se

			encontró evidencia de que la organización haya comunicado y/o recordado las responsabilidades de Seguridad de la Información que permanecen vigentes, ni los derechos de ARCO (Acceso, Rectificación, Cancelación y Oposición) respecto a la desvinculación de los colaboradores.
--	--	--	--

Tabla 101 (Continuación)

A.8 GESTIÓN DE ACTIVOS			
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.8.1 Responsabilidad Sobre los Activos	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		
A.8.1.1 Inventario de Activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información y se debe	C	Se ha identificado que el listado general de activos en el reporte de Excel de la herramienta Aranda incluye tanto los activos utilizados para

	elaborar y mantener un inventario de estos activos.		la prestación de servicios a clientes como los utilizados internamente por la organización. Además, se ha observado que en la CMDB de la herramienta se listan los activos junto con su categoría y el responsable correspondiente.
A.8.1.2 Propiedad de los Activos	Los activos incluidos en el inventario deben contar con un propietario.	C	Se ha identificado que el listado general de activos en el reporte de Excel de la herramienta Aranda incluye tanto los activos utilizados para la prestación de servicios a clientes como los utilizados internamente por la organización. Además, se ha observado que en la CMDB de la herramienta se listan los activos junto con su categoría y el responsable correspondiente.

Tabla 102 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.8.1.3 Uso aceptable de los Activos	Se debe identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos asociados con la información y las instalaciones de procesamiento de la información.	C	Se evidencia la baja de Gabriel Arcega Soto, documentada con la conformación del expediente de baja, el cual incluye diversos elementos como renuncia, baja del biométrico, solicitud de baja de activos, accesos físicos y lógicos, carta de asignación y devolución de activos, y aviso de privacidad

Tabla 103 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.8.1.4 Devolución de Activos	Todos los empleados y los usuarios de partes externas deben devolver todos los activos de la organización en su posesión a la terminación de su empleo, contrato o acuerdo	C	Se evidencia la baja de Gabriel Arcega Soto, documentada con la conformación del expediente de baja, el cual incluye diversos elementos como renuncia, baja del biométrico, solicitud de baja de activos, accesos físicos y lógicos, carta

			de asignación y devolución de activos, y aviso de privacidad
A.8.2 Clasificación de Información	Asegurar que la información reciba un apropiado nivel de protección de acuerdo con su importancia para la organización.		
A.8.2.1 Clasificación de Información	La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad de su divulgación o modificación no autorizada.	C	Se ha establecido un esquema de clasificación de la información que comprende las categorías de confidencial, restringida, interna y pública dentro de la organización.

Tabla 104 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.8.2.2 Etiquetado de información	Se debe desarrollar e implementar un apropiado conjunto de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización	C	La información es etiquetada con las categorías correspondientes (confidencial, restringida, interna y pública) en los encabezados de los documentos. Además, se ha observado que se

			coloca una marca de agua en las hojas de los documentos para facilitar su etiquetado y clasificación.
A.8.2.3 Manejo de Activos	Se deben desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de la información adoptado por la organización.	C	Se ha establecido el "Pr_Gestión de activos y su configuración_V02" actualizado el 1 de febrero del 2023 dentro de la organización. Además, se han definido lineamientos para el manejo de la información, considerando su clasificación, incluyendo el uso de canales seguros, cifrados y VPN.

Tabla 105 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.8.3 Manejo de Medios	Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de información almacenada en medios.		
A.8.3.1 Gestión de Medios Removibles	Se deben implementar procedimientos para la gestión de medios	C	Los puertos USB están bloqueados, a excepción de los

	removibles de acuerdo con el esquema de clasificación adoptado por la organización.		utilizados por directivos y gerentes dentro de la organización.
A.8.3.2 Disposición de Medios	Se deben disponer de manera segura los medios cuando ya no se requieran, utilizando procedimientos formales.	C	Para la destrucción de información física se usa una trituradora de papel. Asimismo, se realiza el borrado de discos para la eliminación de información lógica. Se muestra el "Re_Bitácora de destrucción y borrado_2023" actualizado el 8 de diciembre del 2023 para mantener un registro adecuado de estas actividades.

Tabla 106 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.8.3.3 Transferencia de Medios Físicos	Se deben proteger los medios que contengan información contra acceso no autorizado, mal uso o corrupción durante la transportación.	C	La organización utiliza mensajería interna para la entrega de información, la cual se hace personalmente a los clientes y/o responsables.

			Se muestra el "Re_Acuse de recibo_Infonavit" de la entrega física de información realizada el 15 de agosto del 2023
--	--	--	---

A.9 CONTROL DE ACCESO

A.9.1 Requisitos del Negocio para el Control de Acceso	Limitar el acceso a la información y a las instalaciones de procesamiento de la información.		
A.9.1.1 Política de Control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de la seguridad de la información.	C	Se presenta la "Po_Control de Accesos_V06", actualizado el 20 de octubre del 2023 documento que regula el acceso a los recursos y sistemas de información de la organización. Esta política, en su versión más reciente, se basa en los requisitos del negocio y los estándares de seguridad de la información. Establece principios para la autenticación,

			autorización y monitoreo de acceso, asegurando la integridad y confidencialidad de los activos de información.
--	--	--	--

Tabla 107 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.9.1.2 Acceso a las Redes y los Servicios de la Red	Se debe proporcionar a los usuarios únicamente el acceso a la red y servicios de la red para los que hayan sido específicamente autorizados	C	La provisión de acceso a la red y sus servicios es otorgada exclusivamente a usuarios autorizados, según lo especificado en sus perfiles de acceso correspondientes.

Tabla 108 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.9.2 Gestión del Acceso de Usuarios	Garantizar el acceso de usuarios autorizados y prevenir acceso no autorizado a sistemas y servicios.		
A.9.2.1 Registro y Cancelación de Usuarios	Se debe implementar un proceso formal de registro y cancelación de usuarios para permitir la asignación de derechos de acceso.	C	Se ha identificado la existencia del documento "Re_Solicitud de Acceso_150823", el cual se utiliza para gestionar el servicio de

			acceso dentro de la organización.
A.9.2.2 Provisión de Acceso de Usuarios	Se debe implementar un proceso formal para la provisión de acceso a usuarios para asignar o revocar derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.	C	El caso 2964 se refiere al alta de Mariana Jiménez García, ocurrida el 8 de febrero de 2023. Este caso se presenta para gestionar la asignación de accesos correspondiente.
A.9.2.3 Gestión de Derechos de Acceso Privilegiado	La asignación y uso de los derechos de acceso privilegiado deben restringirse y controlarse.	C	Únicamente el área de operaciones cuenta con accesos privilegiados de administración en el sistema, garantizando así un control adecuado sobre los permisos de acceso.

Tabla 109 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.9.2.4 Gestión de Información Secreta de Autenticación de los Usuarios	La asignación de información secreta de autenticación debe controlarse a través de un proceso de gestión formal.	C	Se observa que los usuarios y contraseñas se envían por medios distintos, y se ha levantado un ticket para definir una nueva contraseña.
A.9.2.5 Revisión de los Derechos de Acceso de Usuario	Los propietarios de activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	C	Se llevó a cabo una revisión de control de acceso de usuarios en el año 2023, la cual se

			realiza de manera semestral.
A.9.2.6 Eliminación o Ajuste de los Derechos de Acceso.	Los derechos de acceso de todos los empleados y usuarios de partes externas a la información e instalaciones de procesamiento de la información deben ser eliminados después de la terminación de su empleo, contrato o acuerdo, o adaptados a los cambios producidos.	C	Se presenta el caso 6566 relacionado con la baja de Gabriel Arcega Soto generado el 25 de octubre del 2023, destinado a la revocación de los accesos derivados de su cambio de puesto. Esto implica la aplicación de restricciones de acceso correspondientes a su nueva posición dentro de la organización.

Tabla 110 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.9.3 Responsabilidad del Usuario	Hacer responsables a los usuarios de salvaguardar su información de autenticación.	C	Se muestra el Re_Carta de asignación de activos_Juan David Mejía Hernández" generada el 7 de noviembre del 2023, donde se identifican las responsabilidades que debe cumplir al utilizar los activos de información. Además, se ha observado que las

			contraseñas se actualizan cada 90 días
A.9.3.1 Uso de Información Secreta de Autenticación.	Se debe exigir a los usuarios que sigan las prácticas de la organización en el uso de su información secreta de autenticación.	C	Se muestra el Re_Carta de asignación de activos_Juan David Mejía Hernández" generada el 7 de noviembre del 2023, donde se identifican las responsabilidades que debe cumplir al utilizar los activos de información. Además, se ha observado que las contraseñas se actualizan cada 90 días

Tabla 111 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.9.4 Control de Acceso a Sistemas y Aplicaciones	Prevenir el acceso no autorizado a los sistemas y aplicaciones.	C	Se ha identificado que el acceso a la información y las funciones de las aplicaciones de los sistemas está restringido de acuerdo con la política de control de acceso mediante la definición de perfiles de acceso.

A.9.4.1 Restricción de Acceso a la Información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones de los sistemas de acuerdo con la política de control de acceso.	C	Se ha identificado que el acceso a la información y las funciones de las aplicaciones de los sistemas está restringido de acuerdo con la política de control de acceso mediante la definición de perfiles de acceso.
--	--	---	--

Tabla 112 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.9.4.2 Procedimiento de Inicio de Sesión Seguros	Cuando se requiere por la política de control de acceso, el acceso a los sistemas y aplicaciones debe controlarse por un procedimiento de inicio de sesión seguro.	C	Los equipos de cómputo deben cumplir con los lineamientos establecidos por la política de creación de contraseñas, incluyendo su periodicidad de cambio.
A.9.4.3 Sistema de Administración de Contraseñas	Los sistemas de administración de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	C	La organización cuenta con lineamientos definidos para la creación de contraseñas, los cuales están respaldados por el Directorio Activo. Además, se ha

			observado que se lleva a cabo el cambio de contraseñas cada 90 días.
A.9.4.4 Uso de Privilegios de los Programas de Utilidades	El uso de programas de utilidades que puedan ser capaces de anular los controles del sistema y de las aplicaciones deben estar restringidas y estrechamente controladas.	C	La organización no utiliza programas, aplicaciones y/o software de utilidades en su operación.

Tabla 113 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.9.4.5 Control de Acceso a Código Fuente del Programa	Se debe restringir el acceso al código fuente del programa.	C	Exclusión
A.10 CRIPTOGRAFÍA			
A.10.1 Controles Criptográficos	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información		

A.10.1.1 Política sobre el Uso de Controles Criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	C	La organización ha implementado una política integral que aborda la seguridad de los equipos utilizados por sus colaboradores. Esta política incluye medidas específicas para proteger la información confidencial y garantizar la integridad de los datos almacenados en los dispositivos. En primer lugar, se ha implementado el cifrado de disco mediante BitLocker en todos los equipos, lo que proporciona una capa adicional de seguridad al proteger los datos almacenados en el disco duro contra accesos no autorizados. Además, para asegurar la confidencialidad de la comunicación con los clientes, se utiliza el software 7zip, que
--	---	---	--

			ofrece un cifrado robusto para los archivos enviados a través de correos electrónicos u otros medios. Asimismo, se ha establecido un protocolo de cifrado para los correos electrónicos, lo que garantiza que cualquier información sensible enviada por esta vía esté protegida de posibles interceptaciones o accesos no autorizados. Se encuentra documentado en la Po_Controles criptográficos_V02 con fecha de actualización del 2 de junio del 2023
--	--	--	--

Tabla 114 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.10.1.2 Gestión de Llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, a través de todo su ciclo de vida.	C	El tiempo de vida designado para las llaves se establece en un período de 1 a 2 años según las políticas establecidas por la organización.

A.11 SEGURIDAD FÍSICA Y AMBIENTAL			
A.11.1 Áreas Seguras	Prevenir el acceso físico no autorizado, daños e interferencia a la información e instalaciones de procesamiento de la información de la organización.		

Tabla 115 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.11.1.1 Perímetro de Seguridad Física	Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen información ya sea sensible o crítica y las instalaciones de procesamiento de la información.	OB	Se muestra el Ma_Seguridad de la organización_V01 fechado el 25 de mayo del 2023 pero no se identifican los controles implementados.
A.11.1.2 Controles Físicos de Entrada	Se deben proteger las áreas seguras mediante controles de entrada apropiados para garantizar que sólo el personal autorizado tenga acceso permitido.	C	Se cuenta con controles de acceso biométrico, circuito cerrado de televisión (CCTV), cercado eléctrico perimetral, sistemas de

			extinción de incendios, registro de ingresos y salidas, dispositivos de detección de humo y de movimiento, así como una zona específica designada para operaciones de carga y descarga
A.11.1.3 Aseguramiento de Oficinas, Salas e Instalaciones	Se debe diseñar y aplicar seguridad física para oficinas, salas e instalaciones.	C	Se cuenta con sistemas de seguridad que incluyen controles de acceso biométrico, circuito cerrado de televisión (CCTV) y dispositivos de detección de movimiento.

Tabla 116 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.11.1.4 Protección contra Amenazas Externas y Ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	C	Se dispone de una infraestructura integral para garantizar la continuidad operativa y la seguridad del entorno. Esto comprende una planta de emergencia, sistemas de alimentación ininterrumpida (UPS), dispositivos de control

			de acceso, sistemas de alarma y una red de cableado eléctrico debidamente instalada.
A.11.1.5 Trabajo en Áreas Seguras	Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras.	C	Se cuenta con controles de acceso biométrico, CCTV, detectores de movimiento. Se han definido lineamientos para trabajar en estas áreas de la organización. Puesto de trabajo limpio, pantalla y escritorio limpio y despejado de papeles.

Tabla 117 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.11.1.6 Áreas de Entrega y Carga	Los puntos de acceso, tales como las áreas de entrega y carga y otros puntos en los que personas no autorizadas puedan entrar en las instalaciones deben ser controlados y, si es posible, aislados de las instalaciones de procesamiento de la información para evitar acceso no autorizado.	C	Se muestra el Ma_Seguridad de la organización_V01 fechado el 25 de mayo del 2023 donde se identifican el estacionamiento como área de carga y descarga.
A.11.2 Equipo	Prevenir la pérdida, daño, robo o comprometer los		

	activos e interrupción de las operaciones de la organización.		
A.11.2.1 Ubicación y Protección de Equipo	El equipo debe estar situado y protegido para reducir los riesgos de amenazas ambientales y peligros, y las oportunidades para el acceso no autorizado.	C	Se lleva a cabo una supervisión continua para garantizar la integridad y la seguridad de los sistemas. Se implementa el cifrado de disco para proteger la información sensible. Además, se activan medidas como el bloqueo por inactividad, la restricción de puertos USB, el control de acceso y la gestión del retiro de consolas para fortalecer la seguridad del entorno.

Tabla 118 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.11.2.2 Servicios Públicos	El equipo debe estar protegido contra fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.	C	La infraestructura incluye tanto una planta de emergencia como sistemas de alimentación ininterrumpida (UPS)

A.11.2.3 Seguridad del Cableado	El cableado de energía y telecomunicaciones que transporten datos o soporten los servicios de la información deben protegerse de interceptación, interferencia y daño.	C	El cableado eléctrico ha sido ocultado y canalizado dentro de canaletas,
A.11.2.4 Mantenimiento de Equipo	El equipo debe mantenerse correctamente para asegurar su continua disponibilidad e integridad.	C	Los mantenimientos a equipos se realizan semestralmente. Se muestra el Re_Mantenimiento a equipo del 11 de enero del 2023 y 25 de marzo del 2023, laptop de Pedro Hernández y el de Erika González, equipo de cómputo el 11 de enero del 23 y 16 de febrero del 2023 Se muestra el Pr_Mantenimiento a electroimán de puertas_V01 fechado el 14 de febrero del 2023. Se muestra el Pr_Mantenimiento de extintores, recarga y mantenimiento_V01 fechado el 16 de mayo del 2023.

			Pr_Mantenimiento de planta de emergencia, UPS, aire acondicionado_V01 fechado el 20 de enero del 2023
--	--	--	--

Tabla 119 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.11.2.5 Retiro de Activos	No se debe sacar del sitio sin autorización previa el equipo, información o software.	C	Se muestra el Re_Carta de retiro y el Re_Carta de asignación de equipo (servidores fechados el 15 de marzo del 2023).

Tabla 120 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.11.2.6 Seguridad de los Equipos y Activos fuera de las Instalaciones	Se debe aplicar seguridad a los activos fuera de las instalaciones tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	C	Se ha identificado la implementación de medidas de seguridad, tales como supervisión permanente, cifrado de disco, activación de bloqueo por inactividad, restricción de puertos USB, control de acceso y gestión del retiro de consolas.
A.11.2.7 Disposición o Reutilización Segura del Equipo	Todos los elementos del equipo que contiene medios de almacenamiento deben ser verificados para garantizar que cualquier	C	Se aplicará borrado seguro y puede ser donado, vendido o desechado. Se muestra la

	dato sensible y software licenciado ha sido eliminado o sobrescrito de manera segura previo a su disposición o reutilización.		Re_Bitácora de borrado seguro fechado el 21 de marzo del 2023. La disposición para el equipo de Medar es almacenamiento.
A.11.2.8 Equipo de Usuario Desatendido	Los usuarios deben garantizar que el equipo desatendido tenga la protección adecuada.	C	Se aplica un bloqueo por inactividad después de tres minutos de inactividad, lo que refuerza la seguridad y la protección de los sistemas ante posibles accesos no autorizados.

Tabla 121 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.11.2.9 Política de Pantalla y Escritorio Limpio	Se debe adoptar una política de escritorio limpio de papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de la información.	C	Se define una Po_Puesto de trabajo libre de papeles y escritorio y pantalla limpia_V01 fechado 5 de enero del 2023 que se valida durante la auditoría.
A.12 SEGURIDAD EN OPERACIONES			
A.12.1 Procedimientos y Responsabilidades Operativas	Garantizar la operación correcta y segura de las instalaciones de procesamiento de la información.		

A.12.1.1 Procedimientos Operativos Documentados	Deben documentarse los procedimientos operativos y estar disponibles para todos los usuarios que los necesiten.	C	La organización ha documentado lo siguiente Pr_Gestión del cambio_V01, Pr_Gestión de la capacidad_V01, Pr_Gestión de la disponibilidad_V01, Pr_Gestión de la configuración_V01, Pr_Diseño y transición de servicios_V01, Pr_Respaldos_V01 Y Pr_Control de documentos, continuidad_V01 fechados el día 19 de mayo del 2023.
--	---	---	--

Tabla 122 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.12.1.2 Gestión del Cambio	Se deben controlar los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten a la seguridad de la información.	OB	Se cuenta con un Pr_Gestión del cambio_V01 fechado el 19 de mayo del 2023 que incluye los elementos solicitados por el requisito. Tipos de cambio: estándar, normal y emergente No ha habido cambios

			internos. Se muestra Aranda, herramienta utilizada para gestionar los cambios a la infraestructura o los cambios en los servicios. Se muestra Re_Caso no. 63 / CHG8268-1-63 fechado el 17 de marzo del 2023 por Saul Gómez del cliente Secretaría de Turismo, se observa debidamente requisitos a la solicitud de cambio, misma que se anexa al caso creado. En Criterios de impacto: en la tabla de tipos de cambio se describen los impactos sin embargo no existe un criterio que sea compatible con lo configurado en la herramienta de Aranda.
--	--	--	--

Tabla 123 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.12.1.3 Gestión de Capacidad	El uso de recursos debe monitorearse, afinarse para realizar proyecciones de los requisitos futuros de la capacidad para garantizar el desempeño requerido de los sistemas.	NC	Se ha constatado que el monitoreo de la capacidad para el año 2023 contempla los umbrales de los servicios y sus componentes, así como los recursos técnicos y los indicadores clave de rendimiento (KPIs). Este monitoreo se lleva a cabo de forma bimestral. Además, se presenta el Fo_Plan de capacidad_V01 correspondiente al día 20 de enero del año 2023, el cual abarca los activos, el período de evaluación, los datos analizados, la audiencia objetivo y los recursos necesarios para garantizar la provisión efectiva de los servicios.
-------------------------------	---	----	---

Tabla 124 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.12.1.4 Separación de Entornos de Desarrollo, Pruebas y Operación.	Se deben separar los entornos de desarrollo, pruebas y operación para reducir los riesgos de acceso no autorizado o cambios al entorno de operación.	C	Se ha constatado la existencia de un entorno de desarrollo que cumple con estándares de seguridad adecuados, lo que contribuye a mitigar riesgos y asegurar la integridad de los sistemas durante el proceso de desarrollo de software.
---	--	---	---

Tabla 125 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.12.2 Protección contra Malware	Garantizar que la información y las instalaciones de procesamiento de la información estén protegidas contra malware.		
A.12.2.1 Controles contra Malware	Se deben implementar controles de detección, Prevención y recuperación para protegerse contra malware y combinarse con una apropiada concientización a usuarios.	C	Se ha verificado que se dispone de un sistema de seguridad informática, específicamente Kaspersky, el cual ha sido instalado en todos los equipos utilizados por la organización para brindar sus servicios.

			Esto asegura una protección integral contra amenazas cibernéticas y contribuye a mantener la integridad y confidencialidad de la información.
--	--	--	---

Tabla 126 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.12.3 Respallos	Proteger contra la pérdida de datos.		
A.12.3.1 Respallos de la Información	Copias de respaldos de la información, software e imágenes de sistemas deben realizarse y probarse regularmente de acuerdo con la política de respaldos acordada.	NC	Se muestra una Re_Bitácora de respaldos fechada el día 8 de febrero del 2023, en la cual se identifica la realización de respaldos completos e incrementales para (ofimática, PRTG, Firewall, switch). Sin embargo, al revisar la bitácora detalladamente, se encuentra que no se ha registrado la realización de respaldos para ninguna de las plataformas mencionadas. Esta

			omisión representa un incumplimiento de los procedimientos establecidos para la realización de respaldos de datos, lo que podría generar riesgos significativos para la integridad y disponibilidad de la información de la organización. Por lo tanto, es necesario revisar y reforzar los procedimientos de respaldo de datos para garantizar que se realicen de manera adecuada y se registren correctamente en la bitácora correspondiente.
--	--	--	---

Tabla 127 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.12.4 Registro y Monitoreo	Registrar eventos y generar evidencia.		
A.12.4.1 Registro de Eventos	Se deben generar, mantener y revisar regularmente los registros de eventos de las	C	Se ha confirmado la presencia de la herramienta de

	actividades de usuarios, excepciones, fallas y eventos de seguridad de la información.		Directorio Activo en sistema dentro de la organización. Esta herramienta es fundamental para la gestión centralizada de usuarios, equipos y recursos dentro del entorno de red, lo que facilita la administración eficiente de los sistemas y contribuye a mantener la seguridad y el orden en el ambiente informático.
--	--	--	---

Tabla 128 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.12.4.2 Protección de la Información del Registro	Se deben proteger con acceso no autorizado y negación de manipulación de la información en las instalaciones/infraestructura del registro.	C	Se ha verificado la presencia de la herramienta de Directorio Activo en el sistema. Además, se observa que la segregación por perfil de usuario impide la modificación de registros y/o archivos de información, lo que fortalece la seguridad y la integridad de los

			datos almacenados en el sistema.
A.12.4.3 Registros del Administrador y Operador	Se deben registrar, proteger y revisar los eventos de las actividades del administrador y del operador de sistemas.	C	Se ha constatado la presencia de la herramienta de Directorio Activo en el sistema. Además, se observa que la segregación por perfil de usuario impide la modificación de registros y/o archivos de información. Se destaca que únicamente el área de Operaciones cuenta con permisos de administración, lo que garantiza un control adecuado sobre los cambios realizados en el sistema y fortalece la seguridad de la información.

Tabla 129 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.12.4.4 Sincronización del reloj	Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de la organización o dominio de seguridad deben	C	Se ha identificado el uso del protocolo NTP (Network Time Protocol) a través del servidor Cronos

	estar sincronizados con una sola fuente de tiempo de referencia.		ubicado en el Centro Nacional de Metrología (CENAM), específicamente en la dirección 1.cronos.cenam.mx.
--	--	--	---

Tabla 130 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.12.5 Control del Software Operacional	Garantizar la integridad de los sistemas operacionales.		
A.12.5.1 Instalación de Software en Sistemas Operacionales	Se deben implementar procedimientos para controlar la instalación de software en sistemas operacionales.	C	Se ha detectado que únicamente el área de operaciones posee privilegios de administración, lo que les otorga la capacidad de instalar software y aplicaciones en los sistemas. Además, se dispone de un listado de software permitido, y cualquier adición a este listado debe ser previamente autorizada por la Dirección General.
A.12.6 Gestión de Vulnerabilidades Técnicas	Prevenir la explotación de vulnerabilidades técnicas.		

Tabla 131 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.12.6.1 Gestión de Vulnerabilidades Técnicas	Se debe obtener información acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados de manera oportuna, evaluar la exposición de la organización a tales vulnerabilidades y tomar medidas apropiadas para tratar los riesgos asociados.	C	Se ha constatado que se llevan a cabo análisis de vulnerabilidades de manera anual en el sistema. Se proporciona información sobre el análisis de vulnerabilidades correspondiente al año 2023, el cual arrojó un total de 40 hallazgos críticos y 15 hallazgos informativos.
A.12.6.2 Restricciones en la Instalación de Software	Se debe establecer e implementar reglas que gobiernen la instalación de software por los usuarios.	C	Se ha detectado que únicamente el área de operaciones posee privilegios de administración, lo que les otorga la capacidad de instalar software y aplicaciones en los sistemas. Además, se dispone de un listado de software permitido, y cualquier adición a este listado debe ser previamente autorizada

			por la Dirección General.
--	--	--	---------------------------

Tabla 132 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.12.7 Consideraciones de Auditoría a Sistemas de Información	Minimizar el impacto de las actividades de la auditoría en los sistemas operacionales.		
A.12.7.1 Controles de Auditoría a los Sistemas de Información	Los requisitos de la auditoría y las actividades que implican la verificación de los sistemas operacionales deben planearse y acordarse cuidadosamente para minimizar las interrupciones a los procesos del negocio.	C	Se ha observado que la organización lleva a cabo auditorías periódicas a la Base de Datos de Gestión de Configuración (CMDB), así como análisis de vulnerabilidades y auditorías de registros.
A.13 SEGURIDAD EN LAS COMUNICACIONES			
A.13.1 Gestión de Seguridad en la Red	Garantizar la protección de la información en las redes e infraestructura de apoyo para el procesamiento de información.	C	Se cuenta con una Po_Firewall_V01 fechado el día 13 de marzo del 23, así como se utiliza el Directorio activo para acceder a los servicios bajo perfiles establecidos.

Tabla 133 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.13.1.1 Controles de Red	Las redes deben gestionarse y controlarse para proteger la información en los sistemas y aplicaciones.	C	La organización ha implementado una segregación de redes dentro de su infraestructura.
A.13.1.2 Seguridad en los Servicios de Red	Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión para todos los servicios de la red deben identificarse e incluirse en los acuerdos de servicios de red, ya sea que estos servicios sean provistos internamente o se sub contraten.	C	Se cuenta con una Po_Firewall_V01 fechado el día 13 de marzo del 23, así como se utiliza el Directorio activo para acceder a los servicios bajo perfiles establecidos.
A.13.1.3 Segregación en Redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes.	C	Se ha identifica un diagrama de red que muestra claramente la segregación de redes, así como la infraestructura del Centro de Operaciones de Seguridad (SOC-NOC) y la red de usuarios de SAYNET.
A.13.2 Transferencia de Información	Mantener la seguridad de la información transferida dentro de una organización		

	y con cualquier entidad externa.		
--	----------------------------------	--	--

Tabla 134 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.13.2.1 Políticas y Procedimientos de Transferencia de Información	Deben existir políticas formales de transferencia, procedimientos y controles para proteger la transferencia de información a través del uso de cualquier tipo de medio de comunicación.	NC	Se ha identificado la existencia de una Po_Convenios de confidencialidad, cifrado de seguridad con contraseñas, 7ZIP, VPN_V01 del 11 de julio del 2023. Esta política no aborda los aspectos necesarios para proteger la transferencia de información adecuada. Se requiere una revisión exhaustiva para desarrollar e implementar políticas y procedimientos adicionales que cumplan plenamente con este requisito y aseguren la seguridad de las comunicaciones de la organización.

Tabla 135 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.13.2.2 Acuerdos de Transferencia de Información	Los acuerdos deben abordar la transferencia segura de la información del negocio entre la organización y partes externas.	C	Se muestra evidencia del contrato con EFD que incluye la cláusula 14 Confidencialidad y privacidad de datos firmado de aceptación. Se muestra contrato con Hospital Satélite, incluye cláusula de confidencialidad y no divulgación, privacidad de datos y acuerdos de transferencia de información, el contrato está firmado.
A.13.2.3 Mensajería Electrónica	La información involucrada en mensajes electrónicos debe estar protegida apropiadamente.	C	Se cuenta con una Po_Convenios de confidencialidad, cifrado de seguridad mediante uso de contraseñas, 7ZIP, VPN_V01 fechada el día 11 de julio del 2023.
A.13.2.4 Acuerdos de Confidencialidad o no Divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación reflejando las	C	Se muestra evidencia del contrato con EFD que incluye la cláusula 14 Confidencialidad y privacidad de datos firmado de aceptación.

	necesidades de la organización para la protección de la información.		Se muestra contrato con Hospital Satélite, incluye cláusula de confidencialidad y no divulgación, privacidad de datos y acuerdos de transferencia de información, el contrato está firmado.
--	--	--	---

Tabla 136 (Continuación)

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.14.1 Requisitos de Seguridad para los Sistemas de Información	Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios sobre redes públicas.		
A.14.1.1 Análisis y Especificación de Requisitos de Seguridad	Los requisitos relacionados con la seguridad de la información deben estar incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	C	atencion@noc-soc-horus.com.mx Mediante una minuta para validar la viabilidad de los requisitos

Tabla 137 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.14.1.2 Servicios de Aplicaciones Seguras en Redes Públicas	La información involucrada en servicios de aplicaciones que pasan sobre redes públicas debe estar protegida de actividades fraudulentas, disputas contractuales y exposición no autorizada y modificación.	C	Se cuenta con una Po_Convenios de confidencialidad, cifrado de seguridad mediante uso de contraseñas, 7ZIP, VPN_V01 fechada el día 11 de julio del 2023.
A.14.1.3 Protección de Aplicaciones de Servicios de Transacciones	La información involucrada en transacciones de servicios de aplicación debe estar protegida para prevenir transmisión incompleta, errores de enrutamiento, alteración de mensajes no autorizados, divulgación no autorizada, duplicación del mensaje no autorizado o reproducción.	C	Se cuenta con una Po_Convenios de confidencialidad, cifrado de seguridad mediante uso de contraseñas, 7ZIP, VPN_V01 fechada el día 11 de julio del 2023.
A.14.2 Seguridad en Desarrollo y Procesos de Soporte	Garantizar que la seguridad de la información se diseña e implementa en el ciclo de vida del desarrollo de los sistemas de información.		

Tabla 138 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.14.2.1 Política de Desarrollo Seguro	Deben establecerse y aplicarse reglas para el	C	Se cuenta con una Po_Desarrollo

	desarrollo de software y sistemas en los desarrollos dentro de la organización.		seguro_V01 fechada el día 7 de julio del 2023, sin embargo, la organización no desarrolla software.
A.14.2.2 Procedimientos de Control de Cambios a Sistemas	Los cambios a los sistemas dentro del ciclo de vida del desarrollo deben controlarse mediante el uso de procedimientos formales de control de cambios.	C	Se cuenta con una Po_Desarrollo seguro_V01 fechada el día 7 de julio del 2023, sin embargo, la organización no desarrolla software.
A.14.2.3 Revisión Técnica de Aplicaciones después de Cambios en la Plataforma de Operación	Cuando cambian las plataformas operativas, las aplicaciones críticas del negocio deben revisarse y probarse para garantizar que no hay un impacto adverso en las operaciones de la organización o en la seguridad.	C	Se cuenta con una Po_Desarrollo seguro_V01 fechada el día 7 de julio del 2023, sin embargo, la organización no desarrolla software.
A.14.2.4 Restricciones a los Cambios en los Paquetes de Software	Se deben disuadir las modificaciones a los paquetes de software, limitar a los cambios necesarios y todos los cambios deben estar estrictamente controlados.	C	Se cuenta con una Po_Desarrollo seguro_V01 fechada el día 7 de julio del 2023, sin embargo, la organización no desarrolla software.

Tabla 139 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.14.2.5 Principios de Ingeniería en Sistemas Seguros	Se deben establecer, documentar, mantener y aplicar principios de ingeniería para sistemas seguros a cualquier esfuerzo de implementación de sistemas de información.	C	Se cuenta con una Po_Desarrollo seguro_V01 fechada el día 7 de julio del 2023, sin embargo, la organización no desarrolla software.
A.14.2.6 Entorno de Desarrollo Seguro	Las organizaciones deben establecer y proteger apropiadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubran todo el ciclo de vida del desarrollo del sistema.	C	Se cuenta con una Po_Desarrollo seguro_V01 fechada el día 7 de julio del 2023, sin embargo, la organización no desarrolla software.
A.14.2.7 Desarrollo de Sistemas Subcontratado (Outsourcing)	La organización debe supervisar y monitorear la actividad del desarrollo de sistemas subcontratados (outsourcing).	C	Se cuenta con una Po_Desarrollo seguro_V01 fechada el día 7 de julio del 2023, sin embargo, la organización no desarrolla software.
A.14.2.8 Pruebas de Seguridad a los Sistemas	Se deben llevar a cabo pruebas de la funcionalidad de seguridad durante el desarrollo.	C	Se cuenta con una Po_Desarrollo seguro_V01 fechada el día 7 de julio del 2023, sin embargo, la organización no desarrolla software.

Tabla 140 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.14.2.9 Pruebas de Aceptación a los Sistemas	Se deben establecer programas de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones.	C	Se cuenta con una Po_Desarrollo seguro_V01 fechada el día 7 de julio del 2023, sin embargo, la organización no desarrolla software.
A.14.3 Datos de Prueba	Garantizar la protección de los datos usados para las pruebas.		
A.14.3.1 Protección de Datos de Prueba	Los datos de prueba deben seleccionarse, protegerse y controlarse cuidadosamente.	C	Se cuenta con una Po_Desarrollo seguro_V01 fechada el día 7 de julio del 2023, sin embargo, la organización no desarrolla software.
A.15 RELACIÓN CON PROVEEDORES			
A.15.1 Seguridad de la Información en Relación con Proveedores	Garantizar la protección de los activos de la organización que sea accesible por los proveedores.		

Tabla 141 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.15.1.1 Política de Seguridad de la Información para la Relación con Proveedores	Se deben acordar con los proveedores y documentarse los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso de proveedores a los activos de la organización.	C	Se ha identificado un Pr_Gestión de compras y proveedores_V01, actualizado el 28 de junio de 2023. Este proceso incluye la gestión de disputas contractuales. Se ha asignado la responsabilidad de gestionar proveedores externos. Dentro de este proceso, se destaca la sección 2.4.5.3 relacionada con la base de datos de proveedores. Esta base de datos contiene información detallada sobre cada proveedor, incluyendo datos de identificación y contacto. Además, se lleva a cabo un control de documentos que deben formar parte del expediente de cada proveedor, como el CIF, el acta constitutiva, comprobantes de
---	--	---	---

			domicilio, entre otros. Hasta la fecha de la documentación, se han registrado un total de 39 proveedores en la base de datos.
--	--	--	---

Tabla 142 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.15.1.2 Abordar la Seguridad dentro de los Acuerdos con Proveedores	Todos los requisitos de seguridad de la información relevantes deben establecerse y acordarse con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar componentes de la infraestructura de TI de la información de la organización.	C	En la base de datos de proveedores (2.4.5.3), se registran los datos de identificación y contacto de cada proveedor, así como un control de documentos que deben estar incluidos en su expediente. Para fortalecer la gestión de seguridad de la información con respecto a los proveedores, se propone evaluar riesgos para identificar vulnerabilidades en sus sistemas y prácticas de seguridad. Además, se sugiere la inclusión de criterios de seguridad en

			el proceso de evaluación de proveedores, la implementación de medidas de mitigación de riesgos y el establecimiento de un seguimiento continuo de su efectividad. Finalmente, se plantea llevar a cabo una campaña de sensibilización para concientizar a los empleados sobre la importancia de la seguridad de la información en las relaciones con los proveedores.
--	--	--	--

Tabla 143 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.15.1.3 Cadena de Suministro en Tecnologías de la Información y Comunicaciones	Los acuerdos con proveedores deben incluir los requisitos para tratar los riesgos de seguridad de la información asociados con la información y los servicios de tecnología de las comunicaciones y la cadena de suministro de productos.	C	En la base de datos de proveedores (2.4.5.3) se almacenan los datos de identificación y contacto de cada proveedor, así como los documentos necesarios para su expediente, como el CIF, el acta constitutiva y comprobantes de domicilio, entre otros. Aunque se establecen contratos con los proveedores y se difunden las políticas de seguridad de la información a través de una lista de distribución, se identifica una carencia significativa: la ausencia de abordaje de los riesgos de seguridad asociados con los proveedores. Esta omisión es débil en la gestión de seguridad de la información de la organización, subrayando la
---	---	---	---

			necesidad de implementar estrategias para evaluar y mitigar tales riesgos para proteger los activos de información.
--	--	--	---

Tabla 144 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.15.2 Administración de Entrega de Servicios de Proveedores	Mantener un nivel acordado de seguridad de la información y la entrega de servicios alineados con los acuerdos de proveedores.		
A.15.2.1 Monitoreo y Revisión de los Servicios de Proveedores	Las organizaciones deben monitorear, revisar y auditar regularmente la entrega del servicio de Proveedores	OB	El Pr_Gestión de compras y proveedores_V01, actualizado el 28 de junio de 2023, incluye disputas contractuales. Responsable de gestionar proveedores externos. 2.4.5.3 base de datos proveedores: proveedor datos de identificación, datos de contacto, control de documentos que debe integrar su expediente (CIF, ACTA, REFORMAS, COMPROBANTE DE

		DOMICILIO, ETC.) se tienen 39 proveedores. Contrato con proveedores Evaluación de proveedores. Se muestra 2.4.5.4 evaluación de proveedores 1er sem. Se identifican 17 proveedores evaluados de los 39 que están en la lista. Se comenta que únicamente se evaluaron a los proveedores a los que se les hizo una compra. Se comunican políticas de SI mediante lista de distribución de envío de políticas de seguridad a proveedores. No se identifica la trazabilidad entre evaluación de proveedores y base de datos de proveedores, ya que no se indica en la base de datos que proveedores están
--	--	---

			activos, se declara que solo se trabajó con 17 pero en la base de datos dice que con todos se tiene un contrato.
--	--	--	--

Tabla 145 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.15.2.2 Gestión de Cambios a los Servicios de Proveedores	Los cambios en la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, deben ser administrados, tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y la revaloración de los riesgos.	C	El cambio de proveedores es gestionado mediante el Pr_Gestión de compras y proveedores_V01, actualizado el 28 de junio de 2023.
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
A.16.1 Gestión de Incidentes d Seguridad de la Información y Mejoras	Garantizar un enfoque consistente y eficaz para la administración de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.		

Tabla 146 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.16.1.1 Responsabilidades y Procedimientos	Se deben establecer responsabilidades y procedimientos de gestión para garantizar una rápida, eficaz y ordenada respuesta a los incidentes de seguridad de la información.	C	La organización cuenta con un Pr_Incidentes de seguridad de la información_V01 fechado el 9 de junio del 2023.
A.16.1.2 Reporte de Eventos de Seguridad de la Información	Los eventos de seguridad de la información deben reportarse a través de canales de gestión apropiados tan rápido como sea posible.	C	Durante el año 2023, no se han reportado incidentes de seguridad de la información en la organización.
A.16.1.3 Reporte de Debilidades de Seguridad de la Información	Se debe exigir a los empleados y contratistas que utilizan los sistemas y servicios de información de la organización anotar e informar cualquier debilidad de seguridad de la información observada o sospechosa en los sistemas y servicios.	C	Durante el año 2023, no se han reportado incidentes de seguridad de la información en la organización.

Tabla 147 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.16.1.4 Evaluación y Decisión sobre Eventos de Seguridad de la Información	Los eventos de seguridad de la información deben evaluarse y se debe decidir si son clasificados como	C	Durante el año 2023, no se han reportado incidentes de seguridad de la información en la organización.

	incidentes de seguridad de la información.		
A.16.1.5 Respuesta a Incidentes de Seguridad de la Información	Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.	C	Durante el año 2023, no se han reportado incidentes de seguridad de la información en la organización.
A.16.1.6 Aprendizaje de Incidentes de Seguridad de la Información	El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de futuros incidentes.	C	Durante el año 2023, no se han reportado incidentes de seguridad de la información en la organización.
A.16.1.7 Recopilación de Evidencia	La organización debe definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de la información que puede servir como evidencia.	C	Durante el año 2023, no se han reportado incidentes de seguridad de la información en la organización.
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO			

Tabla 148 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.17.1 Continuidad de la Seguridad de la Información	Se debe integrar la continuidad de la seguridad de la información en los sistemas de gestión de		

	continuidad del negocio de la organización.		
A.17.1.1 Planeación de la Continuidad de la Seguridad de la Información	La organización debe determinar sus requisitos de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	C	Se muestra el Fo_Plan de continuidad y disponibilidad_V01 fechado 2 de mayo del 2023 (corte de energía eléctrica, corte de comunicaciones, indisponibilidad de instalaciones, ausentismo, emergencia sanitaria, política o social).
A.17.1.2 Implementando la Continuidad de la Seguridad de la Información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.	C	Se muestra el Fo_Plan de continuidad y disponibilidad_V01 fechado 2 de mayo del 2023 (corte de energía eléctrica, corte de comunicaciones, indisponibilidad de instalaciones, ausentismo, emergencia sanitaria, política o social) Los planes de continuidad y disponibilidad son probados al menos una vez al año (septiembre y

		octubre). Se muestra informe de pruebas al plan de continuidad realizados en septiembre, fueron exitositas la pruebas.
--	--	--

Tabla 149 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.17.1.3 Verificación, revisión y evaluación de la Continuidad de la Seguridad de la Información	La organización debe verificar los controles de continuidad de seguridad de la información establecidos e implementados a intervalos regulares con el objetivo de garantizar que son válidos y eficaces durante situaciones adversas.	NC	Se presenta el Fo_Plan de continuidad y disponibilidad_V01 fechado el 2 de mayo de 2023, que aborda situaciones como corte de energía eléctrica, corte de comunicaciones, indisponibilidad de instalaciones, ausentismo, emergencia sanitaria, política o social. Aunque los planes de continuidad y disponibilidad se prueban anualmente en septiembre y octubre, con informes exitosos de pruebas realizadas en septiembre, el incumplimiento radica en la falta de

			verificación regular de los controles de continuidad de seguridad de la información.
--	--	--	--

Tabla 150 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.17.2 Redundancias	Garantizar la disponibilidad de las instalaciones de procesamiento de la información.		
A.17.2.1 Disponibilidad de las Instalaciones de Procesamiento de la Información	Las instalaciones de procesamiento de la información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.	C	Se muestra Re_Diagrama de red fechado 3 abril del 2023 en el que se identifica la redundancia con la que cuenta la organización para los servicios. (enlaces perimetrales, swiches)
A.18 CUMPLIMIENTO			
A.18.1 Cumplimiento con Requisitos Legales y Contractuales			

Tabla 151 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.18.1.1 Identificación de la Legislación Aplicable y Requisitos Contractuales	Todos los requisitos legislativos, regulatorios, contractuales relevantes y el enfoque de la organización	NC	Se muestra la Re_Matriz de cumplimiento fechado el día 24 de marzo del

	para cumplir con estos requisitos deben estar explícitamente identificados, documentados y mantenerse actualizados para cada sistema de información y la organización.		2023 donde identifica los requisitos normativos/ requisitos, fuente, evidencia, revisiones semestrales y observaciones. Sin embargo no refleja de manera completa y actualizada todos los requisitos normativos pertinentes.
A.18.1.2 Derechos de Propiedad Intelectual	Se deben implementar procedimientos apropiados para garantizar el cumplimiento con los requisitos legislativos, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentado.	C	La organización dispone de software licenciado y establece cláusulas de propiedad intelectual en sus contratos. Esta medida garantiza la protección adecuada de los activos intangibles de la empresa y promueve el cumplimiento de las regulaciones pertinentes en materia de propiedad intelectual.

Tabla 152 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
----------------------	-------------------	--------	----------

A.18.1.3 Protección de Registros	Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legales, regulatorios, contractuales y de negocios.	C	Los registros son almacenados de manera segura durante un período de 10 años, conforme a los protocolos y controles de seguridad de la información establecidos por la organización.
A.18.1.4 Privacidad y Protección de Información de Identificación Personal	Se debe asegurar la privacidad y protección de la información de identificación personal conforme sea requerido en la legislación y regulación relevante aplicable.	C	Se cuenta con una Fo_Aviso de privacidad_V01 integral de la organización, el cual está disponible en la página web de la empresa y se entrega al inicio de la relación laboral de los colaboradores, además de mencionarse en los contratos con clientes. Se identifica que la última actualización del Fo_Aviso de privacidad_V01 mostrado en la página es del 12 de enero de 2023, y el aviso de privacidad mostrado y

		firmado por el colaborador Daniel Olvera García tiene fecha de entrada en vigor el 12 de junio de 2023, sin presentar fecha de última actualización en el cuerpo del aviso, lo que constituye una inconsistencia. Dado esto, se confirma que la organización ya ha implementado la homologación de los avisos de privacidad, asegurando la coherencia entre todas las versiones disponibles. Esta acción garantiza que toda la información proporcionada a colaboradores y clientes sea actualizada y consistente, cumpliendo con las regulaciones de protección de datos y manteniendo la transparencia en las
--	--	--

			prácticas de privacidad de la empresa.
--	--	--	--

Tabla 153 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.18.1.5 Regulación de Controles Criptográficos	Los controles criptográficos deben ser usados en cumplimiento con todos los acuerdos, legislación y regulaciones relevantes.	C	Se solicita por contrato el envío de información cifrada con contraseña (7Zip).
A.18.2 Revisión de Seguridad de la Información	Garantizar que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos de la organización.		
A.18.2.1 Revisión Independiente de la Seguridad de la Información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) deben ser revisados	C	Los mantenimientos de equipos se llevan a cabo de manera semestral, durante los cuales se verifica el cumplimiento y la implementación de los controles de seguridad de la información correspondientes.

	independientemente a intervalos planeados o cuando se ocurran cambios significativos.		
--	---	--	--

Tabla 154 (Continuación)

Referencia normativa	Aspecto a evaluar	Calif.	Hallazgo
A.18.2.2 Cumplimiento con Políticas y Normas de Seguridad	Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y procedimientos dentro de su área de responsabilidad con las políticas de seguridad apropiadas, normas y cualquier otro requisito de seguridad.	C	El comité de SGI tiene las atribuciones, obligaciones y restricciones para elaborar, revisar y cumplir las políticas de seguridad de la información y solicitar el cumplimiento a los colaboradores de la organización.
A.18.2.3 Inspección de Cumplimiento Técnico	Los sistemas de información deben ser revisados regularmente para su cumplimiento con las políticas y normas de seguridad de la información de la organización.	C	Se realizan análisis de vulnerabilidades de manera anual. Se muestra análisis de vulnerabilidades 2023 (40 y 15 hallazgos informativos).

3.2.1.4 Actividad 2.4 Realizar pruebas con base en la información recabada en las entrevistas y la revisión documental, llevando a cabo un análisis más detallado al incumplimiento de los requisitos y/o controles.

Implica llevar a cabo el análisis o evaluaciones sistemáticas para verificar la funcionalidad o validez. Esto puede incluir pruebas de productos, software, procedimientos o hipótesis, entre otros aspectos, con el fin de obtener datos que respalden decisiones o mejoras.

3.2.1.4.1 Descripción de la actividad

Implica llevar a cabo evaluaciones con el propósito de verificar la validez este proceso implica la definición clara de objetivos de prueba, la recopilación de datos, el análisis de resultados y la interpretación de los hallazgos. Las pruebas abarcan una amplia gama de áreas. Dependiendo del contexto, las pruebas pueden ser cruciales para validar la calidad, seguridad del sistema antes de su implementación. Con los hallazgos identificados con OB (Observación) y NC (No conformidad) se revisa y analiza con mayor detalle la evidencia presentada como políticas, procedimientos, registros, anexo, manuales y se documenta en el formato de pruebas el cual incluye el objetivo de la prueba, descripción, técnica, requisito o control, interpretación de los hallazgos y breve recomendación de remediación.

3.2.1.4.2 Resultado de la actividad

Tabla 155 Prueba partes interesadas

3.2.1.4.2.1 Prueba: Partes interesadas		
Objetivo de prueba		Evaluar el grado de documentación de las partes interesadas dentro del sistema de gestión de la organización
Descripción de la prueba		Se lleva a cabo entrevistas con miembros clave del equipo del sistema de gestión y otros empleados relevantes para determinar su comprensión y conocimiento de las partes interesadas. Se examina el Ma_Sistema de Gestión Integrado (SGI)_V01 en el cual se indicó la referencia al control referente a partes interesadas
Técnica		Entrevistas, observaciones, revisión de la información documentada, resumen de datos, análisis e indicadores de desempeño.
Requisito Control	/	4.2 Comprensión de las necesidades y expectativas de las partes interesadas

Calificación del hallazgo

NC

Hallazgo

No se encuentra documentadas las partes interesadas, los colaboradores saben la información necesaria para el cumplimiento de necesidades y expectativas, cuentan únicamente con la matriz de partes interesadas en el Ma_Sistema de Gestión Integrado (SGI)_V01

Interpretación de resultados

Se muestra el Ma_Sistema de Gestión Integrado (SGI)_V01 el cual es de carácter interno en su versión 1 publicada el 31 de julio del 2023



Figura 4 Portada manual de sistema de gestión integral

En la página 19 del manual que costa de 23 páginas se ubican las tablas de correspondiente a las necesidades y expectativas de las partes interesadas, así como los responsables, indicadores de satisfacción y evaluación, pero estos se encuentran sin información para la organización

MANUAL DEL SISTEMA DE GESTIÓN INTEGRAL

Clasificación: Interno
Versión: 01
Fecha de última revisión:
31-07-23

COMUNICACIÓN

A fin de comunicar la información del SGI que es de interés para las partes interesadas, la Dirección General determina la siguiente matriz de comunicación:

PARTE INTERESADA	NECESIDADES	EXPECTATIVAS
Nombre de la parte interesada		
Nombre de la parte interesada		
Nombre de la parte interesada		
Nombre de la parte interesada		
Nombre de la parte interesada		

SATISFACCIÓN

Parte interesada	Necesidad	Responsable	Indicador de satisfacción	Evaluación
Nombre de la parte interesada				

Figura 5 Formato de partes interesadas en el manual de sistema de gestión integral

Recomendaciones

Crear un registro formal de partes interesadas que incluya información detallada sobre cada una, como sus necesidades, expectativas, etc.

Tabla 156 Prueba contacto con autoridades

3.2.1.4.2.2 Prueba: Contacto con autoridades

Objetivo de prueba	Verificar la existencia y adecuada documentación de la matriz de contacto con autoridades
Descripción de la prueba	Solicitar copia de la matriz de contacto con autoridades Analizar la documentación proporcionada para verificar si la matriz está correctamente completada. Verificar si la matriz incluye información actualizada y precisa de las autoridades pertinentes
Técnica	Entrevistas, observaciones, revisión de la información documentada, resumen de datos, análisis e indicadores de desempeño.
Requisito / Control	A.6.1.3 Contacto con Autoridad
Calificación del hallazgo	OB
Hallazgo	Se muestra el "Re_Matriz contacto autoridades_2023" actualizado el 23 de agosto del 2023 en el cual solo se incluyen a los grupos de interés especiales.
Interpretación de resultados	Se muestra el documento “Re_Matriz contacto autoridades_2023”. El documento solo cuenta con 2 pestañas la portada del documento llamada Control de documentos y la matriz de grupos de interés  Figura 6 Pestañas del registro matriz contacto autoridades Se muestra la portada del documento la cual solo cuenta con el nombre del documento, clasificación, fecha de última actualización y a que corresponde la última versión generada, en este caso es un documento de nueva creación generado el 23/08/2023.

	A	B	C	D	E	F	G	H		
1	Clasificación:	Interno	Matriz de contacto con autoridades							
2	Fecha de última revisión:	23/08/2023								
3										
4	Matriz de contacto con autoridades									
5										
6									Control de cambios	
7	Versión	Fecha	Descripción							
8	1	23/08/2023	Documento de nueva creación							

Figura 7 Portada del registro matriz de contacto con autoridades

En la pestaña de grupos de interés muestra la clasificación del documento, fecha de última actualización, título del documento y como grupos de interés se muestra únicamente a OWASP, UNAM-CERT, SANS y Alienvault OTX

	A	B	C	D	E
1	Clasificación:	Interno	Matriz de contacto con autoridades especiales		
2	Fecha de última revisión:	23/08/2023			
3					
4	A fin de comunicar la información del SGI que es de interés para las partes interesadas, la Dirección General determina la siguiente matriz				
5					
6	Tema	Audiencia ¿A quién comunicar?	Medio(s)	Periodo de difusión	Responsable(s)
7	¿Qué comunicar?		¿Cómo comunicar?	¿Cuándo comunicar?	¿Quién comunica?
8	Seguridad de las aplicaciones web.	OWASP	Correo	Petición del área de desarrollo	Gestor de operaciones
9	Prácticas de seguridad en el desarrollo de software				
10	Identificación y mitigación de vulnerabilidades en aplicaciones web				
11	Respuesta a incidentes de seguridad informática	UNAM-CERT	Correo	Evento	Gestor de incidentes
12	Técnicas de detección y respuesta a incidentes				
13	Formación y certificaciones en el campo de la seguridad informática.	SANS	Correo	Evento	Responsable de seguridad de la información
14	Seguridad informática				Gestor de incidentes
15	Gestión de incidentes				Responsable de seguridad de la información
16	Ciberseguridad industrial	Alienvault OTX	Correo	Petición de algún área	Gestor de amenazas
17	Información sobre amenazas y ciberinteligencia.				
18	Análisis de amenazas				
19	Mitigación de amenazas cibernéticas				

Figura 8 Matriz de contactos de grupos especiales

Recomendaciones

Actualizar y completar la matriz de contacto con autoridades con la información más reciente y precisa.

Establecer un proceso claro y periódico para la revisión y actualización de la matriz.

Tabla 157 Prueba seguridad en los proyectos

3.2.1.4.2.3 Prueba: Seguridad en los proyectos		
Objetivo de prueba		Evaluar el cumplimiento de los procesos de gestión de riesgos en los proyectos de la organización, identificando si se documentan de manera adecuada y exhaustiva los riesgos asociados a cada proyecto.
Descripción de la prueba		Se revisará la documentación del proyecto "Fo_Implementación de servicio_V04" para verificar si se han identificado y abordado adecuadamente los riesgos, especialmente relacionados con el endpoint para infonavit. También se examinará el proyecto "Re_plan de trabajo Instalación de memorias RAM y discos duros en servidores" para determinar si se han identificado los riesgos asociados con la instalación de hardware en servidores y si se han propuesto medidas para mitigarlos.
Técnica		Entrevistas, observaciones, revisión de la información documentada, resumen de datos, análisis e indicadores de desempeño.
Requisito Control	/	A.6.1.5 Seguridad de la Información en la Administración de Proyectos
Calificación del hallazgo		OB
Hallazgo		Se muestra el "Fo_Implementación de servicio_V04" actualizado el 25 de mayo del 2023 el cual considera endpoint para infonavit, en el documento se aprecia que se consideran los riesgos del proyecto. Se muestra evidencia del proyecto "Re_plan de trabajo_Instalación de memorias RAM y discos duros en servidores" generado el 31 de octubre del 2023, En este caso, la documentación carece de la identificación de riesgos asociados al proyecto, lo cual constituye una deficiencia que requiere atención y corrección inmediata. Es esencial que la organización considere los riesgos en todos sus proyectos, tanto internos como externos. La gestión proactiva de riesgos es fundamental para anticipar obstáculos, tomar medidas preventivas y asegurar el éxito de los proyectos.

Interpretación de resultados

Se muestra el Fo_Implementación de servicio_V04 el cual es de carácter interno en su versión 4 publicada el 25 de mayo del 2023

Clasificación:	Interno	Evaluación de nuevos proyectos															
Fecha de última revisión:	25/05/2023																
Evaluación de nuevos proyectos																	
Control de cambios <table><thead><tr><th>Versión</th><th>Fecha</th><th>Descripción</th></tr></thead><tbody><tr><td>1</td><td>24/08/2020</td><td>Documento de nueva creación</td></tr><tr><td>2</td><td>19/07/2021</td><td>Revisión de idoneidad</td></tr><tr><td>3</td><td>14/05/2022</td><td>Revisión de idoneidad</td></tr><tr><td>4</td><td>25/05/2023</td><td>Revisión de idoneidad</td></tr></tbody></table>			Versión	Fecha	Descripción	1	24/08/2020	Documento de nueva creación	2	19/07/2021	Revisión de idoneidad	3	14/05/2022	Revisión de idoneidad	4	25/05/2023	Revisión de idoneidad
Versión	Fecha	Descripción															
1	24/08/2020	Documento de nueva creación															
2	19/07/2021	Revisión de idoneidad															
3	14/05/2022	Revisión de idoneidad															
4	25/05/2023	Revisión de idoneidad															

Figura 9 Portada del formato evaluación de nuevos proyectos

La evaluación del proyecto únicamente identifica la definición del proyecto (Nombre y objetivos), actividades a realizar y el resultado y no se identifican los riesgos que el nuevo proyecto implica.

Tabla 158 Prueba derechos ARCO

3.2.1.4.2.4 Prueba: Derechos ARCO		
Objetivo de prueba	de	Evaluar el cumplimiento de los procesos de seguridad de la información y la gestión de recursos humanos en relación con la baja y cambio de puesto de Gabriel Arcega Soto en la organización. Se busca determinar si se han seguido los protocolos establecidos para la desvinculación de un colaborador, incluyendo la comunicación de

		responsabilidades de seguridad de la información y los derechos de ARCO.
Descripción de la prueba		Revisar minuciosamente la documentación relacionada con la baja y cambio de puesto de Gabriel Arcega Soto. Se verificará la integridad del expediente de baja y la documentación respaldatoria del cambio de puesto. Se buscará evidencia de la comunicación de responsabilidades de seguridad de la información y el respeto a los derechos de ARCO. El objetivo es identificar posibles fallos en los procesos y proponer mejoras.
Técnica		Entrevistas, observaciones, revisión de la información documentada, resumen de datos, análisis e indicadores de desempeño.
Requisito Control	/	A.7.3.1 Responsabilidades en la terminación o cambio de empleo
Calificación del hallazgo		OB
Hallazgo		Se evidencia la baja de Gabriel Arcega Soto, documentada con la conformación del expediente de baja, el cual incluye diversos elementos como renuncia, baja del biométrico, solicitud de baja de activos, accesos físicos y lógicos, carta de asignación y devolución de activos, y aviso de privacidad. Asimismo, se presenta evidencia del cambio de puesto de Gabriel Arcega Soto, respaldado por la minuta de aprobación del cambio y el perfil de puestos firmado por la parte involucrada generados el 25 de octubre de 2023. Sin embargo, no se encontró evidencia de que la organización haya comunicado y/o recordado las responsabilidades de Seguridad de la Información que permanecen vigentes, ni los derechos de ARCO (Acceso, Rectificación, Cancelación y Oposición) respecto a la desvinculación de los colaboradores.
Interpretación de resultados		Se muestra la carta de renuncia emitida por Gabriel Arcega Soto dirigida a la organización y firmada

A quien corresponda:

Por medio de la presente carta, me dirijo a usted para presentar formalmente mi renuncia al puesto. Esta decisión no ha sido fácil de tomar, pero después de una reflexión cuidadosa y consideración de mis objetivos profesionales y personales, he llegado a la conclusión de que es el momento adecuado para embarcarme en una nueva etapa en mi carrera.

Quiero expresar mi sincero agradecimiento por la oportunidad que me ha brindado de crecer y desarrollarme profesionalmente durante mi tiempo aquí. He disfrutado trabajando con mis colegas y contribuyendo al éxito de la empresa en la medida de mis capacidades.

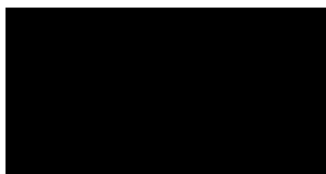
Me comprometo a trabajar estrechamente con usted y mi equipo durante mi período de preaviso para garantizar una transición sin problemas y completar cualquier tarea pendiente. Estoy dispuesto a colaborar en la búsqueda y formación de mi reemplazo, así como a facilitar cualquier proceso necesario para asegurar la continuidad operativa.

Mi último día de trabajo será de acuerdo con el período de preaviso establecido en mi contrato de trabajo. Durante este tiempo, estaré disponible para ayudar en la medida de mis capacidades para asegurar una transición fluida.

Aprecio profundamente la oportunidad de haber formado parte de la Empresa y estoy agradecido por la experiencia y el aprendizaje que he adquirido aquí. Espero que podamos mantenernos en contacto y deseo lo mejor para el futuro de la empresa.

Quedo a su disposición para cualquier consulta adicional y agradezco su comprensión y apoyo en este proceso de transición.

Atentamente,



Gabriel Arcega Soto

Figura 11 Carta de renuncia de Gabriel Arcega Soto

Se muestra la solicitud de la baja del biométrico para Gabriel Arcega Soto firmada por el departamento de recursos humanos

Solicitud de baja de biométrico

25 de octubre del 2023

Estimado [REDACTED]

Por la presente, me dirijo a usted en mi calidad de representante del Departamento de Recursos Humanos, con el propósito de solicitar formalmente la baja del registro biométrico de un empleado bajo su supervisión.

El empleado en cuestión es el **Sr. Gabriel Arcega Soto**, quien ha finalizado la relación laboral con SayNet Soluciones Integrales S.A. de C.V.

Solicitaríamos amablemente que procediera con la eliminación de los datos biométricos del **Sr. Arcega Soto** de todos los sistemas y registros bajo su responsabilidad.

Agradecemos su atención a esta solicitud y cualquier asistencia que pueda brindar para garantizar una transición sin contratiempos.

Quedo a su disposición para proporcionar cualquier información adicional que pueda necesitar.

Atentamente,

A large black rectangular redaction box covering the signature area of the letter.

Figura 12 Solicitud de baja del biométrico de Gabriel Arcega Soto

Se muestra la solicitud de baja de activos, accesos físicos y lógicos correspondientes a la baja de Gabriel Arcega Soto firmada por el responsable de recursos humanos

Solicitud de baja de activos físicos y lógicos

Estimado [REDACTED]

Por la presente, me dirijo a usted en calidad de representante del Departamento de Recursos Humanos, con el propósito de solicitar formalmente la baja de activos de un empleado bajo su supervisión.

El empleado en cuestión es el Sr. Gabriel Arcega Soto, quien ha cesado sus funciones en nuestra empresa y, como resultado, requiere la devolución y baja de los activos que le fueron asignados durante su empleo.

Solicitamos amablemente que proceda con la recopilación de los siguientes activos:

- Laptop
- Teléfono móvil
- Teclado y ratón
- Auriculares
- Dispositivo de almacenamiento externo
- Tarjeta de acceso físico
- Tarjeta de acceso lógico
- Documentos físicos
- Tarjeta de identificación de empleado

Asimismo, requerimos que se desactive cualquier acceso físico o lógico asociado con la cuenta del Sr. Arcega Soto a nuestras instalaciones y sistemas, asegurando así la protección de los activos de la empresa.

Agradecemos su pronta atención a esta solicitud y cualquier asistencia que pueda brindar para garantizar una transición sin contratiempos.

Quedo a su disposición para proporcionar cualquier información adicional que pueda necesitar.

Atentamente,

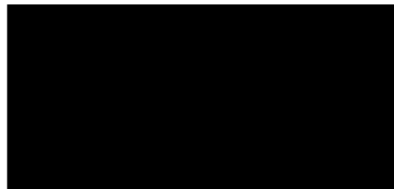
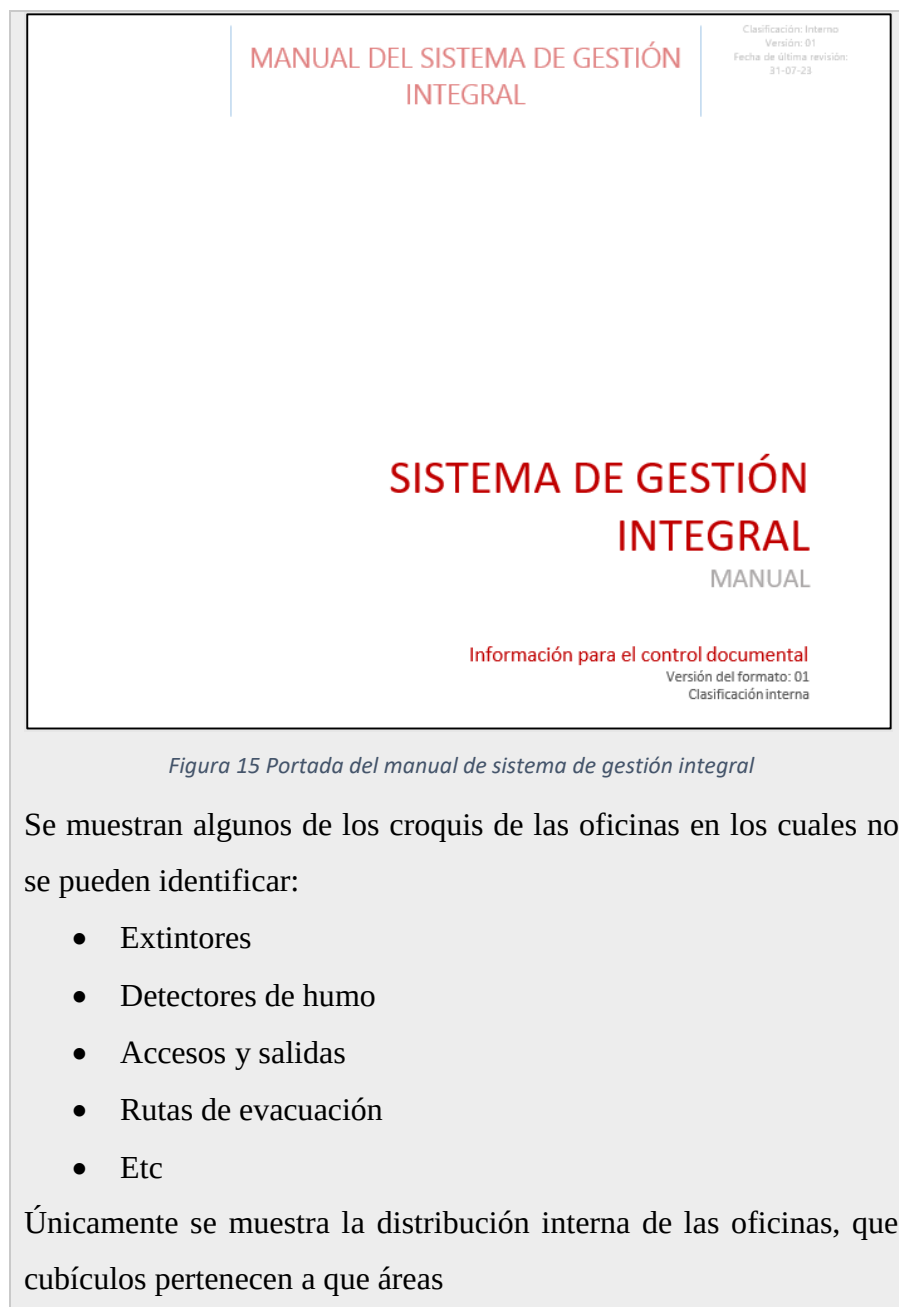


Figura 13 Solicitud de baja de activos físicos y lógicos de Gabriel Arcega Soto

Se muestra el aviso de privacidad el cual especifica las finalidades primarias y secundarias, así como la información a recopilada, con quien se comparte la información personal (se solicita un consentimiento de transferencia de datos), uso de tecnologías de rastreo, como limitarlas y donde se publican los cambios al aviso de privacidad.

Tabla 159 Prueba croquis de la organización

3.2.1.4.2.5 Prueba: Croquis de la organización		
Objetivo de prueba		Verificar la presencia y ubicación de controles de seguridad físicos en el croquis proporcionado
Descripción de la prueba		Se realizará una inspección física del lugar, comparando las ubicaciones especificadas en el croquis con lo que se encuentra realmente en el sitio. Se registrarán todas las discrepancias encontradas, incluyendo la ausencia de controles, ubicaciones incorrectas o cualquier otra inconsistencia identificada durante la inspección.
Técnica		Entrevistas, observaciones, revisión de la información documentada, resumen de datos, análisis e indicadores de desempeño.
Requisito Control	/	A.11.1.1 Perímetro de Seguridad Física
Calificación del hallazgo		NC
Hallazgo		Se muestra el Ma_Seguridad de la organización_V01 fechado el 25 de mayo del 2023 pero no se identifican los controles implementados.
Interpretación de resultados		Se muestra el Ma_Sistema de Gestión Integrado (SGI)_V01 el cual es de carácter interno en su versión 1 publicada el 31 de julio del 2023



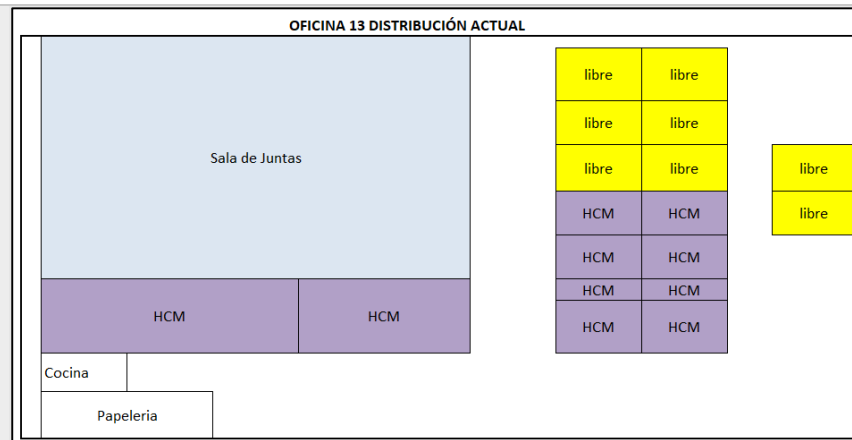


Figura 16 Croquis oficina 13

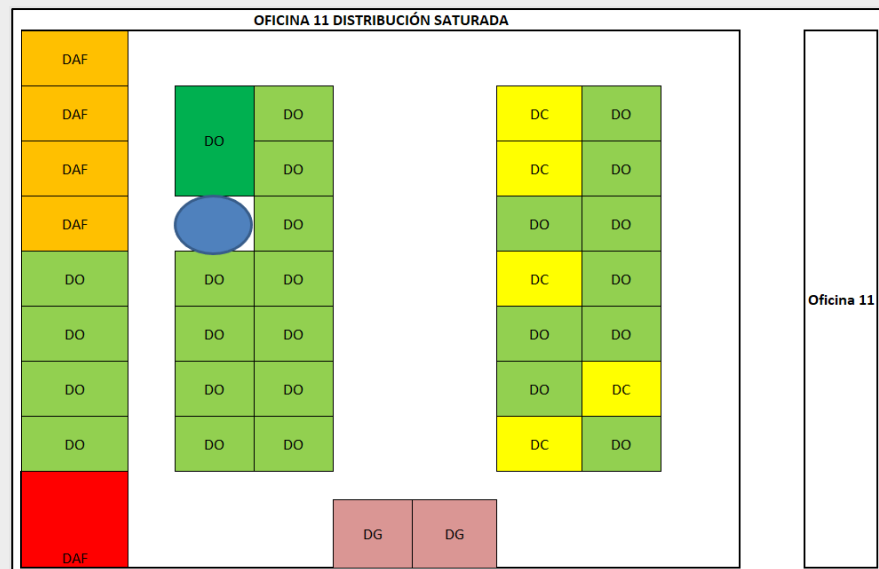


Figura 17 Croquis oficina 11

Recomendaciones

Identificar los controles de seguridad
 Actualizar el croquis con los controles identificados

Tabla 160 Prueba gestión del cambio

3.2.1.4.2.6 Prueba: Gestión del cambio	
Objetivo de prueba	Verificar si se cumplen los criterios de impacto configurados en la herramienta de gestión del cambio (Aranda) con respecto a los tipos de cambio estándar, normal y emergente.
Descripción de la prueba	Evaluar la conformidad del Procedimiento Gestión del cambio_V01 fechado el 19 de mayo del 2023 y la implementación de requisitos

		de cambio sin cambios internos adicionales. Se revisará el Re_Caso no. 63 / CHG8268-1-63 del 17 de marzo del 2023 por Saul Gomez de la Secretaría de Turismo para documentar adecuadamente los requisitos. Se verificará la coherencia de los criterios de impacto establecidos con la configuración de la herramienta de gestión del cambio (Aranda).
Técnica		Entrevistas, observaciones, revisión de la información documentada, resumen de datos, análisis e indicadores de desempeño.
Requisito Control	/	A.12.1.2 Gestión del Cambio
Calificación del hallazgo		OB
Hallazgo		Se cuenta con un Pr_Gestión del cambio_V01 fechado el 19 de mayo del 2023 que incluye los elementos solicitados por el requisito. Tipos de cambio: estándar, normal y emergente No ha habido cambios internos. Se muestra Aranda, herramienta utilizada para gestionar los cambios a la infraestructura o los cambios en los servicios. Se muestra Re_Caso no. 63 / CHG8268-1-63 fechado el 17 de marzo del 2023 por Saul Gomez del cliente Secretaría de Turismo, se observa debidamente requisitos a la solicitud de cambio, misma que se anexa al caso creado. En Criterios de impacto: en la tabla de tipos de cambio se describen los impactos sin embargo no existe un criterio que sea compatible con lo configurado en la herramienta de Aranda.
Interpretación de resultados		Se muestra el Pr_Gestion del cambio el cual es de carácter interno en su versión 1 En la página 1 y 2 del procedimiento que costa de 3 páginas se muestra un registro formal de un cambio solicitado, identificado como "GC-002", el cual fue solicitado por Saul Gomez de la Secretaría de Turismo. Este cambio implica la revisión del caso no.

63 / CHG8268-1-63, fechado el 17 de marzo de 2023. Se observa que se han proporcionado requisitos adicionales para la solicitud de cambio, los cuales están adjuntos al caso creado.

En la sección de Criterios de Impacto se destaca que en la tabla de tipos de cambio se describen los impactos, pero se señala que no existe un criterio que sea compatible con la configuración en la herramienta de Aranda. Esto sugiere que los criterios establecidos en la tabla no abordan completamente la compatibilidad con la herramienta utilizada para gestionar los cambios en la infraestructura o los servicios. Este hallazgo resalta la necesidad de revisar y ajustar los criterios de impacto para garantizar que aborden adecuadamente las consideraciones relacionadas con la herramienta de Aranda y otros sistemas relevantes.

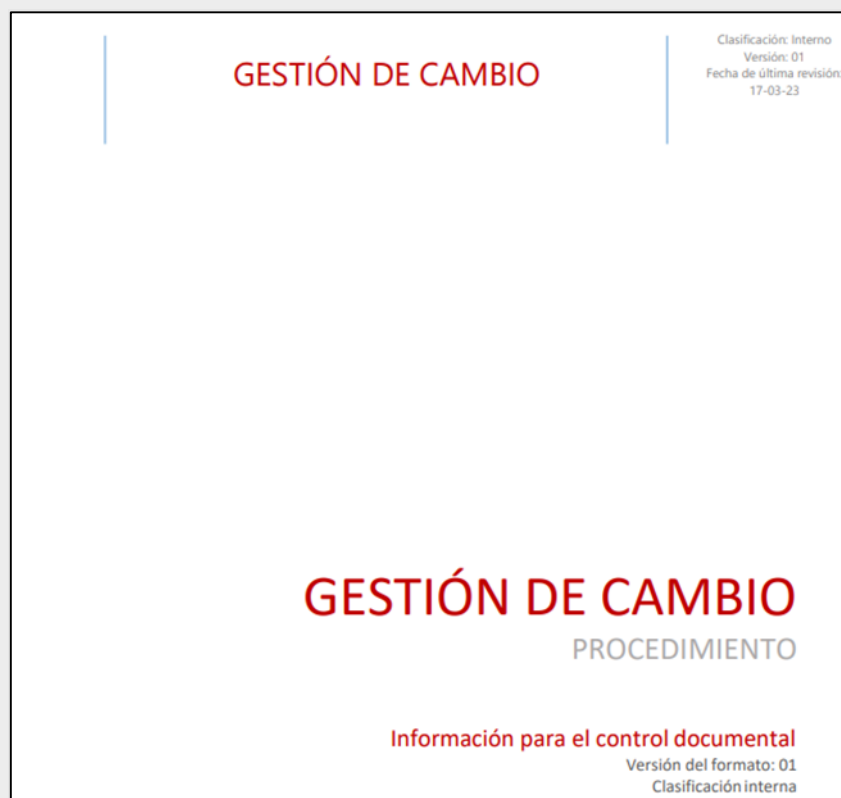


Figura 18 Portada del procedimiento gestión del cambio

GESTIÓN DE CAMBIO		Clasificación: Interno Versión: 01 Fecha de última revisión: 17-03-23
1. Información del Cambio: Número de Cambio: GC-002 Fecha de Solicitud: 17 de marzo de 2023 Solicitante: Saul Gómez (Secretaría de Turismo) Descripción del Cambio: Revisión del caso no. 63 / CHG8268-1-63 y análisis de requisitos adicionales para la solicitud de cambio.		
2. Justificación del Cambio: Razón del Cambio: Se requiere identificar y abordar los requisitos adicionales especificados en el caso no. 63 para garantizar la correcta implementación del cambio. Beneficios Esperados: Garantizar que la solicitud de cambio se cumpla de manera adecuada, evitando posibles conflictos y asegurando la satisfacción del cliente.		
3. Evaluación de Impacto: Criterios de Impacto: La solicitud de cambio está vinculada con la configuración de la herramienta de Aranda. Se debe garantizar que los requisitos adicionales sean compatibles con la configuración existente. Impacto del Cambio: La falta de compatibilidad con la configuración de Aranda podría resultar en dificultades para gestionar el cambio de manera efectiva y en posibles interrupciones en los servicios. Compatibilidad con la Herramienta de Aranda: Se observa que los requisitos adicionales especificados en el caso no. 63 deben ser evaluados cuidadosamente para garantizar su compatibilidad con la herramienta de Aranda.		

Figura 19 Información principal del cambio

4. Plan de Implementación: Fecha de Implementación Propuesta: 25 de marzo de 2023 Recursos Necesarios: Personal técnico para revisar los requisitos adicionales y ajustar la configuración de la herramienta de Aranda si es necesario. Procedimiento de Implementación: Revisión detallada de los requisitos adicionales especificados en el caso no. 63 y ajuste de la configuración de Aranda según sea necesario para garantizar la compatibilidad.	
5. Riesgos y Mitigaciones: Riesgos Asociados: Posibles conflictos con la configuración existente de Aranda, interrupciones en los servicios si no se abordan adecuadamente los requisitos adicionales. Estrategias de Mitigación: Realizar pruebas exhaustivas antes de implementar los cambios en la configuración de Aranda, comunicar cualquier interrupción planificada a los usuarios afectados.	
6. Aprobación del Cambio: Responsable de Aprobación: [Nombre del responsable de gestión de cambios] Fecha de Aprobación: [Fecha de aprobación] Observaciones: Pendiente de aprobación una vez que se revise la evaluación de impacto y el plan de implementación.	
7. Implementación del Cambio: Responsable de Implementación: [Nombre del responsable de implementación] Fecha de Implementación: [Fecha de implementación] Resultados de la Implementación: Los resultados de la implementación se registrarán una vez que se complete	

Figura 20 Plan de implementación

GESTIÓN DE CAMBIO		Clasificación: Interno Versión: 01 Fecha de última revisión: 17-03-23
el proceso.		
8. Seguimiento y Evaluación Post-Implementación: Revisión de Efectividad: Se realizará una revisión posterior a la implementación para asegurar que los requisitos adicionales se hayan abordado correctamente y que la herramienta de Aranda siga funcionando sin problemas. Lecciones Aprendidas: Se documentarán las lecciones aprendidas durante todo el proceso de gestión de cambios para mejorar los procedimientos en el futuro.		

Figura 21 Seguimiento y la evaluación que se llevara a cabo

Recomendaciones	Registro de Criterios de Impacto: Incluir una sección en el formato de gestión de cambio para registrar los criterios de impacto. Mantener este registro actualizado. Revisión de Documentación de Criterios de Impacto: Establecer un proceso para revisar regularmente la documentación de criterios de impacto. Asignar responsables para mantenerla actualizada y programar revisiones formales.
------------------------	--

Tabla 161 Prueba respaldos

3.2.1.4.2.7 Prueba: Respaldos	
Objetivo de prueba	Realizar una evaluación de los procedimientos de respaldo de datos para garantizar su eficacia y cumplimiento.
Descripción de la prueba	Verificar la efectividad y el cumplimiento de los procedimientos establecidos para la realización de respaldos de datos. Se realizará a través de entrevistas, observaciones y revisión de documentación para garantizar que se sigan los procedimientos adecuados y se respalden todas las plataformas críticas identificadas. Se buscarán posibles brechas o deficiencias para asegurar la integridad y disponibilidad de los datos respaldados.
Técnica	Entrevistas, observaciones, revisión de la información documentada, resumen de datos, análisis e indicadores de desempeño.
Requisito Control	/ A.12.3.1 Respaldos de la Información
Calificación del hallazgo	NC
Hallazgo	Se muestra una Re_Bitácora de respaldos fechada el día 8 de febrero del 2023, en la cual se identifica la realización de respaldos completos e incrementales para (ofimática, PRTG, Firewall, switch). Sin embargo, al revisar la bitácora detalladamente, se encuentra que no se ha registrado la realización de respaldos para ninguna de las plataformas mencionadas. Esta omisión representa un

Interpretación de resultados

incumplimiento de los procedimientos establecidos para la realización de respaldos de datos, lo que podría generar riesgos significativos para la integridad y disponibilidad de la información de la organización.

Por lo tanto, es necesario revisar y reforzar los procedimientos de respaldo de datos para garantizar que se realicen de manera adecuada y se registren correctamente en la bitácora correspondiente.

Se muestra el Re_Bitacora del cambio el cual es de carácter interno. Dentro de la bitácora se muestra la fecha de la revisión del procedimiento de los datos, así como también se muestra una tabla donde se identificaron las deficiencias de las plataformas, así como las observaciones de estas deficiencias y por último muestra el responsable de revisión y reforzamiento de los respaldos.

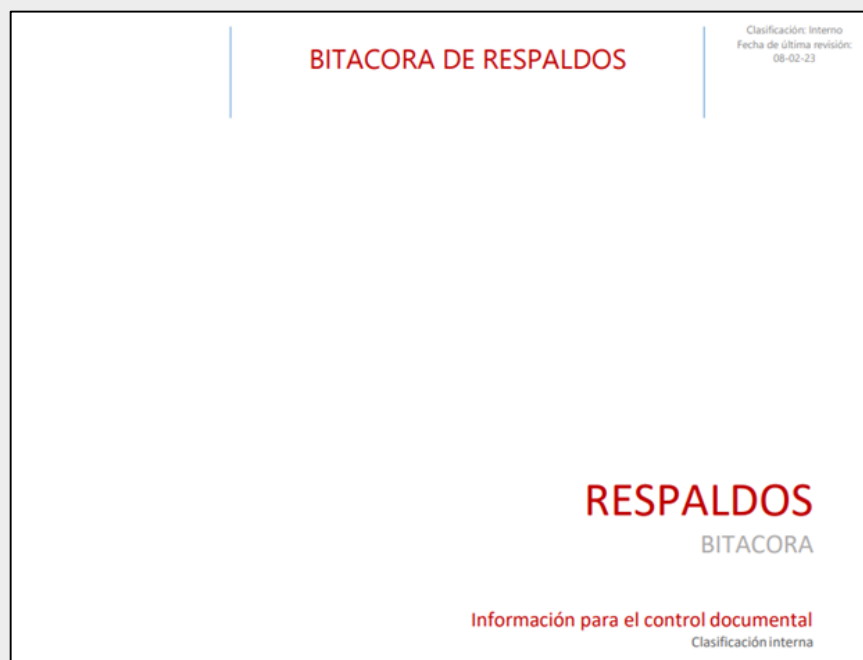


Figura 22 Portada de la bitácora de respaldos

Figura 22 Bitácora de respaldos

2. Responsable de la revisión y reforzamiento de los procedimientos de respaldo de datos:

Nombre del responsable: [REDACTED]
Título/ posición: [REDACTED]
Fecha: 8 de febrero del 2023

Figura 23 Datos de respaldo

Recomendaciones

Mantener los procedimientos de respaldo al día, asegurando que incluyan todas las plataformas críticas y estén fácilmente accesibles para el personal relevante. Principio del formulario

Programar sesiones de capacitación regular para garantizar que el equipo comprenda la importancia de seguir los procedimientos de respaldo y mantener registros precisos.

Tabla 162 Prueba Transferencia de datos

3.2.1.4.2.8 Prueba: Transferencia de datos		
Objetivo de prueba		Evaluar la efectividad de los controles implementados para proteger la transferencia de información sensible dentro de la organización.
Descripción de la prueba		Se llevará a cabo una evaluación exhaustiva de los procedimientos y controles establecidos para la transferencia de información

		confidencial dentro de la empresa. Esto incluirá la revisión de políticas y procedimientos documentados, así como la observación de las prácticas de transferencia de información en la práctica.
Técnica		Entrevistas, observaciones, revisión de la información documentada, resumen de datos, análisis e indicadores de desempeño.
Requisito	/	A.13.2.1 Políticas y Procedimientos de Transferencia de Información
Control		
Calificación del hallazgo		NC
Hallazgo		Se dispone de una Po_Convenios de Confidencialidad_V01, fechada el día 11 de julio de 2023. Sin embargo, no se cuenta con controles adecuados para proteger la transferencia de información.
Interpretación de resultados		Se muestra el Po_Convenio de confidencialidad el cual es de carácter interno en su versión 1 Dentro de la política muestra como objetivo principal establecer un marco integral para proteger la información confidencial de Saynet, abarcando todos los aspectos relacionados con su manejo, transmisión y almacenamiento. Aplica a quienes tengan acceso a información sensible de la empresa, y subraya la importancia de salvaguardar la integridad, confidencialidad y disponibilidad de dicha información siempre.



Figura 24 Portada de Política convenio de confidencialidad

POLÍTICA CONVENIO DE CONFIDENCIALIDAD		Clasificación: Interno Versión: 01 Fecha de última revisión: 11-07-23
ÍNDICE		
01. OBJETIVO Y CAMPO DE APLICACIÓN.....	1	
02. DEFINICIÓN DE INFORMACIÓN CONFIDENCIAL.....	1	
03. CLASIFICACIÓN DE LA INFORMACIÓN.....	1	
04. MEDIDAS DE SEGURIDAD PARA LA TRANSFERENCIA DE INFORMACIÓN.....	1	
05. RECOMENDACIONES GENERALES.....	1	
06. RIESGOS Y SANCIONES	2	

Figura 25 Índice de Política convenio de confidencialidad

POLÍTICA CONVENIO DE CONFIDENCIALIDAD

Clasificación: Interno
Versión: 01
Fecha de última revisión:
11-07-23

01. OBJETIVO Y CAMPO DE APLICACIÓN

El propósito fundamental de esta política es establecer un marco integral para proteger la información confidencial de Saynet, salvaguardando su integridad, confidencialidad y disponibilidad. Esta política se aplica a todos los empleados, contratistas, proveedores y terceros que, de alguna manera, tengan acceso a información sensible perteneciente a la empresa.

02. DEFINICIÓN DE INFORMACIÓN CONFIDENCIAL

Se define como información confidencial cualquier dato, documento o material que, por su naturaleza, no está destinado al público en general y cuya divulgación no autorizada podría tener repercusiones adversas en los intereses comerciales, la reputación o la seguridad de la organización. Esto puede incluir, entre otros, datos financieros, estratégicos, de clientes, de empleados, y cualquier otro tipo de información sensible para la empresa.

03. CLASIFICACIÓN DE LA INFORMACIÓN

La información confidencial será clasificada en distintos niveles de sensibilidad, considerando tanto su contenido como el potencial impacto que su divulgación no autorizada podría ocasionar. Esta clasificación permitirá aplicar medidas de protección proporcionales a la importancia de la información, estableciendo criterios claros para la identificación, manejo y almacenamiento de cada tipo de dato confidencial.

Figura 26 Descripción de información confidencial en distintos niveles.

03. CLASIFICACIÓN DE LA INFORMACIÓN

La información confidencial será clasificada en distintos niveles de sensibilidad, considerando tanto su contenido como el potencial impacto que su divulgación no autorizada podría ocasionar. Esta clasificación permitirá aplicar medidas de protección proporcionales a la importancia de la información, estableciendo criterios claros para la identificación, manejo y almacenamiento de cada tipo de dato confidencial.

04. MEDIDAS DE SEGURIDAD PARA LA TRANSFERENCIA DE INFORMACIÓN

Reconociendo la necesidad imperativa de garantizar la seguridad en la transferencia de información, se implementarán medidas adicionales para proteger la confidencialidad de los datos durante su transmisión. Entre estas medidas se incluyen el establecimiento de protocolos de encriptación robustos, la aplicación de sistemas de autenticación de usuarios para verificar la identidad de los destinatarios autorizados, así como la realización periódica de capacitaciones para el personal en materia de políticas y procedimientos de seguridad de la información.

Además, se promoverá el uso de herramientas tecnológicas avanzadas que permitan monitorear y controlar el flujo de información confidencial dentro y fuera de la organización, detectando y mitigando posibles amenazas a la seguridad de los datos.

05. RECOMENDACIONES GENERALES

Además de las medidas específicas de seguridad, se proporcionarán recomendaciones generales para el manejo seguro de la información confidencial. Estas recomendaciones incluirán pautas sobre la creación y gestión de contraseñas seguras, la protección física de los dispositivos que almacenen información sensible, y la importancia de verificar la autenticidad de los destinatarios antes de compartir cualquier dato confidencial.

Figura 27 Información confidencial en distintos niveles.

POLÍTICA CONVENIO DE CONFIDENCIALIDAD

Clasificación: Interno
Versión: 01
Fecha de última revisión:
11-07-23

06. RIESGOS Y SANCIONES

Se llevará a cabo una evaluación exhaustiva de los riesgos asociados con la divulgación no autorizada de información confidencial, y se establecerán las sanciones correspondientes para aquellos individuos que incumplan con esta política. Estas sanciones pueden incluir medidas disciplinarias internas, así como acciones legales en casos de infracciones graves que puedan comprometer la seguridad y la reputación de la empresa.

Figura 28 Riesgos y sanciones

Recomendaciones	Actualizar y fortalecer los controles de transferencia de información para garantizar su seguridad y confidencialidad. Revisar la política de convenios de confidencialidad y proporcionar capacitación al personal sobre los procedimientos adecuados para la transferencia segura de información
------------------------	--

Tabla 163 Prueba transferencia de información

3.2.1.4.2.9 Prueba: Seguridad de la información	
Objetivo de prueba	Evaluar la efectividad del plan de continuidad y disponibilidad de la organización en garantizar la operatividad frente a situaciones adversas, como cortes de energía, comunicaciones e indisponibilidad de instalaciones.
Descripción de la prueba	Verificar la efectividad y vigencia del plan de continuidad y disponibilidad de la organización en situaciones adversas. Se emplearon diversas técnicas, como entrevistas con el equipo responsable, observaciones de procesos, revisión exhaustiva de la documentación relacionada, resumen de datos relevantes y análisis de indicadores de desempeño. Estos métodos se aplicaron de manera integral para obtener una visión completa de la implementación y el estado del plan, permitiendo identificar tanto fortalezas como posibles áreas de mejora.
Técnica	Entrevistas, observaciones, revisión de la información documentada, resumen de datos, análisis e indicadores de desempeño.
Requisito Control	/ A.17.1.3 Verificación, revisión y evaluación de la Continuidad de la Seguridad de la Información
Calificación del hallazgo	NC
Hallazgo	Se presenta el Fo_Plan de continuidad y disponibilidad_V01 fechado el 2 de mayo de 2023, que aborda situaciones como corte de energía eléctrica, corte de comunicaciones, indisponibilidad de instalaciones, ausentismo, emergencia sanitaria, política o social. Aunque los

Interpretación de resultados

planes de continuidad y disponibilidad se prueban anualmente en septiembre y octubre, con informes exitosos de pruebas realizadas en septiembre, el incumplimiento radica en la falta de verificación regular de los controles de continuidad de seguridad de la información.

Se muestra el Fo_Plan de continuidad y disponibilidad el cual es de carácter interno en su versión 1.

Dentro del plan de continuidad, establece los procedimientos y recursos necesarios para garantizar la operatividad de la organización ante diversas situaciones adversas, como cortes de energía, comunicaciones, indisponibilidad de instalaciones, entre otros. Define roles y responsabilidades dentro del equipo de gestión de crisis, así como acciones específicas para la recuperación de infraestructura, comunicación con stakeholders y la realización de pruebas periódicas para mantener la efectividad del plan. Su objetivo es minimizar el impacto de interrupciones en las operaciones comerciales y asegurar la disponibilidad de servicios críticos en todo momento.

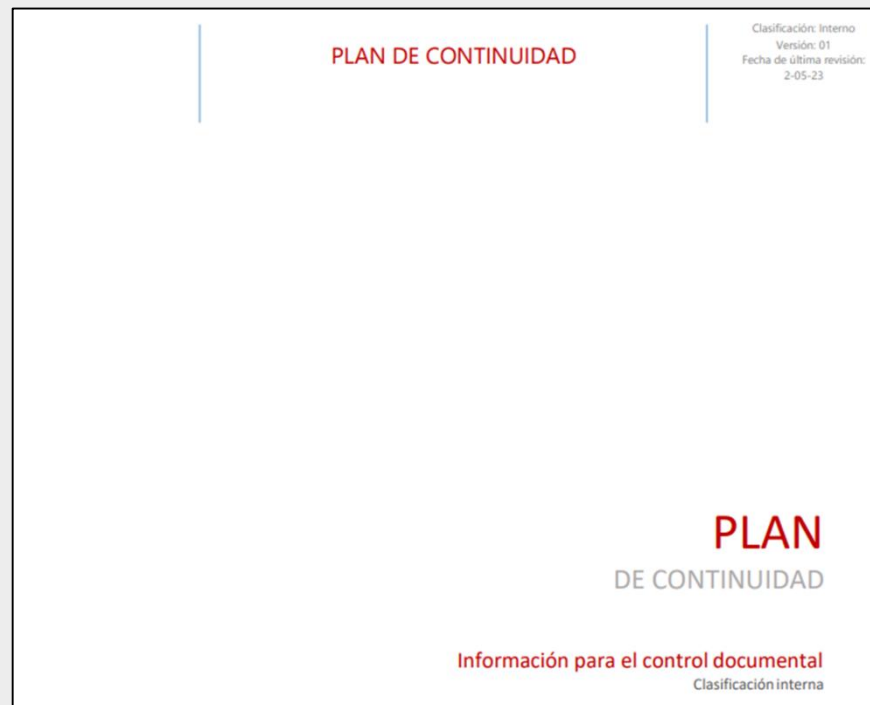


Figura 29 Portada del plan de continuidad

PLAN DE CONTINUIDAD		Clasificación: Interno Versión: 01 Fecha de última revisión: 2-05-23
Nombre del Plan: Plan de Continuidad y Disponibilidad (Fo_Plan_V01)		
Fecha de Emisión: 2 de mayo de 2023		
Situaciones Abordadas:		
• Corte de energía eléctrica • Corte de comunicaciones • Indisponibilidad de instalaciones • Ausentismo • Emergencia sanitaria • Situaciones políticas o sociales		
Procedimientos de Prueba Anual:		
Las pruebas de continuidad y disponibilidad se realizan anualmente en septiembre y octubre. Informes exitosos de pruebas realizadas en septiembre.		
Áreas de Incumplimiento:		
Falta de verificación regular de los controles de continuidad de seguridad de la información, según lo requerido por el estándar.		
Objetivos del Plan:		
Garantizar la continuidad de las operaciones comerciales en situaciones adversas o de emergencia. Minimizar el impacto de interrupciones en la disponibilidad de servicios críticos.		
Equipo de Gestión de Crisis:		
• Nombre: [REDACTED] • Rol y Responsabilidades: director TI • Nombre: [REDACTED] • Rol y Responsabilidades: Líder de recursos humanos • Nombre: [REDACTED]		

Figura 30 Plan de continuidad

Procedimientos de respuesta:
1. Corte de energía eléctrica: Activar generadores de respaldo. Priorizar el uso de energía para equipos esenciales.
2. Corte de comunicaciones: Utilizar sistemas de comunicación alternativos (p. ej., radios, dispositivos móviles).
3. Indisponibilidad de instalaciones: Redirigir operaciones a ubicaciones alternativas si es necesario.
4. Ausentismo: Implementar planes de contingencia para redistribuir tareas y asegurar la continuidad de funciones críticas.
5. Emergencia sanitaria: Seguir las pautas y recomendaciones de las autoridades de salud. Implementar medidas de higiene y distanciamiento social.
6. Situaciones políticas o sociales: Monitorear de cerca la situación y tomar decisiones basadas en la seguridad del personal y la continuidad de las operaciones.

Figura 31 Procedimientos de respuesta

Recomendaciones	PLAN DE CONTINUIDAD Clasificación: Interno Versión: 01 Fecha de última revisión: 2-05-23 Recuperación de Infraestructura: Establecer un plan detallado para la rápida recuperación de la infraestructura física y tecnológica en caso de interrupciones. Planes de Comunicación: Desarrollar planes de comunicación interna y externa para mantener informadas a todas las partes interesadas durante una crisis. Pruebas y Ejercicios de Simulación: Programar pruebas y ejercicios de simulación regulares para evaluar la efectividad del plan y entrenar al personal en su implementación. Actualización Continua: Revisar y actualizar el plan de manera regular para reflejar cambios en el entorno operativo, la tecnología y los riesgos comerciales. Formación y Concienciación: Proporcionar formación y concienciación al personal sobre los procedimientos de respuesta a emergencias y la importancia de la continuidad del negocio. Aprobado por: [Redacted] Fecha de aprobación: 2-may-2024 Este Plan de Continuidad y Disponibilidad será revisado anual/ente y actualizado según sea necesario para garantizar su efectividad y relevancia continua.
	<i>Figura 32 Plan de continuidad</i> Se recomienda establecer un proceso formal para la verificación regular de los controles de continuidad de seguridad de la información, que incluya la realización periódica de pruebas y la actualización continua del plan de continuidad y disponibilidad. Además, se sugiere proporcionar formación al personal y designar responsables para asegurar la implementación efectiva de estas medidas.

Tabla 164 Prueba Requisitos contractuales

3.2.1.4.2.10 Prueba: Requisitos contractuales	
Objetivo de prueba	Verificar el cumplimiento de los requisitos contractuales y legales por parte de la organización.
Descripción de la prueba	Examinar el grado de identificación y cumplimiento de la legislación aplicable y los requisitos contractuales por parte de la organización. Se utilizaron diversas técnicas, como entrevistas con personal relevante, observación de procesos, revisión minuciosa de la información documentada, resumen de datos relevantes, análisis de

Técnica Requisito Control Calificación del hallazgo Hallazgo Interpretación de resultados		indicadores de desempeño y cualquier otro método pertinente para obtener una comprensión integral del cumplimiento de los requisitos
		Entrevistas, observaciones, revisión de la información documentada, resumen de datos, análisis e indicadores de desempeño.
	/	A.18.1.1 Identificación de la Legislación Aplicable y Requisitos Contractuales
		NC
		Se muestra la Re_Matriz de cumplimiento fechado el día 24 de marzo del 2023 donde identifica los requisitos normativos/ requisitos, fuente, evidencia, revisiones semestrales y observaciones, sin embargo, no refleja de manera completa y actualizada todos los requisitos normativos pertinentes.
		Se muestra el Re_Matriz de cumplimiento el cual es de carácter interno. Dentro de la matriz se muestra una estructura organizada que sistematiza los requisitos normativos y las medidas implementadas para su cumplimiento. En ella, se detallan las fuentes de los requisitos, la evidencia correspondiente que respalda el cumplimiento, así como las fechas de las revisiones semestrales programadas. Esta matriz sirve como una herramienta central para monitorear el estado de conformidad con los estándares normativos relevantes. Además, proporciona un marco de referencia para identificar áreas de mejora y abordar posibles no conformidades.

The image shows the front cover of a document titled 'MATRÍZ DE CUMPLIMIENTO'. The cover is white with a light blue header bar at the top. In the top right corner of the header, the text 'Clasificación: interna' and 'Fecha de última revisión: 24-03-23' is printed in a small, dark font. The main title 'MATRÍZ DE CUMPLIMIENTO' is centered on the page in a large, bold, dark blue font. Below the title, there is a subtitle 'Información para el control documental' in a smaller, bold, dark blue font. At the bottom right of the cover, the text 'Clasificación interna' is printed in a small, dark font. The cover is framed by a thin black border.

MATRIZ DE CUMPLIMIENTO				
MATRIZ DE CUMPLIMIENTO			VERSIÓN: 01	
REQUISITOS NORMATIVOS/REQUISITOS	FUENTE	EVIDENCIA	REVISIONES SEMESTRALES	OBSERVACIONES
ISO 27001	Norma ISO 27001	Certificación ISO 27001 vigente	Junio, Diciembre	Cumplimiento adecuado
Ley de Protección de Datos Personales	Legislación Nacional	Política de Privacidad de Datos, Registro de Consentimientos	Marzo, Septiembre	Pendiente de revisión y actualización
Regulación de Ciberseguridad	Entidad Reguladora	Informes de Auditoría de Seguridad	Abril, Octubre	Cumplimiento adecuado
Normativa Laboral	Ministerio de Trabajo	Políticas de Recursos Humanos, Contratos Laborales	Febrero, Agosto	Cumplimiento adecuado
Estándares de Seguridad de la Información	Ministerio de Trabajo	Procedimientos de Auditoría Interna, Planes de Seguridad	Mayo, Noviembre	Evidencia incompleta de actualización

Recomendaciones	Actualizar y completar la Re_Matriz de cumplimiento para reflejar de manera precisa y actualizada todos los requisitos normativos pertinentes, así como establecer un proceso de revisión regular para garantizar su vigencia. Además, se podría sugerir mejorar los procedimientos de identificación y seguimiento de los requisitos contractuales y legales para evitar futuras discrepancias.
------------------------	---

3.2.1.5 Actividad 2.5 Generar recomendaciones para abordar y remediar los hallazgos identificados durante la auditoría que no cumplan o cumplan parcialmente con los requisitos y controles predefinidos.

Consiste en proponer recomendaciones específicas para corregir los hallazgos encontrados durante la auditoría que no cumplen o cumplen parcialmente con los requisitos y controles auditados.

3.2.1.5.1 Descripción de la actividad

Para abordar y remediar los hallazgos identificados durante la auditoría que no cumplan o cumplan parcialmente con los requisitos y controles predefinidos, se considera la evaluación de cada hallazgo identificado durante la auditoría para comprender completamente su naturaleza y la razón por la cual no cumple con los requisitos o controles establecidos.

Detectando cuales son las carencias de la evidencia presentada para obtener la conformidad se general las recomendaciones específicas y factibles para abordar cada hallazgo identificado. Estas recomendaciones deben ser claras, accionables y orientadas a resolver las causas subyacentes y mejorar el cumplimiento con los requisitos y controles.

3.2.1.5.2 Resultado de la actividad

3.2.1.5.2.1 Recomendaciones de remediaciones

Tabla 165 Remediación de hallazgos

Requisito	Descripción	Hallazgo	Acciones de remediación
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Por su efecto o efecto potencial en la capacidad de la organización de proporcionar productos y servicios que satisfagan los requisitos del cliente y los legales	No se encuentra documentadas las partes interesadas, los colaboradores saben la información necesaria para el cumplimiento de necesidades y expectativas, cuentan únicamente con la matriz de partes	Para garantizar una gestión efectiva de las partes interesadas en cualquier proyecto, es fundamental establecer un registro formal que contenga información detallada sobre cada una de ellas. Este registro

	y reglamentarios aplicables, la organización debe determinar: a) las partes interesadas pertinentes al sistema de gestión de la calidad; b) los requisitos pertinentes para el sistema de gestión de la calidad. La organización debe realizar el seguimiento y la revisión de la información sobre estas partes interesadas y sus requisitos pertinentes.	interesadas en el Ma_Sistema de Gestión Integrado (SGI)_V01	debe abarcar aspectos clave como sus necesidades, expectativas, roles y niveles de influencia. Además, es crucial revisar periódicamente esta documentación para mantenerla actualizada y asegurar que refleje con precisión la situación actual de las partes interesadas. Esta revisión regular permite identificar cambios en las necesidades o expectativas de las partes interesadas, así como ajustar las estrategias de gestión de manera oportuna para mantener su compromiso y satisfacción.
--	---	--	--

Tabla 166 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.6.1.3 Contacto con Autoridad	Se deben mantener contactos	Se muestra el "Re_Matriz contacto	Para mantener un flujo eficiente de

	apropiados con las autoridades relevantes	autoridades_2023" actualizado el 23 de agosto del 2023 en el cual solo se incluyen a los grupos de interés especiales.	comunicación y garantizar una respuesta oportuna ante cualquier eventualidad, es crucial mantener actualizada y completa la matriz de contacto con autoridades. Este documento sirve como una herramienta fundamental para identificar y contactar a las partes relevantes en situaciones diversas. Actualizar esta matriz con información precisa y actualizada permite a la organización estar preparada para cualquier escenario, asegurando que se puedan establecer conexiones rápidas y efectivas cuando sea necesario.
--	---	--	---

Tabla 167 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
-----------	-------------	----------	-------------------------

A.6.1.5 Seguridad de la Información en la Administración de Proyectos	La seguridad de la información debe incluirse en la administración de proyectos independientemente del tipo de proyecto.	Se muestra el "Fo_Implementación de servicio_V04" actualizado el 25 de mayo del 2023 el cual considera endpoint para infonavit, en el documento se aprecia que se consideran los riesgos del proyecto. Se muestra evidencia del proyecto "Re_plan de trabajo_Instalación de memorias RAM y discos duros en servidores" generado el 31 de octubre del 2023, En este caso, la documentación carece de la identificación de riesgos asociados al proyecto, lo cual constituye una deficiencia que requiere atención y corrección inmediata. Es esencial que la organización considere los riesgos en todos sus proyectos, tanto	Se propone actualizar el formato vigente, incorporando una sección específica dedicada a la consideración de riesgos. Este enfoque permitirá una evaluación más integral, identificando y valorando los posibles obstáculos y desafíos que podrían surgir durante la ejecución del proyecto. Además, se sugiere llevar a cabo la evaluación del proyecto más reciente, utilizando el nuevo formato actualizado.
---	---	---	--

		internos como externos. La gestión proactiva de riesgos es fundamental para anticipar obstáculos, tomar medidas preventivas y asegurar el éxito de los proyectos.	
--	--	---	--

Tabla 168 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.7.3.1 Responsabilidades en la terminación o cambio de empleo	Las responsabilidades de la seguridad de la información y obligaciones que permanecen validos después de la terminación o el cambio e empleo deben estar definidos, comunicados a los empleados o contratistas y hacerse cumplir.	Se evidencia la baja de Gabriel Arcega Soto, documentada con la conformación del expediente de baja, el cual incluye diversos elementos como renuncia, baja del biométrico, solicitud de baja de activos, accesos físicos y lógicos, carta de asignación y devolución de activos, y aviso de privacidad. Asimismo, se presenta evidencia del cambio de puesto de Gabriel Arcega Soto,	Generar un formato específico para notificar al colaborador al término de su relación laboral sobre sus derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). Este formato debería ser integrado de manera sistemática en la documentación de baja de los colaboradores. De esta forma, se asegura que los empleados puedan ejercer fácilmente sus

		respaldado por la minuta de aprobación del cambio y el perfil de puestos firmado por la parte involucrada generados el 25 de octubre de 2023. Sin embargo, no se encontró evidencia de que la organización haya comunicado y/o recordado las responsabilidades de Seguridad de la Información que permanecen vigentes, ni los derechos de ARCO (Acceso, Rectificación, Cancelación y Oposición) respecto a la desvinculación de los colaboradores.	derechos individuales, promoviendo así una salida laboral transparente y respetuosa que fomente la confianza y el cumplimiento normativo en la organización.
--	--	--	---

Tabla 169 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.11.1.1 Perímetro de Seguridad Física	Se deben definir y utilizar perímetros de seguridad para proteger las áreas	Se muestra el Ma_Seguridad de la organización_V01 fechado el 25 de mayo del 2023 pero no se	Identificar y marcar de manera precisa los siguientes elementos de seguridad: detectores de humo,

	que contienen información ya sea sensible o crítica y las instalaciones de procesamiento de la información.	identifican los controles implementados.	extintores, sistemas biométricos de acceso, salidas de emergencia, puntos de acceso, así como la zona designada para carga y descarga. Este proceso permitirá contar con una representación visual detallada de los controles de seguridad implementados, facilitando tanto la evaluación de su efectividad como la identificación de áreas susceptibles de mejora. Además, la marcación clara de estos elementos en el croquis proporciona una guía práctica para el personal encargado de la seguridad, asegurando que estén plenamente informados sobre la ubicación y disponibilidad de recursos relevantes en situaciones críticas
--	---	--	---

Tabla 170 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.12.1.2 Gestión del Cambio	Se deben controlar los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten a la seguridad de la información.	Se cuenta con un Pr_Gestión del cambio_V01 fechado el 19 de mayo del 2023 que incluye los elementos solicitados por el requisito. Tipos de cambio: estándar, normal y emergente No ha habido cambios internos. Se muestra Aranda, herramienta utilizada para gestionar los cambios a la infraestructura o los cambios en los servicios. Se muestra Re_Caso no. 63 / CHG8268-1-63 fechado el 17 de marzo del 2023 por Saul Gomez del cliente Secretaría de Turismo, se observa debidamente requisitos a la solicitud de	Actualizar los criterios de impacto en la herramienta de Aranda para asegurar que sean compatibles con la configuración actual.

		cambio, misma que se anexa al caso creado. En Criterios de impacto: en la tabla de tipos de cambio se describen los impactos sin embargo no existe un criterio que sea compatible con lo configurado en la herramienta de Aranda.	
--	--	---	--

Tabla 171 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.12.3.1 Respaldos de la Información	Copias de respaldos de la información, software e imágenes de sistemas deben realizarse y probarse regularmente de acuerdo con la política de respaldos acordada.	Se muestra una Re_Bitácora de respaldos fechada el día 8 de febrero del 2023, en la cual se identifica la realización de respaldos completos e incrementales para (ofimática, PRTG, Firewall, switch). Sin embargo, al revisar la bitácora detalladamente, se encuentra que no se han registrado respaldos para ninguna	Reforzar los procedimientos de respaldo de datos y asegurarse de que se realicen de manera adecuada.

		plataforma mencionada. Esta omisión representa un incumplimiento de los procedimientos establecidos para la realización de respaldos de datos, lo que podría generar riesgos significativos para la integridad y disponibilidad de la información de la organización. Por lo tanto, es necesario revisar y reforzar los procedimientos de respaldo de datos para garantizar que se realicen de manera adecuada y se registren correctamente en la bitácora correspondiente.	
--	--	---	--

Tabla 172 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.13.2.1 Políticas y Procedimientos	Deben existir políticas formales de transferencia,	Se dispone de una Po_Convenios de Confidencialidad_V01,	Implementar controles adecuados para proteger la

de Transferencia de Información	procedimientos y controles para proteger la transferencia de información a través del uso de cualquier tipo de medio de comunicación.	fecha el día 11 de julio de 2023. Sin embargo, no se cuenta con controles adecuados para proteger la transferencia de información.	transferencia de información según lo establecido en la Po_Convenios de Confidencialidad_V01.
A.17.1.3 Verificación, revisión y evaluación de la Continuidad de la Seguridad de la Información	La organización debe verificar los controles de continuidad de seguridad de la información establecidos e implementados a intervalos regulares para garantizar que sean válidos y eficaces en situaciones adversas.	Se presenta el Fo_Plan de continuidad y disponibilidad_V01 fechado el 2 de mayo de 2023, que aborda situaciones como corte de energía eléctrica, corte de comunicaciones, indisponibilidad de instalaciones, ausentismo, emergencia sanitaria, política o social. Aunque los planes de continuidad y disponibilidad se prueban anualmente en septiembre y octubre, con informes exitosos de pruebas realizadas en septiembre, el incumplimiento radica	Establecer un plan de verificación regular de los controles de continuidad de seguridad de la información.

		en la falta de verificación regular de los controles de continuidad de seguridad de la información.	
--	--	---	--

Tabla 173 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.18.1.1 Identificación de la Legislación Aplicable y Requisitos Contractuales	Todos los requisitos legislativos, regulatorios, contractuales relevantes y el enfoque de la organización para cumplir con estos requisitos deben estar explícitamente identificados, documentados y mantenerse actualizados para cada sistema de información y la organización.	Se muestra la Re_Matriz de cumplimiento fechado el día 24 de marzo del 2023 donde identifica los requisitos normativos/ requisitos, fuente, evidencia, revisiones semestrales y observaciones, sin embargo, no refleja de manera completa y actualizada todos los requisitos normativos pertinentes.	Revisar exhaustivamente la Re_Matriz de cumplimiento para identificar todos los requisitos normativos pertinentes que deben ser incluidos.

CAPÍTULO IV

RESULTADOS

4.1 Objetivo 3 Entregar Resultados

4.1.1 Actividades

4.1.1.1 Actividad 3.1 Analizar y sintetizar los hallazgos de la auditoría en un informe final.

Implica el análisis y síntesis de todos los hallazgos de la auditoría para crear una visión general de la situación.

4.1.1.1.1 Descripción de la actividad

Conforme al análisis exhaustivo llevado a cabo mediante entrevistas, la minuciosa revisión de los procedimientos y políticas institucionales, así como la evaluación de las evidencias recabadas, todas enfocadas en la lista de verificación correspondiente, se ha confeccionado el presente informe. Con ayuda de la lista de verificación se identifican los hallazgos calificados con NC (No Conformidad) y OB (Observación) y la información del plan de auditoría se genera el informe.

4.1.1.1.2 Resultado de la actividad

4.1.1.1.2.1 Informe de auditoría

1. Alcance

Revisar y evaluar el Sistema de Gestión Integral implementado en el SOC-NOC HORUS, incluyendo los procedimientos, políticas, manuales, anexos, formatos declarados e implementados en los servicios de mesa de ayuda, monitoreo, en sus procesos de atención de incidentes y solicitudes de servicio, atención de problemas, niveles de servicio, procesos de servicios nuevos o modificados, y en todos sus procesos de gestión del servicio y seguridad de la información, ofrecidos por su SOC-NOC Horus, así como, la protección de recursos, servicios y partes interesadas.

2. Objetivo

Verificar si el Sistema de Gestión Integral implementado en la organización es conforme a los requisitos de las normas ISO/IEC 27001:2013 y Anexo A.

3. Equipo auditor

Tabla 174 Equipo auditor

Nombre	Iniciales	Rol
Brenda Itzel Gante Sánchez	BIGS	Auditor en entrenamiento
Lizeth Viridiana Gutiérrez Guerra	LVGG	Auditor en entrenamiento

4. Hallazgos de la auditoria

A continuación, se describen los hallazgos de la auditoría que se identificaron

Tabla 175 Hallazgos de la auditoria

Numeral Requisito	Descripción/Requisitos	Tipo de Hallazgo	Descripción del Hallazgo
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Por su efecto o efecto potencial en la capacidad de la organización de proporcionar productos y servicios que satisfagan los requisitos del cliente y los legales y reglamentarios aplicables, la organización debe determinar: a) las partes interesadas pertinentes al sistema de gestión de la calidad; b) los requisitos pertinentes para el sistema de gestión de la calidad. La organización	NC	No se encuentra documentadas las partes interesadas, los colaboradores saben la información necesaria para el cumplimiento de necesidades y expectativas, cuentan únicamente con la matriz de partes interesadas en el Ma_Sistema de Gestión Integrado (SGI)_V01

	debe realizar el seguimiento y la revisión de la información sobre estas partes interesadas y sus requisitos pertinentes.		
--	---	--	--

Tabla 176 (Continuación)

Numeral Requisito	Descripción/Requisitos	Tipo de Hallazgo	Descripción del Hallazgo
A.6.1.3 Contacto con Autoridad	Se deben mantener contactos apropiados con las autoridades relevantes	NC	Se muestra el "Re_Matriz contacto autoridades_2023" actualizado el 23 de agosto del 2023 en el cual solo se incluyen a los grupos de interés especiales .
A.6.1.5 Seguridad de la Información en la Administración de Proyectos	La seguridad de la información debe incluirse en la administración de proyectos independientemente del tipo de proyecto.	OB	Se muestra el "Fo_Implementación de servicio_V04" actualizado el 25 de mayo del 2023 el cual considera endpoint para infonavit, en el documento se aprecia que se consideran los riesgos del proyecto. Se muestra evidencia del proyecto "Re_plan de trabajo_Instalación de memorias RAM y discos duros en servidores" generado el 31 de octubre del 2023, En este caso, la documentación carece de la

			identificación de riesgos asociados al proyecto, lo cual constituye una deficiencia que requiere atención y corrección inmediata. Es esencial que la organización considere los riesgos en todos sus proyectos, tanto internos como externos. La gestión proactiva de riesgos es fundamental para anticipar obstáculos, tomar medidas preventivas y asegurar el éxito de los proyectos.
--	--	--	---

Tabla 177 (Continuación)

Numeral Requisito	Descripción/Requisitos	Tipo de Hallazgo	Descripción del Hallazgo
A.7.3.1 Responsabilidades en la terminación o cambio de empleo	Las responsabilidades de la seguridad de la información y obligaciones que permanecen validos después de la terminación o el cambio e empleo deben estar definidos, comunicados a los empleados o contratistas y hacerse cumplir.	OB	Se evidencia la baja de Gabriel Arcega Soto, documentada con la conformación del expediente de baja, el cual incluye diversos elementos como renuncia, baja del biométrico, solicitud de baja de activos, accesos físicos y lógicos, carta de asignación y devolución de activos, y aviso de privacidad.

			Asimismo, se presenta evidencia del cambio de puesto de Gabriel Arcega Soto, respaldado por la minuta de aprobación del cambio y el perfil de puestos firmado por la parte involucrada generados el 25 de octubre de 2023. Sin embargo, no se encontró evidencia de que la organización haya comunicado y/o recordado las responsabilidades de Seguridad de la Información que permanecen vigentes, ni los derechos de ARCO (Acceso, Rectificación, Cancelación y Oposición) respecto a la desvinculación de los colaboradores.
--	--	--	---

Tabla 178 (Continuación)

Numeral Requisito	Descripción/Requisitos	Tipo de Hallazgo	Descripción del Hallazgo
A.11.1.1 Perímetro de Seguridad Física	Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen información ya sea sensible o crítica y las	NC	Se muestra el Ma_Seguridad de la organización_V01 fechado el 25 de mayo del 2023 pero no se identifican los controles implementados.

	instalaciones de procesamiento de la información.		
--	---	--	--

Tabla 179 (Continuación)

Numeral Requisito	Descripción/Requisitos	Tipo de Hallazgo	Descripción del Hallazgo
A.12.1.2 Gestión del Cambio	Se deben controlar los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten a la seguridad de la información.	OB	Se cuenta con un Pr_Gestión del cambio_V01 fechado el 19 de mayo del 2023 que incluye los elementos solicitados por el requisito. Tipos de cambio: estándar, normal y emergente No ha habido cambios internos. Se muestra Aranda, herramienta utilizada para gestionar los cambios a la infraestructura o los cambios en los servicios. Se muestra Re_Caso no. 63 / CHG8268-1-63 fechado el 17 de marzo del 2023 por Saul Gomez del cliente Secretaría de Turismo, se observa debidamente requisitos a la solicitud de cambio, misma que se anexa al caso creado.

			En Criterios de impacto: en la tabla de tipos de cambio se describen los impactos sin embargo no existe un criterio que sea compatible con lo configurado en la herramienta de Aranda.
--	--	--	--

Tabla 180 (Continuación)

Numeral Requisito	Descripción/Requisitos	Tipo de Hallazgo	Descripción del Hallazgo
A.12.3.1 RespalDOS de la Información	Copias de respaldos de la información, software e imágenes de sistemas deben realizarse y probarse regularmente de acuerdo con la política de respaldos acordada.	NC	Se muestra una Re_Bitácora de respaldos fechada el día 8 de febrero del 2023, en la cual se identifica la realización de respaldos completos e incrementales para (ofimática, PRTG, Firewall, switch). Sin embargo, al revisar la bitácora detalladamente, se encuentra que no se ha registrado la realización de respaldos para ninguna de las plataformas mencionadas. Esta omisión representa un incumplimiento de los procedimientos establecidos para la realización de respaldos de datos, lo que podría generar riesgos

			significativos para la integridad y disponibilidad de la información de la organización. Por lo tanto, es necesario revisar y reforzar los procedimientos de respaldo de datos para garantizar que se realicen de manera adecuada y se registren correctamente en la bitácora correspondiente.
--	--	--	--

Tabla 181 (Continuación)

Numeral Requisito	Descripción/Requisitos	Tipo de Hallazgo	Descripción del Hallazgo
A.13.2.1 Políticas y Procedimientos de Transferencia de Información	Deben existir políticas formales de transferencia, procedimientos y controles para proteger la transferencia de información a través del uso de cualquier tipo de medio de comunicación.	NC	Se dispone de una Po_Convenios de Confidencialidad_V01, fechada el día 11 de julio de 2023. Sin embargo, no se cuenta con controles adecuados para proteger la transferencia de información.
A.17.1.3 Verificación, revisión y evaluación de la Continuidad de la	La organización debe verificar los controles de continuidad de seguridad de la información establecidos e implementados a	NC	Se presenta el Fo_Plan de continuidad y disponibilidad_V01 fechado el 2 de mayo de 2023, que aborda

Seguridad de la Información	intervalos regulares para garantizar que sean válidos y eficaces en situaciones adversas.		situaciones como corte de energía eléctrica, corte de comunicaciones, indisponibilidad de instalaciones, ausentismo, emergencia sanitaria, política o social. Aunque los planes de continuidad y disponibilidad se prueban anualmente en septiembre y octubre, con informes exitosos de pruebas realizadas en septiembre, el incumplimiento radica en la falta de verificación regular de los controles de continuidad de seguridad de la información.
-----------------------------	---	--	--

Tabla 182 (Continuación)

Numeral Requisito	Descripción/Requisitos	Tipo de Hallazgo	Descripción del Hallazgo
A.18.1.1 Identificación de la Legislación Aplicable y Requisitos Contractuales	Todos los requisitos legislativos, regulatorios, contractuales relevantes y el enfoque de la organización para cumplir con estos requisitos deben estar explícitamente identificados, documentados y mantenerse actualizados	NC	Se muestra la Re_Matriz de cumplimiento fechado el día 24 de marzo del 2023 donde identifica los requisitos normativos/ requisitos, fuente, evidencia, revisiones semestrales y observaciones, sin embargo, no refleja de manera

	para cada sistema de información y la organización.		completa y actualizada todos los requisitos normativos pertinentes.
--	---	--	---

5. Resultados de la evaluación

Tabla 183 Resultados de la evaluación

Normatividad aplicable	No Conformidades	Observación	Conformidades
ISO/IEC 27001:2013 y Anexo A	7	3	134

6. Conclusiones de auditoria

El ejercicio se realizó de manera satisfactoria y con base en lo planificado.

7. Distribución del informe

Se realiza la entrega del Informe al responsable del SGI.

8. Comentarios generales del equipo auditor

- Se identifica el compromiso de los responsables en la atención del ejercicio de auditoría.
- Las herramientas tecnológicas involucradas en la prestación del servicio.
- Se cumplieron los objetivos de auditoría y el ejercicio de concluyo con base en lo planificado y sin contratiempos.
- Se identifica un grado de madurez medio-alto en su Sistema de Gestión Integral.

- Durante el ejercicio se identifica que los nuevos colaboradores están en proceso de conocer, aprender y entender el SGI por lo que es importante mantener la concientización respecto del SGI.

9. Documentos relacionados

- Lista de verificación
- Informe de remediación de hallazgos

Tabla 184 Autorización del informe

Elaborado por:	
	
Brenda Itzel Gante Sánchez Auditor en entrenamiento	Lizeth Viridiana Gutiérrez Guerra Auditor en entrenamiento

4.1.1.2 Actividad 3.2 Elaborar recomendaciones específicas sobre los hallazgos y mejorar las áreas identificadas.

Se deben proporcionar recomendaciones específicas basadas en los hallazgos de la auditoría, destacando las áreas que necesitan mejoras y proponiendo soluciones concretas.

4.1.1.2.1 Descripción de la actividad

Generar un informe basado en las propuestas de remediaciones identificadas durante una auditoría. En el informe, se muestran los controles evaluados, cada uno identificado y acompañado de una descripción detallada. Además, se destacan los hallazgos encontrados durante la auditoría, tales como NC y OB, junto con recomendaciones específicas para su

corrección o mejora. Para cada control evaluado, se resaltan los hallazgos identificados durante la auditoría que no cumplen o cumplen parcialmente, junto con recomendaciones específicas para su remediación. Estas recomendaciones pueden incluir acciones correctivas a tomar, cambios en los procedimientos o mejoras en los sistemas existentes.

4.1.1.2.2 Resultado de la actividad

4.1.1.2.2.1 Informe de recomendación de remediación de hallazgos

1. Alcance

Revisar y evaluar el Sistema de Gestión Integral implementado en el SOC-NOC HORUS, incluyendo los procedimientos, políticas, manuales, anexos, formatos declarados e implementados en los servicios de mesa de ayuda, monitoreo, en sus procesos de atención de incidentes y solicitudes de servicio, atención de problemas, niveles de servicio, procesos de servicios nuevos o modificados, y en todos sus procesos de gestión del servicio y seguridad de la información, ofrecidos por su SOC-NOC Horus, así como, la protección de recursos, servicios y partes interesadas.

2. Objetivo

Verificar si el Sistema de Gestión Integral implementado en la organización es conforme a los requisitos de las normas ISO/IEC 27001:2013 y Anexo A.

3. Equipo auditor

Tabla 185 Equipo auditor

Nombre	Iniciales	Rol
Brenda Itzel Gante Sánchez	BIGS	Auditor en entrenamiento
Lizeth Viridiana Gutiérrez Guerra	LVGG	Auditor en entrenamiento

4. Recomendación de remediación de hallazgos de auditoria

A continuación, se describen los hallazgos de la auditoría que se identificaron y las recomendaciones de remediación.

Tabla 186 Recomendación de remediación de hallazgos de auditoría

Requisito	Descripción	Hallazgo	Acciones de remediación
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Por su efecto o efecto potencial en la capacidad de la organización de proporcionar productos y servicios que satisfagan los requisitos del cliente y los legales y reglamentarios aplicables, la organización debe determinar: a) las partes interesadas pertinentes al sistema de gestión de la calidad; b) los requisitos pertinentes para el sistema de gestión de la calidad. La organización debe realizar el seguimiento y la revisión de la	No se encuentra documentadas las partes interesadas, los colaboradores saben la información necesaria para el cumplimiento de necesidades y expectativas, cuentan únicamente con la matriz de partes interesadas en el Ma_Sistema de Gestión Integrado (SGI)_V01	Crear un registro formal de partes interesadas que incluya información detallada sobre cada una, como sus necesidades, expectativas, etc. Revisar regularmente la documentación de partes interesadas.

	información sobre estas partes interesadas y sus requisitos pertinentes.		
--	--	--	--

Tabla 187 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.6.1.3 Contacto con Autoridad	Se deben mantener contactos apropiados con las autoridades relevantes	Se muestra el "Re_Matriz contacto autoridades_2023" actualizado el 23 de agosto del 2023 en el cual solo se incluyen a los grupos de interés especiales.	Actualizar y completar la matriz de contacto con autoridades con la información más reciente y precisa. Establecer un proceso claro y periódico para la revisión y actualización de la matriz.
A.6.1.5 Seguridad de la Información en la Administración de Proyectos	La seguridad de la información debe incluirse en la administración de proyectos independientemente del tipo de proyecto.	Se muestra el "Fo_Implementación de servicio_V04" actualizado el 25 de mayo del 2023 el cual considera endpoint para infonavit, en el documento se aprecia que se consideran los riesgos del proyecto.	Actualizar el formato para la evaluación de proyectos considerando los riesgos. Realizar la evaluación del proyecto más reciente

		Se muestra evidencia del proyecto "Re_plan de trabajo_Instalación de memorias RAM y discos duros en servidores" generado el 31 de octubre del 2023, En este caso, la documentación carece de la identificación de riesgos asociados al proyecto, lo cual constituye una deficiencia que requiere atención y corrección inmediata. Es esencial que la organización considere los riesgos en todos sus proyectos, tanto internos como externos. La gestión proactiva de riesgos es fundamental para anticipar obstáculos, tomar medidas preventivas y asegurar el éxito de los proyectos.	
--	--	--	--

Tabla 188 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.7.3.1 Responsabilidades en la terminación o cambio de empleo	Las responsabilidades de la seguridad de la información y obligaciones que permanecen validos después de la terminación o el cambio e empleo deben estar definidos, comunicados a los empleados o contratistas y hacerse cumplir.	Se evidencia la baja de Gabriel Arcega Soto, documentada con la conformación del expediente de baja, el cual incluye diversos elementos como renuncia, baja del biométrico, solicitud de baja de activos, accesos físicos y lógicos, carta de asignación y devolución de activos, y aviso de privacidad. Asimismo, se presenta evidencia del cambio de puesto de Gabriel Arcega Soto, respaldado por la minuta de aprobación del cambio y el perfil de puestos firmado por la parte involucrada generados el 25 de octubre de 2023. Sin embargo, no se encontró evidencia de que la organización	Generar un formato para notificar al colaborador al término de la relación laboral que puede hacer uso de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). Integrarlo a la documentación de baja de los colaboradores.

		haya comunicado y/o recordado las responsabilidades de Seguridad de la Información que permanecen vigentes, ni los derechos de ARCO (Acceso, Rectificación, Cancelación y Oposición) respecto a la desvinculación de los colaboradores.	
--	--	--	--

Tabla 189 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.11.1.1 Perímetro de Seguridad Física	Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen información ya sea sensible o crítica y las instalaciones de procesamiento de la información.	Se muestra el Ma_Seguridad de la organización_V01 fechado el 25 de mayo del 2023 pero no se identifican los controles implementados.	Identificar y marcar de manera precisa los siguientes elementos de seguridad: detectores de humo, extintores, sistemas biométricos de acceso, salidas de emergencia, puntos de acceso, así como la zona designada para carga y descarga. Este proceso permitirá

			contar con una representación visual detallada de los controles de seguridad implementados, facilitando tanto la evaluación de su efectividad como la identificación de áreas susceptibles de mejora. Además, la marcación clara de estos elementos en el croquis proporciona una guía práctica para el personal encargado de la seguridad, asegurando que estén plenamente informados sobre la ubicación y disponibilidad de recursos relevantes en situaciones críticas
--	--	--	--

Tabla 190 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
------------------	--------------------	-----------------	--------------------------------

A.12.1.2 Gestión del Cambio	Se deben controlar los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten a la seguridad de la información.	Se cuenta con un Pr_Gestión del cambio_V01 fechado el 19 de mayo del 2023 que incluye los elementos solicitados por el requisito. Tipos de cambio: estándar, normal y emergente No ha habido cambios internos. Se muestra Aranda, herramienta utilizada para gestionar los cambios a la infraestructura o los cambios en los servicios. Se muestra Re_Caso no. 63 / CHG8268-1-63 fechado el 17 de marzo del 2023 por Saul Gomez del cliente Secretaría de Turismo, se observa debidamente requisitos a la solicitud de cambio, misma que se anexa al caso creado.	Asegurarse de que los criterios actualizados estén correctamente implementados en la herramienta de gestión de cambios.
-----------------------------	---	---	---

		En Criterios de impacto: en la tabla de tipos de cambio se describen los impactos sin embargo no existe un criterio que sea compatible con lo configurado en la herramienta de Aranda.	
--	--	--	--

Tabla 191 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.12.3.1 Respallos de la Información	Copias de respaldos de la información, software e imágenes de sistemas deben realizarse y probarse regularmente de acuerdo con la política de respaldos acordada.	Se muestra una Re_Bitácora de respaldos fechada el día 8 de febrero del 2023, en la cual se identifica la realización de respaldos completos e incrementales para (ofimática, PRTG, Firewall, switch). Sin embargo, al revisar la bitácora detalladamente, se encuentra que no se ha registrado la realización de respaldos para ninguna de las plataformas	Implementar los nuevos procedimientos y realizar retroalimentación para asegurar la adecuada documentación en la bitácora.

		mencionadas. Esta omisión representa un incumplimiento de los procedimientos establecidos para la realización de respaldos de datos, lo que podría generar riesgos significativos para la integridad y disponibilidad de la información de la organización. Por lo tanto, es necesario revisar y reforzar los procedimientos de respaldo de datos para garantizar que se realicen de manera adecuada y se registren correctamente en la bitácora correspondiente.	
--	--	---	--

Tabla 192 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.13.2.1 Políticas y Procedimientos de Transferencia de Información	Deben existir políticas formales de transferencia, procedimientos y	Se dispone de una Po_Convenios de Confidencialidad_V01, fechada el día 11 de	Verificar que los controles implementados estén funcionando

	controles para proteger la transferencia de información a través del uso de cualquier tipo de medio de comunicación.	julio de 2023. Sin embargo, no se cuenta con controles adecuados para proteger la transferencia de información.	de manera efectiva según lo establecido en la política de confidencialidad.
A.17.1.3 Verificación, revisión y evaluación de la Continuidad de la Seguridad de la Información	La organización debe verificar los controles de continuidad de seguridad de la información establecidos e implementados a intervalos regulares con el objetivo de garantizar que son válidos y eficaces durante situaciones adversas.	Se presenta el Fo_Plan de continuidad y disponibilidad_V01 fechado el 2 de mayo de 2023, que aborda situaciones como corte de energía eléctrica, corte de comunicaciones, indisponibilidad de instalaciones, ausentismo, emergencia sanitaria, política o social. Aunque los planes de continuidad y disponibilidad se prueban anualmente en septiembre y octubre, con informes exitosos de pruebas realizadas en septiembre, el incumplimiento radica	Realizar pruebas periódicas según lo establecido en el plan y documentar los resultados para futuras revisiones y mejoras.

		en la falta de verificación regular de los controles de continuidad de seguridad de la información.	
--	--	---	--

Tabla 193 (Continuación)

Requisito	Descripción	Hallazgo	Acciones de remediación
A.18.1.1 Identificación de la Legislación Aplicable y Requisitos Contractuales	Todos los requisitos legislativos, regulatorios, contractuales relevantes y el enfoque de la organización para cumplir con estos requisitos deben estar explícitamente identificados, documentados y mantenerse actualizados para cada sistema de información y la organización.	Se muestra la Re_Matriz de cumplimiento fechado el día 24 de marzo del 2023 donde identifica los requisitos normativos/ requisitos, fuente, evidencia, revisiones semestrales y observaciones. Sin embargo no refleja de manera completa y actualizada todos los requisitos normativos pertinentes.	Actualizar la Re_Matriz de cumplimiento para reflejar de manera completa y precisa todos los requisitos normativos pertinentes, asegurando que estén debidamente documentados con la fuente correspondiente, la evidencia, las revisiones semestrales y las observaciones necesarias para garantizar el cumplimiento

			normativo adecuado.
--	--	--	------------------------

5. Documentos relacionados

- Lista de verificación
- Informe de auditoría

Tabla 194 Autorización del informe

Elaborado por:	
	
Brenda Itzel Gante Sánchez	Lizeth Viridiana Gutiérrez Guerra
Auditor en entrenamiento	Auditor en entrenamiento

4.1.1.3 Actividad 3.3 Elaborar los planes de acción basados en los hallazgos y recomendaciones.

Implica analizar hallazgos y recomendaciones para luego desarrollar planes detallados de acción que aborden esos hallazgos y sigan las recomendaciones.

4.1.1.3.1 Descripción de la actividad

Analizar los resultados de investigaciones, evaluaciones o auditorías para identificar áreas de mejora o problemas, se desarrollan planes detallados que describen las acciones específicas que se tomarán para abordar estos hallazgos y seguir las recomendaciones. Estos planes incluyen objetivos claros, pasos concretos, asignación de responsabilidades y un cronograma para su implementación. Su objetivo principal es mejorar procesos, resolver problemas o alcanzar metas específicas dentro de una organización o proyecto. Se realiza un exhaustivo análisis de los resultados derivado de la auditoría, abarcando tanto datos cuantitativos como cualitativos. A partir de estos hallazgos, se elaboran planes detallados que delinean las

acciones concretas a seguir, estableciendo objetivos claros, pasos específicos, asignación de responsabilidades y fechas límite para su implementación. Estos planes se diseñan con el propósito principal de mejorar procesos, resolver dificultades identificadas o alcanzar metas específicas dentro del ámbito de una organización o proyecto, buscando siempre optimizar la eficiencia operativa y la calidad del resultado final.

4.1.1.3.2 Resultado de la actividad

4.1.1.3.2.1 Plan de acción: Partes interesadas

1. Datos generales de la acción

Tabla 195 Datos generales plan de acción 160

Folio	160	Fecha de registro	19-mar-24
Tipo de Acción	Correctiva ☒ Preventiva ☐ Mejora ☐	Prioridad	Baja ☐ Media ☐ Alta ☒
Derivada de	Auditoría interna ☒ Auditoría externa ☐ De la operación ☐ Queja ☐ Problema ☐ Sugerencia ☐ Revisión por la dirección ☐		

2. Descripción del hallazgo

Tabla 196 Descripción del hallazgo plan de acción 160

Requisito Normativo Documento(s), y/o activo afectado	Descripción del hallazgo o Problema
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	No se encuentra documentadas las partes interesadas, los colaboradores saben la información necesaria para el cumplimiento de necesidades y expectativas, cuentan únicamente con la matriz de partes interesadas en el Ma_Sistema de Gestión Integrado (SGI)_V01

3. Análisis de causa raíz

Lluvia de ideas

- Identificar las partes interesadas actuales
- Verificar las necesidades y expectativas
- Llenar los formatos generados ubicados en el Manual

4. Plan de acción

Tabla 197 Plan de acción 160

Descripción breve de la acción a realizar		Llenar la matriz de partes interesadas		
Objetivo / Meta		Tener las partes interesadas documentadas		
No.	Actividad	Fecha de compromiso		Responsables (Iniciales)
		Inicio	Fin	
1	Identificar partes interesadas	19-mar-24	20-mar-24	RCG LVGG
2	Detectar necesidades	21-mar-24	22-mar-24	RCG LVGG
3	Detectar expectativas	25-mar-24	26-mar-24	RCG LVGG
4	Asignar responsable	26-mar-24	26-mar-24	RCG LVGG
5	Definir indicadores de satisfacción	27-mar-24	28-mar-24	RCG LVGG
6	Llenar la matriz de partes asignadas definida en el	28-mar-24	28-mar-24	RCG LVGG

	Ma_Sistema de Gestión Integrado (SGI)_V01			
7	Evaluar	29-mar-24	29-mar-24	RCG LVGG
8	Definir política de revisión	29-mar-24	29-mar-24	RCG LVGG

5. Evaluación del plan de acción

Tabla 198 Evaluación del plan de acción 160

Estatus	Aprobada ☒ Rechazada ☐	La acción fue rechazada por qué:
----------------	---	---

6. Eficacia de la acción realizada

Tabla 199 Eficacia del plan de acción 160

La acción realizada se consideró	Eficaz ☒ Ineficaz ☐	¿Por qué?	Se cumplió el objetivo
El nivel de eficacia de la acción fue	Alto ☒ Medio ☐ Bajo ☐	¿Por qué?	Se cumplieron las actividades en tiempo y forma según lo planificado
Grado de cumplimiento contra el objetivo o meta establecida			Alto ☒ Medio ☐ Bajo ☐
Fecha de Cierre	29-mar-24		

7. Resultados

Se muestra el Ma_Sistema de Gestión Integrado (SGI)_V02 actualizado el 29 de marzo del 2024



Figura 35 Portada del manual del sistema de gestión integral

En la página 18 del Ma_Sistema de Gestión Integrado (SGI)_V02 se ubica la matriz de partes interesadas llena identificando sus necesidades y expectativas de manera clara así como los responsables, nivel de satisfacción y evaluación.

MANUAL DEL SISTEMA DE GESTIÓN INTEGRAL

Clasificación: Interno
Versión: 02
Fecha de última revisión:
29-03-24

COMUNICACIÓN

A fin de comunicar la información del SGI que es de interés para las partes interesadas, la Dirección General determina la siguiente matriz de comunicación:

PORTE INTERESADA	NECESIDADES	EXPECTATIVAS
Clientes	Cumplimiento de plazos de entrega	Flexibilidad en las opciones de compra
	Resolución eficiente de problemas	Transparencia en prácticas de seguridad
	Protección de la información personal proporcionada	Cumplimiento de la empresa con leyes y regulaciones relacionadas con la seguridad de la información.
	Servicios de calidad	
Proveedores	Pagos puntuales	Colaboración en rentabilidad
	Comunicación clara	Transparencia en prácticas de seguridad y comunicación efectiva en caso de incidentes
	Cumplimiento contractual	
	Protección de la información personal proporcionada	
Colaboradores	Salarios y beneficios competitivos	Oportunidades de desarrollo profesional
	Comunicación clara sobre seguridad de la información	Capacitación continua
	Protección de la información personal proporcionada	
	Comunicación clara y transparente	
Competencia	Ambiente de trabajo seguro y saludable	Cumplimiento con estándares éticos y legales en prácticas de seguridad
	Respeto a la propiedad intelectual	Innovación segura y respeto por la propiedad intelectual
	Acceso seguro a la información compartida	
Socios	Cumplimiento de estándares de seguridad informática	Claridad en objetivos de asociación y comunicación transparente
	Transparencia en la comunicación	Flexibilidad para adaptarse a cambios en el entorno de seguridad
Autoridades	Cumplimiento de normativas y regulaciones	Transparencia en prácticas comerciales y cumplimiento de estándares de seguridad
	Presentación oportuna de informes y documentos	Pago de impuestos y tasas de manera oportuna
	Protección de la información personal proporcionada	

SATISFACCIÓN

Parte interesada	Necesidad	Responsable	Indicador de satisfacción	Evaluación
Clientes	Cumplimiento de plazos de entrega	Responsable del servicio	Número de reclamaciones por retraso Porcentaje de entregas a tiempo	Satisfactorio
	Resolución eficiente de problemas	Gestor de Incidentes Gestor de Riesgos	Tiempo promedio de resolución de problemas Porcentaje de problemas resueltos Número de contactos necesarios para la resolución	Satisfactorio
	Protección de la Información Personal proporcionada	Oficial de Privacidad de Datos	Cumplimiento de políticas de retención y eliminación de datos Percepción de seguridad por parte de los clientes Cumplimiento con normativas de privacidad Número de incidentes de violación de datos personales	Satisfactorio

Figura 36 Matriz de partes interesadas del manual del sistema integral

MANUAL DEL SISTEMA DE GESTIÓN INTEGRAL				Clasificación: Interno Versión: 02 Fecha de última revisión: 29-03-24
Proveedores	Pagos Puntuales	Responsable del Servicio Gestor de Proveedores	Comprobantes de pago o transferencias Porcentaje de pagos realizados a tiempo	Satisfactorio
	Seguridad en las transacciones y comunicaciones con la empresa	Responsable de Seguridad de la Información	Índice de integridad en las transacciones Respuesta a solicitudes de información	Satisfactorio
	Cumplimiento contractual	Responsable del SGSI	Contratos vigentes Cero disputas contractuales Cero demandas	Satisfactorio
	Protección de la información personal proporcionada	Responsable en Seguridad de la Información	Respuesta a solicitudes de acceso o modificación de datos Cumplimiento con regulaciones de privacidad aplicables Acuerdos de confidencialidad	Satisfactorio
Colaboradores	Comunicación clara sobre seguridad de la información	Responsable en Seguridad de la Información	Conocimiento sobre Políticas de Seguridad Frecuencia de Comunicaciones sobre Seguridad Accesibilidad a Políticas y Procedimientos Canales de Comunicación Utilizados	Satisfactorio
	Protección de la información personal proporcionada	Oficial de Privacidad de Datos	Percepción de Confidencialidad Sesiones de Formación sobre Protección de Datos Cumplimiento con Normativas de Protección de Datos	Satisfactorio
	Comunicación clara y transparente	Gestor de recursos humanos	Número de canales de comunicación utilizados Índice de claridad en los objetivos organizacionales Número de noticias positivas comunicadas Actualizaciones de políticas y procedimientos comunicadas	Satisfactorio
Competencia	Ambiente de trabajo seguro y saludable	Gestor de seguridad física	Índice de colaboración en investigación y desarrollo ético Acuerdos de licencia y colaboración	Satisfactorio
	Respeto a la propiedad intelectual	Responsable en Seguridad de la Información	Colaboraciones éticas con competidores Número de quejas o denuncias de la competencia	Satisfactorio
	Acceso seguro a la información compartida	Responsable en Seguridad de la Información	Evaluación de la capacidad técnica para el acceso seguro Actualizaciones de seguridad en la información compartida Nivel de confianza de la competencia en las prácticas de acceso	Satisfactorio
	Competencia justa	Responsable del servicio	Índice de participación en investigación y desarrollo Número de colaboraciones exitosas con otras empresas	Satisfactorio

Figura 37 Matriz de partes interesadas del manual del sistema integral

MANUAL DEL SISTEMA DE GESTIÓN INTEGRAL				Clasificación: Interno Versión: 02 Fecha de última revisión: 29-03-24
Socios	Cumplimiento de estándares de seguridad informática	Responsable en Seguridad de la Información	Cumplimiento con estándares de seguridad informática Acuerdos de seguridad informática	Satisfactorio
	Transparencia en la comunicación	Responsable del servicio	Colaboraciones en investigación y desarrollo Iniciativas innovadoras colaborativas	Satisfactorio
Autoridades	Cumplimiento de normativas y regulaciones	Responsable del SGSI	Informes presentados antes del plazo Revisiones o correcciones requeridas Sesiones de revisión de documentos	Satisfactorio
	Presentación oportuna de informes y documentos	Representante de la Dirección Responsable del SGSI Responsable en Seguridad de la Información	Cumplimiento con estándares de seguridad de la información en la presentación de informes Exactitud de la información presentada	Satisfactorio
	Protección de la información personal proporcionada	Responsable en Seguridad de la Información	Número de Incidentes de seguridad que involucran información personal Índice de Accesibilidad no autorizada a información personal Promedio de notificación de brechas de seguridad	Satisfactorio

Figura 38 Matriz de partes interesadas del manual del sistema integral

Se define en el Ma_Sistema de Gestión Integrado (SGI)_V01 una política para la revisión del Sistema de gestión Integral y toda la documentación relacionada a el de manera periódica en la revisión por dirección la cual se hace al menos 1 ves al año.

MANUAL DEL SISTEMA DE GESTIÓN INTEGRAL

Clasificación: Interno
 Versión: 02
 Fecha de última revisión:
 29-03-24

Dirección.

Sistema de Gestión Integral/Procesos del Sistema de Gestión (PSG)/Evaluación y Mejora del SGI /Procedimientos/Revisión por la Dirección

REVISIÓN POR LA DIRECCIÓN

La Alta Dirección revisa periódicamente el SGI mediante el procedimiento **Pr_Revisión por la Dirección** para asegurar su conveniencia, adecuación y eficacia continua. La revisión incluye la evaluación de oportunidades de mejora y la necesidad de efectuar cambios en el SGI, incluyendo la política y los objetivos.

Entradas de la revisión por la dirección

La información de entrada para la revisión por la alta dirección incluye:

- a) Resultados de auditorías internas y/o externas;
- b) Los cambios en las cuestiones externas e internas que sean pertinentes al SGI
- c) Información sobre el desempeño y la eficacia del SGI
- d) Satisfacción del cliente
- e) El grado en que se han logrado los objetivos
- f) Desempeño de los procesos y la conformidad del producto
- g) Resultados de seguimiento y medición
- h) Desempeño de los proveedores externos
- i) La adecuación de los recursos
- j) La eficacia de las acciones para abordar riesgos y las oportunidades
- k) Acciones de seguimiento de revisiones por la dirección previas
- l) Las oportunidades de mejora.

Figura 39 Política de partes interesadas del manual del sistema integral

4.1.1.3.2.2 Plan de acción: Contacto con autoridades

1. Datos generales de la acción

Tabla 200 Datos generales plan de acción 161

Folio	161	Fecha de registro	18-mar-24
Tipo de Acción	Correctiva ☒ Preventiva ☐ Mejora ☐	Prioridad	Baja ☐ Media ☐ ☒ Alta ☐
Derivada de	Auditoría interna ☒ Auditoría externa ☐ De la operación ☐ Queja ☐ Problema ☐ Sugerencia ☐ Revisión por la dirección ☐		

2. Descripción del hallazgo

Tabla 201 Descripción del hallazgo plan de acción 161

Requisito Normativo Documento(s), y/o activo afectado	Descripción del hallazgo o Problema
A.6.1.3 Contacto con Autoridad	Se muestra el "Re_Matriz contacto autoridades_2023" actualizado el 23 de agosto del 2023 en el cual solo se incluyen a los grupos de interés especiales.

3. Análisis de causa raíz

Lluvia de idea

- Identificar autoridades relevantes para la organización
- Agregar una sección específica al documento para las autoridades relevantes

4. Plan de acción

Tabla 202 Plan de acción 161

Descripción breve de la acción a realizar		Documentar autoridades relevantes para la organización		
Objetivo / Meta		Identificar y mantener disponible la información de las autoridades relevantes para la organización disponible a los colaboradores		
No.	Actividad	Fecha de compromiso		Responsables (Iniciales)
		Inicio	Fin	
1	Identificar autoridades	18-mar-24	19-mar-24	GMJ LVGG
2	Completar la matriz	20-mar-24	21-mar-24	GMJ LVGG
3	Definir revisión periódica	22-mar-24	22-mar-24	GMJ LVGG

5. Evaluación del plan de acción

Tabla 203 Evaluación del plan de acción 161

Estatus	Aprobada ☒ Rechazada ☐	La acción fue rechazada por qué:
----------------	---	---

6. Eficacia de la acción realizada

Tabla 204 Eficacia del plan de acción 161

La acción realizada se consideró	Eficaz ☒ Ineficaz ☐	¿Por qué?	Se cumplió el objetivo
El nivel de eficacia de la acción fue	Alto ☒ Medio ☐ Bajo ☐	¿Por qué?	Se cumplieron las actividades en tiempo y forma según lo planificado
Grado de cumplimiento contra el objetivo o meta establecida			Alto ☒ Medio ☐ Bajo ☐
Fecha de Cierre	22-mar-24		

7. Resultados

Se muestra la portada del documento la cual solo cuenta con el nombre del documento, clasificación, fecha de última actualización y a que corresponde la última versión generada, en este caso es un documento actualizado el 22/03/2024.

Clasificación:	Interno	Matriz de contacto con autoridades
Fecha de ultima revisión:	22/03/2024	
Matriz de contacto con autoridades		
Control de cambios		
Versión	Fecha	Descripción
1	23/08/2023	Documento de nueva creación
2	22/03/2024	Se agregan los contactos de las autoridades

Figura 40 Portada del registro matriz de contacto con autoridades

El documento Re_Matriz contacto autoridades_2024" cuanta con 3 pestañas en el libro:

- Control de documentos
- Autoridades
- Grupos de interés

Control de documentos	Autoridades	Grupos especiales
Accesibilidad: es necesario investigar		

Figura 41 Pestañas del registro matriz de contacto con autoridades

La matriz de contacto con autoridades se encuentra llena y con los datos actualizados.

	A	B	C	D	E
1	Clasificación:	Interno	Matriz de contacto con autoridades		
2	Fecha de última revisión:	23/08/2023			
3					
4	A fin de comunicar la información del SGI que es de interés para las partes interesadas, la Dirección General determina la siguiente matriz de comunicación:				
5					
6	Tema	Audiencia	Medio(s)	Periodo de difusión	Responsable(s)
7	¿Qué comunicar?	¿A quién comunicar?	¿Cómo comunicar?	¿Cuándo comunicar?	¿Quién comunica?
8	Emergencias médicas y primeros auxilios.	Cruz roja	Teléfono	Evento	RH
9	Campañas de donación de sangre.				
10	Capacitaciones en atención médica de emergencia.				
11	Incendios estructurales y forestales.	Bomberos	Teléfono	Evento	RH
12	Rescates en casos de accidentes vehiculares.				
13	Prevención de incendios y seguridad en el hogar.				
14	Servicios de emergencia y atención ciudadana.	Locatel	Teléfono	Evento	RH
15	Información sobre trámites y servicios gubernamentales.				
16	Notificaciones de situaciones de riesgo o emergencia en la ciudad.				
17	Derechos de acceso a la información pública.	INAI	Teléfono Correo	Informativo Petición	Finanzas
18	Procedimientos de protección de datos personales.				
19	Transparencia gubernamental y rendición de cuentas.				
20	Certificación de productos y servicios conforme a normativas mexicanas.	NYCE	Teléfono Correo	Informativo Petición	Finanzas
21	Evaluación de conformidad y calidad.				
22	Promoción de estándares y normativas para el desarrollo industrial.				
23	Política económica y fiscal del gobierno.	SHCP	Teléfono Correo	Informativo Petición	Finanzas
24	Presupuesto y finanzas públicas.				
25	Impuestos y regulaciones financieras.				
26					
Control de documentos Autoridades Grupos especiales + : 4					

Figura 42 Matriz de contacto con autoridades

4.1.1.3.2.3 Plan de acción: Seguridad en los proyectos

1. Datos generales de la acción

Tabla 205 Datos generales plan de acción 162

Folio	162	Fecha de registro	19-mar-24
Tipo de Acción	Correctiva ☒ Preventiva ☐ Mejora ☐	Prioridad	Baja ☐ Media ☐ Alta ☒
Derivada de	Auditoría interna ☒ Auditoría externa ☐ De la operación ☐ Queja ☐ Problema ☐ Sugerencia ☐ Revisión por la dirección ☐		

2. Descripción del hallazgo

Tabla 206 Descripción del hallazgo plan de acción 162

Requisito Normativo Documento(s), y/o activo afectado	Descripción del hallazgo o Problema
A.6.1.5 Seguridad de la Información en la Administración de Proyectos	Se muestra el "Fo_Implementación de servicio_V04" actualizado el 25 de mayo del 2023 el cual considera endpoint para infonavit, en el documento se aprecia que se consideran los riesgos del proyecto. Se muestra evidencia del proyecto "Re_plan de trabajo_Instalación de memorias RAM y discos duros en servidores" generado el 31 de octubre del 2023, En este caso, la documentación carece de la identificación de riesgos asociados al proyecto, lo cual constituye una deficiencia que requiere atención y corrección inmediata. Es esencial que la organización considere los riesgos en todos sus proyectos, tanto internos como externos. La gestión proactiva de riesgos es fundamental para anticipar obstáculos, tomar medidas preventivas y asegurar el éxito de los proyectos.

3. Análisis de causa raíz

Lluvia de ideas

- Actualizar el formato de evaluación de proyectos agregando la relación con los riesgos
- Volver a evaluar los proyectos que se encuentren en proceso

- Evaluar los proyectos que inicien

4. Plan de acción

Tabla 207 Plan de acción 162

Descripción breve de la acción a realizar		Realizar una actualización al formato de evaluación de los nuevos proyectos y evaluar los proyectos mas recientes		
Objetivo / Meta		Evaluar los proyectos adecuadamente		
No.	Actividad	Fecha de compromiso		Responsables (Iniciales)
		Inicio	Fin	
1	Actualizar formato	19-mar-24	19-mar-24	GMA LVGG
2	Evaluar los proyectos agregando los riesgos	20-mar-24	22-mar-24	LUC LVGG

5. Evaluación del plan de acción

Tabla 208 Eficacia del plan de acción 162

Estatus	Aprobada ☒ Rechazada ☐	La acción fue rechazada por qué:
----------------	---	---

6. Eficacia de la acción realizada

Tabla 209 Eficacia del plan de acción 162

La acción realizada se consideró	Eficaz ☒	¿Por qué?	Se cumplió el objetivo
	Ineficaz ☐		
El nivel de eficacia de la acción fue	Alto ☒	¿Por qué?	Se cumplieron las actividades en tiempo y forma según lo planificado
	Medio ☐		
	Bajo ☐		

Grado de cumplimiento contra el objetivo o meta establecida	Alto ☒ Medio ☐ Bajo ☐
Fecha de Cierre	22-mar-24

7. Resultados

Se muestra la portada del documento la cual cuenta con la clasificación, fecha de última revisión, control de cambi6n en la cual se especifica que la última versi6n es la actualizaci6n generada para la consideraci6n de los riesgos en la evaluaci6n de los nuevos proyectos

A		B		C		D		E		F		G		H	
Clasificación:		Interno		Evaluación de nuevos proyectos											
Fecha de ultima revisión:		25/05/2023													
Evaluación de nuevos proyectos															
Control de cambios															
Versión		Fecha		Descripción											
1		24/08/2020		Documento de nueva creación											
2		19/07/2021		Revisión de idoneidad											
3		14/05/2022		Revisión de idoneidad											
4		25/05/2023		Revisión de idoneidad											
5		22/03/2024		Se agregan los contactos de las autoridades											

Figura 43 Portada del documento evaluaci6n de nuevos proyectos

Se agrego el apartado de evaluaci6n de riesgos en el formato por lo que la nueva estructura del formato es:

- Descripci6n del proyecto
 - Nombre del proyecto
 - Objetivos
- Riesgos

- Actividades
- Resultado

1		
2	Definición del proyecto	
3	Nombre del proyecto	
4	Objetivos	
5		
6	Riesgos	
7		
8		
9		
0		
1		
2		
3		
4		
5		
6		
7	Actividades	
8		
9		
0		
1		
2		
3		
4		
5		
6		
7		
8		
9		
0		
1		
2	Resultado	
3		
4		

◀ ▶
ID Documento
Instrucciones
Eval proyecto
⊕

Figura 44 Formato actualizado de evaluación de nuevos proyectos

Se realizó la evaluación del proyecto más reciente considerando los riesgos que implica la ejecución de este proyecto, las actividades a realizar con una breve descripción de cada una de ellas y no cuenta con resultados ya que el proyecto se encuentra en proceso.

Definición del proyecto	
Nombre del proyecto	Instalación de memorias RAM y discos duros en servidores
Objetivos	1.-Instalación de memorias RAM
	2.-Instalación de discos duros en servidores
Riesgos	
Descarga eléctrica: Manipular componentes electrónicos, como memorias RAM y discos duros, puede aumentar el riesgo de descargas eléctricas si no se toman las precauciones adecuadas, como usar una pulsera antiestática o tocar una superficie metálica para descargar cualquier electricidad estática acumulada en el cuerpo.	
Daño por estática: La electricidad estática puede dañar los componentes sensibles de la memoria RAM y los discos duros. Es crucial manipular los componentes con cuidado y evitar tocar los contactos dorados con los dedos.	
Daño físico: Durante la instalación, existe el riesgo de dañar los componentes si se manejan de forma brusca o si se aplican fuerzas indebidas al insertarlos en los slots o compartimentos.	
Compatibilidad: Existe el riesgo de incompatibilidad entre la nueva memoria RAM o los discos duros y el servidor, lo que podría resultar en un mal funcionamiento o fallos del sistema.	
existe el riesgo de pérdida de datos en caso de errores durante el proceso de instalación o si los nuevos dispositivos no funcionan correctamente.	
Interferencia electromagnética: La manipulación de componentes electrónicos en un entorno no adecuado puede exponerlos a interferencias electromagnéticas que podrían afectar su funcionamiento.	
Error humano: Los errores durante la instalación, como insertar la memoria RAM o los discos duros en la dirección incorrecta o en el slot equivocado, pueden causar problemas de rendimiento o daños en el hardware.	
Sobrecalentamiento: La instalación de nuevos componentes, especialmente si aumenta la carga de trabajo del servidor, podría provocar un aumento en la temperatura interna del sistema, lo que podría afectar negativamente al rendimiento y la fiabilidad.	
Configuración incorrecta: Si los nuevos componentes no se configuran correctamente después de la instalación, podrían no funcionar según lo esperado o podrían causar problemas de compatibilidad con otros dispositivos o aplicaciones.	
Riesgos de seguridad física: Durante el proceso de instalación, existe el riesgo de lesiones personales debido a cortes, atrapamientos o caídas si no se manejan adecuadamente herramientas o equipos pesados.	
Actividades	
1. Preparación:	
Antes de comenzar, asegúrate de tener las herramientas adecuadas, como destornilladores, guantes antiestáticos (para evitar dañar los componentes con electricidad estática), y las nuevas memorias RAM o discos duros que deseas instalar.	
Apaga completamente el servidor y desconéctalo de la corriente eléctrica.	
2. Acceso al servidor:	
Abre la carcasa del servidor. Esto generalmente se hace quitando los paneles laterales o deslizando una cubierta según el diseño del servidor. Consulta el manual del usuario del servidor si no estás seguro de cómo acceder a su interior.	
3. Localización de los slots de memoria y de los compartimentos de los discos duros:	
Identifica los slots de memoria RAM vacíos en la placa base del servidor. Por lo general, están ubicados cerca del procesador o en un área designada en la placa base.	
Localiza los compartimentos de los discos duros en el chasis del servidor. Pueden ser unidades de disco duro de 3.5 pulgadas o 2.5 pulgadas, dependiendo del servidor.	
4. Instalación de memoria RAM:	
Retira las memorias RAM viejas si es necesario. Presiona los clips en ambos lados de los módulos de RAM para liberarlos y sácalos cuidadosamente de sus ranuras.	
Toma las nuevas memorias RAM y alinea cuidadosamente las muescas en el conector de la memoria con las clavijas correspondientes en el slot de memoria del servidor.	
◀ ▶ ID Documento Instrucciones Eval proyecto +	

Figura 45 Evaluación del proyecto "Instalación de memorias RAM y discos duros en servidores"

4.1.1.3.2.4 Plan de acción: Derechos ARCO

1. Datos generales de la acción

Tabla 210 Datos generales plan de acción 163

Folio	163	Fecha de registro	22-mar-24
Tipo de Acción	Correctiva ☒ Preventiva ☐ Mejora ☐	Prioridad	Baja ☐ Media ☒ Alta ☐
Derivada de	Auditoría interna ☒ Auditoría externa ☐ De la operación ☐ Queja ☐ Problema ☐ Sugerencia ☐ Revisión por la dirección ☐		

2. Descripción del hallazgo

Tabla 211 Descripción del hallazgo plan de acción 163

Requisito Normativo	Descripción del hallazgo o Problema
Documento(s), y/o activo afectado	
A.7.3.1 Responsabilidades en la terminación o cambio de empleo	Se evidencia la baja de Gabriel Arcega Soto, documentada con la conformación del expediente de baja, el cual incluye diversos elementos como renuncia, baja del biométrico, solicitud de baja de activos, accesos físicos y lógicos, carta de asignación y devolución de activos, y aviso de privacidad. Asimismo, se presenta evidencia del cambio de puesto de Gabriel Arcega Soto, respaldado por la minuta de aprobación del cambio y el perfil de puestos firmado por la parte involucrada generados el 25 de octubre de 2023, sin embargo, no se encontró evidencia de que la organización haya comunicado y/o recordado las responsabilidades de Seguridad de la Información que permanecen vigentes, ni los derechos de ARCO (Acceso, Rectificación, Cancelación y Oposición)

	respecto a la desvinculación de los colaboradores.
--	--

3. Análisis de causa raíz

Lluvia de ideas

- Generar una carta de salida que trate de los derechos ARCO
- Solicitar la firma de los colaboradores sean despedidos o se retiren por renuncia

4. Plan de acción

Tabla 212 Plan de acción 163

Descripción breve de la acción a realizar		Desarrollar un formato para los colaboradores despedidos o que renuncien recordando sus derechos ARCO		
Objetivo / Meta		Generar un formato de salida para derechos ARCO		
No.	Actividad	Fecha de compromiso		Responsables (Iniciales)
		Inicio	Fin	
1	Generar formato	22-mar-24	22-mar-24	SGG LVGG

5. Evaluación del plan de acción

Tabla 213 Evaluación del plan de acción 163

Estatus	Aprobada ☒ Rechazada ☐	La acción fue rechazada por qué:
----------------	---	---

6. Eficacia de la acción realizada

Tabla 214 Evaluación del plan de acción 163

La acción realizada se consideró	Eficaz ☒	¿Por qué?	Se cumplió el objetivo
	Ineficaz ☐		
El nivel de eficacia de la acción fue	Alto ☒	¿Por qué?	Se cumplieron las actividades en tiempo y forma según lo planificado
	Medio ☐		

	Bajo ☐		
Grado de cumplimiento contra el objetivo o meta establecida			Alto ☒ Medio ☐ Bajo ☐
Fecha de Cierre	22-mar-24		

7. Resultados

Se muestra la carta de recordatorio de derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) la cual formara parte del paquete de documentación de finalización de la relacion laboral como formato el cual para llenarse se requiere de la siguiente información:

- Nombre del empleado o empleada
- Fecha de salida o cambio de puesto
- Firma del colaborador

Derechos ARCO

Estimado/a [Nombre del Colaborador]:

Por medio de la presente, queremos informarte sobre tus derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) en relación con tus datos personales que han sido recopilados y tratados durante tu empleo en SayNet Soluciones Integrales S.A. de C.V.

De acuerdo con la legislación de protección de datos aplicable, tienes derecho a:

- Acceder a los datos personales que tenemos sobre ti.
- Rectificar cualquier dato inexacto o incompleto.
- Cancelar tus datos personales cuando ya no sean necesarios para los fines que fueron recopilados.
- Oponerte al tratamiento de tus datos personales en ciertas circunstancias.

Si deseas ejercer alguno de estos derechos, por favor, verifica el aviso de privacidad publicado en la página. Estaremos encantados de atender tu solicitud.

Por favor, firma a continuación para confirmar que has recibido esta información y que estás al tanto de tus derechos ARCO.

Nombre: _____

Fecha: _____

Firma: _____

Te agradecemos por tu dedicación y contribución durante tu labor. Te deseamos mucho éxito en tus futuros proyectos.

Figura 46 Formato de carta de derechos ARCO

4.1.1.3.2.5 Plan de acción: Croquis de la organización

1. Datos generales de la acción

Tabla 215 Datos generales plan de acción 164

Folio	164	Fecha de registro	13-mar-24
Tipo de Acción	Correctiva ☒ Preventiva ☐ Mejora ☐	Prioridad	Baja ☐ Media ☐ Alta ☒
Derivada de	Auditoría interna ☒ Auditoría externa ☐ De la operación ☐ Queja ☐ Problema ☐ Sugerencia ☐ Revisión por la dirección ☐		

2. Descripción del hallazgo

Tabla 216 Descripción del hallazgo plan de acción 164

Requisito Normativo Documento(s), y/o activo afectado	Descripción del hallazgo o Problema
A.11.1.1 Perímetro de Seguridad Física	Se muestra el Ma_Seguridad de la organización_V01 fechado el 25 de mayo del 2023 pero no se identifican los controles implementados.

3. Análisis de causa raíz

Lluvia de ideas

- Identificar extintores
- Identificar los detectores de humo
- Identificar los controles de la organización
- Señalética
- Cámaras de vigilancia

4. Plan de acción

Tabla 217 Plan de acción 164

Descripción breve de la acción a realizar		Identificar los controles de seguridad de la organización y actualizar el croquis con esta información		
Objetivo / Meta		Identificar en el croquis los controles de seguridad		
No.	Actividad	Fecha de compromiso		Responsables (Iniciales)
		Inicio	Fin	
1	Identificar los controles físicos de accesos	13-mar-24	20-mar-23	MRG LVGG
2	Identificar las zonas seguras	13-mar-24	20-mar-23	MRG LVGG
3	Identificar las señaléticas	13-mar-24	20-mar-23	MRG LVGG
4	Identificar las zonas de carga y descarga	13-mar-24	20-mar-23	MRG LVGG
5	Identificar los detectores de humo y/o extintores	13-mar-24	20-mar-23	MRG LVGG
6	Documentar el nuevo croquis incluyendo los elementos identificados	20-mar-24	29-mar-24	MRG LVGG

5. Evaluación del plan de acción

Tabla 218 Evaluación del plan de acción 164

Estatus	Aprobada ☒ Rechazada ☐	La acción fue rechazada por qué:
----------------	---	---

6. Eficacia de la acción realizada

Tabla 219 Eficacia del plan de acción 164

La acción realizada se consideró	Eficaz ☒	¿Por qué?	Se cumplió el objetivo
	Ineficaz ☐		

El nivel de eficacia de la acción fue	Alto ☒ Medio ☐ Bajo ☐	¿Por qué?	Se cumplieron las actividades en tiempo y forma según lo planificado
Grado de cumplimiento contra el objetivo o meta establecida			Alto ☒ Medio ☐ Bajo ☐
Fecha de Cierre	29-mar-24		

7. Resultados

Se muestra el Ma_Sistema de Gestión Integrado (SGI)_V02 actualizado el 29 de marzo del 2024



Figura 47 Portada del manual de sistema de gestión integral

Se Muestra el croquis actualizado en donde se puede identificar los controles de seguridad con los que cuenta la organización:

- Biométricos
- Accesos
- Cámaras
- Detector de humo
- Extintor



Figura 48 Croquis oficina 11 actualizado

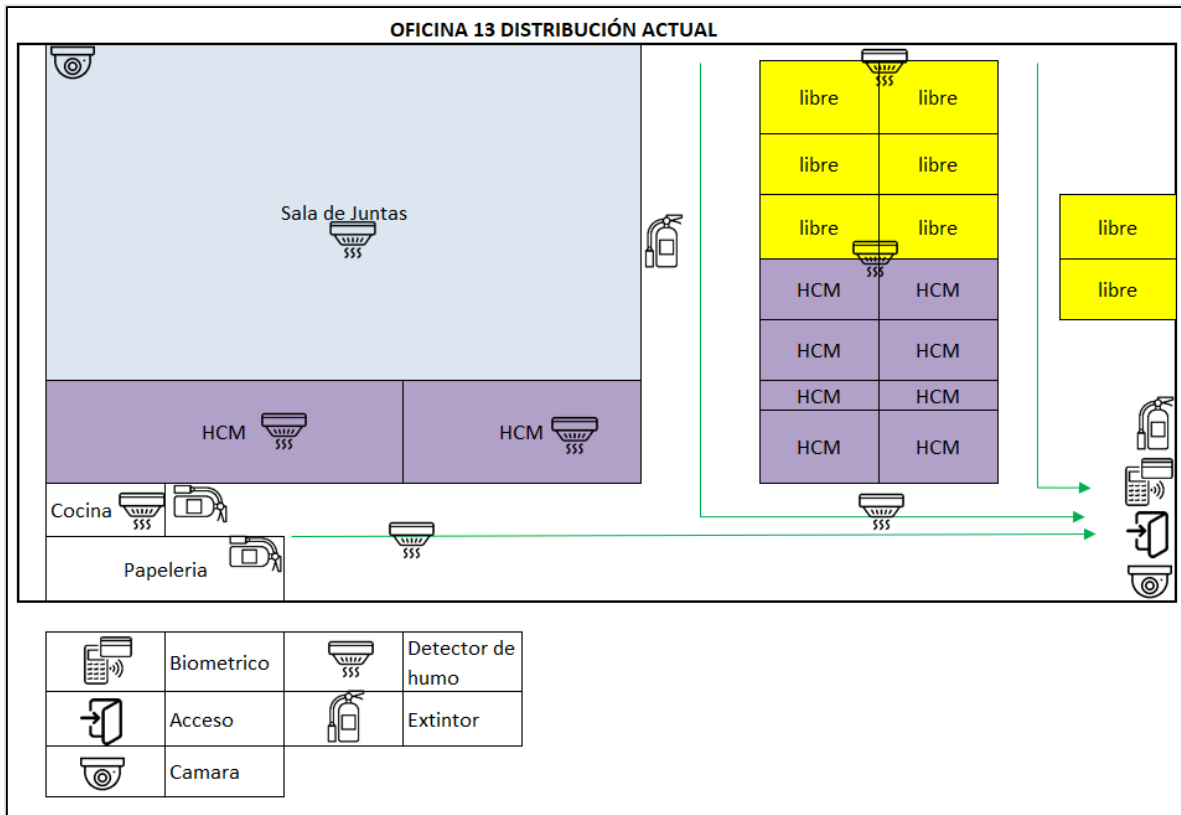


Figura 49 Croquis oficina 13 actualizado

4.1.1.3.2.6 Plan de acción: Gestión del cambio

1. Datos generales de la acción

Tabla 220 Datos generales plan de acción 165

Folio	165	Fecha de registro	17-mar-24
Tipo de Acción	Correctiva ☒ Preventiva ☐ Mejora ☒	Prioridad	Baja ☐ Media ☒ Alta ☐
Derivada de	Auditoría interna ☒ Auditoría externa ☐ De la operación ☐ Queja ☐ Problema ☒ Sugerencia ☐ Revisión por la dirección ☐		

2. Descripción del hallazgo

Tabla 221 Descripción del hallazgo plan de acción 165

Requisito Normativo	Descripción del hallazgo o Problema
---------------------	-------------------------------------

Documento(s), y/o activo afectado	
A.12.1.2 Gestión del Cambio	Se cuenta con un Pr_Gestión del cambio_V01 fechado el 19 de mayo del 2023 que incluye los x solicitados por el requisito. Tipos de cambio: estándar, normal y emergente No ha habido cambios internos. Se muestra Aranda, herramienta utilizada para gestionar los cambios a la infraestructura o los cambios en los servicios. Se muestra Re_Caso no. 63 / CHG8268-1-63 fechado el 17 de marzo del 2023 por Saul Gomez del cliente Secretaría de Turismo, se observa debidamente requisitos a la solicitud de cambio, misma que se anexa al caso creado. En Criterios de impacto: en la tabla de tipos de cambio se describen los impactos sin embargo no existe un criterio que sea compatible con lo configurado en la herramienta de Aranda.

3. Análisis de causa raíz

Lluvia de ideas

- Falta de comunicación entre los equipos de gestión del cambio y los usuarios finales.

- Posible falta de capacitación sobre cómo configurar criterios de impacto en la herramienta de Aranda.
- Desconocimiento de la importancia de tener criterios de impacto compatibles en la herramienta.
- Problemas técnicos o limitaciones de la herramienta que impiden la configuración adecuada de los criterios de impacto.

4. Plan de acción

Tabla 222 Plan de acción 165

Descripción breve de la acción a realizar		Revisión y reforzamiento de los procedimientos de respaldo de datos.		
Objetivo / Meta		Garantizar que los respaldos de datos se realicen de manera adecuada y se registren correctamente en la bitácora correspondiente, reduciendo así los riesgos para la integridad y disponibilidad de la información de la organización.		
No.	Actividad	Fecha de compromiso		Responsables (Iniciales)
		Inicio	Fin	
1	Realizar una revisión detallada del documento Pr_Gestión del cambio_V01 y la configuración actual de la herramienta Aranda para identificar discrepancias entre los tipos de cambio especificados y los criterios de impacto configurados.	17-mar-2024	18-mar-2024	MYG BIGS
2	Modificar los criterios de impacto en la herramienta Aranda para que sean compatibles con los tipos de cambio especificados en el	19-mar-2024	21-mar-2024	MYG BIGS

	documento Pr_Gestión del cambio_V01.			
3	Realizar pruebas exhaustivas para asegurar que los cambios en los criterios de impacto se hayan implementado correctamente y sean efectivos	22-mar-2024	24-mar-2024	MYG BIGS
4	Actualizar el documento Pr_Gestión del cambio_V01 con los cambios realizados en los criterios de impacto y comunicar estos cambios al equipo relevante.	25-mar-2024	27-mar-2024	MYG BIGS
5	Realizar una revisión posterior a la implementación para asegurar que los cambios se hayan realizado de manera efectiva y para identificar cualquier ajuste adicional necesario.	27-mar-2024	28-mar-2024	MYG BIGS

5. Evaluación del plan de acción

Tabla 223 Evaluación del plan de acción 165

Estatus	Aprobada ☒ Rechazada ☐	La acción fue rechazada por qué:
----------------	---	---

6. Eficacia de la acción realizada

Tabla 224 Eficacia del plan de acción 165

La acción realizada se consideró	Eficaz ☒ Ineficaz ☐	¿Por qué?	Se cumplió el objetivo
---	---	------------------	------------------------

El nivel de eficacia de la acción fue	Alto	☒	¿Por qué?	Se cumplieron las actividades en tiempo y forma según lo planificado
	Medio	☐		
	Bajo	☐		
Grado de cumplimiento contra el objetivo o meta establecida				Alto ☒ Medio ☐ Bajo ☐
Fecha de Cierre	28-mar-2024			

7. Resultados

Se muestra el Pr_Gestión de cambio_V02 actualizado el 28 de marzo del 2024

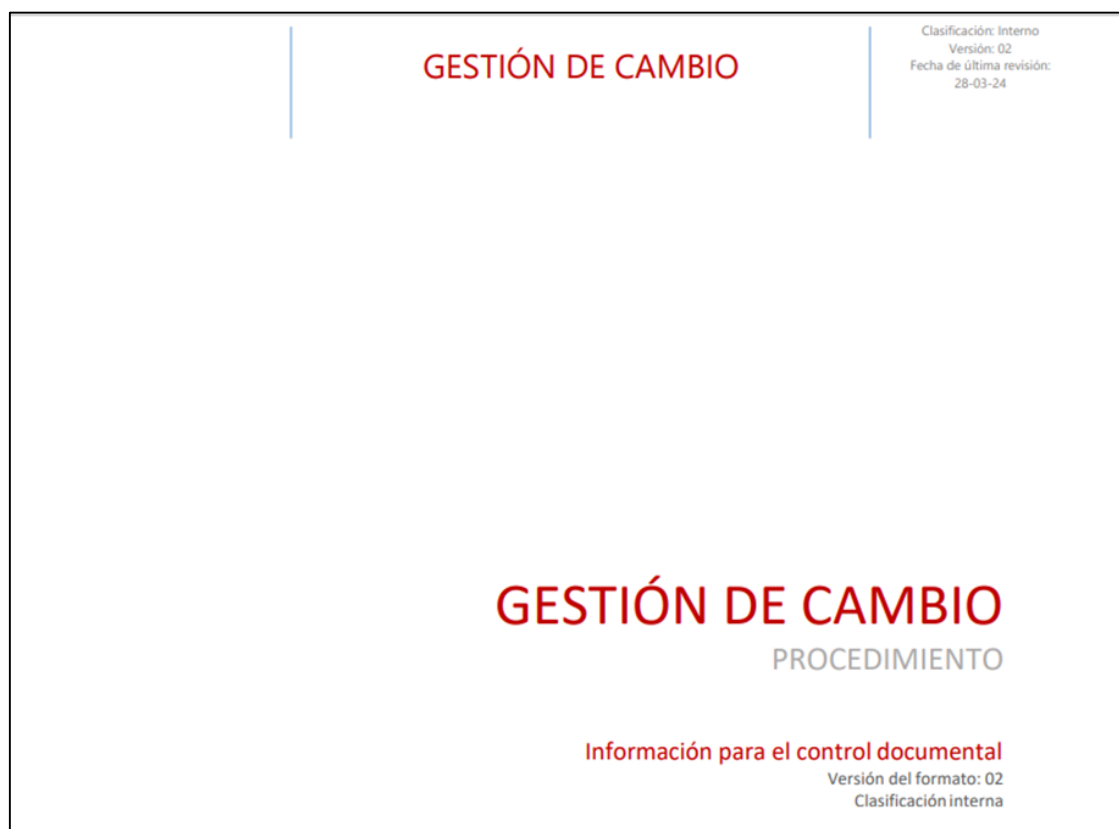


Figura 50 Portada procedimiento gestión del cambio

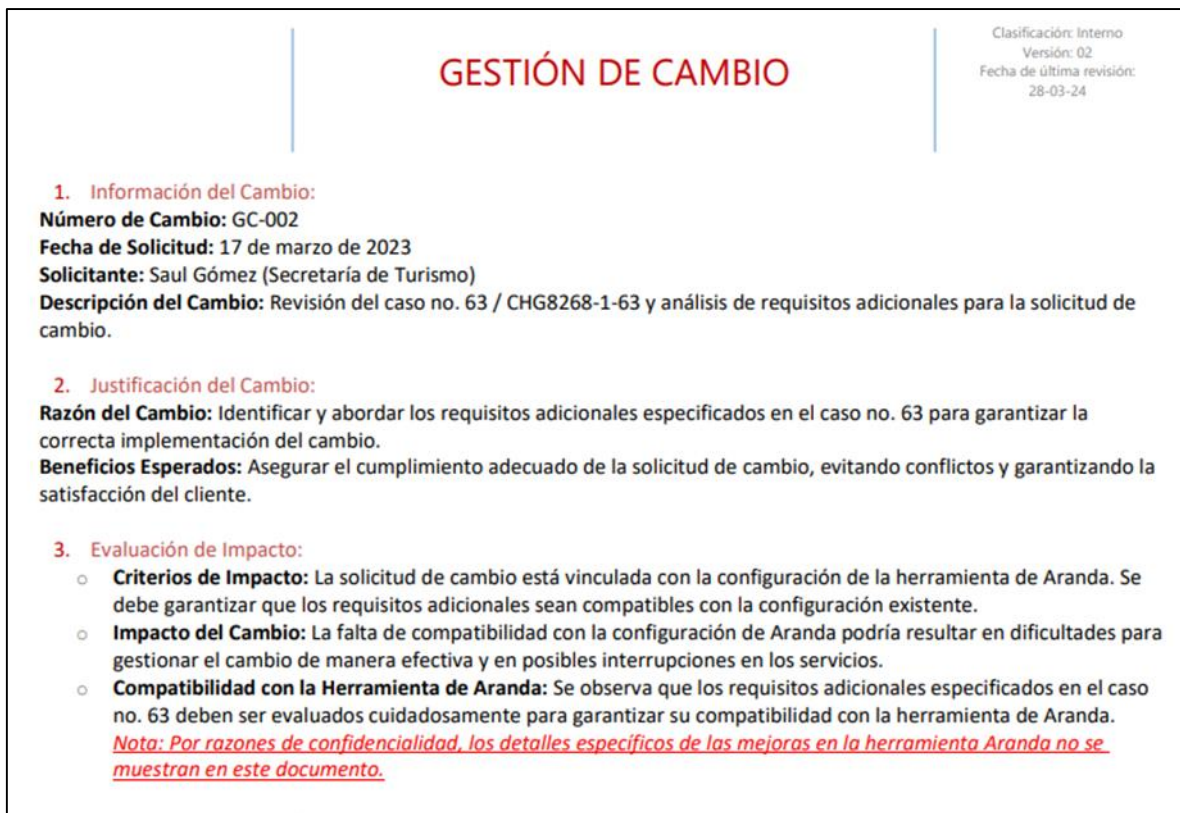


Figura 51 Procedimiento gestión del cambio

Se muestra el procedimiento gestión del cambio donde se menciona la fecha de solicitud se muestra la justificación del cambio donde nos ayuda a abordar los requisitos adicionales, se muestra la evaluación del impacto donde se toman en cuenta los criterios el impacto y la compatibilidad.

4. Plan de Implementación:
Fecha de Implementación Propuesta: 25 de marzo de 2023
Recursos Necesarios: Personal técnico para revisar los requisitos adicionales y ajustar la configuración de la herramienta de Aranda si es necesario.
Procedimiento de Implementación: Seguir el plan de acción propuesto, que incluye la revisión detallada de los requisitos adicionales y el ajuste de la configuración de Aranda según sea necesario para garantizar la compatibilidad.

5. Riesgos y Mitigaciones:
Riesgos Asociados: Posibles conflictos con la configuración existente de Aranda, interrupciones en los servicios si no se abordan adecuadamente los requisitos adicionales.
Estrategias de Mitigación: Realizar pruebas exhaustivas antes de implementar los cambios en la configuración de Aranda, comunicar cualquier interrupción planificada a los usuarios afectados.

6. Aprobación del Cambio:
Responsable de Aprobación: [REDACTED]
Fecha de Aprobación: 25/03/24
Observaciones: Pendiente de aprobación una vez que se revise la evaluación de impacto y el plan de implementación.

7. Implementación del Cambio:
Responsable de Implementación: [REDACTED]
Fecha de Implementación: 26/03/24
Resultados de la Implementación: Los resultados de la implementación se registrarán una vez que se complete el proceso.

8. Seguimiento y Evaluación Post-Implementación:
Revisión de Efectividad: Se realizará una revisión posterior a la implementación para asegurar que los requisitos adicionales se hayan abordado correctamente y que la herramienta de Aranda siga funcionando sin problemas.

Figura 52 Procedimiento gestión del cambio

GESTIÓN DE CAMBIO

Clasificación: Interno
 Versión: 02
 Fecha de última revisión:
 28-03-24

Lecciones Aprendidas: Se documentarán las lecciones aprendidas durante todo el proceso de gestión de cambios para mejorar los procedimientos en el futuro.

Figura 53 Procedimiento gestión del cambio

4.1.1.3.2.7 Plan de acción: Respaldos

1. Datos generales de la acción

Tabla 225 Datos generales plan de acción 166

Folio	166	Fecha de registro	8-mar-24
--------------	-----	--------------------------	----------

Tipo de Acción	Correctiva ☒ Preventiva ☐ Mejora ☐	Prioridad	Baja ☐ Media ☐ Alta ☒
Derivada de	Auditoría interna ☒ Auditoría externa ☐ De la operación ☐ Queja ☐ Problema ☒ Sugerencia ☐ Revisión por la dirección ☐		

2. Descripción del hallazgo

Tabla 226 Descripción del hallazgo plan de acción 166

Requisito Normativo Documento(s), y/o activo afectado	Descripción del hallazgo o Problema
A.12.3.1 Respaldos de la Información	Se muestra una Re_Bitácora de respaldos fechada el día 8 de febrero del 2023, en la cual se identifica la realización de respaldos completos e incrementales para (ofimática, PRTG, Firewall, switch). Sin embargo, al revisar la bitácora detalladamente, se encuentra que no se han registrado respaldos para ninguna plataforma mencionada. Esta omisión representa un incumplimiento de los procedimientos establecidos para la realización de respaldos de datos, lo que podría generar riesgos significativos para la integridad y disponibilidad de la información de la organización. Por lo tanto, es necesario revisar y reforzar los procedimientos de respaldo de datos para garantizar que se realicen de manera adecuada y se registren correctamente en la bitácora correspondiente.

3. Análisis de causa raíz

Lluvia de Ideas:

- Falta de seguimiento adecuado a los procedimientos de respaldo.
- Posible falta de conciencia sobre la importancia de registrar correctamente los respaldos.
- Puede haber deficiencias en los procesos de documentación y registro de las actividades de respaldo.

4. Plan de acción

Tabla 227 Plan de acción 166

Descripción breve de la acción a realizar		Revisión y reforzamiento de los procedimientos de respaldo de datos.		
Objetivo / Meta		Garantizar que los respaldos de datos se realicen de manera adecuada y se registren correctamente en la bitácora correspondiente, reduciendo así los riesgos para la integridad y disponibilidad de la información de la organización.		
No.	Actividad	Fecha de compromiso		Responsables (Iniciales)
		Inicio	Fin	
1	Revisar los procedimientos actuales de respaldo de datos y compararlos con las prácticas recomendadas.	8-mar-2024	9-mar-2024	MGO BIGS
2	Actualizar y clarificar los procedimientos de respaldo de datos, incluyendo la obligación de registrar correctamente todas las actividades de respaldo.	10-mar-2024	11-mar-2024	MGO BIGS
3	Proporcionar capacitación sobre los procedimientos	12-mar-2024	13-mar-2024	MGO BIGS

	actualizados a todo el personal involucrado en la realización y registro de respaldos de datos.			
4	Implementar controles periódicos para asegurar el cumplimiento de los procedimientos de respaldo y registro.	14-mar-2024	15-mar-2024	MGO BIGS

5. Evaluación del plan de acción

Tabla 228 Evaluación del plan de acción 166

Estatus	Aprobada ☒ Rechazada ☐	La acción fue rechazada por qué:
----------------	---	---

6. Eficacia de la acción realizada

Tabla 229 Eficacia del plan de acción 166

La acción realizada se consideró	Eficaz ☒ Ineficaz ☐	¿Por qué?	Se cumplió el objetivo
El nivel de eficacia de la acción fue	Alto ☒ Medio ☐ Bajo ☐	¿Por qué?	Se cumplieron en tiempo y forma
Grado de cumplimiento contra el objetivo o meta establecida			Alto ☒ Medio ☐ Bajo ☐
Fecha de Cierre	15-mar-24		

7. Resultados

Se muestra el Re_Bitacora de respaldos actualizado el 15 de marzo del 2024

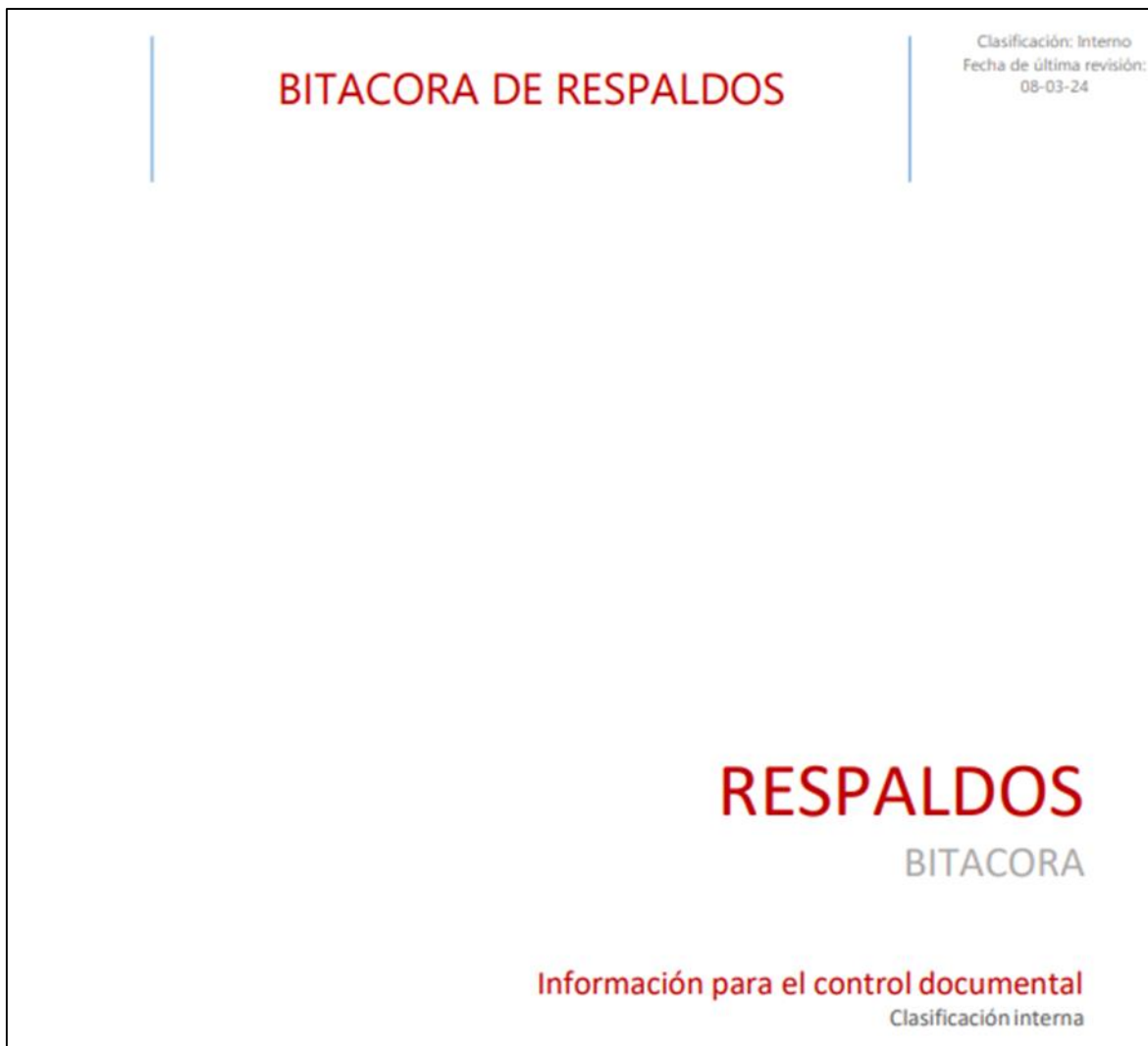


Figura 54 Portada bitácora de respaldos

Se muestra la bitacora de respaldos donde se implementa las plataformas se muestra el tipo de respaldo de cada una de esas plataformas se muestran las observaciones donde se menciona si se mostraron registros, así como las mejoras realizadas.

BITACORA DE RESPALDOS				
Clasificación: Interno Fecha de última revisión: Fecha: 8 de marzo de 2024				
1. Se realizó una revisión exhaustiva de los procedimientos de respaldo de datos para garantizar la integridad y disponibilidad de la información crítica de la organización.				
PLATAFORMA	TIPO DE RESPALDO	OBSERVACIONES	MEJORAS REALIZADAS	FORMATOS
				<i>Nota: Por motivos de confidencialidad, ciertos detalles específicos sobre los procedimientos y configuraciones no se muestran en este documento.</i>
Ofimática	Completo Incremental	No se encontraron registros de respaldos completos ni incrementales para la plataforma de ofimática. Esta omisión representa un riesgo importante para la pérdida de datos relacionados con documentos, hojas de cálculo y presentaciones esenciales para las operaciones diarias.	Se implementó un procedimiento automatizado para realizar respaldos completos e incrementales de los datos de la plataforma de ofimática, utilizando herramientas de respaldo de alta confiabilidad. Se estableció un proceso detallado para la gestión de respaldos, que incluye la programación regular de respaldos, la documentación de cada respaldo realizado, y la verificación periódica de la integridad de los datos respaldados.	Fo_ Registros electrónicos
PRTG	Completo Incremental	De manera similar, no se evidenciaron registros de respaldos para la plataforma de monitoreo PRTG. La falta de respaldos adecuados de esta plataforma podría comprometer la capacidad de monitoreo y diagnóstico de la infraestructura de red.	Se diseñó un proceso completo para respaldar tanto la configuración del sistema como los datos de monitoreo de la plataforma PRTG. Se implementó un sistema de alertas automatizadas para notificar cualquier interrupción en los respaldos programados, permitiendo una respuesta inmediata ante posibles problemas.	Re_ Mensajes correo electrónico o mensajes de texto.
Firewall	Configuración	No se registraron respaldos para la configuración del firewall. La ausencia	Se estableció un procedimiento automatizado para respaldar la	Re_ Cifrado protegidos por contraseña.

Figura 55 Bitácora de respaldos

Clasificación: Interno
 Fecha de última revisión:

		de estos respaldos implica un riesgo considerable en términos de seguridad de red, ya que cualquier interrupción no planificada podría resultar en una exposición no deseada a amenazas cibernéticas.	configuración del firewall de forma regular, utilizando herramientas de respaldo seguras y confiables. Se implementaron controles de acceso y seguridad estrictos para proteger los respaldos del firewall contra accesos no autorizados o manipulaciones indebidas.	
Switch	Configuración	Finalmente, no se encontraron registros de respaldos para la configuración del switch. Esta falta de respaldos podría afectar la conectividad y la gestión eficiente de la red, lo que potencialmente conllevaría a tiempos de inactividad no deseados.	Se diseñó un proceso detallado para respaldar la configuración del switch, que incluye la identificación de los archivos de configuración relevantes, la ejecución de los respaldos de forma programada, y la verificación de la integridad de los datos respaldados. Se establecieron políticas de retención de respaldos, definiendo claramente la duración y frecuencia de almacenamiento de los respaldos, así como los procedimientos para la eliminación segura de los respaldos obsoletos.	Fo_ Gestión de respaldos

1. Responsable de la revisión y reforzamiento de los procedimientos de respaldo de datos:

Nombre del responsable: [REDACTED]

Título/ posición: [REDACTED]

Fecha: 8 de febrero del 2023

2. Responsable de la revisión y reforzamiento de mejoras:

Nombre del responsable: [REDACTED]

Título/ posición: [REDACTED]

Fecha: 8 de marzo del 2024

Figura 56 Bitácora de respaldos

4.1.1.3.2.8 Plan de acción: Transferencia de información

1. Datos generales de la acción

Tabla 230 Datos generales plan de acción 167

Folio	167	Fecha de registro	11-mar-24
Tipo de Acción	Correctiva ☒ Preventiva ☐ Mejora ☐	Prioridad	Baja ☐ Media ☐ Alta ☒
Derivada de	Auditoría interna ☒ Auditoría externa ☐ De la operación ☐ Queja ☐ Problema ☒ Sugerencia ☐ Revisión por la dirección ☒		

2. Descripción del hallazgo

Tabla 231 Descripción del hallazgo plan de acción 167

Requisito Normativo Documento(s), y/o activo afectado	Descripción del hallazgo o Problema
A.13.2.1 Políticas y Procedimientos de Transferencia de Información	Se dispone de una Po_Convenios de Confidencialidad_V01, fechada el día 11 de julio de 2023. Sin embargo, no se cuenta con controles adecuados para proteger la transferencia de información.

3. Análisis de causa raíz

Lluvia de ideas

- Ausencia de controles adecuados para garantizar la protección de la información.
- Falta de procedimientos claros para supervisar y asegurar la transferencia segura de datos.
- Deficiencias en la implementación efectiva de la Po_Convenios de Confidencialidad_V01

4. Plan de acción

Tabla 232 Plan de acción 167

Descripción breve de la acción a realizar		Revisión y reforzamiento de los procedimientos de respaldo de datos.		
Objetivo / Meta		Garantizar que los respaldos de datos se realicen de manera adecuada y se registren correctamente en la bitácora correspondiente, reduciendo así los riesgos para la integridad y disponibilidad de la información de la organización.		
No.	Actividad	Fecha de compromiso		Responsables (Iniciales)
		Inicio	Fin	

1	Realizar una revisión exhaustiva de la Po_Convenios de Confidencialidad_V01 para identificar áreas de mejora y garantizar su total implementación.	11-mar-24	12-mar-24	JGG BIGS
2	Desarrollar e implementar procedimientos claros y efectivos para proteger la transferencia de información, incluyendo controles apropiados.	13-mar-24	15-mar-24	JGG BIGS
3	Proporcionar capacitación al personal pertinente sobre los nuevos procedimientos y la importancia de la protección de la información.	16-mar-24	17-mar-24	JGG BIGS
4	Establecer un sistema de seguimiento y monitoreo continuo para asegurar el cumplimiento de los controles y procedimientos establecidos	18-mar-24	19-mar-24	JGG BIGS
5	Realizar auditorías periódicas para evaluar la efectividad de las medidas implementadas y realizar ajustes según sea necesario.	20-mar-24	21-mar-24	JGG BIGS

5. Evaluación del plan de acción

Tabla 233 Evaluación del plan de acción 167

Estatus	Aprobada ☒ Rechazada ☐	La acción fue rechazada por qué:
----------------	---	---

6. Eficacia de la acción realizada

Tabla 234 Eficacia del plan de acción 167

La acción realizada se consideró	Eficaz ☒ Ineficaz ☐	¿Por qué?	Se cumplió el objetivo
El nivel de eficacia de la acción fue	Alto ☒ Medio ☐ Bajo ☐	¿Por qué?	Se cumplieron las actividades en tiempo y forma según lo planificado
Grado de cumplimiento contra el objetivo o meta establecida			Alto ☒ Medio ☐ Bajo ☐
Fecha de Cierre	21-mar-24		

7. Resultados

Se muestra el Po_Convenio de confidencialidad actualizado el 21 de marzo del 2024



Figura 57 Portada del convenio de confidencialidad

En la política convenio de confidencialidad se muestra el objetivo del por qué se está implementando la política, así mismo se implementaron protocolos de seguridad para la transferencia de información.

POLÍTICA CONVENIO DE CONFIDENCIALIDAD

Clasificación: Interno
Versión: 01
Fecha de última revisión:
11-07-23

ÍNDICE

01. OBJETIVO Y CAMPO DE APLICACIÓN.....	1
02. DEFINICIÓN DE INFORMACIÓN CONFIDENCIAL.....	1
03. CLASIFICACIÓN DE LA INFORMACIÓN.....	1
04. MEDIDAS DE SEGURIDAD PARA LA TRANSFERENCIA DE INFORMACIÓN.....	1
05. RECOMENDACIONES GENERALES.....	1
06. RIESGOS Y SANCIONES	2

Figura 58 índice convenio de confidencialidad

POLÍTICA CONVENIO DE CONFIDENCIALIDAD

Clasificación: Interno
Versión: 01
Fecha de última revisión:
11-07-23

01. OBJETIVO Y CAMPO DE APLICACIÓN

El propósito fundamental de esta política es establecer un marco integral para proteger la información confidencial de Saynet, salvaguardando su integridad, confidencialidad y disponibilidad. Esta política se aplica a todos los empleados, contratistas, proveedores y terceros que, de alguna manera, tengan acceso a información sensible perteneciente a la empresa.

02. DEFINICIÓN DE INFORMACIÓN CONFIDENCIAL

Se define como información confidencial cualquier dato, documento o material que, por su naturaleza, no está destinado al público en general y cuya divulgación no autorizada podría tener repercusiones adversas en los intereses comerciales, la reputación o la seguridad de la organización. Esto puede incluir, entre otros, datos financieros, estratégicos, de clientes, de empleados, y cualquier otro tipo de información sensible para la empresa.

03. CLASIFICACIÓN DE LA INFORMACIÓN

La información confidencial será clasificada en distintos niveles de sensibilidad, considerando tanto su contenido como el potencial impacto que su divulgación no autorizada podría ocasionar. Esta clasificación permitirá aplicar medidas de protección proporcionales a la importancia de la información, estableciendo criterios claros para la identificación, manejo y almacenamiento de cada tipo de dato confidencial.

04. MEDIDAS DE SEGURIDAD PARA LA TRANSFERENCIA DE INFORMACIÓN

Reconociendo la necesidad imperativa de garantizar la seguridad en la transferencia de información, se implementarán medidas adicionales para proteger la confidencialidad de los datos durante su transmisión. Entre estas medidas se incluyen:

Figura 59 Convenio de confidencialidad

- **Protocolos de encriptación robustos:** Se establecerán protocolos de encriptación avanzados para asegurar que la información confidencial se transmita de manera segura, impidiendo su acceso no autorizado durante el tránsito.
- **Autenticación de usuarios:** Se aplicarán sistemas de autenticación de usuarios para verificar la identidad de los destinatarios autorizados antes de permitir la transferencia de información confidencial, garantizando que solo las personas autorizadas puedan acceder a los datos.
- **Capacitación del personal:** Se llevarán a cabo capacitaciones periódicas para el personal en materia de políticas y procedimientos de seguridad de la información, con un enfoque específico en la transferencia segura de datos, promoviendo una cultura de seguridad dentro de la organización.
- **Herramientas tecnológicas avanzadas:** Se promoverá el uso de herramientas tecnológicas avanzadas que permitan monitorear y controlar el flujo de información confidencial dentro y fuera de la organización, detectando y mitigando posibles amenazas a la seguridad de los datos durante la transmisión.

05. RECOMENDACIONES GENERALES

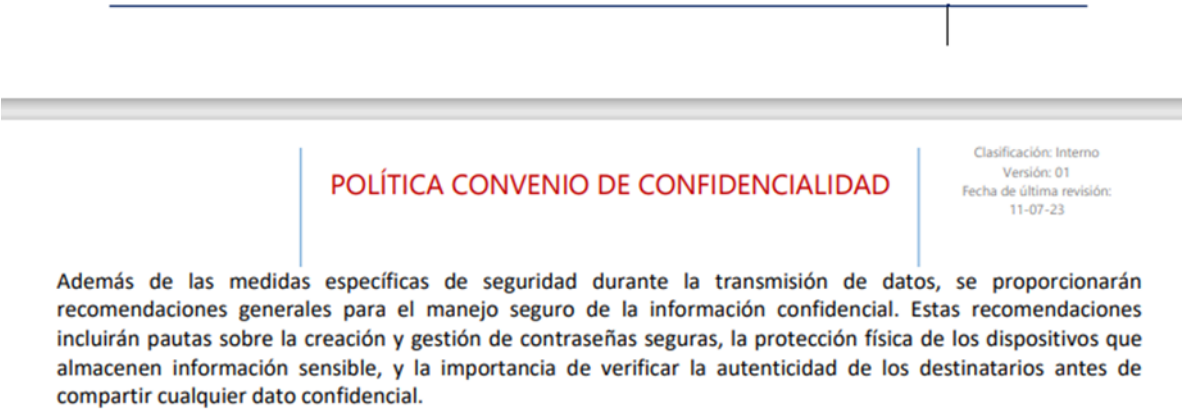


Figura 60 Convenio de confidencialidad

06. RIESGOS Y SANCIONES

Se llevará a cabo una evaluación exhaustiva de los riesgos asociados con la divulgación no autorizada de información confidencial, y se establecerán las sanciones correspondientes para aquellos individuos que incumplan con esta política. Estas sanciones pueden incluir medidas disciplinarias internas, así como acciones legales en casos de infracciones graves que puedan comprometer la seguridad y la reputación de la empresa.

Figura 61 Convenio de confidencialidad

4.1.1.3.2.9 Plan de acción: Seguridad de la información

1. Datos generales de la acción

Tabla 235 Datos generales plan de acción 168

Folio	168	Fecha de registro	2-mar-24
-------	-----	-------------------	----------

Tipo de Acción	Correctiva ☒ Preventiva ☐ Mejora ☐	Prioridad	Baja ☐ Media ☐ Alta ☒
Derivada de	Auditoría interna ☒ Auditoría externa ☐ De la operación ☐ Queja ☐ Problema ☒ Sugerencia ☐ Revisión por la dirección ☐		

2. Descripción del hallazgo

Tabla 236 Descripción del hallazgo plan de acción 168

Requisito Normativo Documento(s), y/o activo afectado	Descripción del hallazgo o Problema
A.17.1.3 Verificación, revisión y evaluación de la Continuidad de la Seguridad de la Información	Se presenta el Fo_Plan de continuidad y disponibilidad_V01 fechado el 2 de mayo de 2023, que aborda situaciones como corte de energía eléctrica, corte de comunicaciones, indisponibilidad de instalaciones, ausentismo, emergencia sanitaria, política o social. Aunque los planes de continuidad y disponibilidad se prueban anualmente en septiembre y octubre, con informes exitosos de pruebas realizadas en septiembre, el incumplimiento radica en la falta de verificación regular de los controles de continuidad de seguridad de la información.

3. Análisis de causa raíz

Lluvia de ideas:

- Falta de verificación regular de los controles de continuidad y seguridad de la información.

4. Plan de acción

Tabla 237 Plan de acción 168

Descripción breve de la acción a realizar		Implementación de un sistema de verificación regular de los controles de continuidad y seguridad de la información.		
Objetivo / Meta		Asegurar la efectividad y actualización de los controles de continuidad y seguridad de la información para garantizar la disponibilidad de los recursos críticos de la organización en situaciones de contingencia.		
No.	Actividad	Fecha de compromiso		Responsables (Iniciales)
		Inicio	Fin	
1	Realizar una evaluación exhaustiva del Fo_Plan de continuidad y disponibilidad_V01 para identificar áreas de mejora en los controles de continuidad y seguridad de la información.	2-mar-24	3-mar-24	KHR BIGS
2	Desarrollar e implementar procedimientos claros para la verificación regular de los controles de continuidad y seguridad de la información, incluyendo la asignación de responsabilidades específicas.	4-mar-24	5-mar-24	KHR BIGS
3	Proporcionar capacitación al personal pertinente sobre los	6-mar-24	7-mar-24	KHR BIGS

	nuevos procedimientos de verificación de controles y su importancia para la continuidad del negocio y la seguridad de la información.			
4	Establecer un sistema de seguimiento y monitoreo continuo para verificar la implementación y efectividad de los controles de continuidad y seguridad de la información.	8-mar-24	9-mar-24	KHR BIGS
5	Realizar auditorías regulares para evaluar la eficacia de los controles implementados y realizar ajustes según sea necesario.	10-mar-24	11-mar-24	KHR BIGS

5. Evaluación del plan de acción

Tabla 238 Evaluación del plan de acción 168

Estatus	Aprobada ☒ Rechazada ☐	La acción fue rechazada por qué:
----------------	---	---

6. Eficacia de la acción realizada

Tabla 239 Eficacia del plan de acción 168

La acción realizada se consideró	Eficaz ☒ Ineficaz ☐	¿Por qué?	Se cumplió el objetivo
El nivel de eficacia de la acción fue	Alto ☒ Medio ☐	¿Por qué?	Se cumplieron las actividades en tiempo y forma según lo planificado

	Bajo ☐		
Grado de cumplimiento contra el objetivo o meta establecida		Alto ☒ Medio ☐ Bajo ☐	
Fecha de Cierre	11-mar-24		

7. Resultados

PLAN DE CONTINUIDAD PLAN DE CONTINUIDAD Información para el control documental Clasificación interna	Clasificación: Interno Versión: 02 Fecha de última revisión: 24-mar-24
--	--

Figura 62 Portada plan de continuidad

Se muestra el plan de continuidad que se implementa de forma anual donde se consideran las operaciones comerciales en situaciones adversas así como se muestran los procedimientos de

respuesta, la infraestructura, los planes de continuación y actualizaciones.

PLAN DE CONTINUIDAD

Clasificación: Interno
Versión: 02
Fecha de última revisión:
24-mar-24

Nombre del Plan: Plan de Continuidad y Disponibilidad (Fo_Plan_V01)

Fecha de Emisión: 24 de marzo de 2024

Situaciones Abordadas:

- Corte de energía eléctrica
- Corte de comunicaciones
- **Indisponibilidad** de instalaciones
- Ausentismo
- Emergencia sanitaria
- Situaciones políticas o sociales

Procedimientos de Prueba Anual:

Las pruebas de continuidad y disponibilidad se realizan anualmente en septiembre y octubre.
Informes exitosos de pruebas realizadas en septiembre.

Áreas de Incumplimiento:

Falta de verificación regular de los controles de continuidad de seguridad de la información, según lo requerido por el estándar.

Objetivos del Plan:

Garantizar la continuidad de las operaciones comerciales en situaciones adversas o de emergencia.
Minimizar el impacto de interrupciones en la disponibilidad de servicios críticos.

Equipo de Gestión de Crisis:

Nombre: [REDACTED]
Rol y Responsabilidades: director de TI

Nombre: [REDACTED]
Rol y Responsabilidades: Líder de Recursos Humanos

Nombre: [REDACTED]
Rol y Responsabilidades: Coordinador de Seguridad

Figura 63 Plan de continuidad

Procedimientos de Respuesta:

1. Corte de energía eléctrica:
Activar generadores de respaldo.
Priorizar el uso de energía para equipos esenciales.
2. Corte de comunicaciones:
Utilizar sistemas de comunicación alternativos (p. ej., radios, dispositivos móviles).
3. Indisponibilidad de instalaciones:
Redirigir operaciones a ubicaciones alternativas si es necesario.
4. Ausentismo:
Implementar planes de contingencia para redistribuir tareas y asegurar la continuidad de funciones críticas.
5. Emergencia sanitaria:
Seguir las pautas y recomendaciones de las autoridades de salud.
Implementar medidas de higiene y distanciamiento social.
6. Situaciones políticas o sociales:
Monitorear de cerca la situación y tomar decisiones basadas en la seguridad del personal y la continuidad de las operaciones.

Recuperación de Infraestructura:

Establecer un plan detallado para la rápida recuperación de la infraestructura física y tecnológica en caso de interrupciones.

Planes de Comunicación:

Desarrollar planes de comunicación interna y externa para mantener informadas a todas las partes interesadas durante una crisis.

Pruebas y Ejercicios de Simulación:

Programar pruebas y ejercicios de simulación regulares para evaluar la efectividad del plan y entrenar al personal en su

Figura 64 Plan de continuidad

PLAN DE CONTINUIDAD

Clasificación: Interno
 Versión: 02
 Fecha de última revisión:
 24-mar-24

implementación.

Actualización Continua:
 Revisar y actualizar el plan de manera regular para reflejar cambios en el entorno operativo, la tecnología y los riesgos comerciales.

Formación y Concienciación:
 Proporcionar formación y concienciación al personal sobre los procedimientos de respuesta a emergencias y la importancia de la continuidad del negocio.

Aprobado por: [REDACTED]

Fecha de Aprobación: 24 de marzo de 2024

Figura 65 Plan de continuidad

4.1.1.3.2.10 Plan de acción: Requisitos contractuales

1. Datos generales de la acción

Tabla 240 Datos generales plan de acción 169

Folio	169	Fecha de registro	24-mar-24
Tipo de Acción	Correctiva ☒ Preventiva ☐ Mejora ☐	Prioridad	Baja ☐ Media ☐ Alta ☒
Derivada de	Auditoría interna ☒ Auditoría externa ☐ De la operación ☐ Queja ☐ Problema ☒ Sugerencia ☐ Revisión por la dirección ☐		

2. Descripción del hallazgo

Tabla 241 Descripción del hallazgo plan de acción 169

Requisito Normativo Documento(s), y/o activo afectado	Descripción del hallazgo o Problema
A.18.1.1 Identificación de la Legislación Aplicable y Requisitos Contractuales	Se muestra la Re_Matriz de cumplimiento fechado el día 24 de marzo del 2023 donde identifica los requisitos normativos/requisitos, fuente, evidencia, revisiones semestrales y observaciones, sin embargo, no refleja de manera completa y

	actualizada todos los requisitos normativos pertinentes.
--	--

3. Análisis de causa raíz

Lluvia de ideas:

- Falta de actualización y completitud en la inclusión de todos los requisitos normativos pertinentes en la Re_Matriz de cumplimiento.

4. Plan de acción

Tabla 242 Plan de acción 169

Descripción breve de la acción a realizar		Revisión y actualización de la Re_Matriz de cumplimiento para incluir de manera completa y actualizada todos los requisitos normativos pertinentes.		
Objetivo / Meta		Actualizar el Re_Matriz de cumplimiento de modo que refleje de manera completa todos los requisitos normativos pertinentes para facilitar la supervisión y cumplimiento de los mismos.		
No.	Actividad	Fecha de compromiso		Responsables (Iniciales)
		Inicio	Fin	
1	Identificar y recopilar todos los requisitos normativos pertinentes que deben ser incluidos en la Re_Matriz de cumplimiento.	24-mar-24	25-mar-24	ASR BIGS
2	Revisar la Re_Matriz de cumplimiento existente y compararla con los requisitos normativos recopilados para	26-mar-24	27-mar-24	ASR BIGS

	identificar las brechas de inclusión.			
3	Actualizar la Re_Matriz de cumplimiento con los nuevos requisitos normativos identificados y asegurarse de que estén debidamente documentados.	28-mar-24	29-mar-24	ASR BIGS
4	Establecer un procedimiento para mantener la Re_Matriz de cumplimiento actualizada de manera regular, incluyendo revisiones semestrales para asegurar su vigencia.	30-mar-24	31-mar-24	ASR BIGS

5. Evaluación del plan de acción

Tabla 243 Evaluación del plan de acción 169

Estatus	Aprobada ☒ Rechazada ☐	La acción fue rechazada por qué:
----------------	---	---

6. Eficacia de la acción realizada

Tabla 244 Eficacia del plan de acción 169

La acción realizada se consideró	Eficaz ☒ Ineficaz ☐	¿Por qué?	Se cumplió el objetivo
El nivel de eficacia de la acción fue	Alto ☒ Medio ☐ Bajo ☐	¿Por qué?	Se cumplieron las actividades en tiempo y forma según lo planificado
Grado de cumplimiento contra el objetivo o meta establecida			Alto ☒ Medio ☐ Bajo ☐
Fecha de Cierre	31-mar-24		

7. Resultados

Se muestra el Re_Matriz con día de última actualización del 24-mar-24



Figura 66 Portada matriz de cumplimiento

Se muestra la matriz de cumplimiento donde se toma como requisitos las normas y las leyes así como muestra la evidencia de lo que se implementa conforme las normas y las leyes y se muestran los meses cuando fue la revisión y las observaciones.

MATRÍZ DE CUMPLIMIENTO				Clasificación: Interno Fecha de última revisión: 24-03-23
MATRÍZ DE CUMPLIMIENTO				VERSIÓN: 01
REQUISITOS NORMATIVOS/REQUISITOS	FUENTE	EVIDENCIA	REVISIONES SEMESTRALES	OBSERVACIONES
ISO 27001	Norma ISO 27001	Certificación ISO 27001 vigente	Junio, Diciembre	Cumplimiento adecuado
Ley de Protección de Datos Personales	Legislación Nacional	Política de Privacidad de Datos, Registro de Consentimientos	Marzo, Septiembre	Pendiente de revisión y actualización
Regulación de Ciberseguridad	Entidad Reguladora	Informes de Auditoría de Seguridad	Abril, Octubre	Cumplimiento adecuado
Normativa Laboral	Ministerio de Trabajo	Políticas de Recursos Humanos, Contratos Laborales	Febrero, Agosto	Cumplimiento adecuado
Estándares de Seguridad de la Información	Ministerio de Trabajo	Procedimientos de Auditoría Interna, Planes de Seguridad	Mayo, Noviembre	Evidencia incompleta de actualización

Figura 67 Matriz de cumplimiento

CONCLUSIONES

Los resultados derivados de la auditoría conforme a la norma ISO/IEC 27001:2015 han revelado una evaluación minuciosa y detallada de los sistemas de información y su seguridad en el ámbito de la organización auditada SayNet Soluciones Integrales S.A. de C.V. Se logró cumplir con los objetivos planteados al inicio del proyecto, lo que refleja no solo una implementación altamente efectiva de metodologías de control interno y seguridad.

A lo largo del proceso de auditoría, se observó una planificación meticulosa y una ejecución que permitió una identificación precisa y contextualizada de los riesgos y vulnerabilidades presentes en el Sistema de Gestión Integral. La aplicación de la terminología propia del campo, fueron elementos cruciales que no solo facilitaron la identificación de áreas de mejora, sino que también condujeron a la formulación de recomendaciones específicas y personalizadas para fortalecer la seguridad de la información en la organización.

La combinación de entrevistas, junto con la minuciosa presentación y revisión de la documentación que respalda el Sistema de Gestión Integral, ha constituido un proceso para evaluar el cumplimiento en relación con el estándar establecido. A través de este enfoque, se logró obtener una visión completa y detallada de la conformidad del sistema con los requisitos establecidos, así como identificar posibles áreas de mejora y oportunidades. Las entrevistas proporcionaron una plataforma interactiva para obtener información directa de

los responsables y actores clave dentro de la organización, permitiendo así una comprensión más profunda de la implementación práctica del sistema. Por otro lado, la revisión documental ofreció una perspectiva estructurada y detallada de los procesos, procedimientos y registros asociados, brindando una base sólida para la evaluación y análisis de la conformidad.

Es importante señalar que, si bien se lograron alcanzar los objetivos principales del proyecto, se identificaron algunas limitaciones como la disponibilidad limitada de ciertos recursos técnicos, la complejidad inherente a ciertos sistemas evaluados y la falta de mantenimiento al SGI. Sin embargo, estas limitaciones no constituyeron obstáculos insuperables, sino más bien oportunidades para la innovación y la adaptación. Se implementaron estrategias adaptativas y soluciones alternativas que, lejos de minimizar el proceso de auditoría, fortalecieron su robustez y relevancia.

COMPETENCIAS DESARROLLADAS

Tabla 245 Competencias

Materia	Específicas
Auditoría Informática y Desarrollo de Proyectos y Aplicaciones	Maneja de los fundamentos teóricos de auditoría general, informática y tecnologías de información, así como su integración para su aplicación en el entorno práctico.
	Identifica interpretación y uso de lineamientos, estándares, marcos referenciales, técnicas y otros conceptos que complementen la unión del conocimiento para la posterior aplicación de la Auditoría informática.
	Describe la terminología propia de la Auditoría a fin de aplicarla en la planificación, ejecución y entrega de resultados del proceso de auditoría informática que incluya la selección de herramientas, técnicas, y las propuestas de actividades de control.
	Comprende del entorno del control interno en las empresas y su concepción en una normativa internacional.
	Argumenta las metodologías para el control interno, seguridad y auditoría informática, a fin de incorporan en el proceso de la auditoría.
Administración de la Función Informática	Manejo de los fundamentos teóricos de seguridad informática para su aplicación en casos prácticos
	Uso e interpretación de los lineamientos, estándares y marcos referenciales que complementen el conocimiento de la asignatura
	Uso de técnicas y herramientas de software para comprender el ambiente de seguridad.
	Estructuración de un plan de continuidad del negocio
	Proponer medidas de seguridad basadas en lineamientos y estándares actuales
Taller de Administración	Comprender y aplicar los principios generales de la administración y su proceso en las estructuras y funciones fundamentales de las organizaciones acorde a las necesidades de la misma, para contribuir

sustantivamente con los procesos de planeación y toma de decisiones, con una visión crítica del contexto empresarial.

Durante la auditoría bajo el estándar 27001:2015 se aplicaron las competencias antes mencionadas de las materias de Auditoría Informática y Desarrollo de Proyectos y Aplicaciones, Administración de la Función Informática y Taller de Administración en el entorno práctico. Con el manejo de los fundamentos teóricos de auditoría general, informática y tecnologías de información, se comprendió la estructura y los procesos de la auditoría en profundidad. Esto permitió identificar, interpretar y utilizar adecuadamente lineamientos, estándares, marcos referenciales y las herramientas necesarias para llevar a cabo la auditoría informática completa y efectiva.

La familiaridad con la terminología propia de la auditoría facilitó la planificación, ejecución y entrega de resultados del proceso de auditoría. Esta comprensión de la terminología también fue crucial para la selección de herramientas y técnicas adecuadas, así como para proponer actividades de control pertinentes.

En relación con el control interno en las empresas, se puede argumentar de manera sólida las metodologías para el control interno, seguridad y auditoría informática. Esto contribuyó a la integración efectiva de estos aspectos en el proceso de auditoría, garantizando una evaluación exhaustiva de los sistemas de información y su seguridad. Además, el dominio de los fundamentos teóricos de seguridad informática permitió aplicarlos en casos prácticos durante la auditoría. La interpretación de lineamientos, estándar y marcos referenciales complementó el conocimiento, asegurando una evaluación completa de la seguridad de la información.

El uso de técnicas y herramientas de software para comprender el ambiente de seguridad fue fundamental para identificar posibles vulnerabilidades y riesgos. La proposición de medidas de seguridad basadas en lineamientos y estándares actuales fueron aspectos clave para garantizar la resiliencia y protección de la organización frente a amenazas informáticas.

Finalmente, la comprensión y aplicación de los principios generales de la administración en las estructuras y funciones fundamentales de las organizaciones permitieron contribuir con los procesos de planeación y toma de decisiones durante la auditoría. Esta visión crítica del

contexto empresarial fue esencial para identificar áreas de mejora y proponer recomendaciones pertinentes para fortalecer la seguridad de la información y los controles internos de la organización auditada.

FUENTES DE INFORMACIÓN

- Deming, E. (6 de Julio de 2014). *ISOTools*. Obtenido de ISOTools:
<https://www.isotools.us/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/>
- Desconocido. (5 de Julio de 2011). *AWS*. Obtenido de Amazon web:
<https://aws.amazon.com/security/>
- Desconocido. (19 de Abril de 2014). *Google*. Obtenido de Google Cloud Services:
<https://cloud.google.com/security>
- Desconocido. (01 de Julio de 2015). *IBM*. Obtenido de IBM: <https://www.ibm.com/security>
- Desconocido. (06 de Mayo de 2017). *Banco Santander*. Obtenido de Banco Santander:
<https://www.santander.com/en/stories/security>
- Desconocido. (1 de Febrero de 2018). *pmg-ssi*. Obtenido de pmg-ssi: <https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/>
- Desconocido. (12 de Febrero de 2021). *Historia Saynet*. Obtenido de Facebook:
<https://www.facebook.com/watch/?v=477101019963257>
- Desconocido. (22 de Septiembre de 2023). *GlobalSuite*. Obtenido de GlobalSuite:
<https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/>
- Desconocido. (31 de Agosto de 2023). *Linked in*. Obtenido de Linked in:
<https://es.linkedin.com/pulse/pol%C3%ADticas-y-procedimientos-de-seguridad-implementaci%C3%B3n>
- Desconocido. (1 de Marzo de 2023). *Red Hat*. Obtenido de Red Hat:
<https://www.redhat.com/es/topics/management/what-is-compliance-management>
- Estevez, M. (26 de Septiembre de 2024). *Izertis*. Obtenido de Izertis: <https://www.izertis.com/es/-/blog/normativa-ciberseguridad>
- Gironzini, M. A. (08 de Junio de 2016). *Auditool*. Obtenido de Auditool:
<https://www.auditool.org/blog/auditoria-externa/importancia-de-la-planificacion-de-una-auditoria>
- Limited, N. Q. (2011). *ISO 27001:2022 Guia de implementacion*. Mexico: NA.
- Melo, S. (30 de Septiembre de 2021). *DataScope*. Obtenido de DataScope:
<https://datascope.io/es/blog/que-es-y-para-que-sirve-una-lista-de-verificacion/>
- Ramirez, J. R. (09 de Septiembre de 2021). *Estrategias de planeacion de la auditoria*. Obtenido de Estrategias de planeacion de la auditoria:
<https://portal.amelica.org/ameli/journal/387/3872816002/html/>

ANEXOS

Anexo 1: Carta de autorización del proyecto

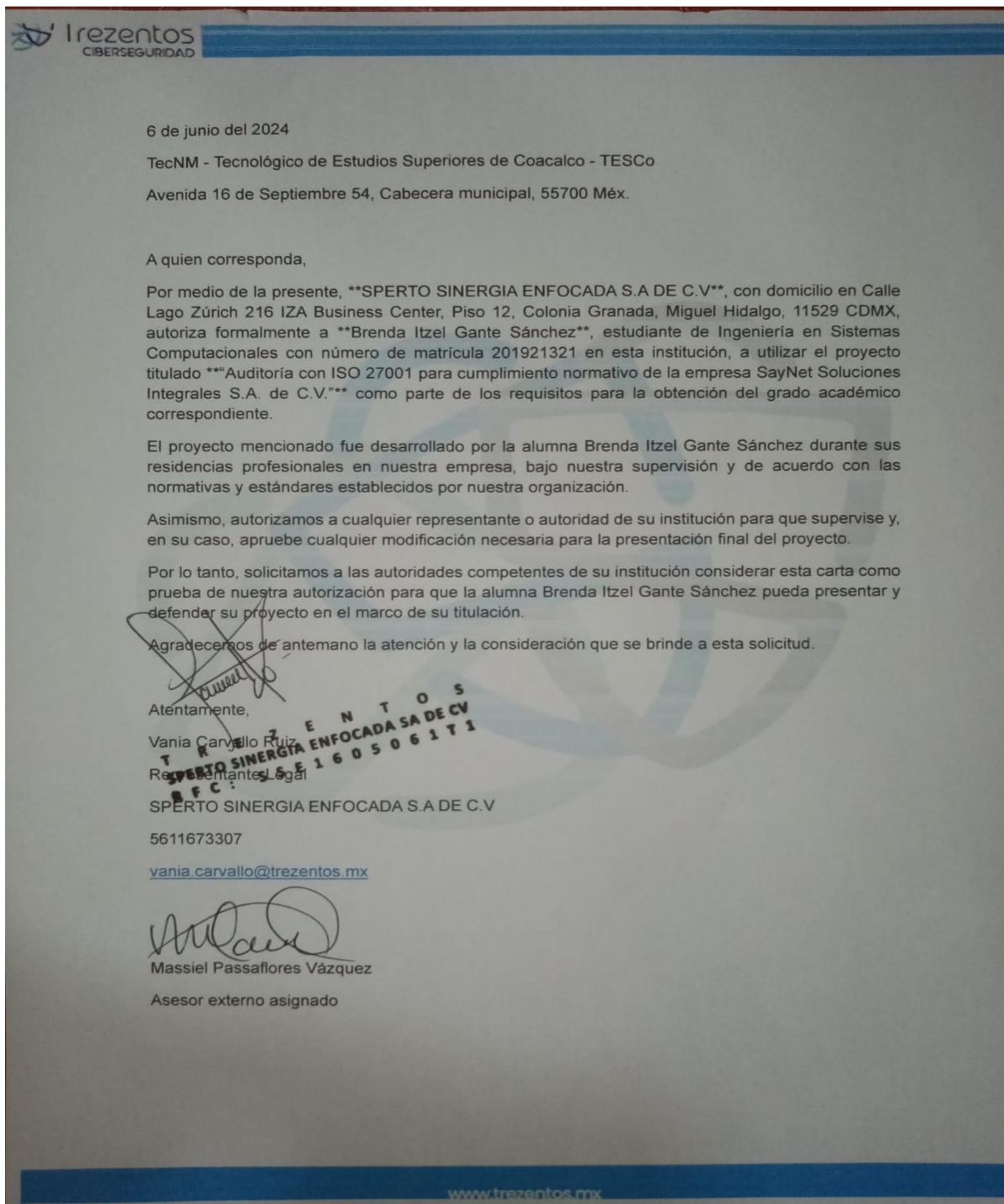


Figura 68 Carta de autorización del proyecto

Anexo 2: Carta de autorización del proyecto



Lago Zurich 245 piso 12, Ampliación Granada, Miguel Hidalgo, C.P. 11529 CDMX.

Figura 69 Carta de autorización del proyecto

Anexo 3: Contrato de confidencialidad[BG13]

DocuSign Envelope ID: E42D61B2-885F-4DF1-B5FA-D547959286F0

1

CONVENIO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN CONFIDENCIAL QUE CELEBRAN POR UNA PARTE LA EMPRESA DENOMINADA SPERTO SINERGIA ENFOCADA SA DE CV A TRAVÉS DE SU REPRESENTANTE LEGAL VANIA CARVALLO RUIZ A QUIÉN EN LO SUCESIVO Y PARA EFECTOS DEL PRESENTE SE DENOMINARÁ "LA EMPRESA", Y POR LA OTRA PARTE POR SU PROPIO DERECHO EL SEÑOR(A) Aranda Itzel Gante Sánchez, Y A QUIÉN EN LO CONSECUTIVO Y PARA EFECTOS DEL PRESENTE CONVENIO SE DENOMINARÁ "EL RECEPTOR", Y DENOMINADAS DE MANERA CONJUNTA COMO "LAS PARTES", AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS.

DECLARACIONES

i. Declara la Empresa a través de su representante legal:

- a. Es una sociedad, debidamente constituida de conformidad con las leyes que rigen en la República Mexicana.
- b. Su domicilio se encuentra en: Ave Lago Zurich 219, Plaza Carso piso12 Colonia Ampliación Granada, Miguel Hidalgo, CDMX C.P. 11529
- a. Su representante legal, cuenta con las facultades suficientes y necesarias para celebrar el presente Convenio y obligar a su representada en términos del mismo y que dichas facultades no le han sido modificadas, limitadas o restringidas en forma alguna a la fecha del presente Convenio.
- b. Ha aplicado cuantiosos recursos humanos, económicos, materiales y administrativos para poder llevar a cabo su objeto social y para lograr un adecuado manejo de la Empresa.
- c. Por la manera en la que se conforma, organiza, administra y procesa la Información Confidencial relacionada con su objeto social y con el manejo mismo de la Empresa, cualquier persona relacionada directa o indirectamente con este sector y mercado, puede fácilmente beneficiarse de ella, explotándola u obteniendo las ventajas competitivas que implica.
- d. Que, en virtud de la relación académica y/o comercial y/o de prestación de servicios que sostiene o pretende sostener el Receptor con la Empresa, dadas las actividades a las que se dedica el primero; desde el día 16/oct/23, el Receptor ha tenido acceso a cierta Información Confidencial de la Empresa, las que se mencionan de manera no limitativa, como: proyectos, material de capacitación, imágenes, contenido, material de estudio e información referente al manejo de la propia Empresa, actividades, instalaciones, su operación, entregables, software, clientes, así como la relacionada en el presente Convenio sus clientes, filiales, subsidiarias y demás compañías relacionadas directa o indirectamente, tanto vinculada con su objeto social y operaciones, como con su manejo y cuestiones estructurales.
- e. Por la delicadeza, valor, ventaja que implica, relevancia y/o características de la documentación e Información Confidencial a la que el Receptor tiene acceso, sea propia de la Empresa, sus filiales, subsidiarias, clientes, de personas jurídicamente relacionadas o de terceros, proyectos, etc. desea que el Receptor: (i) se obligue a guardar plena discreción y confidencialidad de la Información Confidencial que recibe, ya sea de manera escrita, verbal o por cualquier medio, (ii) se obligue a indemnizarle por los daños o perjuicios que el incumplimiento de las obligaciones derivadas de este Convenio pudiera generarle y (iii) sea consciente de las consecuencias jurídicas que el incumplimiento de las obligaciones aquí adquiridas puede generar.

Figura 70 Convenio de confidencialidad declaraciones

II. Declara el Receptor por su propio derecho:

- a. Que cuenta con las facultades legales para obligarse en los términos y condiciones del presente convenio y que entiende los términos del mismo.
- b. Que autoriza revisión y evaluación de antecedentes para integración, esto en caso de no atentar contra establecimientos del código penal federal.
- c. Que derivado de las actividades que realizará como **becario/estudiante/aprendiz**, sostiene conversaciones y tiene o pretende entablar relaciones ("la Relación") con la Empresa.
- a. Su domicilio se encuentra en:
rancho la palma, wda. capullo condominio 46, casa 4
- d. Que cuenta con las facultades suficientes para celebrar el presente Convenio y obligarse en términos del mismo.
- e. Reconoce que, como consecuencia de su Relación con la Empresa, y debido a las actividades que desempeña, tiene pleno acceso a la Información Confidencial que resulta delicada, valiosa, ventajosa y/o relevante para la propia Empresa, para sus clientes, para personas jurídicamente relacionadas con ésta, o para terceros, y que su uso, revelación o divulgación no autorizada, podría causar graves repercusiones jurídicas y económicas a ésta.
- f. Dentro de la documentación e Información Confidencial y exclusiva a la que ha tenido y tendrá acceso, se encuentra, enumerativa mas no limitativamente, proyectos, entregables, clientes, material de capacitación, material de estudio, planes de trabajo, software, licenciamiento, referente al manejo de la propia Empresa, actividades, instalaciones, sus proyectos y actividades operativas, personal, software, proyectos por desarrollar, relaciones comerciales, financieras, estrategias, tarifas, clientes, perfiles de servicios, así como la relacionada en el presente Convenio sus clientes, filiales, subsidiarias y demás compañías relacionadas directa o indirectamente, tanto vinculada con su objeto social y operaciones, como con su manejo y cuestiones estructurales, (la "Información Confidencial").
- g. Manifiesta su anuencia para indemnizar a la Empresa, por cualquier daño o perjuicio que el incumplimiento de las obligaciones aquí contenidas pudiera causarles.
- h. Bajo protesta de decir verdad que, no ha realizado, ni realizará actos de sustracción, destrucción, fotocopiado, duplicado, fotografía, video, sin perjuicio del medio de constancia, archivo o almacenaje, ninguna documentación o Información Confidencial, interna, relevante o delicada para o relacionada con la Empresa, sus prestadores de servicios, colaboradores, clientes, o personas de cualquier manera vinculadas jurídicamente con ella o cualquier tipo de Información Confidencial o interna que pudiera haberle sido entregada para el desempeño de sus actividades y que tenga una trascendencia tal que pudiera causarle algún daño o perjuicio a la Empresa derivado de la sustracción, destrucción o fotocopiado no autorizado por ésta.
- i. Manifiesta bajo protesta de decir verdad que no conserva por sí o a través de interpósita persona, ni ha entregado a tercero alguno o divulgado de cualquier manera, ya sea oral, gráfica o escrita, absolutamente ninguna documentación o Información Confidencial de la Empresa, o relacionada directa o indirectamente con ésta, sea original o copia, sin importar la forma de constancia, archivo o almacenamiento.

III. Declaran las Partes que:

- a. Reconocen y acuerdan que las Declaraciones antes señaladas constituyen el motivo determinante de la voluntad de la Empresa para mantener la Relación con el Receptor.
- b. Por así convenir a sus intereses, es su deseo y libre voluntad obligarse a lo dispuesto por las siguientes:

Figura 71 Declaraciones

CLÁUSULAS

PRIMERA. Objeto: El presente convenio tiene como objeto proteger la Información Confidencial que compartirán las Partes, a efecto de que el Receptor no tome ventaja de la Información Confidencial o interna en mención, que reciba y/o conozca referente y de propiedad de:

SPERTO SINERGIA ENFOCADA, EXPERTOS EN SISTEMAS DE GESTIÓN Y LAS FILIALES, SUBSIDIARIAS Y/O CLIENTES DE EFD QUE SE SUMEN A LAS AQUÍ MENCIONADAS.

Las Partes convienen que toda la Información Confidencial que se revele entre ellas estará amparada por el deber de confidencialidad en términos del presente.

SEGUNDA. Deber de Confidencialidad: El Receptor únicamente utilizará la Información Confidencial facilitada por la Empresa para los fines de la Relación entre las Partes, comprometiéndose el Receptor a mantener la más estricta confidencialidad respecto de la Información Confidencial recibida, advirtiendo del deber de confidencialidad y secreto a los terceros, que por su Relación con el Receptor, deban tener acceso a la Información Confidencial otorgada para el correcto cumplimiento de las obligaciones del Receptor para con la Empresa. En este sentido, se entenderá que el Receptor debe asegurarse que el representante legal o cada persona física o moral que deba acceder a la Información Confidencial por causas legales o debidamente fundadas, revelada por la Empresa se adhiera al compromiso de confidencialidad establecido en el presente acuerdo.

El Receptor y las personas mencionadas en el párrafo anterior no podrán reproducir, modificar, hacer pública o divulgar a terceros la Información Confidencial objeto del presente acuerdo sin previa autorización escrita y expresa de la Empresa.

En caso de que la Empresa otorgue la autorización escrita para facilitar la Información Confidencial a un tercero, se procederá de la siguiente forma:

(i) La Empresa firmará con el tercero un Convenio de confidencialidad previo a que el Receptor proporcione en todo o en parte la Información Confidencial al tercero, para lo cual el Receptor deberá cerciorarse antes de divulgar la Información Confidencial, si efectivamente la Empresa y el tercero firmaron el correspondiente Convenio de confidencialidad.

Además de lo anterior, el Receptor se obliga a no celebrar con ninguna persona física o moral, cualquier tipo de acuerdo, convenio, contrato, negociación o asumir obligaciones que estén en conflicto con el presente acuerdo o que derive o implique el incumplimiento del mismo.

Asimismo, el Receptor adoptará respecto de la Información Confidencial objeto de este convenio las mismas medidas de seguridad que normalmente adoptaría respecto a la Información Confidencial de sus propios negocios o intereses, evitando por todos los medios a su alcance la pérdida, robo o sustracción de la Información Confidencial compartida por la Empresa.

TERCERA. Propiedad De La Información Confidencial: Los derechos de propiedad de la Información Confidencial objeto del presente acuerdo pertenecen únicamente a la Empresa y el hecho de facilitar al Receptor para el objeto mencionado en la cláusula primera no modifica tal situación, lo cual implica que la Empresa conservará para sí los derechos inherentes a la propiedad de la Información Confidencial que se haga llegar a el Receptor.

El Receptor reconoce que la Información Confidencial de cualquier naturaleza, incluso la distribuida, recopilada o discutida en juntas y/o reuniones, documentos en general, políticas, organización, sistemas de administración, Información Confidencial, comercial, tecnología usada y/o desarrollada durante el periodo de su colaboración, procedimientos y todos aquellos hechos, actos e Información Confidencial que con motivo de su trabajo sean de su conocimiento es propiedad de la Empresa y, por lo tanto, se obliga a no utilizar o divulgarla, ya sea directa o indirectamente, en su beneficio o en beneficio de terceras personas, especialmente la descrita de manera enunciativa y no limitativa en el presente convenio.

En consecuencia, en ningún caso y por ningún motivo se entenderá que la Información Confidencial compartida por alguna de las partes constituirá una copropiedad y el Receptor reconoce que el derecho de que la Empresa le comparta Información Confidencial no le otorga ningún derecho de licencia, patente o propiedad intelectual sobre la misma, y que la revelación de la Información Confidencial no originará ninguna obligación a la Empresa de otorgar derecho alguno sobre dicha Información Confidencial.

CUARTA. Uso de la Información Confidencial: El Receptor se obliga a guardar absoluta confidencialidad sobre la Información Confidencial que debido a sus actividades llegue a conocer o tener en su poder, debiendo usar dicha Información Confidencial exclusivamente en beneficio de la Empresa.

Asimismo, el Receptor se obliga a no mantener en su poder copia alguna o reproducción, total o parcial de la documentación o Información Confidencial señalada, bajo cualquier forma o medio de constancia, archivo o almacenamiento, en caso de contravenir con lo anteriormente citado responderá de los daños y perjuicios que ocasione, aunado a las penalidades de las que pueda ser objeto.

El Receptor se obliga a resguardar en todo momento la información ya sea en proceso o producto terminado dentro de los espacios corporativos designados que sean propiedad de la EMPRESA. Por lo tanto, el Receptor no podrá resguardar de forma temporal ni definitiva documentos o información propiedad de la Empresa, sus clientes, filiales, proyectos, colaboradores, socios comerciales en ningún dispositivo personal ni en ningún dispositivo que no sea propiedad de la empresa.

QUINTA. Toda la Información Confidencial, documentación comercial relevante, delicada o secreta de la Empresa tiene el carácter de confidencial bajo el presente instrumento y por tanto de secreto industrial, en los términos del artículo 82 de Ley Federal de Protección a la Propiedad Industrial, por tratarse de aplicaciones de carácter industrial y/o comerciales que se traducen en obtener o mantener una ventaja competitiva o económica frente a terceros en la realización de las actividades económicas que le son propias a la Empresa, y respecto de las cuales se han adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma.

En los términos de los artículos 84 y 85 de la Ley Federal de Protección a la Propiedad Industrial, el Receptor deberá abstenerse de revelar, sin el previo consentimiento por escrito de la Empresa, ya sea durante o después de la terminación del presente Convenio, cualquier secreto industrial.

De acuerdo con lo anterior, el Receptor manifiesta para todos los efectos a que haya lugar, que conoce y entiende cabalmente lo dispuesto en la Ley Federal de Protección a la Propiedad Industrial, conforme al cual, las siguientes conductas inadecuadas respecto del manejo de los secretos industriales se tipifican como delictivas:

***Artículo 402: Son delitos:**

...

III.- Divulgar a un tercero un secreto industrial, que se conozca con motivo de su trabajo, puesto, cargo, desempeño de su profesión, relación de negocios o en virtud del otorgamiento de una licencia para su uso, sin consentimiento de la persona que ejerza su control legal o de su usuario autorizado, LEY FEDERAL DE PROTECCIÓN A LA PROPIEDAD INDUSTRIAL CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN Secretaría General Secretaría de Servicios Parlamentarios Nueva Ley DOF 01-07-2020 90 de 94 habiendo sido prevenido de su confidencialidad, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto;

IV.- Apoderarse de un secreto industrial sin derecho y sin consentimiento de la persona que ejerza su control legal o de su usuario autorizado, para usarlo o revelarlo a un tercero, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a quien ejerce su control legal o a su usuario autorizado;

V.- Usar la información contenida en un secreto industrial, que conozca por virtud de su trabajo, cargo o puesto, ejercicio de su profesión o relación de negocios, sin contar con el consentimiento de quien ejerce su control legal o de su usuario autorizado, o que le haya sido revelado por un tercero, que éste no contaba para ello con el consentimiento de la persona que ejerce su control legal o su usuario autorizado, con el propósito de obtener un beneficio económico o con el fin de causar un perjuicio a quien ejerce el control legal del secreto industrial o su usuario autorizado;

VI.- Apropiarse, adquirir, usar o divulgar indebidamente un secreto industrial a través de cualquier medio, sin consentimiento de quien ejerce su control legal o de su usuario autorizado; con el propósito de causarle perjuicio u obtener un beneficio económico para sí o para un tercero..."

SEXTA. Notificación Requerimiento de Autoridad: Si el Receptor fuera requerido por Autoridad competente de cualquier tipo para revelar Información Confidencial delicada, relevante o Información Confidencial de la Empresa, el Receptor se obliga a dar aviso por escrito a la Empresa dentro de los 3 (tres) días hábiles siguientes a la recepción del documento respectivo, con la finalidad de que esta última pueda ejercitar los actos o derechos que correspondan para salvaguardar sus intereses.

SÉPTIMA. Devolución de la Información Confidencial: El Receptor al momento de la terminación de la Relación con la Empresa, se obliga a devolver en ese mismo momento, absolutamente toda la Información Confidencial que obre en su poder. El Receptor también se obliga a entregar a la Empresa todas las pertenencias de aquél usadas por el Receptor durante la Relación.

OCTAVA. Pena Convencional: El Receptor se obliga a indemnizar inmediatamente a la Empresa con una pena equivalente a \$500,000.00 (quinientos mil pesos 00/100 M.N.), más intereses moratorios desde la fecha de terminación de la Relación hasta la fecha efectiva de pago, a una tasa anual de 10% (diez por ciento), en caso de que la Información Confidencial compartida resulte revelada, divulgada o utilizada por el Receptor de cualquier forma distinta al objeto de este convenio, ya sea de forma dolosa o por mera negligencia aunado a cualquier daño o perjuicio que el incumplimiento de las obligaciones adquiridas en este Convenio le causara.

La obligación anterior, se hará extensiva respecto de los clientes o proveedores de la Empresa, de los cuales obtenga cualquier Información Confidencial, con motivo de la Relación entre el Receptor y la Empresa.

NOVENA. Vigencia: Este Convenio estará en vigor durante todo el plazo de vigencia de la Relación o relaciones de índole comercial que une o unirá a el Receptor con la Empresa y hasta cumplidos 10 (diez) años contados a partir de la fecha de terminación de la Relación entre las Partes.

DÉCIMA. Cumplimiento: El Receptor estará obligado a cumplir sus obligaciones bajo el presente Convenio independientemente del lugar en el que desempeñe sus actividades y respecto de la Información Confidencial de la Empresa, así como de sus subsidiarias o afiliadas, independientemente del lugar en el que éstas desempeñen su negocio, incluyendo sin limitar la República Mexicana, así como en Estados Unidos de Norteamérica, Centroamérica, Canadá, y Sudamérica.

DÉCIMA PRIMERA. Notificaciones: Para cualquier notificación, aviso o comunicado vinculado con este convenio, las Partes señalan como sus domicilios convencionales los siguientes:

LA EMPRESA

Domicilio: ave. Lago Zurich
219, plaza carso piso 12, col.
Ampliación granada cdmx cap
11529
Correo Electrónico:
Vania.carvallo@trezentos.mx

EL RECEPTOR

Domicilio: rancho la palma Ave de los arcos
wda.capullo condominio 46 casa 4 55717
Correo Electrónico: branda.gante@trezentos.mx

DÉCIMA SEGUNDA. Acuerdo Completo: Este Convenio constituye y expresa el total entendimiento entre las Partes en Relación con su objeto, así como su total entendimiento y

Figura 74 Clausulas Ultima Parte

condiciones, ya sean implícitas o expresas, orales o escritas. Ni el Convenio en su totalidad ni alguna parte de este podrán ser alterados, cambiados, renunciados o modificados sino mediante un convenio por escrito debidamente aceptado y firmado por ambas Partes.

DÉCIMA TERCERA. Nulidad: La invalidez o exclusión de alguna de las Cláusulas de este Convenio o parte de ella, no modificará ni alterará el contenido de las cláusulas que permanezcan, mismas que deberán continuar en vigor y en efecto, e interpretadas como si las inválidas o excluidas no hubieren sido insertadas.

DÉCIMA CUARTA. Avisos, Firmas Electrónicas: Las Partes convienen en que el presente Contrato, sus anexos, apéndices, modificaciones, y demás documentos que se otorguen de conformidad con el mismo, podrán celebrarse y entregarse ya sea mediante firma autógrafa, o digitalmente por cada una de ellas utilizando el sistema de firmas electrónicas <<DocuSign>> u otro que convengan que cuente con los certificados emitidos por un Prestador de Servicios de Certificación (PSC), conforme a lo dispuesto por la Ley de Firma Electrónica Avanzada. Cuando se celebren usando dicho sistema, los documentos electrónicos enviados a través de dicho sistema a las direcciones de correo electrónico señaladas por cada parte (o las que las sustituyan conforme al mismo), tendrán el mismo valor que las que cuenten con firma autógrafa, así como presunción de integridad y presunción de atribución de las firmas y se entenderán por hechas o recibidas cuando sean enviadas a la dirección electrónica antes indicada, siempre que no se le haya notificado al emisor un rechazo de la misma por parte de la dirección electrónica del Receptor, de su proveedor de correo o host.

DÉCIMA QUINTA. Interpretación y jurisdicción: Para la interpretación y cumplimiento de este Convenio las Partes aceptan sujetarse a la jurisdicción y leyes de los tribunales competentes de la Ciudad de México, renunciando expresamente a cualquier otro fuero que, por razón de sus domicilios presentes o futuros, o por cualquier otra razón, pudiera corresponderles.

Leído que fue este Convenio por las Partes y enteradas plenamente de su contenido y efectos legales y no existiendo ninguna clase de vicio, dolo o mala fe, ambas lo firman en original en 2 (dos) tantos de conformidad, en Miguel Hidalgo CDMX, el día 08/02/2024.

La Empresa

El Receptor
Por Su Propio Derecho



Vania Carvallo Ruiz

DocuSigned by:
Brenda Itzel Gante Sánchez
646ED77EC6B643B...

Brenda Itzel Gante Sanchez

Figura 75 Firmas Contrato de confidencialidad

Anexo 4: Contrato de confidencialidad^[BG14]

1

CONVENIO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN CONFIDENCIAL QUE CELEBRAN POR UNA PARTE LA EMPRESA DENOMINADA SPERTO SINERGIA ENFOCADA SA DE CV A TRAVÉS DE SU REPRESENTANTE LEGAL VANIA CARVALLO RUIZ A QUIÉN EN LO SUCESIVO Y PARA EFECTOS DEL PRESENTE SE DENOMINARÁ "LA EMPRESA", Y POR LA OTRA PARTE POR SU PROPIO DERECHO EL SEÑOR(A) Lizeth Viridiana Gutiérrez Guerra, Y A QUIÉN EN LO CONSECUTIVO Y PARA EFECTOS DEL PRESENTE CONVENIO SE DENOMINARÁ "EL RECEPTOR", Y DENOMINADAS DE MANERA CONJUNTA COMO "LAS PARTES", AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS.

DECLARACIONES

I. Declara la Empresa a través de su representante legal:

- a. Es una sociedad, debidamente constituida de conformidad con las leyes que rigen en la República Mexicana.
- b. Su domicilio se encuentra en: Ave Lago Zurich 219, Plaza Carso piso12 Colonia Ampliación Granada, Miguel Hidalgo, CDMX C.P. 11529
- a. Su representante legal, cuenta con las facultades suficientes y necesarias para celebrar el presente Convenio y obligar a su representada en términos del mismo y que dichas facultades no le han sido modificadas, limitadas o restringidas en forma alguna a la fecha del presente Convenio.
- b. Ha aplicado cuantiosos recursos humanos, económicos, materiales y administrativos para poder llevar a cabo su objeto social y para lograr un adecuado manejo de la Empresa.
- c. Por la manera en la que se conforma, organiza, administra y procesa la Información Confidencial relacionada con su objeto social y con el manejo mismo de la Empresa, cualquier persona relacionada directa o indirectamente con este sector y mercado, puede fácilmente beneficiarse de ella, explotándola u obteniendo las ventajas competitivas que implica.
- d. Que, en virtud de la relación académica y/o comercial y/o de prestación de servicios que sostiene o pretende sostener el Receptor con la Empresa, dadas las actividades a las que se dedica el primero; desde el día 13 de octubre, el Receptor ha tenido acceso a cierta Información Confidencial de la Empresa, las que se mencionan de manera no limitativa, como: proyectos, material de capacitación, imágenes, contenido, material de estudio e información referente al manejo de la propia Empresa, actividades, instalaciones, su operación, entregables, software, clientes, así como la relacionada en el presente Convenio sus clientes, filiales, subsidiarias y demás compañías relacionadas directa o indirectamente, tanto vinculada con su objeto social y operaciones, como con su manejo y cuestiones estructurales.
- e. Por la delicadeza, valor, ventaja que implica, relevancia y/o características de la documentación e Información Confidencial a la que el Receptor tiene acceso, sea propia de la Empresa, sus filiales, subsidiarias, clientes, de personas jurídicamente relacionadas o de terceros, proyectos, etc. desea que el Receptor: (i) se obligue a guardar plena discreción y confidencialidad de la Información Confidencial que recibe, ya sea de manera escrita, verbal o por cualquier medio, (ii) se obligue a indemnizarle por los daños o perjuicios que el incumplimiento de las obligaciones derivadas de este Convenio pudiera generarle y (iii) sea consciente de las consecuencias jurídicas que el incumplimiento de las obligaciones aquí adquiridas puede generar.

Figura 76 Convenio de confidencialidad declaraciones

II. Declara el Receptor por su propio derecho:

- a. Que cuenta con las facultades legales para obligarse en los términos y condiciones del presente convenio y que entiende los términos del mismo.
- b. Que autoriza revisión y evaluación de antecedentes para integración, esto en caso de no atentar contra establecimientos del código penal federal.
- c. Que derivado de las actividades que realizará como becario/estudiante/aprendiz, sostiene conversaciones y tiene o pretende entablar relaciones ("la Relación") con la Empresa.
- a. Su domicilio se encuentra en:
Av. Nicolás Morelos No. 63, Unidad Morelos 1ra Sección, Coacalco, México
- d. Que cuenta con las facultades suficientes para celebrar el presente Convenio y obligarse en términos del mismo.
- e. Reconoce que, como consecuencia de su Relación con la Empresa, y debido a las actividades que desempeña, tiene pleno acceso a la Información Confidencial que resulta delicada, valiosa, ventajosa y/o relevante para la propia Empresa, para sus clientes, para personas jurídicamente relacionadas con ésta, o para terceros, y que su uso, revelación o divulgación no autorizada, podría causar graves repercusiones jurídicas y económicas a ésta.
- f. Dentro de la documentación e Información Confidencial y exclusiva a la que ha tenido y tendrá acceso, se encuentra, enumerativa mas no limitativamente, proyectos, entregables, clientes, material de capacitación, material de estudio, planes de trabajo, software, licenciamiento, referente al manejo de la propia Empresa, actividades, instalaciones, sus proyectos y actividades operativas, personal, software, proyectos por desarrollar, relaciones comerciales, financieras, estrategias, tarifas, clientes, perfiles de servicios, así como la relacionada en el presente Convenio sus clientes, filiales, subsidiarias y demás compañías relacionadas directa o indirectamente, tanto vinculada con su objeto social y operaciones, como con su manejo y cuestiones estructurales, (la "Información Confidencial").
- g. Manifiesta su anuencia para indemnizar a la Empresa, por cualquier daño o perjuicio que el incumplimiento de las obligaciones aquí contenidas pudiera causarles.
- h. Bajo protesta de decir verdad que, no ha realizado, ni realizará actos de sustracción, destrucción, fotocopiado, duplicado, fotografía, video, sin perjuicio del medio de constancia, archivo o almacenaje, ninguna documentación o Información Confidencial, interna, relevante o delicada para o relacionada con la Empresa, sus prestadores de servicios, colaboradores, clientes, o personas de cualquier manera vinculadas jurídicamente con ella o cualquier tipo de Información Confidencial o interna que pudiera haberle sido entregada para el desempeño de sus actividades y que tenga una trascendencia tal que pudiera causarle algún daño o perjuicio a la Empresa derivado de la sustracción, destrucción o fotocopiado no autorizado por ésta.
- i. Manifiesta bajo protesta de decir verdad que no conserva por sí o a través de interpósita persona, ni ha entregado a tercero alguno o divulgado de cualquier manera, ya sea oral, gráfica o escrita, absolutamente ninguna documentación o Información Confidencial de la Empresa, o relacionada directa o indirectamente con ésta, sea original o copia, sin importar la forma de constancia, archivo o almacenamiento.

III. Declaran las Partes que:

- a. Reconocen y acuerdan que las Declaraciones antes señaladas constituyen el motivo determinante de la voluntad de la Empresa para mantener la Relación con el Receptor.
- b. Por así convenir a sus intereses, es su deseo y libre voluntad obligarse a lo dispuesto por las siguientes:

CLÁUSULAS

PRIMERA. Objeto: El presente convenio tiene como objeto proteger la Información Confidencial que compartirán las Partes, a efecto de que el Receptor no tome ventaja de la Información Confidencial o interna en mención, que reciba y/o conozca referente y de propiedad de:

SPERTO SINERGIA ENFOCADA, EXPERTOS EN SISTEMAS DE GESTIÓN Y LAS FILIALES, SUBSIDIARIAS Y/O CLIENTES DE EFD QUE SE SUMEN A LAS AQUÍ MENCIONADAS.

Las Partes convienen que toda la Información Confidencial que se revele entre ellas estará amparada por el deber de confidencialidad en términos del presente.

SEGUNDA. Deber de Confidencialidad: El Receptor únicamente utilizará la Información Confidencial facilitada por la Empresa para los fines de la Relación entre las Partes, comprometiéndose el Receptor a mantener la más estricta confidencialidad respecto de la Información Confidencial recibida, advirtiendo del deber de confidencialidad y secreto a los terceros, que por su Relación con el Receptor, deban tener acceso a la Información Confidencial otorgada para el correcto cumplimiento de las obligaciones del Receptor para con la Empresa. En este sentido, se entenderá que el Receptor debe asegurarse que el representante legal o cada persona física o moral que deba acceder a la Información Confidencial por causas legales o debidamente fundadas, revelada por la Empresa se adhiera al compromiso de confidencialidad establecido en el presente acuerdo.

El Receptor y las personas mencionadas en el párrafo anterior no podrán reproducir, modificar, hacer pública o divulgar a terceros la Información Confidencial objeto del presente acuerdo sin previa autorización escrita y expresa de la Empresa.

En caso de que la Empresa otorgue la autorización escrita para facilitar la Información Confidencial a un tercero, se procederá de la siguiente forma:

(i) La Empresa firmará con el tercero un Convenio de confidencialidad previo a que el Receptor proporcione en todo o en parte la Información Confidencial al tercero, para lo cual el Receptor deberá cerciorarse antes de divulgar la Información Confidencial, si efectivamente la Empresa y el tercero firmaron el correspondiente Convenio de confidencialidad.

Además de lo anterior, el Receptor se obliga a no celebrar con ninguna persona física o moral, cualquier tipo de acuerdo, convenio, contrato, negociación o asumir obligaciones que estén en conflicto con el presente acuerdo o que derive o implique el incumplimiento del mismo.

Asimismo, el Receptor adoptará respecto de la Información Confidencial objeto de este convenio las mismas medidas de seguridad que normalmente adoptaría respecto a la Información Confidencial de sus propios negocios o intereses, evitando por todos los medios a su alcance la pérdida, robo o sustracción de la Información Confidencial compartida por la Empresa.

TERCERA. Propiedad De La Información Confidencial: Los derechos de propiedad de la Información Confidencial objeto del presente acuerdo pertenecen únicamente a la Empresa y el hecho de facilitar al Receptor para el objeto mencionado en la cláusula primera no modifica tal situación, lo cual implica que la Empresa conservará para sí los derechos inherentes a la propiedad de la Información Confidencial que se haga llegar a el Receptor.

El Receptor reconoce que la Información Confidencial de cualquier naturaleza, incluso la distribuida, recopilada o discutida en juntas y/o reuniones, documentos en general, políticas, organización, sistemas de administración, Información Confidencial, comercial, tecnología usada y/o desarrollada durante el periodo de su colaboración, procedimientos y todos aquellos hechos, actos e Información Confidencial que con motivo de su trabajo sean de su conocimiento es propiedad de la Empresa y, por lo tanto, se obliga a no utilizar o divulgarla, ya sea directa o indirectamente, en su beneficio o en beneficio de terceras personas, especialmente la descrita de manera enunciativa y no limitativa en el presente convenio.

En consecuencia, en ningún caso y por ningún motivo se entenderá que la Información Confidencial compartida por alguna de las partes constituirá una copropiedad y el Receptor reconoce que el derecho de que la Empresa le comparta Información Confidencial no le otorga ningún derecho de licencia, patente o propiedad intelectual sobre la misma, y que la revelación de la Información Confidencial no originará ninguna obligación a la Empresa de otorgar derecho alguno sobre dicha Información Confidencial.

CUARTA. Uso de la Información Confidencial: El Receptor se obliga a guardar absoluta confidencialidad sobre la Información Confidencial que debido a sus actividades llegue a conocer o tener en su poder, debiendo usar dicha Información Confidencial exclusivamente en beneficio de la Empresa.

Asimismo, el Receptor se obliga a no mantener en su poder copia alguna o reproducción, total o parcial de la documentación o Información Confidencial señalada, bajo cualquier forma o medio de constancia, archivo o almacenamiento, en caso de contravenir con lo anteriormente citado responderá de los daños y perjuicios que ocasione, aunado a las penalidades de las que pueda ser objeto.

El Receptor se obliga a resguardar en todo momento la información ya sea en proceso o producto terminado dentro de los espacios corporativos designados que sean propiedad de la EMPRESA. Por lo tanto, el Receptor no podrá resguardar de forma temporal ni definitiva documentos o información propiedad de la Empresa, sus clientes, filiales, proyectos, colaboradores, socios comerciales en ningún dispositivo personal ni en ningún dispositivo que no sea propiedad de la empresa.

QUINTA. Toda la Información Confidencial, documentación comercial relevante, delicada o secreta de la Empresa tiene el carácter de confidencial bajo el presente instrumento y por tanto de secreto industrial, en los términos del artículo 82 de Ley Federal de Protección a la Propiedad Industrial, por tratarse de aplicaciones de carácter industrial y/o comerciales que se traducen en obtener o mantener una ventaja competitiva o económica frente a terceros en la realización de las actividades económicas que le son propias a la Empresa, y respecto de las cuales se han adoptado los medios o sistemas suficientes para preservar su confidencialidad y el acceso restringido a la misma.

En los términos de los artículos 84 y 85 de la Ley Federal de Protección a la Propiedad Industrial, el Receptor deberá abstenerse de revelar, sin el previo consentimiento por escrito de la Empresa, ya sea durante o después de la terminación del presente Convenio, cualquier secreto industrial.

De acuerdo con lo anterior, el Receptor manifiesta para todos los efectos a que haya lugar, que conoce y entiende cabalmente lo dispuesto en la Ley Federal de Protección a la Propiedad Industrial, conforme al cual, las siguientes conductas inadecuadas respecto del manejo de los secretos industriales se tipifican como delictivas:

"Artículo 402: Son delitos:

...

III.- Divulgar a un tercero un secreto industrial, que se conozca con motivo de su trabajo, puesto, cargo, desempeño de su profesión, relación de negocios o en virtud del otorgamiento de una licencia para su uso, sin consentimiento de la persona que ejerza su control legal o de su usuario autorizado, LEY FEDERAL DE PROTECCIÓN A LA PROPIEDAD INDUSTRIAL CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN Secretaría General Secretaría de Servicios Parlamentarios Nueva Ley DOF 01-07-2020 90 de 94 habiendo sido prevenido de su confidencialidad, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto;

IV.- Apoderarse de un secreto industrial sin derecho y sin consentimiento de la persona que ejerza su control legal o de su usuario autorizado, para usarlo o revelarlo a un tercero, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a quien ejerce su control legal o a su usuario autorizado;

V.- Usar la información contenida en un secreto industrial, que conozca por virtud de su trabajo, cargo o puesto, ejercicio de su profesión o relación de negocios, sin contar con el consentimiento de quien ejerce su control legal o de su usuario autorizado, o que le haya sido revelado por un tercero, que éste no contaba para ello con el consentimiento de la persona que ejerce su control legal o su usuario autorizado, con el propósito de obtener un beneficio económico o con el fin de causar un perjuicio a quien ejerce el control legal del secreto industrial o su usuario autorizado;

VI.- Apropiarse, adquirir, usar o divulgar indebidamente un secreto industrial a través de cualquier medio, sin consentimiento de quien ejerce su control legal o de su usuario autorizado; con el propósito de causarle perjuicio u obtener un beneficio económico para sí o para un tercero..."

SEXTA. Notificación Requerimiento de Autoridad: Si el Receptor fuera requerido por Autoridad competente de cualquier tipo para revelar Información Confidencial delicada, relevante o Información Confidencial de la Empresa, el Receptor se obliga a dar aviso por escrito a la Empresa dentro de los 3 (tres) días hábiles siguientes a la recepción del documento respectivo, con la finalidad de que esta última pueda ejercitar los actos o derechos que correspondan para salvaguardar sus intereses.

SÉPTIMA. Devolución de la Información Confidencial: El Receptor al momento de la terminación de la Relación con la Empresa, se obliga a devolver en ese mismo momento, absolutamente toda la Información Confidencial que obre en su poder. El Receptor también se obliga a entregar a la Empresa todas las pertenencias de aquél usadas por el Receptor durante la Relación.

OCTAVA. Pena Convencional: El Receptor se obliga a indemnizar inmediatamente a la Empresa con una pena equivalente a \$500,000.00 (quinientos mil pesos 00/100 M.N.), más intereses moratorios desde la fecha de terminación de la Relación hasta la fecha efectiva de pago, a una tasa anual de 10% (diez por ciento), en caso de que la Información Confidencial compartida resulte revelada, divulgada o utilizada por el Receptor de cualquier forma distinta al objeto de este convenio, ya sea de forma dolosa o por mera negligencia aunado a cualquier daño o perjuicio que el incumplimiento de las obligaciones adquiridas en este Convenio le causara.

La obligación anterior, se hará extensiva respecto de los clientes o proveedores de la Empresa, de los cuales obtenga cualquier Información Confidencial, con motivo de la Relación entre el Receptor y la Empresa.

NOVENA. Vigencia: Este Convenio estará en vigor durante todo el plazo de vigencia de la Relación o relaciones de índole comercial que une o unirá a el Receptor con la Empresa y hasta cumplidos 10 (diez) años contados a partir de la fecha de terminación de la Relación entre las Partes.

DÉCIMA. Cumplimiento: El Receptor estará obligado a cumplir sus obligaciones bajo el presente Convenio independientemente del lugar en el que desempeñe sus actividades y respecto de la Información Confidencial de la Empresa, así como de sus subsidiarias o afiliadas, independientemente del lugar en el que éstas desempeñen su negocio, incluyendo sin limitar la República Mexicana, así como en Estados Unidos de Norteamérica, Centroamérica, Canadá, y Sudamérica.

DÉCIMA PRIMERA. Notificaciones: Para cualquier notificación, aviso o comunicado vinculado con este convenio, las Partes señalan como sus domicilios convencionales los siguientes:

LA EMPRESA

Domicilio: ave. Lago Zurich
219, plaza carso piso 12, col.
Ampliación granada cdmx cap
11529
Correo Electrónico:
Vania.carvallo@trezentos.mx

EL RECEPTOR

Av. Nicolás Morelos No. 63, Unidad Morelos
1ra Sección, Coacalco, México
Correo Electrónico: lizeth.gutierrez@trezentos.mx

DÉCIMA SEGUNDA. Acuerdo Completo: Este Convenio constituye y expresa el total entendimiento entre las Partes en Relación con su objeto, así como su total entendimiento y

condiciones, ya sean implícitas o expresas, orales o escritas. Ni el Convenio en su totalidad ni alguna parte de este podrán ser alterados, cambiados, renunciados o modificados sino mediante un convenio por escrito debidamente aceptado y firmado por ambas Partes.

DÉCIMA TERCERA. Nulidad: La invalidez o exclusión de alguna de las Cláusulas de este Convenio o parte de ella, no modificará ni alterará el contenido de las cláusulas que permanezcan, mismas que deberán continuar en vigor y en efecto, e interpretadas como si las inválidas o excluidas no hubieren sido insertadas.

DÉCIMA CUARTA. Avisos, Firmas Electrónicas: Las Partes convienen en que el presente Contrato, sus anexos, apéndices, modificaciones, y demás documentos que se otorguen de conformidad con el mismo, podrán celebrarse y entregarse ya sea mediante firma autógrafa, o digitalmente por cada una de ellas utilizando el sistema de firmas electrónicas <<DocuSign>> u otro que convengan que cuente con los certificados emitidos por un Prestador de Servicios de Certificación (PSC), conforme a los dispuesto por la Ley de Firma Electrónica Avanzada. Cuando se celebren usando dicho sistema, los documentos electrónicos enviados a través de dicho sistema a las direcciones de correo electrónico señaladas por cada parte (o las que las sustituyan conforme al mismo), tendrán el mismo valor que las que cuenten con firma autógrafa, así como presunción de integridad y presunción de atribución de las firmas y se entenderán por hechas o recibidas cuando sean enviadas a la dirección electrónica antes indicada, siempre que no se le haya notificado al emisor un rechazo de la misma por parte de la dirección electrónica del Receptor, de su proveedor de correo o host.

DÉCIMA QUINTA. Interpretación y jurisdicción: Para la interpretación y cumplimiento de este Convenio las Partes aceptan sujetarse a la jurisdicción y leyes de los tribunales competentes de la Ciudad de México, renunciando expresamente a cualquier otro fuero que, por razón de sus domicilios presentes o futuros, o por cualquier otra razón, pudiera corresponderles.

Leído que fue este Convenio por las Partes y enteradas plenamente de su contenido y efectos legales y no existiendo ninguna clase de vicio, dolo o mala fe, ambas lo firman en original en 2 (dos) tantos de conformidad, en Miguel Hidalgo CDMX, el día 13 de octubre del 2023.

La Empresa



Vania Carvallo Ruiz

El Receptor
Por Su Propio Derecho

DocuSigned by:
Lizeth Viridiana Gutierrez Guerra
E0A4FCB02EC45E

Lizeth Viridiana Gutiérrez Guerra

Figura 81 Firmas Contrato de confidencialidad