



TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DE APIZACO

**MANUAL DE GESTIÓN DOCUMENTAL: DIRECTRICES Y
PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DE LA
CERTIFICACIÓN TISAX EN MÉXICO SONAVOX
ELECTRONICS CO**

TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL

**PARA OBTENER EL TÍTULO PROFESIONAL DE:
INGENIERÍA EN ADMINISTRACIÓN**

**PRESENTA:
ANA PATRICIA PORTILLO HERNÁNDEZ**

**NOMBRE DEL ASESOR:
DR. JOSÉ LUIS MORENO RIVERA**



APIZACO, TLAX., AGOSTO 2025



Apizaco, Tlax., 21/Noviembre/2025.

ASUNTO: Liberación de Proyecto para Titulación Integral.

LIC. CECILIA YARELLY AREGUIN LARA
JEFE DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES
P R E S E N T E.

Por este medio le informo que ha sido liberado el siguiente proyecto para la Titulación Integral:

a) Nombre del Egresado:	ANA PATRICIA PORTILLO HERNÁNDEZ
b) Carrera:	INGENIERÍA EN ADMINISTRACIÓN
c) Número de Control:	20371119
d) Nombre del proyecto:	MANUAL DE GESTIÓN DOCUMENTAL: DIRECTRICES Y PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DE LA CERTIFICACIÓN TISAX EN MÉXICO SONAVOX ELECTRONICS CO.
e) Producto	TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL

Agradezco de antemano su valioso apoyo en esta importante actividad para la formación profesional de nuestros egresados.

ATENTAMENTE

Excelencia en Educación Tecnológica®
Pensar para Servir, Servir para Triunfar®

MTRA. NORMA ANGÉLICA AGUIÑAGA SÁNCHEZ
JEFA DEL DEPARTAMENTO DE CIENCIAS
ECONÓMICO-ADMINISTRATIVAS.

ASESOR
DR. JOSÉ LUIS MORENO RIVERA

NAAS/mcvh



SECRETARÍA DE EDUCACIÓN PÚBLICA
TECNOLÓGICO NACIONAL
DE MÉXICO
INSTITUTO TECNOLÓGICO DE APIZACO
DEPARTAMENTO DE
CIENCIAS ECONÓMICO
ADMINISTRATIVAS



2025
Año de
La Mujer
Indígena

Av. Instituto Tecnológico No. 418, San Andrés Ahuashuatepec,
Municipio de Tzompantepec, Tlaxcala, Mex. C.P. 90491 Tel. (241)
4472010 Ext. 105, e-mail: cea@apizaco.tecnm.mx tecnm.mx |





Educación
Secretaría de Educación Pública



TECNOLÓGICO
NACIONAL DE MÉXICO



Instituto Tecnológico de Apizaco
División de Estudios Profesionales

Tzompantepec, Tlaxcala, **24/Noviembre/2025**

ANA PATRICIA PORTILLO HERNÁNDEZ
EGRESADO(A) DE LA CARRERA DE INGENIERÍA EN ADMINISTRACIÓN
CON NÚMERO DE CONTROL 20371119.
P R E S E N T E.

Por este medio, me permito informar a usted que por aprobación de la comisión revisora asignada para valorar el trabajo que mediante la opción **TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL** y cuyo tema es: **"MANUAL DE GESTIÓN DOCUMENTAL: DIRECTRICES Y PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DE LA CERTIFICACIÓN TISAX EN MÉXICO SONAVOX ELECTRONICS CO."**, conforme a lo establecido en el procedimiento para la obtención del Título Profesional en el Instituto Tecnológico, la División de Estudios Profesionales a mi cargo le otorga la:

AUTORIZACIÓN DE IMPRESIÓN

Debiendo entregar **1 USB** del mismo, apropiadamente empastados, a la brevedad, para presentar su Acto de Recepción Profesional.

Sin otro particular por el momento me despido.

ATENTAMENTE
Excelencia en Educación Tecnológica®
Pensar para Servir, Servir para Triunfar®

CECILIA YARELY ARREGUÍN LARA
JEFA DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES



ccp. Archivo
CYAL/Gsc*



2025
Año de
La Mujer
Indígena

Av. Instituto Tecnológico No. 418, San Andrés Ahuashuatepec,
Municipio de Tzompantepec, Tlaxcala, Mex. C.P. 90491 Tel. (241) 4172010
Ext. 304, e-mail: dep_titulacion@apizaco.tecnm.mx | apizaco.tecnm.mx



Agradecimientos

Este proyecto representa el cierre de una etapa importante en mi formación profesional, y no habría sido posible sin el respaldo, la guía y el compromiso de personas clave en este proceso.

A mi madre Eulalia Hernández Romero, mi padre Emilio Portillo Castillo y mis hermanos, mi más profundo agradecimiento por su amor, confianza y apoyo incondicional, por creer en mí en todo momento y por brindarme la fortaleza emocional para seguir adelante con determinación, incluso en los momentos más desafiantes.

A una persona muy especial que me acompañó durante una etapa fundamental de mi carrera. El apoyo incondicional, la disposición para escucharme, las palabras de aliento y la confianza que siempre deposito en mí, recordándome constantemente la capacidad y fortaleza que forman parte de mi esencia.

A mis profesores de la universidad, especialmente a Guadalupe Rodríguez García y a Karen Aranju Lozano Rojas por compartir sus conocimientos con vocación y entrega. Cada enseñanza, orientación y consejo ha sido fundamental en mi crecimiento académico y personal.

Al Dr. José Luis Moreno Rivera, mi asesor académico, por su acompañamiento, paciencia y guía a lo largo del desarrollo de este proyecto. Su experiencia, claridad y compromiso fueron elementos esenciales para lograr un trabajo estructurado y con sentido.

Al Lic. Josué Alexander Ávila García, asesor por parte de la empresa, por brindarme la oportunidad de integrarme a un entorno profesional real, por su disposición, orientación constante y confianza en mi desempeño.

A todos ustedes, gracias por ser parte de este camino. Cada palabra, cada gesto y cada enseñanza dejaron una huella valiosa en este logro que hoy culmina.

.

Índice

Introducción.....	13
Problemática	14
Objetivos	15
Objetivo General.....	15
Objetivos Específicos	16
Justificación.....	16
Alcances.....	17
Delimitación.....	18
CAPÍTULO I Marco de Referencia	18
1.1. Estado del Arte	18
Gestión Documental en Entornos Organizacionales.....	19
Certificación TISAX en la Industria Automotriz.....	19
Normativas Internacionales y Marco de Seguridad de la Información	20
Tecnología e Innovación en la Gestión Documental	20
1.2. Marco Teórico	21
Auditoría Administrativa.....	21
Gestión de la Calidad	24
Desarrollo Organizacional	27
1.3. Marco Contextual.....	30
Entorno empresarial en Tlaxcala.....	30
Sector automotriz en Tlaxcala	30
Diagnostico Organizacional y Documental.....	30
La Empresa.....	30
Historia	31

Misión.....	31
Visión	32
Valores	32
Giro	32
Ubicación	32
Estructura Organizacional	33
Funciones Clave	33
TI y su Gestión Documental	35
Área de TI en Relación con el Estándar TISAX.....	36
TI en cumplimiento del Estándar TISAX.....	36
Gestión Documental.....	38
Industria Automotriz	39
ENX Association.....	41
VDA (Asociacion Alemania de la Industria Automotriz)	42
ISA (Information Security Assessment)	43
TISAX (Trusted Information Security Assessment Exchange)	44
Seguridad de la Información	46
RGPD (Reglamento General de Protección de Datos)	47
Normas ISO	48
Conceptos Básicos	49
Estándares de Seguridad.....	49
Certificación	49
Manuales.....	50
Políticas de Información	50
Procedimientos de Información	50

TICs en la Gestión Documental	51
Clasificación de la Información.....	52
CAPÍTULO II Metodología de Investigación	52
Diagnóstico organizacional	52
Enfoque Metodológico	53
Tipo de Investigación	53
Técnicas de Recolección de Datos	53
Población y Muestra	56
Población objetivo	56
Muestra	56
Instrumentos Utilizados.....	57
1. Guía de Entrevista.....	57
2. Encuesta	58
3. Observación Directa	60
4. Lista de Cotejo (Checklist)	61
Análisis de Datos	63
Procedimiento para el cálculo de porcentajes en los resultados	63
Análisis de la Entrevista	63
Análisis de la Encuesta	81
Análisis de la Observación Directa.....	91
Análisis de Checklist	96
Diagnostico Documental del Área de TI (Actual)	98
Problemas Detectados	98
Matriz de Factores Internos (MFI) – Proyecto Manual de Gestión Documental	99

Áreas de Mejora Identificadas	102
Evaluación de Impacto Esperado – Implementación del Manual de Gestión Documental	103
CAPÍTULO III Estructura del Manual de Gestión Documental	105
CAPÍTULO IV Implementación de la Propuesta.....	106
Plan de Capacitación del Personal (mayo – junio)	106
Cronograma de Capacitación.....	107
Validación de Formatos Documentales (junio).....	107
Fases de Implementación del Manual (junio - agosto)	108
CAPÍTULO V Seguimiento y Mejora Continua	109
Indicadores de Control y Auditoría	109
Comparación de Indicadores por Periodo (anual).....	110
Plan de Auditoría Interna (agosto - diciembre).....	110
Mecanismos de Retroalimentación y Actualización	111
Resumen de Fechas Clave.....	111
Resultados del Manual de Gestión Documental	112
Conclusiones.....	113
Conclusiones del Proyecto	113
Recomendaciones	115
Experiencia Personal Profesional Adquirida	115
Competencias Desarrolladas y/o Aplicadas	116
Fuentes de Información.....	118
Anexo	123
Manual de Seguridad de la Información	123

Índice de Contenido Visual

Imagen 1: Google Maps	33
Cronograma 1: Capacitación al personal de la empresa.....	107

Índice de Tablas

Tabla 1: Marcas con mayor producción y exportación 2024.....	41
Tabla 2: Resultados de la observación directa	61
Tabla 3: Acceso a información documental	64
Tabla 4: Encontrar documentos con facilidad	64
Tabla 5: Dificultad para encontrar documentos	65
Tabla 6: Principales dificultades al encontrar documentos	66
Tabla 7: Organización de documentos en el área de trabajo	67
Tabla 8: Sistema de clasificación específico.....	68
Tabla 9: Búsqueda de documentación con la clasificación actual	69
Tabla 10: Mejoras sugeridas por los entrevistados.....	70
Tabla 11: Políticas claras sobre el control de versiones de los documentos	71
Tabla 12: Problema al trabajar con versiones antiguas o desactualizadas de un documento.....	72
Tabla 13: Uso de documentos recientes	73
Tabla 14: Medidas de seguridad para proteger los documentos sensibles	74
Tabla 15: Protección de documentos	75
Tabla 16: Política de acceso a documentos confidenciales.....	76
Tabla 17: Descripción del sistema documental.....	78
Tabla 18: Aspectos de la función actual del sistema documental.....	79
Tabla 19: Principales problemas en la gestión documental	80
Tabla 20: Uso de categorías para clasificar documentos	81

Tabla 21: Documentos clasificados de manera uniforme en todas las áreas	82
Tabla 22: Controles de acceso para documentos sensibles.....	82
Tabla 23: Documento asignado por un responsable en custodia	83
Tabla 24: Registros de versiones de documentos	84
Tabla 25: Documentos con fecha de crearon y edición	85
Tabla 26: Documentos críticos protegidos.....	86
Tabla 27: Procedimientos de copia de seguridad de la documentación	87
Tabla 28: Documentación con estándares ISO/IEC 27001 o TISAX	88
Tabla 29: Auditorías al sistema documental	89
Tabla 30: Análisis de la observación directa: escala de ponderación	91
Tabla 31: Categoría y numero de indicadores	91
Tabla 32: Evaluación: clasificación de documentos.....	92
Tabla 33: Evaluación: almacenamiento físico y digital.....	92
Tabla 34: Evaluación: acceso a documentos.....	93
Tabla 35: Evaluación: seguridad en el manejo de documentos.....	93
Tabla 36: Evaluación: cumplimiento con políticas TISAX	94
Tabla 37: Evaluación de ponderación por categoría.....	94
Tabla 38: Promedio general: final de evaluación	95
Tabla 39: Porcentaje de cumplimiento.....	95
Tabla 40: Resumen e interpretación de resultados obtenidos en la lista de cotejo aplicada	97
Tabla 41: Matriz de Factores Internos (MFI) – Proyecto Manual de Gestión Documetal	101
Tabla 42: Evaluación de impacto esperado – Implementación del manual de gestión documental.....	104
Tabla 43: Plan de capacitación del personal (mayo – junio).....	107

Tabla 44: Formatos documentales que requieren revisión	108
Tabla 45: Fases de implementación del manual (junio - agosto).....	109
Tabla 46: Indicadores de control y auditoría	110
Tabla 47: Comparación de indicadores por periodo (anual)	110
Tabla 48: Plan de auditoría interna (agosto - diciembre)	111
Tabla 49: Mecanismos de retroalimentación y actualización	111
Tabla 50: Resumen de fechas clave.....	112

Índice de Gráficas

Gráfica 1: Acceso a información documental	64
Gráfica 2: Porcentaje al encontrar documentos con facilidad	65
Gráfica 3: Porcentaje de dificultad al encontrar documentos	66
Gráfica 4: Porcentaje de Principales dificultades al encontrar documentos	67
Gráfica 5: Porcentaje de organización de documentos en el área de trabajo	68
Gráfica 6: Porcentaje de uso de sistema de clasificación específico	69
Gráfica 7: Porcentaje de búsqueda de documentación con la clasificación actual	70
Gráfica 8: Porcentaje de mejoras sugeridas por los entrevistados.....	71
Gráfica 9: Porcentaje de políticas claras sobre el control de versiones de los documentos.....	72
Gráfica 10: Porcentaje de problema al trabajar con versiones antiguas o desactualizadas de un documento	73
Gráfica 11: Porcentaje de uso de documentos recientes	74
Gráfica 12: Porcentaje de medidas de seguridad para proteger los documentos sensibles	75
Gráfica 13: Porcentaje de protección de documentos.....	76

Gráfica 14: Porcentaje de la política de acceso a documentos confidenciales	77
Gráfica 15: Porcentaje de descripción del sistema documental	78
Gráfica 16: Porcentaje de aspectos de la función actual del sistema documental..	79
Gráfica 17: Porcentaje de los principales problemas en la gestión documental....	80
Gráfica 18: Porcentaje de uso de categorías para clasificar documentos	81
Gráfica 19: Porcentaje de documentos clasificados de manera uniforme en todas las áreas.....	82
Gráfica 20: Porcentaje de controles de acceso para documentos sensibles	83
Gráfica 21: Porcentaje de documentos asignados por un responsable en custodia	84
Gráfica 22: Porcentaje de registros de versiones de documentos	85
Gráfica 23: Porcentaje de documentos con fecha de crearon y edición.....	86
Gráfica 24: Porcentaje de documentos críticos protegidos	87
Gráfica 25: Porcentaje de procedimientos para crear copia de seguridad de la documentación	88
Gráfica 26: Porcentaje de la documentación con estándares ISO/IEC 27001 o TISAX	89
Gráfica 27: Porcentaje de auditorías al sistema documental	90
Gráfica 28: Cumplimiento de la lista de cotejo aplicada.....	97

Introducción

En un entorno empresarial globalizado y altamente competitivo, las organizaciones deben de alinear con estándares internacionales que no solo garanticen la seguridad de la información, sino que también generen confianza entre sus clientes y socios comerciales. En este contexto, la certificación TISAX (Trusted Information Security Assessment Exchange) se ha consolidado como un referente esencial en la industria automotriz y electrónica, al proporcionar un marco robusto para la protección de información sensible, la gestión eficiente de riesgos y la mejora continua de procesos.

Este proyecto tiene como finalidad el desarrollo de un Manual de Gestión Documental, que establecerá las directrices y procedimientos necesarios para la implementación de la certificación TISAX en Sonavox Electronics Co. A través de este manual, se brindará el apoyo necesario para lograr un mejor control en el archivo, recolección, manejo y protección de la información, asegurando el cumplimiento de los requisitos exigidos por dicha certificación.

Así mismo, la obtención de esta certificación representa no solo una mejora en términos de seguridad, sino también una ventaja competitiva. Permitirá a la empresa acceder a nuevos mercados internacionales, fortalecer vínculos con proveedores y clientes, cumplir con regulaciones globales sobre protección de datos y consolidarse como un socio confiable comprometido con altos estándares de calidad y seguridad.

El contenido del presente trabajo se estructura de la siguiente manera:

Capítulo 1: Marco teórico. Se presentan los conceptos fundamentales relacionados con la gestión documental, la seguridad de la información y el marco normativo de la certificación de TISAX.

Capítulo 2: Diagnostico organizacional y documental. Se realiza un análisis detallado actual de la empresa y en su gestión documental el enfoque metodológico utilizado para el desarrollo del proyecto, así como las técnicas de recopilación y análisis de información aplicadas.

Capítulo 3: Propuesta del Diseño del Manual de Gestión Documental. Se desarrolla la estructura del manual, incluyendo políticas, procedimientos y responsabilidades orientadas al cumplimiento de los requisitos de TISAX.

Capítulo 4: Implementación de la Propuesta. Se detalla las acciones necesarias para poner en práctica el Manual de Gestión Documental, con el objetivo de fortalecer la organización, trazabilidad y seguridad de la información dentro de la empresa. La propuesta contempla no solo la elaboración del manual, sino también estrategias de capacitación, validación de formatos y mecanismos para su adecuada adopción en todas las áreas operativas.

Capítulo 5: Seguimiento y Mejora Continua. Una vez implementado el manual, será indispensable establecer un sistema de seguimiento y mejora continua, orientado a evaluar su funcionamiento, detectar desviaciones y garantizar su actualización conforme evolucionen las necesidades de la organización.

Problemática

En la actualidad, Sonavox Electronics Co enfrenta diversos desafíos en la gestión de la información y la protección de datos, reflejados en la creciente demanda de sus socios comerciales y clientes de contar con una infraestructura sólida en seguridad de la información. A pesar de contar con una infraestructura con un sistema de gestión documental, la falta de claridad sobre los procedimientos a seguir y como implementarlos correctamente de acuerdo con las Normativas Internacionales de Seguridad y Protección de Datos en el Sector Automotriz, representa un obstáculo significativo para el crecimiento y la expansión de la empresa.

Cuestionamiento del Problema

1. ¿Cuál es el estado actual de la gestión documental en el área de Tecnologías de la Información de la empresa México Sonavox Electronics Co.?

2. ¿Qué estrategias o herramientas pueden implementarse para mejorar la gestión documental en dicha área, conforme a los requisitos de la certificación TISAX?
3. ¿Qué mecanismos de control y mejora continua pueden aplicarse para asegurar la eficiencia y actualización del sistema de gestión documental propuesto?

Presentándose los siguientes problemas:

- Aunque existe un sistema para el resguardo de los documentos realizados, los administrativos no tienen conocimiento de la importancia del resguardo de la información que manejan cada uno de ellos.
- La documentación esta desordenada y poco accesible lo que provoca dificultades para localizar información de manera oportuna, afectando la productividad del personal.
- La inexistencia de la estructura y clasificación de la información, así como el nombramiento del archivo creado, genera confusión sobre la vigencia y autenticidad de los documentos, poniendo en riesgo la integridad de la información.
- La ausencia de procedimientos definidos y evidencias documentales ordenadas podría generar observaciones o incumplimientos durante auditorías, especialmente en el contexto de estándares como TISAX.

Objetivos

Objetivo General

Diseñar e implementar un Manual de Gestión Documental en el área de Tecnologías de la Información de Sonavox Electronics Co., que permita estandarizar los procesos de manejo, clasificación, almacenamiento y control de la información, con el fin de cumplir con los requisitos de la certificación TISAX, mejorar la eficiencia operativa y reducir riesgos documentales, en un periodo no mayor a seis meses.

Objetivos Específicos

El Manual de Gestión Documental tiene como objetivos específicos los siguientes:

- Realizar un diagnóstico documental del área de Tecnologías de la Información (TI) de la empresa México Sonavox Electronics Co., con el fin de identificar áreas de oportunidad y debilidades en la gestión de la documentación existente.
- Diseñar una propuesta de manual de gestión documental, alineado con los requerimientos de la certificación TISAX, que permita establecer lineamientos claros para el manejo, resguardo y protección de la información dentro del área de TI.
- Definir un conjunto de indicadores de aceptación y mejora continua, que permitan evaluar la implementación del manual propuesto, así como identificar oportunidades para su ajuste y optimización futura.

Justificación

La adopción de un Manual de Gestión Documental con alineamientos de TISAX representa un elemento esencial para Sonavox Electronics Co, ya que permite robustecer la seguridad de la información y garantizar el cumplimiento de Normativas Internacionales exigidas por la industria automotriz.

Ante un entorno empresarial cada vez más exigente y regulado, este manual constituye de herramientas estratégicas para mejorar el control, acceso y resguardo de los documentos, así como los requisitos para el cumplimiento de la protección de la información, asegurando la trazabilidad, integridad y confidencialidad de la información manejada dentro del área de Tecnologías de la información.

Por ello, este manual beneficiará directamente a Sonavox Electronics Co, ya que permitirá:

- Mejora su organización documental, facilitando la ubicación, uso y resguardo de documentos clave.

- Reducir errores operativos, como la duplicidad de información, el uso de versiones obsoletas y la pérdida de documentos importantes.
- Fortalecer su posicionamiento ante clientes y auditores, al demostrar un compromiso con la transparencia, la eficiencia y el cumplimiento de estándares reconocidos internacionalmente como TISAX.
- Incrementar la seguridad de la información, al establecer protocolos claros sobre el manejo de datos sensibles y confidenciales, minimizando riesgos de fuga o el mal uso de la información.

Adicionalmente, el manual tendrá un impacto transversal en otras áreas de la empresa, ya que podría ser utilizado como documento de consulta y referencia para replicar buenas prácticas en otras unidades organizativas. También, será de gran utilidad para futuros estudiantes o profesionales interesados en la gestión documental y en la implementación de sistemas alineados con normas internacionales, promoviendo así una cultura organizacional más robusta, profesional y orientada a la mejora continua

Alcances

De manera específica, el proyecto contempla los siguientes alcances:

- Aplicación exclusiva en el área de Tecnologías de la Información (TI), donde se identificó la necesidad urgente de establecer directrices formales para la gestión documental.
- Clasificación, organización, acceso, almacenamiento y protección de documentos, garantizando un flujo documental eficiente y seguro que facilite la trazabilidad, consulta y uso adecuado de la información.
- Implementación de los niveles de seguridad definidos por el estándar TISAX, asegurando que la información sea tratada conforme a su nivel de confidencialidad y sensibilidad, mediante controles de acceso, autenticación y seguimiento.

Delimitación

Aunque el Manual de Gestión Documental propuesto representa un avance significativo para el área de Tecnologías de la Información, es importante señalar los límites establecidos para el presente proyecto, con el fin de acotar su alcance y establecer expectativas realistas:

- No cubre implementaciones tecnológicas a nivel software, como la adquisición o desarrollo de plataformas digitales para la automatización del sistema documental. El enfoque está centrado en la elaboración del manual y en los procedimientos organizativos documental.
- Realizar capacitación, formación y seguimiento continuo dependerá de la disposición y recursos internos de la empresa.
- Aplica principalmente a documentos internos del área de TI, por lo que no se aborda el ciclo completo de vida de productos o documentación externa relacionada con procesos productivos u operativos de otras áreas.

Estas delimitaciones permiten enfocar los refuerzos del proyecto en la creación del manual de una base sólida para la gestión documental interna, que podrá ser escalada o complementada en fases futuras conforme a las necesidades estratégicas de la empresa.

CAPÍTULO I Marco de Referencia

1.1. Estado del Arte

En el presente apartado se exponen los antecedentes científicos y técnicos relacionados con la gestión documental, la certificación en seguridad de la información (específicamente TISAX) y los marcos normativos y tecnológicos que sustentan el desarrollo del presente proyecto.

La revisión de literatura tiene como objetivo ofrecer un panorama actualizado de los principales hallazgos, enfoques y problemáticas detectadas en investigaciones previas, con el fin de sustentar metodológicamente las decisiones tomadas en el

desarrollo del manual de gestión documental en el área de TI de la empresa Sonavox Electronics Co.

Gestión Documental en Entornos Organizacionales

La gestión documental constituye un eje fundamental en el funcionamiento eficiente de las organizaciones, ya que permite controlar, organizar, preservar y recuperar la información generada durante los procesos administrativos y técnicos. De acuerdo con Marín y Rodríguez (2020) en su estudio publicado en *Redalyc*, la correcta implementación de sistemas de gestión documental impacta positivamente en la toma de decisiones, la transparencia organizativa y la trazabilidad de la información, especialmente en entornos altamente regulados o industriales.

Asimismo, se resalta que los sistemas de gestión documental deben ir acompañados de una política de información clara, procedimientos normalizados, criterios de clasificación y herramientas tecnológicas que permitan garantizar la seguridad y disponibilidad de los documentos (Marín, 2020). Este punto es particularmente relevante en la industria automotriz, donde los ciclos de auditoría, certificaciones y cumplimiento normativo son estrictos.

Certificación TISAX en la Industria Automotriz

La certificación TISAX (Trusted Information Security Assessment Exchange) ha ganado relevancia en los últimos años como un modelo de evaluación de la seguridad de la información orientado al sector automotriz, promovido por la Asociación Alemana de la Industria Automotriz (VDA). Esta certificación no solo aborda aspectos técnicos de protección de la información, sino que exige también la implementación de políticas documentales, controles de acceso, clasificación de la información y cumplimiento de la confidencialidad contractual.

De acuerdo con el estudio de Ríos et al. (Ríos, 2023). TISAX representa una respuesta adaptada a las necesidades del ecosistema de proveedores de la industria automotriz, especialmente ante los retos derivados del intercambio constante de información sensible. Su estructura permite una evaluación objetiva y comparable, facilitando el cumplimiento de normativas como ISO/IEC 27001 y el RGPD.

Normativas Internacionales y Marco de Seguridad de la Información

Diversas normativas internacionales han sido fundamentales en la conformación de marcos sólidos de gestión documental y seguridad de la información. Entre ellas destacan la ISO/IEC 27001, orientada a establecer sistemas de gestión de seguridad de la información (SGSI), y la ISO 15489, que se enfoca específicamente en los sistemas de gestión documental. Estas normas proponen estructuras organizativas, políticas, roles, responsabilidades y controles que permiten garantizar la integridad, disponibilidad y confidencialidad de la información.

González y Pérez (González, 2022) argumentan que la sinergia entre la gestión documental y los sistemas de seguridad de la información es clave para alcanzar niveles altos de gobernanza digital. Su investigación identifica que el uso combinado de tecnologías de clasificación automatizada, encriptación y monitoreo, junto con políticas claras de documentación y retención, son esenciales para cumplir con requisitos regulatorios como el RGPD o la Ley General de Protección de Datos Personales en México.

Tecnología e Innovación en la Gestión Documental

Finalmente, los avances tecnológicos aplicados a la gestión documental han permitido automatizar tareas, reducir errores humanos y mejorar la trazabilidad de los documentos. El uso de sistemas ECM (Enterprise Content Management), herramientas de clasificación inteligente, firmas digitales y

plataformas en la nube son elementos que han transformado los procesos tradicionales de archivo.

Según Mendoza y Ruiz (Mendoza, 2021), el uso de tecnologías de la información no solo mejora la productividad documental, sino que habilita esquemas de cumplimiento más ágiles frente a las exigencias normativas. En particular, en empresas del sector automotriz, donde los procesos deben ser auditables y trazables en tiempo real, estas tecnologías han resultado fundamentales para asegurar la competitividad.

1.2. Marco Teórico

El desarrollo del presente Manual de Gestión Documental, orientado a fortalecer la seguridad de la información y la eficiencia organizacional en la empresa, se respalda en diversas competencias adquiridas a lo largo de la carrera de Ingeniería en Administración. De manera particular, se sustenta en tres materias clave que aportan tanto las bases teóricas como las herramientas prácticas necesarias para su diseño e implementación: Auditoría Administrativa, Gestión de la Calidad, y Desarrollo Organizacional.

A continuación, se detalla el aporte de cada una de ellas al desarrollo e implementación del manual:

Auditoría Administrativa

La auditoría administrativa puede definirse como un proceso integral orientado a evaluar la gestión institucional desde una perspectiva global. De acuerdo con Gómez Ceja, G., la auditoría administrativa se enfoca en analizar las funciones, estructuras y procesos con el objetivo de detectar áreas de oportunidad que permitan optimizar los recursos humanos, financieros y materiales. En este sentido, no solo busca identificar errores o irregularidades, sino también generar propuestas de mejora que contribuyan al desarrollo organizacional (Gómez Ceja, 2019).

Por su parte, Reyes Ponce, A. (Reyes Ponce, 2018) señala que la auditoría administrativa se centra en revisar el cumplimiento de políticas, normas y

procedimientos, asegurando que las actividades realizadas sean congruentes con los objetivos institucionales. En otras palabras, constituye un medio de control y retroalimentación que apoya la toma de decisiones y la planificación estratégica.

Finalmente, Chiavenato destaca que este tipo de auditoría permite evaluar la eficacia de la gestión administrativa en todos los niveles, a través de un enfoque sistemático y objetivo que contribuye a fortalecer la productividad y la calidad de los servicios ofrecidos por la organización (Chiavenato, Introducción a la teoría general de la administración , 2017).

Teorías que sustentan la Auditoría Administrativa

1. Teoría del Control Administrativo

Koontz y Weihrich explican que el control administrativo es una función esencial de la gestión, la cual consiste en medir y corregir el desempeño de las actividades organizacionales para asegurar el cumplimiento de los planes. Esta teoría sustenta la auditoría administrativa, ya que ambas comparten el propósito de verificar que los resultados obtenidos sean congruentes con los objetivos planteados, permitiendo la aplicación de acciones correctivas cuando sea necesario (Koontz, 2016).

2. Teoría de Sistemas

Desde la perspectiva de la teoría de sistemas, la organización se concibe como un conjunto de elementos interdependientes que interactúan para alcanzar un propósito común (Bertalanffy L. v., 1968). La auditoría administrativa adopta este enfoque al analizar la organización de manera integral, considerando que las modificaciones en un área pueden impactar en otras. Así, la auditoría permite comprender las relaciones entre los diferentes subsistemas y su efecto en la eficiencia global.

3. Teoría de la Mejora Continua

La filosofía de la mejora continua, propuesta por Deming, sostiene que los procesos deben revisarse y perfeccionarse de manera constante para garantizar la calidad y competitividad organizacional. En este contexto, la auditoría administrativa funge

como una herramienta de diagnóstico y seguimiento que permite identificar deficiencias, implementar mejoras y fomentar una cultura de calidad dentro de la institución (Deming, 1986).

Procedimiento de la Auditoría Administrativa

El proceso de auditoría administrativa se desarrolla en diferentes etapas que aseguran una evaluación estructurada y coherente. Mantilla plantea que este procedimiento comprende cuatro fases fundamentales:

1. Planeación: En esta etapa se definen los objetivos, alcance, criterios y metodología de trabajo. Se recopila información preliminar y se establecen los instrumentos de auditoría.
2. Examen o evaluación: Consiste en la recopilación y análisis de información mediante entrevistas, observaciones y revisión de documentos, con el fin de detectar áreas problemáticas o de oportunidad.
3. Informe: En esta fase se presentan los hallazgos, conclusiones y recomendaciones que orientarán la toma de decisiones administrativas.
4. Seguimiento: Se verifica el cumplimiento de las acciones correctivas y se evalúa su efectividad para asegurar la mejora continua.

Cada una de estas etapas tiene como finalidad garantizar que la auditoría administrativa sea un proceso ordenado, objetivo y orientado a la optimización de los recursos institucionales (Mantilla, 2015).

Importancia y Aplicación de la Auditoría Administrativa

La aplicación de la auditoría administrativa en el contexto organizacional permite realizar evaluaciones objetivas de los procesos documentales y operativos. Gracias a ella, es posible identificar áreas de mejora, establecer mecanismos de control y asegurar que los procedimientos implementados sean eficientes, seguros y alineados con los objetivos institucionales (Gómez Ceja, 2019). Además, proporciona las bases metodológicas para la elaboración de informes, el seguimiento de hallazgos y la ejecución de acciones correctivas.

De esta manera, la auditoría administrativa no solo se convierte en un medio de diagnóstico, sino también en una herramienta estratégica que promueve la transparencia, la eficacia y la mejora continua en las organizaciones.

Gestión de la Calidad

La gestión de la calidad se define como el conjunto de actividades coordinadas para dirigir y controlar una organización en lo referente a la calidad (9001, 2015). Esta definición, proveniente de la *Norma ISO 9000:2015*, establece que la calidad no es un atributo aislado, sino un resultado de la gestión sistemática de procesos orientados a la mejora continua.

De acuerdo con Juran, la gestión de la calidad implica la planificación, el control y la mejora de la calidad en todas las fases de la organización, con el propósito de satisfacer las necesidades de los clientes y reducir los costos de no conformidad (Juran, 1990). Por su parte, Crosby considera que la calidad es el cumplimiento estricto de los requisitos establecidos, y que su gestión efectiva depende de la prevención de errores más que de la inspección posterior (Crosby P. B., 1996).

En síntesis, la gestión de la calidad es un enfoque integral que busca garantizar la eficiencia de los procesos, la satisfacción del cliente y el cumplimiento de los estándares internacionales aplicables (Evans, 2020)

Fundamentos Teóricos de la Gestión de la Calidad

1. Ciclo PHVA (Planear, Hacer, Verificar, Actuar)

El ciclo PHVA, también conocido como ciclo de Deming, constituye la base metodológica de los sistemas de gestión de la calidad. Según Deming (1986), este modelo de mejora continua propone un proceso cíclico en cuatro etapas:

1. Planear: Identificar oportunidades de mejora y establecer los objetivos.
2. Hacer: Implementar los planes y ejecutar las actividades programadas.
3. Verificar: Evaluar los resultados mediante indicadores y auditorías.

4. Actuar: Estandarizar los logros o aplicar acciones correctivas en caso de desviaciones.

Este ciclo es esencial para mantener la eficacia del sistema de gestión y promover la innovación y la eficiencia organizacional.

2. Teoría de la Mejora Continua

La teoría de la mejora continua, desarrollada por autores como Kaoru Ishikawa y W. Edwards Deming, sostiene que la calidad debe ser un proceso constante y no un objetivo temporal. Ishikawa argumenta que la mejora debe involucrar a todos los miembros de la organización, fomentando la participación y el trabajo en equipo. Este principio impulsa el concepto japonés de *Kaizen*, que promueve pequeños cambios diarios con un gran impacto acumulativo en la productividad y la satisfacción del cliente (Oakland, 2014).

3. Estándares Internacionales de Calidad: ISO 9001

La norma ISO 9001:2015 establece los requisitos para implementar un sistema de gestión de la calidad efectivo. Esta norma se basa en principios como el enfoque al cliente, el liderazgo, la participación del personal, el enfoque a procesos, la mejora continua, la toma de decisiones basada en evidencias y la gestión de las relaciones (9001:2015).

Su aplicación permite asegurar que los procesos organizacionales sean controlados, medibles y alineados con los objetivos estratégicos. Además, proporciona una base sólida para la certificación de sistemas de calidad y para la integración con otros estándares, como TISAX, especialmente relevante en el sector automotriz por su enfoque en la seguridad de la información.

Procedimientos y Aplicación Práctica

La implementación de un sistema de gestión de la calidad requiere la definición clara de procedimientos, responsabilidades y controles documentales. Según Oakland, un sistema efectivo debe incluir las siguientes etapas:

1. Diagnóstico inicial: Evaluación del contexto organizacional y de los requisitos normativos aplicables.
2. Planificación del sistema: Definición de políticas, objetivos y procesos clave.
3. Documentación: Elaboración de manuales, procedimientos e instructivos que aseguren la trazabilidad y el control de las actividades.
4. Implementación: Ejecución de los procesos definidos y capacitación del personal.
5. Auditoría interna y mejora: Revisión periódica del desempeño mediante auditorías y aplicación del ciclo PHVA.

Además, la figura del “dueño del proceso” adquiere relevancia, ya que se encarga de garantizar el cumplimiento de los procedimientos y la efectividad del sistema. Esta responsabilidad es esencial para mantener la conformidad con certificaciones internacionales como ISO 9001 y TISAX, que exigen evidencia documental y controles sobre la seguridad de la información.

Importancia de la Gestión de la Calidad en el Manual Institucional

La gestión de la calidad proporciona las herramientas necesarias para establecer procedimientos estandarizados y garantizar que la documentación institucional cumpla con los requisitos de certificación. Al aplicar los principios de la calidad en la elaboración del manual, se logra uniformidad en los procesos, se definen responsabilidades precisas y se promueve la eficiencia operativa (Crosby P. B., 1996).

Asimismo, la integración de los estándares de calidad y seguridad de la información, como TISAX, permite asegurar la confidencialidad, integridad y disponibilidad de los datos, aspectos fundamentales en sectores altamente regulados como el automotriz. En conjunto, estos elementos fortalecen la confianza de los clientes y contribuyen al desarrollo sostenible de la organización.

Desarrollo Organizacional

Según French y Bell, el desarrollo organizacional es un proceso de cambio planificado que busca aumentar la efectividad de la organización y su capacidad para adaptarse a su entorno mediante intervenciones en sus procesos y estructuras. Este enfoque enfatiza la participación activa de los miembros de la organización en la identificación de problemas y la construcción de soluciones colaborativas (French, 1999).

Para Robbins y Judge, el DO se enfoca en mejorar el desempeño organizacional a través del desarrollo de las personas, los equipos y las relaciones interdepartamentales. Su meta es generar un entorno de trabajo saludable, productivo y alineado con los objetivos estratégicos (Robbins S. P., 2017).

Por su parte, Chiavenato define el DO como un esfuerzo integral, planificado y de largo plazo que busca mejorar la efectividad de la organización mediante la aplicación de conocimientos de las ciencias del comportamiento. Este enfoque reconoce la importancia de la cultura organizacional, la comunicación y el liderazgo como pilares del cambio (Chiavenato, Introducción a la teoría general de la administración , 2017).

Teorías que Sustentan el Desarrollo Organizacional

1. Teoría del Cambio Planificado

Kurt Lewin, considerado uno de los fundadores del campo del desarrollo organizacional, propuso el modelo del cambio planificado, el cual consta de tres etapas:

1. Descongelar: Reconocer la necesidad de cambio y preparar a la organización para modificar sus patrones actuales de comportamiento.
2. Cambiar: Introducir nuevas ideas, procesos o estructuras.
3. Recongelar: Estabilizar el cambio y consolidar las nuevas prácticas.

Este modelo sirve como base para las intervenciones de DO, ya que permite gestionar el proceso de transición organizacional de manera estructurada y participativa (Lewin, 1951).

2. Teoría de Sistemas

La teoría de sistemas aplicada al DO considera que la organización es un conjunto de elementos interrelacionados que deben funcionar en armonía para lograr los objetivos institucionales (Bertalanffy L. v., 1968). Desde esta perspectiva, los cambios en un área, como la gestión documental o los procesos de comunicación interna, repercuten directamente en otras áreas del sistema. Por ello, el DO adopta una visión holística que facilita la comprensión de los problemas organizacionales y el diseño de soluciones integrales.

3. Teoría del Comportamiento Organizacional

El comportamiento organizacional estudia las actitudes, percepciones y relaciones interpersonales dentro de la empresa. Robbins y Judge destacan que comprender estos factores es fundamental para fomentar la motivación, la colaboración y el compromiso del personal. El DO utiliza estos principios para diseñar intervenciones que mejoren la dinámica de equipos, la comunicación y la cohesión organizacional, elementos clave en la ejecución de proyectos estratégicos como la implementación de un manual de gestión documental.

Técnicas e Instrumentos del Desarrollo Organizacional

El proceso de diagnóstico organizacional requiere la aplicación de herramientas que permitan recopilar información precisa sobre la situación actual de la empresa. Entre las técnicas más utilizadas se encuentran:

- Entrevistas dirigidas: Permiten obtener información cualitativa sobre percepciones, experiencias y opiniones del personal respecto a los procesos organizacionales.
- Observación directa: Facilita la identificación de comportamientos, rutinas y problemas reales en el entorno laboral (Werther, 2014).

- Cuestionarios o encuestas de diagnóstico: Permiten evaluar la cultura organizacional, la comunicación interna y la satisfacción laboral.

Aplicación del Desarrollo Organizacional en el Contexto de TI

El diagnóstico realizado al área de Tecnologías de la Información de Sonavox Electronics Co. reveló deficiencias relacionadas con la falta de protocolos estandarizados, la desorganización documental y la limitada comunicación entre los colaboradores. Estos problemas reflejan una ausencia de estructuras formales de control y de mecanismos claros para la gestión de información sensible, lo cual representa un riesgo ante auditorías externas y el cumplimiento de estándares internacionales como TISAX (Automobilindustrie, 2022).

La aplicación de las herramientas del DO permitió identificar las causas raíz de estas problemáticas y proponer estrategias de cambio, tales como la implementación de un Manual de Gestión Documental, la definición de responsabilidades y la mejora de la comunicación interdepartamental. Estas acciones no solo fortalecen la eficiencia operativa, sino que también promueven una cultura organizacional basada en la mejora continua y la seguridad de la información.

Importancia del Desarrollo Organizacional en la Mejora Continua

El DO no se limita a resolver problemas aislados, sino que impulsa una transformación integral orientada al aprendizaje y la adaptación constante. Como señala Beckhard, el desarrollo organizacional fomenta la capacidad de la organización para renovarse y ajustarse a los cambios del entorno (Beckhard, 1969). En el caso de Sonavox Electronics Co., el proceso de desarrollo organizacional no solo busca corregir las deficiencias documentales, sino también promover una cultura de orden, comunicación efectiva y compromiso con los estándares internacionales de calidad y seguridad.

1.3. Marco Contextual

Entorno empresarial en Tlaxcala

De acuerdo con datos recientes, el estado de Tlaxcala cuenta con 72,662 empresas registradas distribuidas a lo largo de sus 60 municipios. De este total, aproximadamente 10,997 corresponden a industrias manufactureras, lo cual representa un sector productivo significativo (Rankeando, 2025).

Sector automotriz en Tlaxcala

Aunque no se dispone de un número exacto de empresas automotrices en el estado, sí se sabe que la región forma parte de corredores industriales relevantes como el corredor Puebla-Tlaxcala, con núcleos como Papalotla, Panzacola y el corredor de Huamantla, donde operan empresas automotrices y fabricantes de componentes. Esta dinámica industrial, aunque menos visible que en estados como Querétaro o Aguascalientes, posiciona a Tlaxcala como una zona emergente dentro del sector automotriz mexicano.

Diagnostico Organizacional y Documental

La Empresa

Sonavox Electronics Co es una empresa de capital chino, especializada en la fabricación de sistemas de audio para la industria automotriz. Fundada en 1975, comenzó a proveer bocinas automotrices a Volkswagen en 1985 y, desde entonces, ha entrado el 95% de su negocio en clientes del sector automotriz como VW, Ford, Audi, General Motors y BMW.

La compañía cuenta con plantas en China, República Checa, Brasil y, desde 2017, en México. En enero de ese año, inauguró su primera planta en el país, ubicada en el Corredor Industrial Xicoténcatl II, en Huamantla, Tlaxcala, con una inversión de 90 millones de pesos. Esta planta tiene una capacidad de producción de 6 millones de sistemas de audio al año, destinados a cubrir la demanda de la industria

automotriz en Puebla y Tlaxcala, especialmente para las firmas de Ford, Audi y Volkswagen.

La instalación de Sonavox en Tlaxcala ha contribuido al desarrollo económico de la región, generando empleos y fortaleciendo la cadena de suministros de la industria automotriz en el centro del país.

Historia

Sonavox Electronics ha evolucionado como un factor clave en la industria de sistemas de audio automotriz, consolidando su presencia global a través de una expansión estratégica. Su incursión en México, concretada en 2017 con la apertura de su planta en Huamantla, Tlaxcala, representó un paso importante para fortalecer su capacidad de producción y atender de manera más eficiente la demanda del sector automotriz en la región.

La decisión de establecer operaciones en Tlaxcala respondió a diversos factores, como su proximidad a importantes ensambladoras de vehículos y a un entorno industrial en crecimiento. Con una inversión significativa, la planta mexicana fue diseñada para producir millones de sistemas de audio anualmente, asegurando el abastecimiento de fabricantes clave y promoviendo el desarrollo tecnológico en la industria.

Desde su llegada a México, Sonavox ha contribuido al dinamismo económico del estado al generar empleos directos e indirectos, así como al integrarse a la red de proveedores de autopartes en el país. Su compromiso con la calidad y la innovación ha sido un pilar fundamental en su crecimiento, reforzando su reputación como proveedor confiable en el sector automotriz.

Misión

Ser la mejor opción para nuestros clientes en productos de audio, destacando a nivel internacional en tecnología, calidad y servicio. Nos comprometemos con la responsabilidad ambiental, la salud y la seguridad de nuestro personal, garantizando un entorno de trabajo seguro y sostenible.

Visión

Acompañar a nuestros clientes con el mejor audio en su automóvil.

Valores

En México Sonavox Electronics la seguridad de nuestros colaboradores es prioridad, por eso nos regimos con: respeto, confianza, honestidad, disciplina, integridad, compromiso y equidad.

Giro

Sonavox Electronics es la manufactura de sistemas de audio y bocinas para el sector automotriz. Se especializa en el diseño, desarrollo y distribución de soluciones acústicas avanzadas para importantes fabricantes de vehículos como Volkswagen, Ford, Audi, General Motors y BMW.

Ubicación

La empresa se encuentra ubicada en la Calle Virgen de la Caridad No. 19, Interior H2, dentro de la Ciudad Industrial Xicohtencatl II, en el municipio de Huamantla, Tlaxcala, México. El código postal correspondiente es 90500.



Estructura Organizacional

La organización de la empresa se compone por distintas áreas funcionales generales, desde la cual se coordinan y supervisan las siguientes direcciones y departamentos:

1. Gerente General
2. Dirección
3. Tecnologías de la Información (TI)
4. Finanzas
5. Recursos Humanos (RRHH)
6. Nóminas
7. Producción
8. Compras
9. Logística
10. Almacén
11. Proyectos
12. Calidad
13. Ingeniería de Producto
14. Ingeniería de Proceso
15. Mantenimiento

Funciones Clave

A continuación, se presenta una descripción concisa de las principales funciones que desempeña cada uno de los departamentos de la empresa.

1. Gerente General: Dirige y supervisa todas las operaciones de la empresa. Define objetivos estratégicos, toma de decisiones clave y coordina con las áreas para asegurar el cumplimiento de metas.

2. Dirección: Apoya al gerente general en la toma de decisiones estratégicas. Monitorea resultados globales y alinea a todas las áreas con los objetivos corporativos.
3. Tecnologías de la Información (TI): Administra la infraestructura tecnológica, los sistemas informáticos y la seguridad de la información. Brinda soporte técnico y asegura la eficiencia digital de los procesos.
4. Finanzas: Gestiona los recursos financieros de la empresa. Elabora presupuestos, controla gastos, realiza análisis financieros y asegura el cumplimiento fiscal y contable.
5. Recursos Humanos (RRHH): Administra El talento humano mediante procesos de reclutamiento, capacitación, desarrollo profesional y clima organizacional. Asegura el cumplimiento de las leyes laborales.
6. Nóminas: Se encarga del cálculo, procesamiento y pago puntual de los sueldos del personal, así como del cumplimiento de obligaciones fiscales y de seguridad social. También gestiona incidencias laborales como ausencias, vacaciones y horas extras.
7. Producción: Encargada de transformar insumos en productos finales conforme a estándares de calidad y eficiencia. Supervisa el rendimiento del personal y maquinaria en planta.
8. Compras: Gestiona la adquisición oportuna de materiales, insumos y servicios. Negocia con proveedores, control e inventarios y asegura calidad y costos adecuados.

9. Logística: Coordina el flujo de materiales y productos terminados. Se encarga del almacenamiento, transporte y distribución, garantizando entregas eficientes y seguras.
10. Almacén: Responsable de la recepción, resguardo, control y distribución de materiales, insumos y productos terminados. Garantiza un inventario ordenado, actualizado y disponible para las operaciones de la empresa.
11. Proyectos: Diseña, implementa y da seguimiento a proyectos estratégicos o de mejora continua. Controla cronogramas, costos y cumplimiento de objetivos técnicos.
12. Calidad: Vigila el cumplimiento de normas y estándares de calidad en productos y procesos, asegurando la satisfacción del cliente y mejora continua.
13. Ingeniería de Producto: Desarrolla nuevos productos y mejorar los existentes según especificaciones técnicas, funcionales y de mercado. Colabora estrechamente con producción y calidad.
14. Ingeniería de Proceso: Optimiza procesos productivos mediante la mejora continua como reducción de desperdicios y uso eficiente de recursos tecnológicos.
15. Mantenimiento: Encargado de conservar en óptimas condiciones las instalaciones, equipos y maquinaria de la empresa, realizando acciones preventivas y correctivas para asegurar la continuidad y seguridad de las operaciones.

TI y su Gestión Documental

El área de Tecnologías de la Información (TI) es responsable de administrar, desarrollar y mantener la infraestructura tecnológica de la empresa, garantizando la operatividad de los sistemas informáticos, redes, software y hardware. Asegurando

que los recursos tecnológicos funcionen de manera eficiente, segura y alineada con los objetivos estratégicos de la organización.

Las funciones clave dentro de esta área se encuentran:

- Implementación y mantenimiento de sistemas de información
- Soporte técnico a usuarios internos
- Gestión de bases de datos y servidores
- Administración de redes y seguridad informática
- Actualización tecnológica e innovación digital
- Apoyo en automatización de procesos

Área de TI en Relación con el Estándar TISAX

El área de TI desempeña un papel fundamental en la gestión documental, al proporcionar las herramientas, plataformas y protocolos que permiten el control, almacenamiento, acceso y protección de la información organizacional.

Su relación directa incluye:

- implementación de sistemas electrónicos de gestión documental (GED), facilitando la digitalización, organización y consulta eficiente de documentos.
- define el control de accesos y seguridad según el nivel de usuario, permisos y medidas de protección.
- administra sistemas de respaldo y recuperación de documentos ante fallos para evitar pérdidas de datos.
- Colabora con áreas de auditoría para asegurar el cumplimiento de normativas como ISO/IEC 27001 o TISAX en lo relativo al manejo de información.
- participa en el diseño e implementación de procesos para el registro, seguimiento y archivo de documentos, lo que mejora la trazabilidad y eficiencia.

TI en cumplimiento del Estándar TISAX

Dentro del contexto de la adherencia al estándar TISAX (Trusted Information Security Assessment Exchange), el departamento de TI desempeña una función

clave en la puesta en marcha y el mantenimiento de un sistema de gestión documental que sea seguro y confiables, cumpliendo con los requisitos de seguridad de la información exigidos por el sector automotriz.

A continuación, se desarrollan las responsabilidades clave en el área de TI en relación con la gestión documental en el marco de TISAX:

1. Colabora en la definición e implementación de los distintos niveles de seguridad como lo son publica, interna, confidencial y restringida), asegurando que se apliquen controles de acceso adecuados según el nivel de sensibilidad de los documentos.
2. Administra perfiles de usuarios, roles y permisos, garantizando que solo el personal autorizado tenga acceso a información sensible, conforme a lo estipulado por el módulo de protección de datos de TISAX.
3. Establece mecanismos de cifrado tanto en tránsito como en reposo para proteger documentos confidenciales o secretos, cumpliendo con los requisitos del conjunto de controles de seguridad de la información de TISAX.
4. Supervisa las políticas de respaldo automático, almacenamiento seguro y recuperación de documentos críticos, asegurando la disponibilidad y continuidad operativa ante cualquier incidente.
5. Implementa soluciones tecnológicas que permiten auditar de manera completa el ciclo de vida de los documentos, incluyendo su creación, modificación, acceso y eliminación, conforme a los principios de trazabilidad y responsabilidad.
6. TI evalúa, desarrolla y/o administra plataformas digitales como servidor, IMS, SIT, SAP que centralicen, organicen y protegen la documentación corporativa.

Garantiza que los requisitos de TISAX, ISO/IEC 27001 y otras normativas relevantes estén completamente integrados en las políticas de seguridad y gestión documental de la organización.

Gestión Documental

La gestión documental es un sistema estructurado que comprende el conjunto de actividades técnicas y administrativas relacionadas con la planificación, control, organización, recuperación, acceso y disposición final de los documentos, con el objetivo de garantizar la eficiencia, integridad y disponibilidad de la información a lo largo de su ciclo de vida.

Este concepto cobra especial relevancia en el contexto de la elaboración de un manual de gestión documental, ya que dicho manual debe establecer los criterios, procedimientos y herramientas que aseguren una gestión documental coherente, segura y alineada con estándares Nacionales e Internacionales. (López, 2019)

Beneficios de implementar un Manual de Gestión Documental.

Implementar un manual de gestión documental proporciona una guía operativa para el manejo eficiente de la información dentro de la organización. Entre los principales beneficios se encuentran:

- Establecimiento de procedimientos estandarizados para la gestión de documentos
- Reducción del riesgo de pérdida o mal manejo de información.
- Cumplimiento normativo con regulaciones y requisitos de Auditoría.
- Acceso oportuno y controlado a la información según niveles de confidencialidad.
- Optimización de tiempos en la locación, uso y resguardo de documentos
- Facilitación de procesos de digitalización coma automatización y trazabilidad (Archivo General de la Nación, 2019)

Procesos clave en la Gestión Documental (aplicables al manual)

El manual debe contemplar los siguientes procesos fundamentales:

- Recepción: registro inicial de documentos, Ya se han generados o recibidos.
- Clasificación: asignación de categorías según el tipo de documento, área o función.
- Registro: inclusión del documento en un sistema (físico o digital) con identificador único.
- Uso y consulta: establecimiento de pautas para el acceso, préstamo o visualización.
- Conservación: almacenamiento seguro conforme el valor legal o administrativo.
- Disposición final: eliminación, digitalización o archivo histórico, según lo definido por el manual. (International Organization for Standardization , 2016)

Industria Automotriz

La industria automotriz comprende todas las actividades económicas orientadas al diseño, desarrollo, producción, distribución y mantenimiento de vehículos automotores. Este sector se caracteriza por su alta integración tecnológica, automatización, y una red de proveedores global que lo convierte en uno de los más complejos del mundo (ENX Association, 2023).

México se ha consolidado como un pilar clave de la industria automotriz global. En esta reflexión exploramos la estructura, los logros y los retos de la industria automotriz mexicana en 2025, destacando sus factores clave de competitividad.

Entre sus principales características se encuentran:

- Tecnología avanzada: Utiliza automatización, inteligencia artificial y robótica en la producción.
- Globalización: Implica una extensa cadena de suministro con proveedores de multiniveles (Tier 1, Tier2, etc.)
- Normatividad estricta: Cumple estándares internacionales de calidad, medio ambiente y seguridad de la información (Force, 2016).

La manufactura de autos en México se ha convertido en un protagonista a nivel mundial. En 2024, el país ensambló 3.9 millones de unidades, un crecimiento del

5.5% respecto al año anterior, según el Instituto Nacional de Estadística y Geografía (INEGI). México es actualmente el séptimo mayor productor de vehículos a nivel global y el primero en América Latina.

Este crecimiento se debe a factores como:

- Ubicación estratégica: Cercanía con Estados Unidos, su principal socio comercial.
- Mano de obra calificada: Técnicos e ingenieros especializados en manufactura automotriz.
- Acuerdos comerciales: T-MEC y tratados con más de 40 países, facilitando la exportación.

Gracias a su ubicación estratégica, fuerza laboral calificada y acuerdos comerciales, el país se posiciona como uno de los principales productores y exportadores de vehículos. Respalados por cifras del INEGI y la Asociación Mexicana de la Industria Automotriz (AMIA).

Marcas con mayor producción en México

El sector de ensamblaje de vehículos en México está liderado por gigantes globales. En 2024, las cinco marcas con mayor producción y exportación fueron:

Marcas con mayor producción y exportación 2024					
NO.	Marca	Unidades producidas	Porcentaje	Unidades exportadas	Porcentaje
1	General Motors	889,072	+23%	830,820	+15.1%
2	Nissan	669,941	-	456,866	+24.5%
3	Stellantis	419,426	-10.3%	353,307	-14.4%)
4	Ford	386,776	+5.9%	379,849	+2.4%
5	Volkswagen	383,312	+9.5%	326,217	+4.6%.

Tabla 1: Marcas con mayor producción y exportación 2024

La industria automotriz es el principal generador de divisas para México, con una balanza comercial superavitaria de 99 mil millones de dólares, según datos de la AMIA. Además, el país es el cuarto mayor exportador de autopartes a nivel mundial y el primer proveedor del mercado estadounidense. (Consejo Nacional de Ejecutivos en Logística y Cadena de Suministro, A.C., 2025)

Certificación en la Industria Automotriz

Las certificaciones aseguran que las empresas proveedoras cumplan con requisitos técnicos, normativos y de seguridad. Algunas de las más relevantes son:

- IATF 16949: Norma internacional de sistemas de gestión de calidad automotriz.
- TISAX (Trusted Information Security Assessment Exchange): Estándar de seguridad de la información promovido por la industria alemana para proteger datos sensibles, especialmente en proveedores tecnológicos.

México se posiciona como el séptimo productor de vehículos a nivel mundial y el primero en América Latina. Alberga plantas de ensamble de marcas globales como Audi, BMW, Ford, General Motors, Honda, Nissan, Toyota y Volkswagen, y una red robusta de proveedores nacionales e internacionales.

Estas certificaciones permiten a las empresas integrarse a cadena de suministro globales, garantizar la protección de datos técnicos y comerciales, y generar confianza en clientes y socios.

ENX Association

La ENX Association es una organización europea sin fines de lucro fundada por los principales fabricantes de automóviles (OEM) y asociaciones del sector automotriz, con el objetivo de garantizar la seguridad de la comunicación y la formación dentro de la cadena de suministro automotriz.

Fue establecida en 2000 y está respaldada por empresas como Volkswagen, BMW, Daimler, Renault, así como por asociaciones internacionales como la VDA (Asociación Alemana de la Industria Automotriz).

Sus funciones principales;

Proporciona una infraestructura Segura para el intercambio de datos entre fabricantes y proveedores, conocida como la Red ENX, utilizada para enviar información técnica crítica de forma protegida.

Responsable de operar y supervisar el esquema de evaluación de seguridad de la información TISAX (Trusted Information Security Assessment Exchange).

Homologar a los proveedores de servicios de auditoría, asegurar la integridad del proceso de evaluación, y facilitar la confianza entre socios comerciales.

establece y promueve requisitos estandarizados de seguridad de la información, protección de datos y cumplimiento normativo en la cadena automotriz global.

VDA (Asociación Alemana de la Industria Automotriz)

La VDA (Verband der Automobilindustrie) es la Asociación Alemana de la Industria Automotriz, una de las organizaciones más influyentes del sector automotriz a nivel global. Agrupa a los principales fabricantes alemanes de automóviles, proveedores de autopartes y fabricantes de remolques, carrocerías y autobuses.

Entre sus funciones se destacan;

Porta voz frente a instituciones gubernamentales, organismos internacionales, y foros de comercio y tecnología.

Define los intereses de la industria automotriz alemana y europea en temas como comercio, innovación, sostenibilidad y regulaciones.

En su desarrollo de estándares técnicos, es responsable de generar normativas y recomendaciones técnicas reconocidas en toda la industria automotriz.

Promueve estándares para proteger la información confidencial, como planos, datos de desarrollo y prototipos, los que llevó a la creación del esquema TISAX junto con la ENX.

Participa en proyectos y alianzas con otras asociaciones del sector a nivel global, promoviendo la innovación tecnológica, la electromovilidad y la transformación digital (VDA, 2020).

ISA (Information Security Assessment)

El ISA (Information Security Assessment) es un conjunto de criterios y controles desarrollados por la VDA (Asociación Alemania de la Industria Automotriz) con el propósito de evaluar la seguridad de la información dentro de las organizaciones que forman parte de la cadena de suministro automotriz. Este instrumento constituye la base de metodología de TISAX, el sistema de evaluación estandarizado en Europa para el sector automotor.

Diseñado específicamente para responder a los desafíos particulares del sector automotriz, en donde la confidencialidad, integridad y disponibilidad de la información técnica, de desarrollo y comercial es crítica para la competitividad y la protección del conocimiento industrial.

Su estructura se organiza en varios módulos que abordan diferentes aspectos clave de la seguridad de la información:

Modulo principal: Contiene controles esenciales basados en el estándar ISO/IEC 27001, y evalúa el sistema de gestión de seguridad de la información (SGSI) de la organización.

Módulos adicionales (según el perfil de evaluación):

- Protección de prototipos
- Protección de datos personales
- Conectividad con terceros (proveedores, clientes)
- Intercambio seguro de datos técnicos
- Protección física de instalaciones

Cada módulo contiene una serie de requisitos que se clasifican con niveles de madurez (de 1 a 5), lo cual permite adoptar la evaluación a distintos contextos y riesgos.

TISAX (Trusted Information Security Assessment Exchange)

Es un esquema de evaluación reconocido en el sector automotriz europeo, diseñado para verificar y garantizar el cumplimiento de estándares de seguridad de la información, protección de datos y gestión de prototipos en organizaciones que forman parte de la cadena de suministro automotriz. Fue desarrollado por la Asociación Alemana de la Industria Automotriz (Verband der Automobilindustrie VDA) y gestionado por la plataforma en ENX. (ENX Association, 2023) (VDA, 2020)

Objetivos de TISAX

- Proteger la confidencialidad, integridad y disponibilidad de la información.
- Establecer un estándar común en seguridad de la información dentro de la industria automotriz.
- Garantizar que los proveedores cumplan con requisitos de seguridad alineados al cliente.
- Evitar auditorias duplicadas mediante el reconocimiento de resultados entre empresas participantes.

Estructura del Modelo TISAX

TISAX se basa en la Norma Internacional ISO/IEC 27001 y utiliza un cuestionario llamado ISA (Information Security Assessment) que divide en módulos:

- Seguridad de la información básica (core)
- Protección de prototipos
- Protección de datos personales
- Conectividad con terceros
- Protección en sitios físicos.

Cada módulo se aplica según el nivel de riesgo del servicio prestado.

Requisitos Principales

- Política de seguridad de la información
- Clasificación de la información
- Gestión de accesos y derechos
- Control de dispositivos y medios de almacenamiento
- Respaldo y recuperación de datos
- Gestión de incidentes de seguridad
- Evaluaciones internas y mejora continua
- Protección física de instalaciones

Funcionamiento del Proceso TISAX

1. Registro en la plataforma ENX.
2. Autodiagnóstico basado en el cuestionario ISA.
3. Contratación de un proveedor de auditoría autorizada por TISAX
4. Realización de auditoría (remota o presencial).
5. Publicación de resultados en la plataforma de TISAX, visibles solo para empresas autorizadas.
6. Vigencia de los resultados: 3 años.

Beneficios de Implementar TISAX

- Reconocimiento en la industria automotriz Internacional.
- Mayor confianza de los socios comerciales.
- Cumplimiento de requisitos legales como RGPD (Reglamento General de Protección de Datos).
- mejora de los controles de la seguridad de la información.
- Acceso a nuevos mercados y clientes que exigen certificaciones.
- Reducción en el número de auditorías por parte de diferentes clientes.

Ventajas competitivas

- Diferenciación frente a otros proveedores
- mejora de la reputación empresarial

- optimización de procesos mediante el enfoque de mejora continua
- estandarización de políticas de seguridad de la información en toda la organización
- refuerzo de la cultura organizacional en torno a la seguridad. (ISO/IEC 27001, 2013)

Seguridad de la Información

La seguridad de la información es un componente estratégico en la industria automotriz moderna, debido al creciente uso de tecnologías digitales, sistemas interconectados, vehículos inteligentes y cadenas de suministro globales. Su función principal es proteger la calidad, integridad y disponibilidad de los datos, tanto internos como compartidos con clientes y proveedores.

La industria automotriz depende en gran medida de la innovación tecnológica, la integración con proveedores y el manejo de información confidencial, incluyendo:

- Diseños de nuevos modelos
- prototipos y tecnologías patentadas
- datos personales de clientes
- conectividad de vehículos
- Software automotriz y datos en la nube

Ante este panorama, las amenazas cibernéticas, las fugas de información y el espionaje industrial representan riesgos críticos. Por ello, contar con políticas sólidas de seguridad de la información no solo se protege los activos de la empresa, sino que garantiza la continuidad del negocio y fortalece la confianza con los socios comerciales. (International Organization for Standardization, 2013)

Factores que Incrementan su Importancia

- Digitalización: La mayoría de los procesos industriales y logísticos están automatizados y conectados.

- Cadenas de suministro globales: Requieren el intercambio constante de datos sensibles con proveedores, quienes también deben cumplir estándares de seguridad.
- Cumplimiento normativo: Normas como TISAX, ISO/IEC 27001 y regulaciones como el RGPD hacen obligatoria la protección de datos.

Consecuencias de una Brecha de Seguridad

Una falla en la seguridad puede resultar en:

- Pérdida de propiedad intelectual
- Daño en reputación
- Sanciones legales y financieras
- Pérdida de contratos con OEMs (fabricantes de equipos originales).
- Interrupciones en la producción o distribución. (Deloitte, 2022)

RGPD (Reglamento General de Protección de Datos)

El Reglamento General de Protección de Datos (RGPD), es una normativa de la Unión Europea que entro en vigor el 25 de mayo de 2018, y cuyo objetivo es proteger los datos personales de los ciudadanos europeos, garantizando su privacidad y regulando como las organizaciones deben de recopilar, almacenar, procesar y compartir dicha información.

Este reglamento sustituye a la anterior Directiva 95/36/CE y tiene aplicación obligatoria para todas las empresas que procesan datos personales residentes en la UE, sin importar dónde esté ubicada la empresa.

La RGDP establece los siguientes principios fundamentales que deben seguir todas las organizaciones al manejar datos personales:

- Licitud, lealtad y transparencia
- Limitación de la finalidad
- Minimización de datos
- Exactitud
- Limitación del plazo de conservación

- Integridad y confidencialidad
- Responsabilidad proactiva (Europea, 2016).

Normas ISO

El estándar TISAX (Trusted Information Security Assessment Exchange) se basa en los principios de gestión de seguridad de la información y calidad, por lo que está estrechamente alineado con normas internacionales reconocidas como la ISO/IEC 27001 enfocada en la seguridad de la información, y la ISO 9001, orientada a la gestión de calidad.

ISO/IEC 27001: Gestión de la Seguridad de la Información

La norma ISO/IEC 27001 establece requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de la información a través de un enfoque basado en el riesgo.

Componentes clave:

- Análisis y tratamientos de riesgos.
- Políticas de seguridad y control de accesos.
- Gestión de incidentes.
- Evaluación continua y auditorías externas. (International Organization for Standardization, 2013)

Este esquema exige la implementación de políticas, procedimientos y controles que gestionen los riesgos relacionados con los activos de información. Esta norma es la base técnica del esquema de TISAX, ya que el cuestionario ISA utilizado en TISAX, está alineado con sus controles. Las empresas ya que aplican ISO/IEC 27001 tienen una ventaja significativa al momento de certificarse bajo TISAX.

ISO 9001: Gestión de la Calidad

La norma ISO 9001 define los requisitos para un Sistema de Gestión de Calidad (SGC), permitiendo a las organizaciones demostrar su capacidad para ofrecer productos y servicios que cumplen con las expectativas del cliente y la normativa aplicable.

- Elementos centrales:
- Enfoque en el cliente.
- Mejora continua.
- Gestión basada en procesos.
- Liderazgo y toma de decisiones basada en evidencia.

De esta manera, permite a las empresas demostrar su capacidad para ofrecer productos y servicios que satisfacen las necesidades del cliente y los requisitos regulados aplicables. Así como también fortalece la estructura organizativa y promueve un enfoque basado en procesos, mejora continua y gestión eficaz; aspectos que son también valorados durante las evaluaciones TISAX.

Aunque ISO 9001 no está directamente vinculada a la seguridad de la información, su integración con ISO/IEC 27001 fortalece el marco organizativo y la eficiencia operativa, lo cual es valioso para cumplir con estándares como TISAX. (International Organization for Standardization, 2015)

Conceptos Básicos

Estándares de Seguridad

Los estándares de seguridad son conjuntos de normas y directrices desarrolladas por organismos internacionales, nacionales o sectoriales, que establecen prácticas y requisitos mínimos para garantizar la protección de activos, personas, información y procesos dentro de la organización. Estos estándares buscan minimizar riesgos, prevenir incidentes y asegurar la continuidad operativa mediante la implementación de controles y procedimientos sistemáticos. (Sistemas de gestión de la seguridad de la información, 2022)

Certificación

La certificación es un proceso formal mediante el cual una entidad independiente verifica que un producto, servicio, sistema o persona cumple con requisitos específicos establecidos en normas, reglamentos o estándares reconocidos. Su objetivo principal es garantizar la calidad, seguridad, cumplimiento normativo o buenas prácticas en un área determinada.

Genera confianza en las partes interesadas, mejoran la reputación empresarial, optimizan procesos y abren oportunidades de negocio, al demostrar un compromiso con la mejora continua, la transparencia y la responsabilidad profesional. (Vargas, 2016)

Manuales

Un manual es un documento estructurado que recopila, organiza y comunica información clave sobre políticas, procesos, funciones o normativa dentro de una organización. Su propósito es servir como guía de consulta estandarizada, permitiendo que los colaboradores comprendan sus funciones, responsabilidades y la forma adecuada de ejecutar tareas o cumplir con reglamentos. Existen diferentes tipos de manuales, como manuales de organización, de procesos, de calidad o de gestión documental. (Calderón, 2016)

Políticas de Información

Las políticas de información son alineamientos generales estratégicos que regulan la forma en que se gestione, accede, protege, comparte y almacena la información dentro de la organización. Estas políticas definen los principios y normas que garantiza la seguridad, integridad, confidencialidad y disponibilidad de los datos, y son fundamentales para cumplir los requisitos legales y estándares internacionales. (International Organization for Standardization, 2013)

Procedimientos de Información

Los procedimientos de información son instrucciones detalladas y específicas que indican cómo ejecutar una actividad relacionada con el manejo de la información, como, por ejemplo, la captura, clasificación, archivo, respaldo o eliminación de documentos. Estos procedimientos describen paso a paso cada acción a seguir, quién ejecuta, en qué momento y en qué condiciones. Su propósito es asegurar la trazabilidad, consistencia y cumplimiento normativo en la gestión de la información. (Sánchez, 2020)

TICs en la Gestión Documental

La aplicación de las Tecnologías de la Información (TI) ha transformado profundamente la gestión documental en las organizaciones modernas, permitiendo automatizar procesos, mejorar la eficiencia en el manejo de la información y garantizar una mayor seguridad en el acceso, almacenamiento y recuperación de documentos.

La TI se integra en todos los procesos del ciclo de vida documental, desde la creación hasta la disposición final, por medio de herramientas digitales como:

- Sistemas de Gestión Documental Electrónica (SGDE): Plataformas que permiten organizar, clasificar, buscar, almacenar y controlar documentos digitales.
- Firmas Digitales: Validan la autenticidad e integridad de los documentos sin necesidad de formatos impresos.
- Digitalización de Archivos Físicos: Conversión de documentos en papel a formato electrónico, facilitando su preservación y consulta.
- Almacenamiento en la Nube: Acceso remoto y seguro a la información desde cualquier dispositivo autorizado por la TI.
- Bases de Datos Documentales: Organización estructurada y búsqueda avanzada de documentos.

Las ventajas de aplicar TI a la gestión documental son:

- Seguridad en control de accesos, cifrado, respaldo automático y seguimiento de modificaciones.
- Agilidad y eficiencia en la búsqueda de documentos, menor tiempo en trámites y flujos de aprobación.
- Organización en la clasificación de datos por metadatos, categorías y versiones controladas.
- Accesibilidad a la información desde cualquier lugar, favoreciendo el teletrabajo.

- Registro de acciones realizadas sobre cada documento (quién accedió, cuándo, qué cambió). (Rodríguez M. A., 2018)

Clasificación de la Información

La clasificación de la información es el proceso mediante el cual una organización categoriza sus datos según el nivel de sensibilidad, valor, y el impacto que podrá tener su divulgación, modificación o pérdida. Su propósito es proteger adecuadamente los activos de información, garantizar la confidencialidad, integridad y disponibilidad, y cumplir con normativas internas y externas.

Los niveles más comunes:

1. Información Pública.
2. Información Interna.
3. Información Confidencial.
4. Información Secreta o Restringida. (Rodríguez M. A., 2021)

Esta clasificación permite establecer niveles de acceso, políticas de usos y medidas de seguridad según el tipo de información tratada. En sectores como el automotriz, donde se manejan datos de diseño, pruebas, desarrollo tecnológico y acuerdos comerciales con fabricantes globales, la correcta clasificación permite cumplir con estándares como TISAX, ISO/IEC 27001 y proteger la información crítica del negocio. (Sánchez, 2020)

Además, es clave para prevenir fugas de información que puedan afectar la propiedad intelectual, los contratos o la reputación de la empresa.

CAPITULO II Metodología de Investigación

Diagnóstico organizacional

El diagnóstico organizacional es un proceso analítico y sistemático que tiene como objetivo estudiar el funcionamiento interno de una organización. Su propósito es

identificar los problemas, desafíos, necesidades y fortalezas que afectan el desempeño y la eficiencia de la empresa.

Este proceso implica la recopilación, análisis e interpretación de datos relacionados con diferentes áreas, tales como: estructura organizativa, comunicación, procesos, recursos humanos, tecnología, cultura organizacional, entre otros (Robbins S. P., 2020).

Enfoque Metodológico

Para llevar a cabo el diagnóstico organizacional, se emplean diversos métodos y técnicas, tanto cualitativas y cuantitativas para abordar el estudio. La investigación se clasifica como aplicada y descriptiva, ya que se busca identificar problemas en la gestión documental y evaluar cómo el manual propuesto podría mejorar esta situación.

La investigación se centra en el área de Tecnologías de la Información de Sonavox Electronics Co, donde se buscará entender a fondo los procesos, las dificultades y las necesidades relacionadas con la gestión documental y el cumplimiento de TISAX.

Tipo de Investigación

Se trata de una investigación aplicada, para generar soluciones prácticas mediante el desarrollo de un manual que ayude a mejorar la gestión documental en el área de TI. Es un enfoque mixto, que integra datos cualitativos como entrevistas, observaciones, y cualitativos como lo son encuestas.

Técnicas de Recolección de Datos

Para identificar las fortalezas y debilidades del sistema de gestión documental actual, es fundamental la recolección de datos para así comprender los requerimientos y áreas de mejora. las siguientes técnicas las siguientes técnicas permitirán obtener información detallada y precisa, y garantizar que la implementación o mejora de las políticas documentales se ajuste a las necesidades organizacionales y normativas de TISAX.

1. Entrevista Semiestructuradas

Para proporcionar flexibilidad y profundizar en temas específicos que surjan durante la conversación, permitiendo una comprensión más extensa del contexto. Realizando una serie de preguntas preparadas con antelación, pero con un espacio para que el entrevistador se exprese libremente y aporte información adicional relevante.

Con finalidad:

- Obtener una visión detallada sobre los problemas actuales en el proceso de gestión documental.
- Identificar las necesidades de mejora en cuanto a clasificación, almacenamiento y acceso a los documentos
- Recoger sugerencias y opiniones sobre posibles soluciones y mejoras para la infraestructura documental.

2. Observación Directa

Se llevará a cabo mediante la supervisión de los procesos actuales de gestión documental dentro de la organización. Esto incluye la forma en que los documentos son clasificados, almacenados, y accedidos por los empleados, permitiendo detectar comportamientos y prácticas que podrían no ser evidentes en entrevistas o encuestas como proporcionando una visión más completa de los procesos.

Con finalidad:

- Evaluar la efectividad y eficiencia de los procesos actuales en tiempo real.
- Identificar áreas problemáticas en la manipulación y almacenamiento de documentos, como posibles vulnerabilidades de seguridad o ineficiencias operativas.
- Detectar posibles desviaciones de las políticas documentales internas y de las normativas de TISAX.

3. Encuesta Interna

Aplicada para conocer sus percepciones y opiniones sobre el manejo del sistema de gestión documental actual, recopilando una cantidad de datos en poco tiempo, permitiendo analizar patrones y tendencia dentro de la organización.

Con finalidad de obtener:

- Recoger la información general sobre la facilidad de uso y accesibilidad de los sistemas de gestión documental actuales.
- Identificar posibles brechas entre las necesidades de los usuarios y la capacidad del sistema de documentación.
- Evaluar el nivel de conocimiento y cumplimiento de las políticas documentales entre los empleados.

4. Análisis Documental

Revisar las políticas existentes en la organización relacionadas con la gestión documental. Esto incluye la evaluación de documentos normativos, políticas internas como manuales de procedimientos y registros relacionados con el cumplimiento de normativas como TISAX como que regulan la protección y manejo de la información.

Para alinear las prácticas internas con las mejores prácticas de la industria y con los requisitos específicos de TISAX.

Permitiendo:

- Revisar y comparar las políticas de gestión documental existentes con las normas y estándares de TISAX para identificar posibles áreas de mejora.
- Asegurar que la organización cumple con los requisitos legales y normativos aplicables en términos de clasificación, almacenamiento y seguridad de la información.

- Identificar cualquier documento o procedimiento obsoleto o que no cumpla con los criterios necesarios para garantizar la eficiencia y seguridad en el manejo de la documentación.

Población y Muestra

La población está constituida por los colaboradores de la empresa Sonavox Electronics Co, con una muestra intencional que se seleccionó a partir de perfiles claves con responsabilidad en el manejo de la documentación, responsables de seguridad de la información y personal administrativo.

Población objetivo

La población incluye personal clave responsable de la gestión documental, tales como:

- Líder de TI
- Responsable de seguridad de la información
- Administrativos encargados del manejo de archivos digitales y físicos.

Muestra

La muestra fue de tipo intencional y estuvo compuesta por 15 colaboradores, seleccionados por su rol estratégico dentro del área de TI y administración.

Se priorizaron los siguientes criterios:

- Personas con responsabilidad en el manejo de documentos como lo son líderes y personal administrativo clave.
- Perfiles que trabajan con diferentes tipos de documentos confidenciales, operacionales, técnicos, etcétera.

Esta muestra permitió obtener una visión representativa de los problemas actuales y de las necesidades específicas del área en relación con la gestión documental.

Instrumentos Utilizados

1. Guía de Entrevista

Para obtener información profunda y detallada sobre las experiencias de los empleados en cuanto a la gestión, a continuación, se manejan preguntas estructuradas en diferentes temáticas para una mejor comprensión.

Acceso a la información

1. ¿Cómo accede generalmente a los documentos que necesiten su trabajo diario?
2. ¿Encuentra con facilidad los documentos que necesita?
3. ¿Ha experimentado dificultades para encontrar algún tipo de documento en los últimos meses? ¿Cuáles fueron esas dificultades?

Clasificación y Organización de Documentos

1. ¿Cómo se organizan los documentos en su área de trabajo? ¿Sigue algún sistema de clasificación específico?
2. ¿Considera que la clasificación actual de los documentos facilita el acceso y la búsqueda de información?
3. ¿En tu opinión, qué mejoras se podrían hacer para organizar mejor los documentos en su área?

Control de Versiones

1. ¿Existen políticas claras sobre el control de versiones de los documentos en su área?
2. ¿Ha tenido algún problema al trabajar con versiones antiguas o desactualizadas de un documento?
3. ¿Cómo se asegura de estar utilizando la versión más reciente de un documento importante?

Seguridad y Protección de Documentos

1. ¿Qué medidas de seguridad existen para proteger los documentos sensibles en su área de trabajo?
2. ¿Cree que los documentos confidenciales están lo suficientemente protegidos?
3. ¿Conoces si hay alguna política de control de acceso a documentos confidenciales? ¿Está siendo aplicada correctamente?

Percepción General

1. ¿Cómo describiría el sistema actual de gestión documental?
2. ¿Qué aspectos considera que funcionan bien en el sistema actual de gestión documental?
3. ¿Cuáles son los principales problemas o desafíos que enfrenta con la gestión documental en su día a día?

2. Encuesta

Para obtener respuestas numéricas y estandarizadas de la cantidad de colaboradores entrevistados, a continuación, se detalla las preguntas con formato cerrado.

1. ¿Con qué frecuencia encuentra fácilmente los documentos que necesita?
 - (1) Nunca
 - (2) Rara la vez
 - (3) A veces
 - (4) Frecuentemente
 - (5) Siempre
2. ¿Considera que el tiempo que tarda en encontrar documentos es razonable?
 - (1) Muy en desacuerdo
 - (2) En desacuerdo
 - (3) Neutral

- (4) De acuerdo
 - (5) Muy de acuerdo
3. ¿Cree que los documentos están correctamente clasificados en su área de trabajo?
- (1) Muy en desacuerdo
 - (2) En desacuerdo
 - (3) Neutral
 - (4) De acuerdo
 - (5) Muy de acuerdo
4. ¿Existen procedimientos documentados para la organización y clasificación de archivos?
- (1) Si
 - (2) No
5. ¿Considera que el control de versiones de los documentos es adecuado?
- (1) Muy inadecuado
 - (2) Inadecuado
 - (3) Neutral
 - (4) Adecuado
 - (5) Muy adecuado
6. ¿Ha trabajado alguna vez con una versión incorrecta o desactualizadas de un documento?
- (1) Si
 - (2) No
7. ¿Sabe quién tiene acceso a los documentos confidenciales en su área?

(1) Si

(2) No

8. ¿Considera que los documentos sensibles están suficientemente protegidos por ejemplo con contraseña, cifrado, etcétera?

(1) Muy en desacuerdo

(2) En desacuerdo

(3) Neutral

(4) De acuerdo

(5) Muy de acuerdo

3. Observación Directa

La observación directa se llevó a cabo durante el desarrollo habitual de las actividades administrativas y técnicas en el área de TI y en los espacios donde se manipulan documentos físicos y digitales. Se utilizó una guía de observación estructurada, diseñada con base en los lineamientos de la norma TISAX y las buenas prácticas de gestión documental.

Durante el ejercicio de observación, se analizaron los siguientes puntos críticos:

Categoría Evaluada	Elementos observados
Clasificación de documentos	Existencia de criterios definidos para la clasificación de archivos, etiquetado uniforme, y diferenciación por tipo de documento.
Almacenamiento físico y digital	Condiciones del espacio de almacenamiento físico, organización digital, respaldo y acceso a plataformas de almacenamiento en la nube o servidores locales.
Acceso a documentos	Facilidad de localización, tiempo promedio para encontrar archivos y acceso por parte de los usuarios autorizados.

Seguridad en el manejo de documentos	Controles visibles de acceso (contraseñas, permisos), uso de medidas físicas (archiveros cerrados, acceso restringido), y prácticas de protección.
Cumplimiento con políticas TISAX	Grado de alineación con políticas internas y requerimientos de la certificación TISAX: confidencialidad, integridad y disponibilidad de la información.

Tabla 2: Resultados de la observación directa

Herramientas utilizadas:

- Guía de observación estructurada
- Cuaderno de campo digital para registrar hallazgos
- Cronómetro para evaluar eficiencia en acceso
- Lista de verificación alineada a los requisitos de TISAX

Duración de la observación:

La observación se realizó durante una jornada laboral típica (8:00 a 17:00 hrs) durante tres días consecutivos, en distintas áreas: oficinas administrativas, área de TI, y zona de archivo físico.

4. Lista de Cotejo (Checklist)

Se utilizó para realizar una auditoría preliminar sobre el cumplimiento de las normativas y estándares relacionados con la gestión documental.

A continuación, se presentan ítems clave en la lista de cotejo:

1. ¿Se utilizan categorías específicas para clasificar los documentos?

(1) Si

(2) No

2. ¿Los documentos están clasificados de manera uniforme en todas las áreas?

(1) Si

- (2) N
3. ¿Se aplican controles de acceso para documentos sensibles?
- (1) Si
- (2) No
4. ¿Cada documento tiene asignado un responsable de su custodia?
- (1) Si
- (2) No
5. ¿Existen registros claros de las versiones de documentos?
- (1) Si
- (2) No
6. ¿Cada versión de un documento tiene una fecha de creación y edición?
- (1) Si
- (2) No
7. ¿Los documentos críticos están protegidos por contraseñas o cifrado?
- (1) Si
- (2) No
8. ¿Existen procedimientos para realizar copias de seguridad de los documentos?
- (1) Si
- (2) No
9. La gestión documental sigue los estándares ISO/IEC 27001 o TISAX?
- (1) Si
- (2) No

10. ¿Se realizan auditorías periódicas del sistema de gestión documental?

(1) Si

(2) No

Análisis de Datos

Se realizará un análisis de datos que integrará métodos cualitativos y cuantitativos, con el fin de alcanzar una visión completa y fundamentada de la situación.

Procedimiento para el cálculo de porcentajes en los resultados

Para determinar el porcentaje correspondiente a cada respuesta obtenida, se emplea la siguiente fórmula:

$$\text{Porcentaje} = \frac{\text{Número de personas que seleccionaron la opción}}{\text{Total de persona entrevistadas}} \times 100$$

Donde:

- Número de personas que seleccionaron la opción: corresponde a la cantidad de entrevistados que eligieron una respuesta específica.
- Total, de personas entrevistadas: en este caso, es de 15 personas.
- 100: convierte el resultado en porcentaje.

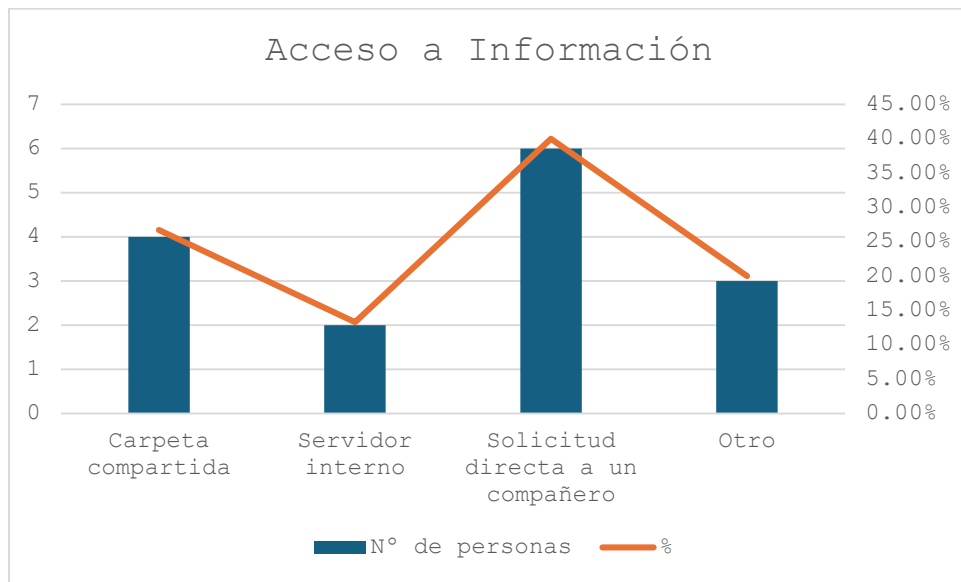
Análisis de la Entrevista

Acceso a la información

1. ¿Cómo accede generalmente a los documentos que necesita?

Opción de respuesta	Nº de personas	%
Carpeta compartida	4	26.7%
Servidor interno	2	13.3%
Solicitud directa a un compañero	6	40.0%
Otro	3	20.0%

Tabla 3: Acceso a información documental



Gráfica 1: Acceso a información documental

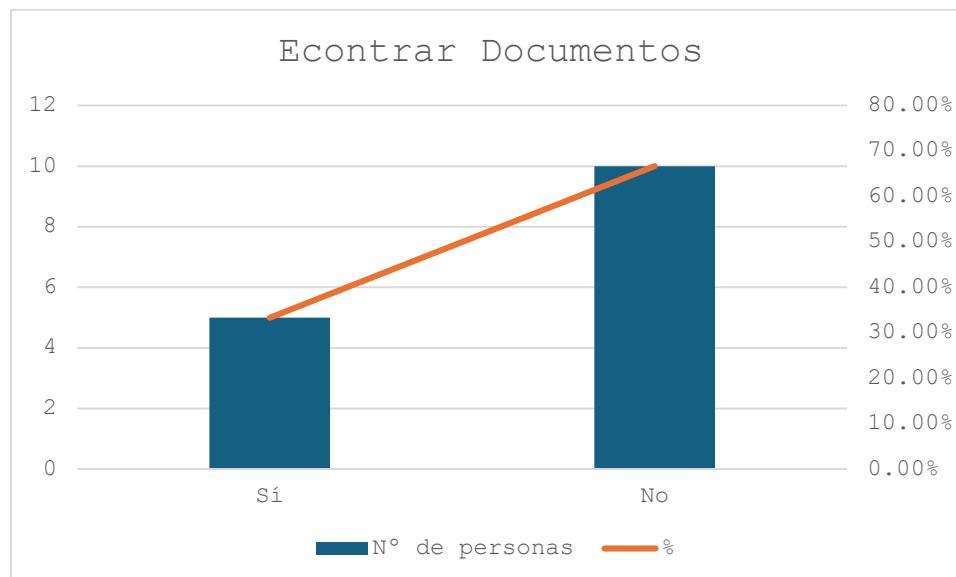
Descripción:

La mayoría de las personas acceden a los documentos solicitándolos directamente a un compañero (40%). Un 26.7% utiliza carpetas compartidas, mientras que el uso de un servidor interno es menos común (13.3%). Un 20% menciona otros medios de acceso. Esto sugiere que no hay un sistema centralizado y eficiente para el acceso a la información.

2. ¿Encuentra con facilidad los documentos que necesita?

Opción de respuesta	N° de personas	%
Sí	5	33.3%
No	10	66.7%

Tabla 4: Encontrar documentos con facilidad



Gráfica 2: Porcentaje al encontrar documentos con facilidad

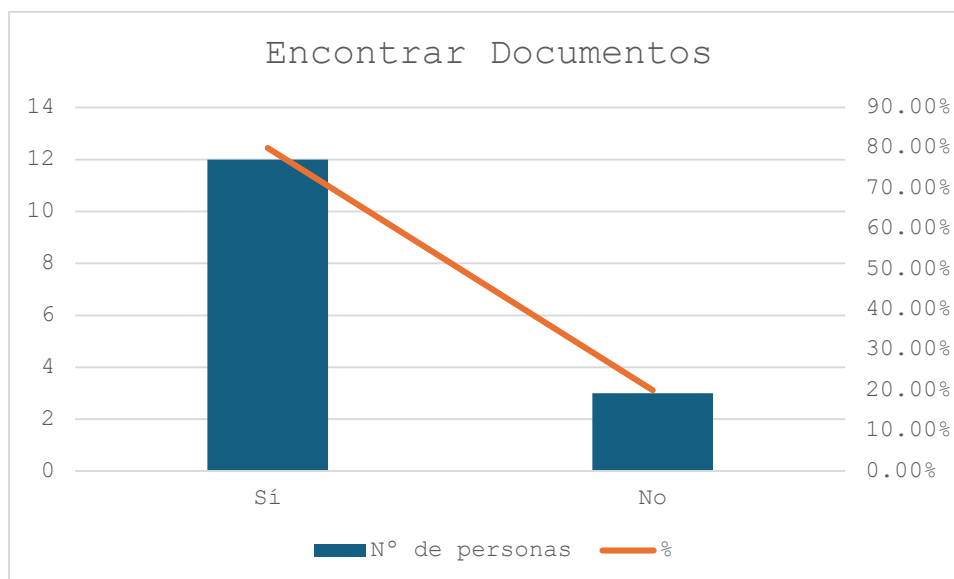
Descripción:

Una mayoría significativa (66.7%) indica que no encuentra con facilidad los documentos que necesita, lo cual evidencia una problemática en la organización o accesibilidad del sistema de documentación actual.

3. ¿Ha experimentado dificultades para encontrar documentos?

Opción de respuesta	Nº de personas	%
Sí	12	80.0%
No	3	20.0%

Tabla 5: Dificultad para encontrar documentos



Gráfica 3: Porcentaje de dificultad al encontrar documentos

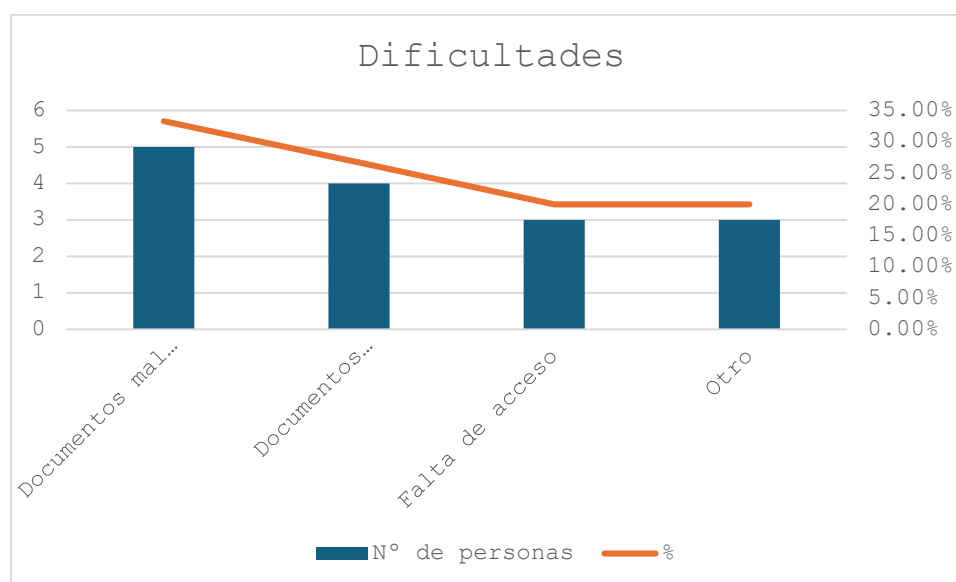
Descripción:

El 80% de los encuestados ha tenido dificultades para encontrar documentos. Esto refuerza el resultado anterior y apunta a una necesidad urgente de mejorar los métodos de almacenamiento y búsqueda de información.

4. Principales dificultades

Principales dificultades	N° de personas	%
Documentos mal clasificados	5	33.3%
Documentos desactualizados	4	26.7%
Falta de acceso	3	20.0%
Otro	3	20.0%

Tabla 6: Principales dificultades al encontrar documentos



Gráfica 4: Porcentaje de Principales dificultades al encontrar documentos

Descripción:

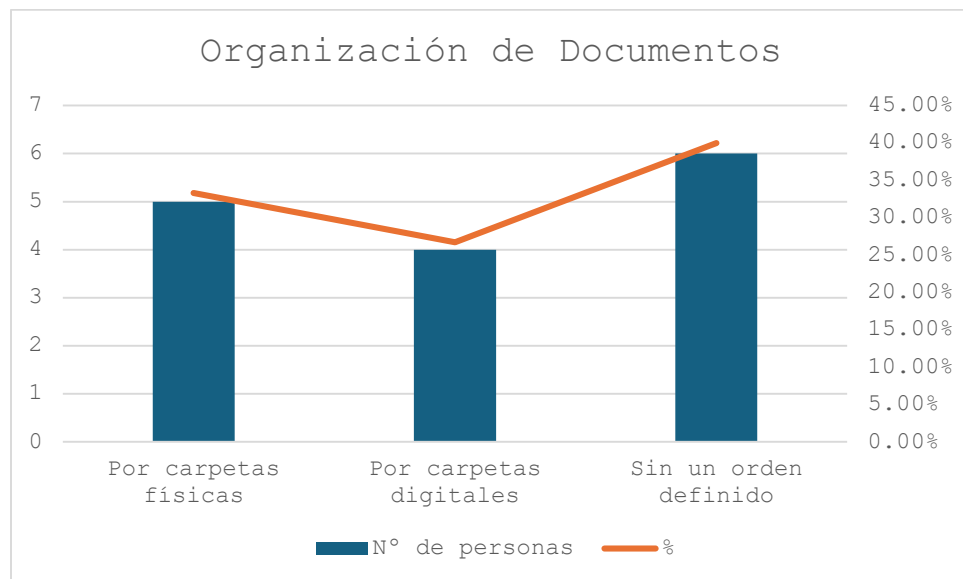
Las dificultades más comunes incluyen documentos mal clasificados (33.3%) y desactualizados (26.7%). También se mencionan la falta de acceso (20%) y otras causas. Esto revela fallas tanto en la gestión como en la actualización y disponibilidad de los documentos.

Clasificación y organización de documentos

1. ¿Cómo se organizan los documentos en su área de trabajo?

Opción de respuesta	N° de personas	%
Por carpetas físicas	5	33.3%
Por carpetas digitales	4	26.7%
Sin un orden definido	6	40.0%

Tabla 7: Organización de documentos en el área de trabajo



Gráfica 5: Porcentaje de organización de documentos en el área de trabajo

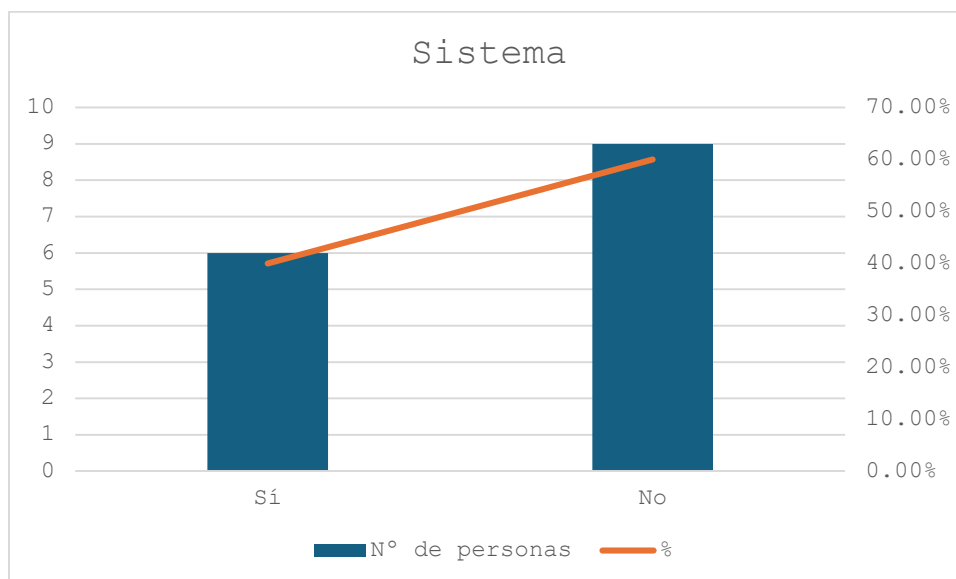
Descripción:

La mayoría de los participantes (40%) indicó que los documentos se organizan sin un orden definido, lo cual revela una falta de estandarización en los procesos de archivo. Un 33.3% usa carpetas físicas y un 26.7% carpetas digitales, lo que refleja una coexistencia de formatos sin un sistema unificado.

2. ¿Sigue algún sistema de clasificación específico?

Opción de respuesta	Nº de personas	%
Sí	6	40.0%
No	9	60.0%

Tabla 8: Sistema de clasificación específico



Gráfica 6: Porcentaje de uso de sistema de clasificación específico

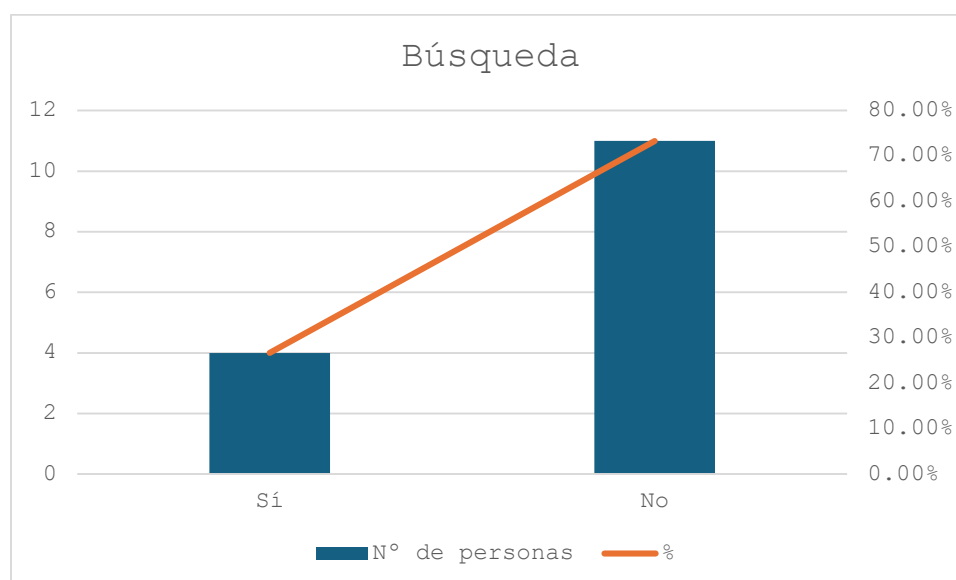
Descripción:

El 60% de los encuestados declaró que no utiliza un sistema de clasificación específico, lo que coincide con los resultados anteriores y pone en evidencia una gestión documental desorganizada. Solo el 40% manifestó seguir algún tipo de sistema.

3. ¿Considera que la clasificación actual facilita la búsqueda?

Opción de respuesta	Nº de personas	%
Sí	4	26.7%
No	11	73.3%

Tabla 9: Búsqueda de documentación con la clasificación actual



Gráfica 7: Porcentaje de búsqueda de documentación con la clasificación actual

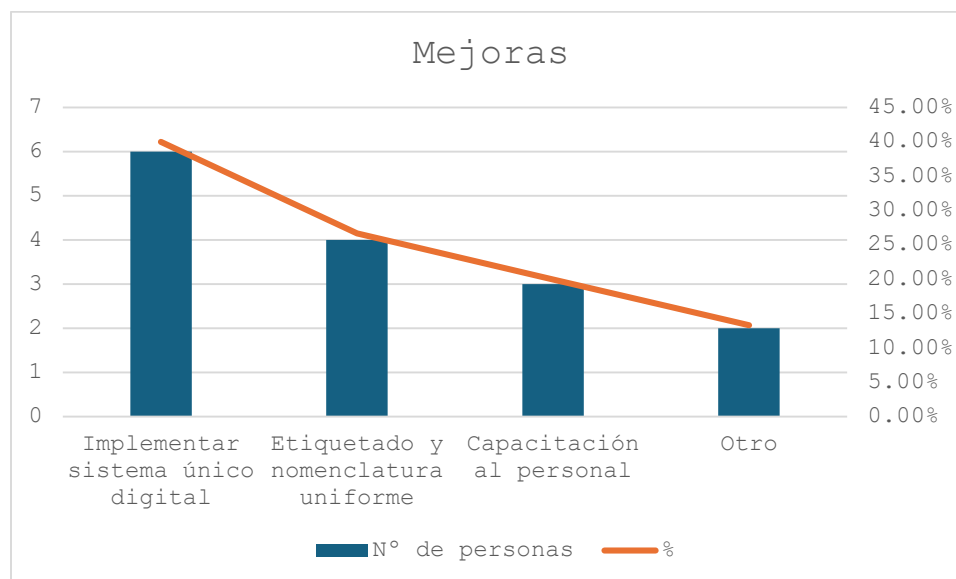
Descripción:

Una amplia mayoría (73.3%) considera que la clasificación actual no facilita el acceso ni la búsqueda de información. Esto sugiere que la falta de un sistema estructurado impacta negativamente en la eficiencia del trabajo y la localización de documentos.

4. Principales mejoras sugeridas

Mejora sugerida	N° de personas	%
Implementar sistema único digital	6	40.0%
Etiquetado y nomenclatura uniforme	4	26.7%
Capacitación al personal	3	20.0%
Otro	2	13.3%

Tabla 8: Mejoras sugeridas por los entrevistados



Gráfica 8: Porcentaje de mejoras sugeridas por los entrevistados

Descripción:

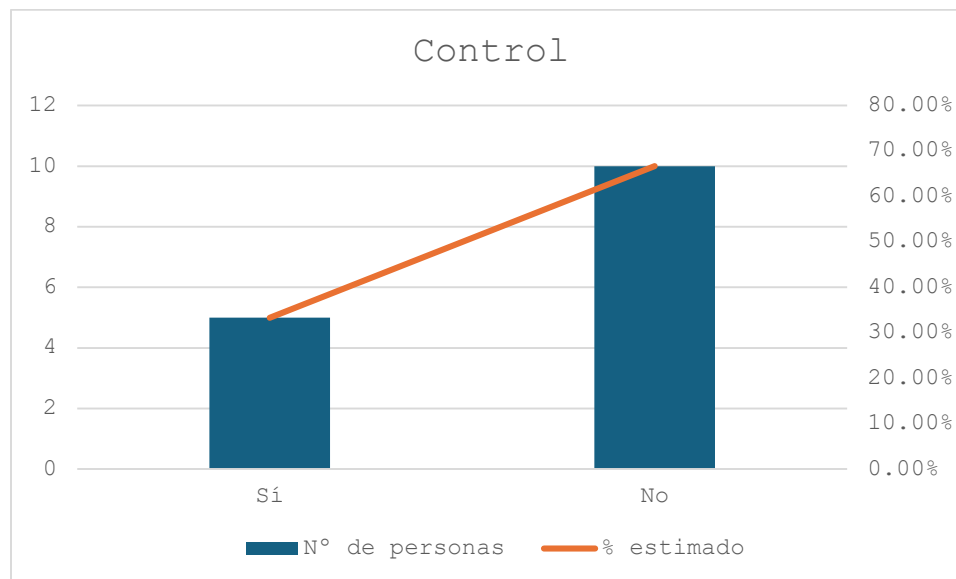
Las principales sugerencias para mejorar la organización documental se centran en la implementación de un sistema digital único (40%), seguido por la necesidad de estandarizar el etiquetado (26.7%) y capacitar al personal (20%). Estas propuestas apuntan a resolver la falta de orden y facilitar el acceso eficiente a la información.

Control de versiones

1. ¿Existen políticas claras sobre el control de versiones de los documentos en su área?

Opción de respuesta	Nº de personas	% estimado
Sí	5	33.3%
No	10	66.7%

Tabla 9: Políticas claras sobre el control de versiones de los documentos



Gráfica 9: Porcentaje de políticas claras sobre el control de versiones de los documentos

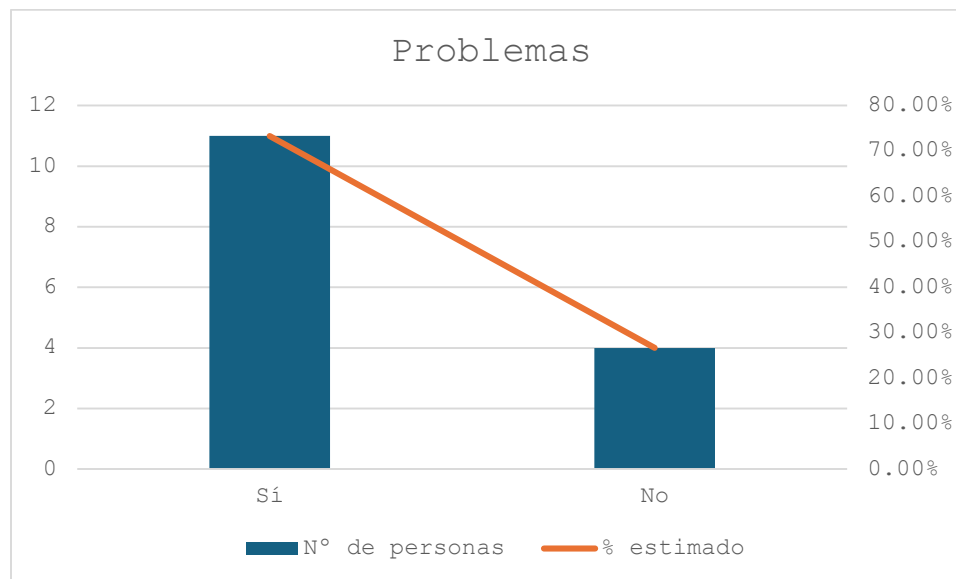
Descripción:

Dos tercios de los encuestados (66.7%) indicaron que no existen políticas claras sobre el control de versiones en su área de trabajo. Esto sugiere una falta de lineamientos formales que podría contribuir a errores o confusión en el manejo de documentos actualizados.

2. ¿Ha tenido algún problema al trabajar con versiones antiguas o desactualizadas de un documento?

Opción de respuesta	Nº de personas	% estimado
Sí	11	73.3%
No	4	26.7%

Tabla 12: Problema al trabajar con versiones antiguas o desactualizadas de un documento



Gráfica 10: Porcentaje de problema al trabajar con versiones antiguas o desactualizadas de un documento

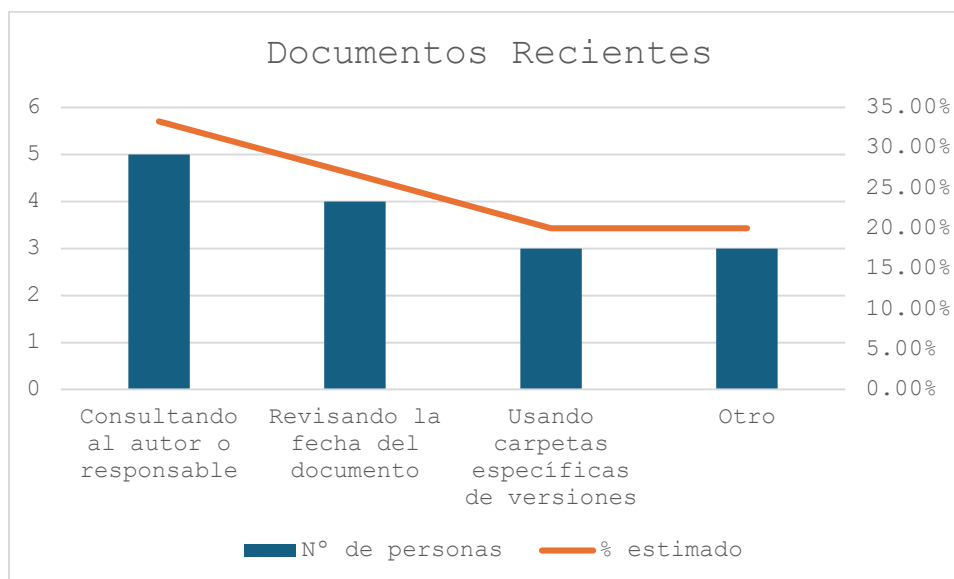
Descripción:

El 73.3% ha tenido problemas al trabajar con versiones antiguas o desactualizadas de documentos. Esto evidencia un impacto negativo directo de la falta de control de versiones, afectando la calidad del trabajo, la comunicación y la toma de decisiones.

3. ¿Cómo se asegura de estar utilizando la versión más reciente de un documento importante?

Método utilizado	Nº de personas	% estimado
Consultando al autor o responsable	5	33.3%
Revisando la fecha del documento	4	26.7%
Usando carpetas específicas de versiones	3	20.0%
Otro	3	20.0%

Tabla 13: Uso de documentos recientes



Gráfica 11: Porcentaje de uso de documentos recientes

Descripción:

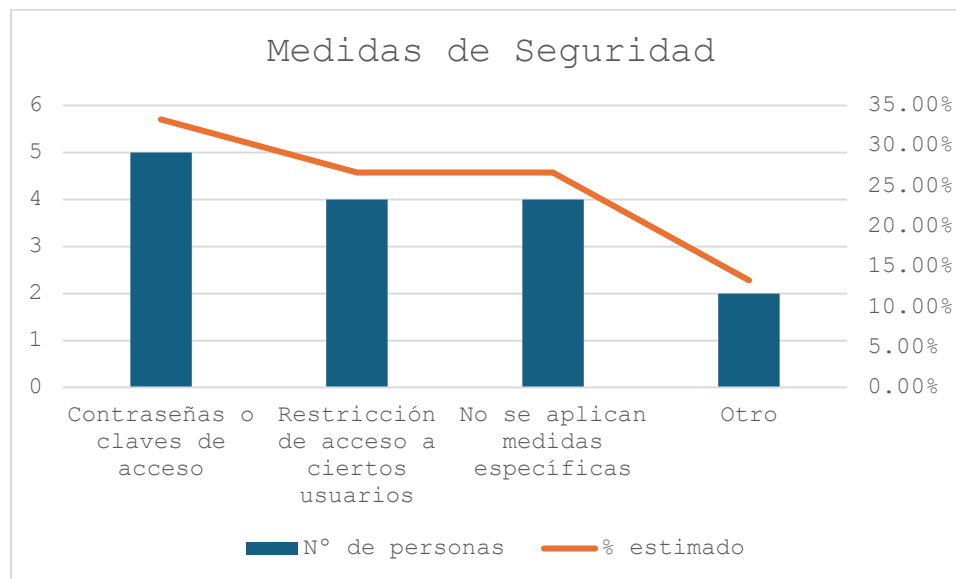
Los encuestados emplean diversas estrategias para asegurarse de usar la versión correcta de un documento, siendo la más común consultar directamente al autor o responsable (33.3%). Sin embargo, la variedad de métodos utilizados sugiere una falta de estandarización en el control de versiones, lo que puede generar incertidumbre.

Seguridad y protección de documentos

1. ¿Qué medidas de seguridad existen para proteger los documentos sensibles en su área de trabajo?

Medidas mencionadas	N° de personas	% estimado
Contraseñas o claves de acceso	5	33.3%
Restricción de acceso a ciertos usuarios	4	26.7%
No se aplican medidas específicas	4	26.7%
Otro	2	13.3%

Tabla 14: Medidas de seguridad para proteger los documentos sensibles



Gráfica 12: Porcentaje de medidas de seguridad para proteger los documentos sensibles

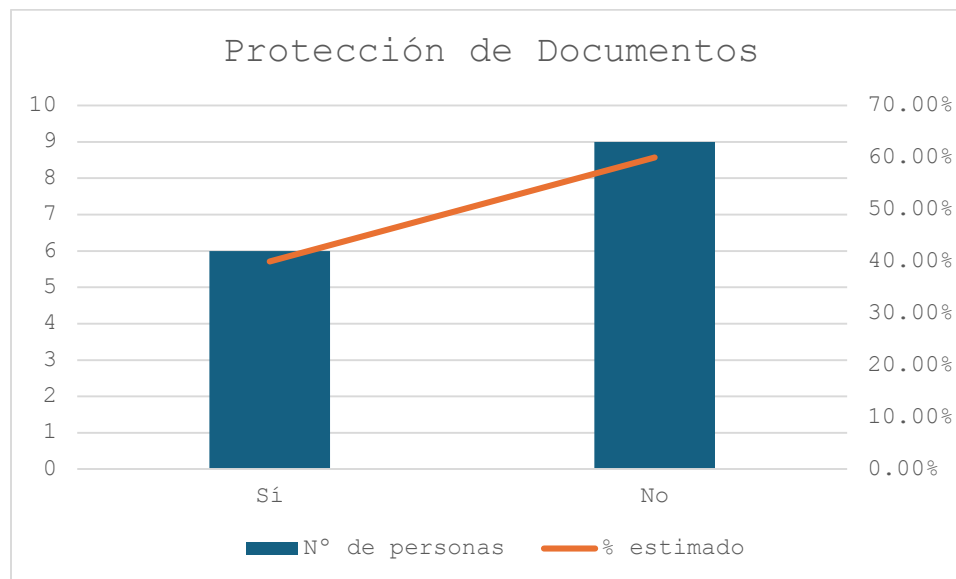
Descripción:

Entre las medidas de seguridad mencionadas, las más comunes fueron el uso de contraseñas o claves de acceso (33.3%) y la restricción de acceso a ciertos usuarios (26.7%). Sin embargo, es preocupante que un 26.7% de los encuestados señaló que no se aplican medidas específicas, lo cual representa un riesgo potencial para la protección de documentos confidenciales.

2. ¿Cree que los documentos confidenciales están lo suficientemente protegidos?

Opción de respuesta	Nº de personas	% estimado
Sí	6	40.0%
No	9	60.0%

Tabla 15: Protección de documentos



Gráfica 13: Porcentaje de protección de documentos

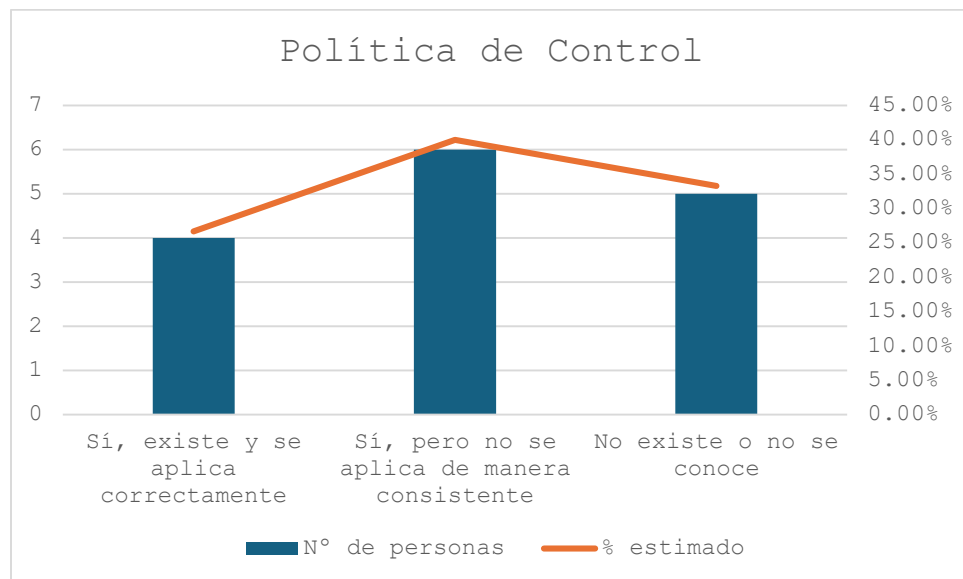
Descripción:

El 60% de los encuestados considera que los documentos confidenciales no están lo suficientemente protegidos, lo cual indica una percepción generalizada de vulnerabilidad en el sistema actual de seguridad documental.

3. ¿Conoce si hay alguna política de control de acceso a documentos confidenciales? ¿Está siendo aplicada correctamente?

Opción de respuesta	Nº de personas	% estimado
Sí, existe y se aplica correctamente	4	26.7%
Sí, pero no se aplica de manera consistente	6	40.0%
No existe o no se conoce	5	33.3%

Tabla 16: Política de acceso a documentos confidenciales



Gráfica 14: Porcentaje de la política de acceso a documentos confidenciales

Descripción:

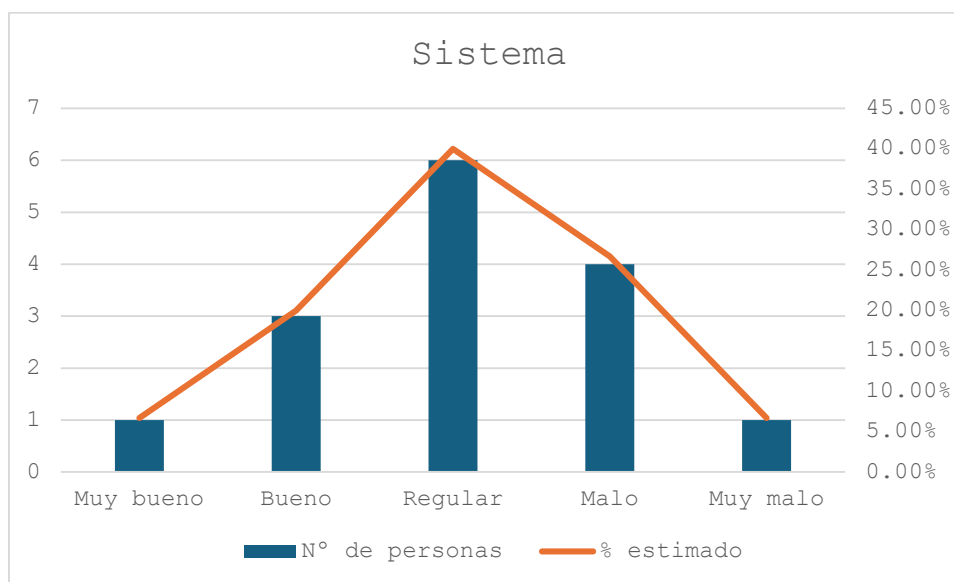
Aunque un 26.7% reconoce que sí existe una política de control de acceso y se aplica correctamente, un 40% indica que la política existe pero no se aplica de manera consistente, y otro 33.3% afirma no conocer o no contar con políticas claras. Esto revela fallas tanto en la implementación como en la comunicación de las medidas de protección de documentos sensibles.

Percepción general

1. ¿Cómo describiría el sistema actual de gestión documental?

Opciones de respuesta	Nº de personas	% estimado
Muy bueno	1	6.7%
Bueno	3	20.0%
Regular	6	40.0%
Malo	4	26.7%
Muy malo	1	6.7%

Tabla 17: Descripción del sistema documental



Gráfica 15: Porcentaje de descripción del sistema documental

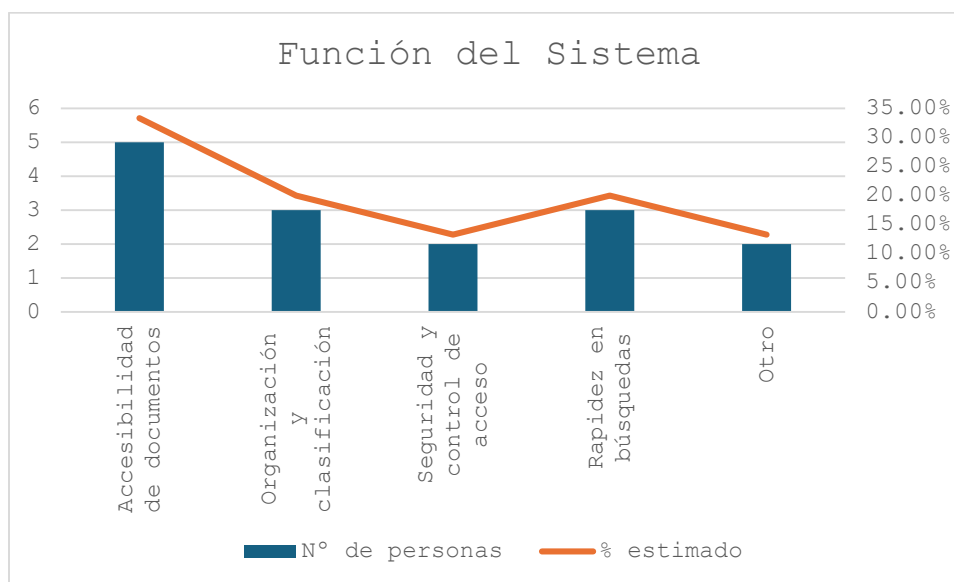
Descripción:

Solo un 26.7% de los entrevistados califica el sistema documental como bueno o muy bueno, mientras que un 46.7% lo considera malo o muy malo. El porcentaje mayoritario, 40%, señala que el sistema es regular, lo que refleja una percepción general de insuficiencia y la necesidad urgente de mejorar el proceso documental.

2. ¿Qué aspectos considera que funcionan bien en el sistema actual de gestión documental?

Opciones de respuesta	Nº de personas	% estimado
Accesibilidad de documentos	5	33.3%
Organización y clasificación	3	20.0%
Seguridad y control de acceso	2	13.3%
Rapidez en búsquedas	3	20.0%
Otro	2	13.3%

Tabla 18: Aspectos de la función actual del sistema documental



Gráfica 16: Porcentaje de aspectos de la función actual del sistema documental

Descripción:

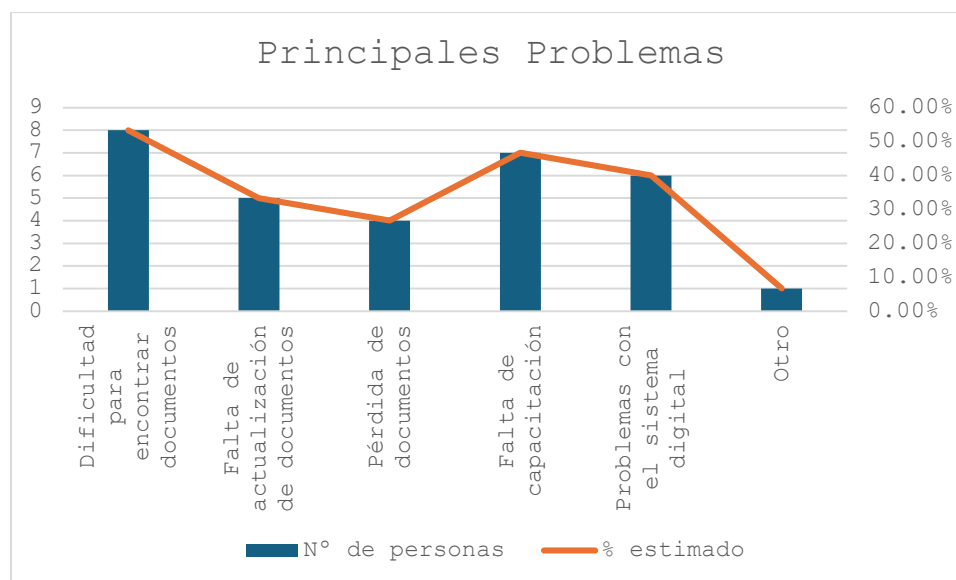
Aunque un 33.3% reconoce que la accesibilidad a documentos es un punto fuerte, la baja valoración de la seguridad y el control de acceso (13.3%) indica deficiencias importantes en la protección de la información. Esto junto con un bajo reconocimiento a la organización sugiere que varios aspectos clave no están funcionando adecuadamente.

3. ¿Cuáles son los principales problemas o desafíos que enfrenta con la gestión documental en su día a día?

Opciones de respuesta	Nº de personas	% estimado
Dificultad para encontrar documentos	8	53.3%
Falta de actualización de documentos	5	33.3%
Pérdida de documentos	4	26.7%
Falta de capacitación	7	46.7%
Problemas con el sistema digital	6	40.0%

Otro	1	6.7%
------	---	------

Tabla 19: Principales problemas en la gestión documental



Gráfica 17: Porcentaje de los principales problemas en la gestión documental

Descripción:

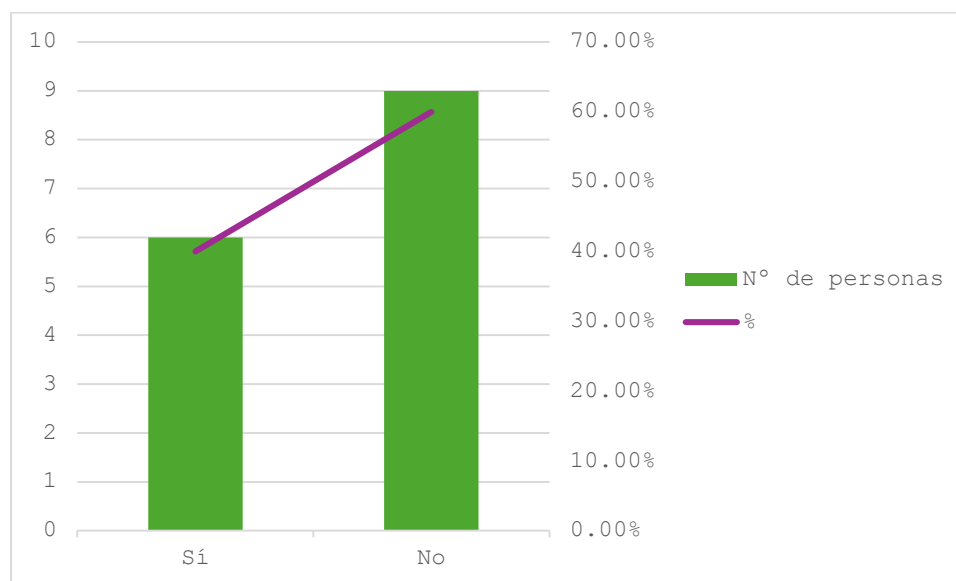
Los resultados muestran que más de la mitad de los entrevistados (53.3%) enfrentan dificultades para encontrar documentos, y casi la mitad (46.7%) reportan falta de capacitación. Además, el 40% menciona problemas con el sistema digital. Estos datos evidencian grandes retos operativos y organizacionales que requieren una intervención estructurada, como la implementación de un manual que estandarice y optimice los procesos.

Análisis de la Encuesta

1. ¿Se utilizan categorías específicas para clasificar los documentos?

Opción de respuesta	Nº de personas	%
Sí	6	40.0%
No	9	60.0%

Tabla 20: Uso de categorías para clasificar documentos



Gráfica 18: Porcentaje de uso de categorías para clasificar documentos

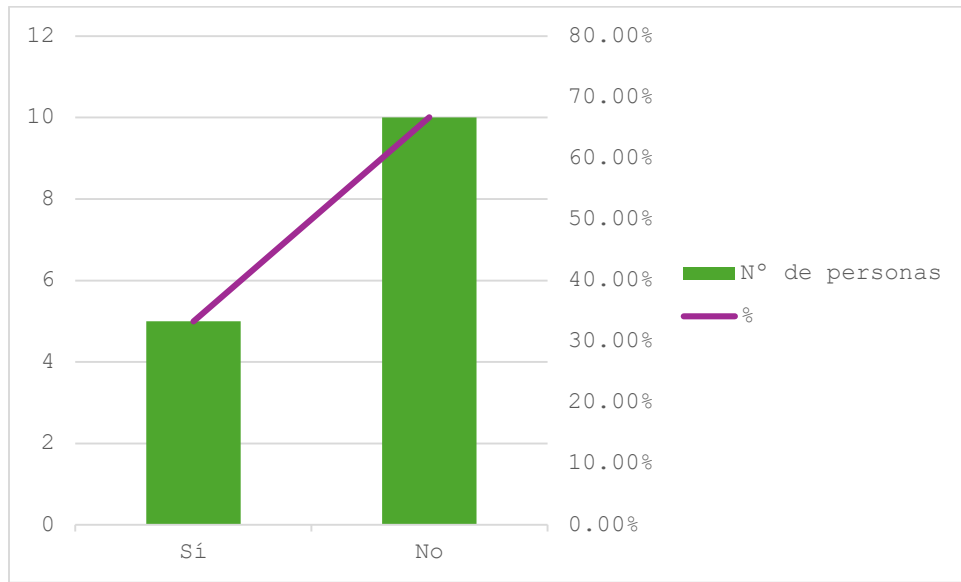
Descripción:

El 60% de los encuestados indica que no se utilizan categorías específicas para clasificar los documentos, lo cual evidencia una falta de estructura clara que puede dificultar la organización y recuperación de la información.

2. ¿Los documentos están clasificados de manera uniforme en todas las áreas?

Opción de respuesta	Nº de personas	%
Sí	5	33.3%
No	10	66.7%

Tabla 21: Documentos clasificados de manera uniforme en todas las áreas



Gráfica 19: Porcentaje de documentos clasificados de manera uniforme en todas las áreas

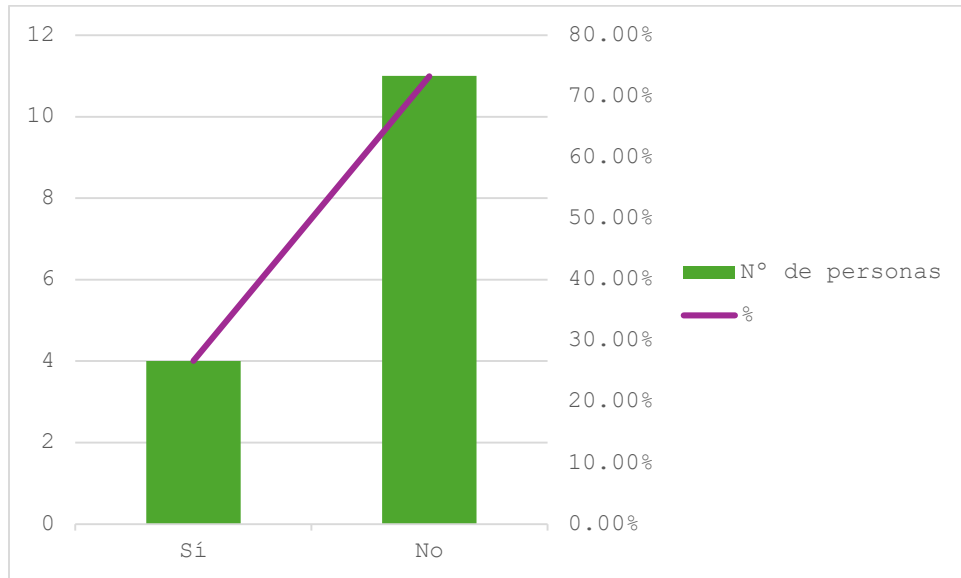
Descripción:

La mayoría (66.7%) afirma que no hay una clasificación uniforme entre áreas, lo que sugiere una gestión documental fragmentada y poco estandarizada. Esto puede generar duplicidad de información, errores o pérdida de trazabilidad.

3. ¿Se aplican controles de acceso para documentos sensibles?

Opción de respuesta	Nº de personas	%
Sí	4	26.7%
No	11	73.3%

Tabla 22: Controles de acceso para documentos sensibles



Gráfica 20: Porcentaje de controles de acceso para documentos sensibles

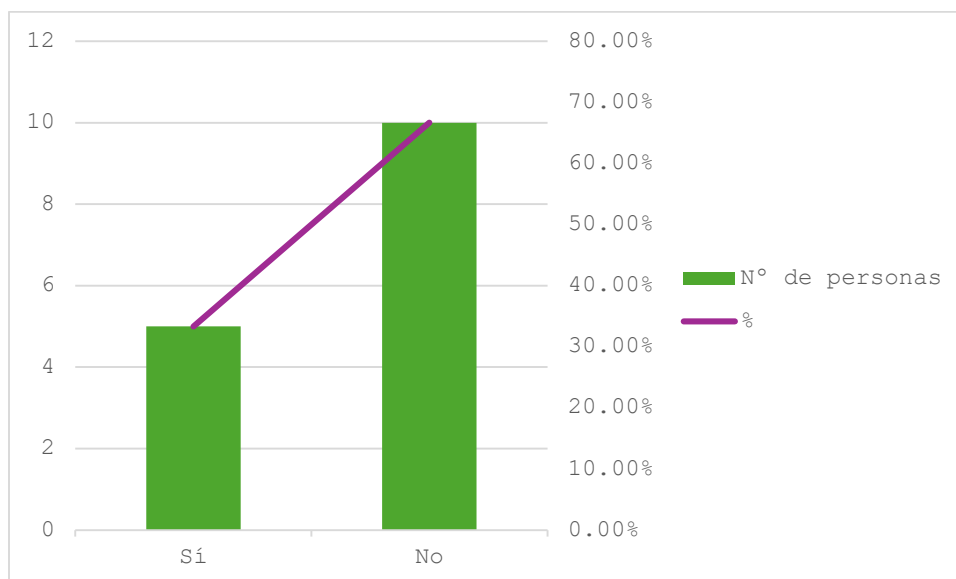
Descripción:

Con un 73.3% de respuestas negativas, queda claro que los controles de acceso a documentos sensibles son deficientes o inexistentes, representando un riesgo importante para la seguridad de la información confidencial.

4. ¿Cada documento tiene asignado un responsable de su custodia?

Opción de respuesta	Nº de personas	%
Sí	5	33.3%
No	10	66.7%

Tabla 23: Documento asignado por un responsable en custodia



Gráfica 21: Porcentaje de documentos asignados por un responsable en custodia

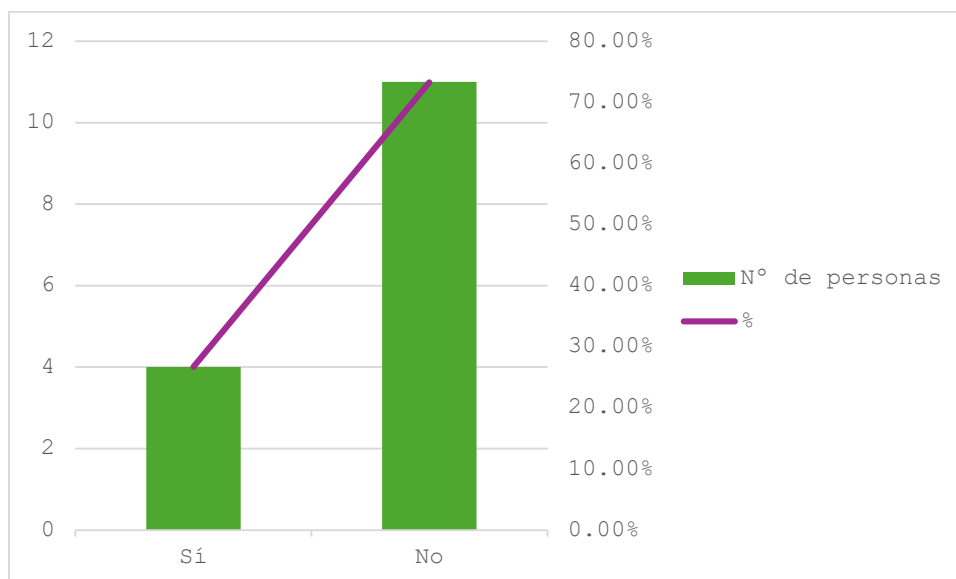
Descripción:

El 66.7% de los encuestados indican que no hay responsables asignados para la custodia de documentos, lo cual compromete la trazabilidad, responsabilidad y control de los archivos institucionales.

5. ¿Existen registros claros de las versiones de documentos?

Opción de respuesta	Nº de personas	%
Sí	4	26.7%
No	11	73.3%

Tabla 24: Registros de versiones de documentos



Gráfica 22: Porcentaje de registros de versiones de documentos

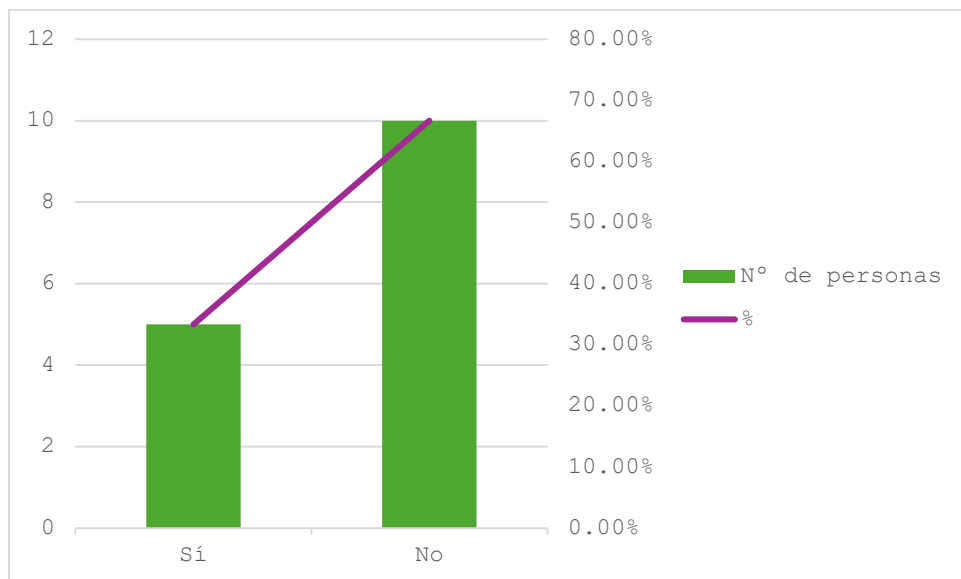
Descripción:

La ausencia de registros de versiones en el 73.3% de los casos muestra una debilidad crítica en el control documental, dificultando la actualización y aumentando el riesgo de usar información obsoleta.

6. ¿Cada versión de un documento tiene una fecha de creación y edición?

Opción de respuesta	Nº de personas	%
Sí	5	33.3%
No	10	66.7%

Tabla 25: Documentos con fecha de crearon y edición



Gráfica 23: Porcentaje de documentos con fecha de crearon y edición

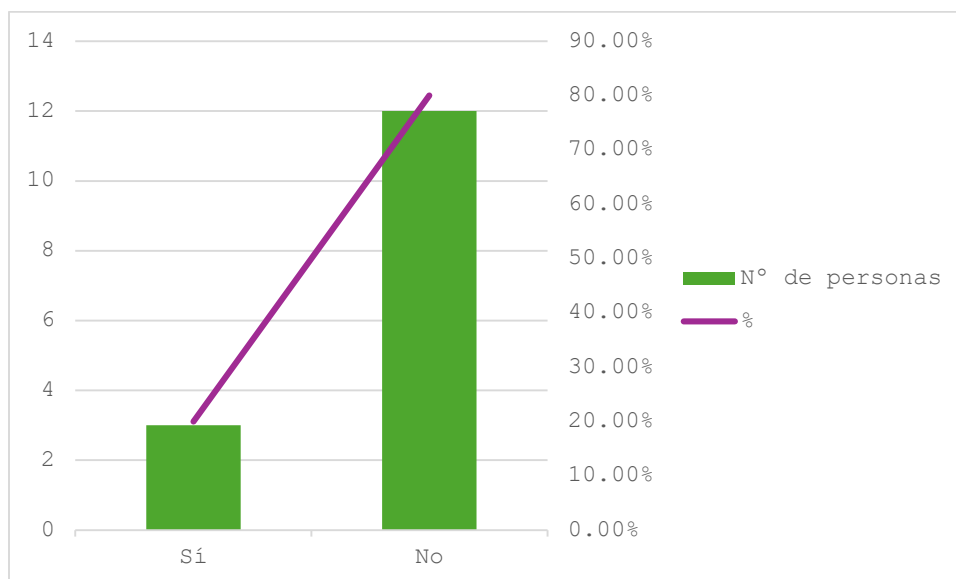
Descripción:

Un 66.7% indica que no se registra la fecha de creación o edición de las versiones de los documentos, lo que impide llevar un control efectivo de los cambios y dificulta auditorías o seguimientos.

7. ¿Los documentos críticos están protegidos por contraseñas o cifrado?

Opción de respuesta	Nº de personas	%
Sí	3	20.0%
No	12	80.0%

Tabla 26: Documentos críticos protegidos



Gráfica 24: Porcentaje de documentos críticos protegidos

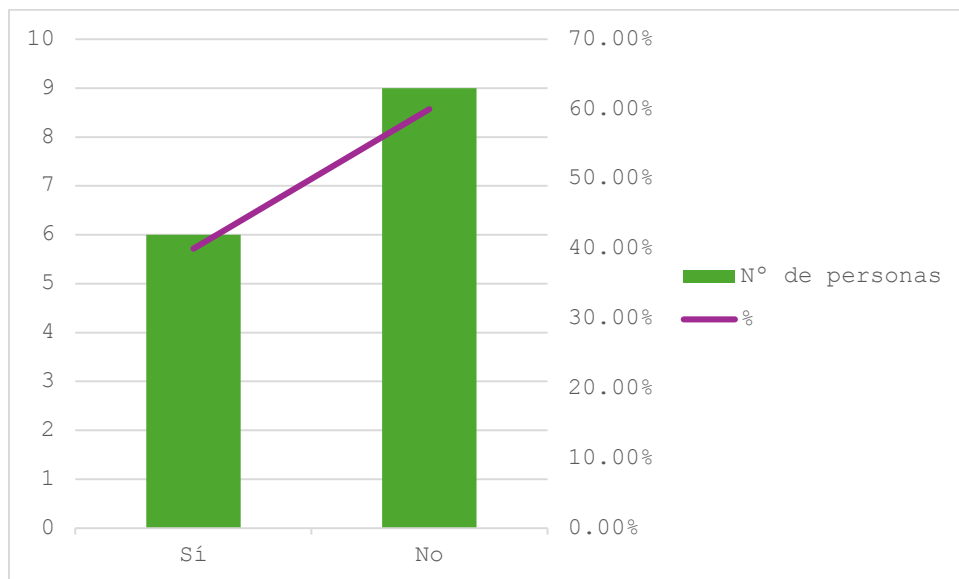
Descripción:

Solo un 20% señala que los documentos críticos están protegidos, mientras que el 80% restante pone en evidencia una grave vulnerabilidad en la seguridad documental que podría comprometer información sensible.

8. ¿Existen procedimientos para realizar copias de seguridad de los documentos?

Opción de respuesta	Nº de personas	%
Sí	6	40.0%
No	9	60.0%

Tabla 27: Procedimientos de copia de seguridad de la documentación



Gráfica 25: Porcentaje de procedimientos para crear copia de seguridad de la documentación

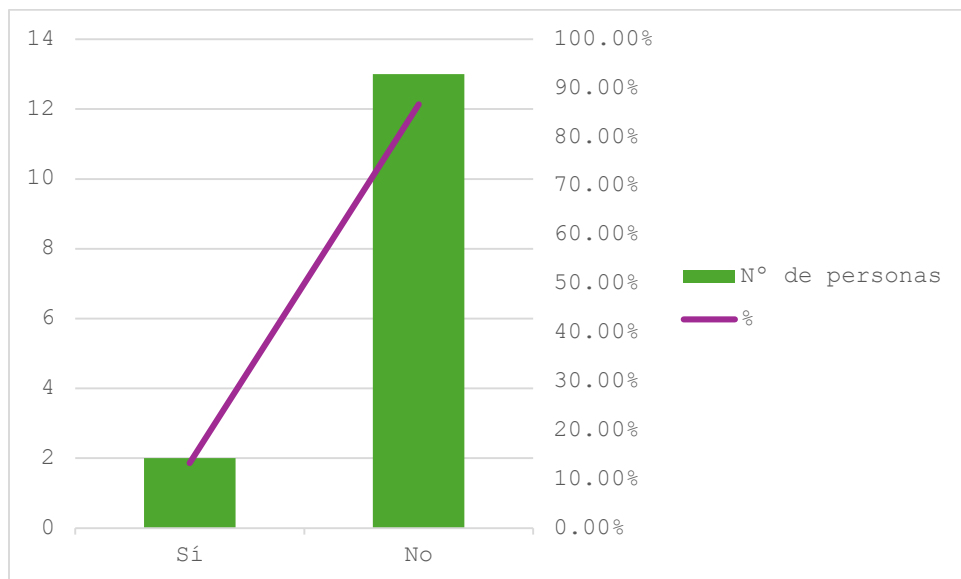
Descripción:

La falta de procedimientos claros de respaldo en el 60% de los casos representa un riesgo alto frente a pérdida de datos por fallas técnicas o errores humanos, comprometiendo la continuidad operativa.

9. ¿La gestión documental sigue los estándares ISO/IEC 27001 o TISAX?

Opción de respuesta	N° de personas	%
Sí	2	13.3%
No	13	86.7%

Tabla 28: Documentación con estándares ISO/IEC 27001 o TISAX



Gráfica 26: Porcentaje de la documentación con estándares ISO/IEC 27001 o TISAX

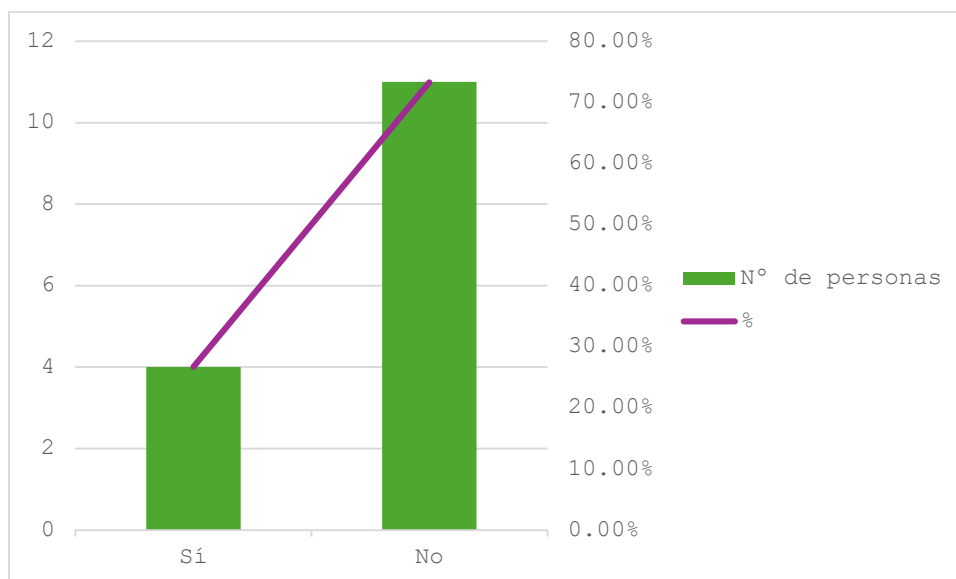
Descripción:

El 86.7% no sigue ningún estándar reconocido, lo que denota una gestión documental alejada de buenas prácticas internacionales. Esta situación reduce la confiabilidad y eficiencia del sistema.

10. ¿Se realizan auditorías periódicas del sistema de gestión documental?

Opción de respuesta	Nº de personas	%
Sí	4	26.7%
No	11	73.3%

Tabla 29: Auditorías al sistema documental



Gráfica 27: Porcentaje de auditorías al sistema documental

Descripción:

La falta de auditorías periódicas (73.3%) muestra que no se evalúa ni se mejora de forma continua el sistema documental, lo que favorece la acumulación de errores, duplicidades y malas prácticas.

Análisis de la Observación Directa

Escala de Ponderación

Se asignó valores según el cumplimiento observado, se usó esta escala:

Cumplimiento	Puntos
✓ Sí	2
⚠ Parcialmente	1
✗ No	0

Tabla 30: Análisis de la observación directa: escala de ponderación

Luego, se suman los puntos obtenidos por cada categoría, con la finalidad de calcular el porcentaje de cumplimiento y así, hacer una evaluación global.

Categorías y número de indicadores

Estas son las 5 categorías y cuántos indicadores observaste en cada una:

Categoría	Nº de indicadores
Clasificación de documentos	3
Almacenamiento físico/digital	4
Acceso a documentos	3
Seguridad documental	3
Cumplimiento con TISAX	4

Tabla 31: Categoría y numero de indicadores

Puntaje máximo por categoría

Fórmula:

$$\text{Puntaje máximo} = \text{Nº de Indicadores} \times 2$$

Las tablas se organizan por categoría evaluada, con indicadores observados y un juicio general (positivo o negativo).

Clasificación de Documentos

Indicador observado	¿Se cumple?	Observación breve

Criterios definidos para clasificación	✗	No hay criterios estandarizados
Etiquetado uniforme	✗	Etiquetado inconsistente entre áreas
Diferenciación por tipo de documento	⚠	Algunos tipos diferenciados, otros no
Evaluación general de la categoría	✗ Negativa	Clasificación poco estructurada y desorganizada

Tabla 32: Evaluación: clasificación de documentos

Almacenamiento Físico y Digital

Indicador observado	¿Se cumple?	Observación breve
Condiciones del espacio físico	✗	Desorden y falta de control físico
Organización de archivos digitales	✗	Carpetas duplicadas y sin estructura clara
Respaldo automático de archivos	✗	No hay respaldo frecuente o automatizado
Acceso a plataformas seguras (nube o servidores)	⚠	Solo algunas áreas usan nube, sin control claro
Evaluación general de la categoría	✗ Negativa	Almacenamiento vulnerable y sin procedimientos

Tabla 33: Evaluación: almacenamiento físico y digital

Acceso a Documentos

Indicador observado	¿Se cumple?	Observación breve
Facilidad de localización	✗	Difícil encontrar documentos en ambos formatos

Tiempo promedio de búsqueda	✗	7–10 minutos en físico; confuso en digital
Acceso limitado a usuarios autorizados	✗	No hay controles de acceso implementados
Evaluación general de la categoría	✗ Negativa	Acceso lento y sin restricciones por usuario

Tabla 34: Evaluación: acceso a documentos

Seguridad en el Manejo de Documentos

Indicador observado	¿Se cumple?	Observación breve
Uso de contraseñas o cifrado en documentos críticos	✗	No se aplican medidas digitales de seguridad
Archiveros cerrados y restringidos físicamente	✗	Archiveros abiertos, sin candados ni control
Prácticas de protección de información	✗	No hay cultura de protección ni controles visibles
Evaluación general de la categoría	✗ Negativa	Seguridad documental inexistente

Tabla 35: Evaluación: seguridad en el manejo de documentos

Cumplimiento con políticas TISAX

Indicador observado	¿Se cumple?	Observación breve
Confidencialidad de la información	✗	No hay control de acceso ni cifrado
Integridad de los documentos	✗	Sin control de versiones ni validaciones
Disponibilidad de documentos clave	⚠	Acceso lento, especialmente en físico

Evidencia de procedimientos TISAX	✗	No hay políticas documentadas ni trazabilidad
Evaluación general de la categoría	✗ Negativa	Incumplimiento evidente de los lineamientos TISAX

Tabla 36: Evaluación: cumplimiento con políticas TISAX

Tabla con Ponderación por Categoría

Categoría	Indicadores evaluados	Puntaje máximo	Puntaje obtenido	% Cumplimiento	Evaluación
Clasificación de documentos	3	6	1 (0+0+1)	16.7%	✗ Deficiente
Almacenamiento físico/digital	4	8	1 (0+0+0+1)	12.5%	✗ Deficiente
Acceso a documentos	3	6	0 (0+0+0)	0.0%	✗ Deficiente
Seguridad en manejo de documentos	3	6	0 (0+0+0)	0.0%	✗ Crítico
Cumplimiento con TISAX	4	8	1 (0+0+1+0)	12.5%	✗ Deficiente

Tabla 37: Evaluación de ponderación por categoría

Tabla Resumen Final

Categoría	% Cumplimiento	Evaluación
-----------	----------------	------------

Clasificación de documentos	16.7%	✗ Deficiente
Almacenamiento físico/digital	12.5%	✗ Deficiente
Acceso a documentos	0.0%	✗ Deficiente
Seguridad documental	0.0%	✗ Crítico
Cumplimiento con TISAX	12.5%	✗ Deficiente
Promedio general	8.3%	✗ Deficiente

Tabla 38: Promedio general: final de evaluación

Evaluación final por categoría

En función del % de cumplimiento, se usa esta escala de interpretación:

% Cumplimiento	Evaluación
0% – 20%	✗ Deficiente
21% – 40%	⚠ Bajo cumplimiento
41% – 70%	⚠ Parcial
71% – 90%	✓ Aceptable
91% – 100%	✓ Óptimo

Tabla 39: Porcentaje de cumplimiento

Interpretación Final:

Con un promedio general de cumplimiento de apenas 8.3%, el sistema de gestión documental observado se encuentra en un estado crítico. Todas las áreas muestran niveles muy bajos de conformidad, especialmente en seguridad y acceso, que no presentan ninguna práctica efectiva.

Este análisis ponderado refuerza contundentemente la necesidad de implementar un Manual de Gestión Documental, que estandarice procedimientos, garantice la

protección de la información y eleve el cumplimiento normativo, especialmente en relación con TISAX e ISO/IEC 27001.

Análisis de Checklist

Porcentaje de Cumplimiento por ítem

Fórmula:

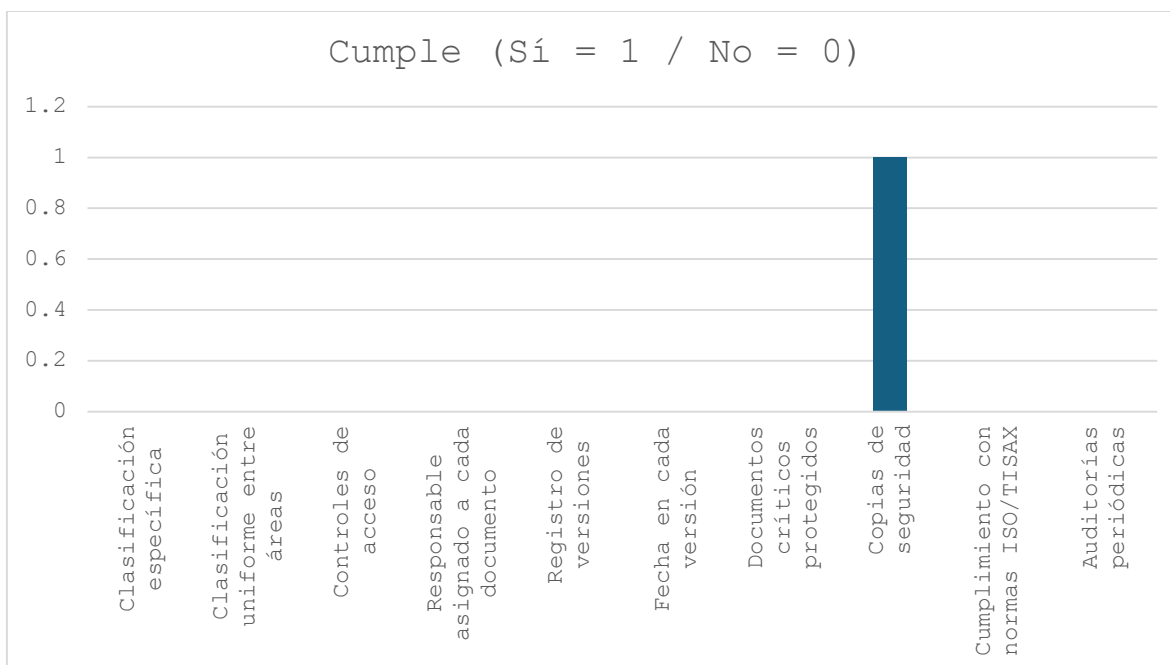
$$\% \text{ Cumplimiento} = (\text{suma de respuestas "Sí"} \div \text{Total de Ítems}) \times 100$$

Para identificar los niveles de cumplimiento en relación con los aspectos clave de la gestión documental evaluados, a continuación, se presenta una tabla que resume e interpreta los resultados obtenidos a partir de la lista de cotejo aplicada:

Ítem	Pregunta	Respuesta simulada	Cumple (Sí = 1 / No = 0)
1	¿Se utilizan categorías específicas para clasificar los documentos?	No	0
2	¿Los documentos están clasificados de manera uniforme en todas las áreas?	No	0
3	¿Se aplican controles de acceso para documentos sensibles?	No	0
4	¿Cada documento tiene asignado un responsable de su custodia?	No	0
5	¿Existen registros claros de las versiones de documentos?	No	0
6	¿Cada versión de un documento tiene fecha de creación y edición?	No	0
7	¿Documentos críticos protegidos con contraseña o cifrado?	No	0
8	¿Procedimientos de copias de seguridad existen?	Sí	1
9	¿La gestión sigue ISO/IEC 27001 o TISAX?	No	0

10	¿Se realizan auditorías periódicas del sistema documental?	No	0
----	--	----	---

Tabla 40: Resumen e interpretación de resultados obtenidos en la lista de cotejo aplicada



Gráfica 28: Cumplimiento de la lista de cotejo aplicada

Análisis general del cumplimiento (Checklist):

La lista de cotejo aplicada como auditoría preliminar muestra un bajo nivel de cumplimiento de las prácticas recomendadas en gestión documental. Solo 1 de 10 ítems fue respondido afirmativamente, lo que representa un cumplimiento del 10%.

Las áreas más críticas son:

- Ausencia de clasificación documental estandarizada
- Falta de control de versiones y trazabilidad
- Nula aplicación de medidas de seguridad digital
- Desalineación con normativas internacionales (ISO 27001 / TISAX)

Estos resultados reflejan la urgente necesidad de diseñar e implementar un Manual de Gestión Documental que incluya políticas, controles de acceso, trazabilidad documental y respaldo de información conforme a buenas prácticas internacionales.

Diagnostico Documental del Área de TI (Actual)

El análisis de la situación actual de la gestión de documentos en el área de tecnologías de la información de Sonavox Electronics Co, se identificaron las principales problemáticas relacionadas con el manejo de la documentación digital y la seguridad de la información.

Problemas Detectados

Con base en los instrumentos aplicados (encuestas, observación directa y listas de cotejo), se identificaron una serie de deficiencias estructurales y operativas en la gestión documental actual. Estos problemas afectan directamente la eficiencia, trazabilidad, seguridad y organización de la información. A continuación, se resumen los principales hallazgos:

1. Acceso desorganizado a los documentos: Predomina el uso de medios informales, como la solicitud directa entre compañeros, sin un repositorio único ni control de acceso claro.
2. Ausencia de criterios estandarizados de clasificación: No existen lineamientos uniformes para ordenar, etiquetar o agrupar los documentos, lo cual dificulta su búsqueda y recuperación.
3. Falta de control de versiones y trazabilidad: Los usuarios enfrentan dificultades para identificar la versión vigente de un documento, lo que aumenta el riesgo de errores operativos y decisiones basadas en información desactualizada.
4. Inexistencia de responsables documentales por archivo o área: No hay claridad sobre quién es el encargado de mantener, actualizar o custodiar los documentos, afectando la responsabilidad y seguimiento.

5. Deficiencias en la seguridad de la información: Se observan prácticas insuficientes de protección para documentos sensibles. En muchos casos no se aplican contraseñas, cifrado ni restricciones de acceso.
6. Falta de alineación con estándares normativos: El sistema documental actual no se encuentra estructurado con base en estándares reconocidos como ISO/IEC 27001 o TISAX.
7. Ausencia de auditorías y revisiones documentales periódicas: No se han establecido mecanismos formales de control o mejora continua sobre los procesos documentales.
8. Baja capacitación del personal en gestión documental: El desconocimiento de buenas prácticas y herramientas genera errores frecuentes y uso inconsistente de los métodos disponibles.

Matriz de Factores Internos (MFI) – Proyecto Manual de Gestión Documental

La Matriz de Factores Internos (MFI) es una herramienta de análisis estratégico que se centra únicamente en factores internos de la organización, clasificándolos en:

- Fortalezas: Capacidades y recursos positivos que la organización puede usar para mejorar o alcanzar objetivos.
- Debilidades: Limitaciones o problemas internos que deben corregirse o minimizarse.

Se usa para evaluar qué tan preparada está la organización para desarrollar un proyecto, en este caso, un Manual de Gestión Documental.

Calcular el Puntaje Ponderado

$$\text{Fórmula: Puntaje ponderado} = \text{Ponderación} \times \text{Calificación}$$

Paso 1: Identificar los factores internos clave, divididos en fortalezas y debilidades.

Paso 2: La ponderación indica la importancia relativa de cada factor en el éxito del proyecto. Va de 0.0 (nada importante) a 1.0 (muy importante) y la suma total de todos los factores debe ser 1.0 (o 100%).

Paso 2: La calificación mide el desempeño actual de la organización en cada factor, de 1 a 4:

- 4 = Excelente / Muy fuerte
- 3 = Bueno / Fuerte
- 2 = Promedio / Debilidad moderada
- 1 = Muy débil / Necesita mejorar urgentemente.

A continuación, se presenta la Matriz de Factores Internos (MFI):

FORTALEZAS (F)			
Factor	Ponderación	Calificación (1-4)	Puntaje ponderado
F1: El personal muestra disposición al cambio y apertura para mejorar los procesos documentales.	0.25	3	0.75
F2: Existen prácticas informales de colaboración para compartir documentos.	0.20	2	0.40
F3: Hay conciencia colectiva sobre las deficiencias del sistema actual.	0.25	3	0.75
F4: Algunas áreas han iniciado el uso de herramientas digitales.	0.30	2	0.60
Suma Fortalezas	1.0		2.5
DEBILIDADES (D)			

Factor	Ponderación	Calificación (1-4)	Puntaje ponderado
D1: No existe una clasificación estandarizada ni uniforme.	0.20	1	0.20
D2: No se realiza un control formal de versiones ni se identifica la fecha de creación o edición.	0.15	1	0.15
D3: La seguridad documental es débil.	0.20	1	0.20
D4: No hay responsables asignados por tipo de documento o categoría.	0.15	2	0.30
D5: El sistema documental no está alineado con estándares como ISO/IEC 27001 o TISAX.	0.15	1	0.15
D6: El personal no ha recibido capacitación formal en gestión documental.	0.15	1	0.15
Suma Debilidades	1.0		1.15

Tabla 41: Matriz de Factores Internos (MFI) – Proyecto Manual de Gestión Documental

Resultado Final

$$\text{Formula: Total MFI} = 2.50 - 1.15 = 1.35$$

- Si el resultado es positivo, la organización tiene más fortalezas que debilidades y el proyecto tiene buenas bases internas.
- Si el resultado es cercano a 0, la organización está equilibrada, pero debe trabajar en sus debilidades.

- Si el resultado es negativo, las debilidades superan a las fortalezas y se requiere intervención urgente.

Interpretación:

Puntaje positivo (1.35) indica que la organización tiene fortalezas importantes que favorecen el proyecto.

Sin embargo, las debilidades documentales son críticas y requieren acciones inmediatas:

- Establecer clasificación estandarizada.
- Implementar control formal de versiones y fechas.
- Mejorar seguridad documental.
- Asignar responsables por categoría de documentos.
- Capacitar al personal en gestión documental.

Áreas de Mejora Identificadas

Dado que la implementación de un sistema digital formal (programa o software) queda fuera del alcance de este proyecto, las acciones se concentrarán en la elaboración de un Manual de Gestión Documental como herramienta principal para estandarizar procesos, acompañado de una capacitación dirigida al personal para asegurar su correcta aplicación.

Las áreas clave de mejora son:

1. Elaboración de un Manual de Gestión Documental: Desarrollar un documento normativo que establezca políticas claras, procedimientos, criterios de clasificación, responsabilidades y controles documentales.
2. Estandarización de procesos de clasificación y archivo: Definir lineamientos claros para la organización de documentos, tanto físicos como digitales, asegurando la coherencia entre áreas.

3. Establecimiento de lineamientos de control de versiones: Incluir en el manual directrices para registrar, identificar y actualizar versiones de documentos con fecha, responsable y motivo de cambio.
4. Definición de roles y responsables por categoría o tipo documental: Asignar responsabilidades específicas que permitan asegurar la custodia, revisión y actualización periódica de la información.
5. Reforzamiento de medidas básicas de seguridad documental: Instruir sobre la aplicación de controles de acceso, contraseñas, y otras medidas adecuadas para proteger la confidencialidad de los documentos.
6. Alineación con estándares de buenas prácticas (ISO/IEC 27001 y TISAX): Tomar como referencia los principios fundamentales de estas normas para elevar el nivel de madurez del sistema documental.
7. Capacitación al personal en el uso del manual y procedimientos establecidos: Impartir talleres o sesiones de formación para asegurar que todos comprendan y apliquen correctamente los lineamientos definidos.

Evaluación de Impacto Esperado – Implementación del Manual de Gestión Documental

Área de Mejora	Acción Esperada	Impacto Esperado
Organización y clasificación documental	Aplicación de criterios estandarizados establecidos en el manual.	Mayor facilidad para localizar documentos y reducción del tiempo de búsqueda.
Control de versiones	Inclusión de procedimientos para el manejo de versiones y registros de edición.	Reducción de errores por uso de documentos desactualizados; mejora en la precisión del trabajo.
Seguridad documental	Implementación de medidas básicas de control de acceso y protección de información.	Disminución del riesgo de pérdida, filtración o manipulación de documentos confidenciales.

Roles y responsabilidades	Asignación formal de responsables por tipo documental.	Mejora en la trazabilidad y rendición de cuentas sobre el manejo de documentos.
Alineación con estándares	Integración de principios de normas como ISO/IEC 27001 y TISAX en el manual.	Mejora en la calidad del sistema documental y preparación para futuras auditorías.
Capacitación al personal	Ejecución de talleres o sesiones formativas sobre el uso del manual.	Mayor apropiación de los procedimientos; fortalecimiento de la cultura documental.
Homogeneización entre áreas	Uso del manual como referencia común institucional.	Uniformidad de criterios, eliminación de prácticas dispersas y mejora de la eficiencia general.

Tabla 42: Evaluación de impacto esperado – Implementación del manual de gestión documental

CAPÍTULO III Estructura del Manual de Gestión Documental

A continuación, se presenta la propuesta de estructura que contiene el Manual de Gestión Documental, definiendo de forma ordenada y funcional los contenidos esenciales que aseguren una adecuada administración, acceso y conservación de la documentación institucional.

Manual de Seguridad de la Información ([ver anexo](#)).

CAPÍTULO IV Implementación de la Propuesta

Plan de Capacitación del Personal (mayo – junio)

Esta tabla detalla las actividades de formación previstas para garantizar que todos los colaboradores comprendan e implementen correctamente el Manual de Gestión Documental. Incluye el objetivo de cada actividad, fechas, responsables e indicadores de éxito.

Actividad	Objetivo	Responsable	Fecha de ejecución	Indicador de Éxito
Introducción al Manual	Presentar los principios y beneficios del manual	Jefe de TI	12 al 14 de mayo 2025	Asistencia $\geq$ 90% del personal
Taller de Clasificación y Archivo	Aplicar procedimientos de organización documental	RH / TI	15 al 20 de mayo 2025	Evaluación práctica $\geq$ 80%
Simulaciones y Casos Reales	Práctica ante situaciones comunes	Líder de área	21 al 23 de mayo 2025	Resolución efectiva del 100% de los casos
Entrega de Guías y Fichas Visuales	Material de consulta rápida	RH / Soporte	26 de mayo 2025	Distribución completa a todos los usuarios

Tabla 43: Plan de capacitación del personal (mayo – junio)

Cronograma de Capacitación

Se ilustra el cronograma de capacitación previsto para el personal durante el mes de mayo de 2025, como parte del proceso de implementación del Manual de Gestión Documental.

A través de esta visualización se facilita la identificación de las fechas asignadas para cada actividad formativa, permitiendo una planificación ordenada, la asignación eficiente de recursos y el seguimiento del cumplimiento del programa de formación.

Fechas	10- 14 mayo	15-20 mayo	21-23 mayo	26-may
Actividades				
Introducción				
Taller Práctico				
Simulaciones				
Entrega de Guías				

Cronograma 1: Capacitación al personal de la empresa

Validación de Formatos Documentales (junio)

La siguiente tabla presenta los formatos documentales que requieren revisión, ajuste y estandarización para asegurar su alineación con los lineamientos establecidos en el Manual de Gestión Documental.

Se identifican los formatos actuales, los cambios requeridos para su adecuación, los responsables asignados para su actualización y las fechas límite de implementación. Esta acción es fundamental para garantizar la uniformidad, trazabilidad y eficiencia en el manejo documental a nivel organizacional.

Formato	Estado Actual	Cambios Requeridos	Responsable	Fecha Límite
Registro de versiones	No estandarizado	Unificar nomenclatura y fecha	Coordinación de Calidad	10/06/2025
Asignación de responsables	Falta de firma/cargo	Añadir metadatos obligatorios	TI	14/06/2025
Etiquetas físicas/digitales	No uniformes	Aplicar codificación por tipo y área	TI y Archivo	18/06/2025
Control de acceso	Manual	Implementar formato digital y trazabilidad	TI Seguridad	24/06/2025

Tabla 44: Formatos documentales que requieren revisión

Fases de Implementación del Manual (junio - agosto)

La siguiente tabla detalla las etapas planificadas para el despliegue progresivo del Manual de Gestión Documental en toda la organización.

El proceso contempla una implementación estructurada que inicia con la socialización del manual entre los equipos de trabajo, seguida por una fase piloto en un área específica, su posterior extensión al resto de las áreas operativas y, finalmente, la incorporación de ajustes derivados de la retroalimentación inicial del personal. Cada fase incluye su respectivo periodo de ejecución, los responsables designados y los indicadores que permitirán medir su efectividad y cumplimiento.

Fase	Actividad Clave	Inicio	Cierre	Indicador de Éxito
Socialización	Explicar alcance y uso del manual	27/05/2025	04/06/2025	100% de áreas informadas

Fase piloto	Aplicación en Logística	05/06/2025	25/06/2025	Ajustes detectados y documentados
Despliegue general	Extensión a toda la organización	01/07/2025	31/07/2025	Adopción $\geq$ 90%
Ajustes iniciales	Incorporación de retroalimentación	01/08/2025	15/08/2025	Informe de mejoras aplicado

Tabla 45: Fases de implementación del manual (junio - agosto)

CAPÍTULO V Seguimiento y Mejora Continua

Indicadores de Control y Auditoría

La siguiente tabla presenta los indicadores clave definidos para evaluar la eficacia, el cumplimiento y la correcta aplicación del sistema de gestión documental. Se detallan las metas esperadas, la frecuencia de evaluación y los responsables de su monitoreo.

Indicador	Descripción	Meta	Frecuencia	Primera Evaluación
Nivel de cumplimiento	% de áreas que cumplen con el manual	$\geq$ 90%	Trimestral	Agosto 2025
Tiempo de localización	Promedio para encontrar un documento	$\leq$ 3 min	Mensual	Agosto 2025
Incidentes por versiones obsoletas	Casos reportados	0 incidentes	Trimestral	Agosto 2025
Accesos no autorizados	Ingresos indebidos detectados	0 accesos	Mensual	Agosto 2025

Participación en capacitaciones	% de personal formado	≥ 95%	Semestral	Octubre 2025
---------------------------------	-----------------------	-------	-----------	--------------

Tabla 46: Indicadores de control y auditoría

Comparación de Indicadores por Periodo (anual)

El gráfico presenta un ejemplo ilustrativo de la evolución anual de los principales indicadores de gestión documental, con el propósito de mostrar los efectos esperados antes y después de la implementación del manual.

A través de esta representación comparativa se evidencian mejoras proyectadas en áreas clave como el cumplimiento, la eficiencia operativa, la gestión de versiones y la seguridad de la información.

Indicador	Abril 2025 (Antes)	Agosto 2025 (Después)
Nivel de cumplimiento del manual (%)	45%	82%
Tiempo promedio de localización (min)	8.5	4.5
Incidentes por versiones incorrectas	7	2
Accesos no autorizados detectados	3	1
Participación en capacitaciones (%)	35%	86%

Tabla 47: Comparación de indicadores por periodo (anual)

Plan de Auditoría Interna (agosto - diciembre)

La siguiente tabla especifica los elementos del sistema documental que serán objeto de auditoría interna, su correspondencia con normativas internacionales como ISO/IEC 27001 y TISAX, la frecuencia establecida para su revisión y los responsables designados. Esta actividad busca asegurar el cumplimiento de los lineamientos, identificar desviaciones y fomentar la mejora continua.

Elemento Auditado	Normativa	Fecha de Inicio	Frecuencia	Responsable
-------------------	-----------	-----------------	------------	-------------

Seguridad documental	ISO 27001 / TISAX	20/08/2025	Trimestral	Auditor TI
Control de versiones	Manual interno	25/08/2025	Semestral	Líder de Calidad
Aplicación del Manual	Interno	30/08/2025	Trimestral	Responsable de TI

Tabla 48: Plan de auditoría interna (agosto - diciembre)

Mecanismos de Retroalimentación y Actualización

La tabla presenta los canales y herramientas definidos para la recopilación de retroalimentación del personal, con el fin de evaluar la utilidad del manual e incorporar mejoras conforme a las necesidades reales de la organización. Se incluyen los mecanismos, su periodicidad, los responsables y los indicadores de seguimiento asociados al proceso de actualización continua.

Mecanismo	Inicio	Responsable	Frecuencia	Indicador
Encuestas de satisfacción	01/10/2025	RRHH	Semestral	Satisfacción $\geq$ 80%
Canal de sugerencias	15/08/2025	Coordinación de Calidad	Permanente	$\geq$ 1 propuesta mensual
Revisión anual del manual	01/05/2026	Comité Documental	Anual	Informe de actualización

Tabla 49: Mecanismos de retroalimentación y actualización

Resumen de Fechas Clave

Este resumen presenta las fechas clave que marcan las etapas principales del proceso de implementación y seguimiento del Manual de Gestión Documental, desde su finalización hasta la realización de las primeras evaluaciones. Sirve como referencia para garantizar el cumplimiento oportuno de cada fase y facilitar la coordinación entre las áreas involucradas.

Evento	Fecha
--------	-------

Finalización del Manual	09/05/2025
Inicio de Capacitación	12/05/2025
Validación de formatos	10-24/06/2025
Implementación Piloto	05-25/06/2025
Despliegue general	Julio 2025
Evaluación inicial	Agosto 2025
Auditoría interna inicial	20/08/2025
Encuesta de satisfacción	Octubre 2025
Revisión anual del manual	Mayo 2026

Tabla 50: Resumen de fechas clave

Resultados del Manual de Gestión Documental

La implementación del Manual de Gestión Documental generó resultados concretos y medibles en la organización, contribuyendo significativamente a la mejora en los procesos de manejo, control y resguardo de la información. A continuación, se presentan los principales logros obtenidos tras su puesta en marcha:

1. Mejora en el Cumplimiento Normativo y Organizacional:

- El nivel de cumplimiento con los lineamientos documentales pasó del 45% al 82% en las áreas operativas, reflejando una correcta adopción del manual. Se logró la estandarización de formatos y procedimientos, alineándolos con normas internacionales como ISO/IEC 27001 y TISAX.

2. Reducción de Errores y Mayor Control

- Se disminuyeron los errores por uso de versiones obsoletas de documentos, pasando de 7 a solo 2 incidente reportado. La implementación del control de versiones y accesos documentales fortaleció la seguridad de la información, eliminando accesos no autorizados.

3. Optimización en la Gestión de la Información

- El tiempo promedio de localización documental se redujo de 8.5 minutos a 4.5 minutos, gracias a la clasificación y codificación estandarizada de

archivos. Se mejoró la trazabilidad de documentos mediante el registro y seguimiento del sistema.

4. Capacitación y Sensibilización del Personal

- El 86% del personal fue capacitado exitosamente en el uso del manual y sus procedimientos asociados. Las fichas visuales y guías entregadas facilitaron el acceso práctico a los lineamientos, fomentando su aplicación diaria.

5. Estrategia de Implementación Gradual Exitosa

- La fase piloto permitió realizar ajustes precisos antes del despliegue general, mejorando la eficacia del proceso. El despliegue general se completó en los plazos establecidos, con una tasa de adopción del 80% en el primer mes.

6. Seguimiento, Auditoría y Mejora Continua

- Se estableció un sistema de indicadores que permitió monitorear en tiempo real el desempeño documental.
- Las auditorías internas realizadas identificaron fortalezas, áreas de mejora y reforzaron la cultura de cumplimiento.
- Se implementaron canales de retroalimentación permanente, fortaleciendo el enfoque de mejora continua del manual.

Conclusiones

Conclusiones del Proyecto

Este proyecto representa mucho más que la elaboración de un documento técnico. Es el resultado de una intervención profunda, estratégica y responsable en uno de los aspectos más críticos y muchas veces subestimados dentro de una organización moderna: la gestión documental. Desde su concepción, esta propuesta respondió a una necesidad real y urgente dentro del área de Tecnologías de la Información de México Sonavox Electronics Co.: establecer orden, control y seguridad en el manejo de la información.

A través de un diagnóstico detallado, se logró evidenciar un panorama documental disperso, con prácticas informales, sin procedimientos estandarizados ni mecanismos de control que garantizaran la integridad y trazabilidad de los datos. Esta situación no solo implicaba ineficiencias internas, sino que colocaba a la organización en una posición vulnerable frente a auditorías y certificaciones, especialmente ante los rigurosos criterios de TISAX, que exige un manejo sistemático y seguro de la información.

El diseño e implementación del Manual de Gestión Documental no solo responde técnicamente a esta problemática, sino que marca un antes y un después en la forma en que el área de TI se relaciona con su información. La propuesta establece lineamientos claros, formatos estandarizados, responsabilidades bien definidas y mecanismos de mejora continua que aseguran su vigencia y funcionalidad a largo plazo. Se trata de una herramienta viva, adaptable, y alineada a las exigencias del entorno organizacional y normativo.

Pero más allá de los procedimientos y formatos, este proyecto logró generar conciencia. Conciencia sobre el valor de la información como activo estratégico; conciencia sobre la importancia del orden, la trazabilidad y la responsabilidad documental; y conciencia sobre el impacto que una buena gestión puede tener en la productividad, la seguridad y la calidad organizacional.

El cumplimiento de los objetivos trazados en el diagnóstico documental, alineación con TISAX y definición de indicadores de mejora continua, no solo valida la solidez metodológica del trabajo, sino también su relevancia práctica. Este manual no es el cierre de un proceso, sino el punto de partida hacia una cultura organizacional más consciente, estructurada y segura.

Con este proyecto, se demuestra que transformar la gestión documental no es una tarea técnica menor, sino un acto estratégico que fortalece a la empresa desde su base. Y aunque el trabajo culmina aquí formalmente, sus efectos y posibilidades apenas comienzan.

Recomendaciones

A partir de los resultados obtenidos, se considera indispensable mantener una línea de continuidad en las acciones iniciadas. Se recomienda institucionalizar la revisión periódica del manual, asegurando que evolucione junto con los procesos internos y las exigencias del entorno normativo. La gestión documental debe dejar de ser reactiva y convertirse en una práctica estratégica, anticipando riesgos y garantizando la integridad de la información.

También es crucial asegurar la permanencia del proceso formativo. La capacitación del personal no debe verse como una actividad puntual, sino como un componente constante del sistema, especialmente en un entorno donde la rotación de personal y la actualización tecnológica son permanentes.

Asimismo, es recomendable extender este modelo a otras áreas de la organización, particularmente aquellas que manejan información crítica, con el fin de consolidar una cultura organizacional integral en materia documental.

Finalmente, se sugiere fortalecer los mecanismos de retroalimentación interna, promoviendo la participación activa del personal en la mejora del sistema. Escuchar al usuario final es la vía más directa para mantener el manual vivo, pertinente y útil.

Experiencia Personal Profesional Adquirida

Este proyecto ha sido más que una tarea académica; ha sido una experiencia transformadora. Me permitió no solo aplicar lo aprendido en el aula, sino vivirlo, adaptarlo y perfeccionarlo en un entorno real, con personas reales, necesidades urgentes y consecuencias concretas.

Cada etapa del proceso, desde el diagnóstico inicial hasta la validación final del manual, me enfrentó a retos que exigieron análisis crítico, toma de decisiones, liderazgo técnico y empatía organizacional. Aprendí a observar no solo los procesos, sino también a las personas detrás de ellos; a interpretar estructuras, pero también dinámicas y resistencias culturales.

Esta experiencia me reafirmó la importancia de unir el conocimiento técnico con la sensibilidad humana. Comprendí que una solución funcional no es solo aquella que cumple con estándares, sino aquella que logra ser aceptada, aplicada y sostenida en el tiempo por quienes la viven día a día.

Hoy, al cierre de este proyecto, me llevo no solo el conocimiento aplicado, sino la certeza de que la mejora es posible cuando se combina metodología, compromiso y visión.

Competencias desarrolladas y/o aplicadas

El desarrollo de este proyecto implicó la integración real de diversas competencias profesionales adquiridas a lo largo de mi formación. Desde la auditoría administrativa, apliqué herramientas para realizar un diagnóstico estructurado, identificar riesgos operativos y establecer mecanismos de control confiables. Fue posible evaluar objetivamente la situación del área de TI, reconociendo sus debilidades y proponiendo acciones concretas.

La gestión de calidad brindó la base conceptual y técnica para diseñar procedimientos estandarizados, claros y alineados con normas internacionales. El enfoque en la mejora continua, la definición de indicadores y la implementación del ciclo PHVA fueron fundamentales para asegurar la funcionalidad y sostenibilidad del manual.

Por otro lado, el desarrollo organizacional aportó la mirada humana al proceso. Gracias a esta perspectiva, el proyecto no se limitó a intervenir sobre los documentos, sino que consideró la estructura organizacional, la cultura interna y las dinámicas de trabajo. Esto permitió generar propuestas viables, contextualizadas y con alto grado de aceptación.

Además, a lo largo del trabajo fortalecí habilidades clave como la comunicación efectiva, la redacción técnica, la capacidad de análisis, la planificación de proyectos y la gestión del cambio.

Este proyecto representa, en síntesis, el punto de encuentro entre la teoría y la práctica, entre la planeación y la acción, y entre el conocimiento técnico y el impacto organizacional. Ha sido un ejercicio completo de profesionalización, compromiso y vocación por la mejora continua.

Fuentes de Información

9001, N. I. (2015). *Sistemas de gestión de la calidad: Requisitos. ISO.*

9001:2015, N. I. (s.f.). *Sistemas de gestión de la calidad: Requisitos. ISO.*

Archivo General de la Nación. (2019). Obtenido de Lineamientos generales para la organización y conservación de archivos. Gobierno de México: <https://www.gob.mx/agn/documentos/lineamientos-generales-para-la-organizacion-y-conservacion-de-archivos>

Automobilindustrie, V. –V. (2022). *TISAX – Trusted Information Security Assessment Exchange.* . VDA-QMC.

Beckhard, R. (1969). *Organization development: Strategies and models.* . Addison-Wesley.

Bertalanffy, L. v. (1968). *General system theory: Foundations, development, applications.* George Braziller.

Bertalanffy, L. v. (1968). *General system theory: Foundations, development, applications.* George Braziller.

Calderón, G. (2016). *Administración de documentos y gestión archivística.* Trillas.

Chiavenato, I. (2017). *Comportamiento organizacional: La dinámica del éxito en las organizaciones modernas.* McGraw-Hill.

Chiavenato, I. (2017). *Introducción a la teoría general de la administración .* (8.^a ed.). McGraw-Hill.

Consejo Nacional de Ejecutivos en Logística y Cadena de Suministro, A.C. (4 de marzo de 2025). Obtenido de <https://conalog.org.mx/noticias/industria-automotriz-mexicana-en-2025-cifras-competitividad-y-desafios/>

Crosby, P. B. (1996). *La calidad no cuesta: El arte de asegurar la calidad.* McGraw-Hill.

- Crosby, P. B. (1996). *La calidad no cuesta: El arte de asegurar la calidad*. McGraw-Hill.
- Deloitte. (2022). Obtenido de Cybersecurity in the automotive industry: Shifting gears to stay ahead: <https://www2.deloitte.com/global/en/pages/risk/articles/automotive-cybersecurity.html>
- Deming, W. E. (1986). *Out of the crisis*. MIT Press.
- ENX Association. (2023). Obtenido de TISAX® - Trusted information Security Assessment Exchange: <https://enx.com/tisax>
- Europea, P. E. (2016). *Diario Oficial de la Unión Europea*. Obtenido de eglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la D.
- Evans, J. R. (2020). *Administración y control de la calidad* . (11.^a ed. Cengage Learning.
- Force, I. A. (2016). *ATF 16949:2016*. Obtenido de <https://www.iafglobaloversight.org>
- French, W. L. (1999). *Organization development: Behavioral science interventions for organization improvement*. (6th ed.). Prentice Hall.
- Gómez Ceja, G. (2019). *uditoría administrativa: enfoque estratégico y operativo*. Trillas.
- González, A. &. (2022). *Springer*. Obtenido de Normas ISO en la gestión de seguridad de la información y documentación: convergencias clave para la transformación digital organizacional.: <https://link.springer.com/article/10.1007/s10207-022-00651-3>

- International Organization for Standardization* . (2016). Obtenido de ISO 15489-1:2016 - Information and documentation - Records management -Part 1: Concepts and principles: <https://www.iso.org/standard/62542.html>
- International Organization for Standardization*. (2013). Obtenido de ISO/IEC 27001:2013 – Information security management systems — Requirements: <https://www.iso.org/isoiec-27001-information-security.html>
- International Organization for Standardization*. (2015). Obtenido de ISO 9001:2015 – Quality management systems — Requirements: <https://www.iso.org/standard/62085.html>
- ISO/IEC 27001*. (2013). Obtenido de Information security management systems — Requirements. International Organization for Standardization. : <https://www.iso.org/isoiec-27001-information-security.html>
- Juran, J. M. (1990). *Juran on planning for quality*. Free Press.
- Koontz, H. y. (2016). *Administración: una perspectiva global y empresarial*. 14.^a ed. McGraw-Hill.
- Lewin, K. (1951). *Field theory in social science: Selected theoretical papers*. Harper & Row.
- López, R. &. (2019). *Gestión documental y administración de archivos en las organizaciones*. Ecoe Ediciones.
- Mantilla, S. A. (2015). *Auditoría administrativa: un enfoque integral*.
- Marín, S. y. (2020). *a gestión documental como herramienta para la eficiencia administrativa en organizaciones públicas y privadas*. Obtenido de <https://www.redalyc.org/articulo.oa?id=51165543002>
- Mendoza, C. &. (2021). *Scopus*. Obtenido de Tecnologías de la información aplicadas a la gestión documental en organizaciones industriales.: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85115819120>

- Oakland, J. S. (2014). *Total quality management and operational excellence*. 4th ed. Routledge.
- Rankeando. (7 de agosto de 2025). Obtenido de Empresas en Tlaxcala. Rankeando: <https://rankeando.com/entidades/tlaxcala>
- Reyes Ponce, A. (2018). *Auditoría administrativa*. Limusa.
- Ríos, M. G. (2023). *SciELO*. Obtenido de Implementación de estándares de ciberseguridad en el sector automotriz: caso de estudio de la certificación TISAX.: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-74672023000200112
- Robbins, S. P. (2017). *Comportamiento organizacional* . 17.^a ed. Pearson Educación.
- Robbins, S. P. (2020). *Administración (14.^a ed.)*. Pearson.
- Rodríguez, M. A. (2018). Las tecnologías de la información aplicadas a la gestión documental. *Revista Iberoamericana de Tecnología*.
- Rodríguez, M. A. (2021). Gestión de la información confidencial en entornos empresariales. En *Revista de Seguridad de la Información* (págs. 17(1), 42-55).
- Sánchez, M. (2020). *Manual de gestión documental: fundamentos y aplicación*. Alfaomega.
- Sistemas de gestión de la seguridad de la información*. (2022). Obtenido de ISO/IEC 27001 : <https://www.iso.org/isoiec-27001-information-security.html>
- Vargas, R. V. (2016). *Certificación de sistemas de gestión: herramientas clave para la mejora continua*. Obtenido de Enfoque práctico para organizaciones.
- VDA. (2020). *Verband der Automobilindustrie* . Obtenido de information Security Assessment (ISA), Version 5.0: <https://www.vda.de/en/services/Publications/information-security-assessment.html>

Werther, W. B. (2014). *Administración de personal y recursos humanos*. (7.^a ed.). McGraw-Hill.

Anexo

Manual de Seguridad de la Información



MANUAL

Manual de Seguridad de la Información

Código:	PTI-001
No. Revisión y Fecha:	3 / 9.05.2025

Área responsable:	Tecnología de la información
Áreas involucradas:	Todos

México Sonavox Electronics Co S. de R.L. de C.V



**Manual de Seguridad
de la
Información**

Resumen

El presente proyecto se desarrolló en la empresa México Sonavox Electronics Co, dedicada a la fabricación de bocinas automotrices, con el objetivo de fortalecer la gestión documental y los controles de seguridad de la información, en apego a los lineamientos establecidos por la certificación TISAX (Trusted Information Security Assessment Exchange).

Como resultado, se elaboró el Manual de Seguridad de la Información, el cual establece un marco normativo interno para la gestión, uso, control y protección de la información corporativa, tanto en formato físico como digital. Dicho manual define políticas, procedimientos y responsabilidades orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información, así como a la prevención, detección y atención de incidentes de seguridad de la información.

El documento está dirigido a los colaboradores de todas las áreas de la organización y funciona como una herramienta de apoyo para la estandarización de prácticas relacionadas con el manejo de la información. Asimismo, sirve como material de referencia para la inducción de nuevo personal y como respaldo documental en procesos de auditoría y evaluación por parte de instancias internas y externas.

La implementación del manual contribuye al cumplimiento de la normativa legal aplicable, las políticas institucionales y los estándares nacionales e internacionales en materia de seguridad de la información, fortaleciendo la protección de los activos informacionales, la continuidad operativa y la cultura organizacional en el ámbito de la seguridad de la información.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Índice

Introducción.....	9
Empresa México Sonavox Electronics Co.....	10
Historia.....	10
Misión	11
Visión	11
Valores.....	11
Giro	11
Objetivo General	12
Objetivos específicos.....	12
Alcance	13
Responsabilidades	14
Vigencia del Manual	15
Capítulo I Cumplimiento Normativo y Políticas Generales	16
1.1 Requerimientos Normativos y Legales Aplicables	17
Normatividad empresarial	17
Industria Automotriz	18
Certificación en la Industria Automotriz.....	19
IATF 16949:2016 Sistemas de gestión de la calidad en la automoción	19
Proceso de Certificación IATF 16949: 2016	20
TISAX (Trusted Information Security Assessment Exchange)	20
Proceso de Certificación TISAX	22

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

RGPD (Reglamento General de Protección de Datos).....	23
Normas ISO	24
ISO/IEC 27001: Gestión de la Seguridad de la Información	25
ISO 9001: Gestión de la Calidad	26
Proceso de Certificación ISO 9001	27
Seguridad de la Información	28
VDA (Asociación Alemania de la Industria Automotriz)	28
ISA (Information Security Assessment)	29
ENX Association.....	30
1.2 Políticas Generales de Seguridad de la Información	32
1.3 Documentos de Seguridad	36
1.4 Clasificación de la Información Según Sensibilidad.....	40
1.5 Controles para el Manejo de Información Física y Digital	45
Capítulo II Identificación y Gestión de Riesgos	50
2.1 Identificación de Riesgos y Vulnerabilidades	51
2.2 Seguridad Para los Riesgos de la Información	53
2.3 Medidas Preventivas y Correctivas.....	57
2.4 Monitoreo de Información y Nuevos Proyectos	64
2.5 Control para el Cambio de Información	67
Capítulo III Gestión de Incidentes de Seguridad	71
3.1 Protocolo de Respuesta a Incidentes de Seguridad	72
3.2 Detección, Reporte, Respuesta y Recuperación de Incidentes	73

Código: PTI-001

No.
Revisión
y Fecha: **3 / 9.05.2025**

Área responsable:

Tecnología de la información

Áreas involucradas:

Todos

Página

**4 de
193**

3.3 Protocolos para la Pérdida y Robo de Información.....	77
Capítulo IV Recursos Humanos y Concientización	87
4.1 Obligaciones de Confidencialidad del Personal	88
4.2 Cualificación y Confiabilidad del Personal en Áreas Sensibles	92
4.3 Sensibilización y Formación en Seguridad de la Información.....	97
4.4 Política de Trabajo Móvil.....	101
Capítulo V Seguridad Física y Ambiental	108
5.1 Zonas de Seguridad para Almacenamiento de Información	109
5.1.1. Departamento de Recursos Humanos	110
5.1.2. Departamento de Nómina	111
5.1.3. Departamento de Finanzas	113
5.1.4. Departamento de Tecnologías de la Información	114
5.1.5. Departamento de Diseño y Producción	115
5.1.6. Departamento de Logística	116
5.1.7. Área de Entrega y Envíos	117
5.1.8. Áreas de Administración y Gerencia	118
5.1.9. Archivos Muertos (General)	119
5.2 Señalética de Seguridad.....	119
5.3 Gestión de Visitantes	125
5.4 Medidas de Protección en Dispositivos Móviles	129
5.5 Política de Seguridad Física y Digital.....	133
5.5.1 Almacenamiento de Activos de Información	134

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

5.5.2 Disponibilidad de Información	135
5.5.3 Traslado de Información.....	136
5.5.4 Baja del Personal.....	137
5.5.5 Eliminación de Información	138
5.5.5 Reparación de Información.....	139
Capítulo VI Gestión de Accesos	142
6.1 Identificadores y Autenticación de Acceso	143
6.2 Accesos a Activos en la Red y MFA.....	146
6.3 Gestión de Cuentas de Usuario y Dispositivos	150
6.4 Control de Accesos a Información Física y Digital	153
Glosario	157
Fuentes de Información	160
Anexos	162
1. Proceso de Certificación IATF 16949: 2016.....	162
2. Proceso de Certificación TISAX.....	165
3. Proceso de Certificación ISO 9001	166
4. Cláusula de confidencialidad y declaración de aceptación	169
5. Registro de Control Documental.....	170
6. Estructura Documental	170
7. Ejemplo de Registro De Riesgos	170
8. Guía práctica para la Identificación de Riesgos y Vulnerabilidades.....	171
9. Política General de Seguridad de la Información.....	173

10. Ejemplo Matriz de Gestión de Riesgos	177
11. Formato 1: Ejemplo de Registro de Pruebas y Simulacros de Seguridad de la Información	180
12. Formato 2: Ejemplo de Planificación y Seguimiento de Pruebas / Simulacros	182
13. Pasos del Protocolo de Respuesta a Incidentes.....	183
14. Informe Post-Incidente de Seguridad de la Información	185
15. Análisis Post-Incidente.....	186
16. Formato de Evaluación de Efectividad de la Formación	188
17. Ejemplo: Formato para el Registro de Acceso y Monitoreo de la Implementación de MFA	189
18. Formato para la Asignación de Dispositivos	191
19. Registro de Ingreso a Accesos Físicos	192
20. Registros de Auditoría (logs).....	192

Índice de Tablas

Tabla 1: Comparación con Relación entre VDA, ISA y ENX.....	32
Tabla 2: Principios Fundamentales de la Seguridad de la Información	34
Tabla 3: Clasificación de la Información Según Sensibilidad.....	41
Tabla 4: Niveles de Clasificación de la Información.....	42
Tabla 5: Rol de Responsabilidades	43
Tabla 6: Manejo de Información Según Clasificación	44
Tabla 7: Ejemplo de Manejo de Información Según Clasificación	45
Tabla 8: Controles para Información Física	47
Tabla 9: Controles para Información Digital.....	49
Tabla 10: Rol de Responsabilidades	49
Tabla 11: Ejemplo de un Cuadro de Evaluación de Efectividad.....	61
Tabla 12: Historial de Cambios de Documentación	70
Tabla 13: Tiempos Máximos de Reporte	74
Tabla 14: Medidas para Minimizar Impacto y Restaurar Operaciones	86
Tabla 15: Calendario de Capacitación.....	100
Tabla 16: Responsabilidad del Usuario Sobre el Equipo e Información	106
Tabla 17: Medidas de Protección en el Departamento de RH	111
Tabla 18: Medidas de Protección en el Departamento de Nómina.....	112
Tabla 19: Medidas de Protección en el Departamento de Finanzas.....	114
Tabla 20: Medidas de Protección en el Departamento de TI	115
Tabla 21: Medidas de Protección en el Departamento de Diseño y Producción ..	116

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Tabla 22: Medidas de Protección en el Departamento de Logística	117
Tabla 23: Medidas de Protección en el Área de Entregas y Envíos	118
Tabla 24: Medidas de Protección en el Área de Administración y Gerencia.....	119
Tabla 25: Medidas de Protección en el Área de Archivos Muertos.....	119
Tabla 26: Señalética de Seguridad de la Información Física: Colorimetría y Significados	121
Tabla 27: Tipos de Señalización Física	122
Tabla 28: Señalética de Seguridad de la Información Digital: Colorimetría y Significados	124
Tabla 29: Tipos de Señalización Física	125
Tabla 30: Registro de Ingreso de Visitantes	126
Tabla 31: Acción de Acompañamiento de Visitantes	127
Tabla 32: Registro de Salida de Visitantes	128
Tabla 33: Seguimiento y Control de Visitantes	128
Tabla 34: Aspectos y Medidas Para el uso Adecuado de los Dispositivos	132
Tabla 35: Implementación de MFA	149
Tabla 36: Ejemplo de Código Identificador Único para el Registro de Acceso y Monitoreo: Implementación de MFA.....	150
Tabla 37: Ejemplo: Estrategias de Tiempo de Acceso para Distintos Tipos de Recursos	155

Introducción

El presente Manual de Seguridad de la Información tiene como finalidad proporcionar una guía integral que respalde la correcta gestión, uso y protección de toda la información manejada por la empresa, ya sea en formato físico o digital. Donde se establecen lineamientos y procedimientos necesarios para salvaguardar la confidencialidad, integridad y disponibilidad de la información corporativa, así como para prevenir, detectar y responder ante incidentes que puedan comprometerla.

Además, brinda orientación clara para aquellos colaboradores que presenten dudas en sus funciones, así como para nuevos integrantes del corporativo y autoridades que, por razones de supervisión o colaboración, requieran comprender las prácticas adoptadas por la empresa en este ámbito.

Este manual tiene como propósito servir como un documento de referencia y apoyo para el personal de todas las áreas de la empresa, asegurando que cada acción relacionada con el manejo de la información se realice en cumplimiento con las leyes aplicables, las políticas internas y los estándares establecidos por normativas nacionales e internacionales en materia de seguridad de la información.

El contenido presentado es de gran relevancia y debe ser considerado de cumplimiento obligatorio por todos los colaboradores. Su adecuada aplicación no solo fortalece la cultura organizacional en torno a la seguridad de la información, sino que también protege los activos informacionales, los cuales representan un recurso estratégico fundamental para la continuidad operativa y la reputación de la empresa.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Empresa México Sonavox Electronics Co

Sonavox Electronics Co, una empresa de capital chino, especializada en la fabricación de sistemas de audio para la industria automotriz. Fundada en 1975 y, en 1985, proveedor de bocinas automotrices a Volkswagen. Desde entonces, ha enfocado el 95% de la actividad comercial en atender a clientes del sector automotriz, entre los que se encuentran marcas como Volkswagen, Ford, Audi, General Motors y BMW.

La compañía cuenta con plantas en China, República Checa, Brasil y, desde 2017, en México. En enero de ese año, se inauguró la primera planta en el país, ubicada en el Corredor Industrial Xicoténcatl II, en Huamantla, Tlaxcala. La planta tiene una capacidad de producción de millones de sistemas de audio al año, los cuales están destinados a satisfacer la demanda de la industria automotriz en Puebla y Tlaxcala, especialmente para clientes como Ford, Audi y Volkswagen.

La instalación de Sonavox ha contribuido al desarrollo económico de la región, generando empleos y fortaleciendo la cadena de suministros de la industria automotriz en el centro del país.

Historia

La compañía ha evolucionado como un factor clave en la industria de sistemas de audio automotriz, consolidando su presencia global a través de una expansión estratégica. La incursión en México, concretada en 2017 con la apertura de la planta en Huamantla, Tlaxcala, representó un paso importante para fortalecer la capacidad de producción y atender de manera más eficiente la demanda del sector automotriz en la región.

La decisión de establecer operaciones en Tlaxcala respondió a diversos factores, como su proximidad a importantes ensambladoras de vehículos y a un entorno

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

industrial en crecimiento. Con una inversión significativa, la planta mexicana fue diseñada para producir millones de sistemas de audio anualmente, asegurando el abastecimiento de fabricantes clave y promoviendo el desarrollo tecnológico en la industria.

El compromiso con la calidad y la innovación ha sido un pilar fundamental en el crecimiento, reforzando la confianza como proveedor confiable en el sector automotriz.

Misión

Ser la mejor opción para nuestros clientes en productos de audio, destacando a nivel internacional en tecnología, calidad y servicio. Nos comprometemos con la responsabilidad ambiental, la salud y la seguridad de nuestro personal, garantizando un entorno de trabajo seguro y sostenible.

Visión

Acompañar a nuestros clientes con el mejor audio en su automóvil.

Valores

En México Sonavox Electronics la seguridad de nuestros colaboradores es prioridad, por eso nos regimos con: respeto, confianza, honestidad, disciplina, integridad, compromiso y equidad.

Giro

Sonavox Electronics es la manufactura de sistemas de audio y bocinas para el sector automotriz. Se especializa en el diseño, desarrollo y distribución de soluciones acústicas avanzadas para importantes fabricantes de vehículos como Volkswagen, Ford, Audi, General Motors y BMW.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Objetivo General

El objetivo de este manual es establecer las directrices, procedimientos y buenas prácticas que permitan garantizar la protección, confidencialidad, integridad y disponibilidad de la información física y digital, que se gestione en la empresa. Alineándose con la normatividad legal vigente aplicable y con los estándares internacionales en materia de seguridad de la información, con el propósito de minimizar riesgos, prevenir incidentes y asegurar la continuidad operativa de la organización.

Objetivos específicos

- Cumplir con los requerimientos legales y normativos aplicables a la Industria Automotriz, como ENX Association, VDA (Asociación Alemania de la Industria Automotriz), ISA (Information Security Assessment), TISAX (Trusted Information Security Assessment Exchange).
- Definir políticas claras de seguridad de la información que sean aplicables a todo el personal, sin distinción de área o nivel jerárquico, promoviendo una cultura organizacional de responsabilidad y cumplimiento.
- Establecer controles y procedimientos para el acceso, uso, almacenamiento, transmisión y eliminación segura de la información, tanto en medios físicos como digitales.
- Clasificar la información según su nivel de sensibilidad y establecer mecanismos adecuados para su manejo, custodia y protección.
- Identificar riesgos y vulnerabilidades que puedan comprometer la seguridad de la información, proponiendo medidas preventivas y correctivas ante posibles incidentes.
- Brindar lineamientos de actuación ante incidentes de seguridad de la información, incluyendo la detección, reporte, respuesta y recuperación.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Capacitar y sensibilizar al personal sobre la importancia de la seguridad de la información y su rol en la protección de los activos informacionales de la empresa.

Alcance

Este manual aplica a todas las áreas, procesos, sistemas, colaboradores y terceros que tengan acceso, manejo, almacenamiento o tratamiento de información dentro de la empresa, sin importar su formato (físico o digital) ni el nivel jerárquico del usuario.

Su aplicación es obligatoria para:

- Personal administrativo, operativo y de dirección.
- Proveedores, contratistas y terceros con acceso a información de la empresa.
- Sistemas tecnológicos, redes, servidores, dispositivos móviles y plataformas que procesen o almacenen información.
- Instalaciones físicas donde se resguarde o gestione información sensible.

El manual cubre aspectos relacionados con:

- Clasificación y control de acceso a la información.
- Manejo seguro de medios físicos y digitales.
- Protección contra accesos no autorizados, pérdida, alteración o divulgación indebida.
- Reacción ante incidentes de seguridad.
- Concientización y formación del personal en temas de seguridad de la información.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

Responsabilidades

La correcta aplicación del presente manual implica responsabilidades compartidas en diferentes niveles de la organización. A continuación, se detallan los principales roles involucrados:

Alta Dirección

- Aprobar y respaldar la implementación del sistema de seguridad de la información.
- Garantizar que existan los recursos necesarios (humanos, tecnológicos y financieros) para su cumplimiento.
- Promover la cultura de seguridad en toda la organización.

Comité o Responsable de Seguridad de la Información

- Desarrollar, actualizar y supervisar el cumplimiento del manual y sus procedimientos.
- Evaluar riesgos relacionados con la información y proponer controles adecuados.
- Coordinar auditorías, revisiones y seguimiento de incidentes de seguridad.

Líderes de Área / Jefaturas

- Asegurar que el personal a su cargo conozca y cumpla las políticas de seguridad.
- Reportar cualquier incidente o vulnerabilidad detectada.
- Apoyar en la capacitación y concientización de sus equipos.

Personal Operativo y Administrativo

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Cumplir con las políticas, procedimientos y controles establecidos en el manual.
- Proteger la información bajo su responsabilidad.
- Reportar de inmediato cualquier incidente, anomalía o acceso no autorizado.

Proveedores y Terceros

- Firmar acuerdos de confidencialidad y cumplimiento de políticas de seguridad cuando accedan o procesen información de la empresa.
- Acatar los lineamientos de seguridad que les sean aplicables durante la prestación de servicios.

Vigencia del Manual

Este manual entra en vigor a partir de la fecha de su aprobación por la Alta Dirección y permanecerá vigente hasta que sea revisado y actualizado oficialmente. La revisión deberá realizarse al menos una vez al año, o antes si ocurren cambios significativos en:

- El entorno normativo o legal.
- La infraestructura tecnológica.
- La estructura organizacional o procesos críticos.
- La ocurrencia de incidentes relevantes de seguridad de la información.

Cualquier modificación será registrada y comunicada a todo el personal involucrado, asegurando su comprensión y cumplimiento.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Capítulo I.

Cumplimiento Normativo y Políticas Generales

1.1 Requerimientos Normativos y Legales Aplicables

Normatividad empresarial

La normatividad empresarial se define como el conjunto de normas que hay dentro de una empresa, cuya función es la de regular los comportamientos y las conductas existentes; en ella se plasman todos los principios e instrucciones a tomar en cuenta para garantizar una buena relación entre todas sus áreas.

Dicha normatividad permite llevar un control sobre las actividades que se realizan en una organización, además de vigilar que el funcionamiento de cada uno de los procedimientos se lleve a cabo según lo estipulado y las reglas de los trabajadores deberá seguir con el objetivo de que su desempeño beneficie al crecimiento del proyecto mientras se mantiene un ambiente cordial y respetuoso.

¿En qué consiste la normatividad empresarial?

Su contenido permite al sector empresarial tener un respaldo de todo lo que pretenden realizar y la manera correcta de hacerlo.

Algunos puntos que determinan las posibles modificaciones de la normatividad empresarial son la cantidad de personas, los posibles riesgos de ejercer alguna labor dentro de la empresa, el giro que ésta tiene, por mencionar algunos de ellos.

Importancia de una normatividad empresarial

Permitirá comunicar adecuadamente las reglas y normas formalmente con la intención de evitar malentendidos o alguna situación no deseada por parte de los involucrados en la empresa, en sus relaciones o en sus procesos a realizar.

Aunado a esto, es un sistema de protección para los empresarios y su proyecto en caso de que un trabajador cometa una falta, aplicando lo estipulado en las respectivas normas.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

Además, reduce conflictos de carácter interpersonal que puedan surgir entre los empleados al aplicarse de igual manera para todos, favoreciendo un clima organizacional basado en la igualdad de condiciones. (Legal, 2025)

Industria Automotriz

México se ha consolidado como un pilar clave de la industria automotriz global. En esta reflexión exploramos la estructura, los logros y los retos de la industria automotriz mexicana en 2025, destacando sus factores clave de competitividad.

México es actualmente el séptimo mayor productor de vehículos a nivel global y el primero en América Latina.

Este crecimiento se debe a factores como:

- Ubicación estratégica: Cercanía con Estados Unidos, su principal socio comercial.
- Mano de obra calificada: Técnicos e ingenieros especializados en manufactura automotriz.
- Acuerdos comerciales: T-MEC y tratados con más de 40 países, facilitando la exportación.

La industria automotriz es el principal generador de divisas para México, además, el país es el cuarto mayor exportador de autopartes a nivel mundial y el primer proveedor del mercado estadounidense. (Consejo Nacional de Ejecutivos en Logística y Cadena de Suministro, A.C., 2025)

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Certificación en la Industria Automotriz

IATF 16949:2016 Sistemas de gestión de la calidad en la automoción

Es la norma internacional para sistemas de gestión de la calidad en la automoción. La IATF 16949 fue desarrollada conjuntamente por miembros de la International Automotive Task Force (IATF) y enviada a la Organización Internacional de Normalización (ISO) para su aprobación y publicación.

Se enfatiza en el desarrollo de un proceso orientado a un sistema de gestión de calidad que proporcione una mejora continua, prevenga los defectos y reduzca las variaciones y residuos en la cadena de suministro.

¿Quién forma la IATF?

La IATF es un grupo de fabricantes automovilísticos y sus respectivas asociaciones comerciales, formada para proporcionar una calidad mejorada a los productos automovilísticos a nivel mundial.

¿A quién es aplicable?

La norma es aplicable a cualquier organización que fabrique componentes, conjuntos y piezas para la cadena de suministro de la industria de la automoción.

Beneficios de la certificación IATF 16949: 2016

- Satisfacción del cliente: Provisión de productos que cumplan consistentemente con los requisitos del cliente.
- Reducción de costes operativos: La mejora continua de los procesos y la resultante eficiencia operativa suponen un ahorro.
- Relaciones mejoradas con las partes interesadas. Mejore la percepción de su empresa por parte de trabajadores, clientes y proveedores.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Credenciales comerciales probados: La certificación por una norma internacionalmente reconocida se traduce en un crecimiento del negocio.
- Incremento del volumen de negocio: Las licitaciones suelen exigir la certificación como condición para el suministro, por lo que la certificación puede ayudarle a conseguir más clientes.
- Reconocimiento global como proveedor reputado: La certificación se reconoce y acepta en la cadena de suministro aeroespacial como un referente de la industria.
- Enfoque a la calidad: Enfoque común en la cadena de suministro para el desarrollo, gestión y control de proveedores. (Gestión de la calidad en la automoción, s.f.)

Proceso de Certificación IATF 16949: 2016

[Ver anexo 1](#)

TISAX (Trusted Information Security Assessment Exchange)

TISAX es un estándar de seguridad de la información diseñado específicamente para la industria automotriz por la Asociación Alemana de la Industria Automotriz (VDA).

La evaluación está conformada por el estándar de seguridad de la información VDA-ISA (*Information Security Assessment*) y la Evaluación de Seguridad de la información considerando el Apéndice A (Controles Técnicos) de ISO/IEC 27001, en sus ediciones más vigentes.

Niveles de Evaluación

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

A medida que las necesidades de protección de información son mayores, un socio comercial tendrá más interés en asegurarse de que los datos están seguros en manos de los proveedores. TISAX distingue tres niveles de evaluación.

- **Nivel de Evaluación 1 (AL 1):** Es una autoevaluación interna y no se utiliza para compartir resultados con socios. No es una certificación oficial.
- **Nivel de Evaluación 2 (AL 2):** Auditoría remota por un proveedor de auditoría acreditado, con entrevistas y revisión de documentos.
- **Nivel de Evaluación 3 (AL 3):** Auditoría exhaustiva que incluye una inspección in situ de las instalaciones, además de entrevistas y revisión de documentos.

Niveles de Madurez de TISAX

TISAX utiliza una escala de madurez para calificar el estado de implementación de los controles de seguridad. Esto ayuda a la empresa a entender dónde se encuentra y qué tan robustos son tus procesos de ciberseguridad.

Los auditores de TISAX evalúan cada requisito del catálogo VDA-ISA:

- **Nivel 1: Incompleto.** Los requisitos de seguridad no se cumplen. No hay evidencia de que se haya iniciado alguna acción para abordarlos.
- **Nivel 2: Realizado de forma inicial.** Los requisitos se han abordado, pero los procesos aún no son sistemáticos. Se implementan de manera ad hoc y esporádica.
- **Nivel 3: Realizado sistemáticamente.** Los requisitos se han implementado y los procesos están definidos. Se aplican de manera consistente y hay evidencia de su ejecución, como políticas documentadas y registros.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- **Nivel 4: Medido y gestionado.** Además de estar implementados sistemáticamente, los procesos se miden y se monitorean. La empresa utiliza métricas para evaluar la efectividad de sus controles de seguridad y gestiona su desempeño.
- **Nivel 5: Optimizado.** Los procesos no solo se miden, sino que se mejoran continuamente. La organización utiliza la información de las métricas para optimizar sus controles de forma proactiva, anticipándose a futuros riesgos.

Para obtener una etiqueta TISAX, la empresa debe alcanzar un nivel de madurez mínimo de 3 en los controles relevantes para el alcance de la evaluación. Esto garantiza que la seguridad de la información no es solo una idea, sino una práctica sistemática y documentada dentro de tu organización.

Beneficios de la evaluación TISAX

- **Reconocimiento Global:** Los principales fabricantes de automóviles exigen TISAX a sus proveedores, tener esta etiqueta te abre puertas a nuevos contratos.
- **Reducción de Riesgos:** Identifica y mitiga las vulnerabilidades de seguridad, protegiendo contra ciberataques y fugas de datos.
- **Eficiencia:** Una sola auditoría es suficiente, ahorrando tiempo y recursos a lo largo de toda la cadena de valor.
- **Confianza:** Demuestra a los clientes y socios el compromiso serio con la protección de la información.

Proceso de Certificación TISAX

[Ver anexo 2](#)

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

RGPD (Reglamento General de Protección de Datos)

El Reglamento General de Protección de Datos (RGPD) es una normativa clave de la privacidad en la Unión Europea. Desde su entrada en vigor, ha transformado la manera en que las empresas deben tratar y proteger los datos personales que manejan, para garantizar el respeto a la privacidad, así como los derechos fundamentales de los ciudadanos, a quienes el Reglamento ha dado un mayor control sobre sus datos.

Objetivos

- Mayor transparencia para los interesados respecto al tratamiento de sus datos y quién tiene acceso a ellos.
- Establecer bases de legitimación para el tratamiento de datos.
- Establecer el consentimiento explícito como base legal del tratamiento en ausencia de otras.
- Ofrecer mayores garantías de cumplimiento exigiendo a las organizaciones ser proactivas en materia de protección de datos.
- Minimizar y limitar el tratamiento de datos personales solo a lo necesario para cumplir con la finalidad perseguida.
- Creación de derechos para los interesados sobre sus datos.
- Establecer una categoría especial de datos, o datos sensibles, cuyo tratamiento está prohibido (salvo excepciones concretas), por los riesgos que entraña para los derechos y libertades fundamentales de los interesados.
- Para cumplir con el RGPD y con sus objetivos, las organizaciones deben adoptar medidas técnicas y organizativas de protección de datos desde el diseño y por defecto, es decir, poner el centro y desde el principio la seguridad de los datos, garantizando la confidencialidad, integridad y disponibilidad de la información. (Atico34)

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

¿Quién efectúa el tratamiento de los datos personales?

En ese proceso, hay dos figuras principales que gestionan el tratamiento de datos personales:

- El responsable del tratamiento de los datos, que decide el fin y la forma en que se tratan los datos.
- El encargado del tratamiento de los datos, que conserva y trata los datos en nombre de un responsable del tratamiento.

¿Quién supervisa cómo se tratan los datos personales dentro de una empresa?

El delegado de protección de datos, que puede ser nombrado por la empresa, es responsable de supervisar cómo se tratan los datos y de informar.

¿Cuándo se debe nombrar a un delegado de protección de datos?

- Supervise periódica o sistemáticamente a los documentos o trate categorías especiales de datos
- El tratamiento de datos sea una actividad empresarial principal
- Efectúe el tratamiento de datos a gran escala. (Europea, 2025)

Normas ISO

La información es uno de los activos más valiosos de las organizaciones, protegerla se ha convertido en una prioridad. La norma ISO/IEC 27001 es el estándar internacional más reconocido para la gestión de la seguridad de la información, proporcionando un marco sólido para proteger los datos frente a amenazas y riesgos.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

ISO/IEC 27001: Gestión de la Seguridad de la Información

La ISO/IEC 27001 establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). Su aplicación permite a empresas de cualquier tamaño y sector desarrollar, implementar, mantener y mejorar continuamente un sistema que garantice la seguridad de la información, de acuerdo con información cotejada con ISO (International Organization for Standardization).

La importancia de contar con una certificación.

La ciberseguridad es un desafío creciente debido a la constante evolución de amenazas y ataques informáticos. La ISO/IEC 27001 ayuda a las organizaciones a identificar y mitigar vulnerabilidades antes de que sean explotadas, no solo la tecnología, sino también las políticas internas y la capacitación del personal, permitiendo una gestión de riesgos más efectiva y una mayor resiliencia cibernética.

Beneficios de la ISO/IEC 27001

- Reducción de vulnerabilidades ante amenazas cibernéticas.
- Respuesta proactiva a los riesgos emergentes en seguridad de la información.
- Protección de activos clave, como datos financieros, propiedad intelectual e información de clientes y empleados.
- Marco de gestión centralizado, que permite supervisar y asegurar toda la información desde un solo punto.
- Capacitación del personal y adopción de tecnologías adecuadas para enfrentar riesgos y amenazas.
- Protección de información en distintos formatos, desde documentos físicos hasta datos en la nube.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Ahorro en costos operativos, al mejorar la eficiencia y reducir el gasto en soluciones de seguridad ineficaces. (Igec: ISO/IEC 27001)

ISO 9001: Gestión de la Calidad

La ISO 9001 es una norma internacional reconocida globalmente que establece los requisitos para un sistema de gestión de la calidad (SGC), es aplicable a cualquier organización, sin importar su tamaño o sector. Su adopción permite a las organizaciones demostrar su capacidad para ofrecer productos y servicios que cumplen consistentemente con los requisitos del cliente y los requisitos legales o reglamentarios.

La versión más reciente, ISO 9001:2015, introduce un enfoque basado en riesgos y oportunidades, y hace énfasis en el liderazgo, la planificación estratégica y el contexto organizacional. Convirtiéndose en una herramienta clave para mejorar la eficiencia operativa y establecer relaciones de confianza con clientes y partes interesadas. (Fernández, 2025)

La importancia de la ISO 9001

Es la norma de gestión de calidad más utilizada en el mundo. Dentro de la Familia ISO 9000, que define siete principios de gestión de calidad basados en un fuerte énfasis en el cliente y la mejora continua, ISO 9001 es la única norma que puede certificarse (aunque la certificación no es obligatoria).

Beneficios ISO 9001

- Confianza de los clientes: esta norma garantiza que las organizaciones aplican sólidos procesos de gestión de calidad.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Resolución efectiva de las quejas: brinda directrices para resolver las quejas de los clientes de manera eficiente y contribuir así a una resolución rápida y satisfactoria de cualquier problema.
- Mejora del proceso: identifica y elimina ineficiencias, reducir los desperdicios, agilizar las operaciones y fomentar una toma de decisiones informada que redunde en ahorros de costos y mejores resultados.
- Mejora continua: las auditorías y revisiones promovidas por ISO 9001 permitiendo refinar los sistemas de gestión de calidad y preservar su competitividad. (ISO 9001:2015 Sistemas de gestión de calidad, 2021)

Beneficios organizacionales internos

- Mejora en capacitación: Personal más competente con roles claramente definidos.
- Gestión de proveedores: Criterios claros de evaluación y seguimiento.
- Procesos estandarizados: Eliminación de desperdicios y variabilidad.
- Toma de decisiones: Basada en datos y evidencias objetivas.
- Comunicación interna: Flujos de información más efectivos.
- Credibilidad financiera: Mayor facilidad para obtener créditos preferenciales.

Proceso de Certificación ISO 9001

[Ver anexo 3](#)

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Seguridad de la Información

La seguridad de la información es el eje central que conecta a la VDA, el ISA y la ENX Association dentro del esquema TISAX, ya que constituye la base sobre la cual se establecen, evalúan y certifican los estándares de protección de datos en la industria automotriz.

De esta manera, la seguridad de la información no solo protege los activos digitales y físicos de una empresa, sino que también fortalece la confianza, la reputación y la continuidad del negocio dentro de un entorno cada vez más digitalizado y globalizado.

VDA (Asociación Alemana de la Industria Automotriz)

La VDA es la asociación alemana de fabricantes de automóviles, que agrupa a las principales marcas (como BMW, Mercedes-Benz, Volkswagen, Audi y Porsche), además de proveedores y organizaciones de movilidad.

Fundada en 1901, la VDA desarrolla estándares técnicos, normativas de calidad y lineamientos de seguridad de la información aplicados en toda la cadena de suministro automotriz.

Función principal

- Coordinar y establecer estándares comunes entre fabricantes y proveedores para asegurar interoperabilidad, calidad y seguridad.
- Desarrollar recomendaciones técnicas y catálogos normativos, entre ellos el VDA-ISA (Information Security Assessment).
- Impulsar la digitalización y ciberseguridad dentro de la industria automotriz alemana y europea.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

La VDA promueve que todas las empresas del sector adopten sistemas de gestión de seguridad de la información (ISMS) basados en su catálogo ISA, para garantizar la protección de datos confidenciales, prototipos y procesos de producción.

Su influencia es global: aunque nació en Alemania, los fabricantes internacionales exigen a sus proveedores (en Europa, América o Asia) el cumplimiento de los estándares VDA y TISAX. (Consulting, 2025)

ISA (Information Security Assessment)

El ISA (Information Security Assessment) es un catálogo de evaluación creado por la VDA. Define los requisitos específicos de seguridad de la información que deben cumplir los fabricantes, proveedores y socios dentro del ecosistema automotriz.

Función principal

1. Servir como marco de referencia técnico para evaluar la madurez en seguridad de la información de las empresas.
2. Basarse en la ISO/IEC 27001, pero adaptada a las necesidades particulares de la industria automotriz, como:
 1. Protección de prototipos.
 2. Seguridad de la información de diseño.
 3. Continuidad de procesos de producción.
 4. Seguridad en plantas y talleres (Operational Technology, OT).

Estructura

El catálogo se divide en dominios y controles, que cubren temas como gestión de riesgos, control de acceso, seguridad física, gestión de incidentes, continuidad del negocio, etc.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Cada control tiene niveles de madurez (1 a 5), lo que permite medir el grado de implementación en la empresa.

Relevancia

- Se utiliza tanto para autoevaluaciones internas como para auditorías oficiales de TISAX.
- La versión más reciente, VDA-ISA 6.0 (2024), amplió su enfoque para incluir disponibilidad de sistemas, no solo confidencialidad.
- Es una herramienta de alineación que garantiza que toda la cadena de suministro automotriz hable “el mismo lenguaje” en materia de ciberseguridad. (Verband der Automobilindustrie (VDA), 2016)

ENX Association

La ENX Association (European Network Exchange Association) es una organización sin fines de lucro fundada por los principales fabricantes automotrices europeos (como BMW, Volkswagen, Daimler, PSA, Renault y Ford).

Tiene sede en Francia y Alemania y actúa como organismo de gobernanza y administrador oficial del esquema TISAX (Trusted Information Security Assessment Exchange).

Función principal

- Gestionar y supervisar el ecosistema TISAX, que permite a las empresas automotrices evaluar, certificar y compartir de manera estandarizada su nivel de seguridad de la información.
- Acreditar a los proveedores de auditorías TISAX.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Mantener la plataforma online de intercambio de resultados TISAX, donde las empresas registradas pueden consultar y compartir su estatus de cumplimiento.

Relevancia

- ENX garantiza que el proceso TISAX sea transparente, confiable y reconocido por toda la industria automotriz europea.
- Evita la duplicación de auditorías: una empresa evaluada bajo TISAX puede compartir su resultado con múltiples fabricantes, lo que reduce costos y tiempos.
- Fomenta una cadena de suministro segura y homogénea, fortaleciendo la confianza digital entre socios. (ENX Association, 2024)

A continuación, se muestra la relación funcional entre las tres entidades clave del esquema TISAX.

Elemento	Tipo / Naturaleza	Rol principal	Relación con TISAX
VDA (Verband der Automobilindustrie)	Asociación alemana de fabricantes automotrices	Desarrolla el catálogo ISA y define los estándares de seguridad de la información en el sector automotriz.	Es el creador del estándar base de TISAX.
ISA (Information Security Assessment)	Catálogo de evaluación (documento técnico)	Define los controles y criterios de seguridad de la información específicos del sector.	Sirve como base técnica para las auditorías TISAX.
Elaboro Nombre firma y puesto: Alexander Ávila / TI		Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta

ENX Association	Organización europea sin fines de lucro	Administra el esquema TISAX, acredita auditores y gestiona los resultados.	Es el organismo de gobernanza del proceso TISAX.
------------------------	---	--	--

Tabla 1: Comparación con Relación entre VDA, ISA y ENX

1.2 Políticas Generales de Seguridad de la Información

Objetivo General

Garantizar que toda la información generada, almacenada, procesada o transmitida por la organización sea protegida adecuadamente frente a accesos no autorizados, pérdida, alteración o divulgación indebida, preservando la confianza y continuidad de las operaciones.

Objetivos Específicos

- Proteger los activos de información de pérdidas, daños o accesos no autorizados.
- Asegurar la continuidad operativa ante incidentes.
- Cumplir con la legislación en materia de protección de datos personales.
- Fomentar la cultura de seguridad entre los colaboradores.
- Establecer responsabilidades claras en materia de seguridad.

Propósito

Establecer las directrices, principios y responsabilidades que permitan proteger los activos de información de la organización frente a riesgos internos o externos,

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

garantizando que toda la información sea utilizada de manera ética, segura y conforme a las leyes y regulaciones aplicables.

Alcance

Esta política aplica a:

- Todo el personal de la organización (empleados, contratistas, practicantes, proveedores de servicios).
- Toda la información, sin importar el medio en que se encuentre (digital, físico, audiovisual).
- Todos los equipos, dispositivos, sistemas informáticos, redes y aplicaciones propiedad o bajo custodia de la organización.
- Incluye tanto los correos electrónicos corporativos como los documentos impresos, bases de datos de clientes, informes internos y respaldos en la nube.

Principios Fundamentales

Principio	Descripción	Ejemplo
Confidencialidad	La información solo puede ser conocida por personas autorizadas.	Un reporte financiero solo puede ser accedido por el área de contabilidad.
Integridad	La información debe mantenerse completa, sin alteraciones indebidas.	Los registros de empleados no pueden modificarse sin autorización.
Disponibilidad	La información debe estar accesible cuando se necesite.	Los servidores críticos deben tener respaldo y redundancia.

Legalidad	Toda acción debe cumplir con las leyes vigentes.	El tratamiento de datos personales se ajusta a la LFPDPPP.
Responsabilidad	Cada usuario es responsable del uso correcto de la información.	Un empleado debe bloquear su sesión al ausentarse de su puesto.
Mejora Continua	Las políticas y controles se revisan y actualizan regularmente.	Se realizan auditorías anuales de seguridad.

Tabla 2: Principios Fundamentales de la Seguridad de la Información

Responsabilidades

Alta Dirección

- Aprobar las políticas y asignar los recursos necesarios.
- Promover una cultura organizacional de seguridad.

Responsable de Seguridad de la Información (RSI)

- Supervisar el cumplimiento de políticas.
- Coordinar auditorías internas y revisiones de riesgo.
- Gestionar incidentes de seguridad.

Área de Tecnologías de la Información (TI)

- Implementar medidas técnicas (contraseñas, cifrado, antivirus, firewall).
- Mantener los sistemas actualizados y respaldados.

Colaboradores y Usuarios

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Cumplir con las políticas y procedimientos establecidos.
- Reportar incidentes o comportamientos sospechosos.
- Proteger contraseñas y dispositivos asignados.

Cumplimiento

Establecido en el artículo 6 de la LFPDPPP, todo empleado que, por razón de su cargo o funciones, tenga acceso a información que contenga datos personales o información confidencial, está obligado a:

- Guardar absoluta confidencialidad sobre dicha información.
- Utilizarla únicamente para los fines autorizados por la empresa.
- Evitar su alteración, pérdida, transmisión o acceso no autorizado.

Con el propósito de garantizar el cumplimiento de las políticas internas de seguridad de la información y la observancia de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), todos los colaboradores, sin excepción, deberán leer, comprender y firmar la *Cláusula de Confidencialidad y Declaración de Aceptación* establecida ([ver anexo 4](#)).

Consecuencias de incumplimiento

El incumplimiento de esta política podrá resultar en:

- Acciones disciplinarias internas, como amonestaciones o suspensión.
- Responsabilidad civil o penal, si se comprometen datos personales o confidenciales.

Se considerará una falta grave a la confidencialidad y una violación directa a la LFPDPPP, conforme al artículo 63 fracción VII del citado ordenamiento.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

Sanciones internas y legales

El empleado que incurra en la divulgación no autorizada de información confidencial estará sujeto a las sanciones internas establecidas en el Reglamento de Trabajo y el Código de Conducta de la empresa, que podrán incluir:

- Amonestación verbal o escrita.
- Suspensión temporal sin goce de sueldo.
- Rescisión de la relación laboral sin responsabilidad para la empresa, conforme al artículo 47 fracción II de la Ley Federal del Trabajo.

Así mismo, la empresa podrá presentar denuncia ante el INAI, autoridad competente en materia de protección de datos personales, para la imposición de sanciones previstas en la LFPDPPP, que pueden incluir:

- Multas de 100 a 320,000 veces el valor diario de la UMA (vigente), duplicables si se trata de datos personales sensibles.

Revisión y Actualización

Esta política será revisada **anualmente o cuando exista un cambio significativo** en la estructura tecnológica, normativa o de procesos.

Toda actualización debe documentarse y ser aprobada por la Dirección y el Responsable de Seguridad de la Información.

1.3 Documentos de Seguridad

Los Documentos de Seguridad constituyen el marco documental que respalda la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI). Garantizando que toda acción relacionada con la seguridad

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

esté formalmente establecida, aprobada, controlada y actualizada, conforme a los requisitos de ISO/IEC 27001 y demás normas aplicables.

Tipos de Documentos

1. **Políticas:** Establecen los principios y lineamientos generales (por ejemplo, política de contraseñas, de respaldo, de uso aceptable, de correo electrónico).
2. **Procedimientos:** Describen paso a paso las acciones que deben realizarse para cumplir con las políticas (por ejemplo, procedimiento de alta y baja de usuarios, gestión de incidentes, clasificación de información).
3. **Instructivos o Guías Técnicas:** Detallan configuraciones o acciones técnicas específicas (por ejemplo, configuración segura de dispositivos, cifrado de discos duros, uso de antivirus).
4. **Registros y Formularios:** Evidencias documentales del cumplimiento de políticas y procedimientos (por ejemplo, registro de incidentes, control de accesos, bitácoras de respaldo).
5. **Plan de Continuidad y Recuperación:** Define estrategias y procedimientos para mantener la operación ante desastres o incidentes graves.

Control Documental

Para asegurar la integridad y trazabilidad de los documentos de seguridad, se implementa un control documental que contempla:

- Asignación de códigos de identificación y números de versión.
- Registro de fecha de creación, revisión y aprobación.
- Designación de un responsable de mantenimiento de cada documento.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Almacenamiento en repositorios seguros y accesibles únicamente para personal autorizado.
- Registro de cambios y control de versiones anteriores.

Ejemplo de *Registro de Control Documental* ([ver anexo 5](#)).

Estructura Recomendada de un Documento de Seguridad

Cada documento debe incluir los siguientes elementos mínimos:

1. Título y Código (ej. PROC-SI-001).
2. Versión y Fecha de Revisión.
3. Objetivo.
4. Alcance.
5. Responsables.
6. Descripción del Procedimiento o Política.
7. Anexos o Formatos.
8. Historial de Cambios.

Ejemplo de *Estructura Documental* ([ver anexo 6](#)).

Disponibilidad y Acceso

- Los documentos se almacenan en un repositorio digital seguro, dentro de la intranet o un sistema de gestión documental.
- Solo el personal autorizado podrá acceder, modificar o imprimir los documentos.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Toda copia impresa deberá identificarse como “Copia No Controlada” para evitar confusiones.

Protección y Confidencialidad

- Los documentos de seguridad se consideran información interna confidencial.
- Está prohibido compartirlos fuera de la organización sin autorización escrita.
- Las versiones obsoletas deben eliminarse o archivarse de forma controlada para evitar confusiones.

Por ejemplo, cuando se actualiza la Política de Contraseñas, la versión anterior se marca como “obsoleta” y se guarda en un repositorio de histórico, accesible solo para auditorías.

Revisión y Actualización

La frecuencia de una revisión documental dentro de una empresa depende del tipo de documento, del sistema de gestión que se aplique.

Tipo de documento:

Políticas y Manuales de Gestión. Cada 1 a 2 años revisar o actualizar cuando haya cambios normativos, estructurales o estratégicos en la empresa.

Procedimientos e Instrucciones de trabajo. Cada 1 año revisar anualmente o antes si se detectan no conformidades o cambios en los procesos

Formatos y registros. Según necesidad o cada 2 años se actualizan cuando cambian los datos a registrar o el proceso asociado.

Documentos legales o normativos. Cada vez que haya una actualización legal o reglamentaria para mantener una vigilancia normativa continua.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Planes (ej. Plan de Calidad, Plan Ambiental, Plan de Seguridad, etc.) Cada año o por proyecto para revisar en cada ciclo de planificación o ante cambios significativos

1.4 Clasificación de la Información Según Sensibilidad

Para establecer un sistema de clasificación de la información que permita determinar el nivel de protección que cada tipo de dato requiere, se debe de realizar de acuerdo con su sensibilidad, valor y riesgo en caso de pérdida, modificación o divulgación no autorizada. Asegurando que se apliquen los controles de seguridad apropiados en su almacenamiento, uso, transmisión y eliminación.

Alcance

Este sistema aplica a toda la información generada, recibida o custodiada por la organización, sin importar:

- Su formato (digital, físico, audiovisual o verbal).
- Su origen (interna o externa).
- Su ubicación (servidores, computadoras, dispositivos móviles o archivos físicos).

Importancia del Cumplimiento

Una clasificación adecuada:

- Reduce el riesgo de fugas de información.
- Facilita la aplicación de controles proporcionales.
- Permite cumplir con la LFPDPPP y auditorías de ISO 27001.
- Refuerza la cultura de seguridad entre todos los colaboradores

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

Criterios de Clasificación

Criterio	Descripción
Valor	Importancia que tiene la información para la organización o sus clientes.
Sensibilidad	Nivel de impacto si la información es divulgada, modificada o destruida sin autorización.
Requisitos Legales	Si la información está sujeta a leyes o regulaciones (ej. LFPDPPP, contratos de confidencialidad).
Impacto en la Reputación	Consecuencias para la imagen institucional en caso de pérdida o mal uso.

Tabla 3: Clasificación de la Información Según Sensibilidad

Niveles de Clasificación de la Información

La organización establece cuatro niveles de clasificación, que determinan el grado de protección y los controles que deben aplicarse:

Nivel	Descripción	Ejemplos	Controles Recomendados
Pública	Información que puede difundirse sin restricción. Su divulgación no causa daño a la organización.	Folletos, comunicados de prensa, información del sitio web público.	Libre acceso, sin requerir medidas de protección especiales.
Interna	Información de uso exclusivo del personal. Su	Procedimientos internos, calendarios de	Almacenamiento en intranet o red interna;

	divulgación podría causar molestias menores o confusión.	actividades, manuales generales.	prohibido publicar externamente.
Confidencial	Información sensible cuyo acceso se limita a personal autorizado. Su exposición puede causar daño operativo o legal.	Datos de empleados, reportes financieros, bases de clientes, contratos, actas administrativas.	Cifrado, contraseñas seguras, acceso con roles definidos, almacenamiento en carpetas seguras.
Restringida / Secreta	Información crítica o estratégica cuya divulgación puede generar graves consecuencias financieras, legales o reputacionales.	Estrategias corporativas, claves maestras, investigaciones en curso, datos biométricos.	Cifrado avanzado, acceso bajo autorización directa, almacenamiento fuera de red pública, registro de accesos.

Tabla 4: Niveles de Clasificación de la Información

Etiquetado de la Información

Cada documento o archivo deberá llevar una etiqueta o marca de clasificación ya sea de manera visible, física o digital, que indique su nivel de sensibilidad.

Ejemplos:

- Físico: Sellos o encabezados en los documentos impresos, como *“Confidencial – Uso Interno”*.

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

- Digital: Metadatos o nombres de archivo como Informe_Financiero_2025_CONFIDENCIAL.pdf.
- Correo Electrónico: Incluir en el asunto la clasificación (Ej. “Asunto: Resultados de Auditoría – Restringido”).

Si la clasificación de la información no está clara, deberá tratarse como Confidencial hasta que se determine su categoría correcta.

Responsabilidades

Rol	Responsabilidad
Propietario de la Información	Determinar la clasificación correcta según la naturaleza del contenido.
Usuarios Autorizados	Cumplir con las políticas y no divulgar información fuera de su nivel de acceso.
Área de Seguridad de la Información / TI	Implementar controles técnicos (cifrado, accesos, respaldos).
Todos los Colaboradores	Proteger la información bajo su custodia y reportar cualquier manejo indebido.

Tabla 5: Rol de Responsabilidades

Manejo de Información Según Clasificación

Actividad	Pública	Interna	Confidencial	Restringida
Almacenamiento	Intranet o web pública	Servidores internos	Servidores seguros con cifrado	Almacenamiento seguro con cifrado y acceso limitado
Transmisión	Libre	Solo entre usuarios internos	Correo cifrado / VPN	Canales cifrados y autenticados, aprobación previa
<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI		<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI		<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta

Impresión	Libre	Solo si es necesario	Controlada, recoger inmediatamente	Prohibida sin autorización escrita
Eliminación	Borrado simple	Borrado simple	Triturado o borrado seguro	Dstrucción física o sobreescritura certificada

Tabla 6: Manejo de Información Según Clasificación

Ejemplo de Aplicación Práctica

Caso 1 – Folleto Informativo de Servicios:	Se distribuye públicamente. • Clasificación: Pública. • Manejo: Puede publicarse en la web y redes sociales sin restricción.
Caso 2 – Reporte de Ventas Trimestral:	Contiene cifras económicas internas. • Clasificación: Confidencial. • Manejo: Solo para gerentes y dirección; se envía mediante correo institucional cifrado.
Caso 3 – Base de Datos de Clientes:	Contiene datos personales (nombres, teléfonos, correos). • Clasificación: Confidencial (según LFPDPPP). • Manejo: Solo personal autorizado del área comercial puede acceder; cifrado obligatorio.
Caso 4 – Clave Maestra del Servidor:	Control total de infraestructura crítica. • Clasificación: Restringida. • Manejo: Solo administradores designados; almacenada en bóveda digital segura.

Tabla 7: Ejemplo de Manejo de Información Según Clasificación

Revisión de Clasificación

Cada área deberá revisar al menos una vez al año la clasificación de su información o cuando cambie su uso, valor o sensibilidad.

El Responsable de Seguridad de la Información deberá aprobar cualquier modificación en los niveles de clasificación.

1.5 Controles para el Manejo de Información Física y Digital

Establecer medidas y procedimientos para proteger la información tanto física como digital, evitando pérdidas, accesos no autorizados, modificaciones indebidas o divulgación no autorizada.

Alcance

Aplica a toda la información generada, recibida o almacenada por la organización, sin importar el formato:

- Digital: servidores, correo electrónico, sistemas en la nube, dispositivos móviles, discos duros, memorias USB.
- Física: documentos impresos, planos, archivos internos, registros en papel, medios ópticos.

Beneficios del Cumplimiento

- Reducción de riesgos de fugas, pérdidas o robos de información.
- Cumplimiento de LFPDPPP, ISO 27001 y NOM-151.
- Mayor control sobre la disponibilidad e integridad de la información.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Facilita la auditoría interna y externa.
- Refuerza la confianza de clientes y socios al demostrar seguridad en el manejo de datos.

Procedimientos Clave

1. Clasificación de Información:

- Toda información debe etiquetarse según Pública, Interna, Confidencial o Restringida antes de almacenarla o compartirla.

2. Manejo de Copias y Respaldos:

- Copias digitales deben cifrarse y almacenarse en ubicaciones seguras.
- Las copias impresas deben registrarse y guardarse en archivadores bajo llave.

3. Compartición de Información:

- Compartir solo con personas autorizadas y mediante canales seguros.
- Prohibido enviar información confidencial a correos externos o públicos.

4. Uso de Dispositivos Móviles:

- Teléfonos, laptops y tablets corporativas deben tener bloqueo por contraseña y cifrado.
- Información confidencial no debe almacenarse en dispositivos personales sin autorización.

5. Destrucción de Información:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Documentos impresos: triturado o incineración.
- Archivos digitales: borrado seguro o sobreescritura certificada.

Controles para Información Física

Control	Descripción	Ejemplo Práctico
Almacenamiento Seguro	Documentos y archivos físicos deben guardarse en lugares seguros, con acceso restringido.	Archivadores con llave en oficinas administrativas; sala de documentos confidenciales con control de acceso.
Registro de Acceso	Llevar bitácora de entrada/salida de personas y documentos.	Formato de registro de visitantes para quienes acceden a la bodega de archivos.
Protección durante Traslado	Documentos sensibles deben trasladarse en sobres o carpetas marcadas y bajo custodia.	Entrega de contratos a otra sucursal mediante mensajería interna con firma de recepción.
Eliminación Segura	Documentos confidenciales deben destruirse de manera irreversible.	Triturado de documentos, desmagnetización de cintas o destrucción de CDs/DVDs.
Etiquetado	Clasificar la información según su sensibilidad.	“Confidencial – Solo Personal Autorizado” en carpetas y sobres.

Tabla 8: Controles para Información Física

Controles para Información Digital

Control	Descripción	Ejemplo Práctico
<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta

Código: PTI-001

No. Revisión y Fecha: 3 / 9.05.2025

Área responsable:
Tecnología de la información
Áreas involucradas:

Todos

Página
48 de 193

Control de Accesos	Usuarios autorizados con contraseñas seguras y roles definidos.	Acceso a la base de datos de clientes solo para personal del área comercial.
Cifrado de Información	Datos sensibles deben cifrarse tanto en reposo como en tránsito.	Cifrado de discos duros con software como BitLocker o Kaspersky, y correos electrónicos mediante S/MIME.
Respaldo y Recuperación	Realizar copias de seguridad periódicas, almacenadas de forma segura.	Backups semanales en servidor seguro y copia en almacenamiento en la nube cifrada.
Protección contra Malware	Uso de antivirus, firewall y actualización de sistemas.	Escaneo automático diario de servidores y estaciones de trabajo.
Control de Medios Portátiles	Uso limitado y seguro de discos externos y dispositivos móviles.	Prohibido almacenar información confidencial en dispositivos personales o en Memorias USB.
Gestión de Correos y Mensajería	Políticas para envío seguro de información.	Enviar información confidencial solo mediante cuentas corporativas y cifrado; no reenviar a correos personales.
Registro de Eventos y Monitoreo	Seguimiento de accesos y acciones realizadas en sistemas críticos.	Auditorías automáticas que registran quién abrió, modificó o eliminó archivos sensibles.

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

Tabla 9: Controles para Información Digital

Responsabilidades

Rol	Responsabilidad
Propietario de la Información	Clasificar información y definir controles de protección.
Usuarios / Colaboradores	Cumplir las políticas de manejo de información; proteger contraseñas y dispositivos.
Área de TI	Implementar cifrado, backups, antivirus y controles de acceso.
Seguridad de la Información	Revisar cumplimiento de controles, auditorías y manejo seguro de información física y digital.

Tabla 10: Rol de Responsabilidades

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Capítulo II.

Identificación y

Gestión de

Riesgos

2.1 Identificación de Riesgos y Vulnerabilidades

En el contexto organizacional, los riesgos se definen como eventos o circunstancias que, si ocurren, pueden afectar negativamente el cumplimiento de los objetivos de la organización, causando pérdidas económicas, operativas, legales o reputacionales.

Por su parte, las vulnerabilidades son debilidades o fallas dentro de los procesos, sistemas o estructuras de la organización que facilitan la materialización de estos riesgos. La identificación adecuada de riesgos y vulnerabilidades permite a la empresa implementar medidas preventivas y correctivas, fortaleciendo su capacidad de resiliencia y asegurando la continuidad operativa.

Tipos de Riesgos

Los riesgos que pueden afectar a una organización son diversos y se clasifican comúnmente en las siguientes categorías:

1. Riesgos tecnológicos: Relacionados con fallas en sistemas de información, ciberataques, pérdida de datos o interrupciones en la infraestructura tecnológica.
2. Riesgos humanos: Derivados de errores, negligencias o comportamientos inadecuados del personal, incluyendo fraudes internos o falta de capacitación.
3. Riesgos operativos: Asociados a fallas en los procesos internos, deficiencias en la cadena de suministro, interrupciones de producción o incumplimiento de procedimientos.
4. Riesgos legales y regulatorios: Proviene del incumplimiento de leyes, normativas y regulaciones aplicables, incluyendo sanciones, multas o litigios.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

5. Riesgos financieros: Involucran pérdidas económicas derivadas de fluctuaciones de mercado, impagos, problemas de liquidez o decisiones financieras inadecuadas.

6. Riesgos estratégicos: Vinculados a la toma de decisiones, cambios en el entorno competitivo o fallas en la planificación organizacional.

Métodos de Identificación

La identificación de riesgos y vulnerabilidades requiere un enfoque sistemático y multidimensional. Entre los métodos más utilizados se encuentran:

- Cuestionarios y encuestas: Herramientas estructuradas para recolectar información sobre posibles riesgos percibidos por el personal.
- Entrevistas: Reuniones con responsables de áreas clave para identificar riesgos críticos desde la perspectiva operativa y estratégica.
- Auditorías internas: Evaluaciones periódicas que permiten detectar debilidades en procesos, controles y sistemas.
- Análisis de procesos y flujos de información: Examen detallado de los procedimientos internos y el manejo de la información para identificar puntos de vulnerabilidad.

Registro de Riesgos

Una vez identificados, los riesgos y vulnerabilidades deben ser documentados en un inventario de riesgos, el cual incluye información relevante como la descripción del riesgo, la causa, la posible consecuencia, la persona responsable de su seguimiento y las medidas de mitigación propuestas como el *Ejemplo de Registro De Riesgos* ([anexo 7](#)).

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

Este registro sirve como base para la toma de decisiones y para el desarrollo de planes de gestión de riesgos.

Prioridad de Riesgos

No todos los riesgos presentan la misma gravedad; por ello, es necesario establecer prioridades según probabilidad de ocurrencia e impacto potencial. Los riesgos se pueden clasificar como:

- Alto: Riesgos con alta probabilidad de ocurrencia y consecuencias significativas.
- Medio: Riesgos que pueden ocurrir con moderada frecuencia y cuya afectación es moderada.
- Bajo: Riesgos con baja probabilidad de ocurrencia y consecuencias mínimas.

Asignar recursos de manera eficiente, enfocándose primero en los riesgos más críticos y reduciendo la exposición de la organización a eventos adversos de acuerdo a *la Guía práctica para la Identificación de Riesgos y Vulnerabilidades* ([ver anexo 8](#)).

2.2 Seguridad Para los Riesgos de la Información

La seguridad de la información es el conjunto de medidas, políticas y procedimientos destinados a proteger los activos de información de la organización frente a accesos, usos, divulgaciones, alteraciones o destrucciones no autorizadas, para garantizar la correcta gestión y protección de los datos durante todo su ciclo de vida.

Este concepto se sustenta en el modelo CIA, compuesto por tres principios fundamentales:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- **Confidencialidad:** Garantiza que la información solo sea accesible para las personas, procesos o sistemas debidamente autorizados, evitando su divulgación indebida.
- **Integridad:** Asegura que la información se mantenga completa, precisa y libre de modificaciones no autorizadas, preservando su veracidad y confiabilidad.
- **Disponibilidad:** Busca que la información esté accesible y utilizable cuando sea requerida por los usuarios o sistemas autorizados, garantizando la continuidad operativa.

Tipos de Amenazas a la Información

La información puede verse afectada por múltiples amenazas, tanto internas como externas. Estas amenazas pueden comprometer uno o varios de los principios del modelo CIA. Entre las más comunes se encuentran:

- **Malware (software malicioso).** Programas diseñados para dañar, alterar o sustraer información, como virus, troyanos, ransomware o spyware.
- **Phishing.** Técnica de suplantación de identidad que busca obtener información confidencial (como contraseñas o datos financieros) mediante engaños.
- **Accesos no autorizados.** Intentos de ingreso a sistemas o datos por parte de personas sin permisos correspondientes.
- **Errores humanos.** Fallos cometidos por los usuarios, como el envío de información a destinatarios incorrectos, contraseñas débiles o eliminación accidental de datos.
- **Fallas de hardware o software.** Defectos técnicos que pueden provocar pérdida o corrupción de información.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Un riesgo que debe ser identificado, evaluado y mitigado oportunamente para preservar la seguridad de los activos informacionales.

Políticas General de Seguridad

Las políticas de seguridad de la información constituyen el marco normativo interno que regula el manejo, uso, almacenamiento y transmisión de los datos dentro de la organización.

Estas políticas deben incluir, entre otros aspectos:

- Definición de niveles de acceso según roles y responsabilidades.
- Reglas para el uso de contraseñas, dispositivos y redes.
- Procedimientos de respaldo y recuperación de información.
- Lineamientos sobre el manejo de información confidencial o sensible.
- Protocolos de respuesta ante incidentes de seguridad.

Para prevenir incidentes de seguridad, minimizar riesgos operativos y garantizar el cumplimiento de las buenas prácticas y normativas aplicables se deberá de cumplir con la *Política General de Seguridad de la Información* ([ver anexo 9](#)).

Roles y Responsabilidades

La correcta gestión de la seguridad de la información requiere una estructura organizativa clara que establezca responsabilidades a distintos niveles:

- Alta Dirección: Define la política general de seguridad, asigna recursos y supervisa su cumplimiento.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Responsable de Seguridad de la Información (RSI) o CISO: Coordina la implementación de medidas de seguridad, gestiona los riesgos y supervisa las auditorías.
- Administradores de sistemas: Garantizan la aplicación técnica de los controles de seguridad (configuración de accesos, mantenimiento de servidores, actualizaciones, etc.).
- Usuarios finales: Cumplen las políticas establecidas, resguardan sus credenciales, reportan incidentes y actúan conforme a los lineamientos de seguridad.

Priorización de Riesgos por Nivel de Impacto y Probabilidad

La gestión de riesgos de la información implica identificar, analizar y evaluar las amenazas potenciales que pueden afectar los activos informacionales.

Para ello, se debe establecer una Matriz de Gestión de Riesgo que clasifique cada amenaza según dos factores principales:

- Impacto: Nivel de daño o consecuencia que tendría la materialización del riesgo sobre la organización (alto, medio o bajo).
- Probabilidad: Frecuencia o posibilidad de ocurrencia del riesgo (alta, media o baja).

Ejemplo Matriz de Gestión de Riesgo ([ver anexo 10](#)).

Normativas y Estándares Aplicables

La seguridad de la información se encuentra regulada por diferentes marcos normativos y estándares internacionales, los cuales establecen buenas prácticas y requisitos mínimos para garantizar una adecuada protección de los datos. Entre los más relevantes se destacan:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Reglamento General de Protección de Datos (RGPD): Norma europea que regula el tratamiento de datos personales y los derechos de los titulares, promoviendo la transparencia y la protección de la privacidad. (*Ver página 18*).
- Norma ISO/IEC 27001: Estándar internacional que especifica los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). ([*Ver ISO/IEC 27001: Gestión de la Seguridad de la Información*](#)).
- Otras normativas complementarias: Pueden incluir leyes nacionales de protección de datos y políticas corporativas internas.

2.3 Medidas Preventivas y Correctivas

Las medidas preventivas y correctivas forman parte esencial de la gestión de la seguridad de la información.

Su objetivo es proteger los activos informáticos (datos, sistemas, redes y personas) frente a amenazas internas o externas, garantizando la confidencialidad, integridad y disponibilidad de la información.

Medidas Preventivas

Son acciones o mecanismos implementados antes de que ocurra un problema, con el fin de reducir riesgos y fortalecer la protección del entorno tecnológico.

Principales Medidas Preventivas:

1. Controles de acceso. Definen quién puede acceder a los recursos del sistema y bajo qué condiciones.
 - Tipos:

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Autenticación: verificar la identidad del usuario (contraseñas, biometría, tokens).
- Autorización: definir qué recursos o acciones puede realizar.
- Auditoría: registro de accesos y acciones.

2. Respaldo de información (Backups)

- Creación de copias de seguridad periódicas de los datos críticos.
- Se deben almacenar en lugares seguros o en la nube, y probar regularmente su restauración.

3. Capacitación y concientización

- Educar al personal en buenas prácticas de seguridad (phishing, contraseñas seguras, manejo de datos).
- Fomenta la cultura de ciberseguridad dentro de la organización.

4. Encriptación de datos

- Protege la información transformándola en un formato ilegible sin clave.
- Se usa tanto para datos en tránsito (transmisiones de red) como en reposo (almacenados).

5. Actualización de software

- Mantener todos los sistemas, aplicaciones y firmware actualizados con los últimos parches de seguridad.
- Reduce vulnerabilidades conocidas.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Medidas Correctivas

Se aplican tras un incidente de seguridad (como un ciberataque, pérdida de datos o falla del sistema). Su propósito es restaurar la normalidad y prevenir futuras recurrencias.

Principales medidas correctivas:

1. Plan de respuesta a incidentes
 - Conjunto de procedimientos para identificar, contener, erradicar y recuperar ante un incidente.
 - Incluye roles y responsabilidades del equipo de respuesta (CSIRT).
Protocolo de Respuesta a Incidentes de Seguridad ([ver capítulo III-3.1](#)).
2. Recuperación de datos
 - Uso de copias de seguridad o sistemas redundantes para restaurar información dañada o perdida.
 - Se evalúa la prioridad de los sistemas críticos (según el Plan de Continuidad del Negocio).
3. Ajuste de controles después de un incidente
 - Tras analizar el evento, se refuerzan o modifican las medidas preventivas.

Evaluación de Efectividad

Consiste en medir si las medidas implementadas cumplen su función y si reducen efectivamente los riesgos.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

Se realiza mediante:

- Auditorías de seguridad: revisión de políticas, configuraciones y registros.
- Pruebas de penetración (pentesting): simulaciones de ataques para detectar vulnerabilidades.
- Indicadores de desempeño (KPIs):
 - Número de incidentes detectados.
 - Tiempo promedio de respuesta (MTTR).
 - Porcentaje de sistemas actualizados.
 - Éxito en recuperación de backups.

Cuadro de Evaluación de Efectividad

Medida Implementada	Indicador de Efectividad (KPI)	Método de Evaluación	Resultado Esperado	Nivel de Cumplimiento
Control de acceso con 2FA	% de accesos no autorizados detectados	Revisión de logs de seguridad	Disminución del 90% de accesos sospechosos	Alto (95%)
Respaldo de información diario	Tiempo promedio de restauración de datos (MTTR)	Prueba de recuperación mensual	Restaurar datos en menos de 30 minutos	Medio (45 min)

Capacitación al personal	% de empleados que aprueban test de ciberseguridad	Evaluación trimestral	85% de aprobación o más	Alto (88%)
Políticas de actualización	% de sistemas con último parche instalado	Auditoría semestral de software	100% de sistemas actualizados	Medio (80%)
Plan de respuesta a incidentes	Tiempo promedio de detección y contención (MTTD/MTTC)	Simulacros de ataque	Responder en menos de 1 hora	Alto (45 min)

Tabla 11: Ejemplo de un Cuadro de Evaluación de Efectividad

- Las medidas con cumplimiento alto indican que los controles son efectivos y deben mantenerse (cuanto mayor sea el porcentaje, más efectiva es la medida)
- Los resultados medios o bajos muestran necesidad de ajuste, como mejorar la automatización, capacitar al personal o reforzar políticas (aquellas por debajo del 80% deben ser revisadas o reforzadas.).

Se recomienda realizar esta evaluación de forma trimestral o semestral, y documentar los resultados en informes internos de seguridad.

Plan de Contingencia

Es un conjunto de estrategias y procedimientos diseñados para garantizar que la empresa pueda continuar operando ante interrupciones graves, desastres naturales

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

o ataques cibernéticos. Su objetivo principal es proteger la información crítica y minimizar el impacto en la operación.

Componentes Principales

Análisis de Impacto al Negocio (BIA)

El BIA permite identificar qué procesos, sistemas y datos son críticos para la empresa y establecer los tiempos máximos de inactividad tolerables (RTO – Recovery Time Objective) y la pérdida de datos aceptable (RPO – Recovery Point Objective).

Acciones para Proteger la Información:

- Clasificación de la información según su importancia y confidencialidad.
- Identificación de activos digitales (servidores, bases de datos, aplicaciones) y físicos (documentos impresos, equipos).
- Evaluación de riesgos: ciberataques, fallas de hardware, incendios, inundaciones, errores humanos.
- Determinación de prioridades de recuperación según impacto financiero y operativo.

Planes de Continuidad del Negocio (BCP)

El BCP define cómo mantener la operación durante una crisis, asegurando que los procesos críticos sigan funcionando.

Estrategias de Protección de la Información:

➤ Digital:

- Respaldo de datos en la nube y en medios físicos externos.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Uso de cifrado para información confidencial.
- Acceso controlado mediante contraseñas robustas y autenticación multifactor.
- Segmentación de la red para limitar el alcance de un ataque cibernético.

➤ **Física:**

- Custodia segura de documentos importantes (cajas fuertes, archivos cerrados).
- Control de acceso a oficinas y centros de datos.
- Sistemas de alarma y vigilancia.
- Políticas de manejo de información impresa (no dejar documentos en escritorios, destruir información sensible obsoleta).

Planes de Recuperación ante Desastres (DRP)

El DRP establece los procedimientos para restaurar sistemas, infraestructura y datos luego de un evento que interrumpa la operación.

➤ **Digital:**

- Restauración de sistemas críticos desde copias de seguridad.
- Uso de centros de datos redundantes o servidores de respaldo.
- Procedimientos para recuperar datos perdidos o comprometidos.

➤ **Física:**

- Protocolos de evacuación y protección de activos críticos.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Recuperación de archivos físicos dañados (por ejemplo, mediante digitalización de documentos).
- Contratos con proveedores de recuperación de información o seguros para desastres físicos.

Pruebas y Simulacros

La efectividad del plan depende de pruebas periódicas y simulacros que identifiquen fallos antes de una crisis real para ello se deberán de registrar en los formatos para documentar simulacros de contingencia, recuperación de datos, respuesta ante incidentes, pérdida de información, o fallas en sistemas.

Actividades Recomendadas:

- Simulacros de desastres digitales: probar restauración de servidores, bases de datos y aplicaciones críticas.
- Ejercicios de evacuación y seguridad física.
- Revisión periódica de políticas y procedimientos de seguridad de información.
- Actualización continua de los planes en función de nuevos riesgos o cambios tecnológicos.

Formato 1: Ejemplo de Registro de Pruebas y Simulacros de Seguridad de la Información ([ver anexo 11](#)).

Formato 2: Ejemplo de Planificación y Seguimiento de Pruebas / Simulacros ([ver anexo 12](#)).

2.4 Monitoreo de Información y Nuevos Proyectos

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

La protección de la información es un proceso continuo que no solo implica resguardar los datos existentes, sino también garantizar que cualquier nuevo proyecto o iniciativa integre la seguridad desde su concepción. Para ello, se implementan estrategias de monitoreo y evaluación continua.

Monitoreo continuo

El monitoreo continuo de la información permite detectar posibles incidentes de seguridad antes de que afecten gravemente a la organización. Entre las prácticas más importantes destacan:

- Supervisión de servidores, bases de datos, aplicaciones y archivos sensibles tanto en entornos digitales como físicos (servidores locales, archivos en papel, registros confidenciales).
- Configuración de notificaciones automáticas ante accesos no autorizados, intentos de intrusión o modificaciones sospechosas de la información.
- Identificación de patrones inusuales en el uso de datos, transferencias de información no habituales o comportamientos atípicos de los usuarios, mediante herramientas de análisis de logs y monitoreo de red.

Evaluación de Nuevos Proyectos

Antes de implementar un nuevo proyecto, producto o servicio, es esencial realizar un análisis exhaustivo de los riesgos que pueda implicar para la información. Este análisis incluye:

1. Reconocimiento de posibles vulnerabilidades, tanto digitales (ciberataques, filtraciones de datos) como físicas (acceso no autorizado a instalaciones, pérdida de documentos).

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

2. Determinación del efecto potencial sobre la confidencialidad, integridad y disponibilidad de la información si el riesgo se materializa.
3. Definición de medidas preventivas y correctivas antes de la puesta en marcha del proyecto.

Integración de Riesgos en Proyectos

La gestión de riesgos debe incorporarse desde la fase de planificación de cualquier proyecto. Las estrategias incluyen:

- Considerar posibles amenazas en todas las etapas del proyecto, desde la planificación hasta la implementación.
- Implementar medidas específicas para reducir los riesgos identificados, incluyendo cifrado de datos, control de accesos y procedimientos de respaldo.
- Evaluar regularmente los riesgos durante el ciclo de vida del proyecto y ajustar las medidas según cambios en el entorno interno o externo.

Integración de la Seguridad en el Ciclo de Vida de Nuevos Proyectos

La seguridad de la información debe estar presente en cada fase del ciclo de vida del proyecto:

1. Planificación: Evaluar riesgos, definir políticas de seguridad y asignar responsabilidades.
2. Diseño: Incorporar controles de acceso, cifrado y medidas de protección física y digital.
3. Implementación: Asegurar que las prácticas de seguridad se cumplan, con pruebas de vulnerabilidad y revisión de accesos.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

4. Operación: Monitorear continuamente el proyecto y sus sistemas asociados.
5. Cierre: Garantizar la correcta eliminación o archivado seguro de información y la documentación de lecciones aprendidas.

Indicadores de Desempeño (KPIs)

- Número de incidentes de seguridad detectados durante el proyecto.
- Porcentaje de controles de seguridad implementados según lo planificado.
- Tiempo promedio de respuesta ante alertas de seguridad.
- Cumplimiento de auditorías de seguridad internas y externas.
- Nivel de concientización del personal involucrado en nuevos proyectos.

Se sugiere implementar un enfoque práctico que incluya registrar toda la información en un dashboard, ya sea en Excel, Power BI o en un sistema de GRC, para tener un control centralizado.

Además, es importante revisar los KPIs de manera mensual y realizar reuniones breves de seguimiento para evaluar el desempeño. También se deben documentar las acciones correctivas aplicadas, garantizando así la mejora continua.

Finalmente, se recomienda capacitar al personal de forma constante, dado que la seguridad depende tanto de la tecnología como de las personas.

2.5 Control para el Cambio de Información

Constituye un conjunto de procedimientos, normas y medidas destinadas a garantizar que cualquier modificación de información crítica de la organización se realice de manera segura, autorizada y trazable.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Este control aplica tanto a la información digital (bases de datos, sistemas, archivos electrónicos) como a la información física (documentos impresos y registros manuales), siguiendo los principios de gestión de la información recomendados por estándares internacionales, tales como ISO/IEC 27001.

Gestión de Cambios

La gestión de cambios asegura que todas las modificaciones en la información crítica se realicen mediante un procedimiento formal, que incluya los siguientes pasos:

1. Solicitud de modificación. Registro detallado que describa la necesidad del cambio y la información afectada.
2. Justificación del cambio. Explicación del propósito, los beneficios esperados y los posibles impactos.
3. Evaluación de riesgos. Identificación de los riesgos asociados al cambio, incluyendo fallas técnicas o errores humanos.

Los cambios deben planificarse cuidadosamente para evitar interrupciones operativas y garantizar la continuidad del negocio. Se recomienda clasificar los cambios de la siguiente manera:

- Cambios menores: Corrección de errores, ajustes puntuales de datos o actualizaciones de formato.
- Cambios mayores: Modificación de procesos, actualización de políticas o alteraciones en datos estratégicos.

Versión de Documentos

Cada documento, ya sea físico o digital, debe contar con un registro de versiones, indicando la fecha, el autor y la naturaleza del cambio.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Principales Medidas:

- Conservar copias de versiones anteriores para garantizar trazabilidad y permitir restauraciones ante errores o inconsistencias.
- Controlar el acceso a los documentos según niveles de confidencialidad, asegurando que únicamente el personal autorizado pueda consultar o modificar versiones críticas.

Autorización de Cambios

Todo cambio significativo debe contar con aprobación formal por parte de los responsables designados, tales como gerentes de área, propietarios de información o comités de seguridad de la información.

Lineamientos:

- Documentar la autorización mediante firma física o digital.
- Evitar la ejecución de cambios sin validación previa, previniendo modificaciones no controladas que puedan comprometer la confiabilidad de la información.

Prevención de Errores y Pérdidas

- Copias de seguridad periódicas (backups) de información digital.
- Resguardo seguro de documentos físicos, en archivos con acceso restringido.
- Revisiones y auditorías periódicas de los cambios para verificar la consistencia de los datos.
- Controles de validación previos a la implementación de cambios, que reduzcan errores humanos y técnicos.

Documentación de Cambios

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Todo cambio debe registrarse en un historial de cambios, incluyendo la siguiente información:

Versión	Fecha de Ejecución	Descripción del Cambio	Motivo y Justificación	Responsable de la Modificación	Aprobación Formal

Tabla 12: Historial de Cambios de Documentación

Permitiendo identificar qué cambios se realizaron, por quién y en qué momento, facilitando auditorías internas y externas.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

Capítulo III.

Gestión de Incidentes de Seguridad

3.1 Protocolo de Respuesta a Incidentes de Seguridad

Se considera Incidente de Seguridad de la información a cualquier evento adverso, confirmado o sospechoso, que afecte o pueda afectar la confidencialidad, integridad o disponibilidad de los activos de información de la organización.

Entre los incidentes más comunes se incluyen, pero no se limitan a:

- Accesos no autorizados a sistemas o información.
- Infecciones por malware, ransomware o virus.
- Pérdida o robo de información o dispositivos.
- Interrupciones no planificadas en los servicios.
- Modificaciones no autorizadas en sistemas o datos.
- Divulgación indebida de información confidencial.

Estructura del Equipo de Respuesta

Un Equipo de Respuesta a Incidentes de Seguridad (ERIS) o Computer Security Incident Response Team (CSIRT) está conformado por personal especializado encargado de gestionar los incidentes de manera eficaz. Su estructura básica puede incluir:

1. Coordinador del equipo. Responsable de dirigir y supervisar la respuesta al incidente, coordinar recursos y mantener comunicación con la alta dirección.
2. Analistas de seguridad. Encargados de detectar, analizar y evaluar el incidente, así como de determinar su alcance e impacto.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

3. Equipo técnico o de contención. Especialistas en sistemas, redes o aplicaciones que implementan medidas de contención, eliminación y recuperación.
4. Representante de comunicación o relaciones públicas. Gestiona la comunicación interna y externa, especialmente si el incidente afecta a clientes, socios o medios.
5. Asesor legal y de cumplimiento. Garantiza que las acciones cumplan con la legislación vigente (por ejemplo, protección de datos personales o notificación de brechas).

Pasos del Protocolo de Respuesta a Incidentes

[Ver anexo 13.](#)

3.2 Detección, Reporte, Respuesta y Recuperación de Incidentes

La detección de incidentes podrá realizarse mediante herramientas automáticas de monitoreo o a través del reporte de usuarios.

La CSI (Coordinación de Seguridad de la Información) deberá implementar y mantener mecanismos que permitan identificar actividades inusuales o potencialmente maliciosas.

Canales de Reporte

Los incidentes deberán reportarse a través de alguno de los siguientes medios oficiales:

- Correo electrónico: seguridad@empresa.com

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Sistema de tickets (categoría “Incidente de Seguridad”).
- Teléfono interno de emergencias TI: (XXX) XXX-XXXX

Tiempos Máximos de Reporte

Nivel de severidad	Ejemplo	Tiempo máximo de reporte
Crítico	Fuga de datos, ransomware, caída de sistemas esenciales	Inmediato (≤ 30 min)
Alto	Acceso no autorizado, malware confirmado	40 min
Medio o Bajo	Correo sospechoso, intento fallido de acceso	1 hora

Tabla 13: Tiempos Máximos de Reporte

Herramientas de Detección

La organización debe contar con mecanismos y herramientas que permitan detectar, registrar y alertar oportunamente sobre actividades que representen una posible amenaza a la seguridad de la información.

Estas herramientas son esenciales para la identificación temprana de incidentes y la prevención de impactos mayores en los activos institucionales.

1. Sistemas de Monitoreo Centralizado (SIEM)

Un SIEM (Security Information and Event Management) recopila, correlaciona y analiza los registros de eventos de diferentes sistemas (servidores, redes, aplicaciones, bases de datos).

Permite:

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Detectar comportamientos anómalos y patrones de ataque.
- Generar alertas automáticas basadas en reglas y umbrales.
- Mantener bitácoras centralizadas para auditoría y análisis forense.

2. IDS/IPS (Sistemas de Detección y Prevención de Intrusos)

Estos sistemas vigilan el tráfico de red en tiempo real:

- IDS (Intrusion Detection System): Detecta intentos de intrusión o tráfico sospechoso.
- IPS (Intrusion Prevention System): Además de detectar, bloquea automáticamente conexiones maliciosas o no autorizadas.

3. EDR (Endpoint Detection and Response)

Solución instalada en equipos finales (computadoras, laptops, servidores) que:

- Supervisa continuamente la actividad del sistema.
- Detecta comportamientos inusuales o malware avanzado.
- Permite aislar equipos comprometidos y responder de forma remota.

4. Antivirus y Antimalware Corporativo

Proveen protección contra amenazas comunes (virus, troyanos, ransomware, spyware).

Deben mantenerse actualizados y configurados para:

- Realizar escaneos automáticos y programados.
- Notificar a la Coordinación de Seguridad ante detecciones críticas.
- Generar reportes periódicos de estado y amenazas.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmín López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

5. Monitoreo de Logs y Eventos

Todos los sistemas críticos (servidores, bases de datos, firewalls, aplicaciones, routers, etc.) deben tener habilitado el registro de eventos (logs).

Estos registros se revisan mediante:

- Herramientas automáticas de análisis de logs.
- Correlación de eventos en el SIEM.
- Revisiones manuales periódicas por personal autorizado.

6. Monitoreo de Infraestructura y Disponibilidad

Se emplean herramientas para verificar:

- Estado de los servicios, redes y servidores.
- Uso de recursos (CPU, memoria, disco, ancho de banda).
- Alertas ante caídas o degradación del servicio.

Ejemplos: *Zabbix, Nagios, SolarWinds, PRTG Network Monitor.*

7. Herramientas de Monitoreo de Correo y Navegación Web

Sistemas de filtro de contenido y detección de amenazas en correos electrónicos y navegación web, que ayudan a:

- Bloquear enlaces o archivos maliciosos.
- Prevenir phishing, spam y descargas no seguras.
- Emitir alertas sobre dominios o direcciones IP sospechosas.

8. Dashboards y Consolas de Alerta

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Todas las herramientas deben integrarse en paneles de control que muestren:

- Incidentes detectados en tiempo real.
- Nivel de severidad e impacto.
- Estado de respuesta y acciones pendientes.

Requisitos de las Herramientas de Detección

- Operar bajo un monitoreo continuo (24/7 o según criticidad).
- Emitir alertas automáticas ante eventos predefinidos.
- Permitir la trazabilidad y registro de todas las acciones detectadas.
- Mantener evidencias para su análisis durante y después del incidente.
- Estar alineadas con las políticas y normativas del Sistema de Gestión de Seguridad de la Información (SGSI).

Proceso de Documentación

Informe Post-Incidente de seguridad de la Información [Ver anexo 14](#).

Análisis Post-Incidente

[Ver anexo 15](#)

3.3 Protocolos para la Pérdida y Robo de Información

Pérdida de Información Física

Posibilidades de pérdida de información física:

- Pérdida debido a que un activo de información físico (documentos en papel, carpetas de trabajo, etc.) es dejado en un lugar no seguro o se extravía sin rastros.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Los documentos de información se dejan olvidados en lugares como salas de reuniones, cafeterías, vehículos, etc.
- Daño o destrucción accidental de los activos de información físicos, como un documento roto, manchado, quemado o dañado sin que se pueda recuperar la información.
- Cuando los documentos físicos con información sensible son retirados sin autorización, sin que se trate necesariamente de un robo.

Acciones en caso de Pérdida de Información Física:

1. Notificación inmediata:

- En caso de pérdida de información física, el responsable debe notificar de inmediato al área de TI y a su superior jerárquico.
- Informar a las autoridades competentes si el incidente involucra información sensible o de alto valor.

2. Acciones inmediatas:

- Si es posible, se deben tomar acciones para recuperar la información perdida (buscar en las áreas donde el activo pudo haber sido olvidado o extraviado).
- Si no se puede recuperar la información perdida, se deberán buscar medios para reponerla de acuerdo con los procedimientos internos de la empresa (reconstituir la información desde copias o archivos respaldados).

3. Análisis post-incidente:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- El incidente debe ser analizado para identificar causas raíz y mejorar los controles de seguridad física, así como prevenir la repetición del incidente.
- En función del análisis, se podrán implementar medidas adicionales para mejorar el almacenamiento y manejo de la información física.

Pérdida de Información Digital

Posibilidades de pérdida de información digital:

- Un dispositivo como un teléfono móvil, laptop o disco duro que contenga información confidencial es dejado en un lugar público, como una cafetería o una sala de espera.
- Un activo de información digital se olvida en un espacio de trabajo, en un vehículo o en otro lugar no seguro.
- Un dispositivo presenta un fallo técnico inesperado, lo que impide recuperar la información almacenada (daños en el disco duro o fallas en la red).
- El daño físico o el mal uso de un dispositivo impide la recuperación de la información almacenada, como la rotura o daño de un equipo informático.

Acciones en caso de Pérdida de Información Digital:

1. Notificación inmediata:

- El responsable debe notificar de inmediato al área de TI sobre la pérdida del activo digital.
- Informar al superior inmediato si la pérdida involucra información confidencial o sensible.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

2. Acciones inmediatas:

- Si el dispositivo perdido o dañado contiene información sensible o confidencial, el equipo de TI tomará las medidas necesarias para borrar remotamente la información del dispositivo.
- Se procederá con la desactivación de todas las cuentas de usuario asociadas al dispositivo perdido o que pueda haber estado comprometido.
- El equipo de TI llevará a cabo un monitoreo exhaustivo para detectar accesos no autorizados, revisando los logs de acceso y actividades sospechosas.

3. Análisis post-incidente:

- Se llevará a cabo una revisión exhaustiva del incidente para identificar vulnerabilidades o debilidades en los controles de seguridad informática y en las políticas de manejo de dispositivos.
- Implementar mejoras en las políticas de cifrado, control de acceso y monitoreo de dispositivos digitales para prevenir incidentes similares.

Robo de Información Física**Posibilidades de robo de información física:**

- Un documento, archivo, equipo o soporte con información sensible es robado de un área de la empresa o mientras se encontraba bajo la custodia de un empleado o tercero autorizado.
- Información o dispositivos robados mientras están siendo trasladados entre diferentes ubicaciones de la empresa.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Acceso físico no autorizado a áreas de almacenamiento de documentos o equipos que contienen información confidencial, lo que permite la sustracción de estos activos.

Acciones en caso de Robo de Información Física:

1. Notificación inmediata:

- El responsable debe notificar de inmediato a las autoridades competentes y al área de TI.

2. Acciones inmediatas:

- Si es posible, se deben tomar medidas para intentar recuperar los activos robados.
- Se debe garantizar que las autoridades sean informadas de inmediato sobre el robo para su investigación.

3. Análisis post-incidente:

- Después de la investigación, se debe realizar un análisis detallado del incidente para identificar las debilidades en la seguridad física y mejorar las medidas de control de acceso y almacenamiento seguro de la información.

Robo de Información Digital

Posibilidades de robo de información digital:

- Un dispositivo como una laptop, teléfono móvil o disco duro con información sensible es robado.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Un atacante obtiene acceso no autorizado a sistemas corporativos a través de métodos como el phishing, la explotación de vulnerabilidades o el robo de credenciales.
- Las credenciales de acceso (como contraseñas o tokens de autenticación) son robadas y utilizadas para acceder a sistemas o información confidencial.

Acciones en caso de Robo de Información Digital:**1. Notificación inmediata:**

- El responsable debe notificar inmediatamente al área de TI sobre el robo del dispositivo o las credenciales.
- Informar a las autoridades competentes para investigar el incidente y tomar las acciones legales necesarias.

2. Acciones inmediatas:

- El equipo de TI intentará borrar remotamente la información del dispositivo robado para evitar que los datos sean accesibles.
- Se procederá con la desactivación de las cuentas y accesos comprometidos, como cuentas de correo electrónico, sistemas internos y servicios en la nube.
- Se llevará a cabo un seguimiento para verificar si se realizaron accesos no autorizados a la información corporativa.

3. Análisis post-incidente:

- Después del incidente, se realizarán ajustes en las políticas de seguridad digital, incluidas mejoras en la autenticación, el cifrado de dispositivos y

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

el monitoreo de accesos para prevenir futuros robos de información digital.

Notificación a Autoridades o Afectados

Cuando ocurre una pérdida o filtración de información, es fundamental cumplir con las obligaciones legales y de transparencia. La notificación oportuna permite mitigar el impacto, mantener la confianza y evitar sanciones.

1. Determinación de Obligaciones Legales

Antes de emitir cualquier notificación, el área responsable debe:

- Identificar el tipo de datos comprometidos (personales, financieros, confidenciales, secretos industriales, etc.).
- Analizar las leyes aplicables, como:
 - Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México).
 - Reglamento General de Protección de Datos – GDPR (si aplica a operaciones internacionales).
- Evaluar los plazos y requisitos de notificación que la normativa establece según la gravedad del incidente.

2. Notificación a Autoridades Regulatorias

En caso de que los datos personales o confidenciales se vean comprometidos, debe realizarse una notificación formal a las autoridades competentes (por ejemplo, el */NAI* en México).

La notificación deberá incluir:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Tipo y alcance de los datos afectados: especificar si se trata de información personal, financiera, médica, corporativa, etc.
- Causa del incidente: origen del fallo (humano, técnico, externo, interno, ciberataque, etc.).
- Medidas adoptadas: acciones de contención, recuperación y prevención implementadas para reducir el daño y evitar recurrencias.
- Fecha y hora de detección del incidente, así como el área responsable de su gestión.

3. Notificación a Personas Afectadas

De manera transparente y oportuna, se debe informar a todos los individuos cuyos datos pudieron verse comprometidos (clientes, empleados o terceros). La comunicación debe ser clara, empática y orientada a la protección del afectado, incluyendo:

- Descripción del incidente: qué sucedió y cuándo.
- Datos comprometidos: tipo de información que podría haberse visto expuesta.
- Riesgos potenciales: cómo podría impactar a las personas.
- Medidas recomendadas: por ejemplo, cambiar contraseñas, monitorear movimientos bancarios, activar alertas de seguridad o contactar al área de soporte.
- Medidas adoptadas por la empresa: acciones que se están tomando para resolver el incidente y evitar que se repita.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Canal de contacto: correo o número telefónico donde los afectados puedan solicitar más información o apoyo.

4. Registro Interno de Notificaciones

Es obligatorio mantener un Registro Documental completo de todas las notificaciones realizadas, incluyendo:

- Fecha y hora de cada notificación.
- Destinatarios (autoridades y personas afectadas).
- Medio utilizado (correo electrónico, carta, comunicado oficial, portal web, etc.).
- Copia o evidencia del envío.
- Respuestas o acuses de recibo recibidos.

Medidas para Minimizar Impacto y Restaurar Operaciones

Tipo de acción	Objetivo	Acciones específicas
Preventivas	Evitar la pérdida o reducir su impacto	• Realizar backups periódicos (locales, remotos, offline). • Implementar cifrado de datos y control de accesos. • Mantener sistemas redundantes (servidores y almacenamiento). • Capacitar al personal en seguridad de información. • Instalar antivirus y sistemas de detección de intrusos.

		Mantener software actualizado y parches de seguridad.
Inmediatas	Minimizar el impacto y contener el incidente	- Identificar la información perdida y la causa. - Aislar los sistemas afectados. - Detener accesos no autorizados o maliciosos. - Notificar al equipo de TI y gerencia. - Activar el plan de recuperación de desastres (DRP).
Correctivas / Restauración	Recuperar datos y restablecer operaciones	- Restaurar datos desde backups confiables. - Verificar integridad de los datos recuperados. - Usar sistemas redundantes para mantener operaciones. - Reparar fallas de hardware o software. - Actualizar sistemas y seguridad para evitar recurrencias. - Analizar causas raíz del incidente y documentar lecciones aprendidas. - Mejorar planes de contingencia y auditorías periódicas.

Tabla 14: Medidas para Minimizar Impacto y Restaurar Operaciones

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

Capítulo IV.

Recursos

Humanos y

Concientización

4.1 Obligaciones de Confidencialidad del Personal

Cláusulas de Confidencialidad en Contratos

Se incorporan cláusulas específicas relacionadas con la seguridad de la información en los contratos laborales para garantizar que todos los empleados comprendan y asuman responsabilidades la protección de los datos sensibles de la empresa.

Las principales cláusulas incluyen:

- I. Confidencialidad. Compromiso de mantener la información de la empresa en estricta confidencialidad.
- II. Protección de información crítica. Obligación de proteger los datos y sistemas clave de la empresa frente a accesos no autorizados o daños.
- III. No competencia. Restricciones para evitar que los empleados utilicen la información adquirida para competir con la empresa.
- IV. Uso de dispositivos y sistemas de la empresa. Normas para el uso adecuado de equipos y recursos tecnológicos proporcionados por la empresa.
- V. Monitoreo y supervisión. Derechos de la empresa para monitorear el uso de recursos tecnológicos y verificar el cumplimiento de las políticas de seguridad.

Políticas Sobre Divulgación de Información

Se establece un compromiso adicional mediante un acuerdo de no divulgación (NDA), que obliga a los empleados a mantener la confidencialidad de la información sensible de la empresa incluso después de la finalización de su relación laboral.

Información Confidencial

La información confidencial que se debe proteger incluye, pero no se limita a:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Información técnica y de producto.
- Planes de negocio, estrategias de marketing y proyecciones financieras.
- Información sobre clientes, proveedores y relaciones comerciales.
- Datos de investigación y desarrollo.
- Cualquier otra información proporcionada por México Sonavox Electronics Co que se considere sensible o propietaria.

Obligación de No Divulgación

El empleado se compromete a:

- No divulgar, distribuir, copiar ni utilizar la información confidencial fuera de su trabajo en la empresa.
- Mantener la información confidencial en estricta confidencialidad y asegurarse de que no sea accesible a personas no autorizadas.

Excepciones a la Confidencialidad

La obligación de no divulgación no será aplicable a:

- Información que sea de dominio público, sin haber sido divulgada por el empleado.
- Información recibida de una fuente ajena a la empresa que no esté sujeta a un acuerdo de confidencialidad.
- Información revelada con el consentimiento previo y por escrito de la empresa.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Duración de la Obligación de Confidencialidad

La obligación de confidencialidad continuará incluso después de la finalización del contrato de trabajo, sin importar el motivo de su terminación.

Acuerdo Completo

Este acuerdo constituye la base legal de las obligaciones del empleado respecto a la información confidencial, y cualquier violación a las condiciones establecidas en él podrá derivar en medidas disciplinarias o legales según lo dispuesto en las políticas de seguridad de la empresa.

Procedimiento para el Manejo de Violaciones a las Políticas

Se ha establecido un procedimiento para gestionar las violaciones a las políticas de seguridad y confidencialidad. Asegurando una respuesta rápida y efectiva ante cualquier incidente que comprometa la seguridad de la información de la empresa.

Identificación de la Violación

- Acceso no autorizado a datos confidenciales o críticos.
- Divulgación indebida de información sensible.
- Uso indebido de recursos tecnológicos.
- Incumplimiento de los procedimientos de seguridad establecidos por la empresa.

Notificación y Registro de Violaciones

Es obligatorio que cualquier violación sea reportada formalmente y registrada en el sistema de gestión de incidentes de la empresa. El informe incluye una descripción detallada del incidente, los datos relevantes, y las personas involucradas.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Investigación Inicial

El área de TI llevará a cabo una investigación inicial para evaluar la gravedad de la violación. Esta investigación incluirá:

- Revisión de registros y análisis de los datos asociados al incidente.
- Entrevistas con las personas involucradas y/o testigos del evento.
- Evaluación de los daños causados y el impacto potencial de la violación.
- Determinación de si hubo un acceso no autorizado a la información crítica o sensible.

Capacitación y Concientización Continua

Implementar un programa continuo de capacitación y concientización en seguridad de la información para todos los empleados, para fomentar un entorno de trabajo seguro y garantizar el cumplimiento de las políticas de seguridad establecidas.

1. Inducción inicial. Llevar a cabo una capacitación para todos los nuevos empleados sobre las políticas de seguridad de la empresa, el manejo adecuado de la información crítica y las mejores prácticas para prevenir vulnerabilidades en el entorno laboral.
2. Sesiones periódicas. Organizar sesiones de capacitación anuales o semestrales para mantener actualizados a los empleados sobre las nuevas amenazas de seguridad, así como sobre las mejores prácticas para proteger los datos de la empresa.
3. Evaluación de la comprensión. Aplicar pruebas periódicas para evaluar el nivel de comprensión de las políticas de seguridad por parte de los empleados y garantizar que estas se sigan correctamente en su día a día.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Obligación de Confidencialidad Adicional

En situaciones donde los empleados tengan acceso a información extremadamente sensible, los acuerdos son más estrictos y detallados, con el fin de proteger la información crítica de la empresa. Además, de establecer medidas de auditoría y monitoreo regulares para garantizar que la información sensible sea manejada de manera adecuada y que se cumpla con las políticas de seguridad establecidas.

Consecuencias por Incumplimiento

Para asegurar el cumplimiento de las políticas de seguridad de la información, se implementarán sanciones disciplinarias graduales:

- I. Primera infracción. Se impondrá una reprimenda escrita junto con un recordatorio sobre la política de confidencialidad.
- II. Segunda infracción. Se procederá con una suspensión temporal, acompañada de una re-capacitación en seguridad de la información.
- III. Infracción grave. En caso de filtración intencionada de datos confidenciales o en su defecto la edición mal intencionada/borrado mal intencionado, se turnará el caso con RH para ejecutar una rescisión de contrato justificada y se evaluarán posibles acciones legales.

4.2 Cualificación y Confiabilidad del Personal en Áreas Sensibles

Criterios de Selección y Evaluación de Personal con Acceso Crítico

Se determinan qué áreas o puestos dentro de la empresa están relacionados con actividades sensibles que puedan comprometer la seguridad de la información. Esto puede incluir:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Acceso a información confidencial. Usuarios que manejan datos clasificados o privados.
- Acceso a infraestructura crítica. Usuarios que trabajan directamente con sistemas, hardware o software que gestionan datos sensibles.
- Manejo de procesos críticos de producción. Áreas que podrían tener acceso a información relevante.
- Posiciones con acceso físico a instalaciones de alto riesgo. Áreas donde se almacenan productos o datos sensibles.

Clasificación de Trabajo Sensible

Se clasifican los trabajos dentro de la organización en función de su nivel de sensibilidad. Esto puede incluir:

- Trabajo crítico, que involucra acceso a sistemas de información y bases de datos de alto nivel o acceso a áreas de producción.
- Trabajo no crítico, tareas que no requieren acceso a información confidencial ni interactúan con sistemas sensibles.

Revisión de Antecedentes y Referencias

Se realizan perfiles detallados de cada puesto clasificado como sensible, especificando las cualificaciones, habilidades, conocimientos y experiencia requeridos.

- Requisitos académicos y profesionales. Títulos universitarios, certificados o licencias profesionales necesarias.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Habilidades técnicas y competencias. Experiencia específica en manejo de software, equipos o protocolos de seguridad que estén relacionados con el manejo de información sensible.
- Conocimiento de normativas de seguridad. Comprensión de las políticas internas y normativas legales aplicables al manejo de información confidencial.

Requisitos de Formación y Capacitación

Se asegura que los empleados reciban formación especializada en seguridad de la información, protecciones de datos y riesgos relacionados.

1. Capacitación inicial. Entrenamiento inicial sobre políticas de seguridad de la información, gestión de datos y procedimientos operativos.
2. Capacitación continua. Programas de formación continua para mantener a los empleados actualizados sobre cambios en las normativas, tecnologías y riesgos de seguridad.
3. Entrenamiento en emergencias y protección de datos. Simulacros y prácticas de respuesta ante incidentes de seguridad, protección de datos sensibles, y prevención de accesos no autorizados.

Cumplimiento de Normativas Internas y Externas

Se hace una verificación de que los empleados estén familiarizados con las políticas internas de la organización, así como las regulaciones legales y normativas externas relacionadas con la seguridad de la información.

- Normativas internas. Asegurar que los empleados entiendan y sigan las políticas internas de seguridad de la información.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Regulaciones externas. Cumplimiento con regulaciones nacionales e internacionales o las regulaciones de protección de datos en el sector automotriz.

Proceso de Verificación de Identidad y Cualificación

Asegurar que los empleados o candidatos sean quienes dicen ser, verificando su identidad de manera rigurosa. Por medio de:

- Documentos de identidad. Comprobar documentos oficiales como pasaportes, identificaciones nacionales o licencias de conducir.
- Validación de identidad en línea. Sistemas de validación de identidad digital (si es necesario).

Validación de Cualificaciones y Experiencia

El proceso de validación de empleados en roles sensibles se asegura que cumplan con los requisitos del puesto mediante:

1. Verificación de títulos académicos y certificaciones. Comprobar que los títulos y certificaciones sean válidos y relevantes para el cargo.
2. Referencias laborales. Contactar para validar la experiencia y desempeño en roles similares.
3. Evaluación de habilidades. Realizar pruebas para confirmar que las competencias del empleado están alineadas con los requisitos del puesto.

Entrevistas y Evaluaciones

Para asegurar que un candidato cumpla con los requisitos técnicos y de seguridad del puesto, se lleva a cabo entrevistas estructuradas y evaluaciones prácticas.

1) Entrevistas técnicas:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Se evalúan los conocimientos técnicos específicos para el trabajo, incluyendo el manejo de sistemas, herramientas, y procedimientos de seguridad.
- Se plantean escenarios prácticos para evaluar la capacidad del candidato para gestionar incidentes de seguridad y aplicar soluciones efectivas.

2) Evaluación de comportamiento:

- Se analizan las competencias del candidato para seguir procedimientos de seguridad establecidos, especialmente en situaciones de alta presión o incidentes de seguridad.
- Se evalúa cómo el candidato prioriza la seguridad en su trabajo y cómo reacciona ante posibles amenazas o riesgos.

Evaluaciones Periódicas de Desempeño

Realizar revisiones periódicas de las cualificaciones de los empleados para asegurar que sigan siendo aptos para manejar información sensible.

- 1) Evaluación Anual. Para asegurar que los empleados mantengan sus habilidades actualizadas.
- 2) Reentrenamiento. Capacitación adicional sobre nuevos riesgos de seguridad o tecnologías en caso de ser necesario.

Documentación y Registros

Mantener un registro detallado de la verificación de identidad, las cualificaciones y la formación de los empleados en roles sensibles para garantizar el cumplimiento de los estándares de seguridad y protección de datos.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- 1) Registro de documentos. Mantener un archivo centralizado con los documentos de identidad, calificaciones y certificaciones de los empleados, asegurando que toda la información esté organizada y accesible.
- 2) Auditoría de registros. Garantizar que los registros estén disponibles, cumpliendo con las normativas de protección de datos, asegurando la transparencia y la trazabilidad.

4.3 Sensibilización y Formación en Seguridad de la Información

Programas de Capacitación Obligatorios

Antes de implementar el plan de capacitación, se identifican los grupos que requieren formación específica en seguridad de la información:

- Nuevos empleados: Inducción en seguridad de la información desde su incorporación.
- Personal con acceso a información sensible: Capacitación especializada en manejo de datos críticos.
- Departamento de TI: Formación avanzada sobre amenazas y estrategias de mitigación.
- Otros grupos de riesgo: Cualquier usuario con acceso a información estratégica o susceptible a ataques.

Plan de Capacitación

Se establece un programa estructurado con contenido adaptado a cada grupo destinatario, para asegurar la comprensión y aplicación de buenas prácticas de seguridad de la información.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

Contenidos de la Capacitación

Cada sesión aborda temas clave para fortalecer la cultura de seguridad dentro de la empresa:

- Política de Seguridad de la Información: Normas y lineamientos internos.
- Identificación y Reporte de Eventos de Seguridad: Métodos para detectar y reportar incidentes.
- Reacción ante Malware: Protocolos para contener y remediar infecciones.
- Política de Cuentas de Usuario y Contraseñas: Uso seguro de credenciales.
- Cumplimiento de Normativas: Regulaciones internas.
- Acuerdos de Confidencialidad: Pautas para compartir información de manera segura.
- Uso de Servicios Externos: Riesgos y buenas prácticas en el uso de almacenamiento en la nube, correos y dispositivos externos.

Frecuencia y Temas (phishing, contraseñas, manejo de datos)

El plan se estructura en sesiones presenciales y virtuales, con metodologías dinámicas para reforzar el aprendizaje.

➤ **Sesión 1: Política de Seguridad de la Información**

Introducción a la política de seguridad, roles y responsabilidades, principios básicos.

- Metodología: Presentación teórica con videos interactivos.

➤ **Sesión 2: Identificación y Reporte de Eventos de Seguridad**

Señales de ataques (phishing, malware), procesos de reporte, protocolos internos.

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

- Metodología: Taller práctico con simulaciones de incidentes.

➤ **Sesión 3: Reacción ante Malware**

Tipos de malware, estrategias de prevención y respuesta.

- Metodología: Guías y protocolos de acción.

➤ **Sesión 4: Política de Cuentas de Usuario y Contraseñas**

Creación de contraseñas seguras, cambio periódico, autenticación multifactor.

- Metodología: Ejercicios prácticos de generación de contraseñas seguras.

➤ **Sesión 5: Cumplimiento de Normativas**

Explicación de normativas internas y externas, consecuencias del incumplimiento.

- Metodología: Seminario interactivo con casos reales.

➤ **Sesión 6: Acuerdos de Confidencialidad**

Importancia de los acuerdos de confidencialidad, manejo de información sensible.

- Metodología: Discusión con ejemplos prácticos.

➤ **Sesión 7: Uso de Servicios Externos**

Riesgos y buenas prácticas en almacenamiento en la nube, correos y dispositivos USB.

- Metodología: Presentación con casos reales y ejercicios prácticos.

Calendario de Capacitación

Se establecen sesiones periódicas según la criticidad del tema y el grupo objetivo:

Frecuencia	Actividad	Grupo Objetivo
Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta

Semanal	Curso de inducción en seguridad de la información	Nuevos empleados
Mensual	Sensibilización en equipos de trabajo	Todos los empleados
Mensual	Información sobre uso seguro de servicios en la nube	Todos los empleados
Trimestral	Capacitación sobre políticas de seguridad	Todos los empleados
Trimestral	Capacitación sobre cumplimiento y acuerdos de confidencialidad	Todos los empleados
Trimestral	Gestión de accesos y cuentas	Todos los empleados
Semestral	Simulación de incidente de seguridad	Personal clave (TI, RRHH, Finanzas)
Semestral	Encuesta de conocimiento en seguridad de la información	Todos los empleados
Anual	Curso sobre contraseñas seguras y autenticación	Todos los empleados
Anual	Curso sobre reacción ante malware	Todos los empleados
Anual	Revisión y actualización de políticas de seguridad	Encargado
Anual	Evaluación de conocimientos y reporte de seguridad	Encargado

Tabla 15: Calendario de Capacitación

Evaluación de Efectividad de la Formación

Formato de Evaluación de Efectividad de la Formación ([ver anexo 16](#))

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

4.4 Política de Trabajo Móvil

Reglas para Trabajo Remoto y Uso de Dispositivos

- I. Los dispositivos utilizados para el trabajo móvil deben ser proporcionados o aprobados previamente por el equipo de TI. No se permite el uso de dispositivos personales para realizar actividades laborales.
- II. Seguridad en los dispositivos:
 - Contraseña o autenticación biométrica.
 - Encriptación de datos.
 - Actualización regular del sistema operativo y aplicaciones.
 - Instalación de software antivirus autorizado por el equipo de TI.
- III. Se prohíbe almacenar información confidencial o sensible en dispositivos móviles, salvo que se utilicen sistemas aprobados por parte de TI para la protección de datos.
- IV. En caso de pérdida o robo de un dispositivo móvil perteneciente a la organización, el empleado deberá notificar de inmediato al departamento de TI para proceder con las acciones de bloqueo remoto, eliminación de datos y evaluación de riesgos, con el fin de minimizar cualquier posible riesgo de ciberseguridad.

Requisitos de Conexión Segura

Requisitos Generales

1. Toda conexión remota deberá establecerse a través de una red privada virtual (VPN) corporativa aprobada y administrada por el área de Seguridad de la Información o Tecnología.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

2. El acceso remoto debe estar limitado a usuarios autorizados y vinculado a perfiles específicos según sus funciones.
3. Se deberá aplicar autenticación multifactor (MFA) como requisito obligatorio para validar la identidad del usuario antes de permitir el acceso.
4. Las conexiones remotas deben cifrar todo el tráfico de datos con algoritmos y protocolos seguros (por ejemplo, AES-256, TLS 1.2 o superior, IPSec).
5. Todo dispositivo que se conecte a la red institucional deberá cumplir con antivirus actualizado, sistema operativo soportado y parches al día.
6. Se prohíbe el uso de redes Wi-Fi públicas o no seguras para acceder a sistemas institucionales, salvo que la VPN corporativa esté activa.

Requisitos Específicos

Conexiones VPN (Virtual Private Network)

- La VPN debe ser provista y gestionada exclusivamente por la organización.
- Las credenciales de acceso son personales e intransferibles.
- Las sesiones de VPN deben registrar:
 - Fecha y hora de conexión y desconexión.
 - Dirección IP de origen.
 - Usuario autenticado.
 - Recursos accedidos.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- La conexión se debe cerrar automáticamente tras periodos de inactividad (máximo 15–30 minutos).
- El área de Seguridad de la Información deberá monitorear continuamente los registros de la VPN para detectar accesos inusuales o intentos fallidos repetidos.

Autenticación Multifactor (MFA)

- La MFA combina al menos dos de los siguientes factores:
 - Algo que el usuario sabe (contraseña o PIN).
 - Algo que el usuario tiene (token físico, aplicación móvil, llave USB de seguridad).
 - Algo que el usuario es (biometría: huella, rostro, etc.).
- Es obligatoria para:
 - Accesos remotos a la red o VPN.
 - Ingreso a aplicaciones críticas (correo corporativo, ERP, CRM, bases de datos sensibles).
 - Acceso administrativo o de privilegio elevado.
- El sistema debe registrar los intentos fallidos y bloquear temporalmente la cuenta tras múltiples errores consecutivos.

El responsable de equipo de TI debe tomar las siguientes precauciones para proteger la información confidencial y sensible mientras trabajan de manera remota:

- Evitar la transmisión de datos sensibles o confidenciales a través de canales no seguros (correos electrónicos sin cifrado). En su lugar, deben utilizarse herramientas autorizadas por TI que garanticen la seguridad de la información.
- Proteger la confidencialidad, integridad y disponibilidad de los datos manejados en los dispositivos móviles, conforme a las políticas de seguridad de documentos.
- Los datos manejados desde dispositivos móviles deben ser respaldados regularmente, utilizando los sistemas de respaldo establecidos por el equipo de TI.

Uso de Aplicaciones y Software.

Utilizar las aplicaciones y software autorizados por el equipo de TI para realizar actividades laborales. Cualquier software no autorizado puede representar un riesgo de seguridad y debe ser aprobado previamente por el equipo de TI.

Todos los dispositivos utilizados para el trabajo móvil deben tener configuradas las actualizaciones automáticas para el sistema operativo y las aplicaciones esenciales, garantizando la instalación de parches de seguridad al momento de su liberación.

Responsabilidad Sobre el Equipo e Información

- Todos los equipos, sistemas y la información generada o gestionada son propiedad de la organización.
- El usuario tiene un uso autorizado y responsable, no propiedad personal.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- La información debe ser utilizada únicamente para fines laborales autorizados.
- Se prohíbe la divulgación a personas no autorizadas.
- Los usuarios deben proteger los equipos contra robos, pérdidas o daños.
- Los accesos a sistemas deben estar resguardados mediante contraseñas seguras y de autenticación.

Responsabilidades del Usuario

Tipo	Responsabilidad
Equipos y dispositivos	• Mantenerlos en buen estado, protegidos de daños, robo o pérdida. • Notificar inmediatamente cualquier incidente o anomalía.
Medios de almacenamiento	• Prohibido el uso de USB o dispositivos extraíbles. • No almacenar información institucional en dispositivos personales o no autorizados. • Toda información debe gestionarse mediante sistemas corporativos autorizados (servidores, nube segura, plataformas internas).
Acceso a sistemas	• Usar credenciales personales, no compartirlas. • Cerrar sesión al finalizar la jornada o cuando el equipo no esté en uso.
Información	• Clasificar, manejar y almacenar la información según la Política de Clasificación de Datos. • Evitar transferencias inseguras.

Reportes de incidentes	Informar de inmediato a la Coordinación de Seguridad cualquier acceso, pérdida, daño o sospecha de compromiso de los activos (ver el Capítulo III. Punto 3.2).
-------------------------------	--

Tabla 16: Responsabilidad del Usuario Sobre el Equipo e Información

Requisitos en Dispositivos Remotos

- Antivirus y EDR activos y actualizados.
- Firewall personal habilitado.
- Cifrado del disco duro (BitLocker, FileVault, etc.).
- Bloqueo automático de pantalla tras inactividad.
- Prohibición de uso compartido de credenciales o sesiones.

Seguridad de los Dispositivos Durante el Traslado

- Los dispositivos deben ser transportados de manera segura y no deben dejarse desatendidos en lugares públicos.
- Se recomienda el uso de maletines o estuches seguros para su traslado.

Recomendaciones al Usuario

- No almacenar contraseñas en navegadores o dispositivos personales.
- Cambiar las contraseñas de acceso remoto cada 90 días o cuando se sospeche compromiso.
- Desconectarse de la VPN al finalizar la sesión laboral.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Notificar de inmediato al área de Seguridad cualquier comportamiento inusual o sospechoso.
- No utilizar USBs ni otros medios extraíbles para almacenar información institucional.

Responsabilidades de la Organización

- Proveer equipos, software y medios de almacenamiento seguros y actualizados.
- Establecer políticas, procedimientos y capacitación sobre el uso responsable de los equipos e información.
- Gestionar la recuperación y respaldo de la información crítica.

Registro y Seguimiento

- Mantener un registro de asignación de equipos y medios de almacenamiento por usuario.
- Todos los incidentes de pérdida, daño o acceso indebido se registrarán y analizarán de acuerdo con el *Capítulo III. Gestión de Incidentes de Seguridad*.

Capítulo V.

Seguridad Física y Ambiental

5.1 Zonas de Seguridad para Almacenamiento de Información

La protección de la información crítica y la infraestructura de la empresa es fundamental para garantizar su continuidad operativa y la seguridad de los datos sensibles. Para lograr esto, se implementan medidas de seguridad tanto físicas como digitales que se distribuyen de acuerdo con el tipo de información y los espacios que requieren protección. A continuación, se detallan las medidas de seguridad aplicadas en diferentes áreas clave de la empresa.

- Seguridad en archivos digitales. Se implementa para proteger la información sensible y garantizar su integridad y disponibilidad, evitando accesos no autorizados, pérdidas de datos o filtraciones.
- Seguridad en áreas físicas restringidas. Se hace para controlar el acceso a espacios críticos y evitar que personas no autorizadas manipulen o roben información confidencial o recursos importantes.
- Seguridad en documentos físicos importantes y archivos muertos. Se toma esta medida para proteger documentos clave contra el robo, la pérdida o la manipulación no autorizada, asegurando su integridad y confidencialidad.
- Seguridad en salas protegidas. Se implementa para resguardar información crítica y confidencial durante reuniones estratégicas, evitando filtraciones o accesos no autorizados que puedan comprometer la empresa.
- Seguridad en SITE (centro de datos). Se hace para proteger la infraestructura tecnológica vital, evitando ciberataques, fallas en el

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

sistema o pérdida de datos críticos mediante un acceso controlado y la protección de los sistemas.

- Seguridad en áreas de entrega y envío. Se establece para prevenir robos, pérdidas o manipulaciones indebidas de mercancía, asegurando que los productos lleguen a su destino de forma segura y bajo un control adecuado.

Medidas de Protección por Departamento

Para facilitar la identificación y mitigación de riesgos en la protección de la información y los activos críticos, se ha desarrollado una matriz de gestión de riesgos de seguridad física y digital. A continuación, se presenta la clasificación de la información por departamento, incluyendo medidas de seguridad física y digital, así como restricciones adicionales:

5.1.1. Departamento de Recursos Humanos

Área Protegida	Medidas de Seguridad	Descripción	Restricciones Adicionales
Documentos Físicos Importantes	 Archivadores y cajas de seguridad con llave.  Control de copias e impresión.  Identificación con sellos de seguridad.	Expedientes de personal, contratos, registros de asistencia, normativas internas. Control de acceso a documentos críticos para evitar filtraciones.	 Prohibido tomar fotografías o escanear sin permiso.  Acceso restringido a expedientes personales.  Todo documento debe devolverse a su ubicación asignada.
Elaboro Nombre firma y puesto: Alexander Ávila / TI		Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta

	 Digitalización y respaldo en servidores.		
Archivos Digitales	 Cifrado de documentos sensibles.  Control de acceso por permisos y roles.  Registro de modificaciones y accesos.  Auditorías periódicas.  Respaldo automático en servidores.	Datos de empleados, contratos digitales, informes de evaluación de desempeño. Control sobre el acceso a la información, solo personal autorizado tiene acceso.	 Eliminación restringida.  Prohibido el almacenamiento en dispositivos personales.

Tabla 17: Medidas de Protección en el Departamento de RH

5.1.2. Departamento de Nómina

Área Protegida	Medidas de Seguridad	Descripción	Restricciones Adicionales
Nómina y Registros de Salarios	 Almacenamiento seguro de documentos relacionados con	Los registros de nómina, pagos y deducciones de los empleados,	 No se permite la visualización o impresión sin autorización

	salarios.  Control de acceso mediante permisos exclusivos.	accesibles solo para personal autorizado.	registrada.  Eliminación restringida sin autorización.
Archivos Físicos de Nómina	 Archivadores y cajas de seguridad con llave.  Control de copias e impresión.  Identificación con sellos de seguridad.	Los archivos físicos que contienen la nómina de los empleados, accesibles solo a personal autorizado.	 Prohibido tomar fotografías o escanear sin permiso.  Acceso restringido a documentos de nómina.
Archivos Digitales de Nómina	 Cifrado de documentos sensibles.  Control de acceso por permisos y roles.  Registro de modificaciones y accesos.	Los archivos digitales relacionados con la nómina se cifran para proteger la información confidencial, accesibles solo a personas autorizadas.	 Eliminación restringida.

Tabla 18: Medidas de Protección en el Departamento de Nómina

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

5.1.3. Departamento de Finanzas

Área Protegida	Medidas de Seguridad	Descripción	Restricciones Adicionales
Documentos Físicos Importantes	 Archivadores y cajas de seguridad con llave.  Control de copias e impresión.  Identificación con sellos de seguridad.  Digitalización y respaldo en servidores.	Facturas, recibos, informes fiscales, registros contables. Control de copias e impresión de documentos, solo con autorización para evitar filtraciones.	 Prohibido tomar fotografías o escanear sin permiso.  Acceso restringido a documentos fiscales y financieros.
Archivos Digitales	 Cifrado de documentos sensibles.  Control de acceso por permisos y roles.  Registro de modificaciones y accesos.	Información financiera digital, balances, reportes contables, declaraciones fiscales. Protección mediante cifrado y control de acceso.	 Prohibido el almacenamiento en dispositivos personales.

	 Auditorías periódicas.		
	 Respaldo automático en servidores.		

Tabla 19: Medidas de Protección en el Departamento de Finanzas

5.1.4. Departamento de Tecnologías de la Información

Área Protegida	Medidas de Seguridad	Descripción	Restricciones Adicionales
SITE (Centro de Datos, Servidores, Backup)	 Acceso ultra restringido solo para personal de TI autorizado.  Monitoreo con cámaras de seguridad.  Suministro eléctrico protegido con UPS y generadores.  Control de temperatura y humedad.	Infraestructura de servidores, respaldo de datos, ciberseguridad, dispositivos de almacenamiento. Y control de acceso sólo para personal autorizado.	 Uso de dispositivos personales no permitido.  Revisión de actividad y accesos.

Archivos Digitales	 Cifrado de documentos sensibles.  Control de acceso por permisos y roles.  Registro de modificaciones y accesos.  Auditorías periódicas.  Respaldo automático en servidores.	Base de datos de usuarios, configuraciones de red, documentación técnica. Protegido con cifrado y control de acceso, se realiza auditoría continua.	 Eliminación restringida.  Prohibido el almacenamiento en dispositivos personales.
--------------------	--	---	---

Tabla 20: Medidas de Protección en el Departamento de TI

5.1.5. Departamento de Diseño y Producción

Área Protegida	Medidas de Seguridad	Descripción	Restricciones Adicionales
Documentos Físicos Importantes	 Archivadores y cajas de seguridad con llave.  Control de copias e impresión.	Planos de diseño, especificaciones técnicas de productos, pruebas de calidad, normativas de producción. Acceso solo para personal autorizado,	 Prohibido tomar fotografías o escanear sin permiso.  Todo documento debe devolverse a

Elabora Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

	 Identificación con sellos de seguridad.  Digitalización y respaldo en servidores.	protección mediante cifrado.	su ubicación asignada.
Archivos Digitales	 Cifrado de documentos sensibles.  Control de acceso por permisos y roles.  Registro de modificaciones y accesos.  Auditorías periódicas.  Respaldo automático en servidores.	Archivos de diseño digital, imágenes y videos de productos. Solo personal autorizado tiene acceso.	 Prohibido el almacenamiento en dispositivos personales.

Tabla 21: Medidas de Protección en el Departamento de Diseño y Producción

5.1.6. Departamento de Logística

Área Protegida	Medidas de Seguridad	Descripción	Restricciones Adicionales
----------------	----------------------	-------------	---------------------------

Archivos de Logística (Inventarios, Recepción, Despacho)	 Control de acceso a registros de inventario.  Registro de entradas y salidas.	Información sensible sobre inventarios y gestión de materiales debe ser protegida con acceso controlado y monitoreado.	 Prohibido el uso de dispositivos móviles en áreas de recepción y despacho.  Acceso restringido a personal asignado.
Áreas de Logística (Almacén, Recepción de Materiales, Despacho de Productos)	 Control de acceso.  Cámaras de seguridad en puntos estratégicos.  Registro de material.	Las áreas físicas donde se gestionan inventarios y se realizan envíos deben estar bajo monitoreo constante y control de acceso riguroso.	 Acceso limitado a personal autorizado.  Uso de dispositivos móviles prohibido en áreas críticas.

Tabla 22: Medidas de Protección en el Departamento de Logística

5.1.7. Área de Entrega y Envíos

Área Protegida	Medidas de Seguridad	Descripción	Restricciones Adicionales
Zona de Carga y Descarga	 Registro detallado de mercancías.  Cámaras de	Monitoreo de las actividades de carga y descarga de productos, con supervisión en	 Prohibido el uso de dispositivos móviles en la zona de carga.

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

	seguridad.  Control de acceso al personal autorizado.	tiempo real para evitar robos y pérdidas.	 Acceso restringido al personal autorizado.
Envíos y Recepción de Paquetería	 Verificación de productos antes del envío.  Control de documentación.  Seguridad en áreas de almacenaje.	Control de la documentación y validación de los productos antes de ser enviados, asegurando la correcta entrega y recepción de estos.	 Uso no autorizado de celulares en áreas de envío.  Inspección detallada de mercancías antes del envío.

Tabla 23: Medidas de Protección en el Área de Entregas y Envíos

5.1.8. Áreas de Administración y Gerencia

Área Protegida	Medidas de Seguridad	Descripción	Restricciones Adicionales
Salas Protegidas (Reuniones Confidenciales, Estrategias)	 Acceso restringido solo a personal autorizado.  Insonorización de salas.  Firmas de confidencialidad obligatorias.	Espacios diseñados para proteger reuniones sensibles de negocio, estrategias	 Prohibido el uso de celulares.  No se permite la salida de documentos sin autorización.
Elaboro Nombre firma y puesto: Alexander Ávila / TI		Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta

		financieras, de marketing, etc. Acceso solo con autorización previa.	
--	--	--	--

Tabla 24: Medidas de Protección en el Área de Administración y Gerencia

5.1.9. Archivos Muertos (General)

Área Protegida	Medidas de Seguridad	Descripción	Restricciones Adicionales
Archivos Muertos (Históricos u Obsoletos)	 Archivado en áreas de almacenamiento físico seguro o digitalizado.  Respaldo y acceso restringido.	Archivos obsoletos o que ya no se utilizan, pero que deben ser mantenidos por razones legales o administrativas conforme a las políticas establecidas. Eliminación o archivado seguro con acceso restringido.	 Eliminación solo bajo protocolos y autorización.  Acceso solo para personal autorizado.

Tabla 25: Medidas de Protección en el Área de Archivos Muertos

5.2 Señalética de Seguridad

La señalética de seguridad representa un componente estratégico dentro del sistema integral de gestión de seguridad de la organización. Su objetivo es comunicar, de manera visual, ágil y estandarizada, los mensajes relacionados con la protección del personal, los activos, las instalaciones y la información corporativa.

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

La implementación adecuada de la señalética, tanto en el entorno físico como en el digital, contribuye a la prevención de incidentes, la mitigación de riesgos y el fortalecimiento de una cultura organizacional orientada a la seguridad, la responsabilidad y el cumplimiento normativo.

Señalética de Seguridad de la Información Física

La señalética de seguridad de la información física es un elemento clave dentro del sistema de gestión de seguridad de la información en la organización.

Su objetivo principal es comunicar, de manera rápida y visual, las normas, advertencias y restricciones relacionadas con la protección de los activos de información, evitando accesos no autorizados y minimizando riesgos asociados a la pérdida, alteración o divulgación de información sensible.

La señalética contribuye a:

- Alertar al personal y visitantes sobre áreas con información sensible.
- Recordar procedimientos de seguridad específicos, como restricciones de acceso o manejo de documentos.
- Fortalecer la cultura organizacional de seguridad y cumplimiento normativo.
- Reducir riesgos de incidentes físicos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información.

Colorimetría y Significados

El uso de colores en la señalética no es arbitrario; cada color transmite un mensaje específico y genera una respuesta rápida y efectiva en las personas. Entre los colores más utilizados se encuentran:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Color	Significado	Aplicación	Ejemplos de Señales
Rojo ●	Peligro, prohibición, emergencia	Áreas con documentación confidencial, gabinetes restringidos	“Prohibido ingresar sin autorización”, “Información confidencial — No copiar”
Amarillo ●	Advertencia o precaución	Documentos sensibles, zonas de clasificación o destrucción	“Documento en revisión — Confidencial”, “Área de destrucción de documentos”
Verde ●	Entorno seguro	Archivos guardados correctamente, áreas de resguardo seguro	“Área segura de resguardo”, “Documentos archivados correctamente”
Azul ●	Acción obligatoria	Uso de credenciales, cierre de archivadores	“Use su gafete de identificación”, “Cierre los archivadores al finalizar”
Gris / Negro ●	Información general	Señalización de procedimientos o recordatorios	“Siga el procedimiento de clasificación documental”

Tabla 26: Señalética de Seguridad de la Información Física: Colorimetría y Significados

Para garantizar su eficacia, la señalética debe:

- Estar ubicada estratégicamente en puntos críticos, como accesos a salas de servidores, archivos físicos o áreas de almacenamiento de información sensible.
- Ser clara, legible y estandarizada en toda la organización.

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

- Complementarse con procedimientos internos y capacitación al personal sobre su significado y aplicación.

Tipos de Señalización

Cada tipo de señal tiene un objetivo específico dentro del sistema de seguridad de la información física:

Tipo de Señalización	Objetivo	Ejemplos
Prohibición	Evitar acciones riesgosas que puedan comprometer la información	“Prohibido sacar documentos”, “No fotografiar información”
Advertencia	Alertar sobre riesgos potenciales	“Documento confidencial — No dejar sin supervisión”
Obligación	Garantizar el cumplimiento de políticas internas	“Destruya la información según el protocolo”
Emergencia / Salvamento	Indicar procedimientos a seguir ante incidentes	“Punto de recolección de documentos ante contingencia”
Informativa / Educativa	Reforzar la cultura de seguridad y buenas prácticas	“Área de documentos en resguardo”

Tabla 27: Tipos de Señalización Física

Señalética de Seguridad de la Información Digital

La señalética de seguridad de la información digital es un elemento clave dentro del sistema de gestión de seguridad de la información de la organización.

Su propósito es comunicar de manera visual y rápida alertas, restricciones y procedimientos relacionados con la protección de datos tanto en plataformas

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

digitales, sistemas internos y correos electrónicos corporativos, como en áreas físicas donde se maneja información confidencial (oficinas, servidores, salas de juntas, etc.).

La señalética digital permite:

- Alertar a los usuarios sobre riesgos o acciones prohibidas en sistemas y plataformas digitales.
- Recordar políticas de manejo seguro de información, como contraseñas, acceso a archivos o almacenamiento en la nube.
- Reforzar la cultura corporativa de seguridad y el cumplimiento normativo en entornos digitales.
- Reducir incidentes de seguridad informática y minimizar riesgos asociados a la pérdida, corrupción o divulgación de datos.

Colorimetría y Significados

El uso de colores en la señalética digital facilita la interpretación rápida de los mensajes y la respuesta inmediata de los usuarios. Entre los más utilizados se encuentran:

Color	Significado	Aplicación	Ejemplos de Señales
Rojo ●	Peligro, prohibición, alerta crítica	Accesos restringidos, intentos de intrusión	“Intento de acceso bloqueado”, “Correo sospechoso detectado”
Amarillo ●	Advertencia	Posibles amenazas o riesgos digitales	“Archivo sospechoso”, “Posible phishing”

Verde ●	Entorno seguro	Conexiones cifradas, archivos validados	“Conexión segura (HTTPS)”, “Archivo cifrado”
Azul ●	Obligación	Cumplimiento de políticas de seguridad digital	“Bloquee su sesión”, “Respalde la información periódicamente”
Gris / Negro ●	Información general / educativa	Mensajes de concientización	“Piense antes de hacer clic”, “Revise la política de uso de datos”

Tabla 28: Señalética de Seguridad de la Información Digital: Colorimetría y Significados

Para que la señalética digital sea útil:

- Debe estar presente en interfaces críticas como dashboards, sistemas de gestión de documentos, plataformas de almacenamiento en la nube y aplicaciones corporativas.
- Debe mantener uniformidad en colores, iconografía y tipografía para asegurar reconocimiento inmediato.
- Debe estar acompañada de procedimientos internos y capacitación al personal sobre su significado y aplicación, garantizando que los usuarios sepan cómo reaccionar frente a cada alerta o instrucción digital.

Tipos de Señalización

Cada tipo de señal tiene un objetivo específico dentro del sistema de seguridad de la información digital:

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

Tipo de Señalización	Objetivo	Ejemplos
Prohibición	Evitar acciones inseguras	“No compartir contraseñas”, “Prohibido copiar archivos fuera de la red corporativa”
Advertencia	Alertar sobre posibles riesgos	“Riesgo de malware”, “Archivo de origen desconocido”
Obligación	Cumplimiento de políticas	“Bloquee su sesión antes de retirarse”, “Utilice contraseñas robustas”
Emergencia / Salvamento	Procedimientos ante incidentes	“Reporte inmediato a TI”, “Procedimiento ante incidente de ciberseguridad”
Informativa / Educativa	Fomentar cultura digital segura	“Protege tu información — Piensa antes de hacer clic”

Tabla 29: Tipos de Señalización Física

5.3 Gestión de Visitantes

Registro de Ingresos y Salidas

Registro de Ingreso

Registrar al visitante de manera adecuada y segura, asegurando que toda la información relevante sea capturada de forma precisa para el control de acceso. El registro se realizará principalmente a través del teléfono móvil establecido por la empresa, con el objetivo de facilitar su visita y garantizar el cumplimiento de las normativas internas de la empresa.

Paso	Acción	Responsable	Detalles	Documentos Requeridos
1	Identificación	Visitante	El visitante deberá ingresar sus	Documento

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

	del visitante		datos (nombre, persona a quien visita, empresa u organización proveniente, fecha, hora de entrada y número de gafete) a través de sistema web en el teléfono móvil proporcionado por la empresa.	de identidad
2	Registro de entrada	Sistema automatizado	El sistema digital registrará los datos proporcionados por el visitante en la base de control de acceso de la empresa.	-
3	Entrega de gafete	Anfitrión	Entregar un gafete de visitante, que servirá como acceso a las áreas permitidas.	Gafete

Tabla 30: Registro de Ingreso de Visitantes

Acompañamiento de Visitantes

Asegurar que el visitante sea acompañado de manera adecuada y eficiente hasta la persona o área de destino dentro de las instalaciones, garantizando su seguridad en todo momento. Este acompañamiento debe incluir una orientación clara dentro de las instalaciones y el cumplimiento estricto de los protocolos internos establecidos por la empresa, con el objetivo de preservar la integridad del visitante y asegurar el cumplimiento de las políticas de seguridad y control de acceso.

Paso	Acción	Responsable	Detalles	Documentos Requeridos
------	--------	-------------	----------	-----------------------

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

1	Notificación a la empresa	Sistema automatizado	Informar que el visitante ha llegado y está registrado.	-
2	Acompañamiento del visitante	Anfitrión	Acompañar al visitante hasta el área solicitada, si es necesario, garantizando su seguridad en todo momento.	-

Tabla 31: Acción de Acompañamiento de Visitantes

Registro de Salida

Establecer un proceso estructurado y detallado para el control de la salida del visitante, garantizando que todos los movimientos dentro de las instalaciones sean debidamente registrados. Este proceso debe asegurar que el visitante complete su visita dentro de los tiempos establecidos, realizando una verificación precisa de su salida.

Paso	Acción	Responsable	Detalles	Documentos Requeridos
1	Confirmación de salida	Sistema automatizado	El visitante confirma su salida en la aplicación mediante el teléfono móvil de la empresa, indicando que ha terminado su visita.	Gafete
2	Registro de salida	Sistema automatizado	El sistema registra la hora de salida del visitante automáticamente.	-
3	Recogida del gafete	Anfitrión	El visitante deberá devolver el gafete al finalizar su visita, confirmar la salida en el sistema	Gafete

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

			para desactivar el acceso.	
--	--	--	----------------------------	--

Tabla 32: Registro de Salida de Visitantes

Seguimiento y Control

Asegurar una correcta supervisión y verificación de todos los registros de visitantes mediante un seguimiento periódico, con el objetivo de asegurar una trazabilidad adecuada de cada visita realizada. Este proceso debe garantizar que la información relacionada con los visitantes esté correctamente organizada, actualizada y disponible para su consulta en todo momento, cumpliendo con los estándares internos de control y seguridad establecidos por la empresa.

Paso	Acción	Responsable	Detalles	Documentos Requeridos
1	Verificación diaria	Sistema automatizado	El sistema verificará diariamente los registros de entrada y salida, generando alertas si falta algún dato o si no se realizó correctamente alguna operación.	Registros de visitas
2	Reporte mensual	Supervisor	El sistema generará un reporte mensual detallado de las visitas realizadas, incluyendo datos sobre número de visitantes, duración de las visitas, y otras métricas.	Registros de visitas

Tabla 33: Seguimiento y Control de Visitantes

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

Recomendaciones Adicionales

Implementar un sistema digital que permita realizar todo el proceso de registro y control de acceso desde el teléfono móvil de la empresa. Este sistema debe ser seguro, con autenticación adecuada y almacenamiento cifrado de los datos.

Es imprescindible garantizar que los visitantes sólo accedan a las áreas autorizadas y bajo estrictos controles. El gafete debe ser utilizado para limitar el acceso y asegurar que los visitantes sean acompañados en todo momento en las áreas sensibles.

La información personal proporcionada por los visitantes debe ser tratada con la máxima confidencialidad. Manteniendo medidas de seguridad para proteger dicha información y evitar su divulgación no autorizada, conforme Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

5.4 Medidas de Protección en Dispositivos Móviles

Los dispositivos informáticos móviles, como laptops y teléfonos, así como los dispositivos de almacenamiento móvil, como discos duros y tarjetas SD proporcionados por la empresa son para ser utilizados exclusivamente para actividades laborales exclusivamente dentro de las instalaciones de la empresa, salvo en casos estrictamente necesarios para trabajar desde casa.

Cualquier uso personal de los dispositivos está estrictamente prohibido. Esto incluye no solo el uso para navegar por Internet, sino también para almacenar información personal o instalar aplicaciones no relacionadas con el trabajo.

El uso fuera de la empresa incrementa el riesgo de pérdida o acceso no autorizado a la información. El uso indebido de los dispositivos puede exponer la información de la empresa a riesgos y poner en peligro la seguridad de los datos.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Medidas de Seguridad Requeridas

1: Cifrado de datos:

Todos los dispositivos deben estar protegidos por cifrado de datos para asegurar que cualquier información almacenada en ellos esté protegida en caso de pérdida, robo o acceso no autorizado. Esto incluye tanto los dispositivos de almacenamiento, así como los dispositivos móviles.

2: Protección de acceso:

Estos deben tener una autenticación robusta, que puede ser una contraseña, PIN, o incluso biometría. Para evitar que personas no autorizadas accedan a la información en los dispositivos

3: Marcado de dispositivos:

Todos los dispositivos deben ser marcados con una identificación única (por ejemplo, número de serie) que facilite su localización en caso de pérdida o robo. Esta identificación debe ser clara y visible, pero también discreta, especialmente cuando se utilizan en presencia de clientes o en espacios públicos. El marcado también debe garantizar que el dispositivo pueda ser identificado fácilmente por el personal de TI de la empresa.

A continuación, se presenta una tabla con los aspectos y las medidas que deben seguirse para el uso adecuado de estos dispositivos:

Aspectos	Medidas
Mantener la seguridad de los dispositivos	Utilizar contraseñas fuertes y únicas para acceder a los dispositivos

	• Activar la autenticación de dos factores (2FA) siempre que sea posible. • No compartir contraseñas ni credenciales con otras personas
Instalar y actualizar software de seguridad	• TI debe asegurar de que los dispositivos tengan un software antivirus o antimalware actualizado. • TI debe de realizar actualizaciones de seguridad del sistema operativo y las aplicaciones de manera regular para proteger de vulnerabilidades
Encriptar información	• Proteger la información sensible almacenada en los dispositivos. • Datos cifrados al ser transmitidos a través de redes no seguras
Protección física del dispositivo	• No dejar los dispositivos desatendidos en lugares públicos o de alto riesgo. • Utilizar candados de seguridad o herramientas de rastreo en caso de pérdida o robo del dispositivo.
Realizar copias de seguridad de la información	• Asegurarse de que la información crítica esté respaldada regularmente, para evitar la pérdida de datos importantes debido a fallos en el dispositivo.
Evitar el acceso a información confidencial en redes no seguras	• Evitar conectarse a redes Wi-Fi públicas sin la debida protección.

Tabla 34: Aspectos y Medidas Para el uso Adecuado de los Dispositivos

Cuando los dispositivos no se utilicen, deben ser almacenados en lugares seguros. Esto incluye:

- Oficinas con acceso restringido o armarios cerrados con llave para evitar que los dispositivos queden expuestos o sean fácilmente accesibles para personas no autorizadas.
- Los dispositivos no deben dejarse desatendidos en lugares.

Restricciones de Uso Fuera de la Empresa

En caso de utilizar un dispositivo fuera de la oficina (como el hogar o en un entorno de trabajo remoto), es fundamental cumplir con las directrices establecidas en la *Política de Trabajo Móvil* ([ver página](#)). Esto abarca el uso de redes seguras y la protección física del dispositivo.

Es fundamental que todos los dispositivos móviles de almacenamiento (como discos duros portátiles, tarjetas SD, etc.) estén cifrados para evitar que los datos puedan ser leídos si el dispositivo se pierde o es robado.

Si un dispositivo no puede ser cifrado completamente debido a limitaciones técnicas, deben implementarse otras medidas de seguridad, como:

- Contraseñas adicionales o software de seguridad adicional que protejan el acceso a la información.
- Bloqueo remoto o funciones de auto-borrado en caso de pérdida o robo.

Es responsabilidad de cada empleado asegurarse de que los dispositivos que usa están protegidos adecuadamente. Si un dispositivo no está protegido de acuerdo

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

con las políticas de seguridad de la empresa, el empleado debe notificar al departamento de TI para tomar las medidas necesarias.

En caso de que un dispositivo se pierda o sea robado, es obligatorio informar de inmediato al departamento de TI. Esto permite a la empresa tomar acción acorde al Procedimiento de Pérdida o Robo de Dispositivos Móviles para bloquear el dispositivo, proteger la información y prevenir accesos no autorizados. Es recomendable que los empleados también implementen medidas adicionales, como el uso de software de rastreo para dispositivos.

Desactivación del Uso de Dispositivos

Cuando un empleado termine su relación laboral con la empresa, se deben tomar las siguientes acciones:

- 1) El departamento de RRHH debe de notificar al área de TI de la baja del personal correspondiente, para que ésta recupere todos los dispositivos proporcionados (laptops, teléfonos, discos duros, etc.) inmediatamente.
- 2) Desactivar todos los accesos a sistemas y plataformas de la empresa, como cuentas de correo electrónico y aplicaciones internas.
- 3) Eliminar toda la información confidencial almacenada en los dispositivos de manera segura.
- 4) El empleado debe firmar un recibo de entrega de dispositivos y el departamento de TI debe registrar las acciones realizadas.

5.5 Política de Seguridad Física y Digital

La organización establece esta política con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información, tanto física como

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

digital, cumpliendo con normas internacionales (ISO/IEC 27001, NIST) y regulaciones locales de protección de datos personales. Esta política define procesos claros, acciones obligatorias y prohibiciones para garantizar que la información se maneje de manera segura en todas sus etapas: almacenamiento, transporte, uso, eliminación y recuperación.

5.5.1 Almacenamiento de Activos de Información

Almacenamiento físico seguro

- I. Los documentos físicos deben guardarse en archivadores, lockers o cuartos de archivo con llave o control electrónico.
- II. Solo el personal autorizado puede acceder a estas áreas.
- III. Se debe llevar un registro de quién accede, cuándo y por qué, para trazabilidad y auditoría.
- IV. Prohibido: Dejar documentos sensibles sin custodia, sobre escritorios o en áreas abiertas.

Almacenamiento digital seguro

- I. Los archivos digitales deben guardarse únicamente en:
 - a. Servidores corporativos con control de acceso basado en roles.
 - b. Servicios de nube corporativa autorizados y cifrados.
- II. Prohibido guardar información corporativa en USBs, discos duros externos personales, teléfonos móviles o correos personales.
- III. Aplicar medidas de seguridad como contraseñas robustas, cifrado y autenticación multifactor.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

5.5.2 Disponibilidad de Información

Planificación de respaldos

Establecer un plan de respaldos, definiendo:

- Qué información respaldar
- Frecuencia (diaria, semanal, mensual) según criticidad
- Tipo de respaldo: completo, incremental o diferencial

Implementación de redundancia

Asegurar que los sistemas críticos tengan redundancia física y lógica:

- Servidores replicados en distintas ubicaciones físicas o centros de datos
- Bases de datos configuradas para failover automático

Almacenamiento Seguro de Respaldos

- Guardar copias de seguridad en medios cifrados y seguros, con control de acceso restringido.
- Prohibido almacenar respaldos en dispositivos personales o medios externos no autorizados.
- Registrar responsable, fecha y ubicación de cada respaldo.

Documentación y Registro

Mantener un registro detallado de todos los respaldos realizados, incluyendo:

- Responsable de la copia
- Fecha y hora

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- Tipo de respaldo
- Ubicación de almacenamiento

5.5.3 Traslado de Información

Transporte físico:

- Colocar documentos en sobres sellados o contenedores cerrados y resistentes.
- Etiquetar únicamente con información mínima para identificarlo internamente, evitando exponer datos sensibles.

Transporte digital:

- Cifrar archivos usando estándares seguros (AES 256, PGP, SFTP).
- Utilizar únicamente canales autorizados (VPN corporativa, correo seguro corporativo).
- Prohibido enviar información por dispositivos personales, correos externos o almacenamiento no autorizado.

Custodia durante el traslado

- Designar responsable de custodia que acompañe físicamente la información durante todo el trayecto.
- Registrar hora de entrega y recepción, así como nombres de quienes manipulan la información.
- Para información digital, asegurarse de que la transferencia sea supervisada o monitoreada mediante sistemas corporativos de control.

Entrega y confirmación

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

1. Verificar la identidad del receptor autorizado antes de entregar la información.
2. Registrar la entrega en un log de traslado, indicando fecha, hora, responsable y estado del activo.
3. Confirmar que la información ha sido recibida íntegra y sin alteraciones.

5.5.4 Baja del Personal

El área de Recursos Humanos debe informar a TI y Seguridad Física sobre la fecha de salida del empleado con suficiente antelación. Se debe incluir información sobre los accesos y activos que posee el empleado.

Revocación de Accesos Físicos

- I. El responsable asignado debe recuperar tarjetas de acceso, llaves de oficinas, lockers o equipos con control de entrada.
- II. Desactivar credenciales electrónicas y cualquier permiso de entrada a áreas sensibles.
- III. Registrar la devolución de los activos físicos.

Revocación de Accesos Digitales

- I. Desactivar todas las cuentas corporativas del empleado:
 - a. Correo electrónico, sistemas internos, ERP, bases de datos y aplicaciones de terceros.
- II. Revocar accesos a la nube corporativa y cualquier sistema de almacenamiento de información digital.
- III. Cambiar contraseñas de cuentas compartidas que el empleado pudiera conocer.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

IV. Registrar la acción en un log de seguridad.

V. Prohibido permitir que el acceso permanezca activo después de la baja.

Recuperación de Activos Corporativos

1. Recoger laptops, teléfonos corporativos, USBs, discos duros externos, documentos y cualquier equipo que contenga información de la empresa.
2. Revisar que los equipos devueltos no contengan información almacenada de forma no autorizada (USB, correo personal, nube externa).
3. Registrar cada activo recuperado, su estado y responsable de la entrega.

5.5.5 Eliminación de Información

Propietario del activo y área de Seguridad de la Información debe determinar qué documentos físicos o archivos digitales de acuerdo a la *Política General de Seguridad de la Información* en el apartado Conservación y Disposición de la Documentación Institucional ([ver anexo 9](#)).

Clasificar la información según su nivel de sensibilidad (Confidencial, Interna, Pública) para aplicar métodos de destrucción adecuados.

Método de Eliminación: Información física

- I. Trituración de papel, destrucción de discos, CD, tarjetas y medios magnéticos.
- II. Uso de trituradoras industriales para información confidencial o sensible.

Método de Eliminación: Información Digital

- I. Borrado seguro de archivos y carpetas mediante software que sobrescriba los datos varias veces (método DoD 5220.22-M o equivalente).

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

- II. Destrucción física de discos duros o memorias externas si la información es extremadamente sensible.
- III. Prohibido simplemente eliminar archivos o enviar documentos a la basura sin destrucción segura.

La información debe permanecer bajo custodia de personal autorizado hasta su destrucción final. Manteniendo el registro detallado de cada activo eliminado:

- Tipo de información
- Nivel de sensibilidad
- Método de eliminación
- Fecha de eliminación y responsable de la eliminación

Evitar que terceros no autorizados tengan acceso durante el proceso.

Verificación de la eliminación

Confirmar que la información ha sido irreversible y completamente destruida, verificando que no pueda ser recuperada por métodos convencionales.

Para información digital extremadamente sensible, realizar un doble borrado o destrucción física.

5.5.5 Reparación de Información

Notificar al área de TI para información digital y área de Seguridad de la Información para física la información que ha sido detectada como dañada, archivos corruptos, bases de datos inaccesibles o documentos físicos deteriorados. Para evaluar la crítica de la información y priorizar su reparación según impacto en la operación.

Recuperación: Información Física:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- I. Reparación de documentos dañados mediante técnicas de conservación o reproducción fiel.
- II. Si el documento es crítico, generar duplicado verificado y almacenar de manera segura.

Procedimiento de restauración física

1. Manipular los documentos con cuidado para evitar daños adicionales.
2. Si es necesario, digitalizar documentos físicos para asegurar su preservación futura.
3. Registrar los cambios y ubicación de los documentos restaurados.

Recuperación: Información Digital

- I. Restauración desde copias de seguridad o respaldos recientes.
- II. Uso de herramientas de recuperación de datos certificadas si los respaldos no están disponibles.

Procedimiento de Restauración Digital

1. Localizar el respaldo más reciente y completo de la información afectada.
2. Verificar la integridad del respaldo antes de restaurarlo.
3. Restaurar la información en un entorno controlado y asegurarse de que se recupere completamente.
4. Registrar responsable, fecha y detalles de la restauración.
5. Prohibido restaurar información en dispositivos personales o sistemas no autorizados.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Código: PTI-001

No.
Revisión
y Fecha: **3 / 9.05.2025**

Área responsable:

Tecnología de la información

Áreas involucradas:

Todos

Página

**141 de
193**

Comprobar que la información restaurada es completa, correcta y accesible. Realizar pruebas si corresponde, como abrir archivos, consultar bases de datos o revisar documentos físicos. Por último, documentar el resultado de la verificación:

- Información dañada
- Método de recuperación
- Responsable y fecha
- Resultado de verificación

*Elaboro Nombre firma y puesto:**Alexander Ávila / TI**Reviso Nombre firma y puesto:**Jazmin López / Analista del SGI**Aprobó Nombre firma y puesto:**Florian Hanft / Gerente de Planta*

Capítulo VI.

Gestión de

Accesos

6.1 Identificadores y Autenticación de Acceso

Los identificadores de acceso como lo son tokens, credenciales, RFID de acceso a las instalaciones se otorgan bajo condiciones controladas, a fin de evitar los usos indebidos y las falsificaciones:

- Se definen los requisitos de seguridad para la generación de los medios de identificación (tipo de medio, nivel de seguridad, etc.).
- El medio de identificación se entrega al usuario junto con instrucciones sobre su uso adecuado.
- Se registra la entrega del medio en un sistema de control, incluyendo datos como la fecha de asignación, usuario asignado y tipo de medio.

Políticas de Usuario y Contraseña Seguras para Dispositivos de la Empresa

Cada usuario recibirá un identificador único (ID de usuario) que le permita acceder a los sistemas de información de manera individual y trazable. Los identificadores genéricos o compartidos están prohibidos, salvo en casos excepcionales debidamente autorizados y registrados.

Todas las cuentas deberán protegerse mediante contraseñas que cumplan los siguientes criterios mínimos:

- Longitud mínima de 12 caracteres.
- Combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
- Prohibición del uso de información personal fácilmente deducible (nombre, fecha de nacimiento, etc.)
- No reutilizar contraseñas entre dispositivos o servicios, ni deben ser similares a las anteriores. El sistema prohíbe la reutilización de las últimas 5 contraseñas.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

I. Renovación y bloqueo:

- Las contraseñas deberán renovarse cada 90 días.
- Después de cinco intentos fallidos consecutivos, la cuenta será bloqueada temporalmente, requiriendo intervención de soporte autorizado para su desbloqueo.

Si en algún momento se sospecha que una contraseña ha sido comprometida (por ejemplo, debido a un ataque externo, una fuga de datos, o actividad sospechosa), se debe proceder de manera inmediata al cambio de la contraseña, sin esperar a los 90 días o a la siguiente fecha programada, notificando previamente al área de TI.

II. Gestión de Contraseñas

- Prohibido almacenar contraseñas en dispositivos personales, como teléfonos móviles personales, computadoras portátiles o tabletas que no sean propiedad de la empresa.
- Las contraseñas no deben escribirse en notas físicas, cuadernos, ni ningún tipo de documento impreso que pueda ser accedido por personas no autorizadas.
- Las contraseñas no deben guardarse en archivos de texto sin cifrar, hojas de cálculo o cualquier otra forma de almacenamiento digital no protegido.
- Las contraseñas no deben de compartirse con otros usuarios, ya sea de forma verbal, por escrito o de cualquier otra manera.

Los colaboradores deben utilizar el gestor de Linux para registrar todas sus contraseñas de manera segura siendo aprobado por la empresa. Este gestor tiene las siguientes restricciones y condiciones de uso:

1. El gestor de contraseñas solo debe ser accesible desde dispositivos corporativos, es decir, no se permite su uso en dispositivos personales (como teléfonos móviles personales, computadoras personales, etc.).

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

2. Cada vez que se realice un cambio de contraseña, el gestor debe registrar de manera automática la hora, la fecha y el usuario que realizó el cambio.
3. Los cambios de contraseñas solo podrán realizarse durante el horario laboral (de lunes a viernes, de 9:00 a 18:00, hora local), minimizando el riesgo de cambios maliciosos o imprevistos fuera de este horario.
4. Para cambiar una contraseña, se debe pasar por un proceso de verificación en dos pasos, lo que agrega una capa adicional de seguridad.
5. Para proteger aún más las contraseñas y evitar ataques o intentos maliciosos de acceso, el sistema limita a un máximo de tres intentos fallidos al intentar cambiar una contraseña. Si se superan estos tres intentos fallidos, el acceso será bloqueado temporalmente, lo que evita que personas no autorizadas sigan intentando cambiar las contraseñas de manera repetida.

Recuperación de contraseñas

1. El usuario debe verificar su identidad con un código de verificación enviado a un dispositivo autorizado (correo electrónico previamente proporcionado).
2. La solicitud de cambio de contraseña solo será aprobada si se confirma que proviene del usuario legítimo, validando el código correctamente.
3. Si la identidad es verificada, el usuario podrá restablecer su contraseña, cumpliendo con los requisitos de seguridad establecidos.

Control de Sesiones y Tiempo de Inactividad

Todos los sistemas deberán implementar mecanismos de control de sesión que identifiquen y autenticuen al usuario de manera continua durante el uso del sistema.

Las sesiones de usuario se cerrarán automáticamente después de 15 minutos de inactividad para minimizar riesgos de acceso no autorizado.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

En sistemas con información sensible, se podrá requerir reautenticación periódica para realizar operaciones críticas, incluso durante una sesión activa.

Uso de Autenticación Multifactor

La autenticación multifactor (MFA) combina al menos dos elementos de autenticación de diferentes categorías:

- Algo que sabes: contraseña o PIN.
- Algo que tienes: token físico, aplicación de autenticación o tarjeta inteligente.
- Algo que eres: biometría, como huella dactilar o reconocimiento facial.

MFA será obligatorio para el acceso a sistemas críticos, aplicaciones de administración, correo corporativo y acceso remoto a la red corporativa. Cualquier excepción a la obligación de MFA deberá ser aprobada por el responsable de seguridad de la información y documentada con justificación y plazo limitado.

Cuando un medio de identificación queda obsoleto o ya no es necesario, se implementa un procedimiento de destrucción física o desactivación digital. Se documenta el procedimiento de eliminación/desactivación para garantizar que el medio no pueda ser reutilizado ni comprometido.

En caso de medios físicos (como tarjetas RFID o fichas criptográficas), se asegura que sean destruidos de manera que no se pueda recuperar ninguna información.

6.2 Accesos a Activos en la Red y MFA

La organización reconoce la necesidad de proteger sus activos de información y la infraestructura tecnológica mediante controles de acceso efectivos, asegurando que solo usuarios autorizados puedan interactuar con servidores, aplicaciones y la red corporativa.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Control de Accesos a Sistemas, Aplicaciones y Red

Acceso a sistemas y autenticación:

- I. El acceso a los sistemas de TI estará restringido únicamente a usuarios debidamente identificados y autenticados, garantizando la integridad y confidencialidad de la información.
- II. Los métodos de autenticación se seleccionarán según una evaluación de riesgos, considerando posibles ataques y accesos no autorizados.
- III. Los usuarios deberán emplear contraseñas seguras, y aquellos con privilegios elevados, como administradores o personal de TI, utilizarán procedimientos de autenticación más robustos, como la autenticación de dos factores (2FA) o sistemas de gestión de acceso.

Principio de menor privilegio y permisos:

- I. Todos los usuarios recibirán permisos estrictamente necesarios para el desempeño de sus funciones.
- II. Los accesos administrativos se otorgarán solo a personal autorizado y serán revisados de manera anual.
- III. Los activos dentro de la red corporativa, incluyendo servidores, aplicaciones, bases de datos y otros recursos críticos, estarán identificados y clasificados, y el acceso a ellos será registrado, monitoreado y restringido según el principio de menor privilegio.

Segmentación y control de redes:

- Los recursos críticos se ubicarán en segmentos de red separados, con controles de acceso específicos según el nivel de sensibilidad de la información.
- Los visitantes o dispositivos externos que necesiten conexión a la red serán ubicados en una red aislada, separada de la red corporativa donde operan los empleados, evitando acceso a información confidencial.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Antes de abandonar las instalaciones, todo dispositivo o usuario visitante será desconectado de la red aislada, garantizando que no pueda mantener acceso no autorizado ni comprometer la seguridad de los sistemas corporativos.

Gestión de cuentas:

Los accesos se concederán mediante solicitudes formalizadas y aprobadas por el responsable del área correspondiente.

Las cuentas de usuario inactivas durante más de 30 días serán deshabilitadas temporalmente hasta su reactivación justificada.

Todo acceso remoto debe realizarse a través de canales seguros, como VPN corporativa, y estará sujeto a autenticación multifactor.

Implementación de MFA

No.	Medida de Seguridad	Descripción	Acción Específica
1	Desactivación de cuentas y accesos	TI será el responsable de desactivar o eliminar cuentas de usuario cuando ya no sean necesarias. RRHH informará a TI cuando un usuario deje la organización o si su cuenta ha estado inactiva durante un tiempo prolongado.	Asegurar que no haya accesos no autorizados tras la salida del usuario o si ya no requiere acceso.
2	Acceso restringido según	Los usuarios solo tendrán acceso a la información y sistemas necesarios para realizar sus	Implementar control de acceso según el

	el principio de menor privilegio	tareas. El acceso a otros recursos será restringido por el área de TI.	principio de menor privilegio.
3	Protección de la información sensible	Toda la información sensible deberá estar protegida mediante cifrado, tanto en reposo como en tránsito. Los datos clasificados como sensibles deben ser cifrados utilizando algoritmos robustos. El acceso será restringido y auditado.	Restringir y auditar el acceso a información sensible.
4	Gestión de datos personales	Los usuarios con acceso a datos personales deben cumplir con las regulaciones de privacidad aplicables. El acceso a estos datos estará limitado a los usuarios autorizados, y se exigirá que estos hayan completado el entrenamiento adecuado.	Formación en manejo y protección de datos a los usuarios que acceden a datos personales.

Tabla 35: Implementación de MFA

Registros de Acceso y Monitoreo

Cada formato de registro debe contar con un código identificador único, el cual permite su trazabilidad, control y localización dentro del sistema documental de la empresa.

Este código es indispensable para distinguir el documento de otros registros del área, facilitando su administración, auditoría y actualización.

Ejemplo el código TI-SOX-MFA-001 representa:

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

Elemento	Significado	Descripción
TI	Tecnologías de la Información	Indica el departamento o área responsable del formato.
SOX	Seguridad y Cumplimiento (SOX = Sarbanes–Oxley o Seguridad Operativa Extendida)	Se usa para relacionar el formato con controles o procesos de seguridad y auditoría. En tu caso, puede significar que el documento está ligado a controles de seguridad y cumplimiento (por ejemplo, TISAX o estándares similares).
MFA	Multi-Factor Authentication (Autenticación Multifactor)	Especifica el tema o proceso que documenta el formato.
001	Número consecutivo	Indica que es el primer formato creado para este proceso o tema dentro del área de TI.

Tabla 36: Ejemplo de Código Identificador Único para el Registro de Acceso y Monitoreo: Implementación de MFA

A continuación, se presenta el Formato para el Registro de Acceso y Monitoreo de la Implementación de MFA (Accesos a Activos en la Red y MFA) ([Ver anexo 17](#)) para documentar los accesos a los sistemas, el uso del MFA (autenticación multifactor) y el seguimiento de actividades de seguridad dentro de la red corporativa.

6.3 Gestión de Cuentas de Usuario y Dispositivos

Creación de cuentas

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

El Departamento de Tecnologías de la Información (TI) será el único responsable de la creación de las cuentas de usuario necesarias para el acceso a los sistemas, aplicaciones, redes y dispositivos corporativos.

Cuando un nuevo empleado o contratista ingrese a la organización, o cuando un trabajador cambie de puesto y requiera nuevos accesos, el Gerente de Área o el Responsable de Recursos Humanos deberá enviar una solicitud formal al Departamento de TI para iniciar el proceso correspondiente.

Modificación de cuentas

En caso de cambio de rol, traslado de área o modificación de responsabilidades, el Departamento de TI actualizará los accesos y permisos del usuario, asegurando que se mantengan los privilegios mínimos necesarios para el cumplimiento de sus nuevas funciones.

Desactivación y eliminación de cuentas

Cuando un empleado o contratista finalice su relación laboral con la empresa, el Departamento de TI deberá desactivar su cuenta de manera inmediata, garantizando la suspensión del acceso a todos los sistemas y dispositivos corporativos.

Las cuentas de usuarios inactivos serán eliminadas en un plazo máximo de treinta (30) días posteriores a su salida, incluyendo la revocación de accesos a redes, aplicaciones, dispositivos y recursos digitales de la empresa.

Asignación de Privilegios Mínimos Necesarios

El acceso a los sistemas y recursos de información deberá regirse por el principio de menor privilegio, el cual establece que cada usuario únicamente tendrá acceso a la información y herramientas necesarias para desempeñar sus funciones laborales.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

El Departamento de TI será responsable de:

- Asignar los permisos iniciales de acceso conforme al rol del usuario en la organización.
- Revisar y validar periódicamente los niveles de acceso asignados.
- Registrar todas las modificaciones de privilegios en los sistemas de control interno.

Cualquier solicitud de acceso adicional deberá ser aprobada por el Gerente de Área y posteriormente autorizada por TI, documentando el motivo, alcance y duración del permiso.

Gestión y Control de Dispositivos

Cada usuario contará con un dispositivo corporativo asignado, el cual quedará registrado en el inventario de activos de TI. Este inventario deberá incluir:

Formato para la Asignación de Dispositivos ([Ver anexo 18](#)).

Todos los dispositivos deberán estar integrados bajo el dominio corporativo y gestionados de manera centralizada por el Departamento de TI.

Seguridad de los Dispositivos

Los administradores de TI deberán garantizar que todos los equipos cuenten con:

- Software de seguridad actualizado (antivirus, firewall, etc.).
- Configuraciones de seguridad conforme a los estándares de la empresa.
- Mecanismos de autenticación segura (usuario y contraseña o biometría).

El inventario de dispositivos será actualizado de forma continua y revisado al menos semestralmente para mantener la trazabilidad de los activos asignados.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

6.4 Control de Accesos a Información Física y Digital

Control de Acceso Físico

Las áreas que contengan información confidencial, equipos críticos o infraestructura tecnológica sensible (como salas de servidores, archivos físicos o centros de datos) deberán contar con mecanismos de control físico que limiten el acceso únicamente al personal autorizado.

Estos controles pueden incluir cerraduras con llave, tarjetas electrónicas, sistemas biométricos o dispositivos de autenticación equivalentes.

Registro de Ingreso a Accesos Físicos

[Ver anexo 19](#)

Se deberá mantener un registro actualizado de todos los ingresos y salidas de personal autorizado, así como de visitantes temporales, quienes deberán ser acompañados en todo momento por un responsable del área correspondiente.

Control de Acceso Lógico (Digital)

Autenticación de Usuarios

Todos los accesos a los sistemas, redes, aplicaciones y bases de datos corporativas deberán estar protegidos mediante mecanismos de autenticación de usuario (contraseña, token o autenticación biométrica).

Políticas de contraseñas

Las contraseñas deberán cumplir con la Políticas de Usuario y Contraseñas Seguras para Dispositivos de la Empresa ([ver 6.1 Identificadores y Autenticación de Acceso](#)), la cual establece los requerimientos mínimos de complejidad, longitud y periodicidad de cambio.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Tiempo de Acceso

El tiempo de acceso a sistemas y áreas físicas dentro de una organización es un componente clave de la seguridad, ya que limita la exposición a riesgos internos y externos.

Para garantizar un control eficiente, se establecen tiempos de acceso diferenciados según el tipo de recurso y la sensibilidad de la información o área para equilibrar la disponibilidad necesaria para las operaciones con la protección de los activos críticos.

A continuación, se presentan un ejemplo práctico con estrategias de tiempo de acceso para distintos tipos de recursos:

Tipo de acceso	Estrategia de tiempo	Implementación
Digital (sistemas internos)	Acceso por turno laboral o sesión limitada	Los empleados pueden ingresar a los sistemas internos únicamente durante su horario laboral, de 8:30 a 18:00. Fuera de ese horario, el acceso se bloquea automáticamente. Esto reduce el riesgo de accesos no autorizados en horas no laborables.
Digital (bases de datos críticas)	Acceso temporal por tarea, con expiración automática	Para bases de datos sensibles, se puede generar una contraseña o token temporal válido solo por el tiempo necesario para completar la tarea (por ejemplo, 2 horas). Una vez transcurrido el tiempo, el acceso caduca automáticamente. Esto minimiza la exposición de información crítica.
Físico (oficinas)	Horario laboral	Se recomienda que el acceso a oficinas se limite al horario laboral estándar, de 8:30 a 18:00. Cualquier ingreso fuera de este horario requiere autorización especial y registro. Esto ayuda a controlar el flujo

		de personas dentro de las instalaciones y facilita la detección de actividades anómalas.
Físico (sala de servidores / áreas sensibles)	Acceso programado, solo con registro	Las áreas de alta seguridad, como salas de servidores, deben requerir registro previo, credencial y autenticación biométrica. El tiempo de acceso se puede limitar entre 30 y 60 minutos por sesión, asegurando que las visitas sean controladas, supervisadas y registradas.
Personal externo / auditorías	Acceso por proyecto	Los proveedores, consultores o auditores externos deben recibir acceso únicamente mientras dure la tarea específica. Este acceso debe estar supervisado y registrado, y revocarse automáticamente al finalizar la actividad. Esto garantiza que terceros no mantengan acceso innecesario a sistemas o áreas sensibles.

Tabla 37: Ejemplo: Estrategias de Tiempo de Acceso para Distintos Tipos de Recursos

Auditorías de Acceso

El Departamento de TI llevará a cabo auditorías periódicas de acceso, tanto físicas como digitales, con el fin de:

- Verificar el cumplimiento de las Políticas de Control de Acceso.
- Detectar accesos no autorizados o anómalos.
- Evaluar la eficacia de los mecanismos de seguridad implementados.

Auditoría de Controles Físicos

El cumplimiento de los controles de acceso físico será auditado por un periodo mínimo de 6 meses por el Departamento de Seguridad o TI, verificando la

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

Código: PTI-001

No.
Revisión
y Fecha: **3 / 9.05.2025**

Área responsable:

Tecnología de la información

Áreas involucradas:

Todos

Página

**156 de
193**

efectividad de los mecanismos de control implementados. Cualquier hallazgo relevante será documentado y comunicado al Comité de Seguridad de la Información, quien determinará las acciones correctivas o preventivas correspondientes.

Auditoría de Accesos Digitales

Se mantendrán registros de auditoría (logs) que permitan rastrear las acciones de inicio de sesión, modificaciones, eliminaciones o accesos a información sensible ([ver anexo 20](#)). Estos registros deberán conservarse por un período mínimo de doce (12) meses y estarán sujetos a revisión por parte del área de Seguridad de la Información.

*Elaboro Nombre firma y puesto:**Alexander Ávila / TI**Reviso Nombre firma y puesto:**Jazmin López / Analista del SGI**Aprobó Nombre firma y puesto:**Florian Hanft / Gerente de Planta*

Glosario

Ad hoc: Es la creación de algo provisional, que sólo va a servir para un determinado propósito.

Backups (Copias de seguridad): Proceso de duplicar y almacenar información de manera segura para poder recuperarla en caso de pérdida, daño, borrado accidental o fallo del sistema.

Bitácora: Registro ordenado y cronológico en el que se documentan actividades, eventos, observaciones o incidencias relacionadas con un proceso, proyecto o sistema.

BitLocker: Herramienta de cifrado de disco desarrollada por Microsoft que permite proteger la información almacenada en un equipo o unidad de almacenamiento.

CD (Compact Disc): Disco óptico utilizado para almacenar datos digitales, como música, documentos o programas informáticos.

Cifrado: Proceso mediante el cual la información se transforma en un formato ilegible para cualquier persona que no tenga la clave o contraseña adecuada para descifrarla.

DVD (Digital Versatile Disc o Digital Video Disc): Disco óptico similar al CD, pero con mayor capacidad de almacenamiento, que varía entre 4.7 y 8.5 gigabytes (GB).

Esporádica: Es algo ocasional, no tiene un vínculo estrecho con un acontecimiento pasado ni es su consecuencia; tampoco continúa desarrollándose en el futuro.

INAI: Es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México. Garantiza que los ciudadanos puedan acceder a información pública y proteger sus datos personales.

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

Incineración de documentos: Método de eliminación total de documentos mediante su quema controlada, reduciéndolos a cenizas para impedir cualquier posibilidad de recuperación.

Información Pública: Datos o documentos que pueden ser divulgados sin restricciones, ya que su difusión no representa riesgo para la organización ni para las personas.

Información Interna: Información destinada exclusivamente al uso dentro de la organización. No debe divulgarse fuera sin autorización, aunque su exposición no causaría daños graves.

Información Confidencial: Datos cuyo acceso está limitado a personal autorizado, ya que su divulgación podría generar perjuicios a la organización, clientes o empleados.

Información Restringida: Información de máxima sensibilidad, cuyo acceso está estrictamente limitado. Su divulgación no autorizada podría causar daños graves o críticos a la organización.

Inspección In Situ: Es un proceso de evaluación que se realiza en el lugar donde se llevan a cabo las operaciones, con el fin de verificar el cumplimiento de normativas y la efectividad de los sistemas implementados.

Kaspersky: es una empresa especializada en ciberseguridad y desarrolladora de software antivirus y de protección informática.

Memoria USB: Dispositivo de almacenamiento portátil que permite guardar, transportar y transferir información digital entre computadoras y otros dispositivos.

MFA (Multi-Factor Authentication): Método de autenticación que requiere más de un factor para verificar la identidad de un usuario

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Señalética: Conjunto de señales visuales que indican restricciones, advertencias y permisos en áreas específicas para garantizar el cumplimiento de políticas de seguridad.

S/MIME (Secure/Multipurpose Internet Mail Extensions): Estándar de seguridad para el correo electrónico que permite cifrar y firmar digitalmente los mensajes enviados.

Triturado de documentos: Proceso físico mediante el cual los documentos en papel son desmenuzados o cortados en pedazos pequeños utilizando una trituradora, con el fin de evitar su reconstrucción o lectura.

UMA (Es la Unidad de Medida y Actualización en México): Se utiliza como referencia para calcular obligaciones, pagos, multas y prestaciones, en lugar de usar el salario mínimo, para que los valores no se vean afectados por cambios en los salarios.

VPN (Virtual Private Network o Red Privada Virtual): Es una tecnología que permite crear una conexión segura y cifrada entre tu dispositivo (computadora, teléfono, etc.) e internet.

Fuentes de Información

Atico34, F. (s.f.). *Protección de datos*. Obtenido de Reglamento general protección de datos: <https://protecciondatos-lopd.com/empresas/rgpd-reglamento-general-proteccion-datos/>

Consejo Nacional de Ejecutivos en Logística y Cadena de Suministro, A.C. (4 de marzo de 2025). Obtenido de <https://conalog.org.mx/noticias/industria-automotriz-mexicana-en-2025-cifras-competitividad-y-desafios/>

Consulting, A. (2025). *New VDA ISA 6.0 Version for TISAX*. Obtenido de <https://www.ariolconsulting.com/en/new-vda-isa-6-0-version-for-tisax/>

ENX Association. (2024). Obtenido de TISAX – Trusted Information Security Assessment Exchange: FAQs and Governance.: <https://portal.enx.com/en-us/TISAX/faqs/>

Europea, U. (3 de marzo de 2025). *Protección de Datos conforme al reglamento RGPD*. Obtenido de https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Fernández, M. (17 de julio de 2025). *ISO:9001 Norma de la gestión de calidad*. . Obtenido de <https://plannfocus.com/iso-9001-resumen-completo-de-la-norma-de-gestion-de-calidad/>

Gestión de la calidad en la automoción. (s.f.). Obtenido de La IATF 16949:2016: <https://www.nqa.com/es-mx/certification/standards/iatf-16949#:~:text=LalATFesungrupodefabricantesautomovil%C3%ADsticosysusrespectivasasociacionescomerciales,formadaparaproporcionarunacalidadmejoradaalosproductosautomovil%C3%ADsticosanivelmundial.Todaslaso>

Código: PTI-001

No.
Revisión
y Fecha: **3 / 9.05.2025**

Área responsable:

Tecnología de la información

Áreas involucradas:

Todos

Página

**161 de
193**

ISO 9001:2015 Sistemas de gestión de calidad. (2021). Obtenido de
<https://www.iso.org/es/contents/data/standard/06/20/62085.html>

Legal, E. (2025). *Despacho de Abogados.* Obtenido de
<https://elanlegal.com.mx/normatividad-empresarial/#:~:text=La%20normatividad%20empresarial%20se%20define,relaci%C3%B3n%20entre%20todas%20sus%20%C3%A1reas.>

Igec: ISO/IEC 27001. (s.f.). Obtenido de La Norma Clave para la Seguridad de la Información: <https://lgec.com.mx/iso-iec-27001-la-norma-clave-para-la-seguridad-de-la-informacion>

Verband der Automobilindustrie (VDA). (2016). Obtenido de Recommendation on Information Security (VDA ISA).: https://www.vda.de/de/themen/digitalisierung/daten/informationssicherheit?utm_source=chatgpt.com

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

Anexos

1. Proceso de Certificación IATF 16949: 2016

PROCESO DE CERTIFICACIÓN IATF 16949: 2016

1. Solicitud de presupuesto

Deberá rellenar un formulario de solicitud (QRF) para que NQA pueda entender su empresa, su complejidad y sus requisitos.

2. Auditoría

La auditoría consta de dos visitas obligatorias que forman la auditoría de certificación inicial. Tenga en cuenta que debe ser capaz de demostrar que su sistema de gestión ha estado plenamente operativo durante un mínimo de 3 meses y que ha sido sometido a una revisión por la dirección y a un ciclo completo de auditorías internas.

*Nota: puede haber requisitos adicionales para algunas de las normas más técnicas.

3. Auditoría de certificación inicial: Fase 1

El objetivo de esta auditoría es confirmar que su organización está preparada para la evaluación completa. Esta evaluación tendrá lugar en el centro de su sistema de gestión (normalmente la sede central) y será una auditoría de revisión documental.

Durante la fase 1, su auditor:

- Confirmará la exactitud de la información que ha presentado durante el proceso de solicitud.
- Confirmará que el sistema de gestión se ajusta a los requisitos de la norma.
- Confirmará el estado de implantación de su(s) sistema(s) de gestión.
- Confirmará el alcance de la certificación.
- Verificará la evaluación del cumplimiento legal.

El resultado de la fase 1 será:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Un informe que identifique las áreas de preocupación (AOC) que, si no se abordan, podrían plantearse como no conformidades en la auditoría de fase 2.
- La programación de la fase 2.
- Un plan de auditoría para la fase 2.

2. Auditoría de certificación inicial: Fase 2

El objetivo de esta auditoría es confirmar que el sistema de gestión se ajusta plenamente a los requisitos de la norma elegida en la práctica. Si realiza trabajos in situ o tiene más de un lugar que desea incluir en el alcance de su certificación, el auditor también tendrá que auditar estas actividades o lugares.

Durante la fase 2, su auditor:

- Documentará la conformidad del sistema con la norma mediante pruebas objetivas.
- Realizará auditorías por muestreo de los procesos y actividades definidos en el alcance de la certificación.
- Visitará cualquier ubicación remota, sitios adicionales o actividades remotas para evaluar la eficacia del sistema de gestión fuera del sitio
- Informará de cualquier no conformidad u oportunidad de mejora
- Elaborará un plan de mantenimiento y acordará una fecha para el primer mantenimiento.

Si el auditor identifica alguna no conformidad mayor, la certificación no podrá emitirse hasta que se adopten y verifiquen las medidas correctivas. Los requisitos de acreditación estipulan que, si esto no se completa en un plazo de 6 meses, no se puede recomendar la certificación sin una nueva auditoría de fase 2.

Este requisito se extiende a cualquier no conformidad relativa a los procesos de auditoría interna o de revisión de la gestión específicamente para la ISO 27001. La certificación no puede ser emitida para la norma ISO 27001 hasta que haya pruebas suficientes para demostrar que las disposiciones de revisión por la dirección y las auditorías internas del SGSI se han implementado, son eficaces y se mantienen.

3. Certificación

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmín López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

Si supera la auditoría con éxito, se determina que sus operaciones y procesos cumplen con el alcance de certificación dentro de la norma o normas aplicables. En consecuencia, se toma una decisión de certificación y, si es positiva, NQA emitirá el certificado correspondiente, la cual le permitirá promocionar su certificado.

¿Cuánto tiempo es válida la certificación?

Una vez obtenida la certificación, se emitirá un certificado que tendrá una validez de 3 años. Se mantiene mediante auditorías de mantenimiento anuales (auditorías parciales) y una auditoría de recertificación cada 3 años (auditoría completa del sistema).

Las auditorías de mantenimiento se realizan anualmente para garantizar que el cumplimiento de la(s) norma(s) elegida(s) se mantiene a lo largo del ciclo de certificación de tres años.

La frecuencia y la duración del mantenimiento dependen de factores como:

- Tamaño y estructura de la organización.
- Complejidad y riesgo de las actividades.
- Número de normas de sistemas de gestión incluidas en el ámbito de la certificación.
- Número de centros incluidos en el ámbito de la certificación.

Durante la auditoría de mantenimiento debe demostrar la mejora continua. Este es un requisito fundamental de todas las normas ISO y algo de lo que NQA siempre apuesta.

¿Qué pasa si la empresa sufre algún cambio?

Se ofrece todas las opciones para cambiar y adaptar su alcance de certificación/normas/sistema de gestión para que se ajuste a los requisitos de su empresa. El enfoque de colaborativo de certificación está diseñado para que su programa de certificación se adapte a los requisitos de su empresa, y no al revés.

¿Debo contratar a un consultor?

Los consultores profesionales pueden ayudarle a evaluar sus procesos actuales y orientarle en las áreas en las que puede haber problemas que deban abordarse antes de la auditoría de certificación. La contratación de un consultor no es un

requisito para la certificación, pero sirve como recurso adicional y como garantía de que su proceso de certificación tendrá éxito.

2. Proceso de Certificación TISAX

PROCESO DE CERTIFICACIÓN TISAX

1. Preparación (Autoevaluación):

- Primer Paso: Realiza una autoevaluación exhaustiva de tu empresa utilizando el catálogo VDA-ISA 6.0.
- Identifica Brechas: Detecta las no conformidades y crea un plan de acción para corregirlas.

2. Registro en el Portal ENX:

- Insíbete: Regístrate en la plataforma ENX, el organismo que administra TISAX.
- Define tu Alcance: Selecciona el alcance de tu evaluación, los objetivos de seguridad y los socios con los que compartirás los resultados.

3. Auditoría y Niveles de Evaluación:

- Selecciona un proveedor de auditoría acreditado por ENX.
- El nivel de evaluación determinará el tipo de auditoría:
 - Nivel 2 (AL 2): Auditoría remota. Se revisan documentos y se realizan entrevistas virtuales.
 - Nivel 3 (AL 3): Auditoría exhaustiva in situ. Además de la revisión de documentos, un auditor visita físicamente tus instalaciones.

4. Plan de Acción Correctiva y Cierre:

- Si hay hallazgos en la auditoría, debes implementar un plan de acción para corregirlos.
- El auditor verificará la implementación de las acciones correctivas en un seguimiento.

5. Obtención de la Etiqueta y Publicación:

- Una vez superada la evaluación, el proveedor sube el informe al portal ENX.
- Tu empresa recibe las etiquetas TISAX (por ejemplo, “Protección de la Información Confidencial”).
- Finalmente, decides con qué socios de la industria compartir los resultados.

¿Cuánto dura la certificación?

La etiqueta TISAX es válida por tres años.

Idioma: VDA-ISA 6.0 ha establecido el inglés como idioma de trabajo principal.

Se publicó en octubre de 2023 y es la base obligatoria para todas las nuevas evaluaciones solicitadas a partir del 1 de abril de 2024.

Si existen discrepancias en otras traducciones, la versión en inglés prevalecerá.

3. Proceso de Certificación ISO 9001**PROCESO DE CERTIFICACIÓN ISO 9001****Paso 1: Diagnóstico y planificación estratégica**

Actividades principales del diagnóstico:

- Mapeo de procesos actuales: Identificación de todas las actividades que agregan valor.
- Evaluación de cumplimiento: Análisis detallado de cada cláusula de la norma.
- Identificación de brechas: Documentación de deficiencias y oportunidades de mejora.
- Análisis de recursos: Evaluación de capacidades internas disponibles
- Definición del alcance: Determinación exacta de qué incluir en la certificación.
- Cronograma realista: Establecimiento de tiempos para cada fase del proyecto.

La planificación estratégica incluye la formación del equipo de proyecto. Este equipo debe incluir representantes de cada área funcional que esté dentro del alcance de certificación.

Paso 2: Diseño del sistema de gestión de calidad

- Política de calidad: Declaración del compromiso organizacional con la calidad.
- Objetivos de calidad: Metas específicas, medibles y alcanzables.
- Mapa de procesos: Representación visual de todos los procesos y sus interrelaciones
- Manual de calidad (opcional): Documento que describe el alcance y operación del sistema.
- Procedimientos documentados: Instrucciones detalladas para actividades críticas.
- Formatos y registros: Evidencias de la operación del sistema.

Paso 3: Implementación y documentación del sistema

- Capacitación del personal: Entrenamiento en nuevos procedimientos y responsabilidades.
- Despliegue de procedimientos: Puesta en operación de los procesos diseñados.
- Generación de registros: Documentación de evidencias de funcionamiento.
- Medición de indicadores: Seguimiento del desempeño de procesos clave.
- Comunicación interna: Información regular sobre avances y resultados.
- Ajustes y mejoras: Correcciones basadas en la experiencia práctica.

Paso 4: Auditoría interna y mejora continua

La auditoría interna es la oportunidad de identificar y corregir problemas antes de la auditoría de certificación.

Objetivos de la auditoría interna:

- Verificar cumplimiento: Confirmación de que el sistema opera según lo documentado.
- Detección de desviaciones y oportunidades de mejora.
- Análisis de si el sistema logra los objetivos planificados.

Código: PTI-001

No.
Revisión
y Fecha: **3 / 9.05.2025**

Área responsable:

Tecnología de la información

Áreas involucradas:

Todos

Página

**168 de
193**

- Identificación de acciones correctivas y preventivas necesarias.
- Desarrollo de competencias internas de auditoría.
- Preparación del equipo para la auditoría externa.

Proceso de auditoría interna:

- Planificación: Definición de alcance, criterios y cronograma de auditorías.
- Preparación: Revisión de documentación y preparación de listas de verificación.
- Ejecución: Realización de entrevistas, observaciones y revisión de registros.
- Reporte: Documentación de hallazgos y no conformidades identificadas.
- Seguimiento: Verificación de implementación de acciones correctivas.
- Cierre: Confirmación de que las no conformidades han sido resueltas.

Paso 5: Certificación externa y evaluación final

La auditoría de certificación es realizada por un organismo certificador acreditado e independiente. Este proceso tiene dos etapas claramente diferenciadas.

Etapas 1 – Revisión documental:

- Revisión de documentación: Evaluación de políticas, procedimientos y registros.
- Verificación de preparación: Confirmación de que el sistema está listo para auditoría.
- Identificación de aspectos críticos: Determinación de áreas de mayor riesgo.
- Planificación de Etapa 2: Definición del enfoque para la auditoría en sitio.

Etapas 2 – Auditoría en sitio:

- Evaluación de implementación: Verificación de que el sistema opera efectivamente.
- Entrevistas con personal: Confirmación del conocimiento y aplicación de procedimientos.
- Revisión de registros: Análisis de evidencias de funcionamiento del sistema.
- Observación de procesos: Verificación de conformidad con requisitos documentados.

*Elaboro Nombre firma y puesto:**Alexander Ávila / TI**Reviso Nombre firma y puesto:**Jazmin López / Analista del SGI**Aprobó Nombre firma y puesto:**Florian Hanft / Gerente de Planta*

- Reunión de cierre: Presentación de hallazgos y decisión de certificación.

4. Cláusula de confidencialidad y declaración de aceptación

Cláusula de Confidencialidad y Declaración de Aceptación

Prohibición de divulgación no autorizada

Queda estrictamente prohibido que cualquier empleado revele, transfiera o comparta información personal o confidencial de clientes, proveedores o compañeros de trabajo con terceros no autorizados, ya sea por medios físicos, digitales o verbales, sin contar con el consentimiento expreso del titular de los datos o la autorización escrita de la empresa.

El incumplimiento de esta disposición constituye una falta grave a la confidencialidad y una violación a lo establecido por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

Declaración de aceptación

Yo, _____, reconozco haber leído, comprendido y aceptado el contenido de la presente Política General de Seguridad de la Información, comprometiéndome a cumplir con las disposiciones aquí establecidas durante y después de mi relación laboral con la empresa.

Asimismo, declaro estar consciente de que el incumplimiento de estas obligaciones podrá derivar en sanciones conforme al Reglamento Interno de Trabajo y a la legislación aplicable.

Nombre del empleado

Puesto

Firma y fecha

5. Registro de Control Documental

Documento	Código	Versión	Fecha	Responsable	Estado
Política de Contraseñas	POL-SI-01	2.0	01/09/2025	RSI	Vigente
Procedimiento de Respaldo	PROC-SI-04	1.2	12/08/2025	TI	En revisión
Plan de Recuperación	PLAN-SI-03	1.0	22/04/2025	Dirección	Vigente

6. Estructura Documental



Código:	PROC-SI-002
No. Revisión y Fecha:	1.3 / 9.05.2025

Procedimiento	
Procedimiento de Alta y Baja de Usuarios	
Área responsable:	Tecnología de la información
Áreas involucradas:	TI
Página	1 de 1

Objetivo: Establecer el proceso de creación y eliminación de cuentas de usuario para garantizar la trazabilidad y seguridad de accesos.

Alcance.

Responsables.

Descripción del Procedimiento o Política.

Anexos o Formatos.

Historial de Cambios.

Fecha de cambio	Responsable	No. De versión	Observaciones

7. Ejemplo de Registro De Riesgos

Riesgo	Tipo	Causa	Impacto	Probabilidad	Responsable	Mitigación
Fallo de servidor	Tecnológico	Infraestructura obsoleta	Alto	Media	TI	Actualizar servidores y
Elaboro Nombre firma y puesto: Alexander Ávila / TI		Reviso Nombre firma y puesto: Jazmin López / Analista del SGI		Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta		

						respaldos diarios
Error en facturación	Humano	Falta de capacitación	Medio	Alta	Finanzas	Capacitación y doble verificación

8. Guía práctica para la Identificación de Riesgos y Vulnerabilidades

Paso 1: Formar el equipo de riesgos

1. Selecciona responsables de cada área crítica: TI, operaciones, finanzas, legal, recursos humanos.
2. Define roles:
 - Coordinador de riesgos: supervisa todo el proceso.
 - Responsables de área: identifican y reportan riesgos.
 - Analista de riesgos: consolida información y mantiene el inventario actualizado.

Paso 2: Definir el alcance

1. Lista los procesos, sistemas y áreas que se evaluarán primero.
2. Prioriza áreas críticas para la operación y la continuidad del negocio.

Ejemplo:

- Sistemas de información y servidores.
- Procesos financieros y contables.
- Atención al cliente y soporte.

Paso 3: Identificar riesgos

Usa métodos combinados:

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

- Cuestionarios: enviar a responsables de área con preguntas sobre posibles fallas o amenazas.
- Entrevistas: reuniones cortas para profundizar en riesgos críticos.
- Auditorías internas: revisión de procedimientos, registros y sistemas de control.
- Mapeo de procesos: diagramas de flujo para detectar puntos vulnerables.

Paso 4: Registrar los riesgos

Crea un inventario de riesgos usando esta plantilla básica:

I D	Riesgo	Tipo	Causa/Vulnerabilidad	Impacto	Probabilidad	Prioridad	Responsable	Medidas de Mitigación
1	Fallo de servidor	Tecnológico	Infraestructura obsoleta	Alto	Media	Alta	TI	Actualizar servidores y realizar respaldos diarios
2	Error en facturación	Humano	Falta de capacitación	Medio	Alta	Alta	Finanzas	Capacitación y doble verificación de facturas
3	Incumplimiento legal	Legal	Desconocimiento de normativa	Alto	Baja	Media	Legal	Actualización periódica de regulaciones y auditorías internas

Notas:

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

Código: PTI-001

No.
Revisión
y Fecha: **3 / 9.05.2025**

Área responsable:

Tecnología de la información

Áreas involucradas:

Todos

Página

**173 de
193**

- Impacto: Alto / Medio / Bajo según gravedad de consecuencias.
- Probabilidad: Alta / Media / Baja según frecuencia esperada.
- Prioridad: Determinada combinando impacto y probabilidad.

Paso 5: Analizar y priorizar riesgos

Evalúa cada riesgo según impacto y probabilidad.

Clasifica en:

- Alta prioridad: atender de inmediato.
- Media prioridad: planificar acciones correctivas.
- Baja prioridad: monitorear periódicamente.

Paso 6: Definir medidas de mitigación

Para cada riesgo identificado, establece acciones concretas, responsables y plazos.

Ejemplos:

- Actualizar software o infraestructura tecnológica.
- Capacitación periódica del personal.
- Revisiones y controles internos más estrictos.
- Procedimientos documentados y revisados regularmente.

Paso 7: Monitorear y actualizar

- Establece revisiones periódicas (trimestrales, semestrales o anuales).
- Actualiza el inventario ante cambios en procesos, normativas o amenazas externas.
- Comunica los resultados y medidas a todo el personal involucrado.

9. Política General de Seguridad de la Información

Objetivo

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

Establecer las normas, procedimientos y responsabilidades necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información institucional, protegiendo los activos tecnológicos, los sistemas, los documentos y los datos frente a accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas.

Asimismo, definir los tiempos y métodos de conservación de la documentación física y digital de la organización, en cumplimiento con la legislación mexicana aplicable y las normas internacionales de gestión y seguridad de la información.

Alcance

Estas políticas aplican a todos los empleados, contratistas, proveedores y terceros que accedan a los sistemas de información, redes, equipos o datos de la organización, así como a cualquier persona que genere, manipule o custodie documentos institucionales en formato físico o digital.

Definición de Niveles de Acceso Según Roles y Responsabilidades

Los niveles de acceso se asignarán conforme al principio de privilegio mínimo, garantizando que cada usuario solo disponga de los permisos estrictamente necesarios para cumplir sus funciones.

Se establecen tres niveles básicos:

- Nivel 1 – Público: acceso a información de libre consulta.
- Nivel 2 – Interno: acceso restringido a personal autorizado.
- Nivel 3 – Confidencial: acceso exclusivo a personal directivo o responsable de áreas críticas.

Todo acceso será autorizado por el responsable de seguridad informática y documentado en los registros correspondientes. El acceso se revocará de forma inmediata cuando el usuario cambie de rol o finalice su relación laboral o contractual.

Reglas para el Uso de Contraseñas, Dispositivos y Redes

- Las contraseñas deben:

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Contener al menos 8 caracteres, incluyendo mayúsculas, minúsculas, números y símbolos.
 - Ser cambiadas cada 90 días o cuando se sospeche de una posible vulneración.
 - No compartirse bajo ninguna circunstancia.
- Los dispositivos corporativos (computadoras, tablets, teléfonos) deben:
 - Estar protegidos mediante contraseñas o bloqueo biométrico.
 - Utilizar únicamente software autorizado por el departamento de TI.
 - Mantenerse actualizados con los parches de seguridad.
- El uso de redes Wi-Fi públicas o no seguras para acceder a sistemas institucionales está prohibido.
- Todo acceso remoto deberá realizarse mediante VPN corporativa y con autenticación multifactor (MFA).

Procedimientos de Respaldo y Recuperación de Información

- El respaldo de datos deberá realizarse de forma periódica (diaria, semanal o mensual según criticidad).
- Las copias de seguridad se almacenarán en medios seguros, preferiblemente cifrados y en ubicaciones físicas distintas.
- Los procedimientos de recuperación ante desastres deberán ser probados al menos una vez al año.
- La responsabilidad del mantenimiento y verificación de las copias recaerá en el área de sistemas o tecnología.

Lineamientos Sobre el Manejo de Información Confidencial o Sensible

- I. Se considera información confidencial toda aquella relacionada con clientes, empleados, finanzas, proyectos, estrategias o cualquier otro dato protegido por ley o contrato.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- II. La divulgación, copia o transferencia de información confidencial requiere autorización expresa de la dirección.
- III. La información sensible deberá almacenarse cifrada y transmitirse solo mediante canales seguros (HTTPS, SFTP, VPN).
- IV. Todo documento físico o digital que contenga información confidencial deberá ser destruido de forma segura una vez finalice su uso.

Conservación y Disposición de la Documentación Institucional

Con base en las normas ISO/IEC 27001:2022, ISO 15489-1:2016, y la legislación mexicana (Código Fiscal de la Federación, Ley Federal del Trabajo y Código Civil Federal), la empresa deberá conservar su documentación conforme a los siguientes plazos mínimos:

- Documentación contable y fiscal: 5 años, según el Artículo 30 del Código Fiscal de la Federación.
- Documentos laborales y de personal: 5 años después de la terminación de la relación laboral, conforme a los Artículos 804 y 805 de la Ley Federal del Trabajo.
- Documentos legales, societarios y contractuales: 10 años, conforme a los plazos de prescripción del Código Civil Federal.
- Registros de seguridad de la información (logs, auditorías, respaldos): entre 1 y 3 años, conforme al control A.18.1.3 de la ISO/IEC 27001:2022.

Durante su periodo de vigencia, los documentos deberán conservarse de forma que se garantice su autenticidad, integridad, confidencialidad y disponibilidad, tanto en formato físico como digital.

Una vez vencido el tiempo de conservación, los documentos deberán eliminarse de manera segura y verificable:

- Los físicos, mediante trituración o incineración controlada.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

- Los digitales, mediante borrado criptográfico o sobreescritura múltiple, conforme a la ISO/IEC 27040:2015 sobre seguridad en almacenamiento de datos.

Protocolos de Respuesta Ante Incidentes de Seguridad

Ante cualquier incidente (virus, intrusión, fuga de datos, robo de dispositivo, etc.), el usuario deberá notificar inmediatamente al responsable de seguridad o al área de TI.

El equipo de respuesta a incidentes realizará:

1. Identificación del incidente.
2. Contención para evitar su propagación.
3. Erradicación de la causa raíz.
4. Recuperación de los sistemas afectados.
5. Análisis posterior para mejorar las medidas preventivas.

Todos los incidentes deben registrarse en un informe oficial que incluya descripción, impacto, medidas tomadas y recomendaciones.

10. Ejemplo Matriz de Gestión de Riesgos

Para facilitar la identificación y mitigación de riesgos, la siguiente tabla describe los colores a utilizar para la elaboración de la Matriz de Gestión de Riesgos según los niveles de probabilidad y riesgo identificados:

Color de Impacto	Impacto	Probabilidad	Nivel de Riesgo	Descripción
Verde (●)	Bajo	Baja	Bajo	Este color indica que el impacto es bajo, el riesgo es controlado y la probabilidad de que ocurra es mínima. Los riesgos en esta categoría no requieren acciones urgentes, ya que su probabilidad y consecuencias son menores.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

Código: PTI-001

No. Revisión y Fecha: 3 / 9.05.2025

Área responsable:
Tecnología de la información
Áreas involucradas:

Todos

Página
178 de 193

Amarillo (●)	Medio	Media	Moderado	El color amarillo se utiliza para situaciones con un riesgo medio. Aunque la probabilidad de ocurrir no es tan alta, se debe prestar atención a posibles cambios o evoluciones en la situación. Requiere vigilancia para evitar que el riesgo aumente.
Rojo (●)	Alto	Alta	Alto	Este color representa un riesgo elevado. La probabilidad de que ocurra es alta, y su impacto podría ser considerable. Se deben tomar medidas preventivas inmediatas para mitigar el riesgo y evitar consecuencias graves.

Se ha desarrollado un ejemplo de matriz de gestión de riesgos de seguridad de la información por departamento, según su impacto y probabilidad de ocurrencia, estableciendo medidas de control específicas y responsables para su gestión.

Departamento	Riesgo Identificado	Impacto	Probabilidad	Nivel de Riesgo (Alto, Medio, Bajo)	Medidas de Mitigación	Responsable
TI (Tecnologías de la Información)	Ataques cibernéticos (malware, ransomware, phishing)	●	●	●	Implementación de firewalls, antivirus, autenticación multifactor, capacitación en ciberseguridad	CISO / Administrador de Seguridad
	Vulnerabilidades en software utilizado por la empresa	●	●	●	Aplicación de parches de seguridad, pruebas de	Equipo de Desarrollo de Software

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

Código: PTI-001

No. Revisión y Fecha: 3 / 9.05.2025

Área responsable:
Tecnología de la información
Áreas involucradas:

Todos

Página
179 de 193

					penetración periódicas	
	Acceso no autorizado a sistemas internos	●	●	●	Políticas de control de acceso, monitoreo de actividad, auditorías de seguridad	Administrador de Sistemas
Finanzas	Robo de información financiera y datos bancarios	●	●	●	Cifrado de datos, control de accesos, monitoreo de transacciones	Director Financiero
	Errores humanos en el manejo de información contable	●	●	●	Implementación de doble validación, capacitación en gestión documental	Jefe de Contabilidad
Producción y Operaciones	Fallos en la infraestructura tecnológica (servidores, bases de datos)	●	●	●	Implementación de planes de respaldo y recuperación ante desastres	Administrador de Infraestructura TI
	Robo o pérdida de documentos físicos con información técnica	●	●	●	Digitalización de documentos, acceso restringido	Jefe de Producción
Recursos Humanos	Fuga de datos personales de empleados	●	●	●	Restricción de acceso a datos sensibles, protocolos de manejo de	Jefe de Recursos Humanos

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

Código: PTI-001

No. Revisión y Fecha: 3 / 9.05.2025

Área responsable:
Tecnología de la información
Áreas involucradas:

Todos

Página
180 de 193

					información confidencial	
	Suplantación de identidad (phishing) en procesos de contratación	●	●	●	Concientización del personal, verificación en múltiples canales	Reclutador
Ventas y Marketing	Exposición de información de clientes en canales inseguros	●	●	●	Uso de plataformas seguras, cifrado de bases de datos	Director de Ventas
	Publicación de información sensible en redes sociales	●	●	●	Políticas de comunicación corporativa, monitoreo de publicaciones	Gerente de Marketing
Almacén y Logística	Acceso no autorizado a registros de inventario	●	●	●	Implementación de controles de acceso, auditorías frecuentes	Jefe de Almacén
	Robo o extravío de dispositivos con información sobre envíos	●	●	●	Cifrado de datos en dispositivos móviles, uso de aplicaciones seguras	Coordinador de Logística

11. Formato 1: Ejemplo de Registro de Pruebas y Simulacros de Seguridad de la Información

Código del Formato: TI-SEG-PS-001

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

Código: PTI-001

No. Revisión y Fecha: 3 / 9.05.2025

Área responsable:
Tecnología de la información
Áreas involucradas:

Todos

Página
181 de 193
Versión: 1.0

Fecha de Emisión: ____ / ____ / ____

Área Responsable: Tecnologías de la Información

Tipo de Prueba: ☐ Física ☐ Digital ☐ Mixta

Datos Generales

N.º Registro	Fecha de la Prueba / Simulacro	Tipo de Evento	Objetivo de la Prueba	Lugar Sistema Evaluado	Responsable del Ejercicio

Descripción del Escenario

(Describir brevemente el tipo de incidente simulado: pérdida de información, corte eléctrico, intento de intrusión, incendio, etc.)

Actividades Realizadas

Hora	Acción / Actividad Ejecutada	Responsable	Resultado Obtenido
09:00	Se desconecta el servidor de respaldo	TI	Correcto
09:05	Activación de protocolo de recuperación	Equipo TI	Correcto
09:20	Restauración desde copia de seguridad	Administrador TI	Parcial (faltaron archivos 2023)

Evaluación de Resultados

Indicador	Resultado Esperado	Resultado Obtenido	Cumple (Sí/No)	Observaciones / Comentarios
Tiempo máximo de respuesta	≤ 30 min	40 min	No	Se requiere optimizar respaldo automático

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

Código: PTI-001

No. Revisión y Fecha: 3 / 9.05.2025

Área responsable:
Tecnología de la información
Áreas involucradas:

Todos

Página
182 de 193

Comunicación interna	Fluida	Fluida	Sí	—
Seguridad de datos	Sin pérdida	Pérdida parcial	No	Revisar políticas de respaldo

Conclusiones y Recomendaciones

(Anotar observaciones finales y acciones correctivas para fortalecer el plan.)

Firmas de Validación

Elaboró (Responsable del Simulacro)
Revisó (Área de Seguridad / TI)
Aprobó (Dirección o Auditor Interno)

12. Formato 2: Ejemplo de Planificación y Seguimiento de Pruebas / Simulacros

Código del Formato: TI-SEG-PS-002

Propósito: Planificar y registrar las pruebas periódicas del plan de continuidad y recuperación de información.

Año / Período	Tipo de Prueba o Simulacro	Fecha Programada	Fecha Realizada	Frecuencia	Estatus	Responsable	Observaciones
2025	Simulacro de pérdida de datos	15/02/2025	15/02/2025	Anual	Ejecutado	Ana Portillo	Revisión exitosa

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

2025	Simulacro de incendio	10/05/2025	12/05/2025	Semestral	Ejecutado	Seguridad	Coordinación buena
2025	Simulacro de ataque cibernético	20/09/2025	Pendiente	Anual	En planeación	TI	Revisión de protocolo MFA

13. Pasos del Protocolo de Respuesta a Incidentes

Preparación

- Crear un equipo de respuesta a incidentes (Incident Response Team – IRT) con roles claros:
 - Líder del equipo
 - Analista de seguridad
 - Responsable de comunicaciones
 - Soporte TI
- Mantener inventario de activos críticos como lo son servidores, bases de datos, dispositivos, aplicaciones, etc.
- Definir políticas de seguridad ([ver página](#))
- Establecer herramientas de monitoreo y detección: antivirus, firewall, sistemas de detección de intrusos (IDS/IPS).
- Capacitar al personal para reconocer señales de ataque (phishing, ransomware, accesos sospechosos).

Acciones

1. El personal detecta el incidente y notifica inmediatamente al IRT.
2. Registrar fecha, hora, tipo de ataque y sistemas afectados.
3. No intentar resolver el problema sin autorización, para evitar empeorar la situación.

Contención

<i>Elaboro Nombre firma y puesto:</i> Alexander Ávila / TI	<i>Reviso Nombre firma y puesto:</i> Jazmin López / Analista del SGI	<i>Aprobó Nombre firma y puesto:</i> Florian Hanft / Gerente de Planta
---	---	---

1. Desconectar sistemas comprometidos de la red (computadoras, servidores, dispositivos externos).
2. Bloquear cuentas afectadas o sospechosas.
3. Activar medidas de seguridad adicionales (firewall, segmentación de red).
4. Mantener registro detallado de todas las acciones tomadas.

Análisis

1. Identificar tipo de ataque (ransomware, malware, phishing, DoS, intrusión interna).
2. Determinar sistemas, datos y usuarios afectados.
3. Revisar logs y registros de seguridad para rastrear actividad sospechosa.
4. Evaluar la criticidad del incidente para priorizar acciones de recuperación.

Erradicación

1. Limpiar archivos maliciosos o eliminar malware.
2. Aplicar parches de seguridad a sistemas vulnerables.
3. Cambiar contraseñas y credenciales comprometidas.
4. Confirmar que no queden rastros de la amenaza.

Recuperación

1. Restaurar sistemas afectados desde respaldos seguros.
2. Verificar que los sistemas funcionen correctamente y que los datos sean íntegros.
3. Monitorizar los sistemas durante un tiempo para detectar posibles reinfecciones.
4. Informar a la dirección sobre el estado de recuperación.

Comunicación

1. Notificar al equipo de dirección y área legal sobre el incidente.

<i>Elaboro Nombre firma y puesto:</i> <i>Alexander Ávila / TI</i>	<i>Reviso Nombre firma y puesto:</i> <i>Jazmin López / Analista del SGI</i>	<i>Aprobó Nombre firma y puesto:</i> <i>Florian Hanft / Gerente de Planta</i>
--	--	--

2. Informar a los usuarios internos sobre medidas de seguridad (por ejemplo: cambiar contraseñas).
3. En caso de fuga de datos, cumplir con las normativas legales de notificación (según país y tipo de información afectada).

14. Informe Post-Incidente de Seguridad de la Información

Código del Formato: INF-SEG-[Año de emisión - Número consecutivo del informe] (INF → Informe/ SEG → Seguridad)

Versión: 1.0

Fecha de emisión: [dd/mm/aaaa]

Elaborado por: [Nombre / Cargo]

Revisado por: [Nombre / Cargo]

Aprobado por: Comité de Seguridad de la Información

Datos Generales del Incidente

Campo	Descripción
Número de incidente:	[Código asignado por el sistema o bitácora]
Fecha y hora de detección:	[dd/mm/aaaa – hh:mm]
Fecha y hora de resolución:	[dd/mm/aaaa – hh:mm]
Reportado por:	[Nombre del usuario o área]
Área afectada:	[Ej. Finanzas / Sistemas / RRHH]
Tipo de incidente:	[Malware, fuga de información, acceso no autorizado, denegación de servicio, etc.]
Clasificación de severidad:	[Crítico / Alto / Medio / Bajo]

Descripción del Incidente

Describir detalladamente lo ocurrido, indicando el contexto, los sistemas o activos comprometidos, cómo se detectó el incidente y las primeras acciones realizadas.

Código: PTI-001

No.
Revisión
y Fecha: **3 / 9.05.2025**

Área responsable:

Tecnología de la información

Áreas involucradas:

Todos

Página

**186 de
193**

Ejemplo: “El día [fecha] se detectó una conexión no autorizada al servidor de correo electrónico desde una dirección IP externa...”

Cronología de Eventos (Línea de Tiempo)

Fecha / Hora	Evento	Responsable
[dd/mm/aaaa – hh:mm]	[Evento o acción realizada]	[Nombre / Cargo]

Impacto y Alcance

Sistemas o servicios afectados: [Listar]

Datos comprometidos: [Confidencial, restringido, público, etc.]

Impacto en operaciones: [Parcial / Total / Nulo]

Duración de la afectación: [Horas / Días]

Usuarios o clientes afectados: [Cantidad o descripción]

Acciones Realizadas

- Contención. Describa las medidas inmediatas aplicadas para detener la propagación del incidente.
- Erradicación. Indique las acciones realizadas para eliminar la causa raíz o vulnerabilidad explotada.
- Recuperación. Describa el proceso de restauración de sistemas, validación de respaldos y pruebas de funcionamiento.

15. Análisis Post-Incidente**Causa Raíz**

Explique las causas técnicas, humanas o de proceso que originaron el incidente.

Ejemplo: “Se identificó que el servidor afectado no contaba con los parches de seguridad actualizados.”

Evaluación de Controles

¿Los controles de detección funcionaron adecuadamente?

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

Código: PTI-001

No.
Revisión
y Fecha: 3 / 9.05.2025

Área responsable:

Tecnología de la información

Áreas involucradas:

Todos

Página

187 de
193

¿Se siguió el procedimiento establecido?

¿Hubo desviaciones o fallas en la respuesta?

Lecciones Aprendidas

Enumere los hallazgos más relevantes y aprendizajes derivados del incidente.

Plan de Acción Correctiva y Preventiva (CAPA)

Acción	Tipo (C/P)	Responsable	Fecha compromiso	Estado
[Ej. Implementar doble autenticación en acceso remoto]	C	[Nombre]	[dd/mm/aaaa]	[Pendiente / En curso / Cerrada]

Conclusiones

Resumen general del incidente, efectividad de la respuesta y evaluación final del impacto.

Ejemplo: “El incidente fue contenido en menos de 2 horas. No se identificó pérdida de datos; sin embargo, se reforzaron los controles de acceso remoto.”**Anexos**

- Evidencias (logs, capturas, reportes del SIEM, correos).
- Diagramas o mapas de red afectados.
- Actas del Comité de Seguridad.
- Otros documentos de soporte.

Elaborado por**Revisado por****Aprobado por**

Nombre:

Nombre:

Nombre:

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta

Código: PTI-001

No. Revisión y Fecha: 3 / 9.05.2025

Área responsable:
Tecnología de la información
Áreas involucradas:

Todos

Página
188 de 193

Cargo:	Cargo:	Cargo:
Fecha:	Fecha:	Fecha:

16. Formato de Evaluación de Efectividad de la Formación

Empresa: _____

Departamento / Área: _____

Periodo Evaluado: _____

Responsable de Evaluación: _____

Información de la Capacitación

Actividad Curso	/ Frecuencia	Grupo Objetivo	Objetivo de la Capacitación

Método de Evaluación

Criterio Evaluado	Método / Instrumento	Indicadores de Efectividad	Resultado Obtenido (%)	Cumplimiento (Sí/No)
Conocimiento adquirido	Cuestionario / Prueba	≥ 80% respuestas correctas		
Aplicación práctica	Observación / Simulación	Cumplimiento de pasos / procedimientos		
Participación / compromiso	Encuesta / Checklist	Nivel de participación ≥ 85%		
Reducción de incidentes	Auditoría / Registro	Disminución ≥ 10% anual		
Elaboro Nombre firma y puesto: Alexander Ávila / TI		Reviso Nombre firma y puesto: Jazmin López / Analista del SGI		Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta

Código: PTI-001

No.
Revisión
y Fecha: **3 / 9.05.2025**

Área responsable:

Tecnología de la información

Áreas involucradas:

Todos

Página

**189 de
193****Resultados Generales**

Fortalezas Identificadas	Áreas Mejora de	Acciones Reforzamiento Correctivas /

Conclusiones y Recomendaciones

(Breve análisis del impacto de la capacitación, nivel de efectividad global y recomendaciones para próximas sesiones o ajustes al plan de formación).

AprobaciónNombre / Cargo (Responsable del
área)Nombre / Cargo (Encargado de Seguridad de la
Información)_____
Firma y fecha_____
Firma y fecha**17. Ejemplo: Formato para el Registro de Acceso y Monitoreo
de la Implementación de MFA****Código del Formato:** TI-SOX-MFA-001**Versión:** 1.0**Fecha de Emisión:** ____ / ____ / ____**Área Responsable:** Tecnologías de la Información (TI)**Revisión:** ____ / ____ / ____**Elaboró:** _____**Aprobó:** _____

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

Código: PTI-001

No.
Revisión
y Fecha: **3 / 9.05.2025**

Área responsable:

Tecnología de la información

Áreas involucradas:

Todos

Página

**190 de
193****Datos del Acceso**

N.º Registro	Fecha y Hora del Acceso	Usuario / Empleado	ID de Usuario / Correo	Activo o Sistema Accedido	Dirección IP / Ubicación	Método de Autenticación	Estado MFA (Exitoso / Fallido)	Resultado del Acceso (Permitido / Denegado)
001	12/11/2025 08:32	Juan Pérez	jperez@sonavox.com	Servidor de archivos TI	192.168.1.45	Contraseña + Token móvil	Exitoso	Permitido
002	12/11/2025 08:36	María Gómez	mgomez@sonavox.com	Correo corporativo	192.168.1.58	Contraseña + Código SMS	Fallido	Denegado
...	...	...	...	...	...	...	...	...

Monitoreo de Actividad

Fecha de Revisión	Administrador / Auditor	Incidencias Detectadas	Acciones Correctivas / Observaciones	Evidencia Adjunta (Sí/No)	Firma del Revisor
12/11/2025	Luis Martínez	Intentos fallidos consecutivos de acceso a servidor de TI.	Bloqueo temporal de cuenta y revisión de logs.	Sí	
...	...	...	...	...	...

Observaciones Generales

(Espacio destinado para anotar hallazgos relevantes, recomendaciones o eventos inusuales relacionados con la autenticación multifactor o accesos no autorizados.)

Elaboro Nombre firma y puesto: Alexander Ávila / TI	Reviso Nombre firma y puesto: Jazmin López / Analista del SGI	Aprobó Nombre firma y puesto: Florian Hanft / Gerente de Planta
---	---	---

18. Formato para la Asignación de Dispositivos

ID del Activo	Tipo de Dispositivo	Marca y Modelo	Número de Serie / ID Único	Usuario Responsable	Área / Departamento
Número consecutivo o código interno único del equipo.	Especificar el tipo: laptop, PC, teléfono móvil, tableta, impresora, etc.	Identificar el fabricante y modelo del equipo.	Registrar el número de serie o etiqueta de inventario del dispositivo.	Nombre completo del colaborador al que se le asigna el dispositivo.	Departamento donde el usuario desempeña sus funciones.
Fecha de Asignación	Día, mes y año en que se entrega el equipo.				
Fecha de Devolución (si aplica)	Día, mes y año en que el dispositivo es devuelto o reasignado.				
Estado Operativo del Equipo	Seleccionar una opción: <i>Operativo / En reparación / Dañado / En baja / En actualización.</i>				
Condiciones al Entregar / Devolver	Describir el estado físico (ejemplo: "sin daños", "con rayones leves", "batería reemplazada").				
Responsable de TI / Entrega	Sello de TI		Firma del Usuario Responsable		
Nombre y firma de la persona del área de TI que entrega o recibe el equipo.			Firma del colaborador que recibe o devuelve el dispositivo.		

19. Registro de Ingreso a Accesos Físicos

Nº	Nombre Completo	Tipo de Persona (Empleado / Visitante / Proveedor)	Área a la que Accede	Nivel de Restricción	Motivo del Ingreso	Hora de Ingreso	Hora de Salida	Autorizado por	Firma
1				●/●/●/●/					

20. Registros de Auditoría (logs)

Campo	Descripción / Instrucción de llenado
ID de Registro	Número consecutivo único asignado automáticamente o manualmente.
Fecha y Hora del Evento	Indicar el momento exacto en que ocurrió la acción (formato: DD/MM/AAAA HH:MM:SS).
Usuario / ID de Usuario	Nombre o código del usuario que realizó la acción.
Departamento / Área	Área o departamento al que pertenece el usuario.
Dirección IP / Dispositivo	Dirección IP o identificador del dispositivo desde el cual se realizó la acción.
Tipo de Acción	Seleccionar una de las siguientes opciones: • Inicio de sesión / cierre de sesión • Creación • Modificación • Eliminación • Acceso a información sensible
Descripción Detallada del Evento	Explicar brevemente qué acción se realizó (por ejemplo: "Usuario modificó el archivo de nómina del mes de octubre").
Datos o Archivo Afectado	Especificar el nombre del archivo, módulo o sistema afectado.
Nivel de Sensibilidad de la Información	Seleccionar: ● Pública



MANUAL

Manual de Seguridad de la Información

Código: PTI-001

No.
Revisión
y Fecha: **3 / 9.05.2025**

Área responsable:

Tecnología de la información

Áreas involucradas:

Todos

Página

**193 de
193**

	● Interna ● Confidencial ● Secreta/Restringida
Resultado / Estado	Indicar si la acción fue exitosa o fallida (por error o intento no autorizado).
Responsable de Validación / Revisión	Nombre y cargo del responsable que revisa y valida el registro.
Observaciones / Comentarios	Campo libre para anotar detalles adicionales o medidas correctivas.

Elaboro Nombre firma y puesto:

Alexander Ávila / TI

Reviso Nombre firma y puesto:

Jazmin López / Analista del SGI

Aprobó Nombre firma y puesto:

Florian Hanft / Gerente de Planta