



TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Sistema de gestión de seguridad con estándar ITIL y
Remedy Service Desk para control de cuentas de
correo electrónicos y aplicaciones de red Aliat.

Informe Técnico de Residencias Profesionales

Para obtener el título en:

INGENIERÍA EN SISTEMAS
COMPUTACIONALES

Especialidad

Auditoria en seguridad informática

Presenta:

Eduardo Uriel Junco Ortiz
201920263

Asesor:

Matra. Diana Marisol Prado Oseguera

Coacalco de Berriozábal, Méx. Febrero, 2025

AGRADECIMIENTOS

En primera instancia, quiero agradecer a mi asesora del Tesco, la Maestra Diana Marisol Prado Oseguera, por proporcionarme sus conocimientos a cerca de las auditorias, sus consejos y puntos de vista ayudaron a ampliar los parámetros y las direcciones del estudio que se realizó. La paciencia, dedicación, enfoque y pasión por la especialidad son de las virtudes que me inspiraron a dar lo mejor de mí en el transcurso y desarrollo del proyecto.

A mi asesor Pedro Joaquín Paredes Talavera, quiero agradecerle por la oportunidad de trabajar y sumergirme en un espacio laboral real, además de ser el proveedor de información para desarrollar el proyecto. Su tranquilidad al hablar, la amabilidad con la que trata a su gente y la integración que fomenta a sus empleados son algunos de los rasgos que un buen líder, considero, deben ser parte de un buen jefe.

A mi supervisor Luis Alberto Maldonado Espinosa, quiero agradecerle por la confianza, apoyo y orientación que me brindo para llevar a cabo las actividades tanto de la empresa como del proyecto. Su paciencia al enseñar, el carisma que lo hace destacar en el área y su forma de resolver los problemas fueron de gran ayuda e inspiración en el con prendimiento y desarrollo de nuevas habilidades, sin olvidar la experiencia laboral que me ofreció el realizar diferentes tareas dentro de la empresa.

Por último, quiero agradecer al personal de Mesa de Servicio por mostrarme lo que implica un ambiente laboral sano y brindar sus conocimientos en el área y a mis familiares por el apoyo y las ideas que ayudaron al desarrollo del proyecto.

Atentamente

Eduardo Uriel Junco Ortiz

Estudiante del Tecnológico de Estudios Superiores de Coacalco.

30 abril de 2024

RESUMEN

El siguiente documento se en realizar un análisis de riesgo del sistema Remedy y los usuarios de Outlook 365 de estudiantes en la empresa Red Univercom. La información necesaria para llevar a cabo esta evaluación se recopila mediante una investigación a través de sus páginas oficiales y revisión de las normas internas de la empresa.

Para garantizar un enfoque integral, se utilizan las mejores prácticas establecidas en los libros de ITIL, COBIT 5 y el ISO 17799 con el fin de seguir y brindar las recomendaciones que estos ofrecen al enfoque al valor del servicio a las empresas y a la seguridad y disponibilidad de los sistemas. Además, se llevaron a cabo entrevistas al personal que conforma Mesa y que se encarga de la gestión de los sistemas a evaluar y se crearon cuadros de evaluación de riesgos para identificar las posibles vulnerabilidades y amenazas del área y los sistemas.

El análisis de riesgos permite identificar y valorar las vulnerabilidades potenciales, amenazas y puntos críticos en el área de Mesa de Servicio en conjunto con el sistema Remedy que es con el que opera Mesa, también resalto la falta de disponibilidad y la importancia de los usuarios de Outlook 365 para los estudiantes. Con base en los resultados obtenidos, se proponen soluciones y medidas preventivas y correctivas para mitigar los riesgos identificados y fortalecer a la empresa.

Este proyecto no solo proporciona una visión detallada de la seguridad del sistema, sino que también ofreció recomendaciones específicas para mejorar la resistencia y la integridad del entorno informático de Red Univercom, asegurando así una gestión más eficiente de los servicios y una protección efectiva contra posibles incidentes de seguridad.

ÍNDICE DE CONTENIDOS

AGRADECIMIENTOS	2
RESUMEN.....	3
ÍNDICE DE CONTENIDOS	4
ÍNDICE DE FIGURAS.....	8
ÍNDICE DE TABLAS.....	10
CAPÍTULO I: GENERALIDADES DEL PROYECTO	12
1.1. INTRODUCCIÓN	13
1.2. DESCRIPCIÓN DE LA EMPRESA.....	14
1.2.1. Nombre, razón social	14
1.2.2. Ubicación	14
1.2.3. Organigrama	15
1.2.4. Sector productivo de la empresa.....	16
1.2.5. Misión	16
1.2.6. Visión	16
1.2.7. Filosofía y/o Valores	16
1.2.8. Breve historia de la empresa	17
1.3. DESCRIPCIÓN DEL PUESTO O ÁREA DE TRABAJO.....	18
1.3.1. Agente Mesa de Servicio	18
1.3.2. Funciones principales.....	19
1.3.3. Objetivos.....	19
1.4. PROBLEMA POR RESOLVER.....	20
1.5. OBJETIVOS	21
1.5.1. Objetivo general	21
1.5.2. Objetivos específicos	21
1.6. JUSTIFICACIÓN	22
CAPÍTULO II: MARCO TEÓRICO	23
2.1. Estado del arte.....	24
2.2. Marco conceptual.....	28
2.2.1. Definición de riesgo	28
2.2.2. Definición de amenaza	28
2.2.3. Definición de vulnerabilidad	29
2.2.4. Definición de probabilidad.....	29

2.2.5. Definición de impacto.....	29
2.2.6. Que es y la importancia del análisis de riesgo	29
2.2.7. Tratamiento de los riesgos de seguridad	30
2.2.8. Herramientas y técnicas en el Análisis de Riesgo	31
2.2.8.1 Análisis FODA.....	31
2.2.9. ITSM (Information Technology Service Management)	32
2.2.10. SLA	32
2.2.11. Remedy Service Desk.....	32
2.2.12. HCM (Human Capital Management).....	33
2.2.13. Campus Solution	33
2.3. Marco metodológico.....	33
2.3.1. Tipo de análisis de riesgo	33
2.3.2. Población y muestra	33
2.3.3. Técnicas e instrumentos de recolección de información.....	34
2.3.4. Cuadro Metodológico para el desarrollo del proyecto.....	34
2.3.5. Normas, estándares y librerías utilizadas.	37
2.3.5.1. ITIL v4.....	37
2.3.5.2. COBIT	43
2.3.5.3. ISO 17799 - 2005.....	47
CAPÍTULO III: DESARROLLO.....	54
3.1. Objetivo. Identificar el entorno general de Red Univercom S.C y el papel que desempeña el área de Mesa de Servicios y Centro de Servicios Compartidos para conseguir los objetivos de la empresa.	55
3.1.1. Actividad. Revisar la misión, visión, giro y razón social de la empresa Red Univercom S.C para identificar el propósito y sus objetivos a mediano y largo plazo.....	55
3.1.2. Actividad. Revisar las funciones, procesos, procedimientos, responsabilidades, objetivos, metas y la estructura organizacional del área de Mesa de Servicios y Centro de Servicios Compartidos y como se ligan a los objetivos generales de la empresa.....	61
3.2. Objetivo. Analizar información detallada sobre los servicios que el área ofrece a los usuarios, referente a correo electrónico y Remedy por parte de la empresa.....	66
3.2.1 Actividad. Establecer los formatos de las entrevistas, análisis FODA y matrices de evaluación que se usaran para la recopilación y análisis de la información.....	66
3.2.2. Actividad. Solicitar información acerca de los servicios de correo electrónico y Remedy a través de una entrevista al personal que conforma el área en evaluación	72
3.2.3. Actividad. Analizar las respuestas recopiladas en las encuestas para identificar los riesgos que los participantes perciben en relación con los servicios de correo electrónico y	

Remedy.....	81
3.2.4. Actividad. Identificar posibles vulnerabilidades y amenazas en los servicios de correo electrónico y Remedy a través del análisis FODA.	83
3.3. Objetivo. Emplear un análisis de riesgo según las amenazas y vulnerabilidades encontradas.	87
3.3.1. Actividad. Examinar los riesgos que podrían impedir el normal desenvolvimiento de las operaciones en la empresa.	88
3.3.2. Actividad. Establecer el nivel de la exposición al riesgo	90
3.3.3. Actividad. Compilar las vulnerabilidades y que tan severamente podrían afectarse las operaciones en la empresa	94
3.4. Seleccionar los escenarios probables y de mayor impacto, con el objetivo de abordarlos de manera inmediata.....	97
3.4.1. Resultados.	97
CAPÍTULO IV: RESULTADOS	101
4.1. Proponer las estrategias sustentadas en ITIL 4 y en otros estándares de seguridad; y adaptarlas a las necesidades específicas a los servicios de correo electrónico y Remedy que se ofrecen.....	102
4.1.1. Aplicar las cuatro dimensiones de la gestión de servicios para comprender y abordar diversos aspectos en la prestación de servicios de TI.	102
4.2. Actividad. Recomendar las posibles soluciones a los riesgos a fin de brindar alternativas de solución.....	106
4.2.1. Resultados.	106
4.3. Actividad. Estructurar las propuestas y posibles soluciones con base al modelo de mejora continua ITIL y otros estándares.	112
4.3.1. Propuestas para el riesgo de saturación del uso de la cantidad de cuentas disponibles para usuarios O365	112
4.3.2. Propuesta para el riesgo retraso en los procesos generales y mala imagen con respecto a la operatividad de la empresa.	119
4.3.3. Propuestas para el riesgo la empresa se queda sin servicios para atender solicitudes administrativas y de negocio, servicios financieros, servicios escolares y servicios de TI afectando la operatividad total.	130
4.3.4. Propuestas para el riesgo la empresa atiende solicitudes administrativas y de negocio, servicios financieros, servicios escolares y servicios de TI operando inadecuadamente.	135
4.3.5. Propuestas para el riesgo pérdida y/o robo de información	140
CONCLUSIONES.....	145
COMPETENCIAS DESARROLLADAS.....	146

FUENTES DE INFORMACIÓN	148
ANEXOS.....	150
ANEXO 1. Descripción de puesto del agente de mesa.....	150
ANEXO 2. Política seguridad de la información	155
ANEXO 3. Política control de accesos.	157
ANEXO 4. Política institucional de baja de personal.....	163
ANEXO 5. Política de certificación y recertificación de usuarios en los sistemas informáticos ...	165
ANEXO 6. Acuerdo que establece las bases mínimas de información para la comercialización de los servicios educativos que prestan los particulares.	167
ANEXO 7. Reglamento General para estudios de Licenciatura y Posgrado modalidad: Escolarizada, Mixta y No Escolarizada.....	168

ÍNDICE DE FIGURAS

Figura 1. Ubicación Campus Coacalco	14
Figura 2. Organigrama Campus Coacalco	15
Figura 3. Organigrama de Mesa de Servicio	18
Figura 4. Sistema del valor del servicio (SVS).	38
Figura 5. Las cuatro dimensiones de la gestión de servicios.....	40
Figura 6. Modelo de mejora continua ITIL.....	42
Figura 7. El Objetivo de Gobierno: Creación de Valor.	44
Figura 8. Enfoque de gobierno	45
Figura 9. Catalizadores COBIT.....	46
Figura 10. Personal líder de las áreas.	56
Figura 11. Área administrativa-financiera y capital humano.....	56
Figura 12. Servicios escolares.	57
Figura 13. Vinculación.....	57
Figura 14. Personal educativo.....	58
Figura 15. Mentoría y Retención	59
Figura 16. Admisiones.....	60
Figura 17. Modelo operacional.	62
Figura 18. Catálogo de servicios generales y financieros.....	63
Figura 19. Catálogo de servicios de TI.....	63
Figura 20. Catálogo de servicios de negocio	64
Figura 21. Puestos y personal de Mesa de Servicio	65
Figura 22. Ejemplo de cuadro de análisis FODA.....	69
Figura 23. Ejemplo de cuadro de identificación de riesgos.	69
Figura 24. Ejemplo de evaluación de los riesgos.	69
Figura 25. Ejemplo de probabilidad e impacto	70
Figura 26. Ejemplo de escalas de probabilidad del riesgo	70
Figura 27. Ejemplo de tabla de recomendaciones para la mitigación de riesgos.....	71
Figura 28. Ejemplo de perdidas monetarias y de nivel de servicio	71
Figura 29. Cuadro de propuestas de solución	72
Figura 30. Ejemplo de tabla de especificaciones de los procesos a implementar.	72
Figura 31. Las cuatro dimensiones de la gestión de servicios.....	103
Figura 32. Diagrama de proceso para la eliminación de usuarios O365.....	115

Figura 33. Servicios de Office 365 para estudiantes.....	118
Figura 34. Servicios proporcionados y atendidos por Agentes de Mesa de Servicio.....	120
Figura 35. Servicios atendidos el Gerente de Mesa y el Coordinador de CSC	121
Figura 36. Diagrama de proceso para la notificación y seguimiento de Tickets.....	123
Figura 37. Ejemplo de servidor ProLiant DL360 Gen10	131
Figura 38. Ejemplo de procesador Intel Xeon Gold 5218R.	132
Figura 39. Diagrama de proceso para la capacitación de alumnos del registro y uso de Remedy.	137
Figura 40. Diagrama de proceso para la capacitación de administrativos.....	139
Figura 41. Servicios ofrecidos por TERAMIND	141
Figura 42. Ejemplo de visualización de empleados de TERAMIND	142
Figura 43. Ejemplo de reportes de aplicaciones y sitios web.	142
Figura 44. Ejemplo de reportes de aplicaciones y sitios web.	143
Figura 45. Ejemplo de más tipos de reportes	143
Figura 46. Ejemplo de descripción general de la productividad	144

ÍNDICE DE TABLAS

Tabla 1. Estado del arte	24
Tabla 2. Metodologías para el desarrollo del proyecto	34
Tabla 3. FODA Mesa de Servicio	84
Tabla 4. FODA Servicios de correo	85
Tabla 5. FODA Servicios de Remedy.	86
Tabla 6. Identificación de riesgo 1	88
Tabla 7. Identificación de riesgo 2	89
Tabla 8. Identificación de riesgo 3	89
Tabla 9. Identificación de riesgo 4	89
Tabla 10. Identificación de riesgo 5	90
Tabla 11. Métrica de probabilidad e impacto.....	90
Tabla 12. Tabla de vulnerabilidad 1	91
Tabla 13. Tabla de vulnerabilidad 2	91
Tabla 14. Tabla de vulnerabilidad 3	92
Tabla 15. Tabla de vulnerabilidad 4	92
Tabla 16. Tabla de vulnerabilidad 5	92
Tabla 17. Tabla de vulnerabilidad 6	93
Tabla 18. Tabla de vulnerabilidad 7	93
Tabla 19. Tabla de vulnerabilidad 8	93
Tabla 20. Tabla de vulnerabilidad 9	94
Tabla 21. Tabla de vulnerabilidad 10	94
Tabla 22. Tabla de valoración al riesgo.....	95
Tabla 23. Cuadro de escalas de probabilidad del riesgo.....	96
Tabla 24. Cuadro de pérdidas monetarias.	96
Tabla 25. Recomendaciones para la mitigación de riesgos según ITIL 4 y otros estándares.	98
Tabla 26. Cuadro de propuestas de solución al riesgo 1	107
Tabla 27. Cuadro de propuestas de solución al riesgo 2	108
Tabla 28. Cuadro de propuestas de solución al riesgo 3	109
Tabla 29. Cuadro de propuestas de solución al riesgo 4	110
Tabla 30. Cuadro de propuestas de solución al riesgo 5	111
Tabla 31. Descripción detallada del proceso de depuración de cuentas de correo institucionales de alumnos.	113

Tabla 32. Indicé de matriculación de estudiantes en el ciclo cuatrimestral y semestral actual	117
Tabla 33. Descripción detallada del proceso de notificaciones del estatus de los tickets en espera.	122
Tabla 34. Tabla de comparación de Azure y AWS.....	128
Tabla 35. Comparativa de precios en los servicios de Azure IA y Amazon Lex	128
Tabla 36. Descripción detallada del proceso de capacitación de estudiantes del uso de Remedy.	136
Tabla 37. Procesos para la capacitación de administrativos.....	138

CAPÍTULO I: GENERALIDADES DEL PROYECTO

1.1. INTRODUCCIÓN

El presente trabajo aborda el desarrollo de un análisis de riesgo, el cual se puede definir como un proceso sistemático y estructurado diseñado para identificar, evaluar y comprender los posibles riesgos que pueden afectar a un sistema, proyecto, organización o cualquier entidad. Pretende una identificación exhaustiva de amenazas potenciales, la evaluación de la probabilidad e impacto de dichas amenazas, y la implementación de estrategias para mitigar, transferir o aceptar los riesgos identificados. En este caso, este enfoque ampliado incluye la utilización de diversas herramientas y metodologías, como la revisión de normativas y estándares, la realización de entrevistas con partes interesadas, la recopilación de datos mediante investigaciones, y la referencia a frameworks como ITIL, COBIT 5 y ISO 17799.

Este análisis de riesgo busca identificar las vulnerabilidades de Mesa de Servicio, el sistema Remedy y los servicios de Outlook 365 actuales con ayuda del análisis FODA, priorizar las vulnerabilidades que tengan la mayor probabilidad de suceder junto con el mayor grado de impacto en la operatividad que puede causar a la empresa. Mediante una valoración se clasificarán en orden de prioridad las vulnerabilidades identificadas y se realizarán las propuestas de solución.

Posteriormente haciendo uso de un cuadro de perdidas es como se escala las perdidas monetarias y de valor a los servicios que ocasionan las vulnerabilidades, además, en base a las diferentes vulnerabilidades, amenazas y riesgos se harán recomendaciones que las guías y estándares proponen para mitigar perdidas y asegurar los sistemas de TI para posteriormente proponer soluciones que pueden ser temporales o bien una forma definitiva de contrarrestar las vulnerabilidades en base a las recomendaciones.

Este proyecto se limita a trabajar con los sistemas de Remedy y los servicios de Outlook 365, Red Univercom cuenta con más sistemas de trabajo, sin embargo, los antes mencionados son con los que más interacción e influencia tiene Mesa de Servicio, con el resto de los sistemas se tiene una interacción limitada reportar y solucionar problemas técnicos para los usuarios solicitantes.

1.2. DESCRIPCIÓN DE LA EMPRESA

1.2.1. Nombre, razón social

Red Univercom.

1.2.2. Ubicación

Av. Zarzaparrillas 85, Villa de las Flores, 55700 San Francisco Coacalco, Méx.



Figura 1. Ubicación Campus Coacalco.

(Fuente: Elaboración propia).

1.2.3. Organigrama

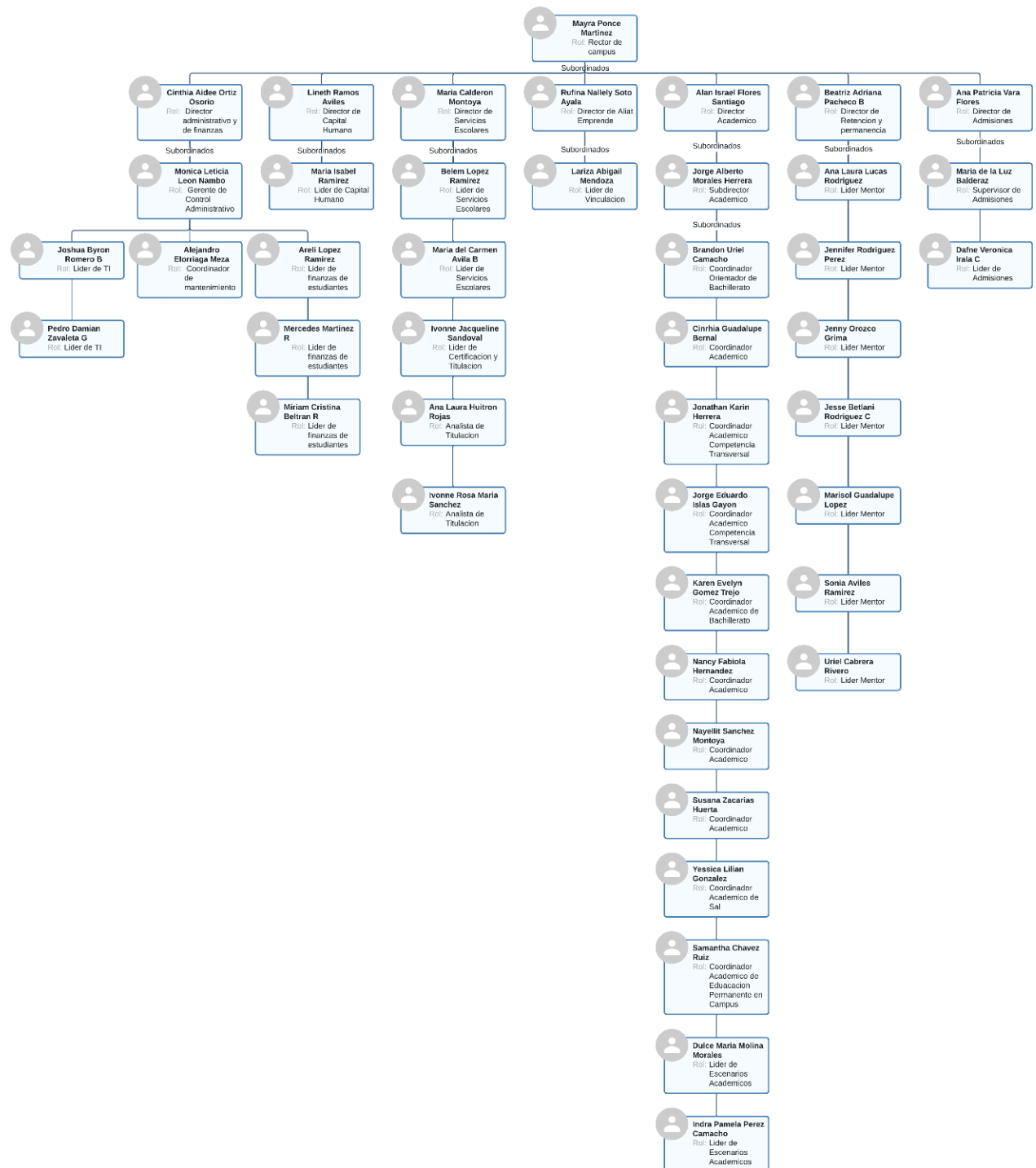


Figura 2. Organigrama Campus Coacalco.

(Fuente: Elaboración propia).

1.2.4. Sector productivo de la empresa

Servicios educativos.

1.2.5. Misión

Impartir programas académicos de calidad en los niveles de educación media superior y superior, a través de nuestra red de universidades, mejorando continuamente los servicios orientados al estudiante, en un ámbito que favorece la integridad y la accesibilidad, impulsando la empleabilidad de nuestros egresados para que contribuyan a una mejor sociedad.

1.2.6. Visión

Ser una institución reconocida por su prestigio y el excelente desempeño de sus egresados en el campo laboral, su capacidad de emprendimiento y su contribución a nuestro país.

1.2.7. Filosofía y/o Valores

Accesibilidad: promovemos el acceso y pertenencia de los alumnos, profesores, egresados y colaboradores, de manera que se sientan apoyados y valorados en un ambiente de dignidad, respeto y empatía.

Responsabilidad: Tomamos decisiones conscientes, asumimos y respondemos por nuestros compromisos con los alumnos, colaboradores, egresados y con la sociedad.

Integridad: Actuamos de forma ética somos respetuosos y congruentes en todo lo que realizamos, dando cumplimiento con la legislación y haciendo en todo momento lo correcto.

Excelencia: Brindamos la mejor experiencia a nuestros estudiantes en su ingreso, acompañamiento a lo largo de sus estudios y seguimiento de nuestros egresados.

Liderazgo: A través de nuestras acciones ideas y actitudes, inspiramos y motivamos a otros a dar lo mejor de sí mismos, para alcanzar sus metas y generar un impacto positivo en la sociedad. Somos un ejemplo para nuestras comunidades

Innovación: Promovemos un ambiente de trabajo de colaboración e innovación para adaptarnos y responder de forma eficiente y efectiva al entorno.

1.2.8. Breve historia de la empresa

En 2016 nació con la Misión de Impulsar la movilidad social mediante el acceso a la educación y la innovación social para ampliar oportunidades de estudiantes vulnerables.

En Fundación Aliat trabajamos todos los días para que la educación deje de ser un privilegio y sea una oportunidad para todos. Creemos que solo a través de la educación podemos cambiar el presente y futuro de las personas.

Además del acceso a la educación, la Fundación busca complementar las estrategias de innovación, emprendimiento y conexión con la comunidad, que lleva a cabo Aliat Universidades, entendiéndolas como fundamentales para desarrollar en los estudiantes conocimientos, habilidades y actitudes básicas para su desarrollo personal y profesional.

Fundación Aliat es una asociación civil sin ánimo de lucro, autorizada por el SAT para recibir donativos deducibles de impuestos y apoyando los principios del Pacto Mundial en materia de derechos humanos, derechos laborales y la lucha contra la corrupción.

1.3. DESCRIPCIÓN DEL PUESTO O ÁREA DE TRABAJO

1.3.1. Agente Mesa de Servicio

Los Centros de Servicios Compartidos son un área conformada por personas, procesos y tecnologías concentradas en un mismo lugar, haciendo lo mismo para diferentes clientes internos de una compañía que opera en diferentes lugares mediante procesos estandarizados, esto significa que, en vez de tener varias áreas de personas, tecnología y procesos duplicados en diferentes lugares, se concentra una sola en un lugar específico.

Estructura organizacional del área de Mesa de Servicios y Centro de Servicios Compartidos.

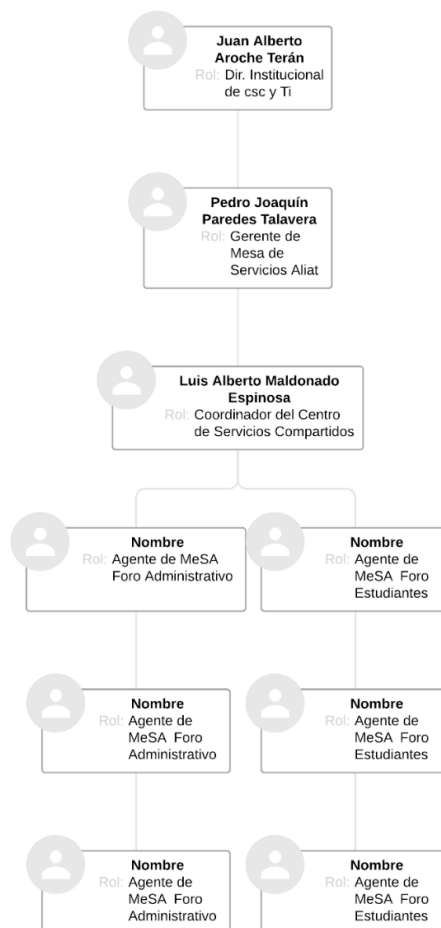


Figura 3. Organigrama de Mesa de Servicio.

(Fuente: Elaboración propia).

1.3.2. Funciones principales

El ocupante de este puesto debe tener diversas funciones dirigidas a producir determinados resultados finales, agregue las que considere necesarias. Redactar cada función de la siguiente manera: ¿Qué hace?, ¿Dónde lo hace? y ¿Para qué lo hace?

- 1) Brindar atención a reportes vía telefónica.
- 2) Atender reportes mediante las herramientas de gestión de Tickets (incidencias/requerimientos).
- 3) Mantener al usuario informado de los cambios tecnológicos.
- 4) Dar seguimiento al incidente hasta su solución final.
- 5) Verificar el estatus del reporte de usuario con el área/departamento al que fue asignado.
- 6) Asignar el incidente al siguiente nivel de atención.
- 7) Documentar el problema.
- 8) Interpretar y documentar a nivel técnico el reporte del incidente para poder escalarlo al siguiente nivel, llevando a cabo todo lo necesario para cumplir con procedimientos y políticas del área de informática.
- 9) Aplicación de encuesta en línea al momento de la resolución del reporte de servicio.
- 10) Registrar en la herramienta de gestión de incidencias las calificaciones y comentarios que se otorgaron por parte de los usuarios.

1.3.3. Objetivos

Las áreas de servicios compartidos concentran todas las áreas, ya sea de finanzas, Recursos Humanos, servicios legales, fiscales, compras, funciones de ventas comerciales, etc., y en una sola estructura para quitar las actividades transaccionales y así los directores de área den mayor atención a las actividades estratégicas para que los equipos se especialicen.

Estos modelos hacen más eficientes las operaciones dentro de las empresas, buscan reducir costos y mejorar la calidad y control con el que se realizan las actividades para mantener un alto nivel de especialización gracias a que las compañías se enfocan en su negocio principal, y se eleva su nivel de servicio y calidad. Para conocer más a fondo los requisitos, interacciones y ámbitos que requiere un agente de Mesa de Servicio, consultar el Anexo 1.

1.4. PROBLEMA POR RESOLVER

Red Univercom es una institución privada que brinda educación media superior, superior y de posgrado, esta institución brinda a sus estudiantes y trabajadores parte de sus servicios educativos y administrativos mediante la generación y proporción de una cuenta de correo de dominio propio mediante los servicios de O365 de Microsoft y aplicaciones educativas como Mi red Aliat (que abarca servicios como pagos en línea, las clases de los estudiantes, servicios escolares, servicios de atención y soporte técnico, entre otros) y aplicaciones administrativas como Remedy (para atención de servicios y soporte técnico a administrativos y estudiantes), HCM (que lleva el control de los empleados), Campus Solution (que se usa para información de trabajadores y gestión administrativa de estudiantes), etc.

Estas aplicaciones se pueden ver vulneradas por factores que muchas veces no se tienen en cuenta como pueden ser malas prácticas del manejo de las aplicaciones por parte de los usuarios como pueden ser trabajadores o los propios estudiantes, provocando el manejo inadecuado de las aplicaciones en conjunto con un mal manejo de la información dentro de estas, el ingreso no intencionado de malware en equipos y/o sistemas, software desactualizado o servidores que usan tecnologías anticuadas y causan retraso en las aplicaciones. Estas causas y mas no previstas pueden provocar pérdida de información, un bajo control en las operaciones, retardo en el proceso de servicio a los usuarios e incluso el detenimiento parcial o total de las operaciones, generando una mala imagen de los servicios de la institución, junto con pérdidas monetarias a la empresa.

1.5. OBJETIVOS

1.5.1. Objetivo general

Realizar un análisis de riesgo para evaluar los servicios de correo electrónico, Remedy y medios de seguridad asociados basados en el estándar ITIL y otros.

1.5.2. Objetivos específicos

1. Identificar el entorno general de Red Univercom S.C y el papel que desempeña el área de Mesa de Servicios y Centro de Servicios Compartidos para conseguir los objetivos de la empresa.
2. Analizar información detallada sobre los servicios que el área ofrece a los usuarios referente a correo electrónico y Remedy por parte de la empresa.
3. Emplear un análisis de riesgo según las amenazas y vulnerabilidades encontradas.
4. Proponer las estrategias sustentadas en ITIL 4 y en otros estándares de seguridad; y adaptarlas a las necesidades específicas a los servicios de correo electrónico y Remedy que se ofrecen.

1.6. JUSTIFICACIÓN

Red Univercom buscan brindar un servicio educativo y administrativo rápido, seguro y de calidad tanto para sus trabajadores y sus estudiantes. Una de sus herramientas principales es Remedy, una plataforma de gestión de incidencias académicas, administrativas y financieras. Sin embargo, esta plataforma presenta vulnerabilidades, tanto por factores técnicos como por el uso e interacción de los usuarios.

Aliat, como institución comprometida en priorizar la atención a sus alumnos, requiere una solución técnica que permita Mesa de Ayuda identificar los posibles riesgos que enfrenta el sistema actualmente. De este modo, se pueden priorizar aquellos que son más frecuentes y que podrían afectar significativamente el sistema o las operaciones. Además, esta solución debe apoyar la planificación frente a posibles adversidades, fortaleciendo la resiliencia del área, fomentando el cumplimiento de las normas internas de la empresa y facilitando un mejor control del personal y de los sistemas.

Al lograr un control más riguroso y al considerar las vulnerabilidades del sistema, Red Univercom podrá identificar con mayor claridad las áreas de mejora tanto en el sistema como en sus procesos internos, lo cual redundará en un servicio de mejor calidad en beneficio de todo el personal y alumnado que conforman la red. Esto, a su vez, permitirá proyectar una mejor imagen ante la sociedad.

La metodología propuesta para el análisis se basa en la guía ITIL v4, reconocida internacionalmente por su enfoque en la gestión de servicios. Además, se emplearán normas y estándares como COBIT e ISO 17799, los cuales buscan un control y una seguridad mayores en los sistemas empresariales, asegurando que Red Univercom se mantenga actualizado en guías y metodologías de seguridad.

A nivel profesional, este proyecto tiene como objetivo identificar las vulnerabilidades y áreas de oportunidad en el área de Mesa de Ayuda de Red Univercom, proponiendo soluciones y estrategias para mejorar el servicio y fortalecer la infraestructura de soporte.

CAPÍTULO II: MARCO TEÓRICO

2.1. Estado del arte

A continuación, se muestran un análisis de diferentes trabajos que marcan el contexto de uso de estándar ITIL y otras normas a cerca de la seguridad y la atención de clientes, de esta forma se pueden conocer hechos sobre dichos trabajos y sus implementaciones en el tiempo.

Tabla 1. Estado del arte.

(Fuente: Elaboración propia).

Fuente	Titulo	Estrategias y/o Técnicas	Resultados Obtenidos
(López Goytia et al., 2019)	“Propuesta de mejora basada en el marco ITIL, para la atención de tickets del proceso de administración de incidentes en una empresa proveedora de equipos médicos”	Este proyecto busca la implementación de las TI por medio de ITIL como marco referencial a cerca de las buenas prácticas en el diseño, administración y ejecución de servicios enfocado en el problema de la distribución de equipos médicos.	Se propone un software el cual cuenta con una pantalla amigable para los usuarios en base a las prácticas de disponibilidad de ITIL 4, propone también que el software no se quede con solo la mejora propuesta si no que pueda mejorarse en el proceso y con las interacciones que esta tenga siempre y cuando se cumpla la satisfacción del usuario.

Tabla 1. Estado del arte (Continuación).

(AYALA SOTO, 2023)	“Implementación de las buenas prácticas de ITIL v4 y su influencia en la gestión de servicios del área de Service Desk de la empresa S.C.R. s. a. c.”	Se utilizarán metodologías de investigación aplicada y explicativa para estructurar la problemática y corroborar que el uso de las buenas prácticas de ITIL V4 beneficiara a la empresa SCR S.A.C con base en datos estadísticos y mediante el estudio del personal de la empresa.	Se concluyo que la implementación de buenas prácticas en base a ITL V4 beneficio a la gestión de servicios, encontrando mejoras significativas en la atención de incidentes, tiempos de entrega de reportes y satisfacción del usuario, reduciendo el tiempo de resolución en un 42.7%. También tiene como recomendación la capacitación del personal según las buenas prácticas de ITIL para una mayor eficiencia de servicios de TI.
---------------------------	---	--	---

Tabla 1. Estado del arte (Continuación).

(HERNÁNDEZ ECHEVERRÍA, 2021)	“Propuesta para el mejoramiento de procesos y gestión de riesgos ti del área programación y control de la compañía EMTELCO S.A.S., basada en las buenas prácticas de ITIL 4 y COBIT 2019”	Utiliza las propuestas de ITIL para la gestión y los alinea a la empresa, siendo estas la gestión estratégica, de seguridad de la información, de riesgos, de servicio, entre otros. Busca la implementación de la mejora continua. Realiza una evaluación de riesgos en base a COBIT 2019 para denotar los riesgos que padece la empresa.	Se da a conocer el estado en el que se encuentra la empresa EMTELCO S.A.S., indicando las faltas de esta y proporcionando recomendaciones como pueden ser maximizar el uso de herramientas en la empresa, implementar las practicas ITIL y COBIT para aprovechar ambos, una mejora en la organización de la empresa, centralizar la información con herramientas de TI, dar mantenimiento a las plataformas o mejorar lo ya existente y no implementar actividades ITIL o COBIT si no son necesarias o útiles para la empresa.
-------------------------------------	---	--	--

Tabla 1. Estado del arte (Continuación).

(Daniel Caballero, 2021)	“Análisis y Gestión de Riesgo en Proyectos Software Un nuevo modelo integrando la metodología SEI y Magerit3”	Mediante el uso de diferentes metodologías para la gestión de riesgo, se busca realizar un análisis el cual determine la mejor forma de generar actividades para el control y cuidado de los activos, también busca gestionar posibles incidencias en los activos tecnológicos, y además busca comunicar la información de los riesgos y la aplicación de acciones preventivas e incidencias implicadas en los mismos.	Se concluyo que la mayoría de las organizaciones modifican las metodologías del análisis y gestión del riesgo en base a sus necesidades, adaptando métodos en base a otro método, en otras palabras, integrando características de otras metodologías, permitiendo ser adoptados por cualquier organización.
---------------------------------	--	--	--

2.2. Marco conceptual

Es necesario contextualizar ampliamente en que consiste un análisis de riesgo y los términos que manejan las normas y la gestión de servicios, a continuación, se muestra la explicación de los conceptos necesarios para entender más a fondo el proyecto.

2.2.1. Definición de riesgo

Un riesgo en el ámbito empresarial puede entenderse como los posibles daños y pérdidas potenciales que pueden presentarse en el proyecto, estas pueden ser vulnerabilidades y amenazas de seguridad. “El riesgo es el efecto de la incertidumbre y dicha incertidumbre puede tener efectos positivos o negativos. Una desviación positiva que surge de un riesgo puede proporcionar una oportunidad, pero no todos los efectos positivos del riesgo tienen como resultado oportunidades.” (International Organization for Standardization, 2015).

De esta forma se identifican aspectos que pueden mejorarse y/o prevenirse, sin embargo, en caso de haber una cantidad considerable de estos, es necesario priorizar aquellos que puedan tener un mayor impacto las operaciones, determinar esto requiere de un análisis de los riesgos.

2.2.2. Definición de amenaza

“Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.” (JTC 1, Comité Técnico Conjunto ISO/IEC, 2005, pág. 15), las amenazas también pueden interpretarse como agentes externos a la empresa, sistema o elemento evaluado, estas amenazas están fuera del control de la empresa, por ejemplo, algún desastre natural, cambios en las leyes o bien ciberataques.

2.2.3. Definición de vulnerabilidad

“La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.” (JTC 1, Comité Técnico Conjunto ISO/IEC, 2005, pág. 15), las vulnerabilidades se consideran como los defectos internos de la empresa, área o sistema, por ejemplo, falta de alguna actualización en los sistemas de seguridad, falta de capacitación al personal en el uso de los sistemas, falta de comunicación interna etc.

2.2.4. Definición de probabilidad

“Posibilidad de que algún evento determinado suceda” (Financial Crime Academy, 2024), en un análisis de riesgo este indicador marca la frecuencia en la que algún riesgo pueda ocurrir.

2.2.5. Definición de impacto

“Determina el efecto o consecuencia de que el evento ocurra” (Financial Crime Academy, 2024), en el análisis de riesgo el impacto determina que tan grave es el riesgo, por ejemplo, que tanto puede afectar a las operaciones, los sistemas o finanzas de la empresa.

2.2.6. Que es y la importancia del análisis de riesgo

El análisis de riesgo y la evaluación de riesgo buscan que se identifiquen, cuantifiquen y prioricen los riesgos, esto mediante la comparación de los objetivos de la empresa. Los resultados de dicho análisis son los que guiarán a la empresa en su toma de decisiones en cuanto a la prioridad de los riesgos, ayudando a mantener la seguridad de la información junto con la implementación de controles que mitiguen o prevengan los riesgos.

El análisis de riesgo debe hacerse mediante un enfoque sistemático que permita calcular la magnitud de los riesgos, pueden realizarse a la empresa en general o bien en secciones concretas, pudiendo abarcar áreas como el personal de la empresa, los sistemas que

conforman a la empresa o un sistema en concreto, los procesos que manejan, los servicios que ofrece, entre otros.

Es recomendable que los análisis de riesgo se hagan de manera periódica y sobre todo cuando se tiene algún cambio significativo en la empresa, por ejemplo, en las políticas de seguridad, cambio de personal, etc.

Los análisis deben tener un alcance definido y un objetivo claro para evitar divagar en las ramas y perder el enfoque del análisis. (JTC 1, Comité Técnico Conjunto ISO/IEC, 2005, ISO/IEC 27002:2005)

2.2.7. Tratamiento de los riesgos de seguridad

Al determinar el probabilidad e impacto de los riesgos y clasificar el nivel de prioridad de atención de los riesgos, las opciones utilizadas para mitigar los riesgos pueden ser:

- Aplicar controles o reglas, por ejemplo, en los sistemas, en el uso que les da el personal a sus herramientas de trabajo y demás funciones que ayuden a reducir los riesgos.
- Se pueden aceptar riesgos que no vayan en contra de la política de la empresa o bien que no presenten una amenaza grave para la institución y los sistemas, de esta manera es posible centrarse en aquellos que representen un mayor peligro.
- Capacitar al personal para evitar acciones que generen riesgos por falta de información.

Las empresas deberán tener presente que, pese a los controles, metodologías y demás tareas que se realicen para mitigar los riesgos, no se puede lograr la seguridad completa sin embargo contar con métodos como la monitorización frecuente, evaluar, ser más eficiente y mejorar los controles de seguridad, apoyan a los objetivos de la organización (JTC 1, Comité Técnico Conjunto ISO/IEC, 2005, Pág. 18).

2.2.8. Herramientas y técnicas en el Análisis de Riesgo

Estas herramientas y técnicas son las que permitirán analizar la información recopilada para identificar las posibles vulnerabilidades y amenazas, posteriormente determinar el nivel de peligro que generan (Team Asana, 2024).

2.2.8.1 Análisis FODA

El análisis FODA, acrónimo de Fortalezas, Oportunidades, Debilidades y Amenazas, es una herramienta que permite identificar los aspectos clave que destacan al objeto de evaluación, por ejemplo, en el mercado, frente a otras empresas o sistemas. A su vez, facilita la comparación con aquellos elementos que representan debilidades o factores que obstaculizan su desarrollo. Este balance contribuye a determinar si el objetivo evaluado cumple adecuadamente con su función o si carece de los recursos necesarios para lograrlo.

Al realizar un análisis FODA es necesario hacerse algunas preguntas y tener en cuenta que hay aspectos que son de manera interna y/o externa, permitiendo identificar las fortalezas, debilidades, oportunidades y amenazas.

- **Fortaleza – Interno:** Es aquello en lo que destaca la entidad a estudiar, aquello que lo diferencia de los demás. Para identificar las fortalezas se pueden responder preguntas como: ¿Cuáles son los puntos fuertes?, ¿Con que ventajas se cuenta?, ¿Qué se tiene de diferente?, ¿En qué se diferencia con la competencia?

- **Debilidades – Interno:** Son los problemas y defectos internos, por ejemplo, que el personal no esté debidamente capacitado a utilizar los sistemas de la empresa, para identificar debilidades se pueden hacer preguntas como: ¿Qué se puede mejorar?, ¿De que carece el proyecto, personal o sistema?

- **Oportunidades – Externo:** Son factores externos que ofrecen beneficios potenciales y pueden ser aprovechados por la empresa. Algunas preguntas que pueden ayudar a identificar estas oportunidades incluyen: ¿Qué cambios en leyes o normativas pueden afectar a la empresa de manera favorable?, ¿Qué innovaciones tecnológicas podrían ser implementadas en las operaciones?, ¿Qué aspectos de la relación con socios comerciales podemos mejorar para generar valor?

- **Amenazas – Externo:** Son situaciones externas que pueden perjudiciales, estos agentes están fuera del control de la institución. Algunas preguntas que pueden ayudar a identificar las amenazas son: ¿Qué cambios en leyes o normativas pueden perjudicar a la empresa?, ¿Qué obstáculos externos pueden perjudicar a la empresa?

Una vez identificados las fortalezas, debilidades, oportunidades y amenazas, ayudara a que la empresa tenga más claro el panorama respecto a lo que está evaluando y se tomen mejor las decisiones respecto a los riesgos que las vulnerabilidades y amenazas puedan generar (Muñoz Martínez & Prieto de Diego, 2016, pág. 83-86).

2.2.9. ITSM (Information Technology Service Management)

Los servicios de gestión de TI, “refiere a un conjunto de capacidades organizacionales especializadas que se pueden apalancar para la creación de valor en la forma de servicios” (ITIL México, s. f.). Esto se puede representar en los procesos y sistemas que se usen para brindar servicios y genera valor.

2.2.10. SLA

Hace referencia al acuerdo de nivel de servicio, es el contrato de establecimiento de las responsabilidades y obligaciones entre la empresa y el cliente, es decir, que se definen los tiempos esperados de atención para presentar un nivel de servicio de calidad (AXELOS Limited, 2019).

2.2.11. Remedy Service Desk

Es un software de gestión de servicios desarrollado por BMC Software, un derivado de los servicios que ofrece BMC Remedy IT Service Management, diseñado para gestionar y optimizar los incidentes y solicitudes dentro de la empresa (BMC Software, Inc., 2024).

2.2.12. HCM (Human Capital Management)

Es un sistema en la nube proporcionado por Oracle para procesos de recursos humanos para las empresas, el cual se utiliza para gestionar la información administrativa de los empleados, es decir, información referente a su puesto de trabajo, información básica del empleado, por ejemplo, ID del empleado, nombre, edad, fecha de contratación, estado del empleado, etc. (Oracle Corporation, 2024).

2.2.13. Campus Solution

Software proporcionado por Oracle para llevar un control de los estudiantes e información de estos como puede ser información financiera, información básica del estudiante, campus al que pertenece y estado del estudiante (Oracle Corporation, 2024).

2.3. Marco metodológico

2.3.1. Tipo de análisis de riesgo

Se realizar un análisis de tipo cualitativo, este análisis busca asignar un valor numérico o nivel a los riesgos, la puntuación se determinará por las experiencias de la empresa. Como métodos de recolección de la información para el análisis cuantitativo esta la lluvia de ideas, entrevistas y evaluaciones por parte de expertos, la investigación documental se realiza apoyándose en fuentes de carácter documental, esto es, en documentos de cualquier especie; en este caso las normas ISO, el framework COBIT y las librerías ITIL v4.

2.3.2. Población y muestra

Población: se refiere al universo, conjunto o totalidad de elementos sobre los que se investiga o hacen estudios.

En este proyecto la población es el personal de Mesa de Servicio Aliat que lo conforman los dos encargados del área y los siete Agentes de Mesa

Muestra: Muestra es una parte o subconjunto de elementos que se seleccionan previamente de una población para realizar un estudio.

Debido a que en este proyecto se busca analizar todo el sistema que trabaja Mesa de Servicio es necesario trabajar con todo el personal que interactúa con el sistema, por ello la muestra se conforma por la población del proyecto que son los nueve integrantes de Mesa de Servicio.

2.3.3. Técnicas e instrumentos de recolección de información

Para la realización de este proyecto la técnica de recopilación de información fue mediante la realización de una entrevista al personal de Mesa de Servicio instrumentada en un cuestionario enfocado en describir a detalle las interacciones, normas y métodos de prevención de incidentes actuales.

2.3.4. Cuadro Metodológico para el desarrollo del proyecto.

Tabla 2. Metodologías para el desarrollo del proyecto.

(Fuente: Elaboración propia).

Actividades	Técnicas	Herramientas	Metas
1.1. Revisar la misión, visión, giro y razón social de la empresa Red Univercom S.C para identificar el propósito y sus objetivos a mediano y largo plazo.	Investigación y recopilación de información de la empresa.	Documentos, Internet y Word como procesador de textos.	Contextualizar y conocer la empresa.
1.2. Revisar las funciones, procesos, procedimientos, responsabilidades, objetivos, metas y la estructura organizacional del área de Mesa de Servicios y Centro de Servicios Compartidos y como se ligan a los objetivos generales de la empresa.	Recopilación de información e investigación de campo.	Entrevistas, internet y Word como procesador de textos.	Conocer las funciones del Área de Mesa de Servicio de Aliat Universidades.

2.1. Establecer los formatos de las entrevistas, análisis FODA y matrices de evaluación que se usaran para la recopilación y análisis de la información.	Formulación de preguntas de entrevista y diseño de cuadros y tablas.	Internet, libros y Word como procesador de textos.	Establecer los diseños de la formatearía que se utilizara para la entrevista, análisis FODA y cuadro de probabilidad e impacto.
--	--	--	---

Tabla 2. Metodologías para el desarrollo del proyecto (Continuación).

2.2. Solicitar información acerca de los servicios de correo electrónico y Remedy a través de una entrevista al personal que conforma el área en evaluación.	Elaboración de una entrevista de preguntas abiertas.	Word como procesador de textos.	Conocer más a detalle los servicios de correo y Remedy.
2.3. Analizar las respuestas recopiladas en las encuestas para identificar los riesgos que los participantes perciben en relación con los servicios de correo electrónico y Remedy.	Analizar la información recopilada en las entrevistas.	Word como procesador de textos.	Conocer los procesos para la identificación de los riesgos.
2.4. Identificar posibles vulnerabilidades y amenazas en los servicios de correo electrónico y Remedy a través del análisis FODA.	Análisis e identificación de las fortalezas, oportunidades, debilidades y amenazas.	Word como procesador de textos.	Enumerar los criterios en los que destacan y se pueden mejorar de los servicios mencionados.
3.1. Examinar los riesgos que podrían impedir el normal desenvolvimiento de las operaciones en la empresa.	Clasificación de las vulnerabilidades.	Word como procesador de textos.	Enumerar las vulnerabilidades e identificar los riesgos que conllevan.
3.2. Establecer el nivel de la exposición al riesgo.	Estimación y valoración de los riesgos.	Word como procesador de textos.	Estructurar un cuadro de probabilidad e impacto y establecer que vulnerabilidades son mayormente probables y cuales afectan en mayor medida a la empresa.
3.3. Compilar las vulnerabilidades y que tan severamente podrían afectarse las operaciones en la empresa.	Evaluación de las amenazas.	Word como procesador de textos.	Escalar la probabilidad y el impacto de los rasgos identificados.
3.3.1. Seleccionar los escenarios probables y de mayor impacto con el objetivo de abordarlos de manera inmediata.	Organizar las afectaciones según la que cause mayor impacto y se más probable a que suceda.	Word como procesador de textos.	Organizar las vulnerabilidades de mayor a menor probabilidad e impacto para después calcular cuánto afecta a la empresa monetariamente y cuanto afecta al nivel del servicio.

Tabla 2. Metodologías para el desarrollo del proyecto (Continuación).

4.1 Aplicar las cuatro dimensiones de la gestión de servicios para comprender y abordar diversos aspectos en la prestación de servicios de TI.	Análisis de la gestión de servicios actual.	Documentos y Word como procesador de textos.	Identificar que parte de las cuatro dimensiones de ITIL se ve afectada por las afectaciones identificadas.
4.2. Recomendar las posibles soluciones a los riesgos a fin de brindar alternativas de solución.	Planificar las mejoras según las guías y estándares.	Documentos y Word como procesador de textos.	Idealizar y proponer soluciones a las afectaciones en base a los estándares.
4.3. Estructurar las propuestas y posibles soluciones con base al modelo de mejora continua ITIL y otros estándares.	Estructurar las propuestas en base a las recomendaciones de los estándares.	Word como procesador de textos.	Estructurar las propuestas en base a las guías y estándares.

2.3.5. Normas, estándares y librerías utilizadas.

A continuación, se muestran los marcos referenciales que se utilizarán en el proceso de implementar buenas prácticas de seguridad y reforzar los métodos ya establecidos.

2.3.5.1. ITIL v4

Descripción: ITIL 4 es una revisión al marco de trabajo más ampliamente aceptado a nivel mundial para la Administración de Servicios de TI (ITSM).

Uso: ITIL 4 proporciona la guía que necesitan las organizaciones para abordar los nuevos desafíos de la administración de servicios y utilizar el potencial de la tecnología moderna. Está diseñado para garantizar un sistema flexible, coordinado e integrado para el gobierno y la gestión efectiva de los servicios habilitados para TI.

Criterios que emplear: ITIL en sus distintas versiones busca darle valor al servicio que las empresas ofrecen, por lo que en sus lineamientos cuenta con lo siguiente:

Sistema de valor de servicio SVS.

Es el conjunto de aspectos que deben abordarse en la gestión del servicio los cuales interactúan con la cadena de valor del servicio.

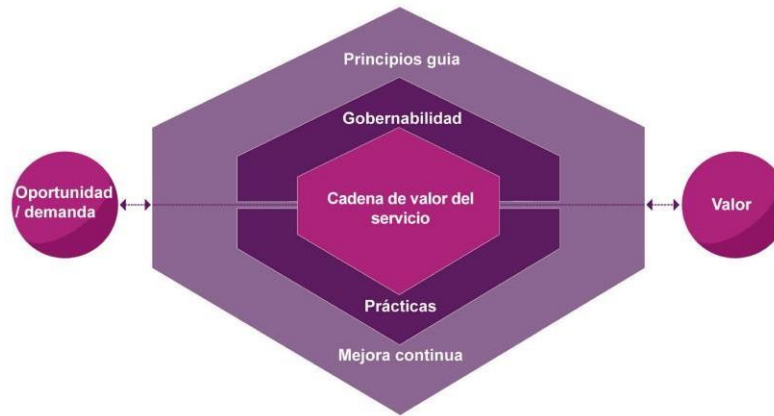


Figura 4. Sistema del valor del servicio (SVS).

(Limited, AXELOS, 2019).

Principios Guías: Son recomendaciones que pueden guiar a una organización en cualquier circunstancia, independiente de los cambios en sus objetivos, estrategias, tipo de trabajo o estructura de gestión.

- **Gobierno:** Los medios por los cuales una organización es dirigida y controlada. Por ejemplo, políticas organizacionales, códigos internos.
- **Mejora Continua:** Actividad recurrente realizada en todos los niveles de una organización para garantizar que el desempeño satisfaga continuamente las expectativas de los interesados.
- **Cadena de Valor de Servicio:** Un conjunto de actividades relacionadas que una organización realiza para generar valor, entregando un producto o servicio para sus clientes.
- **Prácticas:** Conjunto de recursos organizacionales diseñados para realizar un trabajo o cumplir objetivos.

Por su parte, la Cadena de Valor del Servicio (SVC) es la parte operativa del Sistema de Valor del Servicio (SVS). Es un modelo que nos asistirá a conceptualizar la creación, entrega

y mejora continua de los servicios a nivel operativo, no representa un ciclo de vida o una secuencia de actividades sino un conjunto de elementos en los que las practicas puede ser útil.

- **Planificar:** La creación de planes, políticas, normativas y el establecimiento de la dirección de un determinado flujo de valor.
- **Mejorar:** La garantía de mejora continua de las prácticas, productos y servicios ofrecidos por la organización.
- **Involucrar:** El establecimiento de buenas relaciones con todas las partes interesadas y los usuarios finales, para ofrecer transparencia y una comprensión clara de los productos y servicios.
- **Diseño y transición:** El aseguramiento de que los productos y servicios ofrecidos satisfagan continuamente las demandas de las partes interesadas.
- **Obtener/construir:** La disponibilidad de los componentes del servicio, como el hardware, el software, los servicios, etc., en el momento y lugar en que se necesitan.
- **Entregar y soportar:** La garantía de que los servicios se prestan y respaldan de forma que puedan satisfacer las expectativas de las partes interesadas.

Las cuatro dimensiones de la gestión de servicios.

La gestión eficaz de los servicios de TI es más que la mera gestión de la tecnología. También incluye las diferentes organizaciones dentro de la empresa y las personas que participan en ellas, las relaciones con proveedores y socios, y los diferentes procesos y tecnologías utilizados, si no se abordan adecuadamente las 4 dimensiones las organizaciones pueden tener dificultades para prestar sus servicios o cumplir los requisitos de calidad o eficiencia.

Pueden interactuar de manera impredecible en función del nivel de complejidad e incertidumbre que rodea a la organización, se aplica a todos los servicios gestionados y al sistema de valor de servicios en general.

Tenerlas en cuenta para cada servicio y considerar cada una de ellas a la hora de gestionar y mejorar el sistema de gestión del servicio a todos los niveles.

1. **Organización y personas:** funciones y responsabilidades, estructuras organizativas, cultura y requisitos de personal y sus competencias, entender como está estructurada y gestionada la empresa, así como comprender y aclarar los

roles, responsabilidades y autoridades que existen o se necesitan para apoyar la estrategia de la organización y la forma elegida de trabajo.

2. **Información y tecnología:** para el soporte de los servicios y apoyo a la gestión de estos servicios.
3. **Socios y proveedores:** pueden ser otras empresas, otras actividades o todos los equipos que participan en la prestación uso y gestión de los servicios
4. **Flujos de valor y procesos:** acciones emprendidas para crear valor a los consumidores.



Figura 5. Las cuatro dimensiones de la gestión de servicios.

(Limited, AXELOS, 2019).

Los 7 principios guía de ITIL.

Representan los elementos centrales de ITIL y de la gestión de servicios. Estos principios apoyan a la mejora continua de las organizaciones en todos los niveles.

- 1) **Centrarse en el valor:** Todos los esfuerzos realizados deben estar relacionados, directa o indirectamente, a la producción de valor para las partes interesadas. Es decir, cuando tomemos una decisión, por ejemplo, el agregar, modificar o quitar un servicio, debemos de tener claras las implicaciones para el negocio y/o los usuarios que consumirán el servicio.

- 2) **Comience donde se encuentre:** Este principio nos invita a aprovechar los recursos existentes (tecnológicos, humanos, de gestión, etc.) para construir nuevas ofertas en nuestro entorno. Lo más probable es que nos pueda asistir en no tener que empezar desde cero.
- 3) **Progrese de forma iterativa mediante la retroalimentación:** Se refiere a que no pretendamos acabar un proyecto en un solo gran esfuerzo. Es mejor verlo como la suma de muchos esfuerzos pequeños que puedan ir dejando resultados positivos lo más rápido posible y al final se acumulen en la totalidad del proyecto.
- 4) **Piense y trabaje holísticamente:** ITIL 4 nos instiga a tener una visión integral, comprendiendo que ningún servicio actúa de manera independiente. Todos los servicios en nuestro entorno tienen una serie compleja de relaciones que debemos tener presente para poder lograr nuestros objetivos.
- 5) **Colabore y promueva la visibilidad:** Este principio guía nos invita a buscar la participación de todas las partes interesadas en nuestros esfuerzos de ITSM, promover la transparencia de información y evitar esconder las consecuencias (positivas o negativas), de nuestras actividades.
- 6) **Manténgalo simple y práctico:** Este principio tiene como propósito ayudarnos a simplificar las actividades en nuestro entorno, debemos buscar eliminar las cosas que no produzcan valor y reducir a la menor cantidad de pasos posibles en los procedimientos y procesos.
- 7) **Optimice y automatice:** Debemos estar siempre en búsqueda de la optimización de los recursos a través de la automatización tecnológica de todas las tareas posibles, de manera que los valiosos recursos humanos se puedan enfocar en donde verdaderamente puedan aportar valor.

Estos principios ayudan a guiar a las organizaciones a su trabajo, adoptando un enfoque de gestión de servicios y aplican las buenas prácticas de ITIL las necesidades y circunstancias específicas (gobernanza).

Modelo de mejora continua

La mejora continua se lleva a cabo en todas las áreas y en todos los niveles de la organización, desde la estratégica hasta la operativa. La mejora continua es importante para una organización por varias razones, que incluyen:

- El entorno del negocio y las preferencias del cliente para los servicios cambian constantemente, por lo que el proveedor del servicio debe mantenerse alineado con los requisitos cambiantes del negocio.

- El panorama tecnológico continúa cambiando, y si una organización no se aprovecha de la tecnología en evolución, sus servicios pronto se volverán obsoletos.
- Los servicios proporcionados por la organización deben revisarse y actualizarse continuamente para obtener oportunidades de mejora, de lo contrario, pierden la alineación y tienen poco valor.

Para maximizar la efectividad de los servicios, cada persona que contribuye a un servicio debe tener en mente la mejora continua y siempre debe buscar oportunidades para mejorar.

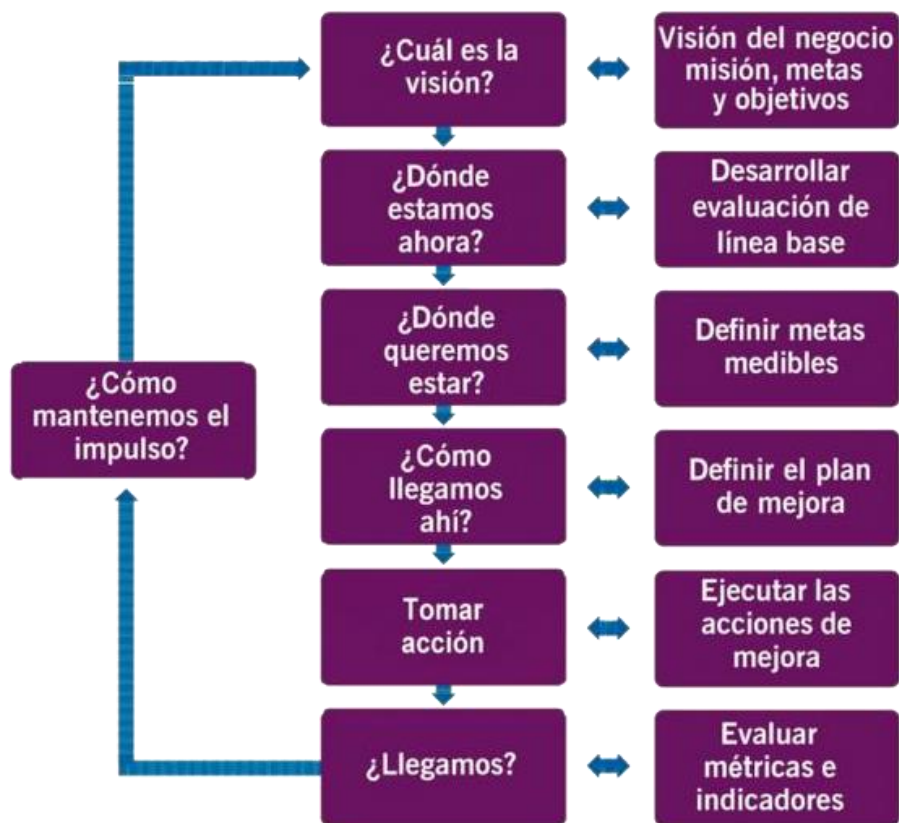


Figura 6. Modelo de mejora continua ITIL.

(Limited, AXELOS, 2019).

2.3.5.2. COBIT

Descripción: COBIT proviene de “Control Objectives for Information and Related Technology” (Objetivos de control para tecnologías de la información y tecnologías relacionadas) y fue desarrollado por la asociación profesional de auditores de IT y auditores ISACA.

COBIT es un marco de referencia popular que ayuda a las empresas a alcanzar sus objetivos comerciales. Este especifica qué objetivo y procesos deben utilizarse dentro de una empresa para garantizar un gobierno corporativo eficiente. El objetivo es alinear las áreas de TI y de negocio para garantizar una colaboración eficiente dentro de la empresa.

Uso: COBIT se utilizó principalmente como una herramienta para los auditores, sin embargo, posteriormente se convirtió en una herramienta importante para la gestión de IT en las empresas. ISACA está constantemente en desarrollo y es utilizado en todo el mundo y se adapta al progreso tecnológico.

COBIT 5 cumple con los estándares internacionales e integra las pautas y modelos de IT más importantes, por ejemplo:

- ITIL
- COSO
- PRINCE2
- Val IT
- Risk IT
- ISO-Estándares (ISO 27001 o ISO 27002)

Criterios que emplear: COBIT emplea 5 principios y una guía de implementación de estos principios para que las empresas puedan gobernar y gestionar su tecnología.

Principio 1: Satisfacer las Necesidades de las Partes Interesadas

Las empresas buscan crear valor para sus accionistas, por ello tienen que crear ese valor como un objetivo más de gobierno, este valor consiste en generar beneficios con un coste óptimo

en recursos y minimizando los riesgos, dichos beneficios pueden ser financieros, comerciales o de servicio. Lo anterior se puede resumir en la siguiente figura.



Figura 7. El Objetivo de Gobierno: Creación de Valor.

(ISACA, 2012).

Principio 2: Cubrir la Empresa de Extremo-a-Extremo

El objetivo de COBIT al cubrir la empresa de extremo a extremo es:

- Integrar el gobierno de la empresa TI en el gobierno corporativo. Es decir que el sistema propuesto por COBIT se puede adaptar al cualquier sistema de gobierno que manejen las empresas y se alinea a las últimas visiones de gobierno.

o Cubrir todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. COBIT contempla los servicios de TI más relevantes y los procesos de negocio que se manejan tanto de manera interna como de manera externa.

Enfoque de Gobierno

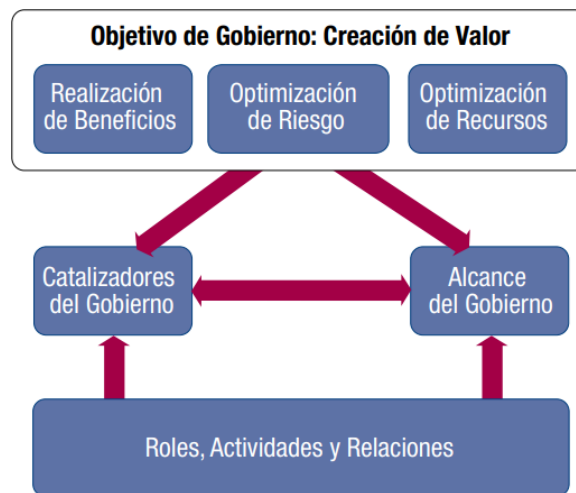


Figura 8. Enfoque de gobierno.

(ISACA, 2012).

Para COBIT el objetivo de gobierno es la creación del valor, y requiere de ciertos criterios a tomar en cuenta para conseguirlo.

Principio 3: Aplicar un Marco de Referencia Único Integrado

Usar un solo marco de gobierno integrado puede ayudar a las organizaciones a brindar valor óptimo de sus activos y recursos de TI. COBIT, por ejemplo:

- Se alinea con otros estándares y marcos de referencia relevantes y, por tanto, permite a la empresa usar COBIT 5 como el marco integrador general de gestión y gobierno.
- Es completo en cuanto a la cobertura de la empresa, proporcionando una base para integrar de manera efectiva otros marcos, estándares y prácticas utilizadas. Un marco general único sirve como una fuente consistente e integrada de guía en un lenguaje común, no-técnico y tecnológicamente agnóstico.
- Proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente.
- Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA. ISACA ha investigado las áreas clave del gobierno corporativo durante muchos años y ha desarrollado marcos tales como COBIT, Val IT, Risk IT

Framework, BMIS, la publicación Información sobre Gobierno de TI para la Dirección (Board Briefing on IT Governance) e ITAF para proporcionar guía y asistencia a las empresas. COBIT 5 integra todo este conocimiento.

Principio 4: Hacer Posible un Enfoque Holístico

Catalizadores COBIT 5

Los catalizadores son factores que, individual y colectivamente, influyen sobre si funcionara la gobernanza y la gestión de TI. Los catalizadores son guiados por la cascada de metas, es decir, objetivos de alto nivel relacionados con TI definen lo que los diferentes catalizadores deberían conseguir. COBIT describe siete categorías de catalizadores:

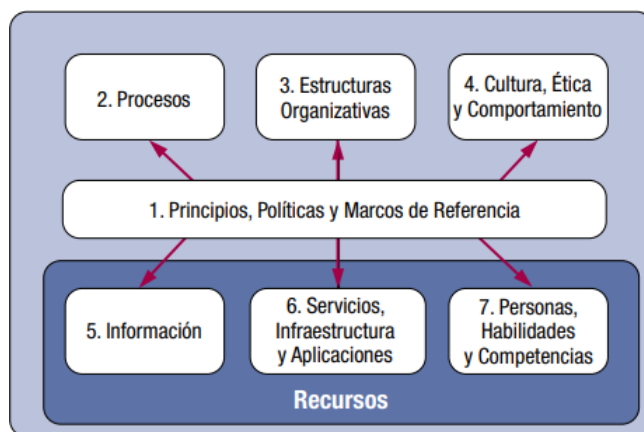


Figura 9. Catalizadores COBIT.

(ISACA, 2012).

Principio 5: Separar el Gobierno de la Gestión

COBIT 5 marca una diferencia entre la gestión y el gobierno.

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas;

estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

Contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (Plan, Build, Run and Monitor - PBRM), y proporciona cobertura extrema a extremo de las TI. Los nombres de estos dominios han sido elegidos de acuerdo con estas designaciones de áreas principales, pero contienen más verbos para describirlos:

- Alinear, Planificar y Organizar (Align, Plan and Organise, APO)
- Construir, Adquirir e Implementar (Build, Acquire and Implement, BAI)
- Entregar, dar Servicio y Soporte (Deliver, Service and Support, DSS)
- Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, MEA)

2.3.5.3. ISO 17799 - 2005

Descripción: La norma ISO 17799 es un estándar internacional de alto nivel para la administración de la seguridad de la información, orienta a preservar principios como; la Confidencialidad, donde asegura que únicamente el personal autorizado tenga acceso a la información, la Integridad que garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas y Disponibilidad que asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

Uso: Dirige y da soporte a la gestión de la seguridad de la información en concordancia con los requisitos de la organización, la legislación y las regulaciones, va dirigida a cualquier tipo de organización o de compañía, privada o pública. Si la organización utiliza sistemas internos o externos que poseen informaciones confidenciales, si depende de estos sistemas para el funcionamiento normal de sus operaciones o si simplemente desea probar su nivel de seguridad de la información conformándose a una norma reconocida.

Criterios que emplear: Dada la extensión de la norma ISO 17799 se tomaron en cuenta los siguientes apartados que son afines a lo que se desea realizar en este proyecto.

Evaluación y tratamiento del riesgo

- **Evaluación de los riesgos de seguridad**

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

Tratamiento de los riesgos de seguridad

Para aquellos riesgos donde la decisión del tratamiento del riesgo ha sido aplicar los controles apropiados, estos controles debieran ser seleccionados e implementados para satisfacer los requerimientos identificados por la evaluación del riesgo. Los controles debieran asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

- 1) Los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales;
- 2) Objetivos organizacionales;
- 3) Requerimientos y restricciones operacionales;
- 4) Costo de implementación y operación con relación a los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización;
- 5) La necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

Organización de la seguridad de la información

- **Organización interna**

Se debiera establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

Si fuese necesario, se debiera establecer una fuente de consultoría sobre seguridad de la información y debiera estar disponible dentro de la organización. Se debieran desarrollar contactos con los especialistas o grupos de seguridad externos, incluyendo las autoridades relevantes, para mantenerse actualizado con relación a las tendencias industriales, monitorear los estándares y evaluar los métodos y proporcionar vínculos adecuados para el manejo de los incidentes de seguridad de la información. Se debiera fomentar un enfoque multidisciplinario para la seguridad de la información.

Seguridad de recursos humanos

- **Durante el empleo**

La empresa se asegurará de que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

- **Conocimiento, educación y capacitación en seguridad de la información**

Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceras personas debieran recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral.

Gestión de las comunicaciones operacionales

- **Procedimientos y responsabilidades operacionales**

Asegurar la operación correcta y segura de los medios de procesamiento de la información.

Se debieran establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados.

- **Procedimientos de operación documentados**

Los procedimientos de operación debieran especificar las instrucciones para la ejecución detallada de cada trabajo incluyendo:

- 1) Procesamiento y manejo de información;
- 2) Copia de seguridad o respaldo;
- 3) Requerimientos de programación de horarios, incluyendo las interdependencias con otros sistemas, los tiempos de culminación y horarios de los primeros y últimos trabajos;
- 4) Instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema;
- 5) Contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas;
- 6) Instrucciones para el manejo de output especial y medios, tales como el uso de papelería especial o el manejo de output confidencial incluyendo los procedimientos para la eliminación segura del output de trabajo fallidos;
- 7) Procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema;
- 8) La gestión de la información del rastro de auditoría y registro del sistema.

Gestión de la entrega de servicio de terceros

Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.

La organización debiera chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados por la tercera persona.

- **Monitoreo y revisión de los servicios de terceros**

El monitoreo y revisión de los servicios de terceros debiera asegurar que se cumplan los términos y condiciones de seguridad de los acuerdos, y que se manejen apropiadamente los incidentes y problemas de seguridad de la información. Esto debiera involucrar una relación y proceso de gestión de servicio entre la organización y la tercera persona para:

- 1) Monitorear los niveles de desempeño del servicio para chequear adherencia con los acuerdos;
- 2) Proporcionar información sobre incidentes de seguridad de la información y la revisión de esta información por terceros y la organización conforme lo requieran los acuerdos y cualquier lineamiento y procedimiento de soporte;
- 3) Revisar los rastros de auditoría de terceros y los registros de eventos de seguridad, problemas operacionales, fallas, el monitoreo de fallas e interrupciones relacionadas con el servicio entregado;
- 4) Resolver y manejar cualquier problema identificado.

- **Manejo de cambios en los servicios de terceros.**

El proceso de manejar los cambios en el servicio de terceros necesita tomar en cuenta los cambios realizados por la organización para implementar:

- Aumentar los servicios ofrecidos actualmente;
- Desarrollo de cualquier aplicación y sistema nuevo;
- Modificaciones o actualizaciones de las políticas y procedimientos de la organización;
- Controles nuevos para solucionar incidentes de la seguridad de la información y para mejorar la seguridad;

- 1) Cambios en los servicios de terceros para implementar;
- 2) Cambios y mejoras en las redes;
- 3) Uso de tecnologías nuevas;
- 4) Adopción de productos nuevos o versiones más modernas;
- 5) Desarrollo de herramientas y ambientes nuevos;
- 6) Cambios en la ubicación física de los medios del servicio;
- 7) Cambio de vendedores.

Planeación y aceptación del sistema

Se debieran realizar proyecciones de los requerimientos de la capacidad futura para reducir el riesgo de sobrecarga en el sistema.

Se debieran establecer, documentar y probar los requerimientos operacionales de los sistemas nuevos antes de su aceptación y uso.

Gestión de la capacidad

Se debiera monitorear, afinar el uso de los recursos y se debieran realizar proyecciones de los requerimientos de capacidad futura para asegurar el desempeño requerido del sistema.

Se debieran aplicar la afinación y monitoreo del sistema para asegurar y, cuando sea necesario, mejorar la disponibilidad y eficiencia de los sistemas. Se debieran establecer detectores de controles para indicar los problemas en el momento debido. Las proyecciones de requerimientos futuros debieran tomar en cuenta los requerimientos de los negocios y sistemas nuevos y las tendencias actuales y proyectadas en las capacidades de procesamiento de la información de la organización.

Monitoreo

Busca detectar las actividades de procesamiento de información no autorizadas.

Se debieran monitorear los sistemas y se debieran reportar los eventos de seguridad de la información. Se debieran utilizar bitácoras de operador y se debieran registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información.

Una organización debiera cumplir con todos los requerimientos legales relevantes aplicables a sus actividades de monitoreo y registro.

- **Registro de fallas**

Se debieran registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con los problemas con el procesamiento de la información o los sistemas de comunicación. Debieran existir reglas claras para manejar las fallas reportadas incluyendo:

- 1) Revisión de los registros de fallas para asegurar que las fallas se hayan resuelto satisfactoriamente;
- 2) Revisión de las medidas correctivas para asegurar que los controles no se hayan visto comprometidos, y que la acción tomada haya sido completamente autorizada.

Adquisición, desarrollo y mantenimiento de los sistemas de información

- **Seguridad en los procesos de desarrollo y soporte**

Mantener la seguridad del software y la información del sistema de aplicación. Se debiera controlar estrictamente los ambientes del proyecto y soporte. Los gerentes responsables por los sistemas de aplicación también debieran ser responsables por la seguridad del ambiente del proyecto o el soporte. Ellos debieran asegurar que todos los cambios propuestos para el sistema sean revisados para chequear que no comprometan la seguridad del sistema o el ambiente de operación.

CAPÍTULO III: DESARROLLO

3.1. Objetivo. Identificar el entorno general de Red Univercom S.C y el papel que desempeña el área de Mesa de Servicios y Centro de Servicios Compartidos para conseguir los objetivos de la empresa.

Para comprender adecuadamente una empresa, es fundamental informarse sobre los aspectos que la constituyen y la identifican. Asimismo, conocer en detalle el área específica que se va a evaluar permitirá obtener una visión clara del panorama y entender la razón de ser de dicha área.

3.1.1. Actividad. Revisar la misión, visión, giro y razón social de la empresa Red Univercom S.C para identificar el propósito y sus objetivos a mediano y largo plazo.

Para conocer de forma general el lugar a evaluar en este caso Aliat universidades y Red Univercom se realiza una investigación a cerca de las metas y objetivos de la empresa, mediante la página web oficial de Aliat Universidades se puede recabar la información de su misión, visión, filosofía y valores y además y breve descripción de los objetivos, para obtener información más detallada se recurrirá a documentos internos para conocer sus objetivos, estructura interna áreas que maneja y el personal que conforma al Campus.

3.1.1.1. Resultados.

Nombre de la entidad económica: Red Univercom.

¿Quiénes son?: Aliat Universidades está conformada por 7 instituciones de Educación Superior, en 13 estados de la República, 28 campus, una plataforma de programas de educación en línea y cerca de 50 mil estudiantes.

Ubicación de una de las sedes de la entidad económica: Av. Zarzaparrillas 85, Villa de las Flores, 55700 San Francisco Coacalco, Méx.

Organigrama de los empleados en el campus:

Líderes de área:

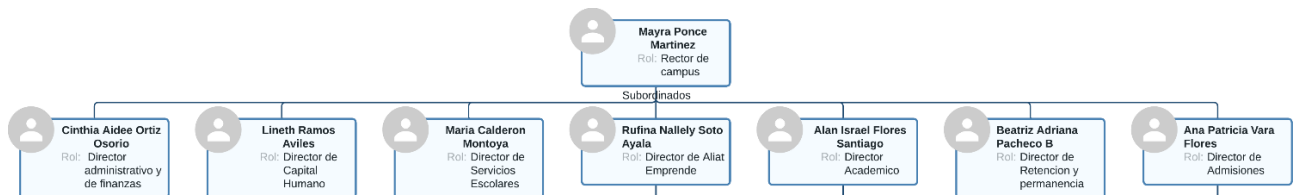


Figura 10. Personal líder de las áreas.

(Fuente: Elaboración propia).

Personal que conforma el área Financiera y de capital humano:

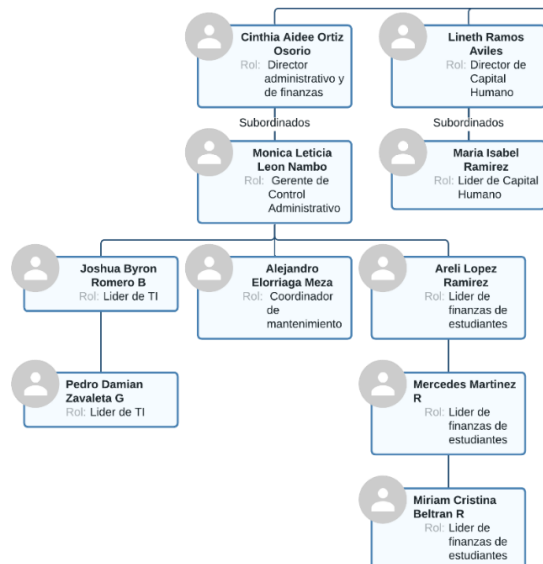


Figura 11. Área administrativa-financiera y capital humano.

(Fuente: Elaboración propia).

Personal que conforma el área de Servicios escolares:

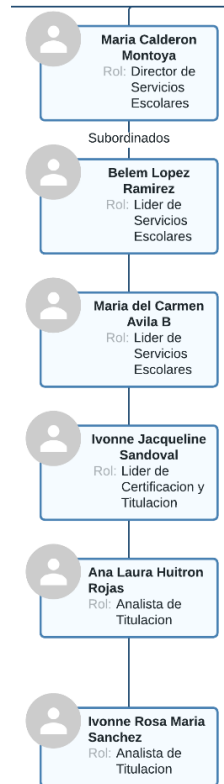


Figura 12. Servicios escolares.

(Fuente: Elaboración propia).

Personal que conforma el área de vinculación:

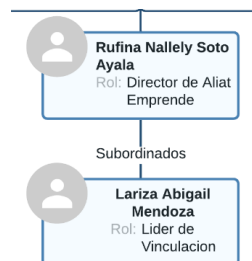


Figura 13. Vinculación.

(Fuente: Elaboración propia).

Personal que conforma el área educativa:



Figura 14. Personal educativo.

(Fuente: Elaboración propia).

Personal que conforma el área de mentoría y retención estudiantil:

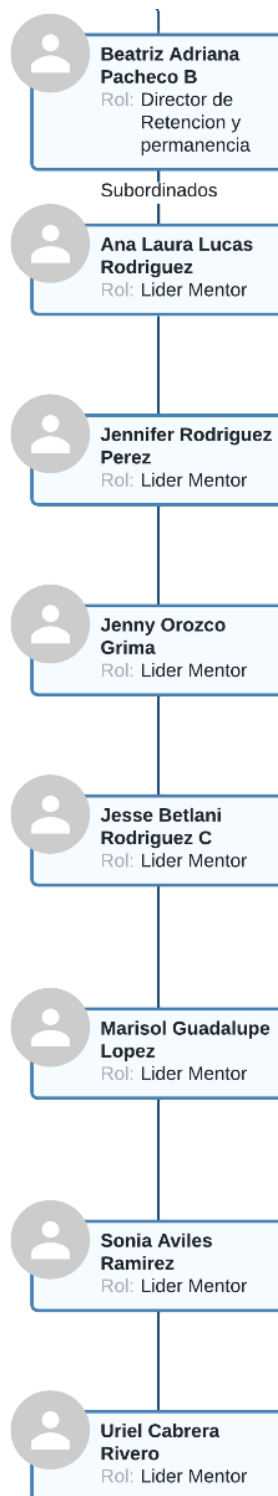


Figura 15. Mentoría y Retención.

(Fuente: Elaboración propia).

Personal que conforma el área de admisiones:



Figura 16. Admisiones.

(Fuente: Elaboración propia).

Sector productivo de la empresa: Servicios educativos.

Misión: Que cada estudiante, docente y colaborador pueda ser la mejor versión de sí mismo y alcance un futuro mejor. ¡Ser mí mejor yo!

Visión: Educación, la llave para transformar vidas.

Filosofía y/o Valores:

- **Innovación:** La conformidad es fracaso. Por eso siempre buscamos nuevas y mejores opciones para alcanzar nuestras metas.
- **Perseverancia:** Convicción de que nadie sabe cuál es su límite y que a través de disciplina, esfuerzo e inteligencia puede alcanzar sus sueños.
- **Agilidad:** Pensamos como líderes, actuamos emprendedores.
- **Excelencia:** Es nuestro estándar y el camino que recorreremos para ser los mejores.
- **Responsabilidad:** Somos 100% responsables; Cero Culpables.

3.1.2. Actividad. Revisar las funciones, procesos, procedimientos, responsabilidades, objetivos, metas y la estructura organizacional del área de Mesa de Servicios y Centro de Servicios Compartidos y como se ligan a los objetivos generales de la empresa.

A fin de conocer el área particular a evaluar, se realiza una entrevista al personal del área de Mesa de Ayuda o mejor conocida en Aliat como Mesa de Servicio; es un área relativamente reciente dentro de Aliat universidades, por lo que muchas de sus funcionalidades son propensas a cambios, readaptaciones e incluso a la implementación de nuevos procesos. Sin embargo, para conocer el área más a profundidad es necesario investigar otras empresas que adopten esta estrategia, que significa y a que se dedica el área de Mesa de ayuda, adicionalmente, dado que ITIL permite adaptarse a las necesidades de cada empresa, es necesario acudir a documentos internos y/o la propia página oficial de Aliat, la cual permitirá obtener información de cómo es que Mesa de Ayuda está adaptada en Aliat y de las funcionalidades que se tienen hasta el momento. De lo entrevistado e investigado se obtuvo lo siguiente:

3.1.2.1. Resultados.

La mesa de servicios es una herramienta esencial para la gestión de servicios de una empresa. Funciona como un centro de atención y gestión, mediante el cual organizaciones públicas y privadas pueden ofrecer una amplia gama de servicios empresariales y de TI a sus usuarios internos y externos.

En Aliat la función de mesa de servicios y de TI es ser el punto de contacto a la recepción de incidentes y requerimientos en la operación basado en las mejores prácticas de ITIL.

Mesa de Servicio trabaja con clientes, los cuales están divididos en administrativos y estudiantes y/o Docentes, el medio de contacto que manejan es mediante correo electrónico, llamadas telefónicas autoservicio y aplicaciones móviles.

Cada requerimiento que se haga será recibido por Mesa de Ayuda, son registrados en la herramienta Remedy la cual es un ITSM (Information Technology Service Management) el cual esta alineado a ITIL.

Los procesos por seguir en Mesa de Servicio en primera estancia, cuando es por medio de un correo electrónico dirigido a Mesa de Ayuda, un Agente de Mesa revisa dicho correo, genera

un ticket y lo asigna el ticket al agente de atención correspondiente y entra al flujo de atención. Al trabajar en autoservicio, el cliente puede generar el ticket directamente.

Mesa de Servicio trabaja en tres niveles, el nivel uno consiste en la recepción, registro y asignación; En el modo de autoservicio, va directamente a la asignación. Este primer nivel está enfocado a resolver problemáticas muy básicas, por ejemplo, revisión de cuentas de correo, problemas en servicios de correo y aplicaciones, etc. En caso de que el problema persista o el agente de primer nivel desconozca los métodos de resolución, es cuando se escala al siguiente nivel de servicio.

El siguiente nivel o Nivel dos de servicio está dividido en torres de servicio las cuales están catalogadas en Servicios Administrativos y de Negocio, Servicios Financieros, Servicios Escolares y Servicios de TI. Dependiendo el foro solicitante podrá tener acceso a ciertos servicios. El primer y segundo nivel se encuentran dentro de la institución Aliat.

El tercer nivel es atendido por las empresas proveedoras de los servicios, en el caso de Aliat sus proveedores son Microsoft, Oracle, Telmex, entre otros.

Lo anterior se ejemplifica en el siguiente cuadro:

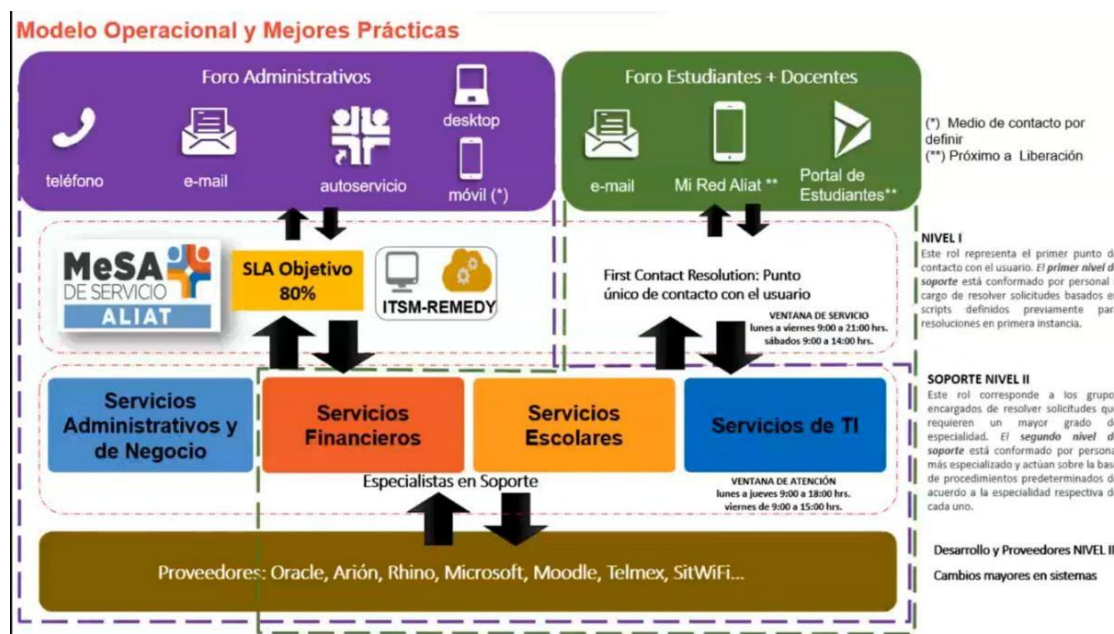


Figura 17. Modelo operacional.

(Red Univercom, 2020).

Cada solicitud (Ticket) genera un SLA que puede aumentar y tiene un tiempo de atención distinto. Por ello es por lo que se tienen catálogos de servicios, los cuales dividen los servicios en categorías, servicios generales, servicios financieros, servicios de TI y servicios de negocio, alineados a las torres de servicio mostrados en la imagen del Modelo operacional.

Catálogo de servicios Definición de SLA por servicio					
MeSA DE SERVICIO ALIAT					
CATEGORIA DE SERVICIO	SERVICIO	ESTATUS	Acuerdo - SLA	PRIORIDAD	Total
Servicios generales	Servicio de Incidencias y Requerimientos de Telefonía Móvil	En línea	24 hrs	Baja	6
	Bitácora de Asistencia – Limpieza y Vigilancia	En línea	16 hrs	Baja	
	Reporte de Incidencias y Requerimientos de Mensajería	En línea	16 hrs	Baja	
	Solicitud de Factura para Baja por Sinistro	En línea	16 hrs	Baja	
	Movimiento de Activo Fijo	En línea	40 hrs	Baja	
	Solicitud de Estado de Cuenta	En línea	8 hrs	Media	
Servicios Financieros	Solicitud de Alta de Proveedores	En línea	24 hrs	Baja	16
	Comprobaciones y Reembolsos	En línea	40 hrs	Baja	
	Solicitud de Alta de Proveedores Honorarios Docentes	En línea	24 hrs	Baja	
	Anticipo a Empleados	En línea	40 hrs	Baja	
	Solicitud de Alta y Asignación de Artículos	En línea	10 hrs	Baja	
	Solicitud de Cotización	En línea	24 hrs	Baja	
	Alta de Valores de Segmentos Contables	En línea	24 hrs	Baja	
	Google y Facebook	En línea	8 hrs	Media	
	Devolución de Pago al Alumno	En línea	8 hrs	Media	
	Recibos Estándar	En línea	8 hrs	Media	
	Condonaciones	En línea	8 hrs	Media	
	Solicitud de Combinaciones Contables	En línea	4 hrs	Media	
	Orden de Compra Urgente	En línea	8 hrs	Media	
	Consulta de Artículos	En línea	8 hrs	Media	
	Solicitud de Comprobantes	En línea	8 hrs	Media	
	Reclasificaciones	En línea	8 hrs	Media	

Figura 18. Catálogo de servicios generales y financieros.

(Red Univercom, 2020).

Catálogo de servicios Definición de SLA por servicio					
MeSA DE SERVICIO ALIAT					
CATEGORIA DE SERVICIO	SERVICIO	ESTATUS	Acuerdo - SLA	PRIORIDAD	Total
Servicios de TI	Combo Incidentes CRM	En línea	2 hrs	Alta	19
	Análisis y Gestión de Nuevos Requerimientos a los Sistemas	En línea	N/A	N/A	
	Gestión de Correo Electrónico Institucional	En línea	8 hrs	Media	
	Habilitación de Servicios de Voz	En línea	16 hrs	Baja	
	Infraestructura Red de Datos	En línea	Conectividad remota - VPN	Baja	
	Conectividad remota - VPN	En línea	Apertura de puertos	Baja	
	Infraestructura Red de Datos	En línea	Configuración de acceso a Internet	Media	
	Configuración de acceso a Internet	En línea	Acceso a la red inalámbrica	Media	
	Infraestructura Red de Datos	En línea	Acceso a la red inalámbrica	Media	
	Acceso a la red inalámbrica	En línea	8 hrs	Media	
	Instalación de Equipos de Cómputo de Oficina	En línea	16 hrs	Baja	
	Instalación y/o Configuración de Software Institucional	En línea	8 hrs	Media	
	Mantenimiento Preventivo/Correctivo a Equipo de Cómputo Institucional	En línea	8 hrs	Alta	
	Lentitud en Aplicaciones Administrativas	En línea	10 min	Crítica	
		En línea	2 hrs	Crítica	
		En línea	16 hrs	Media	
		En línea	2 hrs	Alta	
	No Disponibilidad de Aplicaciones Administrativas	En línea	10 min	Crítica	
		En línea	4 hrs	Media	
		En línea	16 hrs	Baja	

Figura 19. Catálogo de servicios de TI.

(Red Univercom, 2020).

Catálogo de servicios Definición de SLA por servicio					
					MeSA DE SERVICIO ALIANZA
CATEGORIA DE SERVICIO	SERVICIO	ESTATUS	Acuerdo - SLA	PRIORIDAD	Total
Servicios de Negocio	Matriculación/Reinscripción/Baja Prepa Flex	En línea	1 hra	Alta	13
	Solicitud de Carga de Datos en Campus Solutions	En línea		Alta	
	Apertura Lógica de Nueva Zona o Campus	En línea	68 días	Baja	
	Expansión-Apertura Lógica de Nueva Zona o Campus	En línea	30 días	Media	
	Matriculación/Re-inscripción/Baja Programa Empréndete	En línea	6 hrs	Media	
	Facturación Anticipada / Manual	En línea	8 hrs	Media	
	Carga de Datos Docentes	En línea	8 hrs	Media	
	Atención de Solicitudes de Aplicaciones Administrativas	En línea	4 hrs	Media	
	Generación de Reportes	En línea	8 hrs	Media	
	Administración de Cuentas de Acceso a Aplicaciones Administrativas	En línea	6 hrs	Media	
	Administración de Envío de Correos Masivos (Comunicados)	En línea	N/A	N/A	
	Mantenimiento preventivo/correctivo al sistema	En línea	N/A	N/A	
	Timbrado de Nómina	En línea	N/A	N/A	

Figura 20. Catálogo de servicios de negocio.

(Red Univercom, 2020).

Son servicios que son de alta demanda en la empresa, sin embargo, Mesa de Servicio no atiende situaciones que se encuentran fuera de sus categorías ya identificadas, en ocasiones requiere reforzar con las demás áreas en casos poco comunes o que requieren un proceso diferente. Mesa de Servicio cuenta con un catálogo de servicios tipificado. Este catálogo de servicios puede ser ampliado conforme los usuarios levanten incidencias o enviando solicitudes y requerimientos, se van tipificando y cuantificando.

Entonces la estructura organizacional del área de Mesa de Servicios y Centro de Servicios Compartidos es una rama del área de TI dentro de la institución, esta área cuenta con un gerente el cual se encarga de catalogar y establecer nuevos servicios, su segundo al mando en el área se encarga de gestionar las funcionalidades de la aplicación y a los agentes de mesa de servicio y por último se tienen a los agentes de masa los cuales atienden las solicitudes que llegan al área pero, estos agentes son enfocados a plataformas y/o solicitudes distintas, por lo que mesa de servicio queda distribuida como en el esquema siguiente:

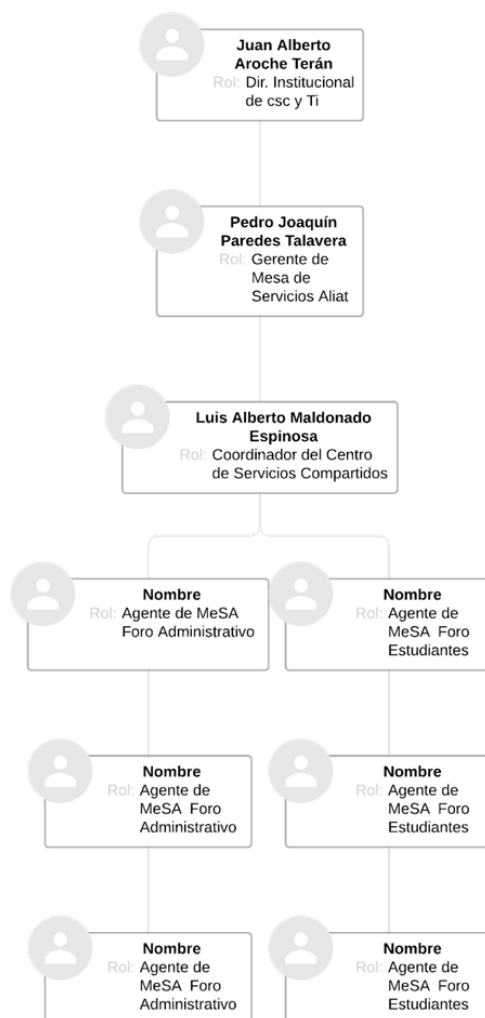


Figura 21. Puestos y personal de Mesa de Servicio.

(Fuente: Elaboración propia).

Este personal tiene como funciones principales cubrir lo siguiente:

- Brindar atención a reportes vía telefónica.
- Atender reportes mediante las herramientas de gestión de tickets (incidencias/requerimientos), asignado un folio al incidente y manteniendo al usuario informado del estatus del ticket que se han generado en su nombre.
- Mantener al usuario informado de los cambios tecnológicos.
- Dar seguimiento al incidente hasta su solución final.
- Verificar el estatus del reporte de usuario con el área/departamento al que fue asignado.

- Asignar el incidente al siguiente nivel de atención.
- Documentar el problema.
- Interpretar y documentar a nivel técnico el reporte del incidente para poder escalarlo al siguiente nivel, llevando a cabo todo lo necesario para cumplir con procedimientos y políticas del área de informática.
- Aplicación de encuesta en línea al momento de la resolución del reporte de servicio.
- Registrar en la herramienta de gestión de incidencias las calificaciones y comentarios que se otorgaron por parte de los usuarios.

Los objetivos de Mesa de Servicios es la de concentrar todas las áreas, ya sea de finanzas, Recursos Humanos, servicios legales, fiscales, compras, funciones de ventas comerciales, etc., y en una sola estructura para quitar las actividades transaccionales y así los directores de área den mayor atención a las actividades estratégicas para que los equipos se especialicen.

Además, cada Ticket se monitorea teniendo en cuenta el día de creación, quien los creo, el estado en el que se encuentran y si están dentro de la ventana de servicio (SLA), de esta forma se tiene el historial del Ticket y del servicio para además tener un seguimiento, control y atención en tiempo y forma de estos.

3.2. Objetivo. Analizar información detallada sobre los servicios que el área ofrece a los usuarios, referente a correo electrónico y Remedy por parte de la empresa.

Comprender cómo mesa de servicios compartidos ofrece atención mediante los sistemas que la empresa gestiona permitirá conocer con mayor detalle los procesos involucrados y cómo el área brinda soporte a estudiantes, docentes y personal administrativo.

3.2.1 Actividad. Establecer los formatos de las entrevistas, análisis FODA y matrices de evaluación que se usaran para la recopilación y análisis de la información.

A fin de documentar con precisión este análisis, se hace un diseño y selección de formatos para su pertinente documentación. Se diseñan las preguntas abiertas que se aplican al personal de Mesa de Servicio encargados de las funciones de correo electrónico y manejo del ITSM Remedy, que después de realizada la entrevista se verá sujeta a un resumen recopilatorio de datos importantes. Al ser un área con poco personal se optó por una

entrevista para recabar la mayor información posible a cerca de dichos servicios, posteriormente se establecerán los formatos de las tablas y recuadros que tendrá el análisis FODA, Identificación de riesgos y probabilidad e impacto, que se utilizarán para examinar la información recabada.

3.2.1.1. Resultados.

Entrevista para el personal encargado de los servicios de correo electrónico.

Las siguientes preguntas se formularon de manera abierta para comprender e identificar las funciones, interacciones y contextualizar la prestación de los servicios de correo en Red Univercom.

Las preguntas que se realizaran en la entrevista son las siguientes:

- 1) ¿Quién es el encargado de los servicios de correo electrónico?
- 2) ¿Cuáles son los roles que se manejan en esos servicios?
- 3) ¿Cuál es el procedimiento para brindar los servicios de correo electrónico?
- 4) ¿Los procedimientos están documentados?
- 5) Cuando sucede algún incidente de seguridad ¿Qué es lo primero que se hace?
- 6) ¿Qué tan común es que presenten fallos en los servicios de correo electrónico?
- 7) ¿Qué problemas han sido más frecuentes en los servicios de correo electrónico?
- 8) ¿En que afectaría si no estuvieran disponibles los servicios de correo electrónico?
- 9) ¿Qué prácticas de seguridad se llevan a cabo en los servicios de correo electrónico?
- 10) ¿Estas prácticas de seguridad están bajo alguna norma o estándar?, ¿Cuáles?
- 11) ¿Cuál es el proceso para crear las cuentas de correo electrónico?
- 12) ¿Qué otras aplicaciones y funciones dependen del correo electrónico tanto de estudiantes, docentes y administrativos?
- 13) ¿Se está al tanto del límite de los servicios de correo electrónico proporcionados por el proveedor?

Entrevista para el personal encargado de los servicios de Remedy.

De igual manera, para conocer el funcionamiento y la operación que se tiene con el ITSM Remedy se le aplicaran preguntas abiertas al encargado de gestión y operación de dicha herramienta.

Las preguntas que se realizaran en la entrevista son las siguientes:

- 1) ¿Qué es Remedy y para que le sirve a la institución?
- 2) ¿Quién es el encargado de brindar los servicios de Remedy?
- 3) ¿Cuáles son los roles que se manejan en Remedy?
- 4) ¿Cuál es el procedimiento para brindar los servicios de Remedy?
- 5) ¿Los procedimientos están documentados?
- 6) Cuando sucede algún incidente de seguridad ¿Qué es lo primero que se hace?
- 7) ¿Qué tan común es que presenten fallos en los servicios de Remedy?
- 8) ¿Qué problemas han sido más frecuentes en los servicios de Remedy?
- 9) ¿En que afectaría si no estuvieran disponibles los servicios de Remedy?
- 10) ¿Qué prácticas de seguridad se llevan a cabo en los servicios de Remedy?
- 11) ¿Estas prácticas de seguridad están bajo alguna norma o estándar?, ¿Cuáles?
- 12) ¿Qué otras aplicaciones y funciones dependen de Remedy tanto de estudiantes, docentes y administrativos?

Entrevista al encargado de Infraestructura Tecnológica y Seguridad de Aliat

- 1) ¿Cuáles fueron los problemas técnicos que llevaron a la migración del sistema?
- 2) ¿Hubo razones económicas que impulsaron la migración?
- 3) ¿El nuevo servidor ofrece el rendimiento y velocidad esperados?
- 4) ¿El nuevo servidor ofrece una mayor escalabilidad para afrontar crecimientos futuros?
- 5) ¿Cómo se planificó y ejecutó el proceso de migración?
- 6) ¿Cuáles fueron los problemas durante la migración y cómo se abordaron?
- 7) ¿El servidor en el que se migró el sistema es propiedad de la empresa o es proporcionado por un proveedor externo?
- 8) ¿Cuál es el modelo y especificaciones técnicas de dicho servidor?
- 9) En caso de que el servidor principal presente algún problema:
- 10) ¿Cuentan con algún plan de contingencia? ¿En qué consiste?
- 11) ¿Cuentan con algún servidor auxiliar?
- 12) ¿Cuentan con algún respaldo de la información?
- 13) ¿Se realizan revisiones posteriores para mejorar los protocolos de respuesta y planes de contingencia?

Una vez recabada la información mediante un cuadro de análisis FODA se destacarán los puntos fuertes y dificultades, partiendo de la propia empresa hasta el área la cual se está evaluando.

FORTALEZAS	OPORTUNIDADES
DEBILIDADES	AMENAZAS

Figura 22. Ejemplo de cuadro de análisis FODA.

(Fuente: Elaboración propia).

En esta tabla se busca agrupar a aquellas vulnerabilidades y amenazas que generen un riesgo en común, de esta forma permite visualizar cuales son los riesgos que deben de ser atendidos lo antes posible para mitigar la mayor parte de vulnerabilidades y amenazas posible.

Vulnerabilidad	Amenaza	Riesgo

Figura 23. Ejemplo de cuadro de identificación de riesgos.

(Fuente: Elaboración propia).

Para determinar la probabilidad de que alguna vulnerabilidad ocurra y el nivel de impacto que está tiene en la operatividad de la empresa se usara el siguiente cuadro el cual determinara los valores mediante la percepción que los usuarios tienen de los ámbitos a evaluar.

	Vulnerabilidad:				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Probabilidad	Raro	Poco Probable	Moderado	Casi Seguro	seguro
¿Con que frecuencia considera que ocurre este riesgo?					
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					

Figura 24. Ejemplo de evaluación de los riesgos.

(Prado, 2009).

Una vez evaluada la probabilidad y el nivel de impacto de estas se tabularán para determinar si son amenazas que afectan gravemente a la operación, de esta forma se puede tener una idea de la gravedad y atención que se le tiene que dar a las diferentes vulnerabilidades.

Nivel de impacto Probabilidad	Descripción de la vulnerabilidad o amenaza				
	1. Insignificante	2. Menor	3. Significativo	4. Mayor	5. Severo
1. Raro					
2. Poco Probable					
3. Moderado					
4. Casi Seguro					
5. Seguro					

Figura 25. Ejemplo de probabilidad e impacto.

(Prado, 2009).

En esta tabla se busca ordenar las vulnerabilidades priorizando las que tengan una alta probabilidad de suceder y que causen un mayor impacto en la organización y las operaciones diarias.

Vulnerabilidades	Probabilidad	Impacto	Nivel de prioridad

Figura 26. Ejemplo de escalas de probabilidad del riesgo.

(Fuente: Elaboración propia).

Una vez determinado el orden de atención de las vulnerabilidades se colocarán las recomendaciones que los estándares, normas y guías establecen para prevenir dichos riesgos.

Vulnerabilidades	Amenazas	Riesgos	Recomendaciones

Figura 27. Ejemplo de tabla de recomendaciones para la mitigación de riesgos.

(Fuente: Elaboración propia).

Al establecer las vulnerabilidades se determinarán las afectaciones monetarias que conlleva el no atender cualquiera de las vulnerabilidades y en base a ITIL, establecer la pérdida en el valor del servicio.

Vulnerabilidad	Perdida monetaria aproximada del impacto de la vulnerabilidad (MXN)	Pérdida de Valor en el nivel del servicio.

Figura 28. Ejemplo de pérdidas monetarias y de nivel de servicio.

(Fuente: Elaboración propia).

En esta tabla se busca determinar las propuestas que ayuden a prevenir y/o solucionar los riesgos, dichas propuestas deben estar basadas en las recomendaciones que las diferentes normas, estándares y guías proponen, las propuestas son de tres tipos, la propuesta preventiva es una solución inmediata que pueda mitigar el riesgo de manera temporal o que abarque el mayor número de amenazas y vulnerabilidades posibles, la propuesta correctiva busca remediar con el riesgo, las amenazas y las vulnerabilidades por completo, puede requerir de una inversión o una mejora en el proceso y la propuesta de pago puede funcionar como una propuesta correctiva la cual puede tratarse de una única inversión o bien puede ser un nuevo gasto que se puede tener la empresa que solucione la problemática.

Riesgo	
Amenaza	Vulnerabilidad
Recomendaciones	
Propuesta Preventiva	
Propuesta Correctiva	
Propuesta de Pago	

Figura 29. Cuadro de propuestas de solución.

(Fuente: Elaboración propia).

Si alguna de las soluciones requiere una mejora en algún proceso o la implementación de un nuevo proceso, se usará la siguiente tabla para describir la actividad a seguir para realizar el proceso, así como la persona encargada de gestionar la actividad.

No.	Puesto u/o sistema	Descripción de la actividad.

Figura 30. Ejemplo de tabla de especificaciones de los procesos a implementar.

(Fuente: Elaboración propia).

3.2.2. Actividad. Solicitar información acerca de los servicios de correo electrónico y Remedy a través de una entrevista al personal que conforma el área en evaluación.

Los servicios y aplicaciones que maneja Red Univercom dependen tanto de la herramienta Remedy que los provee BMC Remedy ITSM y los Servicios de correo electrónico que los provee Microsoft. De esta forma es necesario realizar dos entrevistas de preguntas abiertas, una referente a los servicios de correo electrónico la cual se le aplicara al Gerente de servicios Pedro Joaquín Paredes Talavera y otra referente a los servicios de Remedy que se le aplicara al Coordinador de CSC y encargado de supervisar el ITSM Remedy Luis Alberto Maldonado

Espinoza para conocer cómo es que trabajan estos dos servicios y si es que dependen entre sí, ambos encargados forman parte del área de Mesa de Servicio.

3.2.2.1. Resultados.

Respuestas del encargado de los servicios de correo a la entrevista.

La respuesta del encargado a las preguntas respecto a los servicios de correo son las siguientes:

- **Eduardo Uriel (Entrevistador):** Buenos días, esta entrevista es referente a lo que es los sistemas de correo electrónico, los servicios. Ahora sí que, para comenzar, ¿podría decirnos su nombre y el puesto o cargo que ocupa?
- **Pedro Joaquín (Entrevistado):** Mi nombre es Pedro Paredes, ocupo el cargo de Gerente de Servicios Centralizados, Cadena B, y Mesa de Servicio Aliat.
- **Eduardo Uriel (Entrevistador):** Para comenzar, la primera pregunta es, ¿quién es el encargado de proporcionar los servicios de correo electrónico?
- **Pedro Joaquín (Entrevistado):** Este es un servicio que se solicita a través de Capital Humano, en todo lo que es el onboarding, nuevas contrataciones y nosotros, como Mesa de Servicio, lo gestionamos, o gestionamos el alta, generamos el alta, tanto en O 365 como en el directorio activo, pero siempre considerando una solicitud vía Ticket Remedy de Capital Humano.
- **Eduardo Uriel (Entrevistador):** La siguiente pregunta es, ¿cuáles son los roles que se manejan en esos servicios? En los servicios de correo electrónico.
- **Pedro Joaquín (Entrevistado):** Como tal tenemos usuarios que son de tipo administrativo, con una licencia asociada a ellos en particular, docentes y estudiantes.
- **Eduardo Uriel (Entrevistador):** ¿cuál es el procedimiento para brindar los servicios de correo electrónico en esos roles?
- **Pedro Joaquín (Entrevistado):** Si es un administrativo, como te digo, tiene que venir desde una solicitud inicial de Capital Humano, nosotros validamos en HCM que exista ya dado de alta el colaborador y con base a esto damos la creación de la cuenta siguiendo el estándar, que es nombre y apellido, más el dominio a la institución que pertenece, para el tema de docentes, también hacemos esta revisión, pero nos aseguramos que su rol sea de docente y en el tema de estudiantes, lo que hacemos es revisamos en Campus Solution, que es nuestro sistema de gestión financiera y académica, que el estudiante esté activo en lo que es su programa plan del ciclo actual y podemos entonces dar de alta a los usuarios, si no se cumplen estas reglas de negocio, nosotros no damos de alta a ningún usuario, administrativo o docente y estudiante.

- **Eduardo Uriel (Entrevistador):** La siguiente pregunta es, ¿cuáles son los procedimientos? ¿Están documentados?
- **Pedro Joaquín (Entrevistado):** Sí, existen políticas, y existe la política de atención mesa de servicio y la política de capital humano, alta de usuarios.
- **Eduardo Uriel (Entrevistador):** La siguiente pregunta es, cuando sucede algún incidente de seguridad, ¿qué es lo primero que se hace?
- **Pedro Joaquín (Entrevistado):** Inicialmente, la cuenta se le cambia la contraseña, se deshabilita el inicio de sesión, se deshabilita la cuenta y se informa a seguridad informática para que nadie más haga uso de la cuenta y también a sol icitud de capital humano.
- **Eduardo Uriel (Entrevistador):** La siguiente pregunta es, ¿qué tan común es que se presenten fallos en los servicios de correo electrónico?
- **Pedro Joaquín (Entrevistado):** Bueno, siendo un servicio administrado por el proveedor que es Microsoft, es difícil que se presente, sí se ha llegado a presentar y hemos tenido suspensión, pero no más allá de dos o tres horas en todos los servicios de O365.
- **Eduardo Uriel (Entrevistador):** ¿Qué problemas han sido más frecuentes en esos servicios de correo electrónico?
- **Pedro Joaquín (Entrevistado):** El problema más recurrente es que el usuario no puede iniciar sesión o porque desconoce su contraseña o porque no está haciendo correcto uso del proceso a la autenticación dos pasos que hoy se requiere para asegurar la personalidad del usuario de la cuenta.
- **Eduardo Uriel (Entrevistador):** La pregunta que sigue es, ¿en qué afectaría si no tuvieran disponibles los servicios de correo electrónico?
- **Pedro Joaquín (Entrevistado):** Bueno, el correo electrónico para nosotros hoy en operación es una herramienta de emisión crítica, propiamente si no la tenemos afecta la operación sin detenerla en un 100%, pero sí afecta muchos de los flujos que se tienen porque incluso las autorizaciones y flujos en los procesos están basados en el envío de correo electrónico, entonces no teniéndolo tendríamos una afectación prácticamente de un 99% de suspensión de la actividad.
- **Eduardo Uriel (Entrevistador):** La siguiente pregunta sería, ¿qué prácticas de seguridad se llevan a cabo en los servicios de correo electrónico?
- **Pedro Joaquín (Entrevistado):** Bueno, las prácticas de seguridad son las que competen directamente al usuario. Se les informa al momento de hacerles la entrega de su contraseña que son contraseñas personalizadas, no transferibles y que deben de estar haciendo cambio de su contraseña con regularidad y obviamente que hagan uso de la autenticación dos pasos que siempre está activa, en ningún momento se para.
- **Eduardo Uriel (Entrevistador):** La pregunta que sigue sería, ¿estas prácticas de seguridad están bajo alguna norma o estándar? Y si es así, ¿cuáles?
- **Pedro Joaquín (Entrevistado):** Son políticas de seguridad, políticas de seguridad de nosotros, están en reglamento interno, no estoy claro a qué norma podría estar

afectando, pero son cuestiones internas y hacen referencia a nuestro reglamento interno de trabajo.

- **Eduardo Uriel (Entrevistador):** La pregunta que sigue, ¿cuál es el proceso para crear las cuentas de correo electrónico?
- **Pedro Joaquín (Entrevistado):** Ya te lo había comentado, una solicitud de capital humano, una validación a la procedencia de que el usuario esté contratado, que tenga el rol que se menciona, que el estudiante esté activo al programa y plan y con esto es como se generarán las cuentas. Obviamente asignándole la licencia de uso que le corresponde, según su rol.
- **Eduardo Uriel (Entrevistador):** La pregunta que sigue es, ¿qué otras aplicaciones y funciones dependen del correo electrónico, tanto de estudiantes, docentes y administrativos?
- **Pedro Joaquín (Entrevistado):** Como te decía, prácticamente dependen todas, el correo electrónico incluso lo utilizamos como single sign-on para nuestra red móvil, apps estudiantes, apps docentes, pago en línea, Remedy, son varias las aplicaciones que están relacionadas al correo electrónico, flujos de autorización, Service Now, todo lo que es el proceso de asignación, respuesta, está basado sobre el correo electrónico hay varios que están ahí y los que te mencioné son los más importantes.
- **Eduardo Uriel (Entrevistador):** Y como última pregunta, ¿se está al tanto del límite de los servicios de correo electrónico proporcionados por el proveedor?
- **Pedro Joaquín (Entrevistado):** Lamentablemente sí, porque esto ya nos ha llegado a afectar, como tú lo sabes, en la creación de cuentas. De repente ya hemos llegado al límite de nuestra cuota y esto hace que sí estemos revisando y depurando nuestras cuentas con cierta regularidad, que es la actividad en la cual viniste a apoyarnos.
- **Eduardo Uriel (Entrevistador):** Ok, eso sería todo. Muchas gracias.
- **Pedro Joaquín (Entrevistado):** Gracias a ti.

Respuestas del encargado de los servicios de Remedy a la entrevista.

La respuesta del encargado a las preguntas respecto a los servicios de Remedy son las siguientes:

- **Eduardo Uriel (Entrevistador):** Buenas tardes, esta entrevista es referente acerca de los servicios de Remedy, así que para empezar por favor nos puede decir su nombre y el puesto que ocupa.
- **Luis Alberto (Entrevistado):** Sí, mi nombre es Luis Alberto Maldonado, soy coordinador de Centro de Servicios Compartidos.
- **Eduardo Uriel (Entrevistador):** Ok, para empezar la primera pregunta es ¿qué es Remedy y para qué le sirve a la institución?

- **Luis Alberto (Entrevistado):** Remedy es el ITSM que ocupamos dentro de la empresa para poder llevar todo lo que es el seguimiento de los tickets.
- **Eduardo Uriel (Entrevistador):** Ok, siguiente pregunta ¿quién es el encargado de brindar los servicios de Remedy?
- **Luis Alberto (Entrevistado):** En este caso soy yo el encargado de hacer toda la configuración de los servicios de Remedy y todo lo que es el seguimiento de estos también.
- **Eduardo Uriel (Entrevistador):** Ok, siguiente pregunta ¿cuáles son los roles que se manejan en Remedy?
- **Luis Alberto (Entrevistado):** Existen dos roles, un rol es principalmente que es el de usuario solicitante y el de gestor o usuario asignado.
- **Eduardo Uriel (Entrevistador):** Ok, ¿los procedimientos están documentados? Esos que se usan para dar los servicios o el alta.
- **Luis Alberto (Entrevistado):** Sí, todos nuestros procedimientos están documentados y se basan sobre lo que es el ITIL.
- **Eduardo Uriel (Entrevistador):** Ok, cuando sucede algún incidente de seguridad ¿qué se hace? ¿Qué es lo primero que se hace?
- **Luis Alberto (Entrevistado):** Principalmente cuando es por tema de vulnerabilidad se hace lo que es el reinicio de contraseñas de los correos electrónicos para poder detener ahí el proceso y no haya fuga de información.
- **Eduardo Uriel (Entrevistador):** Ok, ¿qué tan común es que se presenten fallas en los servicios de Remedy?
- **Luis Alberto (Entrevistado):** Últimamente sí ha ocurrido bastantes fallas en cuestión de lentitud, estamos trabajando ahorita para poder cambiar la infraestructura a otro servidor y poder tener un mejor servicio.
- **Eduardo Uriel (Entrevistador):** Ok, ¿y qué problemas han sido más frecuentes
- **Luis Alberto (Entrevistado):** Principalmente la lentitud en el servidor.
- **Eduardo Uriel (Entrevistador):** Ok, ¿en qué afectaría si no estuvieran disponibles los servicios de Remedy?
- **Luis Alberto (Entrevistado):** Pues prácticamente estaríamos deteniendo toda la operación ya que en la actualidad Remedy es un punto de contacto para localizarse. Que es el soporte de administrativos, docentes y alumnos. Entonces el tener detenido la plataforma de mesa de servicio sí impactaría bastante en la operación.
- **Eduardo Uriel (Entrevistador):** Ok, ¿qué prácticas de seguridad se llevan a cabo en los servicios de Remedy?
- **Luis Alberto (Entrevistado):** Ahorita vamos a aplicar algunos parches para poder hacer algunas actualizaciones acerca de la herramienta y pues principalmente se tiene actualizado.
- **Eduardo Uriel (Entrevistador):** ¿estas prácticas de seguridad están bajo alguna norma o estándar y si es así, ¿cuáles?
- **Luis Alberto (Entrevistado):** Sí, Remedy está basado sobre las mejores prácticas que es el ITIL y es principalmente lo que es la contestación del alumno o del usuario

de uno a uno. Si el usuario pide información, únicamente al usuario se le entrega esa información, no a algún tercero.

- **Eduardo Uriel (Entrevistador):** Ok, y como última pregunta, ¿qué otras aplicaciones y funciones dependen de Remedy, tanto en estudiantes, docentes o administrativos?
- **Luis Alberto (Entrevistado):** En la actualidad tenemos ligado a Remedy con otros aplicativos como es la app de estudiantes y app docentes y estamos por migrar a algunos otros servicios como desde páginas web, nos pueden contactar los alumnos o los estudiantes para poder generar alguna solicitud.
- **Eduardo Uriel (Entrevistador):** Ok, eso sería todo. Muchas gracias. Muchas gracias.

Respuestas a la entrevista del subdirector de Infraestructura Tecnológica y Seguridad de Aliat

Como complemento se realizó una entrevista al subdirector de Infraestructura Tecnológica y Seguridad de Aliat. A cerca del proceso de migración de Remedy, el cual se tenía planeado desde hace un tiempo.

- **Eduardo Uriel (Entrevistador):** Hola, mi nombre es Eduardo Uriel Junco Ortiz. Voy a realizar una entrevista referente a la migración de los servicios de Remedy. Por favor, ¿podría empezar diciéndome cuál es su nombre y el cargo que ocupa?
- **Carlos Bermeo (Entrevistado):** Sí, Carlos Bermeo Cruz. Soy subdirector de Infraestructura Tecnológica y Seguridad, igualmente de TI, aquí en Aliat.
- **Eduardo Uriel (Entrevistador):** Ok. La primera pregunta sería, ¿cuáles fueron los problemas técnicos que llevaron a la migración del sistema?
- **Carlos Bermeo (Entrevistado):** Ok. La primera de ellas es una estrategia por mejorar el performance del mismo sistema, ¿no?, Ya que empezaba a presentarse las lentitudes, por ahí más constantes acerca de las bases, depuraciones, etcétera. O sea, ya se estaba viendo limitado en recursos, en primera. En segunda, un poquito de obsolescencia acerca de los equipos actuales, en los equipos anteriores, más bien en los que estaban. Y que, pues, dado la actualización, precisamente, tecnológica ya de los equipos, pues tuvimos que hacer esta migración, ¿no? Pasarlo de una tecnología a otra.
- **Eduardo Uriel (Entrevistador):** Ok. ¿Había razones económicas que impulsaron la migración?
- **Carlos Bermeo (Entrevistado):** Sí, una parte, sí, era económica, también, dado que conservarlo en un equipo más, digamos, con mayor antigüedad, pues esto nos traía un mayor coste de mantenimiento, ¿no? Acerca de este equipo que estaba. Y, pues,

lo hicimos más eficiente al pasarlo a un equipo de... de nueva generación, un equipo que todavía, a lo mejor, tiene piezas disponibles, que cuenta con una póliza extendida de soporte y todo esto, pues, tiene, pues, de cierta manera, también un menor coste de mantenimiento, el que lo tengamos en un equipo más reciente.

- **Eduardo Uriel (Entrevistador):** Ok. ¿El nuevo servidor ofrece el rendimiento y velocidad esperados?
- **Carlos Bermeo (Entrevistado):** Sí, sí, este, dado que es un equipo, pues, digamos, reciente. Última generación con un procesador mucho mejor, unos discos, este, antes eran de estado mecánico los discos, ahora son discos de estado sólido. Entonces, pues, sí, mejoran en diversos, este, factores y aspectos las condiciones en las cuales está físicamente y, pues, esto hace que mejore el performance del sistema.
- **Eduardo Uriel (Entrevistador):** Ok. ¿El nuevo servidor ofrece mayor escalabilidad para afrontar crecimientos futuros?
- **Carlos Bermeo (Entrevistado):** Sí. El nuevo servidor todavía está preparado como para crecer más en discos, aunque, aunque, este, para los requerimientos que tiene el sistema, digamos que está, en donde está alojado, está sobrado. Entonces, digamos que, por el momento, hablar de una escalabilidad del sistema en caso de requerirse, ¿no? Está con muy buenos recursos, por lo menos asegurado en unos tres años, está asegurado con recursos suficientes. Aun así, el servidor soporta, pues, mayores capacidades, tanto de disco, memoria, etcétera, ¿no? El procesador.
- **Eduardo Uriel (Entrevistador):** Ok. ¿Cómo se planificó y ejecutó el proceso de migración?
- **Carlos Bermeo (Entrevistado):** Bien. Primeramente, nació de la necesidad, ajá, que nos exponía, pues, el equipo que lleva el sistema, ¿no? De Remedy y todo lo que es mesa de servicio y todos ellos. En su día a día empezaban a notar esta... Esta deficiencia, este, esta lentitud, el problema con el trabajo, etcétera. Entonces, de ahí es que se comienza un análisis acerca de cuáles eran las causas. Se empieza a ver algunas... Intentar levantar el sistema de una manera que fuera, este, más eficiente a través de ciertos tuneos a la base, de mantenimientos, etcétera. Por ahí también... También el proveedor del sistema colaboró con parte de ellos para poder, este, ir, ir, este, metiendo mano al sistema y hacerle algunas mejoras. Como esto no funcionó, pues, siguió el siguiente paso, pues, ya era incrementar recursos, ¿no? Planear una nueva estrategia incluso de separación de servidores. Entonces, ¿por qué? Porque el servidor de aplicación estaba dentro del mismo servidor. Se habían quedado compactados dentro del servidor de base de datos, entonces, y otros dos servidores auxiliares. Entonces, de tres servidores en los cuales se tenía, se fue a cuatro. Se decidió separar el servidor de base de datos, el servidor de aplicación, y entonces, con base en ello, se hicieron las condiciones necesarias, porque necesitábamos el apoyo también del proveedor, este, del sistema para, para ciertos, eh, volver a poner en, en sintonía el, el sistema una vez que lo migráramos. Y, bueno, nosotros, igual, empezamos con el plan de trabajo, en cuestión de tiempo, en cuestión de esfuerzos, después de ahí se toma la fe, la, la, de si se expone el, el, pues, a nuestro comité de TI donde decimos, ok, estas son las, las fechas, esto es lo que nos llevamos en ventana,

costos, todo. Una vez que tenemos esta planeación, que, en sí, el mismo proceso es general para todos los proyectos que hacemos, se expone, nos, nos liberan la ventana de servicio, se avisa a toda nuestra comunidad de usuarios de que va a haber una ventana de servicio. Y, entonces, es cuando, cuando tomamos la, la, la acción, ¿no? Empezamos a ejecutar el plan conforme lo establecimos.

- **Eduardo Uriel (Entrevistador):** Ok. Eh, ¿el servidor en el que se migró el sistema es propiedad de la empresa o es proporcionado por algún proveedor externo?
- **Carlos Bermeo (Entrevistado):** No, es propiedad de la empresa, es propiedad de Aliat, este, está en nuestras instalaciones, en nuestro propio data center que tenemos aquí en Ciudad de México, está alojado el servidor, este, aunque, como ya mencioné, es un servidor físico y está los, estos servidores a los que se migraron son servidores virtuales, trabajamos bajo una virtualización de servidores físicos.
- **Eduardo Uriel (Entrevistador):** Ok. Eh, ahora que me dice que el servidor es propio, eh, ¿cuál es el modelo y las especificaciones técnicas de dicho servidor?
- **Carlos Bermeo (Entrevistado):** El servidor es un servidor, este, HP. Déjame ver si tengo aquí el modelo. Este, de, de ese servidor, eh, el servidor es un HP, tiene, eh, dos procesadores, eh, Xeon, Xeon Gold, este, de, igual, déjame revisar por acá, debo tener las especificaciones bien, pero bueno, tiene, eh, tiene dos procesadores, eh, Xeon Gold, tiene, este, 256 GB en RAM, Disco tiene un total de, me parece que son 7.8 terabytes de almacenamiento, esto en un arreglo de RAID 5. Entonces, pues de cierta manera tiene ahí todos los recursos disponibles, que, si bien están compartidos con algunos otros sistemas, en este momento el servidor yo creo que anda en carga en una capacidad de un 30%, de su capacidad, 30-40% de su capacidad, para lo que realmente estamos explotándolo. Todo está virtualizado a través de Hyper-V, Microsoft Hyper-V, entonces ahí es donde levantamos estos servidores virtuales.
- **Eduardo Uriel (Entrevistador):** Ok, en dado caso de que el servidor principal presente algún problema, ¿cuentan con algún plan de contingencia?
- **Carlos Bermeo (Entrevistado):** Sí, nuestro plan de contingencia es a través de respaldos, es decir, toda información, todos los servidores que viven dentro de ese equipo, o de cualquier equipo que tenemos, son respaldados a través de una herramienta que se llama VIM. Esta hace respaldos diarios, hacemos respaldos diarios por las noches, de la totalidad de servidores, tanto de todo, y hacemos respaldo de todo, lo que contenga datos, bases de datos, aplicaciones, el mismo servidor y sus configuraciones, o sea, todo se respalda diariamente, y se almacena por ahí de un histórico, un histórico, dependiendo cada servidor, se almacena un histórico de respaldos. Entonces, cuando hay algún contratiempo con el sistema, con algo que haya fallado, algún desastre, lo que sea, tenemos, pues no es el único servidor que tenemos, tenemos diversidad de servidores, en los cuales nos podemos guiar, para poder levantar en todo momento, con características similares, en el cual podemos, en caso de algún desastre, poder, con ese respaldo que hicimos, levantar una máquina de cero, y cargarle todos los datos que tenía. Esto, si nos llevará aproximadamente, dependiendo el tamaño del servidor, por ejemplo, para el caso de estos, nos llevará

unas dos, tres horas, para levantar el sistema de nuevo, y poder tenerlo de nuevo, o en línea.

- **Eduardo Uriel (Entrevistador):** Ok. ¿Y cuentan con algún servidor auxiliar?
- **Carlos Bermeo (Entrevistado):** Servidor auxiliar, o sea, ¿auxiliar te refieres a que lo tengamos como indisponible, por el caso de que este falle?
- **Eduardo Uriel (Entrevistador):** Sí, o sea, tener un segundo servidor de respaldo, en caso de que...
- **Carlos Bermeo (Entrevistado):** Tenemos un par de servidores, en el sitio, en el data center, que aún no están sin uso, están completamente ahí detenidos, no, bueno, detenidos, en cierto sentido, porque si algo nos llega a fallar, tenemos esta parte, tenemos también pólizas extendidas, todo esto, que nos ayuda a tener una disponibilidad del servicio con un SLA alto, ¿no? Entonces, tenemos este tipo de pólizas contratadas, y a la vez tenemos, sí, un par de equipos ahí, de referencia, y si no, también tenemos, manejamos recursos en la nube, donde podemos, de pronto, dar de alta servicios que nos ayuden a mitigar, de inmediato, la... la acción, o el desastre que tengamos, ¿no? La contingencia.
- **Eduardo Uriel (Entrevistador):** Ok. Y... Bueno, ya me dijo que tiene un Back-up de la información, entonces... ¿Se realizan revisiones posteriores para mejorar los protocolos de respuesta y planes de contingencia?
- **Carlos Bermeo (Entrevistado):** A ver, ¿me repites la pregunta?
- **Eduardo Uriel (Entrevistador):** Sí, o sea, ¿se realizan revisiones posteriores para mejorar los protocolos de respuesta y planes de contingencia, en dado caso de que se llegue a dar algún incidente?
- **Carlos Bermeo (Entrevistado):** Sí, digamos que cuando ha pasado, lo que sí es que revisamos qué fue lo que falló, ¿no? Hacemos un post-mortem, lo que llevamos acá. Es decir, revisamos, a ver, ¿falló infraestructura? ¿Falló la red? ¿Falló el trono del disco? ¿Qué fue lo que falló, ¿no? ¿Algún problema de seguridad? Lo que sea. Y entonces, con base en eso, pues, si es algo que todavía existe el riesgo latente o presente para que vuelva a suceder, ¿no? Entonces, aplicamos ciertos parches, ciertas mejoras, condiciones al servidor, lo que sea, para que esto no vuelva a ocurrir. Y si no, pues, simplemente, a lo mejor, si fue alguna falla de disco o algo que ya traía como alarmado y que, en ese momento, pues, tronó, como cualquier aparato electrónico, pues, de cierta manera, se mejora en el nuevo recurso donde se haya colocado, ¿no? Sí. Pero, bueno, sí hacemos un cierto análisis y mejoramos las condiciones de lo que haya ocurrido, en todo caso, ¿no? O nuestro protocolo de mejorar el protocolo, ¿no? Como dices, en todo caso, hasta ahorita, creo que eso ha sido lo más funcional para este tipo de sistemas que se pueden volver a levantar de manera eficiente. Y, bueno, manejamos algunos otros procesos que todavía son más robustos, pero para otro tipo de servicios que aún tienen una prioridad más arriba, ¿no? Para sistemas como son sistemas de pagos, sistemas de nóminas, etcétera, donde, pues, son muy transaccionales, a lo mejor, y de esta manera, pues, garantizamos con procesos más robustos en ellos todavía la continuidad. Pero para

este tipo de sistemas, los que hemos elegido este tipo de recuperación nos han resultado bastante eficientes.

- **Eduardo Uriel (Entrevistador):** Ok, bueno, eso sería todo. Muchas gracias, le agradezco por el tiempo.

3.2.3. Actividad. Analizar las respuestas recopiladas en las encuestas para identificar los riesgos que los participantes perciben en relación con los servicios de correo electrónico y Remedy.

Una vez realizadas las entrevistas se llevan a cabo dos resúmenes de la información recopilada, un resumen de la información referente a los servicios de correo electrónico y otro referente al ITSM Remedy, con el fin de clasificar sus inseguridades, esta recopilación tomara en cuenta información referente a las vulnerabilidades y defectos que puedan resaltarse en las respuestas obtenidas, también se tomaran en cuenta observaciones encontradas de acuerdo al trabajo desarrollado en el tiempo que se permitió operar con el sistema.

3.2.3.1. Resultados.

Servicios de correo

Los servicios de correo electrónico en Red Univercom son proporcionados por Microsoft, a su vez la gestión de estos servicios la tiene Mesa de Servicios y Centro de Servicios Compartidos Aliat, los cuales se usan para crear cuentas de O 365 tanto a su personal administrativo, docentes y estudiantes, cada usuario cuenta con una licencia dependiendo del rol en el que se encuentre, adicionalmente, dentro del rol de administrativos se subdividen las licencias y permisos dependiendo del puesto en el que se encuentre el trabajador. Para dar de alta en los servicios de O 365, mediante la plataforma Remedy se hace una solicitud vía ticket de alta de usuario, en ese ticket se especifica el rol que ejercerá dicho usuario, para su comprobación, mediante HCM y Campus Solution se cercioran del estado del usuario al cual se dará de alta, si no cumple con los criterios no se da de alta al usuario. Lo anterior mencionado se debe alinear a las políticas internas de la empresa.

En cuestiones bajas de usuarios, el proceso a seguir es que mediante una solicitud vía ticket o correo, se realice la inhabilitación del inicio de sesión del correo solicitado, sin embargo por cuestiones de reglamento no se pueden eliminar las cuentas de correo de administrativos y docentes por el valor y el tipo de información que manejan, únicamente se deshabilita y se

bloquea el inicio de sesión de dicha cuenta, respecto a cuentas de estudiantes, debido a saturación en los servicios de correo respecto a cantidad de cuentas, se realiza una selección y eliminación de cuentas de aquellos estudiantes que se encuentren inactivos en Campus Solution por más de un año.

Los procesos antes mencionados no se encuentran documentados, sino que se realiza una capacitación a los empleados para realizar las funciones que desempeñara en su puesto, y para dudas o procesos que se desconocen, el personal de Mesa de Servicio, dependiendo del área en el que se enfoca el trabajador, puede resolver dicha duda o bien se le puede delegar la tarea.

Por último, la gran mayoría de las operaciones del área de Mesa de Servicio dependen de que los servicios de Microsoft se encuentren operativos, que se cuente con una buena recepción de internet y que haya luz en el edificio. Por lo que, si alguno de estos tres elementos llegara a fallar, se atrasarían los flujos de trabajo o en el peor de los casos se detendrían casi en un cien por ciento las operaciones.

Servicios Remedy

Remedy es un ITSM el cual se usa para gestionar los tickets, dicho sistema es gestionado por el coordinador del centro de servicios, él es el encargado de llevar las altas, bajas y asegurarse del funcionamiento del sistema.

En la plataforma manejan dos tipos de usuario solicitante y el de gestor o usuario asignado, el primer tipo de usuario se asigna a estudiantes y algunos administrativos, la vista de alumnos contiene solicitudes de cuestiones académicas para los alumnos, la vista de administrativos contiene solicitudes académicas, financieras y administrativas dependiendo del puesto del trabajador. El gestor o usuario asignado es un usuario con ciertos permisos administrativos y las funciones que se le asignan dependen del puesto y las tareas que desempeña el trabajador.

En cuestiones de seguridad e interacción con los usuarios solicitantes, se busca interactuar únicamente con los solicitantes y en caso de ser vulnerado se realiza un rastreo, además se realizan en ocasiones parches de seguridad para mantener la plataforma actualizada. Sin embargo, la plataforma presento recientemente problemas en el tráfico de las solicitudes viéndose en ciertas ocasiones superada la capacidad y tratada mediante un reinicio al sistema, este reinicio detiene las operaciones de Mesa de Servicio en su totalidad, así como las

funciones de sus aplicaciones causando que se retrasen el resto de las operaciones empresariales.

3.2.4. Actividad. Identificar posibles vulnerabilidades y amenazas en los servicios de correo electrónico y Remedy a través del análisis FODA.

Después de recopilar, resumir los conocimientos obtenidos de las operaciones de los servicios de correo electrónico junto con Remedy y haber separado la información de las posibles vulnerabilidades que estos poseen, se llevan a cabo los correspondientes análisis FODA, estos análisis FODA se aplicaran al área de Mesa de Servicio tomando en cuenta la información recopilada y lo observado en dicha área, el segundo FODA será para los servicios de correo electrónico, de igual manera se toman en cuenta lo recopilado y lo observado en el manejo de dicho servicio y de cómo es que se debería utilizar según el reglamento interno de Aliat, y por último, un análisis FODA al ITSM Remedy que abarca lo recopilado junto con trabajos realizados en la propia herramienta.

3.2.4.1. Resultados.

Análisis FODA Mesa de Servicios Compartidos.

El análisis que se realiza al área de Mesa de Servicio busca denotar los atributos del área y visualizar las opciones que hacen destacar al área y las que se pueden mejorar, sin embargo, el área tiene poco más de 3 años implementada en la empresa y el manual operacional o reglamento de Mesa de Servicio no se encuentra plenamente terminado. Lo que se buscaba conseguir con esta área, es centralizar los incidentes y requerimientos operativos dentro de Aliat, y dado que el área es relativamente reciente muchas de sus operaciones se pueden ver sujetas a cambios o replanteamientos de los mismos, dependiendo de las necesidades que surgen ya sea por implementación nuevas tecnologías, actualizaciones de servicios o reordenamiento de procesos; anteriormente muchos de estos procesos los realizaban más de un área y el resto no lo sabía y se duplicaba dicho proceso, lo cual causaba un retraso en las operaciones y duplicidad de información. Al tratarse de una institución educativa existen periodos y temporadas en los que la carga de trabajo puede variar, por ende, en Mesa de Servicio sucede lo mismo y en ocasiones se pueden ver superadas las cargas para el personal del área.

Tabla 3. FODA Mesa de Servicio.

(Fuente: Elaboración propia).

FORTALEZAS	OPORTUNIDADES
1) Centralización de las solicitudes en una sola área. 2) Buena comunicación entre los empleados sobre cualquier incidente.	1) Estructurar manuales de procesos y procedimientos para atención de solicitudes de peticiones en Remedy asociadas al área de TI. 2) Evaluaciones a las capacidades y conocimientos en el personal para la operación relacionada con la TI. 3) Capacitación inmediata al personal sobre las nuevas funcionalidades que pueda tener el sistema. 4) Notificaciones por actualización de estatus de tickets en espera.
DEBILIDADES	AMENAZAS
1) Procesos explicados de manera oral. 2) Cuestionamientos repetitivos provocado por malas prácticas de los usuarios. 3) Área con muy poco personal. 4) Dependencia completa del área a usar la herramienta Remedy. 5) No se realizan notificaciones constantes de los estados en los que se encuentran los tickets en espera.	1) Interrupciones por fallas en servicios de luz o internet. 2) Dependencia de otras áreas. 3) Poca banda ancha designada a los trabajadores por parte de la empresa.

Conclusión del FODA de Mesa de Servicio.

El área de mesa de servicio por ser un área reciente dentro de Aliat y que centraliza múltiples solicitudes y requerimientos, tiene muchas funcionalidades que pueden mejorar y a su vez muchos aspectos a fortalecer para aumentar la eficiencia de la misma, esto incluye una mejora en el manejo de las solicitudes junto con notificaciones de estatus para mantener informado a los usuarios de las condiciones en las que se encuentran sus solicitudes, lo anterior sumado a un manual y evaluación que se les puede aplicar al personal respecto al manejo de TI, puede mejorar la capacidad y la eficiencia de Mesa, también se muestra que Mesa de Servicio depende en su totalidad de la disponibilidad del sistema Remedy lo cual significa que si en algún momento llegara a fallar causaría la suspensión total de las actividades en el área junto con un retraso en los procesos, también debiera tomarse en cuenta que los equipos de los trabajadores se encuentren asegurados y que no se les dé un mal uso a estos.

Análisis FODA servicios de correo electrónico.

El siguiente análisis FODA busca denotar las afectaciones que puedan tener los servicios de correo electrónico proporcionados por Microsoft actuales, así como el manejo que se le da en el área de Mesa de servicio y como es que el personal brinda estos servicios a alumnos, docentes y administrativos. Debido al tiempo que se tiene con dichos servicios y a la expansión que tiene la empresa educativa a lo largo del país, puede que estos servicios se vean cada vez excedidos e incluso limitados a las necesidades. Por lo que el análisis FODA, conforme a lo observado y trabajado y solicitado busca comprender y denotar como es que los servicios actuales afectan en el desempeño del servicio que proporciona Aliat con el correo electrónico. Este análisis se realizó mayormente con la información proporcionada por el encargado de gestionar estos servicios el Gerente de servicios Pedro Joaquín Paredes Talavera y las personas que trabajan mayoritariamente en este el Coordinador de CSC Luis Alberto Maldonado Espinoza y el Agente de Mesa de Servicio Gerardo Sandoval Cárdenas.

Tabla 4. FODA Servicios de correo.

(Fuente: Elaboración propia).

FORTALEZAS	OPORTUNIDADES
1) Tipificación de usuarios según las políticas de la empresa.	1) Negociar la mejora en los servicios que ya se tienen. 2) Procedimientos para dar seguimiento al estado y depuración de cuentas.
DEBILIDADES	AMENAZAS
1) Falta de un seguimiento en la depuración de cuentas. 2) Mal uso de los sistemas por parte de los usuarios.	1) Ataques de personas externas que puedan acceder a información confidencial. 2) Servicios de Microsoft limitados por la ausencia de correo. 3) Interrupciones por fallas en servicios de luz o internet.

Conclusión del FODA de los servicios de Correo electrónico.

Dado que los servicios de correo electrónico están proporcionados por un proveedor externo existe la probabilidad de que cuando estos fallen no haya mucho que la empresa pueda hacer al respecto además de que debido al tiempo, y expansión que ha tenido la empresa a nivel nacional y dado que es una institución educativa que atiende a una gran cantidad de estudiantes a nivel nacional los servicios actuales se han visto superados lo cual indica que se tiene que reestructurar el convenio que tienen con el proveedor de servicios de correo electrónico para ampliar dichos servicios y/o realizar depuraciones de usuarios y cuentas que puedan encontrarse en desuso o que simplemente ya no sean de utilidad para la empresa,

descartando la eliminación cuentas que por reglamento interno no puedan ser eliminadas ya sea por información que contengan o el uso posterior que se le pueda dar.

Análisis FODA servicios de Remedy.

Remedy es un sistema que busca gestionar las solicitudes de incidencias y requerimientos pedidos por alumnos docentes y administrativos, actualmente Remedy se encuentra disponible en computadoras y como una aplicación móvil, para administrativos pueden acceder al sistema través del navegador y/o navegador del móvil pudiendo realizar solicitudes de servicios administrativos y de negocio, servicios financieros, servicios escolares y servicios de TI. Para alumnos pueden acceder mediante la aplicación de Mi Red Aliat y/o a través del portal de estudiantes, pudiendo solicitar servicios financieros, servicios escolares y servicios de TI. Sin embargo, únicamente personal y alumnos que se encuentren activos dentro de la empresa pueden acceder a este servicio. Se tiene pensado que este sistema se pueda expandir e implementar a más áreas o departamentos dentro de la empresa como pueden ser la página web oficial de Aliat. Adicionalmente este sistema puede ampliarse dependiendo de las necesidades de servicio que surjan lo cual trae consigo, que mientras más servicios maneje mayor serán las solicitudes que se hagan y mayor será el tráfico de Red que este sistema maneje el FODA busca denotar los riesgos de que estos servicios se vean superados y tener alternativas o proponer mejoras para el propio sistema.

Tabla 5. FODA Servicios de Remedy.

(Fuente: Elaboración propia).

FORTALEZAS	OPORTUNIDADES
1) Interacción con administrativos, docentes y estudiantes.	1) Implementación de nuevas funciones en más áreas de la empresa para. 2) Se pueden establecer nuevos servicios a las necesidades que se presenten. 3) Capacitación para el uso de Remedy

Tabla 5. FODA Servicios de Remedy (Continuación).

DEBILIDADES	AMENAZAS
1) Tráfico de solicitudes al servidor de Remedy superado. 2) Cualquier usuario tendría acceso información que no corresponden a su puesto. 3) Mal uso de los sistemas por parte de los usuarios. 4) Falta de especificación en los errores producidos en los sistemas.	1) Ataques de personas externas que puedan acceder a información confidencial. 2) Incapacidad de BMC Remedy para proporcionar sus servicios provenientes del proveedor. 3) Errónea tipificación de servicio por parte del usuario solicitante. 4) Posible limitación que pueda tener BMC Remedy en el diseño de nuevas funcionalidades. 5) Duplicación de solicitudes y saturación del servicio del soporte técnico por parte de los usuarios solicitantes. 6) Interrupciones por fallas en servicios de luz o internet.

Conclusión del FODA del servicio Remedy.

Remedy es un servicio proporcionado por un proveedor de software, dicho software está diseñado para implementar una mesa de ayuda en las empresas y puede ser adaptado a las necesidades de esta, sin embargo en Aliat, este servicio puede verse superado por la cantidad de solicitudes, la cantidad y los tipos de usuarios que maneja al abarcar administrativos, docentes y alumnos y los servicios que Aliat ofrece a través de Remedy, lo anterior junto con el mal uso que los usuarios pueden darle a este sistema ya sea por la falta de capacitación o la inexperiencia que las personas tengan al usar este tipo de soluciones tecnológicas, puede desencadenar problemas como un tráfico de solicitudes demasiado alto para el propio sistema o que el usuario solicitante realice más de un proceso similar en repetidas ocasiones, acumulando solicitudes innecesarias y un retraso en el flujo de trabajo.

3.3. Objetivo. Emplear un análisis de riesgo según las amenazas y vulnerabilidades encontradas.

La metodología de análisis de riesgos permitirá cuantificar las vulnerabilidades y riesgos existentes, así como presentar de manera visual cuáles deben ser atendidos con mayor prioridad.

3.3.1. Actividad. Examinar los riesgos que podrían impedir el normal desenvolvimiento de las operaciones en la empresa.

Al haber realizado los análisis FODA del área de Mesa de Servicio, de los servicios de correo electrónico y el sistema de servicio Remedy, se seleccionan las vulnerabilidades y amenazas que puedan desencadenar algún riesgo, el objetivo es plantear que vulnerabilidades y amenazas se pueden contraatacar para prevenir esos posibles riesgos, de esta forma permitirá posteriormente proponer y plantear soluciones.

3.3.1.1. Resultados.

Tabla 6. Identificación de riesgo 1.

(Fuente: Elaboración propia).

Vulnerabilidad	Amenaza	Riesgo
V1. Área con muy poco personal. V2. No se realizan notificaciones constantes de los estados en los que se encuentran los tickets en espera.	A1. Dependencia de otras áreas.	R1. Retraso en los procesos generales y mala imagen con respecto a la operatividad de la empresa.

Tabla 7. Identificación de riesgo 2.

(Fuente: Elaboración propia).

Vulnerabilidad	Amenaza	Riesgo
V1 Dependencia completa del área a usar el sistema Remedy. V2. Tráfico de solicitudes al servidor de Remedy superado.	A1. Incapacidad de BMC Remedy para proporcionar sus servicios provenientes del proveedor. A2. Poca banda ancha designada a los trabajadores por parte de la empresa. A3. Posible limitación que pueda tener BMC Remedy en el diseño de nuevas funcionalidades. A4. Interrupciones por fallas en servicios de luz o internet.	R1. La empresa se queda sin servicios para atender solicitudes administrativas y de negocio, servicios financieros, servicios escolares y servicios de TI afectando la operatividad total.

Tabla 8. Identificación de riesgo 3.

(Fuente: Elaboración propia).

Vulnerabilidad	Amenaza	Riesgo
V1. Procesos explicados de manera oral. V2. Cuestionamientos repetitivos provocados por malas prácticas de los usuarios. V3. Falta de especificación en los errores producidos en los sistemas.	A1. Duplicación de solicitudes y saturación del servicio del soporte técnico por parte de los usuarios solicitantes. A2. Errónea tipificación de servicio por parte del usuario solicitante.	R1. La empresa se queda con servicios para atender solicitudes administrativas y de negocio, servicios financieros, servicios escolares y servicios de TI operando inadecuadamente.

Tabla 9. Identificación de riesgo 4.

(Fuente: Elaboración propia).

Vulnerabilidad	Amenaza	Riesgo
V1. Falta de un seguimiento en la depuración de cuentas.	A1. Servicios de Microsoft limitados por la ausencia de correo.	R1. Saturación del uso de la cantidad de cuentas disponibles para usuarios O365.

Tabla 10. Identificación de riesgo 5

(Fuente: Elaboración propia).

Vulnerabilidad	Amenaza	Riesgo
V1. Cualquier usuario tendría acceso información que no corresponden a su puesto. V2. Mal uso de los sistemas por parte de los usuarios.	A1. Ataques de personas externas que puedan acceder a información confidencial.	R1. Pérdida y/o robo de información.

3.3.2. Actividad. Establecer el nivel de la exposición al riesgo.

Una vez que se identificaron los riesgos es necesario evaluar la frecuencia y el nivel de afectación que pueden ocasionar las vulnerabilidades en la empresa; la evaluación se realiza conforme a lo considere el personal de Mesa de Servicio (6 personas), las cuales tienen una idea más clara al interactuar con los servicios de manera frecuente.

3.3.2.1. Resultados.

Métrica de evaluación.

Esta métrica será la utilizada para colocar un valor numérico a la probabilidad e impacto y dependiendo del escalado que obtengan las vulnerabilidades.

Tabla 11. Métrica de probabilidad e impacto.

(Fuente: Elaboración propia).

Valor	Probabilidad	Impacto
1	Raro	Insignificante
2	Poco probable	Menor
3	Moderado	Significativo
4	Casi seguro	Mayor
5	Seguro	Severo

Tablas de evaluación de riesgos.

Conforme a las vulnerabilidades visualizadas en los análisis FODA y a los riesgos que estas vulnerabilidades implican, es necesario ordenar las vulnerabilidades respecto al nivel de prioridad con el que se tengan que atender. A continuación, se presentan las tablas con las evaluaciones cuantitativas hechas por el personal de esta área a fin de hacer una priorización con las calificaciones de las más altas a las menores.

Tabla 12. Tabla de vulnerabilidad 1.

(Prado, 2009).

	Vulnerabilidad 1: Área con muy poco personal.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Probabilidad	Raro	Poco Probable	Moderado	Casi Seguro	seguro
¿Con que frecuencia considera que ocurre este riesgo?			2		1
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			2	1	

Tabla 13. Tabla de vulnerabilidad 2.

(Prado, 2009).

	Vulnerabilidad 3: No se realizan notificaciones constantes de los estados en los que se encuentran los tickets en espera.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Probabilidad	Raro	Poco Probable	Moderado	Casi Seguro	seguro
¿Con que frecuencia considera que ocurre este riesgo?	1		2		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			1		2

Tabla 14. Tabla de vulnerabilidad 3.

(Prado, 2009).

	Vulnerabilidad 4: Tráfico de solicitudes al servidor de Remedy superado.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Probabilidad	Raro	Poco Probable	Moderado	Casi Seguro	seguro
¿Con que frecuencia considera que ocurre este riesgo?	1	1	1		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			1		2

Tabla 15. Tabla de vulnerabilidad 4.

(Prado, 2009).

	Vulnerabilidad 5: Falta de especificación en los errores producidos en los sistemas.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Probabilidad	Raro	Poco Probable	Moderado	Casi Seguro	seguro
¿Con que frecuencia considera que ocurre este riesgo?	1				2
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?				1	2

Tabla 16. Tabla de vulnerabilidad 5.

(Prado, 2009).

	Vulnerabilidad 6: Dependencia completa del área a usar el sistema Remedy.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Probabilidad	Raro	Poco Probable	Moderado	Casi Seguro	seguro
¿Con que frecuencia considera que ocurre este riesgo?	1	1			1
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					3

Tabla 17. Tabla de vulnerabilidad 6.

(Prado, 2009).

Vulnerabilidad 7: Procesos explicados de manera oral.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Probabilidad	Raro	Poco Probable	Moderado	Casi Seguro	seguro
¿Con que frecuencia considera que ocurre este riesgo?				2	1
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			3		

Tabla 18. Tabla de vulnerabilidad 7.

(Prado, 2009).

Vulnerabilidad 8: Cuestionamientos repetitivos provocado por malas prácticas de los usuarios.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Probabilidad	Raro	Poco Probable	Moderado	Casi Seguro	seguro
¿Con que frecuencia considera que ocurre este riesgo?		3			
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			3		

Tabla 19. Tabla de vulnerabilidad 8.

(Prado, 2009).

Vulnerabilidad 10: Falta de un seguimiento en la depuración de cuentas.					
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Probabilidad	Raro	Poco Probable	Moderado	Casi Seguro	seguro
¿Con que frecuencia considera que ocurre este riesgo?				1	2
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					3

Tabla 20. Tabla de vulnerabilidad 9.

(Prado, 2009).

	Vulnerabilidad 11: Cualquier usuario tendría acceso información que no corresponden a su puesto.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Probabilidad	Raro	Poco Probable	Moderado	Casi Seguro	seguro
¿Con que frecuencia considera que ocurre este riesgo?		2	1		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?					3

Tabla 21. Tabla de vulnerabilidad 10.

(Prado, 2009).

	Vulnerabilidad 12: Mal uso de los sistemas por parte de los usuarios.				
Nivel de impacto	Insignificante	Menor	Significativo	Mayor	Severo
Probabilidad	Raro	Poco Probable	Moderado	Casi Seguro	seguro
¿Con que frecuencia considera que ocurre este riesgo?			3		
¿Qué nivel de impacto tendría este riesgo si sucede en la empresa?			2		1

3.3.3. Actividad. Compilar las vulnerabilidades y que tan severamente podrían afectarse las operaciones en la empresa.

Una vez evaluado y escalado las vulnerabilidades, es necesario ordenar estas vulnerabilidades según el nivel de peligro que estos generan en Mesa de servicio y a la empresa, con el fin de visualizar cuales son las vulnerabilidades que se tiene que atender lo antes posible para mitigar las pérdidas y posteriormente realizar las propuestas y soluciones a las vulnerabilidades de mayor impacto.

3.3.3.1. Resultados.

Una vez calificadas las vulnerabilidades, se ordenan de mayor a menor según la métrica que a continuación se presenta; así mismo, en seguida se calcula la magnitud del riesgo, multiplicando la probabilidad por el nivel de impacto, con el fin de obtener el nivel de prioridad. De igual manera, se presenta una tabla ya respetan este nivel de prioridad con los aproximados de pérdida económica que se pueden tener si alguno de esto fallará, así como su afectación en servicios. Esta información son aproximaciones transmitidas por el personal involucrado en esta área.

Magnitud del riesgo

Mediante la siguiente tabla se determinará el nivel de riesgo de las vulnerabilidades según lo que el personal encuestado considera que es más probable y que cause una mayor afectación en mesa de servicio y por ende a la empresa.

Tabla 22. Tabla de valoración al riesgo.

(Prado, 2009).

Nivel de impacto Probabilidad	Descripción de la vulnerabilidad o amenaza				
	1. Insignificante	2. Menor	3. Significativo	4. Mayor	5. Severo
1. Raro	1 Bajo	2 Bajo	3 Bajo	4 Bajo	5 Bajo
2. Poco Probable	2 Bajo	4 Bajo	6 Bajo	8 Medio	10 Medio
3. Moderado	3 Bajo	6 Bajo	9 Medio	12 Medio	15 Alto
4. Casi Seguro	4 Bajo	8 Medio	12 Medio	16 Alto	20 Alto
5. Seguro	5 Bajo	10 Medio	15 Alto	20 Alto	25 Alto

A continuación, se tabularán las vulnerabilidades y el nivel de atención que se les deben dar a dichas vulnerabilidades.

Tabla 23. Cuadro de escalas de probabilidad del riesgo.

(Fuente: Elaboración propia).

Vulnerabilidades	Probabilidad	Impacto	Nivel de prioridad
Falta de un seguimiento en la depuración de cuentas.	5 Seguro	5 Severo	25 Alto
Falta de especificación en los errores producidos en los sistemas.	5 Seguro	5 Severo	25 Alto
Dependencia completa del área a usar el sistema Remedy.	5 Seguro	5 Severo	25 Alto
Tráfico de solicitudes al servidor de Remedy superado.	3 Moderado	5 Severo	15 Alto
No se realizan notificaciones constantes de los estados en los que se encuentran los tickets en espera.	3 Moderado	5 Severo	15 Alto
Procesos explicados de manera oral.	4 Casi Seguro	3 Significativo	12 Medio
Cualquier usuario tendría acceso información que no corresponden a su puesto.	2 Poco Probable	5 Severo	10 Medio
Mal uso de los sistemas por parte de los usuarios.	3 Moderado	3 Significativo	9 Medio
Área con muy poco personal.	3 Moderado	3 Significativo	9 Medio
Cuestionamientos repetitivos provocados por malas prácticas de los usuarios.	2 Poco Probable	3 Significativo	6 Bajo

Tabla 24. Cuadro de pérdidas monetarias.

(Fuente: Elaboración propia).

Vulnerabilidad	Perdida monetaria aproximada del impacto de la vulnerabilidad (MXN)	Afectaciones calculadas en los servicios.
Falta de un seguimiento en la depuración de cuentas.	---	Saturación del sistema.
Falta de especificación en los errores producidos en los sistemas.	---	Perdida de 3 horas-hombre netas en un lapso de 48 a 60 horas.
Dependencia completa del área a usar el sistema Remedy.	\$500,000 en un día campus	---
Tráfico de solicitudes al servidor de Remedy superado.	\$250,000 en un día campus	---

Tabla 24. Cuadro de pérdidas monetarias (Continuación).

No se realizan notificaciones constantes de los estados en los que se encuentran los tickets en espera.	---	Afectaciones de moderadas a ceberas en el proceso del usuario solicitante
Procesos explicados de manera oral.	\$100,000 en un día campus.	Un proceso mal explicado desencadenaría a una pérdida en el área financiera.
Cualquier usuario tendría acceso información que no corresponden a su puesto.	---	Riesgo de vulnerar información personal que la institución tiene a su resguardo.
Mal uso de los sistemas por parte de los usuarios.	---	Afectaciones a la productividad de los Agentes de Mesa.
Área con muy poco personal.	---	Afectaciones al rendimiento y resultado de los agentes de Mesa de Servicio.
Cuestionamientos repetitivos provocados por malas prácticas de los usuarios.	---	Afectaciones al rendimiento de los Agentes de Mesa y la percepción del usuario solicitante.

3.4. Seleccionar los escenarios probables y de mayor impacto, con el objetivo de abordarlos de manera inmediata.

Una vez ordenados los escenarios por prioridad de atención y las afectaciones y pérdidas que pueden provocar tanto monetariamente como del valor del servicio, se hace una relación entre afectaciones encontradas, los riesgos que se pueden materializar y las recomendaciones de las guías, normas y estándares para la seguridad y el mejoramiento del desempeño de trabajo, como un análisis que contiene toda la perspectiva estudiada. Cabe mencionar que una o varias amenazas, así como vulnerabilidades pueden estar asociadas a un sólo o varios riesgos.

3.4.1. Resultados.

Tabla 25. Recomendaciones para la mitigación de riesgos según ITIL 4 y otros estándares.

(Fuente: Elaboración propia).

Vulnerabilidad	Amenaza	Riesgo	Recomendación
V1. Falta de un seguimiento en la depuración de cuentas.	A1. Servicios de Microsoft limitados por la ausencia de correo.	R1. Saturación del uso de la cantidad de cuentas disponibles para usuarios O365.	Las recomendaciones que brinda ITIL respecto a esta situación sería la cadena de valor del servicio, la cual junto a COBIT 5 en el apartado de alineación, planificación y organización de las actividades de gobierno y gestión de TI establecen que las organizaciones deben contar con la gestión de sus proveedores y los acuerdos de los servicios (APO09 Y APO10).
V1. Dependencia completa del área a usar el sistema Remedy. V2. Tráfico de solicitudes al servidor de Remedy superado.	A1. Incapacidad de BMC Remedy para proporcionar sus servicios provenientes del proveedor. A2. Poca banda ancha designada a los trabajadores por parte de la empresa. A3. Posible limitación que pueda tener BMC Remedy en el diseño de nuevas funcionalidades. A4. Interrupciones por fallas en servicios de luz o internet.	R1. La empresa se queda sin servicios para atender solicitudes administrativas y de negocio, servicios financieros, servicios escolares y servicios de TI afectando la operatividad total.	ITIL maneja que tanto el personal como los sistemas y las demás áreas trabajen holísticamente. COBIT recomienda una gestión de la arquitectura empresarial, junto con una gestión de la seguridad (APO03, APO13), y en base al ISO 17799 se debe de contar con un plan de continuidad del negocio a fin de evitar eventos que interrumpen la disponibilidad de los servicios.

Tabla 25. Recomendaciones para la mitigación de riesgos según ITIL 4 y otros estándares (Continuación).

V1. No se realizan notificaciones constantes de los estados en los que se encuentran los tickets en espera. V2. Área con muy poco personal.	A1. Dependencia de otras áreas.	R1. Retraso en los procesos generales y mala imagen con respecto a la operatividad de la empresa.	ITIL maneja el servicio como un todo por lo que propone que se tenga un equilibrio entre sus cuatro dimensiones de la gestión del servicio una de ellas consta en las organizaciones y personas en ella propone que el personal debe tener claro el objetivo de la organización, siendo en este caso la atención a los requerimientos, también indica que el personal debe tener claro las líneas de reporte para tener manejo de las responsabilidades de los empleados y de las actividades que llevan a cabo, también insta que se debe contar con un modelo de comunicación para actividades, roles y demás asuntos ya sean internos o con los usuarios solicitantes.
V1. Procesos explicados de manera oral. V2. Cuestionamientos repetitivos provocados por malas prácticas de los usuarios. V3. Falta de especificación en los errores producidos en los sistemas.	A1. Duplicación de solicitudes y saturación del servicio del soporte técnico por parte de los usuarios solicitantes. A2. Errónea tipificación de servicio por parte del usuario solicitante.	R1. La empresa se queda con servicios para atender solicitudes administrativas y de negocio, servicios financieros, servicios escolares y servicios de TI operando inadecuadamente.	ITIL junto al ISO 17799 propone una seguridad de los recursos humanos que se establezcan claramente las actividades y los flujos de trabajo además recomienda una correcta designación de los roles y que el personal se encuentre adecuadamente capacitado. COBIT recomienda asegurar la optimización al riesgo al evaluar, orientar y supervisar.

Tabla 25. Recomendaciones para la mitigación de riesgos según ITIL 4 y otros estándares (Continuación).

V1. Cualquier usuario tendría acceso información que no corresponden a su puesto. V2. Mal uso de los sistemas por parte de los usuarios.	A1. Ataques de personas externas que puedan acceder a información confidencial.	R1. Pérdida y/o robo de información.	Las prácticas de gestión ITIL establece un marco de gestión de incidentes y de problemas, en el establece que la empresa debe contar con prácticas de gestión de problemáticas antes de que se vuelvan incidentes que afecten a la operatividad. COBIT establece propone una mitigación al riesgo junto con una gestión de la seguridad de la información para prevenir las perdidas o el robo. El ISO 17799 establece que se deben realizar evaluaciones de riesgos de seguridad y contar con una política de seguridad de la información, así como la clasificación del tipo de información que se esté manejando para establecer controles de acceso a la información.
--	---	--	--

CAPÍTULO IV: RESULTADOS

4.1. Proponer las estrategias sustentadas en ITIL 4 y en otros estándares de seguridad; y adaptarlas a las necesidades específicas a los servicios de correo electrónico y Remedy que se ofrecen.

4.1.1. Aplicar las cuatro dimensiones de la gestión de servicios para comprender y abordar diversos aspectos en la prestación de servicios de TI.

A fin de ofrecer una propuesta para solucionar las situaciones de riesgo con forme a las solicitudes de la empresa, se ha tomado como referencia mayormente el estándar Information Technology Infrastructure Library (ITIL), que en español significa Biblioteca de Infraestructura de Tecnologías de la Información, como apoyo principal para las soluciones de seguridad.

ITIL establece cuatro principios fundamentales los cuales al trabajar en armonía permite que las empresas ofrezcan de una mejor manera sus productos y servicios, a su vez estos cuatro fundamentos se ven influenciados por factores externos los cuales mejoran o empeoran uno o algunos de los pilares de la gestión de servicios. En Mesa de Servicio de Aliat estos pilares y factores externos pueden llegar a afectar negativamente el desempeño no solo del área de Mesa si no que afectan al desempeño del resto de departamentos y servicios que la componen, por lo que se colocaran como están planteadas las dimensiones y como es que están siendo afectados actualmente en Mesa de Servicio de Aliat.

4.1.1.1. Resultados.

Las cuatro dimensiones de la gestión de servicios de ITIL.

ITIL maneja cuatro pilares fundamentales para gestionar los servicios:

- Organización y personas
- Información y tecnología
- Socios y proveedores
- Flujos de valor y procesos

Los cuales en caso de que alguno de ellos no se ejerza de manera adecuada puede afectar al resto y a los productos y servicios que estos pilares buscan generar el valor del servicio. A su vez estos pilares son influenciados por la complejidad que pueda tener la empresa y factores externos, estos factores también pueden afectar a la generación de valor en los servicios.

Lo anterior se puede ejemplificar en la siguiente imagen:



Figura 31. Las cuatro dimensiones de la gestión de servicios.

(TZALOA, 2023).

Mesa de Servicio y las cuatro dimensiones de la gestión de servicios.

En Mesa de Servicio de Aliat se entiende que el valor se le quiere otorgar a la atención en tiempo y forma a las solicitudes que se realizan, ahora tras el análisis es necesario especificar como Aliat maneja estas dimensiones y que está afectando el equilibrio de estas.

1) Organizaciones y Personas

Se conforma por el personal que conforma al área, los roles y responsabilidades que se le otorgan al personal, la estructura y valores organizacionales que se manejan en la empresa. Mesa de Servicio es un área que está conformada por 7 agentes de mesa asignados a labores de administrativas, financieros, escolares y de TI, dichas labores se ven repartidas entre los agentes de mesa que conforman el área, estos agentes son a su vez gestionados por el coordinador del Centro de Servicios Compartidos, este Coordinador se encarga de orientar y dirigir a los agentes de mesa. El Coordinador CSC se encuentra bajo la orden directa del Gerente de servicios el cual es el encargado del área de mesa de servicios y cadena B encargados de labores en otras plataformas Institucionales. El Gerente de servicios es el encargado de asignar y gestionar los servicios con los que trabaja Mesa y en caso de ausencia por cualquier motivo el Coordinador CSC es el encargado de tomar las decisiones y gestión de estos servicios.

El modo de operar consiste en niveles de atención, estos niveles se van escalando, dependiendo de si el nivel anterior no es capaz de resolver la solicitud, estos pueden escalar de un agente de mesa a otro que trabaje o resuelva problemáticas específicas o al Coordinador

CSC y sucesivamente; al ser un área pequeña y centralizada, permite que todos los trabajadores se encuentren en una misma zona, haciendo que existe mucha comunicación e interacción entre los trabajadores lo cual facilita la atención de problemáticas en el momento y de forma oportuna; En Mesa de Servicio mantiene un ambiente laboral cordial y amistoso entre empleados al igual entre jefes y empleados. Sin embargo, pese a que su estructura organizacional este bien definida muchos de los procesos y roles de trabajo no quedan del todo claros, en ocasiones se brindan capacitaciones explicadas únicamente de manera oral, lo cual provoca tanto usuarios solicitantes de servicios como propios agentes de mesa recurran a realizar frecuente mente cuestionamientos respecto a cómo operar o ejercer ciertos servicios, en ocasiones puede desencadenar a una atención inadecuada a los usuarios solicitantes y que en periodos donde la carga de trabajo supera al poco personal que opera en esta área, aumenta el riesgo a que sucedan este tipo de situaciones.

2) Información y tecnología

Este apartado busca que las empresas tengan un manejo de la información eficiente, así como un buen manejo y cuidado de esta, siempre tomando en cuenta la disponibilidad, confiabilidad y accesibilidad de esta, y junto a un personal con los conocimientos y habilidades de cubrir con las necesidades que el área necesite dependiendo del giro de la empresa al que se vaya a implementar estas funciones. También busca que las empresas cuenten con las tecnologías necesarias para mejorar y agilizar lo que ofrecen, pueden ser servicios, productos, etc.

Mesa de Servicio Aliat trata de centralizar peticiones de tipo administrativas, financieras, servicios escolares y servicios de TI, por lo que tiene acceso a los sistemas de trabajo de Aliat (HCM y Campus Solution) y dependiendo del puesto en el que se encuentre el trabajador de Mesa, es como se limitan los accesos y modificaciones que pueden hacer en dichos sistemas. Manejan información financiera de estudiantes, tratan con información referente a puestos de trabajo, escolaridad y estatus de los trabajadores y alumnos y también son los encargados de brindar accesos a los servicios de correo, aplicaciones y ciertos permisos a administrativos, docentes y estudiantes; para trabajar mesa de servicio cuenta con el sistema Remedy el cual es el que gestiona y distribuye las solicitudes entre los agentes de Mesa. Para trabajar con todos los sistemas anteriores los agentes de Mesa cuentan con un equipo de cómputo proporcionado por la empresa para llevar a cabo sus labores. Ahora bien, al ser mesa un lugar que centraliza las funciones, depende de muchas de las demás áreas de la empresa, lo cual en ocasiones causa una lenta atención a los usuarios solicitantes por la espera de respuesta del área auxiliar, esto junto al hecho de la cantidad de trabajadores que puede haber en un solo campus puede llevar a que en algún periodo de sobrecarga de trabajo para todo el campus como puede ser un nuevo ciclo escolar o un cierre de año, se puede ver superado el tráfico de red del campus causando una lentitud en los servicios de internet y dado que Mesa de

Servicio depende en su totalidad de Remedy, si este sistema se ve interrumpido, toda el área detendría sus operaciones.

3) Socios y proveedores

Muchas de las empresas requieren de proveedores que le puedan brindar productos o servicios que complementen las funcionalidades de la empresa, esto implica que la relación entre la empresa proveedora y cliente deben de contar con una cordial relación, también puede haber asociaciones donde ambas cooperen para cumplir algún objetivo. Para esto también es necesario que entre clientes, proveedores y asociaciones existan contratos, acuerdos e historiales donde se estipulen los términos y condiciones de la forma en la que trabajaran en dicha asociación.

Aliat universidades al ser una empresa dedicada a la educación privada, requiere de servicios y aplicaciones para sus administrativos y estudiantes, ser capaz de tener una gestión eficiente y brindar una gran variedad de ofertas educativas. En Mesa se encarga de gestionar los servicios Microsoft, encargados de proveer el correo para el personal y estudiantes, gestiona las altas y bajas en los sistemas y aplicaciones como brightspace y Mi red Aliat; lo antes mencionado se realiza mediante solicitudes, estas solicitudes las gestiona el sistema Remedy, el cual es un servicio proporcionado por el proveedor BMC Remedy, una empresa que ayuda a otras a implementar una mesa de servicio en base a ITIL. No obstante actualmente, el sistema Remedy al atender una gran cantidad de solicitudes diferentes y de distintos tipos de usuarios ocasiono que el número de interacciones que se tienen con el sistema se vea superado y el servidos en el que se aloja no cumpla con la suficiente banda ancha para la cantidad de solicitudes, ocasionando lentitud en el sistema y en ocasiones que se vea sujeto a reinicios para estabilizar las solicitudes y particularmente los servicios de creación de cuentas de correo de Microsoft, específicamente para cuentas de estudiantes, se ha alcanzado el límite de usuarios que se pueden crear lo cual ha ocasionado que surja la necesidad de depurar las cuentas y eliminar cuentas de estudiantes que llevan bastante tiempo inactivos en sistema, esto surgió a causa de la gran cantidad de estudiantes que se manejan a nivel nacional; esto también pone a prueba los servicios que se tienen de los proveedores.

4) Flujos de valor y procesos

Este apartado busca que las empresas establezcan flujos de trabajo para mejorar la eficiencia del servicio, para hacerlo, se apoyan con el SVS y los servicios y productos que ofrece la empresa; el flujo de valor consiste en que los trabajadores sean capaces de mejorar su desempeño mediante la comprensión de los flujos de trabajo e interacción que tendrán, se

podría decir que busca que los empleados conozcan a la cadena de mando, de esta manera, se tendría un flujo de trabajo capaz de generar valor, descartando cualquier actividad o interacción innecesaria y así poder tener una mayor productividad y además estar abiertos a mejoras de cualquier circunstancia (procesos, tecnologías, etc.). Para esto es necesario que las empresas cuenten con procesos bien definidos, esto incluye instrucciones de trabajo y el personal que se verá involucrado en el proceso.

En Mesa de Servicio Aliat, como su propio nombre indica, brinda atención a los usuarios que pueden ser administrativos, docentes y estudiantes. Todos los usuarios pueden hacer múltiples solicitudes a Mesa de Servicios de tipo administrativas y de negocio, servicios financieros, servicios escolares y servicios de TI, y la forma de enviar las solicitudes es a través de un correo a Ayuda en Línea, o mediante un ticket a través de Remedy, cada uno de los servicios son manejados por un agente de mesa distinto y el proceso varía dependiendo del tipo de solicitud que se haga y dependiendo de las áreas que se vean implicados en dicho proceso, si en dado caso la solicitud no pueda ser resuelta por el Agente de Mesa que es el primer nivel, escala al siguiente nivel que serían el Coordinador de CSC y/o el Gerente de Servicios, y si no es posible que los encargados lo resuelvan, escalaría al último nivel que serían los proveedores de los servicios, a pesar de que se tiene claramente definido el flujo de mando y los procesos a seguir, muchas veces no se llega a notificar adecuadamente el estado o que tan avanzado se encuentran algunas de las solicitudes que se encuentran a la espera por autorización de otra área o bien por complicaciones inesperadas que puedan surgir, ocasionando que los usuarios no reciban información actualizada en esos tipos de casos, también existen casos en los que tanto el usuario como los propios sistemas no notifican adecuadamente del tipo de error o disfuncionalidad que padecen, incluso existe la posibilidad de errores humanos como una mala tipificación del servicio que se desea solicitar, o que repitan dos o más veces una misma solicitud, ocasionando retrasos en los procesos y trabajo extra para los Agentes de Mesa.

4.2. Actividad. Recomendar las posibles soluciones a los riesgos a fin de brindar alternativas de solución.

Una vez comprendido el contexto según las dimensiones de ITIL, se propone una serie de propuestas asociadas a los riesgos vulnerabilidades y amenazas, así como el estándar ITIL algunos otro de seguridad como lo es COBIT, para ofrecer una serie de propuestas de solución adaptadas a estos contextos de forma correctiva y preventiva, para la institución.

4.2.1. Resultados.

Tabla 26. Cuadro de propuestas de solución al riesgo 1.

(Fuente: Elaboración propia).

Riesgo	
Saturación del uso de la cantidad de cuentas disponibles usuarios O365.	
Vulnerabilidad	Amenaza
Falta de un seguimiento en la depuración de cuentas.	Servicios de Microsoft limitados por la ausencia de correo.
Recomendaciones	
Las recomendaciones que brinda ITIL respecto a esta situación sería la cadena de valor del servicio, la cual junto a COBIT 5 en el apartado de alineación, planificación y organización de las actividades de gobierno y gestión de TI establecen que las organizaciones deben contar con la gestión de sus proveedores y los acuerdos de los servicios (APO09 Y APO10).	
Propuesta Preventiva	
Realizar un proceso para la eliminación de usuarios estudiantes que se encuentran inactivos en sistema de un determinado periodo de tiempo.	
Propuesta Correctiva	
Monitoreo de la cantidad de usuarios disponibles y usuarios utilizados en el servicio, la empresa debe tener conocimiento pleno del límite de usuarios totales que proporciona Microsoft O365 a Red Univercom para realizar limpieza de usuarios preventivamente e incluso reestructurar su contrato para la ampliación de servicios con el proveedor.	
Propuesta con Costo	
Establecer con el proveedor de servicios de correo electrónico un incremento en los servidores y/o servicios de O365 mediante una reestructuración de contrato el cual tiene un costo aproximado entre \$70 000 y \$100 000 pesos, o bien un incremento dinámico de servicios de creación de usuarios, teniendo flexibilidad de ampliación únicamente en dicho servicio, esto aumentaría los costos gradualmente conforme se requieran más servicios.	

Tabla 27. Cuadro de propuestas de solución al riesgo 2.

(Fuente: Elaboración propia).

Riesgo	
Retraso en los procesos generales y mala imagen con respecto a la operatividad de la empresa.	
Vulnerabilidad	Amenaza
• Área con muy poco personal. • No se realizan notificaciones constantes de los estados en los que se encuentran los tickets en espera.	• Dependencia de otras áreas.
Recomendaciones	
ITIL maneja el servicio como un todo por lo que propone que se tenga un equilibrio entre sus cuatro dimensiones de la gestión del servicio una de ellas consta en las organizaciones y personas en ella propone que el personal debe tener claro el objetivo de la organización, siendo en este caso la atención a los requerimientos, también indica que el personal debe tener claro las líneas de reporte para tener manejo de las responsabilidades de los empleados y de las actividades que llevan a cabo, también insta que se debe contar con un modelo de comunicación para actividades, roles y demás asuntos ya sean internos o con los usuarios solicitantes.	
Propuesta Preventiva	
El personal encargado de atender las solicitudes debiera notificar al usuario solicitante del estado en el que se encuentra su ticket, en dado caso de que presente alguna problemática para brindar mayor comunicación y retroalimentación por ambas partes.	
Propuesta Correctiva	
Reestructurar el organigrama de Mesa de Servicio debido a que la demanda de solicitudes es superior a la cantidad de personal con el que se cuenta, por ello se propone la contratación de 1 persona más para poder atender estas peticiones. De igual manera la gestión de solicitudes requiere de un mayor seguimiento por parte del personal, sobre todo aquellas solicitudes que lleguen a presentar algún tipo de dificultad o escalado en el nivel de atención a fin de mantener informados a los usuarios y al personal mediante notificaciones constantes en los tickets.	
Propuesta con Costo	
Reestructurar el organigrama de Mesa de Servicio debido a que la demanda de solicitudes es superior a la cantidad de personal con el que se cuenta, es por ello que se propone la contratación de 1 persona más para poder atender estas peticiones, el cual costaría su sueldo de entre \$12000 y \$18000 pesos mensuales dependiendo de los salarios manejados por la empresa más las prestaciones que la empresa ofrezca y para mejorar la gestión de las solicitudes de servicios, sería necesario que la empresa integre un proceso que pueda ser ejecutado a través de un software o un complemento dentro de Remedy que interactúe con los usuarios; el cual ayude o guíe a los usuarios a realizar sus solicitudes o responder las dudas más comunes de los usuarios, este tendría un costo aproximado de entre \$12000 y \$18000 pesos anualmente y que además podría implantarse en otras plataformas.	

Tabla 28. Cuadro de propuestas de solución al riesgo 3.

(Fuente: Elaboración propia).

Riesgo	
La empresa se queda sin servicios para atender solicitudes administrativas y de negocio, servicios financieros, servicios escolares y servicios de TI afectando la operatividad total.	
Vulnerabilidad	Amenaza
• Dependencia completa del área a usar el sistema Remedy. • Tráfico de solicitudes al servidor de Remedy superado.	• Incapacidad de BMC Remedy para proporcionar sus servicios provenientes del proveedor. • Poca banda ancha designada a los trabajadores por parte de la empresa. • Posible limitación que pueda tener BMC Remedy en el diseño de nuevas funcionalidades. • Interrupciones por fallas en servicios de luz o internet.
Recomendaciones	
ITIL maneja que tanto el personal como los sistemas y las demás áreas trabajen holísticamente. COBIT recomienda una gestión de la arquitectura empresarial, junto con una gestión de la seguridad (APO03, APO13), y en base al ISO 17799 se debe de contar con un plan de continuidad del negocio a fin de evitar eventos que interrumpan la disponibilidad de los servicios.	
Propuesta Preventiva	
Actualizar tanto los servidores como el software de Remedy permitiría que tanto los usuarios que realizan solicitudes como los usuarios que trabajan en las solicitudes, puedan operar mejor en el sistema.	
Propuesta Correctiva	
Actualizar tanto los servidores como el software de Remedy permitiría que tanto los usuarios que realizan solicitudes como los usuarios que trabajan en las solicitudes, puedan operar mejor en el sistema. Además, contar con un servidor secundario que pueda operar casi de manera inmediata en caso de que el servidor principal colapse ayudaría a que las áreas que trabajen y dependan del sistema Remedy, no permanezcan demasiado tiempo sin los servicios.	
Propuesta con Costo	
Actualizar tanto los servidores como el software de Remedy permitiría que tanto los usuarios que realizan solicitudes como los usuarios que trabajan en las solicitudes, puedan operar mejor en el sistema, estos servidores tendrían un costo de entre \$65000 a \$75000 pesos por servidor dependiendo de los componentes que estos tengan y teniendo una vida útil de entre 5 a 8 años o más. Además, contar con un servidor secundario que pueda operar casi de manera inmediata en caso de que el servidor principal colapse permitiría que las áreas que trabajen y dependan del sistema Remedy, no permanezcan demasiado tiempo sin los servicios. Adicionalmente contar con un software que realice respaldos de la información del sistema de manera automática, evitaría hacer estos respaldos de manera manual esto tendría un costo de aproximadamente \$25000 pesos.	

Tabla 29. Cuadro de propuestas de solución al riesgo 4.

(Fuente: Elaboración propia).

Riesgo	
La empresa atiende solicitudes administrativas y de negocio, servicios financieros, servicios escolares y servicios de TI operando inadecuadamente.	
Vulnerabilidad	Amenaza
• Procesos explicados de manera oral. • Cuestionamientos repetitivos provocados por malas prácticas de los usuarios. • Falta de especificación en los errores producidos en los sistemas.	• Duplicación de solicitudes y saturación del servicio del soporte técnico por parte de los usuarios solicitantes. • Errónea tipificación de servicio por parte del usuario solicitante.
Recomendaciones	
ITIL junto al ISO 17799 propone una seguridad de los recursos humanos que se establezcan claramente las actividades y los flujos de trabajo además recomienda una correcta designación de los roles y que el personal se encuentre adecuadamente capacitado. COBIT recomienda asegurar la optimización al riesgo al evaluar, orientar y supervisar.	
Propuesta Preventiva	
Informar a los estudiantes acerca de cómo pueden incorporarse al sistema Remedy y como es que funciona este sistema ayudando a que los alumnos conozcan a detalle los servicios, atenciones y tramites que Mesa de Servicio les puede brindar a través de Remedy, también ayudaría a que los alumnos sean capaces de realizar las solicitudes de manera adecuada y mitigar repeticiones de estas o problemas de especificación en los servicios que los alumnos requieren.	
Propuesta Correctiva	
Contar con manuales de operación, capacitación inmediata cuando se integra alguna nueva funcionalidad o sistema y evaluaciones de desempeño al personal de trabajo, demostraría el rendimiento y capacidad de los trabajadores de Mesa de Servicio, y brindar capacitaciones a usuarios que interactúen constantemente con el sistema ya sean trabajadores o alumnos, mitigaría el mal manejo que le den al sistema y ayudaría a demostrar el funcionamiento a los usuarios.	
Propuesta con Costo	
Invertir en la capacitación y en manuales de uso tanto para personal administrativo invirtiendo aproximadamente \$10000 en videos o programas educativos como para estudiantes invirtiendo \$5000 en algún video explicativo.	

Tabla 30. Cuadro de propuestas de solución al riesgo 5.

(Fuente: Elaboración propia).

Riesgo	
Pérdida y/o robo de información.	
Vulnerabilidad	Amenaza
• Cualquier usuario tendría acceso información que no corresponden a su puesto. • Mal uso de los sistemas por parte de los usuarios.	• Ataques de personas externas que puedan acceder a información confidencial.
Recomendaciones	
Las prácticas de gestión ITIL establece un marco de gestión de incidentes y de problemas, en el establece que la empresa debe contar con prácticas de gestión de problemáticas antes de que se vuelvan incidentes que afecten a la operatividad. COBIT establece propone una mitigación al riesgo junto con una gestión de la seguridad de la información para prevenir las perdidas o el robo. El ISO 17799 establece que se deben realizar evaluaciones de riesgos de seguridad y contar con una política de seguridad de la información, así como la clasificación del tipo de información que se esté manejando para establecer controles de acceso a la información.	
Propuesta Preventiva	
Revisión preventiva de los permisos en los usuarios de los trabajadores con accesos a sistemas de información sensible para la empresa.	
Propuesta Correctiva	
Tener limitados los accesos a información confidencial o de alto valor para la empresa, requiere de controles de seguridad como una mayor limitación en los accesos a páginas de internet que no sean de relevancia para la empresa, contar con un perfilado de usuarios en Remedy, para la limitación en la visualización de tickets entre los Agentes de Mesa para que los que sean asignados por sistema a un Agente de Mesa solo los pueda visualizar el trabajador y los superiores.	
Propuesta con Costo	
Implementación de un software que monitoree de manera interna los equipos de los trabajadores y prevenga amenazas internas, este software tendría un costo de \$2500 pesos anuales.	

4.3. Actividad. Estructurar las propuestas y posibles soluciones con base al modelo de mejora continua ITIL y otros estándares.

Este apartado contiene una serie de soluciones preventivas descrita a detalle que se implementarán en la empresa junto con recomendaciones y seguimientos que se deberían de establecer para monitorear los servicios, así como prevenir al área de Mesa a que sucedan nuevamente este tipo de incidentes.

4.3.1. Propuestas para el riesgo de saturación del uso de la cantidad de cuentas disponibles para usuarios O365

Las siguientes propuestas tienen como objetivo presentar diversas soluciones viables para el personal de mesa de servicio, con el fin de prevenir la saturación de los servicios de O365.

4.3.1.1. Propuesta 1. Proceso de eliminación de cuentas de estudiantes inactivos en un periodo de tiempo específico.

Realizar un proceso para la eliminación de usuarios O365 de estudiantes, a fin de prevenir la saturación de los servicios que Microsoft ofrece para usuarios de O365 en Red Univercom y optimizar su rendimiento, para ello se determinaron parámetros de discriminación que ayuden a determinar los usuarios candidatos a ser eliminados para lograr este objetivo.

Los cuales, en sistema deben tener las siguientes condiciones para su eliminación:

- Programa finalizado: Debe haber transcurrido un periodo de tiempo determinado a partir de que el estudiante haya culminado su ciclo educativo dentro de la institución y que basado en las estadísticas del Campus Coacalco que es el campus más grande con el que cuenta la Red Aliat es un periodo de 3 años en el cual el alumno ya no regresa a la institución.
- Baja definitiva: Que al momento de la revisión se determine en el sistema que han pasado por lo menos 12 meses, 2 semestres o 3 cuatrimestre de inactividad del alumno en cuestión y se encuentre con el estatus que se le asigna al estudiante en los siguientes casos:

- Por adeudo de ciclos anteriores, que según el nivel académico que curse o haya cursado (bachillerato o nivel superior), las variables son distintas, en el caso del nivel medio superior y según las leyes del consumidor es 3 colegiaturas vencidas según el artículo 7 del acuerdo que establece las bases mínimas de información para la comercialización de los servicios educativos que prestan los particulares que se encuentra en el anexo 5, y en el caso de nivel superior, el reglamento de la institución dictamina que los servicios al consumir se suspenderán después de 2 colegiaturas vencidas que se puede ver en el anexo 6.
 - Por cambio de residencia definitiva y que el alumno haya manifestado no desear continuar en Red Univercom en alguna otra cede.
 - Por situaciones psicosociales, como puede ser trastornos psicológicos, enfermedades que eviten el reincorporamiento al régimen educativo de manera permanente, problemas legales, etc.
- Baja temporal: en este caso no será sujeto a eliminación a menos que haya transcurrido 12 meses, 2 semestres o 3 cuatrimestres en los que el alumno no haya manifestado su deseo de reincorporarse nuevamente a la institución. Se entiende por baja temporal casos como:

Por enfermedad, lesiones, embarazos, situaciones económicas, problemas laborales o problemas psicológicos que se encuentren dentro del rango establecido.

Para realizar este proceso es necesario realizar una discriminación la cual consiste en descartar aquellos alumnos que se encuentren activos actualmente en sistema, alumnos cuyo estatus esté finalizado y que no supere el año de culminación (en caso de que el alumno desee realizar alguna maestría o doctorado). El resto de los alumnos serian considerados para la eliminación de su usuario siempre y cuando cumpla con los criterios antes mencionados.

Tabla 31. Descripción detallada del proceso de depuración de cuentas de correo institucionales de alumnos.

(Fuente: Elaboración propia).

No.	Puesto u/o sistema	Descripción de la actividad.
1	Gerente de Mesa	El gerente de mesa realiza una solicitud a dirección de TI de aquellos alumnos que tienen su registro en sistema en un periodo de tiempo posterior a terminar su ciclo educativo. Existe la posibilidad de que se tengan que

		realizar cambios en la solicitud por falta de información o que se detalle más, en dado caso de que se tenga que detallar más se tendría que rehacer la solicitud, si no la solicitud pasaría al encargado de dirección de TI para que la apruebe y responda la solicitud.
2	Gerente de Mesa	Envía la solicitud a la dirección de TI

Tabla 31. Descripción detallada del proceso de depuración de cuentas de correo institucionales de alumnos (Continuación).

3	Dirección de TI	Recibe la solicitud y se encarga de evaluar y determinar si es posible proporcionar la información solicitada. Al recibir la solicitud existe la posibilidad de que falte información y el solicitante tenga que detallar más y/o rehacer la solicitud, o que se realice la solicitud correctamente. Se encarga de aceptar o rechazar la solicitud, en caso de ser rechazado se terminaría el proceso si no pasaría a extraer la información solicitada.
4	Campus Solution	A través de este sistema se genera un archivo que almacene la información de los alumnos en sistema.
5	Dirección de TI	Filtra la información a lo solicitado y se lo envía al Gerente de Mesa.
6	Dirección de TI	Envía el archivo con las especificaciones solicitadas.
7	Gerente de Mesa	Recibe el archivo con la información solicitada
8	Gerente de Mesa	Delega al personal que tiene a su cargo la gestión de la eliminación de los usuarios en los sistemas.
9	Coordinador de CSC	Selecciona la información referente a los correos que procederá a eliminarse.
10	Servicios Microsoft	Se carga el archivo al centro de administración de Microsoft con la información que se eliminara. Existe la posibilidad de que la información que se carga en el archivo se encuentre de manera errónea por lo que si llega pasar se tendría que cargar nuevamente la información corregida si no es el caso se quedaría en el apartado de eliminados.
11	Servicios Microsoft	El centro de administración de Microsoft envía los usuarios de correo al apartado de usuarios eliminados.
12	Coordinador de CSC	Realiza un seguimiento mediante un reporte de la cantidad de información eliminada.
13	Servicios Microsoft	Borra definitivamente la información de manera permanente después de 1 mes.

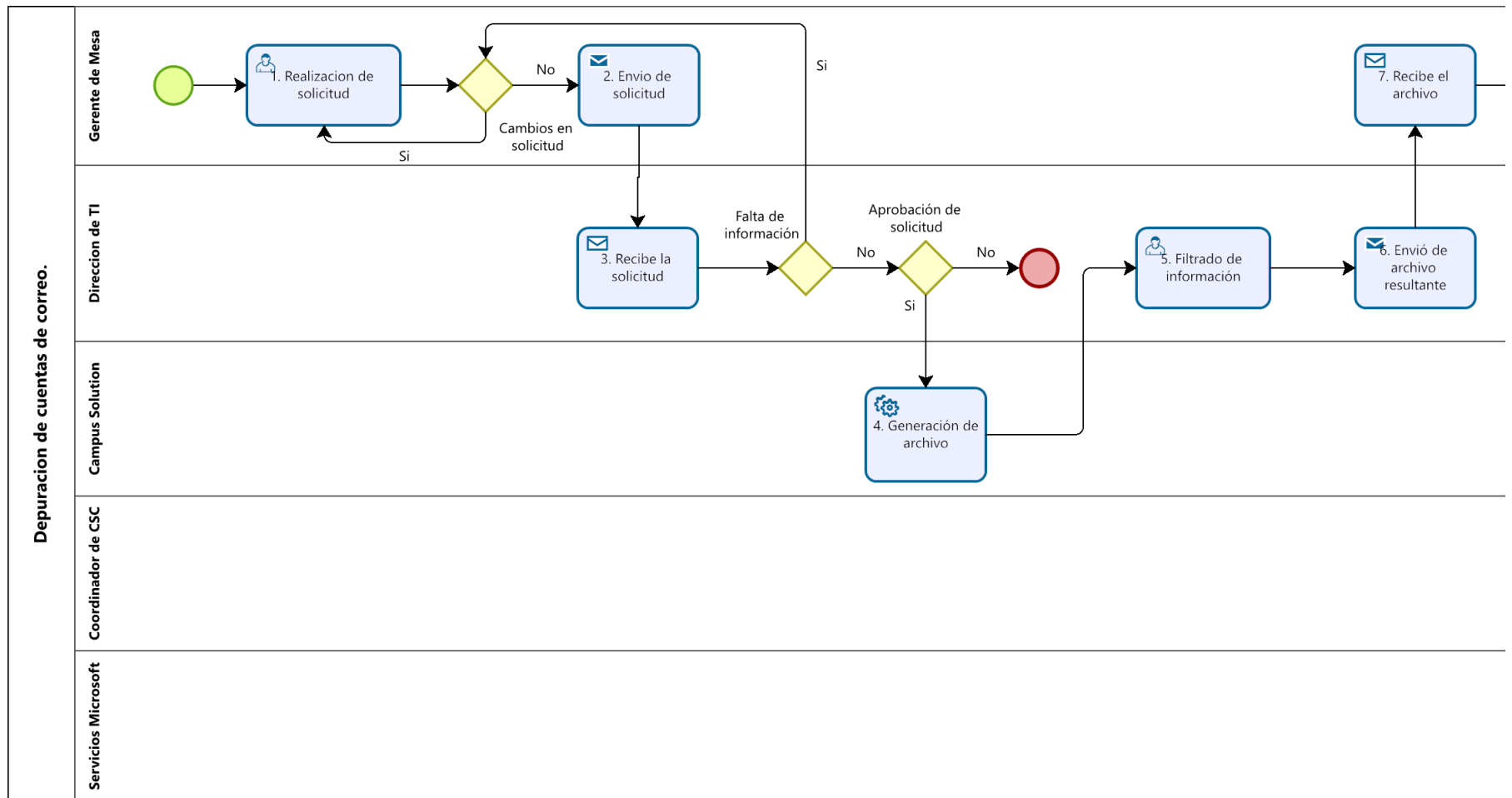


Figura 32. Diagrama de proceso para la eliminación de usuarios O365.

(Fuente: Elaboración propia).

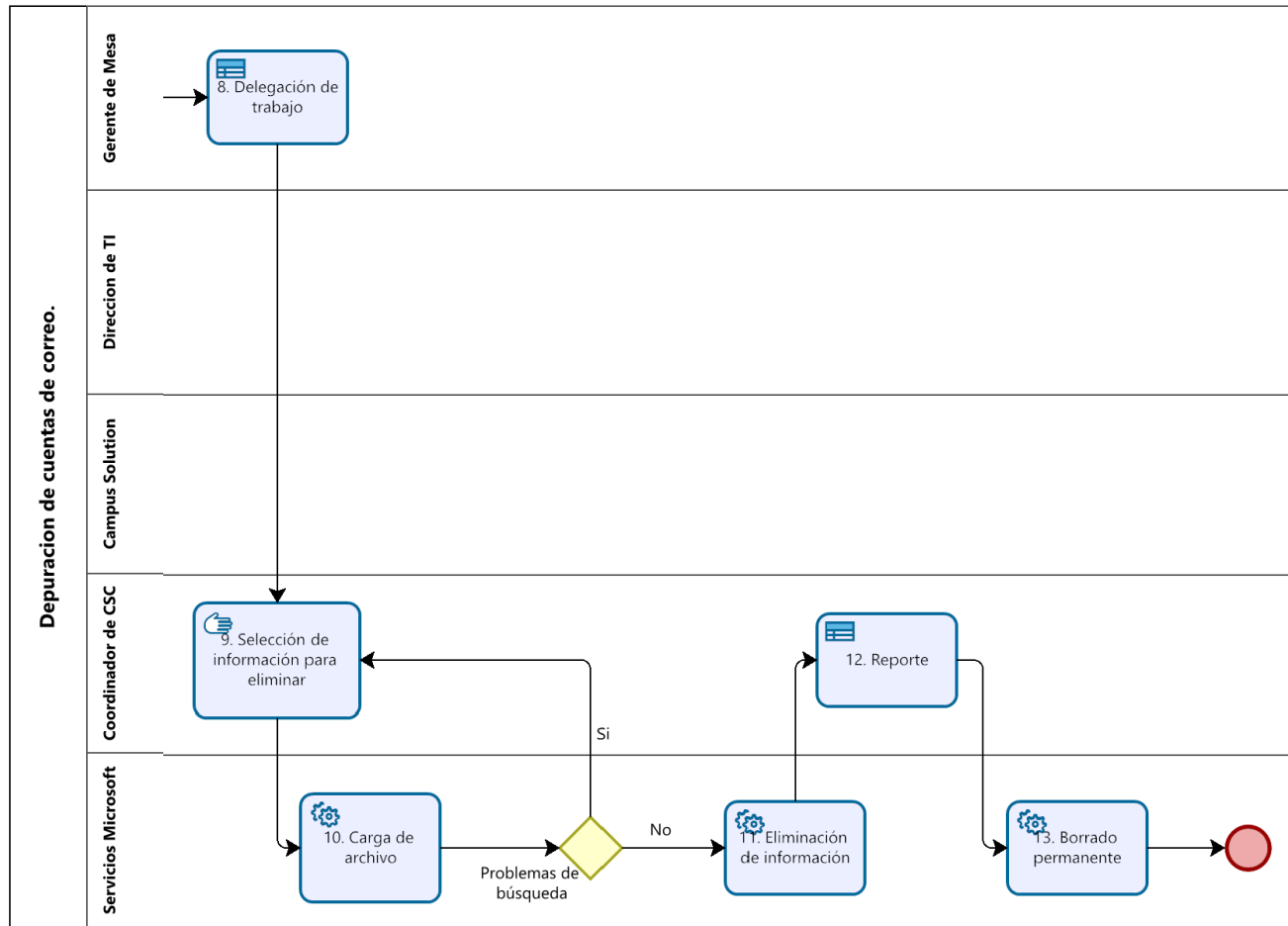


Figura 32. Diagrama de proceso para la eliminación de usuarios O365 (Continuación).

4.3.1.2. Propuesta 2. Monitoreo y/o reestructuración de contrato con proveedor.

Monitoreo de la cantidad de usuarios disponibles y usuarios utilizados en el servicio, la empresa debe tener conocimiento pleno del límite de usuarios totales que proporciona Microsoft O365 a Red Univercom para realizar limpieza de usuarios preventivamente e incluso establecer con el proveedor de servicios de correo electrónico un incremento en los servidores y/o servicios de O365 mediante una reestructuración de contrato, o bien un incremento dinámico de servicios de creación de usuarios, teniendo flexibilidad de ampliación únicamente en dicho servicio, esto aumentaría los costos gradualmente y conforme se requieran más servicios.

Actualmente en Red Univercom maneja un contrato con Microsoft de 500,000 usuarios de Office 365 que engloban usuarios administrativos, docentes y estudiantes a nivel nacional, el personal de Mesa de Servicio, encargado de gestionar los servicios de altas de usuarios administrativos, docentes y estudiantes en los servicios de Microsoft, tenían la idea de que los usuarios de estos servicios para estudiantes eran ilimitados, sin embargo, se comprobó que no era así, por lo que una reestructuración de contrato para la actualización de los servicios y/o negociación para la mejora de estos, debe tomar en cuenta el crecimiento de alumnos matriculados por año. Para este ejercicio se tomó como muestra el crecimiento de alumnos matriculados según la estimación del Campus ETAC Coacalco y debido a que maneja tres ciclos cuatrimestrales y dos semestrales, se manejó un periodo en el que tanto ciclo cuatrimestral y semestral en los que ambos iniciaron en enero del 2024.

Tabla 32. Indicé de matriculación de estudiantes en el ciclo cuatrimestral y semestral actual.

Alumnos matriculados	Alumnos Reinscritos	Alumnos de nuevo ingreso	Crecimiento de matrícula en porcentaje
3300	2825	475	15%

Este índice de crecimiento de alumnos activos, reescritos y de nuevo ingreso es una estimación del ciclo que se inició en enero del 2024 únicamente del Campus ETAC Coacalco que es el campus más grande de Aliat.

Por lo que se debe llevar un monitoreo de la cantidad de usuarios O365 de los que se disponen actualmente, saber cuántos usuarios ya se tienen en uso y cuantos quedan disponibles para que en dado caso de que la cantidad alumnos activos supere el límite de usuarios de los que se disponen se tenga contemplado el crecimiento en los servicios.

Actualmente, el contrato que se tiene con Microsoft respecto a sus servicios con Red Univercom, se puede ver sujeto a una reestructuración por el tiempo que se tiene con el

mismo y además por las posibles mejoras nuevas en los servicios que Microsoft puede haber agregado actualmente y que por la antigüedad del contrato actual no se puedan ver reflejados en Red Univercom.

Para los alumnos Microsoft ofrece los servicios de Office 365 Educación. Estos servicios requieren que la institución este avalada como una organización educativa, de esta forma ofrece sus servicios básicos de manera gratuita o bien si se requieren servicios más completos, es posible que requieran de una negociación en base a las necesidades de Red Univercom.

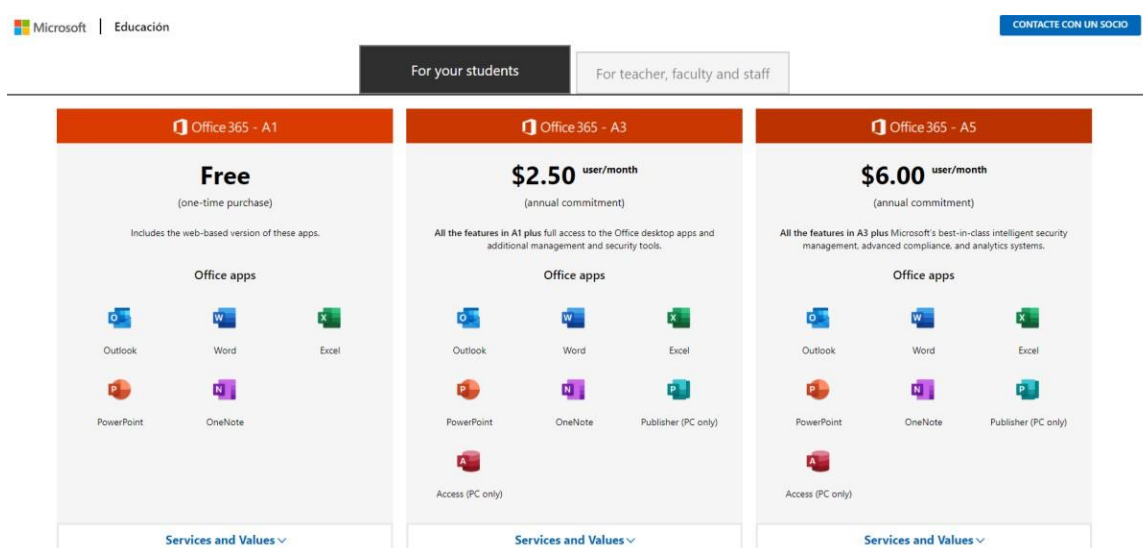


Figura 33. Servicios de Office 365 para estudiantes.

(Microsoft, 2024).

El modelo de servicio que se muestra aquí toma en cuenta la cantidad de usuarios que se tengan activos y del tipo de licencia que maneje, esta modelo es muy dinámico, es decir solo pagas por lo que se está usando de manera mensual, que puede ser útil en una escala pequeña, en este caso para Red Univercom al ser una empresa de educación privada a nivel nacional requeriría un modelo de negocio en el cual se tenga un cierto margen de disponibilidad que pueda incrementarse si es necesario de manera anual a fin de tener un seguimiento y evitar pérdidas monetarias innecesarias.

4.3.2. Propuesta para el riesgo retraso en los procesos generales y mala imagen con respecto a la operatividad de la empresa.

Para una institución educativa de carácter privada, la imagen ante la sociedad puede influir en la matriculación de nuevos alumnos y la generación de convenios, esta imagen puede verse influida por ejemplo por como brindan la atención a sus alumnos y a su personal.

4.3.2.1. Propuesta 1. Fortalecer la atención a los usuarios mediante un mayor seguimiento, notificaciones e interacción.

En este proceso la vulnerabilidad que se detectó fue en el seguimiento a los tickets que llegan mesa de servicios, cuando esto pasa, hoy en día, el seguimiento se da al momento en que el usuario vuelve a preguntar por el estado del ticket solicitado, provocando según la guía de buenas prácticas empresariales ITIL, una pérdida de valor en el servicio.

La propuesta que se hace en este caso es que el personal encargado de atender las solicitudes deberá notificar al usuario solicitante del estado en el que se encuentra su ticket, y en dado caso de que presente alguna problemática, se debe mantener informado al usuario solicitante para brindar una mejor atención, mantener un adecuado seguimiento y así obtener una retroalimentación para ambas partes.

Mesa de servicio es un área que trabaja por niveles de atención, el primer nivel es conformado por los agentes de masa los cuales son los encargados de atender las solicitudes más comunes como atención en solicitudes de alumnos, tramites escolares o financieros, asignación de becas, etc. En el caso en el que se presente alguna problemática fuera del protocolo como alguna anomalía en información académica o financiera de alumnos, problemáticas en los servicios y aplicaciones o algún otro problema que requiera atención administrativa, es cuando la solicitud sube a el segundo nivel de atención el cual se encarga de administrar los servicios, generación de reportes, e incluso la creación y desactivación de usuarios entre otras funciones de carácter administrativo, en dado caso de que la incidencia este más allá del alcance de las funcionalidades de Mesa de Servicio, como pueden ser problemáticas en la distribución de los servicios de correo electrónico, aplicaciones móviles para estudiantes, docentes o administrativos por parte del proveedor y problemas en servicios básicos como luz o internet, es cuando se recurre al tercer nivel de atención el cual es recurrir directamente a los proveedores de servicios para reportar los problemas que su cliente está teniendo.

Tipos de solicitudes que resuelve un Agente de Mesa.

Los agentes de mesa se encargan de atender los siguientes tipos de solicitudes:

CATEGORIA DE SERVICIO	SERVICIO	ESTATUS	Acuerdo - SLA	PRIORIDAD	Total
Servicios de Negocio	Matriculación/Reinscripción/Baja Prepa Flex	En línea	1 hra	Alta	13
	Solicitud de Carga de Datos en Campus Solutions	En línea		Alta	
	Apertura Lógica de Nueva Zona o Campus	En línea	68 días	Baja	
	Expansión-Apertura Lógica de Nueva Zona o Campus	En línea	30 días	Media	
	Matriculación/Re-inscripción/Baja Programa Empréndete	En línea	6 hrs	Media	
	Facturación Anticipada / Manual	En línea	8 hrs	Media	
	Carga de Datos Docentes	En línea	8 hrs	Media	
	Atención de Solicitudes de Aplicaciones Administrativas	En línea	4 hrs	Media	
	Generación de Reportes	En línea	8 hrs	Media	
	Administración de Cuentas de Acceso a Aplicaciones Administrativas	En línea	6 hrs	Media	
	Administración de Envío de Correos Masivos (Comunicados)	En línea	N/A	N/A	
	Mantenimiento preventivo/correctivo al sistema	En línea	N/A	N/A	
	Timbrado de Nómina	En línea	N/A	N/A	
CATEGORIA DE SERVICIO	SERVICIO	ESTATUS	Acuerdo - SLA	PRIORIDAD	Total
Servicios generales	Servicio de Incidencias y Requerimientos de Telefonía Móvil	En línea	24 hrs	Baja	6
	Bitácora de Asistencia – Limpieza y Vigilancia	En línea	16 hrs	Baja	
	Reporte de Incidencias y Requerimientos de Mensajería	En línea	16 hrs	Baja	
	Solicitud de Factura para Baja por Sinistro	En línea	16 hrs	Baja	
	Movimiento de Activo Fijo	En línea	40 hrs	Baja	
	Solicitud de Estado de Cuenta	En línea	8 hrs	Media	
Servicios Financieros	Solicitud de Alta de Proveedores	En línea	24 hrs	Baja	16
	Comprobaciones y Reembolsos	En línea	40 hrs	Baja	
	Solicitud de Alta de Proveedores Honorarios Docentes	En línea	24 hrs	Baja	
	Anticipo a Empleados	En línea	40 hrs	Baja	
	Solicitud de Alta y Asignación de Artículos	En línea	10 hrs	Baja	
	Solicitud de Cotización	En línea	24 hrs	Baja	
	Alta de Valores de Segmentos Contables	En línea	24 hrs	Baja	
	Google y Facebook	En línea	8 hrs	Media	
	Devolución de Pago al Alumno	En línea	8 hrs	Media	
	Recibos Estándar	En línea	8 hrs	Media	
	Condonaciones	En línea	8 hrs	Media	
	Solicitud de Combinaciones Contables	En línea	4 hrs	Media	
	Orden de Compra Urgente	En línea	8 hrs	Media	
	Consulta de Artículos	En línea	8 hrs	Media	
	Solicitud de Comprobantes	En línea	8 hrs	Media	
	Reclasificaciones	En línea	8 hrs	Media	

Figura 34. Servicios proporcionados y atendidos por Agentes de Mesa de Servicio.

(Red Univercom, 2020)

Estas solicitudes en ocasiones presentan problemas que superan el conocimiento y el perfil de puesto para atender las discrepancias en este caso las limitaciones serian cambios en la información en aplicaciones de Campus Solution y HCM, aplicados al apartado de finanzas, recursos humanos y cualquier tipo de información sensible que no le corresponda al área o usuario particular, en esos casos es cuando se acude al Coordinador de CSC o al Gerente de Mesa de Servicio los cuales representan el segundo nivel de atención.

Tipos de solicitudes que resuelve el coordinador de CSC o superiores.

El Gerente de Mesa y el Coordinador de CSC normalmente se encargan de delegar las solicitudes y atender incidencias de carácter administrativo, sin embargo, existen situaciones anormales al protocolo y situaciones de carácter crítico que requieren de la atención de personal de alto rango para mitigar el fallo en las operaciones de la empresa, por ejemplo:

CATEGORIA DE SERVICIO	SERVICIO	ESTATUS	Acuerdo - SLA	PRIORIDAD	Total
Servicios de TI	Combo Incidentes CRM	En línea	2 hrs	Alta	19
	Análisis y Gestión de Nuevos Requerimientos a los Sistemas	En línea	N/A	N/A	
	Gestión de Correo Electrónico Institucional	En línea	8 hrs	Media	
	Habilitación de Servicios de Voz	En línea	16 hrs	Baja	
	Infraestructura Red de Datos Conectividad remota - VPN	En línea	Conectividad remota - VPN	Baja	
	Infraestructura Red de Datos Apertura de puertos	En línea	Apertura de puertos	Baja	
	Infraestructura Red de Datos Configuración de acceso a Internet	En línea	Configuración de acceso a Internet	Media	
	Infraestructura Red de Datos Acceso a la red inalámbrica	En línea	Acceso a la red inalámbrica	Media	
	Instalación de Equipos de Cómputo de Oficina	En línea	8 hrs	Media	
	Instalación y/o Configuración de Software Institucional	En línea	16 hrs	Baja	
	Mantenimiento Preventivo/Correctivo a Equipo de Cómputo Institucional	En línea	8 hrs	Media	
	Lentitud en Aplicaciones Administrativas	En línea	8 hrs	Alta	
		En línea	30 min	Crítica	
		En línea	7 hrs	Crítica	
		En línea	16 hrs	Media	
	No Disponibilidad de Aplicaciones Administrativas	En línea	7 hrs	Alta	
		En línea	30 min	Crítica	
		En línea	4 hrs	Media	
		En línea	16 hrs	Baja	

Figura 35. Servicios atendidos el Gerente de Mesa y el Coordinador de CSC.

(Red Univercom, 2020)

Estos servicios requieren permisos de administrador los cuales solo los poseen altos rangos dentro de Mesa de Servicio, además se encargan de dar seguimiento a los casos especiales que llegan a surgir en cualquiera de las solicitudes como pueden ser problemas en las aplicaciones de los estudiantes (Mi red Aliat, Brightspace o portales de servicios en línea), problemáticas financieras como duplicidad en recibos, pagos no reflejados en sistemas o casos que requieran algún seguimiento con alguna otra área en particular o bien en dado caso de que alguno de estos casos particulares sean por problemas más allá de Mesa de servicio y las áreas de Red Univercom, es que se realiza un reporte a los proveedores de servicios que son el tercer nivel de atención.

Tipos de solicitudes que resuelven los proveedores de servicio.

Los proveedores son el ultimo nivel de atención debido a que son ellos los encargados de proveer funcionalidades que complementen la operatividad de administrativos, docentes y estudiantes, estas problemáticas pueden ser interrupciones en los servicios, actualizaciones o

parches que los proveedores realicen en sus tecnologías, incumplimiento en los servicios según los contratos y la sostenibilidad que los proveedores deben tener para proporcionar sus servicios a largo plazo.

El proceso que se propone para mantener al usuario solicitante informado y llevar un seguimiento a las incidencias es el siguiente:

Tabla 33. Descripción detallada del proceso de notificaciones del estatus de los tickets en espera.

(Fuente: Elaboración propia).

No.	Puesto u/o sistema	Descripción de la actividad.
1	Usuario	Estudiante o administrativo que genera un ticket de cualquier tipo de solicitud que necesite como se muestran las figuras 25 y 26.
2	Agente de Mesa	Recibe un ticket de cualquier tipo de problemas de servicios administrativos, servicios de TI, servicios escolares y financieros. Si es una solicitud que el agente de mesa pueda resolver mostrados en la figura 25, el Agente lo resuelve, si presenta problemas se notifica al Coordinador de CSC.
2.1	Agente de Mesa	En caso de que no se presente ninguna problemática o anomalía en la operatividad el Agente de Mesa resuelve el ticket.
3	Coordinador de CSC	Recibe, evalúa y/o resuelve la problemática de la incidencia como las que se muestran en la figura 26, que el agente de mesa no pudo resolver.
3.1	Coordinador de CSC	Si es posible que el Coordinador de CSC resuelva la incidencia, realiza la atención correspondiente o le indica al Agente de Mesa la solución.
3.2	Coordinador de CSC	En caso de que no se presente ninguna problemática o anomalía en la operatividad el Coordinador de CSC resuelve la incidencia.
4	Agente de mesa	Si no es posible resolverse en Mesa de Servicios se notifica al usuario del estatus de su solicitud para darle seguimiento e informar al usuario solicitante
4.1	Agente de mesa	Envía una notificación al tercer nivel de atención a cerca de la incidencia.
4.2	Áreas de Soporte técnico	Recibe la notificación de la problemática presentada.
4.3	Áreas de Soporte técnico	Resuelven la incidencia.

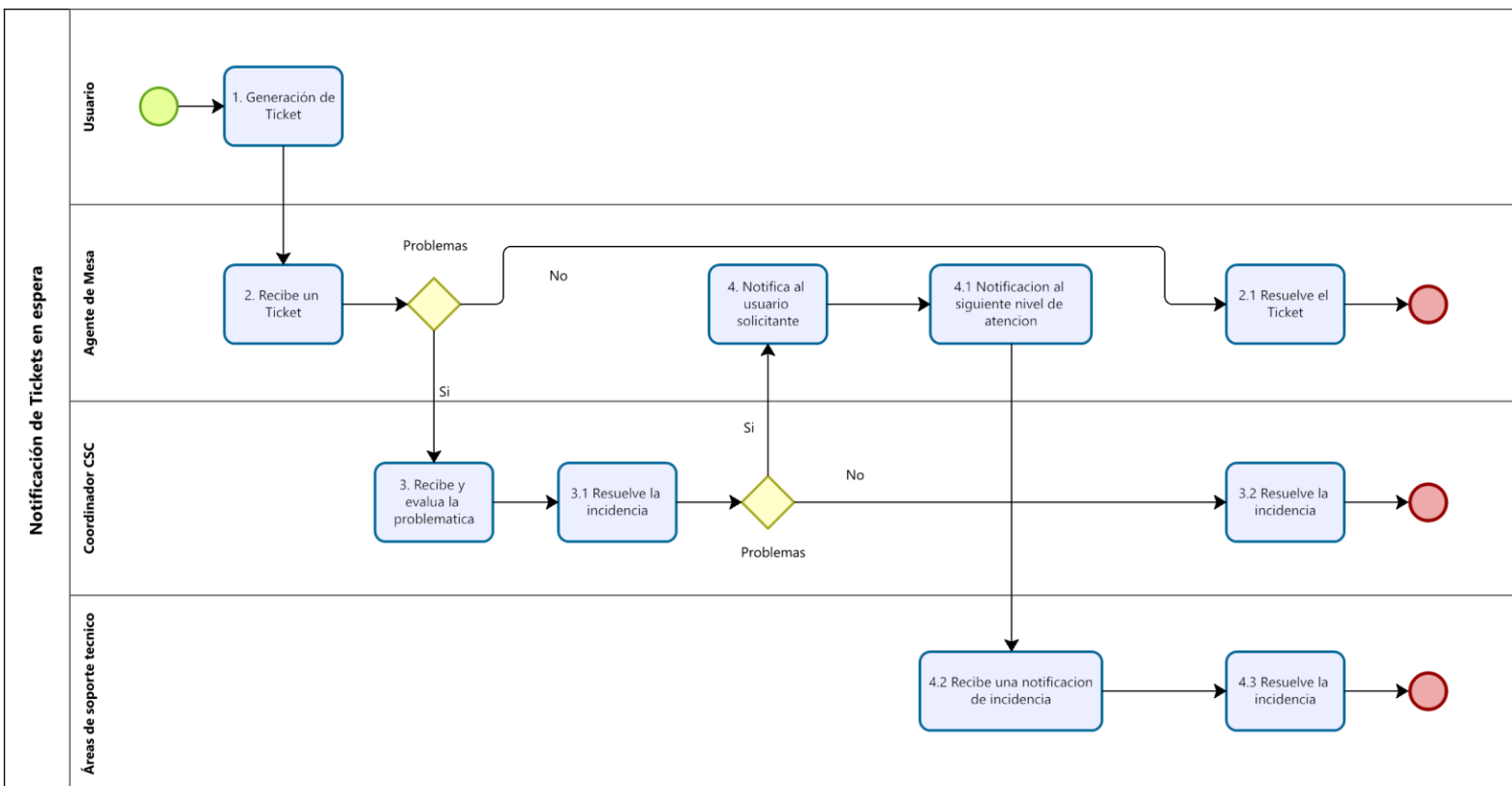


Figura 36. Diagrama de proceso para la notificación y seguimiento de Tickets.

(Fuente: Elaboración propia).

4.3.2.2. Propuesta 2. Contratación de personal adicional para Mesa de Servicio.

Reestructurar el organigrama de Mesa de Servicio debido a que la demanda de solicitudes es superior a la cantidad de personal con el que se cuenta, es por ello por lo que se propone la contratación de 1 persona más para poder atender estas peticiones.

Requisitos para un agente de Mesa de Servicio.

Características personales

ESCOLARIDAD			
	Estudiante		Trunca
X	Carrera Técnica	X	Pasante
	Maestría	X	Licenciatura
	Otro (explicar):		

ÁREAS DE ESCOLARIDAD			
	Abogado	X	Finanzas
X	Administración		Ingeniería
	Actuario		Ingeniería Industrial
	Comunicación		Medicina
	Contaduría	X	Sistemas
	Economía		Telecomunicaciones
	Otros (especifique):		

MANEJO DE PC							
X	Word	X	Excel	X	PowerPoint	X	Outlook
X	Otros (especifique):	Herramientas de Gestión de Incidencias o ITSM ejemplo (OSTicket; Remedy Footprint; etc.)					

IDIOMAS			
Idioma:	Inglés	Porcentaje:	No necesario
Otros (especifique):			

EXPERIENCIA	
Años	Área
2	Soporte Técnico; HelpDesk

Otros requerimientos.

Contar con actitud de servicio, tolerancia a la frustración.

Indicadores de desempeño.

Nombre	Unidad de medida
En definición con la Dirección de CSC y TI	

Competencias.

Competencias genéricas	Grado				
	1 Ausencia	2 Básico	3 Dominio	4 Avanzado	5 Experto
Servicio al cliente			X		
Liderazgo			X		
Trabajo en equipo			X		
Orientación a resultados			X		
Apertura al cambio			X		
Planeación, organización y control		X			
Solución de problemas			X		
Comunicación asertiva			X		
Trabajo bajo presión			X		

Propósito del Agente de Mesa de Servicio.

Brindar atención vía telefónica y/o remota a los usuarios del segmento administrativo sobre los reportes de tecnología y/o servicios de negocio proporcionando atención de primer nivel, basados en procedimientos relevados con anterioridad para resoluciones en primera instancia.

Funciones principales de Agente de Mesa de Servicio.

- 1) Brindar atención a reportes vía telefónica.
- 2) Atender reportes mediante las herramientas de gestión de tickets (incidencias/requerimientos), asignado un folio al incidente y manteniendo al usuario informado del estatus del ticket que se han generado en su nombre.
- 3) Mantener al usuario informado de los cambios tecnológicos.
- 4) Dar seguimiento al incidente hasta su solución final.

- 5) Verificar el estatus del reporte de usuario con el área/departamento al que fue asignado.
- 6) Asignar el incidente al siguiente nivel de atención.
- 7) Documentar el problema.
- 8) Interpretar y documentar a nivel técnico el reporte del incidente para poder escalarlo al siguiente nivel, llevando a cabo todo lo necesario para cumplir con procedimientos y políticas del área de informática.
- 9) Aplicación de encuesta en línea al momento de la resolución del reporte de servicio.
- 10) Registrar en la herramienta de gestión de incidencias las calificaciones y comentarios que se otorgaron por parte de los usuarios.

Retos del Agente de Mesa de Servicio.

- 1) Resolver el 90% de los reportes de los usuarios que puedan ser solucionados por el primer nivel de soporte, en caso de poder ser resueltos.
- 2) Mantener al usuario informado del estatus del ticket que se han generado en su nombre.

Propuesta 3

Integrar un proceso que pueda ser ejecutado a través de un software o un complemento dentro de Remedy que interactúe con los usuarios; el cual ayude o guíe a los usuarios a realizar sus solicitudes o responder las dudas más comunes de los usuarios.

Dos de las mejores opciones que actualmente son recomendables en la industria de Inteligencia artificial son los servicios de Bot de Azure IA y Amazon Lex que es una rama de los servicios de AWS (Amazon Web Service).

Tabla 34. Tabla de comparación de Azure y AWS.

Servicios	Servicios que ofrece	Logos
Servicio de Bot de Azure AI	El Servicio de Bot de Azure AI proporciona un entorno de desarrollo integrado para la creación de bots. Su integración con Power Virtual Agents , una plataforma con poco código totalmente hospedada permite a los desarrolladores con distintas capacidades técnicas crear bots de inteligencia artificial conversacionales sin necesidad de código.	
Amazon Lex de AWS	Servicio para crear interfaces de conversación con voz y texto en cualquier aplicación. Las organizaciones pueden utilizar Amazon Lex para implementar la interfaz conversacional que prefieran en sus procesos empresariales y casos de uso a fin de alcanzar sus objetivos y mejorar la satisfacción de los clientes y superar sus expectativas.	

Tabla 35. Comparativa de precios en los servicios de Azure IA y Amazon Lex

Servicios de Chat Bots	Comparativa de precios
Servicio de Bot de Azure AI	Ofrece dos tipos de servicios, canales de uso general y canales Premium. - Servicios generales son gratuitos - Servicios Premium: - o Servicios de IA Estándar tiene un costo de 10 dólares mensuales y un número ilimitado de documentos gestionados. - o Servicios de Bot de Azure IA S1 de canales premium 1,000 solicitudes a 0.50 dólares
Amazon Lex IA conversacional para chat bots.	Ofrece servicios de entrada de voz y texto. - Las solicitudes de voz tienen un costo de 0.004 dólares por solicitud. - Las solicitudes de texto tienen un costo de 0.00075 dólares por solicitud.

Como se puede observar, Azure ofrece servicios gratuitos que, si bien no pueden llegar a ser los más rápidos al estar disponibles para todos aquellos que trabajan con estos servicios gratuitos, permite que se puedan utilizar estos servicios a modo de prueba y tener una evaluación del desempeño y que ofrecerían estos servicios. Amazon Lex ofrece precios más accesibles, sin embargo, los precios varían dependiendo el tipo de solicitud que se haga.

Beneficios de Servicio de Bot de Azure AI

Aprovechando que Red Univercom trabaja actualmente con algunas de las ramas de los servicios de Microsoft, con Azure ofrece soluciones en la nube, en este caso, para la integración de los servicios de un Chat Bot en Remedy para la resolución de problemas simples a cerca del uso del sistema, servicios que pueden solicitar los usuarios, preguntas frecuentes e incluso el proceso a seguir para la solicitud de tramites. Lo anterior podría orientarse al tipo de usuario que interactúa con el sistema, en este caso estudiantes y administrativos.

Los servicios de Power Virtual Agents que facilitan la creación de Bots sin necesidad de código trae consigo los siguientes beneficios, permite que se puedan crear y probar Bots de manera más rápida, se pueden mejorar los Bots con el paso del tiempo permitiendo que estos sean capaces de predecir temas futuros y permite que se implementen las funcionalidades de IA de manera segura manteniendo la gobernanza.

Beneficios de Amazon Lex

Amazon Lex es un servicio para crear interfaces de conversación con voz y texto en cualquier aplicación, los beneficios de implementar Amazon Lex son los siguientes:

- Permite diseñar y crear interfaces de conversación sofisticados a elección del desarrollador.
- Permite la centralización de solicitudes con integración prediseñada para soluciones de centros de contacto.
- Paga únicamente por las solicitudes que se hagan y no por cuotas mínimas.

En este caso se utilizaría Amazon Lex para servicio al cliente mediante un autoservicio usando agentes virtuales para la resolución de consultas de los clientes de una manera más rápida, serviría un enrutador de servicio inteligente para dirigir a los usuarios con el agente

o el área adecuada y para la productividad de la empresa al proporcionar respuestas a las preguntas más frecuentes que se tengan de Remedy o bien si se desea integrar a más servicios, se podrían proporcionar respuestas a preguntas frecuentes de soporte técnico, finanzas, etc.

4.3.3. Propuestas para el riesgo la empresa se queda sin servicios para atender solicitudes administrativas y de negocio, servicios financieros, servicios escolares y servicios de TI afectando la operatividad total.

Dado que mesa de servicio y centro de servicios compartidos son áreas centralizadas, la interrupción de su funcionamiento puede ocasionar retrasos en los procesos, lo que podría entorpecer las operaciones, generar pérdidas económicas e incluso afectar la imagen de la empresa.

4.3.3.1. Propuesta 1. Actualizar hardware y software de la plataforma de Mesa de Servicio.

Actualizar tanto los servidores como el software de Remedy permitiría que tanto los usuarios que realizan solicitudes como los usuarios que trabajan en las solicitudes, puedan operar mejor en el sistema.

Actualmente los sistemas de Remedy, han presentado problemas de lentitud en la plataforma, lo cual provoca una ineficiencia en la resolución de solicitudes para los Agentes de Mesa por lo que afecta al rendimiento del área de Mesa de Servicio, esto se debe a que el servidor que aloja al sistema se encuentra muy desactualizado. Este servidor es de una generación pasada que usa discos duros mecánicos lo cual provoca retrasos en la ejecución de las tareas del servidor y por ende afecta a la ejecución de Remedy por lo que es necesario implementar un nuevo servidor que aloje el sistema Remedy. En base a las normativas es que se tiene contemplado el mejoramiento de los dispositivos, se maneja que los dispositivos tengan una vida útil de por lo menos 5 años, pasado este periodo de tiempo es que se realizaran cambios, mantenimientos y/mejoras de hardware y software.

Se propone utilizar un servidor de nueva generación el cual utilice discos duros de estado sólido por los beneficios de velocidad y capacidad que estos ofrecen, a su vez, deben contar con procesadores diseñados para servidores, por la cantidad de solicitudes que Remedy llega a manejar.

Los dispositivos y software por el que se optó serían la mejora necesaria para alojar el sistema Remedy son:

Servidor ProLiant DL360 Gen10

Servidor en formato rack, diseñado para montarse en bastidores. Su diseño compacto y su capacidad para instalarse en racks lo hacen adecuado para entornos de centro de datos, proporciona seguridad, agilidad y flexibilidad sin afectar al rendimiento. Es compatible con los procesadores escalables Intel Xeon y aporta un aumento de rendimiento de hasta el 71 % y de un 27 % en núcleos. La tecnología HPE Silicon Root of Trust para proteger sus servidores de ataques, detectar posibles intrusiones y recuperar el firmware esencial de su servidor de forma segura. La recuperación segura permite al firmware del servidor regresar al último estado bueno conocido o a los ajustes de fábrica después de detectar código comprometido.

El servidor viene con un conjunto completo de servicios ofrecidos por HPE Pointnext, que ofrecen seguridad, reducen el riesgo y ayudan a los clientes a aprovechar la agilidad y la estabilidad. Los servicios de HPE Pointnext simplifican todas las fases del recorrido de la TI.

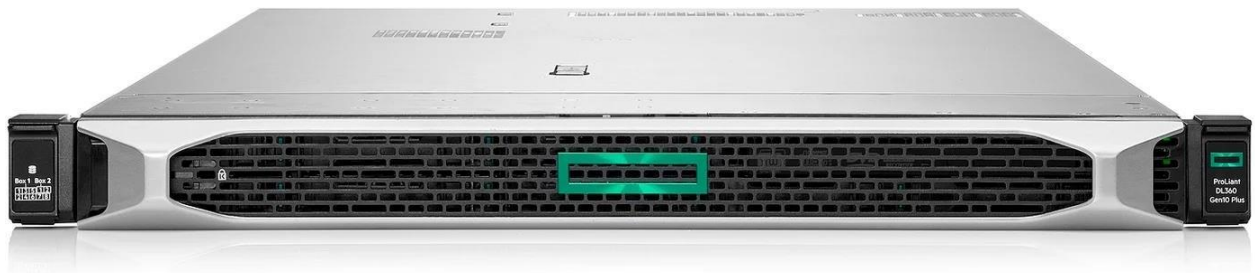


Figura 37. Ejemplo de servidor ProLiant DL360 Gen10.

(Hewlett Packard Enterprise).

Intel Xeon Gold 5218R

Es parte de la familia de procesadores Intel Xeon Escalable de segunda generación, se basa en la arquitectura x86-64. Está diseñado para servidores y estaciones de trabajo empresariales que requieren un rendimiento sólido y confiable.

Este procesador cuenta con 20 núcleos físicos y 40 hilos de ejecución gracias a la tecnología Hyper-Threading de Intel. Esto permite la ejecución simultánea de múltiples tareas y mejora la eficiencia del rendimiento en entornos multitarea. Ofrece soporte para memoria DDR4-2667, permitiendo configuraciones de memoria de alta capacidad y ancho de banda para manejar cargas de trabajo intensivas en datos.



Figura 38. Ejemplo de procesador Intel Xeon Gold 5218R.

(Intel, 2024).

Windows server 2019

Es el sistema operativo que tiende un puente entre los entornos locales y los servicios de Azure que activan los escenarios híbridos maximizando las inversiones existentes. Aumenta la seguridad y reduce el riesgo empresarial con múltiples capas de protección integradas en el sistema operativo. Haz que la infraestructura de tu centro de datos evolucione para conseguir una mayor eficiencia y mejora con una infraestructura hiperconvergente. Windows Server 2019 también te permite crear aplicaciones nativas de la nube y modernizar las más tradicionales con contenedores y microservicios.

Requisitos de hardware para Windows Server

1) Procesador

El rendimiento del procesador depende no solo de su frecuencia de reloj, sino también de su número de núcleos y tamaño de la caché.

Mínimo:

- Procesador de 64 bits a 1,4 GHz
- Compatible con el conjunto de instrucciones x64
- Admite DEP y NX
- Admite CMPXCHG16b, LAHF/SAHF y PrefetchW
- Admite la traducción de direcciones de segundo nivel (EPT o NPT)

2) RAM

Mínimo:

- 512 MB (2 GB para la opción de instalación Servidor con Experiencia de escritorio)
- Tipo ECC (código de corrección de errores) o tecnología similar para implementaciones de host físicos

Requisitos de espacio en disco y del controlador de almacenamiento

Los equipos que ejecutan Windows Server deben incluir un adaptador de almacenamiento que sea compatible con la especificación de arquitectura PCI Express. Los dispositivos de almacenamiento persistente en servidores clasificados como unidades de disco duro no deben ser PATA. Windows Server no admite ATA, PATA, IDE y EIDE para unidades de arranque, página o datos.

Mínimo: 32 GB

Requisitos del adaptador de red

Mínimo:

- Un adaptador Ethernet con un rendimiento de al menos 1 gigabit por segundo
- Compatible con la especificación de arquitectura PCI Express.

Un adaptador de red que admite la depuración de red es útil, pero no es un requisito mínimo.

Un adaptador de red que admite el entorno de ejecución previo al arranque es útil, pero no es un requisito mínimo.

4.3.3.2. Propuesta 2. Implementar los servicios de Cove Data Protection para la generación de respaldos.

Con el fin de reducir los tiempos de inactividad operativa total de Remedy, pérdida de información y evitar la realización de respaldos de manera manual, se propone la integración de un software que se encargue de realizar los respaldos de manera automática en los periodos de tiempo que la empresa desee y que dichos respaldos puedan ser almacenados en algún servidor auxiliar o bien en la nube.

N-ABLE es una empresa que ofrece el Cove Data Protection que brinda soluciones de respaldos y almacenamiento en la nube, de esta manera se puede llevar una gestión de los respaldos de manera segura y automáticamente.

Servicios que ofrece y ahorros al implementar Cove Data Protection

N-ABLE ofrece sus servicios dependiendo las necesidades de la empresa ofreciéndolos de manera completa o parcial con sus respectivos aumentos o disminuciones en los costos. Ofrece servicios de protección de servidores, protección de estancias de trabajo, protección de datos de Microsoft 365 junto con el almacenamiento en la nube, no requiere un dispositivo de tecnología exclusiva, no requiere almacenamiento local para copias de seguridad, pruebas de recuperación de manera automática, generación de archivos de seguridad y una recuperación flexible de la información.

Se estima que actualmente por los servicios de copias de seguridad actuales se puede estar pagando \$69,000 dólares anuales y al implementar estos servicios se calcula que se estaría pagando un total de \$21,000 dólares anualmente, obteniendo un ahorro de \$48,000 dólares anuales.

Beneficios de N-ABLE

Cove se encuentra en el cuadrante de líderes de G2 en el ámbito de copia de seguridad en línea para pequeñas empresas. Debido a que:

- Realiza copias de seguridad más frecuentes y de manera rápida, así como una reducción de su tamaño para aligerar el almacenamiento.
- Recuperación ante desastres de una manera más inteligente.
- Cuenta con un panel de control multiusuario unificado para que los encargados trabajen en una sola pantalla.
- Almacenamiento de las copias de seguridad en la nube privada del proveedor.
- Recuperación de sistemas ante desastres localmente, fuera de las instalaciones o en Microsoft Azure.
- Interfaz intuitiva y con vistas rápidas para optimizar el tiempo.
- Copias de seguridad de Microsoft 365 con soluciones integradas.
- Almacenamiento local opcional.

4.3.4. Propuestas para el riesgo la empresa atiende solicitudes administrativas y de negocio, servicios financieros, servicios escolares y servicios de TI operando inadecuadamente.

La detención total de las operaciones de mesa de servicio y centro de servicios compartidos puede causar afectaciones graves. También, la generación de solicitudes en categorías incorrectas o mal especificadas también tiene el potencial de retrasar el funcionamiento de la empresa, afectando la eficiencia operativa.

4.3.4.1. Propuesta 1. Informar a los alumnos del uso de la aplicación de Mesa de Servicio.

Informar a los estudiantes acerca de cómo pueden incorporarse al sistema Remedy y como es que funciona este sistema ayudando a que los alumnos conozcan a detalle los servicios, atenciones y tramites que Mesa de Servicio les puede brindar a través de Remedy, también ayudaría a que los alumnos sean capaces de realizar las solicitudes de manera adecuada y mitigar repeticiones de estas o problemas de especificación en los servicios que los alumnos requieren. Una forma de asegurarse de que los alumnos comprendieron el funcionamiento de Remedy y el proceso a seguir, podría hacerse mediante una evaluación que podría generarse de forma gratuita por medio de los formularios de Google.

Tabla 36. Descripción detallada del proceso de capacitación de estudiantes del uso de Remedy.

(Fuente: Elaboración propia).

No.	Encargados.	Descripción de la actividad.
1	Mesa de Servicio	Genera un video tutorial del proceso a seguir para que los alumnos generen su alta en Mesa de Servicio junto con una explicación de cómo pueden realizar solicitudes de problemas de TI, problemas escolares y problemas financieros, cada uno con un submenú con diferentes peticiones.
2	Mentores	Distribuye a los alumnos el video tutorial y una evaluación para que los estudiantes demuestren que comprendieron el proceso y las funcionalidades de Remedy.
3	Alumnos	Revisan el video y realizan la evaluación referente al manejo de Remedy, si el alumno no aprueba la evaluación, no podrá realizar su alta y tendrá que realizar la evaluación nuevamente.
4	Mentores	Proporcionan los medios necesarios para que los alumnos puedan realizar su alta en Mesa de Servicio y tengan acceso a Remedy.
5	Alumnos	Realizan su solicitud de alta de usuario de Mesa de Servicio colocando información como su ID, nombre y si necesita realizar algún tipo de trámite y la envían a Mesa de Servicio
6	Mesa de Servicio	Reciben la solicitud de alta de usuario en Mesa de Servicio.
7	Mesa de Servicio	Se asegura de que el solicitante se encuentre activo en el sistema y genera el usuario.
8	Mesa de servicio	Notifica al alumno de que su usuario esta creado.

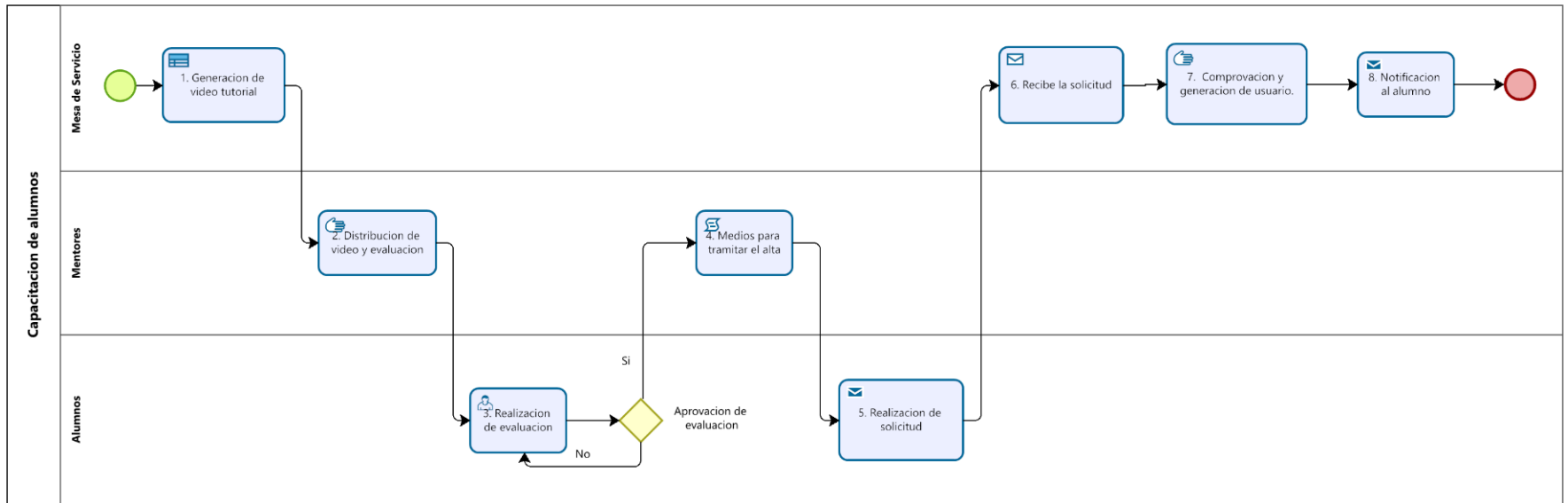


Figura 39. Diagrama de proceso para la capacitación de alumnos del registro y uso de Remedy.

(Fuente: Elaboración propia).

4.3.4.2. Propuesta 2. Capacitar al personal administrativo del uso de la plataforma Remedy.

Invertir en la capacitación y evaluación de aptitudes a los usuarios administrativos que interactúan constante mente con el sistema Remedy para que estos, sean capaces de comprender el funcionamiento y manejo de este sistema, así se evitaría la duplicidad de peticiones y un mal manejo o especificación de peticiones. Una manera gratuita de realizar una evaluación seria mediante los formularios de Google.

Tabla 37. Procesos para la capacitación de administrativos.

(Fuente: Elaboración propia).

No.	Puesto u/o sistema	Descripción de la actividad.
1	Directivos	Planean la implementación de nuevas funcionalidades al sistema Remedy que afecta a administrativos y docentes.
2	Infraestructura Tecnológica y Seguridad Aliat	Genera un video tutorial de las funcionalidades que tiene Remedy o que se implementaran, se realizan los videos correspondientes a las vistas e interacciones que pueden tener los diferentes usuarios, debido a que no todos los usuarios pueden llegar a interactuar de la misma forma con el sistema.
3	Mesa de servicio	Notifica de manera masiva a aquellos trabajadores o clientes a los cuales les afectaran las nuevas funcionalidades.
4	Directivos	Realizan pruebas al personal administrativo para asegurar que comprenden y dominan el funcionamiento del nuevo sistema o funcionalidades.
5	Mesa de servicio	Anuncia a los trabajadores o clientes que se realizara la ventana de mantenimiento para la integración o actualización de las nuevas funcionalidades en repetidas ocasiones.
6	Infraestructura Tecnológica y Seguridad Aliat	Realiza el mantenimiento o integración en los periodos de tiempo definidos, según la planeación establecida.

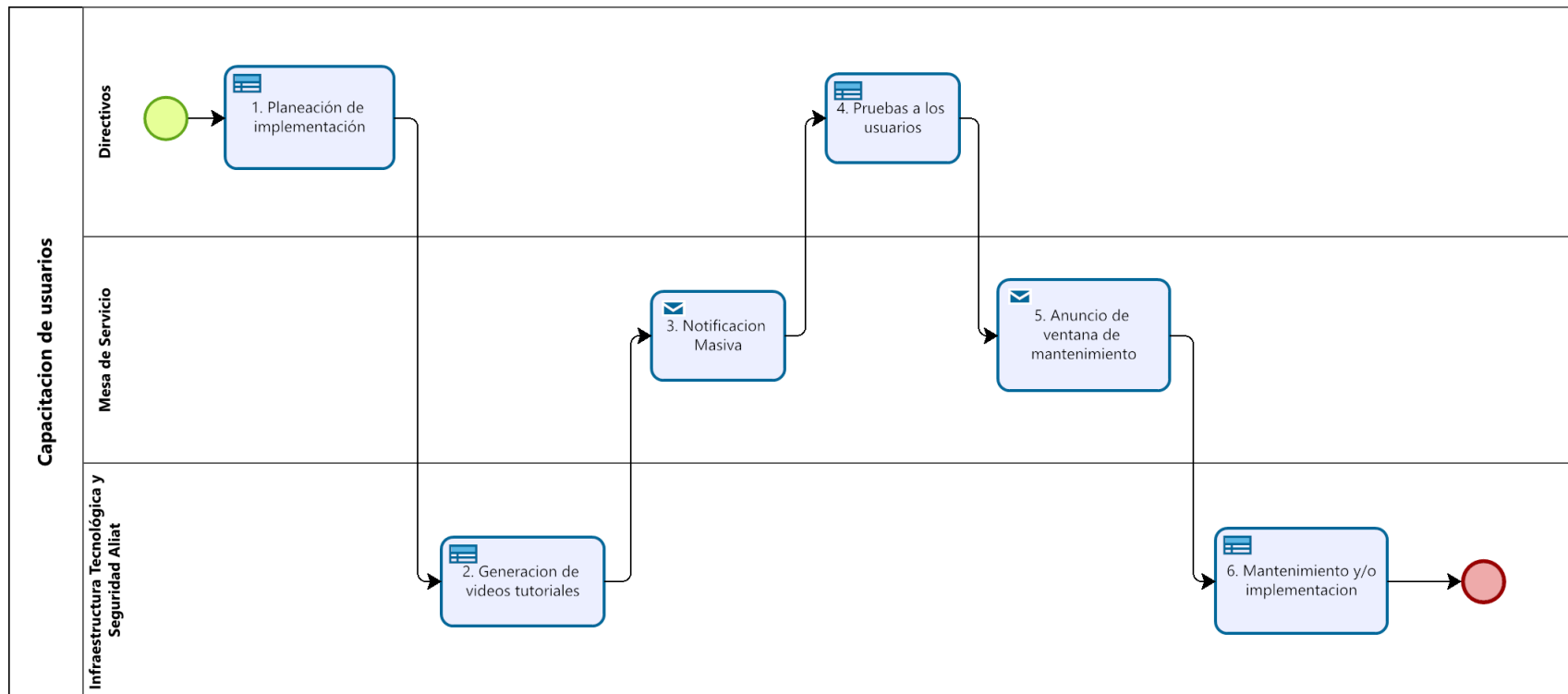


Figura 40. Diagrama de proceso para la capacitación de administrativos

(Fuente: Elaboración propia).

4.3.5. Propuestas para el riesgo pérdida y/o robo de información.

La información es uno de los recursos intangibles más valiosos para cualquier organización, por lo que garantizar la protección de datos confidenciales y prevenir su divulgación indebida debe ser una prioridad para las empresas.

4.3.5.1. Propuesta 1. Implementar los servicios de TERAMIND para el control de empleados.

Implementación de un software que monitoree de manera interna los equipos de los trabajadores y prevenga amenazas internas, esto permitiría llevar un mayor control en los equipos que la empresa proporciona a sus empleados.

La propuesta para ejercer este control en los equipos de los usuarios es TERAMIND el cual es un software que ayuda al monitoreo de empleados y detección de amenazas internas que puedan ser ocasionadas por los empleados en tiempo real, así como una graficación de la productividad que los empleados demuestran. Ofrece sus servicios en la nube o de manera local dependiendo las necesidades o soluciones que la empresa requiera, a su vez permite grabar sesiones en tiempo real de los empleados y exportar dichas grabaciones, permite tener accesos remotos de los equipos de los empleados, permite generar reportes de casi todas las actividades que realizan los empleados o en las que pudieron haber participado, incluyendo aplicaciones y sitios web visitados, reportes sobre correos electrónicos, infracciones a normas o políticas, entre otras muchas otras funcionalidades de control.

Servicios que ofrece TERAMIND.



Figura 41. Servicios ofrecidos por TERAMIND.

(TERAMIND, 2024).

- Registra y monitorea toda la actividad de los empleados en tiempo real, previniendo el uso negligente e indebido de los equipos a fin de hacer cumplir las políticas de la empresa.
- Limita los daños ocasionados por los usuarios malintencionados y negligentes que pueden suceder dentro de la organización. Combina DLP (Data Loss Prevention o prevención de pérdida de datos) y análisis del comportamiento del usuario para ofrecer conocimientos incomparables y capacidades de intervención de actividades maliciosas.
- Permite monitorear el rendimiento de los trabajadores para optimizar el esfuerzo laboral. Brinda información y permitirle controlar cuánto tiempo pueden dedicar a cada actividad.
- Prevención de pérdida de datos avanzado basado en contenido en archivos, portapapeles, correos electrónicos, mensajes instantáneos, documentos impresos e incluso lo que el usuario ve en su pantalla basado en comportamiento y contenido.

Ejemplificación de las funcionalidades que TERAMIND ofrece.

En este ejemplo de la visualización de empleados muestra si el empleado se encuentra activo, el equipo que se le asignó al empleado, la tarea más recurrente a la que accede el empleado y la actividad que está desempeñando en tiempo real junto con los tiempos. De esta forma se puede determinar si los empleados desempeñan las actividades que le corresponden y si se encuentran trabajando en sus horarios correspondientes lo anterior se ejemplifica en la figura 42.

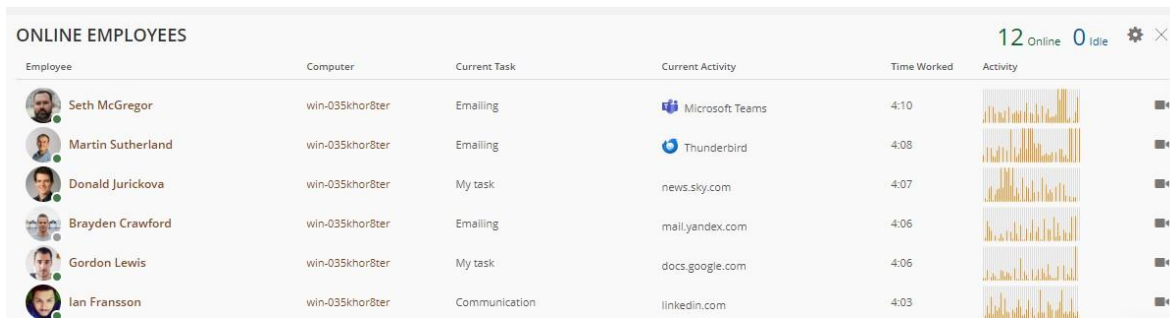


Figura 42. Ejemplo de visualización de empleados de TERAMIND.

(TERAMIND, 2024).

Este apartado es el ejemplo de la generación de reportes BI que es posible generar, permite realizar filtrados dependiendo de la información que se desee conocer como por ejemplo los sitios web más visitados, aplicaciones más utilizadas, horas de actividad de los empleados, desempeño de los empleados y mucho más, lo anterior se ejemplifica en las figuras 43,44 y 45.



Figura 43. Ejemplo de reportes de aplicaciones y sitios web.

(TERAMIND, 2024)

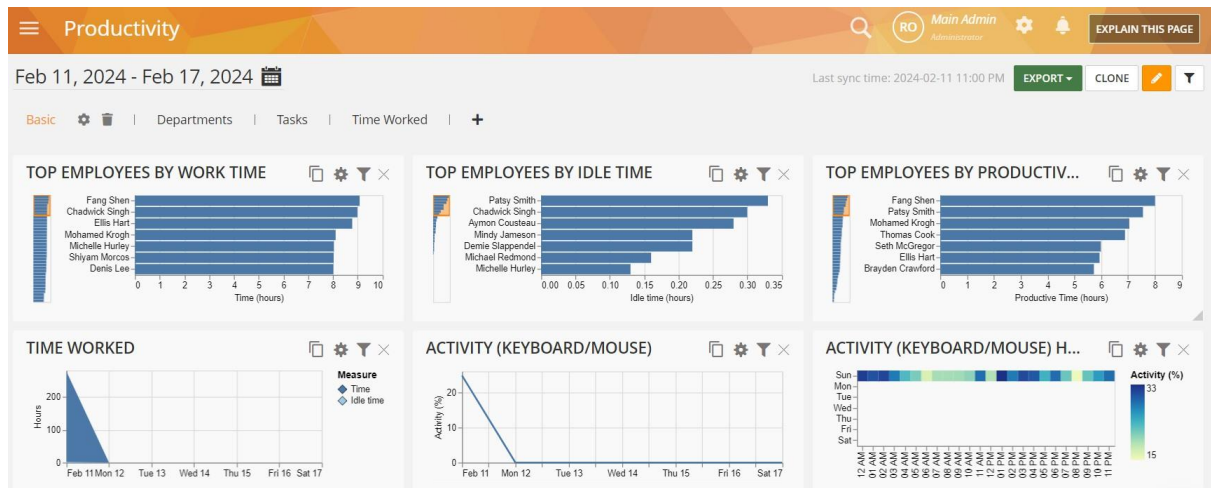


Figura 44. Ejemplo de reportes de aplicaciones y sitios web.

(TERAMIND, 2024)

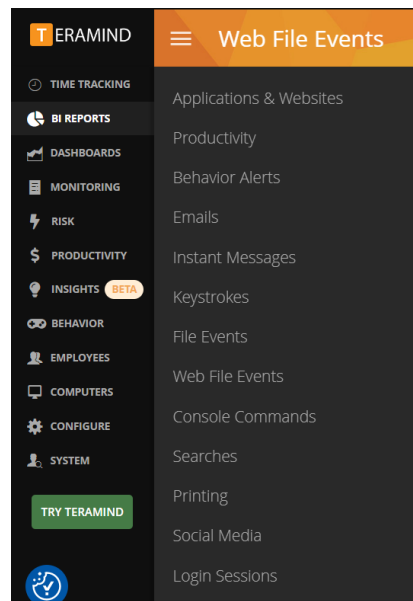


Figura 45. Ejemplo de más tipos de reportes.

(TERAMIND, 2024)

TERAMIND también permite graficar el desempeño de la empresa o bien por empleado, por ejemplo, de manera general al mes contabilizando las horas laboradas, el nivel de actividad por empleado, etc.

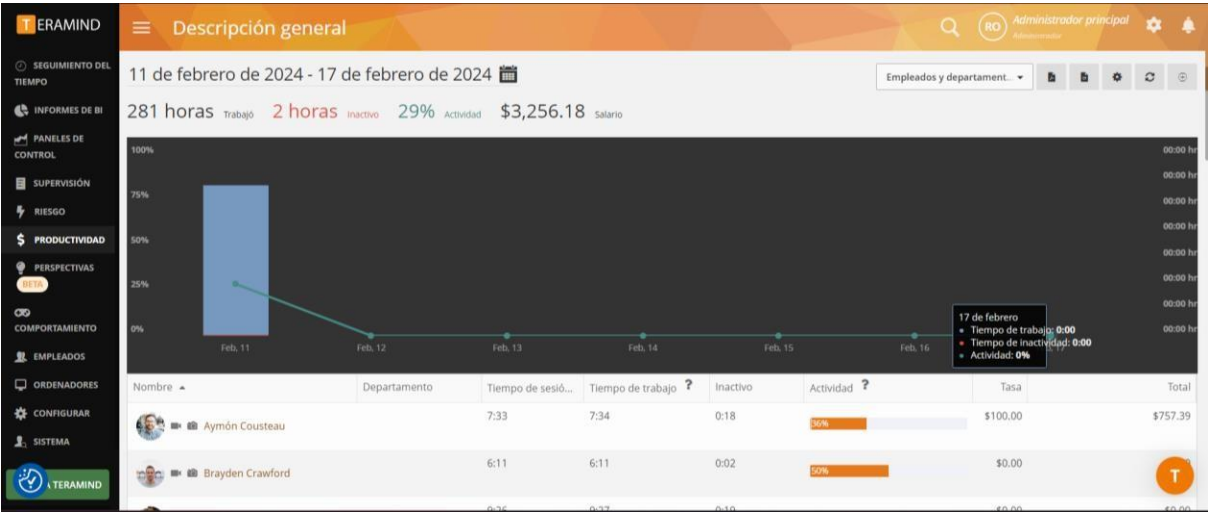


Figura 46. Ejemplo de descripción general de la productividad.

(TERAMIND, 2024)

CONCLUSIONES

Para culminar este proyecto, la investigación, planeación estructuración, evaluación y emisión de resultados del análisis de riesgos permitieron denotar las virtudes y defectos del área y los sistemas evaluados lo cual es un punto de vista adicional al denotar las carencias de la empresa.

Se evaluó que en Red Univercom hablando específicamente de Mesa de Servicio Aliat, al ser un área creada reciente mente en Aliat, muchas de las funcionalidades y labores que ejercen, pueden ser modificados y readaptados a las necesidades que surgen en la empresa, esto quiere decir que muchas de las tareas que ejercen los empleados pueden cambiar o se pueden readaptar a las funciones que agregue la empresa, sin embargo al carecer de un manual y un reglamento específico de Mesa de Servicio muchas de sus funcionalidades, personal y servicios no se encuentran limitados o estrictamente reforzados por una normas que limiten a los trabajadores y a su vez no esclarece la meta del área a sus trabajadores.

Al mismo tiempo de que Mesa de Servicio se estableció en Aliat, se incorporó un sistema que permitiera gestionar solicitudes de Administrativos y estudiantes en cuestiones de servicios Administrativos, servicios Financieros, Servicios Escolares y servicios de TI de manera centralizada para brindar una mayor atención, control y manejo de la información, sin embargo, por el tiempo y el tipo de tecnologías donde se almacenaba anteriormente el sistema, es que se optó por una actualización de los servidores donde se alojaban, a su vez se utilizó un sistema operativo más actual para mayor seguridad del sistema, y así mejorar el rendimiento y agilizar al sistema tanto para los usuarios solicitantes como para el personal administrativo que operaba con el sistema.

Debido al crecimiento de la empresa a nivel nacional y a la falta de limpieza en los servicios de software que son proporcionados por proveedores, específicamente hablando de los servicios de correo Outlook 365, muchas de los demás servicios se ven afectados a la falta de usuarios de O365 para los estudiantes, los cuales son los usuarios más numerosos que ocupan este servicio, debido a esto, la imagen de Mesa y de Aliat se puede afectar al no brindar un servicio educativo adecuado y careciente de Tecnologías de la información.

COMPETENCIAS DESARROLLADAS

Fundamentos de investigación

Competencia:

1. Aplica los elementos de la investigación documental para elaborar escritos académicos de su entorno profesional.

Esta competencia se utilizó para realizar la investigación pertinente de información referente a la empresa, leyes, normas y guías, servicios y las soluciones propuestas, permitiendo el desarrollo de un proyecto más profesional y orientado al ámbito laboral.

Administración de la Función Informática

Competencia:

1. Manejo de los fundamentos teóricos de seguridad informática para su aplicación en casos prácticos.

Esta competencia permitió que en base a los conceptos que se tienen de la seguridad informática, se realizaran las propuestas más a fines y que brindaran la mayor seguridad posible.

2. Uso e interpretación de los lineamientos, estándares y marcos referenciales que complementen el conocimiento de la asignatura.

Esta competencia se utilizó a la hora de investigar y basar el proyecto a las normas y guías más afines a los objetivos de la empresa o bien a que el proyecto se orientara a los reglamentos a los que la empresa es a fin.

4. Proponer medidas de seguridad basadas en lineamientos y estándares actuales.

Esta parte permitió que las propuestas y soluciones a las problemáticas estuvieran alineadas a la normativa interna de la empresa y a los estándares y guías con los que trabaja la empresa.

Auditoria Informática de Desarrollo de Proyectos y Aplicaciones

Competencia:

1. Identifica interpretación y uso de lineamientos, estándares, marcos referenciales, técnicas y otros conceptos que complementen la unión del conocimiento para la posterior aplicación de la Auditoría informática.

Esta competencia permitió realizar el proyecto en base a como se debe llevar a cabo un análisis de riesgo y a seguir las sugerencias que las normativas proponen para asegurar los equipos o que en el caso de las guías conservar el valor en la atención y los servicios.

FUENTES DE INFORMACIÓN

- Amazon Web Services. (s.f.). *AWS*. Amazon Web Services. <https://aws.amazon.com/es/lex/?p=ft&c=ai&z=4>.
- Ayala Soto, A. B. (2023, abril). *Facultad de Ingeniería y Arquitectura: Escuela Profesional de Ingeniería de Sistemas*. Universidad Autónoma del Perú. <https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/2517/Ayala%20Soto%2C%20A.%20B.%2C%20%26%20Caso%20Rojas%2C%20C.%20A..pdf?sequence=1&isAllowed=y>.
- BMC Software, Inc. (2024). Remedy IT Service Management (ITSM). Recuperado de <https://www.bmc.com/it-solutions/remedy-itsm.html>
- Caballero, S. D. (2021). *Análisis y gestión de riesgo en proyectos software*. Universidad Nacional de Misiones, Facultad de Ciencias Exactas, Químicas y Naturales. https://www.fceqyn.unam.edu.ar/mti/wp-content/uploads/TFM_CaballeroSergio.pdf.
- Financial Crime Academy. (2024, julio 11). Metodología de clasificación de riesgos: Contenido de la evaluación de la probabilidad y el impacto en 2022. <https://financialcrimeacademy.org/es/metodologia-de-clasificacion-de-riesgos-contenido-de-la-evaluacion-de-la-probabilidad-y-el-impacto-en-2022/>
- Hernández Echeverría, A. E. (2021, junio 16). *Propuesta para el mejoramiento de procesos y gestión de riesgos TI del área programación y control de la compañía EMTELCO S.A.S., basada en las buenas prácticas de ITIL 4 y COBIT 2019*. Universidad Santo Tomás, Facultad de Ingeniería de Telecomunicaciones, Bogotá, D.C. <https://repository.usta.edu.co/bitstream/handle/11634/34928/2021andreshernandez.pdf?sequence=1>.
- Hewlett Packard Enterprise. (2019). *HPE ProLiant DL360 Gen10 Server*. Hewlett Packard Enterprise. <https://www.intesiscon.com/ficheros/manuales-tecnicos/174-especificaciones-tnicas-HPE-ProLiant-DL360-Gen10-Server.pdf>.
- IBM. (s.f.). *¿Qué es ITSM?* IBM Cloud. <https://www.ibm.com/mx-es/topics/it-service-management#:~:text=el%20siguiente%20paso-,%C2%BFQu%C3%A9%20es%20ITSM%3F,objetivos%20establecidos%20por%20la%20empresa>.
- Intel. (s.f.). *Intel Xeon Gold 5218R Processor: Specifications*. Intel. <https://www.intel.la/content/www/xl/es/products/sku/199342/intel-xeon-gold-5218r-processor-27-5m-cache-2-10-ghz/specifications.html>.
- International Organization for Standardization. (2015). ISO 9001:2015 (es): Sistemas de gestión de la calidad. <https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:es>
- ITIL México. (s. f.). ITIL México. Recuperado el 6 de noviembre de 2024, de <https://www.itil.com.mx/>

- ISACA. (2012). *COBIT 5*. ISACA.
- JTC 1, Comité Técnico Conjunto ISO/IEC. (2005). *ISO/IEC 27002:2005—Code of practice for information security controls*. ISO/IEC.
- AXELOS Limited. (2019). *ITIL 4 foundation*. AXELOS Limited.
- López Goytia, J. L., Peña Alfaro, E. M., & Zarco Istiga, A. L. (2019, diciembre 17). *Propuesta de mejora basada en el marco ITIL para la atención de tickets del proceso de administración de incidentes en una empresa proveedora de equipos médicos* (Tesis de maestría). Instituto Politécnico Nacional. <https://tesis.ipn.mx/bitstream/handle/123456789/27930/PROPUESTA%20DE%20MEJORA%20BASADA%20EN%20EL%20MARCO%20ITIL%2C%20PARA%20LA%20ATENCI%C3%93N%20DE%20TICKETS%20DEL%20PROCESO%20DE%20ADMINISTRACI%C3%93N%20DE%20INCIDENTES%20EN%20UNA%20EMPRESA%20PROVEEDORA%20>.
- Microsoft. (s.f.). *Evaluate Windows Server 2019*. Microsoft. <https://www.microsoft.com/es-es/evalcenter/evaluate-windows-server-2019>.
- Microsoft Azure. (2024). *Azure*. Microsoft Azure. <https://azure.microsoft.com/>
- Muñoz Martínez, C., & Prieto de Diego, J. (2016). Programa modular en logística, transporte, cadena de suministro, dirección de operaciones y proyectos: Módulo 13: Procesos operativos y auditorías de proyectos. Editorial Sanz y Torres.
- N-ABLE. (2024). *Backup trial*. N-ABLE. <https://www.n-able.com/es/lp/backup-trial>.
- Oracle Corporation. (2024). Gestión del Capital Humano (HCM) en la Nube de Oracle. Oracle. Recuperado el 6 de noviembre de 2024, de <https://www.oracle.com/mx/human-capital-management/>
- Oracle Corporation. (2024). PeopleSoft Campus Solutions: Key Features and Benefits. Recuperado el 6 de noviembre de 2024, de https://docs.oracle.com/cd/E52319_01/infoportal/cs.html#tab3
- Red Univercom. (2020, abril 2). *Mesa de ayuda*. Aliat Universidades. <http://aliat.org.mx/kosmo/mesa-de-ayuda/>.
- Secretaría de Gobernación (SEGOB). (1992, octubre 3). *Diario Oficial de la Federación*. https://dof.gob.mx/nota_detalle.php?codigo=4655028&fecha=10/03/1992#gsc.tab=0.
- Team Asana. (2024, febrero 3). Cómo realizar un análisis de riesgos y ejemplos. Asana. <https://asana.com/es/resources/project-risks>
- Teramind. (2024). *Teramind*. Democompany. <https://democompany.teramind.co/>.
- TZALOA. (2023). *Las cuatro dimensiones*. TZALOA. <https://tzaloea.com/courses/itil-v4-foundation/lessons/las-cuatro-dimensiones-2/>

ANEXOS

ANEXO 1. Descripción de puesto del agente de mesa.

Datos de Identificación

Nombre del puesto	Agente Mesa de Servicio
Empresa	Red Univercom
Área	CEAS – On Aliat
Nombre del jefe inmediato	Pedro Joaquín Paredes Talavera
Puesto del jefe inmediato	Gerente de Servicios
Fecha de elaboración	01/05/2020
Nombre de quien elabora este formato	
Puesto de quien elabora este formato	
Centro de costos	3150 - 4190

Descripción del Puesto

1. *Propósito básico del puesto*

Indicar la razón principal de existir o contribución del puesto a la organización. Redactar de la siguiente manera: ¿Qué hace?, ¿Dónde lo hace?, ¿De acuerdo con qué? y ¿Para qué lo hace?

Brindar atención vía telefónica y/o remota a los usuarios del segmento administrativo sobre los reportes de tecnología y/o servicios de negocio proporcionando atención de primer nivel, basados en procedimientos relevados con anterioridad para resoluciones en primera instancia.

2. *Funciones principales*

El ocupante de este puesto debe tener diversas funciones dirigidas a producir determinados resultados finales, agregue las que considere necesarias. Redactar cada función de la siguiente manera: ¿Qué hace?, ¿Dónde lo hace? y ¿Para qué lo hace?

1. Brindar atención a reportes vía telefónica.
2. Atender reportes mediante las herramientas de gestión de tickets (incidencias/requerimientos), asignado un folio al incidente y manteniendo al usuario informado del estatus del ticket que se han generado en su nombre.
3. Mantener al usuario informado de los cambios tecnológicos.
4. Dar seguimiento al incidente hasta su solución final.

5. Verificar el estatus del reporte de usuario con el área/departamento al que fue asignado.
6. Asignar el incidente al siguiente nivel de atención.
7. Documentar el problema.
8. Interpretar y documentar a nivel técnico el reporte del incidente para poder escalarlo al siguiente nivel, llevando a cabo todo lo necesario para cumplir con procedimientos y políticas del área de informática.
9. Aplicación de encuesta en línea al momento de la resolución del reporte de servicio.
10. Registrar en la herramienta de gestión de incidencias las calificaciones y comentarios que se otorgaron por parte de los usuarios.

3. Distribución de tiempos

El ocupante de este puesto debe dedicar un tiempo determinado a cada una de sus actividades. Defina la manera en que estos tiempos se distribuyen. Redactar la función y el porcentaje de tiempo que le dedica sobre una base mensual.

Función	Tiempo destinado a la actividad (%)
1. Atención de reportes vía herramientas de gestión de tickets (incidencias/requerimientos).	50
2. Registrar los incidentes reportados, a través de la herramienta de gestión de incidencias.	30
3. Gestión con los usuarios para interpretación y documentación de reportes para el siguiente de nivel de resolución de incidentes.	10
4. Documentar y llevar a cabo todo lo necesario para cumplir con procedimientos y políticas del área de informática.	10
Total, de tiempo destinado a funciones mensuales	100

4. Entorno

a. El puesto trabaja en función de:

(Marque con "x" máximo dos opciones)

X	Instrucciones claras	X	Objetivos a corto plazo
X	Rutinas e instrucciones establecidas	X	Objetivos a mediano plazo
X	Programa de trabajo		Objetivos a largo plazo
	Otro (explicar):		

b. Toma de decisiones:

Mencione las decisiones más importantes o relevantes que pueda tomar el puesto, sin necesidad de aprobación.

1. Sin toma de decisiones.
2.
3.

c. Retos del puesto:

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Mencione los tres principales desafíos o retos a los que se enfrenta el puesto.

1.-Resolver el 90% de los reportes de los usuarios que puedan ser solucionados por el primer nivel de soporte, en caso de poder ser resueltos.

2.- Mantener al usuario informado del estatus del ticket que se han generado en su nombre.

d. Relaciones internas (Contacto interpersonal)

Mencione las cuatro más importantes o relevantes, especifique el puesto, área y la razón principal del contacto.

Puesto / Área	¿Para qué?
Usuarios Administrativos Campus	Resolver los reportes de los usuarios que puedan ser solucionados por el primer nivel de soporte, en caso de poder ser resueltos.
	Mantener al usuario informado del estatus del ticket que se han generado en su nombre.
Usuarios Corporativo	Resolver los reportes de los usuarios que puedan ser solucionados por el primer nivel de soporte, en caso de poder ser resueltos.
	Mantener al usuario informado del estatus del ticket que se han generado en su nombre.
Personal de CSC	Asignación de incidente al siguiente nivel de atención.
Personal de TI	Asignación de incidente al siguiente nivel de atención.

e. Relaciones externas

Mencione las cuatro más importantes o relevantes, especifique el puesto, área y la razón principal del contacto.

Puesto / Área	¿Para qué?

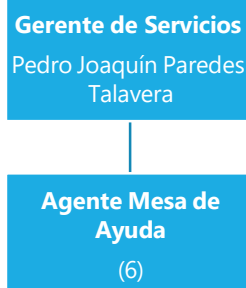
5. Manejo de recursos (Dimensiones)

Las cifras más importantes para el año en curso, expresadas en pesos anuales, sobre las cuales el puesto tiene influencia directa (ejemplo: volumen de ingresos, captación, compras, gastos de servicio que el puesto controla o cualquier otro valor monetario significativo). O bien, cantidad de recursos no monetarios (ejemplo: número de proveedores, usuarios, oficinas, etc.).

Concepto	(\$, %, N °)

6. Organigrama del puesto (ubicación en la estructura organizacional)

Señalar nombre y puesto del jefe, así como subordinados directos (ejemplo gráfico).



Perfil del Puesto

Considerar el perfil del puesto, no del ocupante. Marque con una "x".

1. Características personales

ESCOLARIDAD			
	Estudiante		Trunca
X	Carrera Técnica	X	Pasante
	Maestría	X	Licenciatura
	Otro (explicar):		

ÁREAS DE ESCOLARIDAD			
	Abogado	X	Finanzas
X	Administración		Ingeniería
	Actuario		Ingeniería Industrial
	Comunicación		Medicina
	Contaduría	X	Sistemas
	Economía		Telecomunicaciones

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

	Otros (especifique):	
--	----------------------	--

MANEJO DE PC							
X	Word	X	Excel	X	PowerPoint	X	Outlook
X	Otros (especifique):	Herramientas de Gestión de Incidencias o ITSM ejemplo (OSTicket; Remedy Footprint; etc.)					

IDIOMAS			
Idioma:	Inglés	Porcentaje:	No necesario X
Otros (especifique):			

EXPERIENCIA	
Años	Área
2	Soporte Técnico; HelpDesk

2. Otros requerimientos

Señalar algún requerimiento específico del perfil del puesto (certificaciones, trabajo por turnos, necesidad de viajar, automóvil, etc.).

Contar con actitud de servicio, tolerancia a la frustración.

Indicadores de desempeño y competencias

1. Indicadores de desempeño

Nombre	Unidad de medida
En definición con la Dirección de CSC y TI	

2. Competencias

Competencias genéricas	Grado				
	1 Ausencia	2 Básico	3 Dominio	4 Avanzado	5 Experto
Servicio al cliente			X		
Liderazgo			X		
Trabajo en equipo			X		
Orientación a resultados			X		
Apertura al cambio			X		
Planeación, organización y control		X			
Solución de problemas			X		
Comunicación asertiva			X		
Trabajo bajo presión			X		

(Red Univercom, 2020)

ANEXO 2. Política seguridad de la información.

[...]6.1 De la Generalidades

6.1.1 La Red Aliat Universidades, está convencida que un elemento fundamental para cumplir con la misión y los objetivos estratégicos de negocio, es garantizar la entrega y prestación de sus servicios a través de la generación de valor para sus usuarios, por medio de procesos que permitan regular el ciclo de vida del servicio (diseño, transición, entrega y mejora del mismo), así como la reducción de riesgos, que pudieran afectar la integridad, confidencialidad y disponibilidad de la información o la dispuesta bajo su custodia por la naturaleza de sus actividades.

6.1.2 Se debe proteger la información contra daños, alteración, difusión o pérdida, de acuerdo con su confidencialidad, valor y criticidad.

6.1.3 El área de TI es responsable de realizar respaldos de la información contenida en los sistemas de Aliat, y salvaguardarlos, por el tiempo requerido de acuerdo con las políticas de conservación de información histórica de cada área.

6.1.4 Todos los colaboradores son responsables de respaldar y conservar su información en los diferentes medios oficiales que le sean facilitados por la institución, actualmente se cuenta para ello la suite de Microsoft Office 365.

6.1.6 La Red Aliat Universidades opera bajo un entorno normativo de seguridad de la información, alineado a las políticas corporativas, a los objetivos estratégicos, requerimientos de la organización, a las leyes y regulaciones locales y federales, prevalecientes en la región donde se ubique.

6.1.7 Todo el personal debe leer y alinearse a las políticas y procedimientos, que les serán administrados a través de una estructura organizacional que soporta y mantiene requisitos de seguridad de la información, acorde a las necesidades de la organización.

6.1.8 Todos los empleados de planta, temporales, de nuevo ingreso y todos aquellos que hayan tenido un cambio significativo en sus responsabilidades recibirán periódicamente concientización, capacitación o entrenamiento, relacionado a la seguridad de la información.

6.1.9 Toda la documentación referente a la Seguridad de la Información de la Red Aliat Universidades, inclusive (sin limitación), las políticas, normas y procedimientos, debe ser clasificada como "Interna", a menos que haya sido expresamente creada para ser utilizada para procesos de negocios externos o por socios.

6.1.10 La Red Aliat Universidades se reserva el derecho de revocar los privilegios sobre el uso de la tecnología para el procesamiento de la información a cualquier usuario que haga mal uso de esta.

[...]

(Aliat Universidades, 2023)

ANEXO 3. Política control de accesos.

[...]

6.1 De las generalidades de Control de Accesos

6.1.1 Deben establecerse y mantenerse controles de acceso con el fin de no permitir accesos no autorizados y preservar la confidencialidad, integridad y disponibilidad de la información.

6.1.2 Los perfiles de puesto deberán ser definidos por los directores de área en conjunto con Capital Humano, con el visto bueno del responsable de Seguridad TI.

[...]

6.1.4 El responsable de Seguridad TI deberá asegurar que cualquier sistema que maneje información ya sea crítica o sensible, haga uso de un control de acceso basado en contraseña.

6.1.5 El acceso y los privilegios a las aplicaciones, bases de datos, sistemas operativos y componentes de red, serán restringidos con base en el perfil de cada usuario y en ninguna circunstancia podrán ser alterados o rebasados.

6.1.6 Los usuarios deberán ser únicos e intransferibles, no está permitido el uso de cuentas genéricas. En caso de identificarse este tipo de cuentas, deberán determinarse las acciones a realizar para que sean eliminadas.

6.1.7 Se deberá limitar el uso de las cuentas de servicio, la creación de estas deberá estar debidamente justificada, además de tener un responsable asignado (persona que solicita la creación de la cuenta) y cumplir con los lineamientos de creación de contraseña descritos en la presente política, además se deben conceder dichas cuentas solo los derechos y permisos necesarios para ejecutar su servicio.

6.1.8 En caso de que la persona responsable de la cuenta de servicio sea dada de baja o cambie sus actividades en Aliat Universidades, el director del área deberá asignar a una persona responsable y se deberá realizar el cambio de la contraseña, coordinando los cambios para minimizar el tiempo de inactividad del servicio.

6.1.9 Al momento de crear una cuenta de usuario, se deberá considerar el primer nombre, seguido de un “.” y primer apellido, para generar el identificador de dicha cuenta, en los sistemas que lo permitan. En caso de que el nombre de usuario se repita, se deberá tomar en cuenta la primera letra del segundo apellido.

6.1.10 Las cuentas de acceso son de carácter personal e intransferible y es responsabilidad del usuario garantizar que es el único que conoce las contraseñas para utilizar dichas cuentas de acceso, por lo tanto, toda actividad realizada con las cuentas de acceso es responsabilidad del usuario al que pertenecen.

6.2 De la gestión de altas, bajas, cambios en los accesos de usuarios

6.2.1 El alta, baja o cambio de usuarios en los sistemas de Aliat deberá realizarse de acuerdo con lo indicado en el proceso [ABC de cuentas de usuario](#).

6.2.2 Toda alta, baja o cambio en los accesos de recursos tecnológicos y a la información misma de la organización, deberá realizarse formalmente mediante correo electrónico el cual puede ser solicitado por el área de Capital Humano o en su defecto por el Gerente de área o Rector.

6.2.3 Tanto las altas, bajas o cambios a las cuentas de usuarios, deben ser ejecutadas con base a las necesidades y aprobación de estos, no se procederá a realizar ningún alta, cambio y/o baja de acceso sin la solicitud correspondiente y la previa autorización del Gerente de área.

6.2.4 El director de Tecnologías de Información deberá asegurar que el personal a su cargo autentifique la identidad del usuario, cada vez que se asigne una nueva cuenta, así como la necesidad real de la existencia, para algún proceso de la organización.

6.2.5 El usuario solicitante del acceso entiende y es consciente que toda inactividad superior a noventa (90) días, produce una revocación automática de todos los privilegios de su identificador de usuario.

6.2.6 La Red Aliat Universidades se reserva el derecho de revocar los privilegios sobre el uso de la tecnología para el procesamiento de la información a cualquier usuario que haga mal uso de esta.

6.2.7 El responsable de Seguridad TI, en conjunto con el área de Control Interno deberá realizar recertificaciones de usuarios de los sistemas de ALIAT Universidades al menos una vez al año [...].

6.2.8 Se deberán considerar como obligatorios los siguientes aspectos al momento de revisar/validar los usuarios y perfiles de acceso registrados:

- Cambio de puesto de los usuarios registrados, por lo cual realizan nuevas responsabilidades en la que se desempeña o que se le atribuyen nuevas funcionalidades en los sistemas dentro de su mismo puesto de trabajo.
- Bajas de personal de la organización.
- Nuevas funcionalidades y/o roles en el sistema por cambios en la operación.
- Usuarios con acceso al sistema validando si el perfil que tienen asignado coincide con las funciones laborales que realizan.

6.2.9 El responsable de Seguridad TI establece fechas de vencimiento a máximo una (1) semana y bloqueo automático para todos los identificadores de usuario almacenados en los sistemas de Aliat, que producto de una auditoría, no haya sido posible identificar una Solicitud para la gestión de accesos (FO-TI-01) asociada.

6.2.10 El responsable de Seguridad TI deberá asegurar que todos los usuarios y sus actividades son monitoreados periódicamente, dando prioridad a las aplicaciones e infraestructura crítica, así como mantener y revisar los registros cuando el sistema lo permita, de acuerdo con el proceso de Monitoreo de cuentas de usuario.

6.3 De la gestión de cuentas privilegiadas

6.3.1 La asignación de privilegios a cuentas de usuario para acceso a aplicaciones y sistemas debe estar basada en las necesidades de puestos, áreas y/o funciones encargadas de cubrir la demanda operativa.

6.3.2 La asignación y uso de accesos con privilegios especiales (p.ej. permisos de administrador) debe estar restringida y controlada. Cualquier excepción a los perfiles estándar o privilegios especiales debe ser autorizada por el propietario del sistema de información.

6.3.3 Las cuentas con privilegios creadas para una aplicación, sistema o tarea específica no deben ser usadas para ejercer actividades personales, de convicción, de negocio privado o para ejecutar actividades diferentes para las que fue creado.

6.3.4 Se debe evitar el uso compartido de usuarios de acceso con privilegios especiales (p.ej. permisos de administrador), en caso de que esto sea necesario porque así se requiere operativamente será necesario que todos los colaboradores que compartan credenciales firmen una carta responsiva de asignación de claves que describa los riesgos y responsabilidades de uso compartido.

6.3.5 Los derechos de acceso privilegiado deben ser revisados de manera trimestral y quedar registrados.

6.3.6 Se deberán mantener monitoreos de las actividades realizadas con las cuentas privilegiadas y de servicio, cuando los sistemas así lo permitan.

6.3.7 Las cuentas privilegiadas y de servicio deberán ser revisadas periódicamente y aquellas que no resulten necesarias sean redundantes o tengan periodos largos de desuso deberán ser eliminadas o deshabilitadas de acuerdo con el proceso de Monitoreo de vigencia de cuentas privilegiadas y de servicio, se debe reducir al mínimo posible el número de este tipo de cuentas.

6.4 De la gestión de contraseñas

6.4.1 Todo el personal deberá tener un identificador único y una contraseña personal, la cual debe ser secreta e intransferible para acceder a los recursos tecnológicos de la Red Aliat Universidades; asimismo, será responsable de toda actividad realizada con su usuario. La organización se reserva el derecho de investigar y sancionar cualquier abuso.

6.4.2 La entrega de contraseña por primera vez para el inicio de sesión en Windows y correo electrónico será de manera oral, al momento de la entrega del equipo, con la cual ingresará al sistema y en automático se le pedirá el cambio para poder iniciar sesión.

6.4.3 Los sistemas deberán forzar a que el usuario final modifique su contraseña en el primer inicio de sesión, antes de hacer uso de los recursos de tecnología de información, las excepciones deberán ser justificadas y documentadas.

6.4.4 Los sistemas deben configurarse de manera que sólo se permitan máximo tres (3) intentos fallidos para introducir la contraseña; cuando se excede el número de intentos, se desactiva la cuenta y solamente podrá reiniciarse a través del personal del Mesa de Servicio, siempre y cuando el identificador de usuario haya sido plenamente identificado.

6.4.5 La recuperación de contraseña debe realizarse por medio de Mesa de Servicio o si la aplicación lo permite, de forma automática a través de ella.

6.4.6 La construcción de contraseñas debe cumplir con los siguientes requisitos:

- Longitud mínima de ocho (8) caracteres.
- Al menos una letra mayúscula.
- Al menos una letra minúscula.
- Al menos un número.
- Al menos un carácter especial.

Nota: Toda excepción deberá tener autorización del responsable de Seguridad TI

6.4.7 Los usuarios no deben emplear ninguna estructura o característica de contraseña que pueda dar como resultado una contraseña predecible, como derivaciones de identificadores

de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical.

6.4.8 Se deberá exigir a los usuarios el cambio de contraseña, al menos una vez cada (3) meses. Se debe evitar el uso de contraseñas anteriores o históricas.

6.4.9 Las contraseñas para correo de voz no deben ser obligadas a cumplir las normas de construcción de contraseñas, pero los usuarios deben seleccionar una contraseña que sea distinta a su extensión telefónica, su número de oficina, su número de empleado y cualquier otro número que pudiera deducirse con facilidad.

6.4.10 No deberán almacenarse contraseñas fijas legibles en ubicaciones en donde las personas no autorizadas las pudieran descubrir.

6.5 Gestión de acceso a las Aplicaciones, Sistemas Operativos y Bases de datos

6.5.1 Los desarrolladores no podrán construir o desplegar identificadores de usuarios secretos o contraseñas que tengan privilegios especiales y que no se encuentren claramente descritos en la documentación generalmente disponible del sistema.

[...]

6.5.3 Se debe restringir el acceso a los sistemas operativos por medio de mecanismos de autenticación capaces de:

- Autenticar usuarios autorizados de acuerdo con esta Política.
- Registrar accesos exitosos y fallidos.
- Registrar el uso de privilegios especiales.
- Proveer medios apropiados de autenticación.
- Cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

6.5.4 Para las aplicaciones, bases de datos y los sistemas de información se deberá.

- Controlar el acceso a las funciones de los usuarios de acuerdo con esta Política.

- Proveer protección contra accesos no autorizados que se generen a partir de una utilidad, sistema operativo, o software malicioso, capaz de anular los controles de la aplicación, base de datos o sistemas de información.

6.6 Gestión de Acceso a la red

6.6.1 El director de TI se reserva el derecho a bloquear, ocultar, negar o discontinuar el servicio de acceso a la red en cualquier momento y sin previo aviso a cualquier usuario y en representación de la Red Aliat Universidades.

6.6.2 El permitir el acceso a las redes y a los servicios de ALIAT Universidades no debe comprometer su seguridad. Para esto, se deben utilizar:

- Segregación entre las redes y la red pública inalámbrica.
- Mecanismos de autenticación aplicados para usuarios y equipos.
- Gestión en los accesos otorgados a los usuarios externos y proveedores.

[...]

(Red Univercom, 2023)

ANEXO 4. Política institucional de baja de personal

[...]

5.1 De las Generalidades

5.1.1. Todas las bajas de personal deberán ser notificadas y solicitadas a la Dirección Institucional de Capital Humano por medio de la Gerencia de Relaciones Laborales y Seguridad Social para las bajas forzadas y por medio de Capital Humano Campus para las bajas por renuncia y termino de contrato.

5.1.2. La Gerencia de Relaciones Laborales y Seguridad Social validará la documentación que proporcionen las Direcciones de Capital Humano en Campus que soporten y justifiquen la baja forzada.

5.1.3. Las Direcciones de Capital Humano y el jefe inmediato analizarán las causas de baja y en su caso complementará la información de la solicitud, debiendo acompañar en todos los casos, llamadas de atención por escrito, actas administrativas y plan de mejora no exitoso. [...]

5.1.4. En todos los casos de baja de personal, se considerarán las causales que establece la Ley y el reglamento Interno de Trabajo, al Código y programa que se definan en la Institución.

5.1.5. Las bajas de personal aplicaran en los siguientes casos:

- Baja por renuncia: Cuando el Trabajador manifieste voluntariamente por escrito su deseo de dar por terminada la relación laboral con la Institución.
- Baja por término de contrato: Cuando concluye el contrato de trabajo por obra o tiempo determinado.
- Baja forzada o por solicitud: Cuando por necesidades de la Institución o cuando el trabajador incurre en alguna falta conforme a lo establecido en la Ley, políticas, procedimientos, Código y al Programa y los reglamentos de conducta que se definan en la Institución acompañándose de documentos que solventen y justifiquen la solicitud como lo es llamadas de atención por escrito. Actas administrativas y plan de mejora no exitoso.

[...]

5.1.10. El mismo día de la baja, el colaborador deberá de entregar los equipos asignados de cómputo o telefonía, contraseñas y cuentas en sistemas, así como los documentos relacionados con su puesto, credencial de la Institución, de acceso al edificio o estacionamiento (según aplique) conforme al formato de Entrega/Recepción FO-CH-27, siendo el jefe inmediato, los Directores de Capital Humano en Campus y Coordinador de Relaciones Laborales en Corporativo los responsables de resguardar los activos antes señalados y entregarlos al área que corresponda.

5.1.11. [...] También es responsabilidad de la Dirección de Capital Humano en Campus y Administración de personal y Compensaciones en Corporativo solicitar la baja del empleado a los sistemas de la Institución al área de Mesa de Servicio Aliat con base a la información que se desprende del formato de Entrega/Recepción mediante un ticket en el Sistema Informático Remedy, la cancelación de cada acceso que le fue asignado al colaborador, el mismo día en que se aplique la baja. Esta solicitud se enviará electrónicamente a Mesa de Servicio Aliat quien ejecutará el mismo día la aplicación de baja en los sistemas. Recibiendo Capital Humano de Campus y Administración de personal y Compensaciones en Corporativo la confirmación del ticket por parte de mesa de ayuda vía correo electrónico.

[...]

(Red Univercom, 2022)

ANEXO 5. Política de certificación y recertificación de usuarios en los sistemas informáticos

[...]

5.1 Generalidades

5.1.1. La Certificación y Recertificación de Usuarios aplica para todos los empleados que tienen asignada una cuenta de acceso a un sistema informático de Aliat Universidades.

5.1.2. La certificación se realiza a todas las cuentas de usuarios que están asignadas a un empleado vigente.

5.1.3. La certificación de usuario se realiza una vez al año en el primer trimestre y tiene una vigencia de 12 meses.

5.1.4. La Certificación o Recertificación de usuario, se realiza por sistema informático a la cuenta de acceso que tiene asignada el usuario.

5.1.5. El Perfil autorizado de roles, responsabilidades y permisos en la Certificación o Recertificación del usuario es responsabilidad del Líder del área.

5.1.6. El usuario es responsable de hacer buen uso de la cuenta de acceso que se le ha asignado conforme a la política a la Política de Control de Acceso.

5.1.7. En caso de que el usuario detecte que tiene asignado en su perfil un Rol, Responsabilidad o Permiso que no le corresponde a su puesto de trabajo o que genere un conflicto de segregación de funciones, debe de notificar a su Líder de área para que éste lo analice.

Obtención del perfil del usuario.

5.1.8. La Subdirección de Seguridad e Infraestructura es responsable de obtener el perfil de acceso al sistema informático de cada cuenta de usuario, perfil en el que se listan todas las responsabilidades, roles y privilegios asignados; así como de enviar vía correo electrónico dicho perfil al Líder de área para que, en su turno, revise los accesos asignados.

Validación del Perfil del usuario

5.1.9. La cuenta de usuario a Certificar / Recertificar, debe ser validada de que está asignada a un colaborador vigente de Aliat Universidades.

5.1.10. Durante la revisión del perfil del usuario, se valida que los Roles, Responsabilidades y Permisos asignados son los exclusivamente necesarios para que el usuario realice las tareas de su puesto de trabajo.

5.1.11. Los Roles, Responsabilidades y Permisos asignados en la certificación del usuario son revisados a detalle, y de ser necesario por los diferentes líderes del área de los módulos en el sistema informático a los que apuntan los permisos, para validar que no presentan conflictos de segregación de funciones según la PO-TI-03 Política de Segregación de Funciones.

Ajuste del Perfil del Usuario

5.1.12. Si durante la validación de los Roles, Responsabilidades y Permisos, se detecta que uno o varios de estos no corresponden al perfil del puesto de trabajo del usuario o que generan conflictos de segregación de funciones, se procede a eliminarlos. [...]

Consideraciones especiales

5.1.15. Los casos no previstos en la presente política, así como las posibles excepciones a las disposiciones contenidas en la misma, serán resueltos y/o autorizados por la Dirección de Tecnologías de la Información.

5.1.16. La presente política deja sin validez a todas las políticas, procesos, procedimientos, memorándums, correos electrónicos, o documentos que hagan referencia a la Política para la certificación y rectificación de usuarios en los sistemas informáticos que, a la fecha de publicación de este documento, hayan estado vigente.

(Red Univercom, 2020)

ANEXO 6. Acuerdo que establece las bases mínimas de información para la comercialización de los servicios educativos que prestan los particulares.

[...]

ARTICULO 7o. El incumplimiento de la obligación de pago de tres o más colegiaturas, equivalentes a cuando menos tres meses, por los padres de familia, tutores o usuarios, libera a los prestadores del servicio educativo de la obligación de continuar con la prestación, debiéndose observar para ello, las disposiciones aplicables, a efecto de que se asegure al alumno la educación básica su permanencia en el Sistema Educativo Nacional.

Los prestadores del servicio educativo deberán notificar la posibilidad de adoptar la medida a que se refiere el párrafo anterior con quince días de anticipación y los padres de familia, tutores o usuarios tendrán, en su caso, los siguientes derechos.

- I. Recibir la documentación oficial que le correspondan en un plazo no mayor de quince días a partir del momento en que la solicite, sin costo alguno, y
- II. Presentar exámenes extraordinarios en igualdad de condiciones que los demás alumnos, previo el pago de los derechos que correspondan. [...]

(SEGOB, 1992)

ANEXO 7. Reglamento General para estudios de Licenciatura y Posgrado modalidad: Escolarizada, Mixta y No Escolarizada.

[...]

TÍTULO II

DE LA INSCRIPCIÓN Y LA REINSCRIPCIÓN

CAPÍTULO I. DEL CALENDARIO ESCOLAR

Artículo 6. La Institución dará a conocer el Calendario Escolar para cada periodo por conducto de Servicios Escolares y de la plataforma educativa, para su consulta, observancia y cumplimiento en todos los campus de la Institución.

Artículo 7. La duración del ciclo lectivo es la siguiente:

- I. Licenciatura
 - a. Cuatrimestral de 14 semanas efectivas de trabajo académico.
 - b. Semestral de 16 semanas efectivas de trabajo académico.

- c. Semestral de Ciencias de la Salud, de 18 semanas efectivas de trabajo académico.
- II. Posgrado (Especialidad, Maestría y Doctorado)
 - a. Semestral, de 18 semanas efectivas de trabajo académico.
 - b. Cuatrimestral, de 14 semanas efectivas de trabajo académico.

Artículo 8. La duración mínima será de acuerdo con la totalidad de los créditos del paquete académico conforme al nivel y temporalidad.

CAPÍTULO II

DE LA INSCRIPCIÓN Y REINSCRIPCIÓN

Artículo 9. La Institución llevará a cabo la inscripción a primer ingreso y reingreso, así como la reinscripción a las asignaturas correspondientes, considerando lo siguiente:

- I. Los aspectos de comercialización del servicio educativo, dispuestos en el acuerdo que establece las bases mínimas de información para la comercialización de los servicios educativos que prestan los particulares, publicado en el Diario Oficial de la Federación del 10 de marzo de 1992 y la Ley de Educación.
- II. Apego a las fechas indicadas en el Calendario Escolar, que se difundirán con la debida oportunidad.
- III. Sólo podrán cursar el ciclo lectivo correspondiente, los estudiantes que realicen dichos trámites en las fechas a que hace referencia el numeral I de este artículo. De lo contrario, perderán su derecho a cursar ese ciclo lectivo.
- IV. Para cursar la asignatura es requisito indispensable, la inscripción a la misma en tiempo y forma, verificable mediante la tira de materias.
- V. La Institución admite estudiantes en calidad de oyentes con el fin de apoyar el desarrollo de certificaciones y evaluación continua del solicitante.

Artículo 10. Son estudiantes de primer ingreso aquellos que se matriculan por primera vez a un plan de estudios de la Institución, incluyendo estudiantes que ingresen por equivalencia o revalidación.

Artículo 11. Son estudiantes de reingreso aquellos que renuevan, mediante el pago de su reinscripción, su voluntad de permanecer en la Institución.

[...]

Artículo 70. La Institución no otorgará ningún servicio cuando el estudiante presente tres o más colegiaturas, equivalentes a cuando menos tres meses vencidos, la institución deberá notificar lo anterior con quince días de anticipación al interesado.

[...]

TÍTULO X

DE LAS BAJAS

CAPÍTULO ÚNICO

DE LAS DISPOSICIONES GENERALES

Artículo 149. Los estudios que el estudiante realice en la Institución pueden verse interrumpidos por alguna de estas causas de baja y su aplicación en apego al procedimiento de Aliat Universidades:

- I. **Voluntaria**, que se debe realizar de manera personal y por escrito en Servicios Escolares, de acuerdo con el procedimiento establecido para ello. Dicha baja podrá ser solicitada por los padres o tutores, presentando documentación legal de autorización del estudiante. Para que la baja sea válida será necesario tener cubiertas las colegiaturas devengadas a la fecha en que se solicita la baja y no tener adeudos en otros departamentos de la Institución. Estas bajas podrán solicitarse de forma temporal o definitiva.
- II. **Académica**, es aquella que ocurre como consecuencia de tener un bajo desempeño académico. Estas bajas se dan conforme con las siguientes condiciones:

- a. Si el estudiante reprueba 4 (cuatro) o más materias en plan rígido en un periodo, se aplica la baja temporal. El estudiante sólo podrá cursar nuevamente el semestre o cuatrimestre, una vez que regularice su situación académica, acreditando las materias que tiene pendientes de cursar y se incorporará como estudiante regular con el grupo que corresponda en los tiempos en que tenga sus materias aprobadas. Si el estudiante reprueba nuevamente una cantidad de materias que genere una baja en el semestre o cuatrimestre, se le aplicará baja definitiva y el estudiante ya no podrá inscribirse en la misma carrera.
- b. Si el estudiante tiene sin acreditar 4 (cuatro) materias de plan rígido después de concluir el siguiente periodo de regularización, causa baja temporal. El estudiante que se encuentre en esta situación podrá cursar nuevamente las materias que adeude, en su caso acreditarlas en algún periodo de regularización. Esta baja no podrá ser por un periodo mayor a 2 (dos) años, de lo contrario se convierte en baja definitiva.
- c. En el caso de las Licenciaturas en Salud, aquellos estudiantes que reprueben la materia de Prácticas de Campo Clínico en periodo ordinario causarán baja temporal y podrán cursarla nuevamente cuando se oferte la materia. Esto sin exceder el tiempo máximo que puede durar una baja temporal (2 años).
- d. No aprobar 3 materias o más en 2 ciclos consecutivos en plan rígido, anteriores.
- e. Cuando el estudiante cometa fraude académico y/o plagio consistente en presentar como suyas tesis, proyectos, trabajos o documentos, cuyos derechos sean de otras personas.

III. **Administrativa**, se da cuando el estudiante:

- a. Se inscribió a la modalidad escolarizada y alcanza el 20% de inasistencias continuas a partir del primer día de clases, sin dar aviso alguno de las mismas ni efectuar el trámite de baja.
- b. Se inscribió a la modalidad mixta (modular) y sin dar aviso alguno ni efectuar el trámite de baja, tiene inasistencias continuas en un módulo y no se presenta al inicio del siguiente módulo.
- c. Omite la entrega de documentos requeridos para su inscripción en los plazos establecidos por Servicios Escolares. Esta omisión lleva a perder el derecho a

cursar y acreditar las materias en las cuales está inscrito, y debe cubrir las colegiaturas que hasta ese momento adeude, quedando a resguardo las calificaciones que hubiera acreditado y tendrá un plazo de dos años para regularizar sus estudios de nivel inmediato anterior.

- d. Presente documentación presuntamente Carente de Validez, como se indique por la autoridad competente.
- e. Omite reinscribirse en las fechas establecidas en el Calendario Escolar.
- f. Tiene un máximo de tres colegiaturas vencidas, equivalentes a cuando menos tres meses.
- g. Cuando el estudiante deje de asistir a clases sin aviso anticipado, o máximo por un periodo continuo mayor a 20% del ciclo lectivo, se aplica este tipo de baja.

IV. **Disciplinaria**, es aquella que se aplica cuando el estudiante incurre en faltas a este Reglamento, o aquellos aplicables al uso de las instalaciones y servicios para el desarrollo de las actividades académicas dentro y fuera de la Institución.

Artículo 150. La Baja Administrativa podrá ser por el tiempo de vigencia del Reconocimiento de Validez Oficial de Estudios del Plan de Estudios correspondiente.

Artículo 151. La Baja Disciplinaria podrá ser baja temporal o definitiva, dependiendo de la resolución que las autoridades académicas determinen a razón de la falta cometida.

Artículo 152. Las bajas temporales no podrán exceder del tiempo de vigencia del plan de estudios; de ser el caso, el estudiante podrá solicitar nuevamente su ingreso a primer ciclo del plan de estudios modificado o actualizado sujetándose a la vigencia del plan de estudios en curso o reincorporarse a otro plan mediante el proceso de equivalencia. En todos los casos, la reincorporación o ingreso de los estudiantes, deberá solicitarse ante el Comité de Admisiones.

Artículo 153. En el caso de que el estudiante presente tres colegiaturas vencidas, equivalentes a cuando menos tres meses, la Institución se reserva el derecho de aplicar su baja administrativa del ciclo al que fue inscrito.

Artículo 154. Si el estudiante que ha causado baja requiera un Certificado Parcial, deberá solicitarlo a la Institución en un periodo máximo de 3 semanas posteriores a la baja, realizando el pago correspondiente.

[...]

(Red Univercom, 2024)