UNIVERSIDAD HISPANOAMERICANA

ESCUELA DE INGENIERÍA INFORMÁTICA

TESIS PARA OBPTAR POR EL GRADO DE LICENCIATURA

TÍTULO DEL PROYECTO

AUDITORIA BASADA EN CIBERSEGURIDAD UTILIZANDO LA NORMA ISO/IEC 27002 PARA EL DESARROLLO DE UN PLAN ESTRATÉGICO DE SEGURIDAD INFORMÁTICA APLICANDO LOS CONTROLES TECNOLÓGICOS EN EL ÁREA DE INFRAESTRUCTURA DEL DEPARTAMENTO DE TI EN COMERCIAL DE SEGUROS CORREDORA DE SEGUROS S.A, EN EL PERÍODO 2025-2026

Sustentante:

Leonardo Solera Ovares

Tutor:

Alejandro Bogantes Salazar

Diciembre, 2025

Tabla de contenido

Índice de Tablas

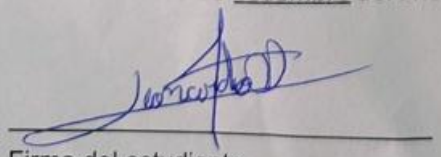
Índice de ilustraciones

DECLARACIÓN JURADA

DECLARACIÓN JURADA

Yo Leonardo Solera Ovares, mayor de edad, portador de la cédula de identidad número1-1358-0273 egresado de la carrera de Ingeniería Informática de la Universidad Hispanoamericana, hago constar por medio de este acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura en Ingeniería Informática con Énfasis en Sistemas de Información, juro solemnemente que mi trabajo de investigación titulado: Auditoría basada en Ciberseguridad utilizando la norma ISO/IEC 27007 para el Desarrollo de un plan Estratégico de Seguridad Informática aplicando los Controles Tecnológicos en el Área de Infraestructura del Departamento de TI en Comercial de Seguros Corredora de Seguros S.A, en el período 2025-2026. es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los 26 días del mes de setiembre del año dos mil veinticinco.



Firma del estudiante

Cédula: 1-1358-0273

CARTA DE APROBACIÓN DEL TUTOR

CARTA DEL TUTOR

San José, 25 de setiembre de 2025

Carrera Ingeniería Informática
Universidad Hispanoamericana

Estimados señores:

El estudiante **Leonardo Solera Ovares**, cédula de identidad número **113580273,** me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado "AUDITORIA BASADA EN CIBERSEGURIDAD UTILIZANDO LA NORMA ISO/IEC 27002 PARA EL DESARROLLO DE UN PLAN ESTRATÉGICO DE SEGURIDAD INFORMÁTICA APLICANDO LOS CONTROLES TECNOLÓGICOS EN EL ÁREA DE INFRAESTRUCTURA DEL DEPARTAMENTO DE TI EN COMERCIAL DE SEGUROS CORREDORA DE SEGUROS S.A, EN EL PERÍODO 2025-2026", el cual ha elaborado para optar por el grado académico de **Licenciatura** en Ingeniería Informática.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	10%
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	20%
C)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	30%
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	20%
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	20%
	TOTAL		**100**

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,
ALEJANDRO BOGANTES SALAZAR (FIRMA)
Firmado digitalmente por ALEJANDRO BOGANTES SALAZAR (FIRMA)
Fecha: 2025.09.25 18:01:35 -06'00'

Msc. Alejandro Bogantes Salazar
Cédula identidad: 303940389
Carné Colegio Profesional: 4644

CARTA DE APROBACIÓN DEL LECTOR

CARTA DE LECTOR

San José, 09 de Diciembre 2024.

Universidad Hispanoamericana
Sede Llorente
Carrera

Estimado señor

El estudiante **Leonardo Solera Ovares**, cédula de identidad **113580273**, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "**AUDITORIA BASADA EN CIBERSEGURIDAD UTILIZANDO LA NORMA ISO/IEC 27002 PARA EL DESARROLLO DE UN PLAN ESTRATÉGICO DE SEGURIDAD INFORMÁTICA APLICANDO LOS CONTROLES TECNOLÓGICOS EN EL ÁREA DE INFRAESTRUCTURA DEL DEPARTAMENTO DE TI EN COMERCIAL DE SEGUROS CORREDORA DE SEGUROS S.A, EN EL PERÍODO 2025-2026**", el cual ha elaborado para obtener su grado de **LICENCIATURA**

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación. He verificado que se han hecho las modificaciones correspondientes a las observaciones indicadas.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte.

MARCO VINICIO SOTO MONGE (FIRMA)

Firmado digitalmente por MARCO VINICIO SOTO MONGE (FIRMA)
Fecha: 2025.12.09 22:20:21 -06'00'

Marco Vinicio Soto Monge
110360428
4720

CARTA DE AUTORIZACIÓN DEL CENIT

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 10 de diciembre de 2025

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Leonardo Solera Ovares con número de identificación 1-1358-0273 autor (a) del trabajo de graduación titulado AUDITORIA BASADA EN CIBERSEGURIDAD UTILIZANDO LA NORMA ISO/IEC 27002 PARA EL DESARROLLO DE UN PLAN ESTRATÉGICO DE SEGURIDAD INFORMÁTICA APLICANDO LOS CONTROLES TECNOLÓGICOS EN EL ÁREA DE INFRAESTRUCTURA DEL DEPARTAMENTO DE TI EN COMERCIAL DE SEGUROS CORREDORA DE SEGUROS S.A, EN EL PERÍODO 2025-2026 presentado y aprobado en el año 2025 como requisito para optar por el título de LICENCIATURA EN INGENIERÍA INFORMÁTICA CON ÉNFASIS EN SISTEMAS DE INFORMACIÓN; (SI / NO) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente, LEONARDO SOLERA OVARES (FIRMA)

Firmado digitalmente por LEONARDO SOLERA OVARES (FIRMA)
Fecha: 2025.12.10 16:14:07 -06'00'

Firma y Documento de Identidad

ANEXO 1 (Versión en línea dentro del Repositorio)
LICENCIA Y AUTORIZACIÓN DE LOS AUTORES PARA PUBLICAR Y PERMITIR LA CONSULTA Y USO

Parte 1. Términos de la licencia general para publicación de obras en el repositorio institucional

Como titular del derecho de autor, confiero al Centro de Información Tecnológico (CENIT) una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, el autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito.

b) Autoriza al Centro de Información Tecnológico (CENIT) a publicar la obra en digital, los usuarios puedan consultar el contenido de su Trabajo Final de Graduación en la página Web de la Biblioteca Digital de la Universidad Hispanoamericana

c) Los autores aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) Los autores manifiestan que se trata de una obra original sobre la que tienen los derechos que autorizan y que son ellos quienes asumen total responsabilidad por el contenido de su obra ante el Centro de Información Tecnológico (CENIT) y ante terceros. En todo caso el Centro de Información Tecnológico (CENIT) se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

e) Autorizo al Centro de Información Tecnológica (CENIT) para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

f) Acepto que el Centro de Información Tecnológico (CENIT) pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

g) Autorizo que la obra sea puesta a disposición de la comunidad universitaria en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en las "Condiciones de uso de estricto cumplimiento" de los recursos publicados en Repositorio Institucional.

SI EL DOCUMENTO SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA O UNA ORGANIZACIÓN, CON EXCEPCIÓN DEL CENTRO DE INFORMACIÓN TECNOLÓGICO (CENIT), EL AUTOR GARANTIZA QUE SE HA CUMPLIDO CON LOS DERECHOS Y OBLIGACIONES REQUERIDOS POR EL RESPECTIVO CONTRATO O ACUERDO.

DEDICATORIA

Este proyecto, culmen de años de esfuerzo y aprendizaje, lo dedico con todo mi corazón.

En primer lugar, a mi querida madre Ivette Ovares Camacho, cuyo amor incondicional ha sido el motor de mi vida, gracias por cada sacrificio, por cada palabra de aliento, por creer en mí incluso cuando yo dudaba. Su ejemplo de perseverancia y trabajo duro es mi mayor inspiración y esta meta alcanzada es, en gran parte, gracias ella.

A mi hijo, Sebastián Solera, por su apoyo constante, sus risas compartidas y por ser un gran compañero de vida. Su amor me da la fuerza para seguir adelante.

A Paola Gamboa, por su paciencia infinita, su comprensión en los momentos de estrés y cansancio.

Gracias por acompañarme en este camino y por celebrar conmigo cada pequeño avance.

Finalmente, a mis profesores y mentores, por su invaluable guía, su conocimiento y su confianza en mi capacidad. Gracias por sembrar en mí la curiosidad y la pasión por esta disciplina.

Este logro es para todos ustedes.

Con todo mi cariño y amor.

AGRADECIMIENTOS

Primeramente, le agradezco a Dios ante todo porque sin él no estaría aquí en este momento tan importante. Llegar a este punto no hubiera sido posible sin la invaluable ayuda y el apoyo de muchas personas, a quienes deseo expresar mi más sincera gratitud, en especial a mis papás por brindarme el regalo de una excelente educación y por ser un ejemplo para seguir.

A muchos de mis profesores que durante tantos años de carrera por su constante motivación y confianza en este proyecto. Sus valiosas orientaciones no solo enriquecieron enormemente mi trabajo, sino que también me impulsaron a explorar nuevas perspectivas y a desarrollar una visión crítica más profunda. Su guía fue fundamental en cada etapa.

A la Universidad Hispanoamericana y a la Facultad de Ingeniería Informática, por ofrecerme la plataforma académica, los recursos y un entorno de extraordinario de aprendizaje que hicieron posible mi formación y la realización de esta investigación.

A todos los que, de una u otra forma, contribuyeron a este logro, mi más sincero y profundo agradecimiento.

Con gratitud,

RESUMEN

Contexto

Comercial de Seguros Corredora de Seguros S.A. es una empresa costarricense que cuenta con más de 27 años operando en el mercado asegurador. Actualmente, la organización se encuentra expuesta a importantes riesgos de seguridad debido a debilidades en su infraestructura tecnológica que podrían ser aprovechadas por ciberdelincuentes, la carencia de medidas de ciberseguridad bien definidas, sumada al incremento en la complejidad de las amenazas cibernéticas, ha puesto en evidencia la urgencia de mejorar significativamente los aspectos de seguridad informática, especialmente en lo que respecta a la infraestructura del Departamento de Tecnologías de Información.

Objetivo

Desarrollar un plan estratégico de seguridad informática fundamentado en los controles tecnológicos de la norma ISO/IEC 27002, dirigido a reducir los riesgos cibernéticos en el área de infraestructura del Dpto. de TI y garantizar la continuidad operativa de Comercial de Seguros Corredores de Seguros S.A durante el período 2025-2026.

Método

La investigación adoptó un enfoque cuantitativo de tipo exploratorio-descriptivo, empleando técnicas de recolección de datos mediante entrevistas estructuradas, observación directa y cuestionarios aplicados al personal técnico responsable de la infraestructura tecnológica. Se realizó un diagnóstico integral que abarcó aspectos administrativos, técnicos y de percepción, evaluando el cumplimiento de 16 controles tecnológicos específicos de la norma ISO/IEC 27002.

La metodología incluyó análisis de brechas de seguridad, identificación de vulnerabilidades y priorización de controles según criticidad y recursos disponibles.

Resultados

El diagnóstico reveló brechas significativas en múltiples controles tecnológicos: ausencia de cifrado en dispositivos terminales, registros incompletos de accesos privilegiados, falta de pruebas periódicas de vulnerabilidades, carencias en enmascaramiento de datos, y deficiencias en la segregación de redes. Se identificó un cumplimiento parcial en 12 de los 16 controles evaluados, con fortalezas en respaldos de información e instalación controlada de software. La infraestructura presenta una base sólida, pero requiere mejoras sustanciales en documentación, monitoreo avanzado y redundancia de sistemas.

Conclusión

Se logró crear satisfactoriamente un plan completo de seguridad informática que atiende de forma ordenada cada una de las vulnerabilidades encontradas, ofreciendo recomendaciones puntuales, sugerencias de herramientas tecnológicas y una estrategia de implementación organizada por prioridades. Este plan proporciona un marco sólido que permitirá a la organización transformar su enfoque actual de seguridad, alineándolo con los estándares internacionales que define la norma ISO/IEC 27002 y estableciendo los cimientos necesarios para mantener un proceso permanente de mejoramiento en materia de ciberseguridad.

Palabras Clave

Ciberseguridad, ISO/IEC 27002, controles tecnológicos, seguridad de la información, plan estratégico de seguridad, gestión de vulnerabilidades, infraestructura tecnológica, auditoría de seguridad, corredora de seguros.

CAPÍTULO I: PROBLEMA DEL PROYECTO

1. Antecedentes y Justificación del Proyecto

1.1. Marco De Referencia Empresarial

1.1.1 Antecedentes del contexto de la empresa

Comercial de Seguros Corredora de Seguros S.A, con más de 27 años de trayectoria, es una compañía de gran renombre en el sector de seguros costarricense. Es responsable de llevar a cabo diversos estudios y cotejar las distintas protecciones disponibles para salvaguardar el valor de su empresa y lo que es relevante para usted.

Comercial de Seguros Corredora de Seguros S.A al igual que numerosas otras entidades de seguros, son particularmente vulnerables a los ciberataques debido al enorme volumen de información sensible que gestiona, trabaja en un entorno digital cada vez más avanzado y se encuentra vulnerable a diversas amenazas y ataques cibernéticos.

El incremento y la regularidad de los ciberataques a nivel mundial han hecho que la seguridad de la información sea una de las principales preocupaciones de todas las empresas, independientemente de su tamaño o sector.

La naturaleza del negocio de Comercial de Seguros Corredora de Seguros S.A, implica la gestión de grandes cantidades de información delicada sobre cada uno de sus clientes, lo que los convierte en un objetivo atractivo para los ciberdelincuentes. El robo o la pérdida de esta información puede causar no solo pérdidas financieras, sino también en daños legales y de reputación.

1.1.2 Justificación del Proyecto

Comercial de Seguros Corredora de Seguros S.A., debido a su larga trayectoria y reputación en el mercado, la empresa está expuesta a muchos riesgos cibernéticos que pueden comprometer la integridad de sus operaciones, la confianza de sus clientes y su reputación. Esta situación se ha vuelto cada vez más urgente debido a la falta de controles de ciberseguridad y la creciente complejidad de las ciber amenazas.

Con base en los problemas específicos identificados, se evidencia una carencia generalizada en los lineamientos de gestión de seguridad de la información.

La falta de una metodología de auditoría tomando como base los marcos de buenas prácticas crea un entorno propicio para que ocurran incidentes de seguridad.

1.2. Definición del Problema

1.2.1 Problemática

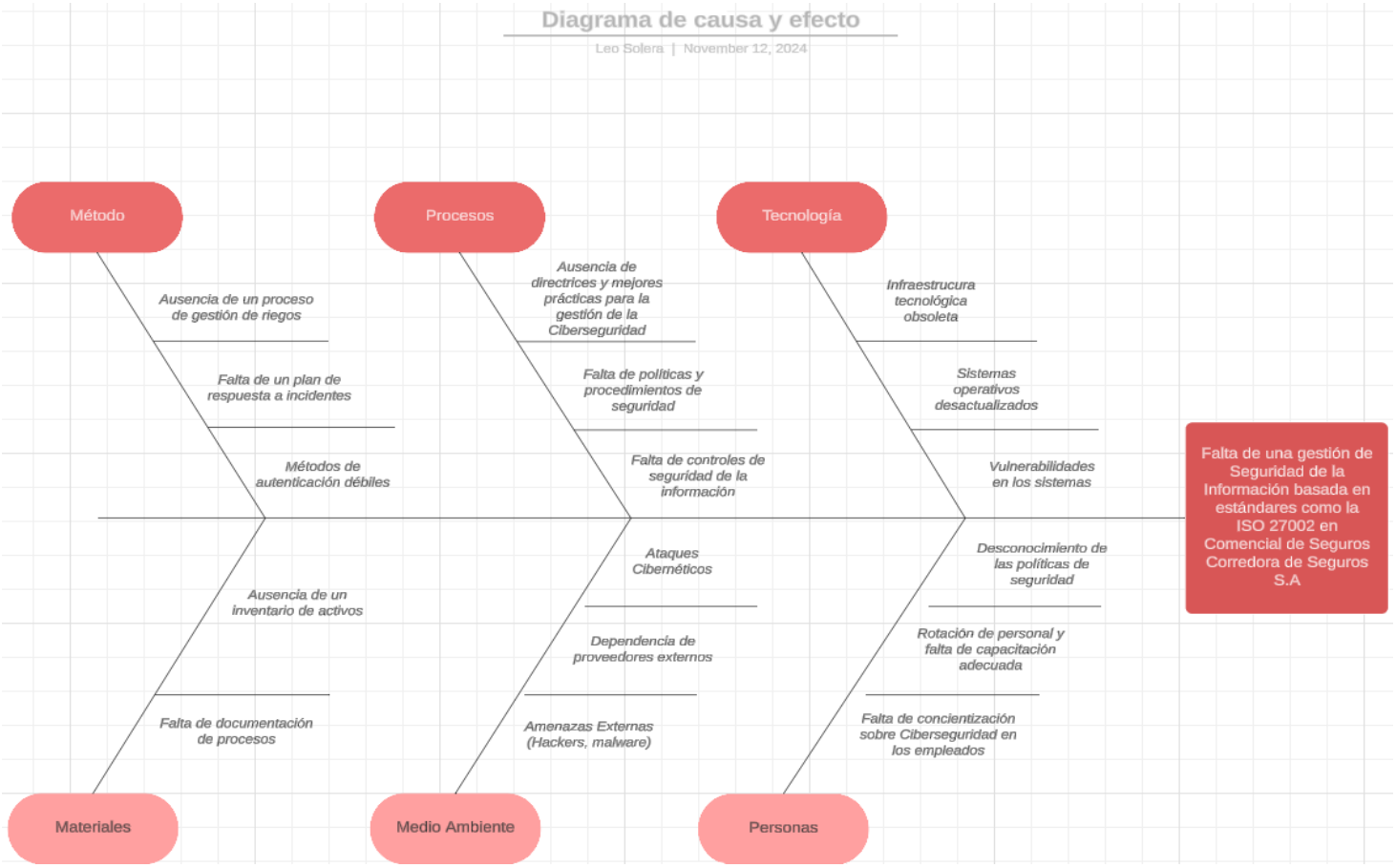
La ausencia de directrices y mejores prácticas para la gestión de la Ciberseguridad en el área de Infraestructura dentro del Dpto. de TI, de la organización Comercial de Seguros Corredora de Seguros S.A lo expone a riesgos como brechas de seguridad, altos costos en la recuperación de información, reparación de sistemas ante algún ciberataque, daños a la reputación de la organización y posibles interrupciones en sus operaciones.

Las corredoras de seguros hoy en día, al igual que muchas otras empresas, son vulnerables a estas amenazas que pueden comprometer la integridad de su información, la continuidad de sus operaciones y la confianza de sus clientes.

Para mitigar estos riesgos es esencial fortalecer la Ciberseguridad mediante un plan estratégico de seguridad informática basándose en los controles tecnológicos adecuados de la ISO 27002, de acuerdo con los riesgos que enfrentan.

1.2.2 Diagrama de Ishikawa

Ilustración 1: Diagrama de causa y efeto



Fuente: Elaboración propia

1.2.3 Problema General

¿Cómo puede la organización mejorar su postura de Ciberseguridad en el área de Infraestructura dentro del Dpto. TI mediante la implementación de un plan estratégico de seguridad informática basado en los controles tecnológicos de la ISO 27002, para la protección de sus activos de información, mitigar los riesgos cibernéticos y garantizar la continuidad del negocio?

1.2.4 Problemas Específicos

- Falta de un plan estratégico de seguridad informática seguro en el área de Infraestructura del Dpto. de TI.
- Falta de no tener implementado controles tecnológicos basados en la norma ISO27002 en el área de Infraestructura expone a la organización a ser más vulnerable por los ciberdelincuentes y con mayor riesgo de ciberataques
- Riesgo de pérdida de información confidencial, la organización maneja un alto volumen de datos sensibles de sus asociados, los cuales podrían ser objeto de robo o filtración de esta en caso de un ciberataque.
- Los ataques cibernéticos pueden provocar costos considerables para la entidad, que incluye costos vinculados a la recuperación de datos, la restauración de sistemas, la administración de crisis y perjudicar la imagen de la empresa.

1.3. Objetivos del Proyecto

1.3.1 Objetivo General

Desarrollar un plan estratégico de seguridad informática basado en los controles tecnológicos de la norma ISO 27002 permitiendo una reducción de los riesgos cibernéticos en el área de Infraestructura del Dpto. de TI en Comercial de Seguros Corredora de Seguros S.A y su continuidad del negocio durante el año 2025.

1.3.2 Objetivos Específicos

1. Analizar la situación actual de la infraestructura tecnológica existente de la entidad, mediante una evaluación de diagnóstico basada en los controles tecnológicos de ISO 270002, con la finalidad en la detección de brechas y vulnerabilidades de seguridad que comprometan la confidencialidad, integridad y disponibilidad de la información.
2. Identificar los controles tecnológicos que cumplen con la seguridad informática según lo dicta la norma ISO 27002, a través de un análisis comparativo con la infraestructura actual, para determinar el nivel de cumplimiento y las oportunidades de mejora en la gestión de vulnerabilidades.
3. Realizar una priorización de cada uno de los controles tecnológicos seleccionados de la norma ISO 27002, mediante el análisis de riesgos que evalúe la criticidad, impacto y viabilidad de implementación, para establecer un plan estratégico de seguridad informática con actividades y procesos de auditoría de manera periódica.

4. Desarrollar un plan de seguridad informática, mediante la definición de políticas, procedimientos y controles técnicos alineados con la ISO 27002, para garantizar el uso seguro de los recursos y activos de información en Comercial de Seguros Corredora de Seguros S.A.
5. Desarrollar una propuesta de implementación del plan de seguridad informática que incluya recursos necesarios, responsables y métricas de cumplimiento, para facilitar la adopción efectiva de las políticas y controles de seguridad en Comercial de Seguros Corredora de Seguros S.A.

1.4. Alcance y limitaciones

1.4.1 Alcance del proyecto

El foco central del proyecto es el poder fortalecer la postura de Ciberseguridad del área de Infraestructura del Dpto. de TI en la organización de Comercial de Seguros Corredora de Seguros S.A, realizando un análisis de la infraestructura tecnológica pudiendo identificar las brechas de seguridad actuales y mediante un plan estratégico de seguridad informática poder establecer controles tecnológicos de seguridad basados en la norma ISO 27002, para a la gestión de la seguridad informática. De esta manera contribuir a minimizar la probabilidad y gestión de incidentes de seguridad.

Dicho de otra manera, el proyecto de poder implementar un plan de Ciberseguridad en Comercial de Seguros Corredora de Seguros S.A es vital para poder proteger los activos de la organización y garantizar la continuidad.

1.4.2 Limitaciones del proyecto

- La disponibilidad de recursos económicos para la adquisición de alguna herramienta o solución.
- El factor de tiempo para poder realizar el proyecto no podrá abordar todos los controles que incluyen la norma ISO 27002.
- Si la empresa depende de proveedores externos, esto podría dificultar un poco el avance del proyecto.
- Los colaboradores podrían resistirse al cambio en algún proceso o procedimiento que se vaya a implementar en la organización.

1.5. Cronograma del Proyecto

Ilustración 2: Cronograma de trabajo

AUDITORIA BASADA EN CIBERSEGURIDAD UTILIZANDO LA NORMA ISO/IEC 27002 PARA EL DESARROLLO DE UN PLAN ESTRATÉGICO DE SEGURIDAD INFORMÁTICA APLICANDO LOS CONTROLES TECNOLÓGICOS EN EL ÁREA DE INFRAESTRUCTURA DEL DEPARTAMENTO DE TI EN COMERCIAL DE SEGUROS CORREDORA DE SEGUROS, S.A EN EL PERÍODO 2025-2026

ACTIVIDADES	Meses	Enero				Febrero				Marzo				Abril				Mayo				Junio				Julio				Agosto				eptiemb	
	Semanas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
Entrega del anteproyecto																																			
Aprobación del anteproyecto y asignación de tutor																																			
Desarrollo del Capitulo I: Planteamiento del Problema																																			
Entrega del capitulo I y matriz de coherencia																																			
Revisión y aprobación de capitulo I por parte del tutor																																			
Desarrollo del Capitulo II: Marco Teórico																																			
Búsqueda de conceptos																																			
Recolección de la información																																			
Realización del marco teórico																																			
Entrega del capitulo II																																			
Revisión y aprobación de capitulo II por parte del tutor																																			
Desarrollo del Capitulo III: Marco Metodológico																																			
Analizar el enfoque de la investigación																																			
Recolectar la información necesaria a cerca del proyecto																																			
Entrega del capitulo III																																			
Revisión y aprobación de capitulo III por parte del tutor																																			
Desarrollo del Capitulo IV: Diagnóstico																																			
Identificación y recolección de datos de la situación actual																																			
Analizar las necesidades del cliente																																			
Definir los resultados actuales para determinar ejecución del proyecto																																			
Entrega del capitulo IV																																			
Revisión y aprobación de capitulo IV por parte del tutor																																			
Desarrollo del Capitulo V: Diseño y Desarrollo del Proyecto																																			
Desarrollo el plan estratégico de seguridad informática																																			
Desarrollo de la propuesta de implementación para plan estratégico																																			
Entrega del capitulo V																																			
Revisión y aprobación de capitulo V por parte del tutor																																			
Desarrollo del Capitulo VI: Conclusiones y recomendaciones																																			
Análisis de desempeño y conclusiones																																			
Redacción sobre las recomendaciones																																			
Entrega del capitulo VI																																			
Revisión y aprobación de capitulo VI por parte del tutor																																			

Fuente: Elaboración propia

CAPÍTULO II: MARCO TEÓRICO

2. Conceptos Generales

Actualmente vivimos en un mundo donde la digitalización, avanza exponencialmente, siendo la seguridad de la información y la ciberseguridad, pilar de la continuidad y fiabilidad de la operación de cualquier organización. A continuación, en este segundo capítulo, explicito todos los conceptos utilizados para la elaboración del plan estratégico de una empresa, me parece importante poder contar con estos conceptos para poder discernir y gestionar los riesgos de ciberseguridad y así proteger la información e infraestructura tecnológica.

Iniciaremos con conceptos fundamentales de seguridad de la información, ciberseguridad y riesgos cibernéticos, es importante explorar estos términos ya que son la base para poder entender las amenazas y retos actuales.

Seguidamente profundizaremos conocimientos de una infraestructura tecnológica, vulnerabilidades y normativas que rigen su protección, destacando la importancia de reconocer y mitigar los riegos.

El foco principal en la investigación del proyecto se centra en la Norma ISO/IEC 27002 la cual introduciremos conceptos importantes, proporcionando directrices y controles detallados para lograr de manera exitosa el desarrollo de éste.

Finalmente, mediante el desarrollo de un plan estratégico de seguridad informática reforzaremos la seguridad de Comercial de Seguros Corredora de Seguros S.A, es importante mantener un marco robusto y proactivo para garantizar la protección de los activos digitales en una organización.

2.1 Conceptos Fundamentales de Seguridad de la Información

De acuerdo con el autor Vega (2021) describe la definición de seguridad de la información en la que afirma que, “Según la ISO/IEC (2016), la seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada” (pág. 9).

Con referencia a la noción anterior, podemos afirmar que la seguridad de la información se refiere a proteger los activos de información al implementar políticas, controles de protección de datos e implementar determinadas acciones dentro y fuera de una organización.

De hecho, esto significa que es necesario cuidar todos los activos críticos de una organización para evitar pérdidas de información, así como garantizar la confianza de los clientes y de los propios empleados. Esto es un proceso continuo que necesita ser actualizado con frecuencia debido a las nuevas amenazas que surgen.

La información es un recurso que para una organización tiene valor por diferentes motivos. Por ejemplo, existen empresas que trabajan día a día y dependen tener acceso a cierta información que las ayuda en su funcionamiento. Imaginemos el no tener acceso a la información o el perderla, sería un problema catastrófico para la organización, por esto la importancia de proteger la información puede resultarle crucial a la empresa.

2.1.1 Los tres pilares de la seguridad de la información: La tríada CID

Es un modelo común que constituye la base para el desarrollo de sistemas de seguridad de la información. Se utilizan para encontrar vulnerabilidades y métodos para crear soluciones, la confidencialidad, integridad y disponibilidad conforman las piedras angulares de una protección de la información sólida, que crean la base de la infraestructura de seguridad de una empresa. (Fortinet, 2025).

Es esencial para las organizaciones ya que ayuda en identificar y evaluar riesgos, poder diseñar e implementar medidas de seguridad y así poder mantener una mejor postura de seguridad.

Ilustración 3: Pilares de la seguridad de la información

Fuente: Wallarm (s.f).

Recuperado de https://www.wallarm.com/

2.1.2 Conceptos

- Confidencialidad: La privacidad es parte integral de la seguridad de la información. Todas las empresas deberían implementar las medidas necesarias que se requieren para restringir el acceso a la información y suministrarla únicamente al personal debidamente autorizado.
- Integridad: Se espera que todas las empresas protejan la integridad de todos los datos e información en cada etapa de su vida. Colocar en funcionamiento un SGSI bien hecho significa que usted reconoce la necesidad de mantener los datos precisos, honestos y sin clones, evitando que personas no identificadas entren y tomen el control de ellos o interfieran con ellos.
- Disponibilidad: Continuidad del negocio – se proporciona un mantenimiento continuo del hardware físico junto con actualizaciones de sistema recurrentes. Se asegura que los usuarios debidamente identificados (esos que tienen permisos para acceder) tengan un nivel confiable y resistente de acceso a los datos cuando se necesite.

2.1.3 ¿Por qué se debería usar la tríada CID?

Es de gran valor para las organizaciones el poder evaluar lo que salió mal y lo que funcionó después de algún incidente de riesgo, un sistema de seguridad de información que carezca de uno de los tres elementos de la tríada de la CID puede decirse que es insuficiente, por ejemplo, si una empresa es atacada por un ransomware y detiene la operativa, podemos deducir que la disponibilidad se vio comprometida, pero los sistemas implementados aún podrían mantener su confidencialidad en la información.

2.2 Ciberseguridad

Escuchar frases en donde se utilizan palabras como ataques cibernéticos, ciber menazas, software malicioso, virus informático, suplantación de identidad, hackers, y ciber fraude por mencionar algunas, es cada vez más común. Esto, hace referencia a los múltiples riesgos que existen al momento de conectar un dispositivo a la red formando un ecosistema mejor conocido como ciberespacio.

> La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada. (Corletti Estrada, 2020, p.29)

Según la definición que plantea Estrada, podríamos decir que la ciberseguridad es una disciplina que se enfoca en resguardar la infraestructura computacional y toda aquella información incluida o circulante y que tiene como objetivo el minimizar los riesgos mediante el uso de estándares protocolos, métodos y diferentes herramientas informáticas; la seguridad informática abarca la protección de hardware, software, información, cualquier tipo de activo que sea de valor para una empresa.

Le importancia reside en evitar que la información confidencial caiga en manos de los ciberdelincuentes o personas no autorizadas, lo que podría convertirla en información privilegiada y generar riesgos importantes.

Ilustración 4: Ciberseguridad

Fuente: Itop Academy (s.f).
Recuperado de https://itop.academy/

Demos tener muy claros que la definición de **"Seguridad de la información"** no debe ser confundida con la de **"Seguridad informática",** ya que esta última solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no únicamente en los medios informáticos.

2.2.1 Amenaza

> Una amenaza de ciberseguridad se refiere a cualquier situación o caso que pueda tener consecuencias negativas para las operaciones, funciones, marca, reputación o imagen percibida de una empresa. Una amenaza de este tipo también puede afectar al acceso a los datos, su integridad y su valor, así como a las personas, los procesos y las tecnologías que participan en la gestión de dichos datos. Las amenazas cibernéticas suelen surgir cuando un ciberataque establece como objetivo los datos, sistemas informáticos, redes o dispositivos de una organización para obtener un acceso no autorizado o explotar cualquier vulnerabilidad del sistema de información, y comprometer así su confidencialidad, integridad o disponibilidad. (Hewlett Packard Enterprise, 2024, párrafo primero).

De acuerdo con lo expuesto en el artículo publicado por HPE (2024), los ciberataques son la principal causa de las amenazas a la ciberseguridad. Los ciberdelincuentes o también llamados cibercriminales buscan explotar todas aquellas vulnerabilidades en las que se encuentren expuestos en los sistemas para de esa manera poder obtener acceso no autorizado a información confidencial, robo de datos y se de esa manera extorsionar a las empresas, o únicamente causar daños.

Deberíamos diseñar programas de ciberseguridad eficaces para poder identificar todas las amenazas y destruirlas lo más pronto posible. Muchas de las tecnologías actuales son diseñadas para detener las amenazas antes de que ingresen en una red o en su búsqueda y destrucción de los que han entrado sin ser invitados.

Con la alta demanda en la creciente sofisticación de los ciberataques, muchos de los programas de ciberseguridad se centran tanto en detener los ataques como en garantizarle al negocio una continuidad.

Las amenazas constantemente se encuentran en evolución, por lo que existen diferentes categorías en métodos de ataques más comunes que siguen planteando un desafío para los programas de ciberseguridad. Exploraremos la definición de los ataques más comunes.

2.2.2 Tipos de amenazas más comunes

Virus: Software dañino que se propaga y replica de un equipo a otro.

Phishing: Técnica empleada por los atacantes que envían correos electrónicos o SMS falsificados, que crean el papel de fuentes confiables, con el objetivo de engañar a las víctimas y sondear información privada, como las contraseñas, números de cuenta o datos o tarjetas de crédito, lo que les permite acceder a sus datos o robar dinero.

Malware: Engloba cual programa que perjudique a un sistema informático, de los más habituales se hallan los troyanos, spyware, así como adware.

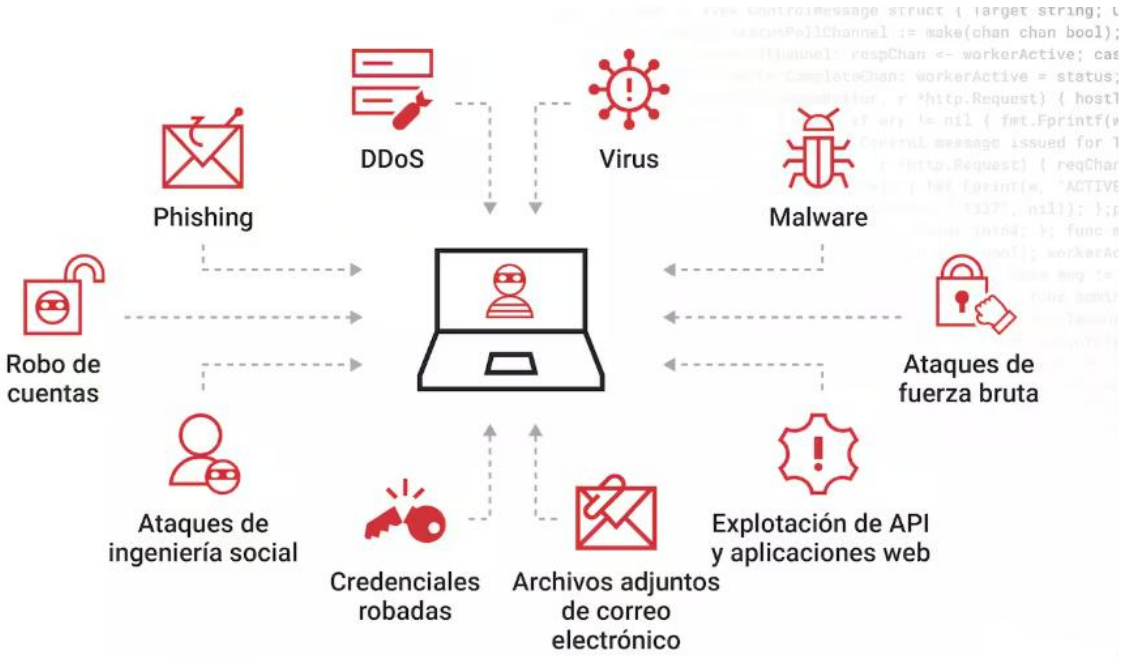
Ransomware: Es un tipo de malware que bloquea el acceso a los sistemas e información mediante una técnica de cifrado de datos, este tipo de ataque se realiza a través de sitios web o correos electrónicos y explota vulnerabilidades, en algunos casos, afectan múltiples computadoras y servidores, este tipo de ataque puede activarse días o semanas después de la infección y propagarse a través de las redes internas de una organización. Algunos ransonware están diseñados para evadir diferentes tipos de antivirus, por lo que es crucial evitar sitios sospechosos o enlaces desconocidos.

DoS y DDoS: DoS es intentar hacer que un sistema se vuelva inaccesible o bloquear sus servicios mediante la sobrecarga de tráfico, mientras que DDoS multiplica los sistemas que hacen esto, es aún más efectivo en interrumpir un sitio web o sistema.

Ataque de fuerza bruta: Se basa en la adivinación de las credenciales de algún acceso por probar miles de, o de millones, de combinaciones distintas hasta que se descubra la correcta. Por lo general, los ciberdelincuentes utilizan bots para automatizar el proceso,

Ataques de ingeniería social: Es una técnica que utilizan los cibercriminales para manipular a las personas para que compartan información confidencial, para que descarguen algún tipo de software que no deberían, visitar sitios en internet malicioso e inclusive que envíen dinero a los delincuentes.

Ilustración 5: Tipos de vectores de ataque más comunes



Fuente: Akamai (s.f).

Recuperado de https://akamai.com/

2.2.3 Vulnerabilidades

> Una vulnerabilidad en materia de seguridad se refiere a una debilidad u oportunidad en un sistema de información que los cibercriminales pueden explotar y obtener acceso no autorizado a un sistema informático. Las vulnerabilidades debilitan los sistemas y abren la puerta a ataques maliciosos. (Simplilearn, 2024)

Siguiendo lo expuesto podemos decir que las vulnerabilidades son debilidades en el hardware, software e inclusive en los procedimientos, y que son la puerta de entrada para que los cibercriminales puedan acceder a los diferentes sistemas, un fallo técnico de deficiencia de un programa puede permitir a que una persona no autorizada tenga acceso de manera remota a información confidencial y sensible.

2.2.4 ¿Cuáles son los tipos más comunes de vulnerabilidades en seguridad?

1. Las vulnerabilidades de red: Son fallas en la infraestructura de hardware o software de una entidad que permiten a los cibercriminales acceder y provocar daños. Estas áreas de exposición pueden ir desde un acceso inalámbrico mal protegido o deficientemente asegurado, hasta equipos de perímetro como los firewalls que se encuentren mal configurados y que no protegen la red en general.
2. Las vulnerabilidades del sistema operativo: Dentro de un SO existen exposiciones que permiten a los ciberdelincuentes ocasionar daños en cualquier dispositivo donde se encuentre instalado un sistema operativo. Un claro ejemplo en donde se aprovechan las vulnerabilidades del SO es un ataque de denegación de servicio (DoS, DDoS).

El software que no cuente con sus parches de seguridad actualizados también crea vulnerabilidades del sistema operativo, porque el sistema que ejecuta la aplicación queda expuesto, lo que a veces puede poner en peligro toda la red.

3. Las vulnerabilidades de proceso: Esta se generan cuando los procedimientos que se supone que actúan como medidas de seguridad resultan insuficientes. Entre las más conocidas podemos mencionar un proceso común como es la de la autenticación, en la que lo usuarios, e incluso los administradores de TI, utilizan contraseñas débiles.
4. Las vulnerabilidades humanas: Este tipo de vulnerabilidades son creadas por errores de los usuarios y que pueden exponer en riesgos las redes, hardware y datos confidenciales. Podríamos decir que representan la amenaza más importante debido al aumento de trabajadores remotos y móviles. Entre los ejemplos de vulnerabilidades humanas más comunes en materia de ciberseguridad es el abrir algún archivo adjunto proveniente de algún correo electrónico y que el mismo se encuentre infectado con algún tipo de malware.

Ilustración 6: Proceso de gestión de vulnerabilidades

Fuente: Gub (s.f).

Recuperado de https://www.gub.uy/

2.2.5 Riesgo

> Se denomina riesgo a la posibilidad de que un sistema sufra un incidente de seguridad y que una amenaza se materialice causando una serie de daños. Para medir el riesgo de un sistema informático se debe asumir que existe una vulnerabilidad ante una amenaza. El riesgo es, por lo tanto, la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad existente. (Ambit-bst, 2022).

Dicho lo anterior la visión estratégica de la seguridad debe ser reflejada en herramientas aplicadas de manera planificada con objetivos claros y revisados de manera periódica, para que sean implementadas en los procesos de toda la organización. Estos procesos se definen como aquellos que buscan la identificación y evaluación de los riesgos, así como también adoptar los pasos para su reducción a un nivel aceptable y devendrán en programas que serán la base para la adopción de medidas de gestión, controles técnicos, procedimentales y normativos, que mitiguen los riesgos a los que se encuentra expuesta la información.

Ilustración 7: Interacción entre vulnerabilidades, amenazas y riesgos

Fuente: Magazcitum (s.f)

Recuperado de https://www.magazcitum.com.mx/

2.3 Riesgos Cibernéticos

Los sistemas de TI son fundamentales para casi todas las facetas de las empresas modernas. Desde el procesamiento de datos de los clientes hasta el rastreo de la logística en la cadena de suministro, estas tecnologías permiten a las empresas operar de una manera más eficiente y efectiva, pero a medida que crecen las capacidades y oportunidades, también lo hacen los riesgos, cada nuevo punto final del sistema ya sea un dispositivo móvil, un servidor o cualquier otro, representa un nuevo vector de ataque, lo que significa que las organizaciones deben estar más alerta que nunca para proteger sus activos digitales de los ciberataques.

> El término "riesgo cibernético" se refiere al daño que representan estas amenazas cibernéticas. Puede presentarse de varias formas, desde pérdidas financieras hasta *daños a la reputación* e incluso *sanciones legales* asociadas a la falta de cumplimiento de la seguridad de los datos. Y, a medida que la transformación digital sigue modificando la manera en que funcionan los negocios en el mundo, el riesgo cibernético aumenta de forma significativa. (Servicenow, 2023, párrafo segundo).

Considerando lo anterior se menciona la importancia de los sistemas de TI en las organizaciones modernas y de acuerdo con su crecimiento la manera en que aumentan los riesgos cibernéticos se enfatiza que el riesgo cibernético no solo implica pérdidas financieras, si no también daños a la reputación y posibles sanciones legales, lo cual es un punto clave en el contexto actual de transformación digital. En el siguiente apartado incluiremos ejemplos concretos de ataques recientes a organizaciones en Costa Rica.

2.3.1 Organizaciones costarricenses que han sufrido de ataques cibernéticos

Desde el pasado 17 de abril del 2022, Costa Rica se vio envuelto en una ola de ciberataques sin precedentes de índole extorsivo por el grupo de Conti y Hive Ransomware Group, los cuales son grupos organizados que generan variantes de ransonware-as-a-service (RaaS) provenientes de Rusia. Este tipo de modelo de negocio se distingue al poseer un panel de administración desde donde las personas que contratan el servicio generan y administran los perfiles de las víctimas a fin de recoger información relevante.

Si revisamos las más importantes instituciones públicas de Costa Rica, podemos hacer referencia al Ministerio de Hacienda, que fue la primera entidad en sufrir un ataque del tipo Ransomware, siendo que pasaron unos meses antes de que sufriera un ataque otra institución pública, llegando así a la Caja Costarricense de Seguro Social (CCSS), el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICCIT), el Instituto Meteorológico Nacional (IMN), Radiográfica Costarricense (RACSA), la Refinadora Costarricense de Petróleo (Recope), etc.

2.3.2 Dos años después, ¿Cómo se ha preparado el país para enfrentar futuras amenazas?

Las compañías costarricenses tanto instituciones públicas y privadas, son el máximo exponente de la confianza en el importante juicio crítico de la seguridad cibernética del país, esta gran sensibilidad que poseen le ha proporcionado a una asignación más robusta de recursos financieros para fortalecer las defensas cibernéticas para el ámbito de las instituciones gubernamentales y empresas privadas del país. De entre las acciones que se añadirán con una cierta confianza, se incluirán las siguientes: la implementación de medidas de control más estrictas que limiten el

acceso a información sensible por parte de los usuarios autorizados de las organizaciones, el uso de métodos de autenticación multifactor (MFA/2FA), la puesta en marcha de protocolos de acceso que se alineen con los estándares y buenas prácticas de seguridad, la implementación de tácticas de defensa específicas para hacer frente a los ataques de ransomware, visto que son muchos los puntos de los que tienen que hacer más de una vez hincapié en la integridad absoluta de los datos en distintas áreas vulnerables como correos electrónicos, perímetros de red y estaciones de trabajo.

Cada una de estas estrategias de defensa incluyen la adopción de soluciones sofisticadas en la detección de amenazas que se fundamentan en inteligencia artificial y machine learning, así como la adopción de una próxima generación de firewalls que incorporan capacidades de deep packet inspection, así como análisis del comportamiento de la red.

No obstante, lo conseguido hasta el presente, la primera línea es la obligación de tener un punto de vista que sea continuo en la creación de la ciberseguridad. Esto significa una dedicación todavía existencial a la formación del personal en las prácticas del sector y la cultura de la ciberseguridad, con la inclusión del recorrido de técnicas como las técnicas de análisis forense y los procedimientos de respuesta a incidentes.

Ilustración 8: Riesgo Cibernético

Fuente: Redseguridad (s.f).

Recuperado de https://www.redseguridad.com/

2.4 Infraestructura Tecnológica

> La infraestructura de TI es todo lo que necesita para crear y ejecutar aplicaciones de software en una organización. Incluye hardware, componentes de red, su sistema operativo, almacenamiento de datos y varios tipos de software que una organización utiliza para prestar servicios de TI y ejecutar soluciones de software internas. Tradicionalmente, la administración de la infraestructura de TI era compleja debido a los requisitos de auto compra y a la fuerte inversión inicial. También tenía las complejidades del mantenimiento y las actualizaciones que tenían que realizarse internamente. Sin embargo, ahora contamos con la computación en la nube y los proveedores de nube de terceros pueden administrar completamente la mayoría de los requisitos de infraestructura de TI. Las organizaciones tienen la flexibilidad de elegir los componentes de infraestructura que desean comprar y los que desean usar como servicio. (Amazon Web Services, 2022, párrafo primero).

A partir de lo expuesto en la citada publicación, se puede obtener una visión nítida sobre la relevancia que tiene una infraestructura de TI para las empresas y cómo esta ha ido evolucionando en el tiempo. Además, en esta publicación se expresa la complejidad que representaba su gestión (de la infraestructura) tradicional, teniendo en cuenta los costos de adquisición iniciales y el mantenimiento, lo cual contrasta con la versatilidad que ofrece la computación en nube. Asi mismo, tiene interés el hecho de que los proveedores de nube permiten a las empresas poder optimizar los recursos de que disponen y la computación en nube fomenta un modelo que proporciona infraestructura como servicio que permite la reducción de los costos y, por lo tanto, la escalabilidad. Sin embargo, unido a lo anterior, hubiese estado bien mencionar respecto a algunos

retos asociados a este modelo, como la seguridad de los datos o la dependencia de terceros, para ofrecer una visión más equilibrada.

Ilustración 9: Infraestructura TI

Fuente: DatacenterDynamics (s.f).
Recuperado de https://www.datacenterdynamics.com/en/

2.4.1 ¿Cuáles son los componentes de una infraestructura de TI?

Tomando como referencia lo antes mencionado la infraestructura de TI es que el conjunto de hardware, software, redes y servicios conectados que componen el entorno de TI de una organización. Cada componente de la infraestructura de TI brinda diferentes servicios que contribuyen a la eficiencia general del sistema.

2.4.2 Componentes

Hardware de TI: Hace referencia a todos los dispositivos y máquinas físicas que una organización utiliza en su entorno de TI, los servidores y dispositivos de almacenamiento que brindan recursos de red a una empresa forman parte del hardware.

Software de TI: Una infraestructura de TI de software incluye sistemas operativos, bases de datos, servidores de aplicación, middlware, administración de relaciones con los clientes (CRM), sistemas de administración de contenidos, software de virtualización.

Infraestructura de red: Permite a las organizaciones conectarse a Internet y así poder establecer conexiones entre las diferentes oficinas o centros de datos. La infraestructura de red se utiliza para transmitir y recibir información a través de Internet, rede de área local (LAN), redes de área extensa (WAN), protocolos de red.

Centros de datos: Son ubicaciones físicas que almacenan una variedad de dispositivos de hardware en un lugar único y centralizado. Estos centros de datos requieren componentes físicos adicionales, como por ejemplo equipos de refrigeración y sistemas de seguridad.

Servicios en la nube: Hacen referencia a distintas plataformas que una empresa de terceros brinda a una organización, puede utilizar aplicaciones de software como servicio (SaaS) con la finalidad de eliminar la necesidad de aplicaciones locales.

Infraestructura de seguridad: Se utiliza para proteger, cifrar y salvaguardar los datos de una organización, los sistemas de autenticación, autorización, los sistemas de detección, prevención y los protocolos de cifrado pertenecen a esta categoría de seguridad.

2.4.3 Tipos de Infraestructura de TI

Infraestructura tradicional: La organización es la dueña de toda la infraestructura de TI que utiliza. Por lo tanto, tendrá toda su información en sus servidores ubicados localmente o en sus propios centros de datos. Con este método la empresa no utiliza servicios tercerizados y no tienen la propiedad de utilizar infraestructuras de otras compañías

Infraestructura en la nube: Hace referencia a los recursos y servicios adquiridos por medio de la computación en la nube. Pueden ser alquilados o prestados a través del Internet, la mejor forma de hacerlo es asociarse con algún proveedor de nube pública, el proveedor de la nube compra y da mantenimiento a toda la infraestructura de TI, mientras que la organización accede a ella mediante la virtualización.

Infraestructura híbrida: Este enfoque hace uso de los servicios en la nube para optimizar o cubrir cualquier brecha que se produzca. Se obtiene un entorno de TI que mezcla recursos de diferentes proveedores de nube y centros de datos propios locales que pueden satisfacer diferentes necesidades con eficiencia y de manera económica.

Ilustración 10: Infraestructura tradicional, nube e hibrida

Fuente: Ikusi (s.f).

Recuperado de https://www.ikusi.com/es/

2.5 Marcos, Estándares y Normas

2.5.3 ¿Qué es un marco de ciberseguridad?

> Un marco de ciberseguridad es, esencialmente, un sistema de estándares, pautas y buenas prácticas para gestionar los riesgos que surgen en el mundo digital. Por lo general, coinciden con los objetivos de seguridad de tu empresa, como evitar el acceso no autorizado al sistema con controles (como solicitar un nombre de usuario y contraseña). (Gutierrez, 2024, párrafo cuarto).

En virtud de lo anterior, los marcos de ciberseguridad abordan un enfoque de marco como las del aseguramiento a los activos digitales. El marco pretende dar a los gestores de la seguridad un tipo fiable y sistemático de reducir el riesgo cibernético, pese a lo complejo que sea el entorno. De forma general, los marcos de ciberseguridad son utilizados a menudo de forma obligatoria o, al menos, con grandes incentivos aquellas organizaciones que deben de cumplir una serie de regulaciones.

2.5.4 Marcos de ciberseguridad más conocidos

Existen muchos marcos distintos, sin embargo, unos pocos dominan el mercado.

- *Marco del Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU, para Mejorar la Ciberseguridad de la Infraestructura Crítica (NIST CSF).*

Está diseñado para proteger infraestructura crítica como plantas de energía y represas contras ataques cibernéticos. Sin embargo, sus principios pueden aplicarse a cualquier institución que busque mejorar su seguridad.

Este marco es bastante amplio y detallado, se basa en cinco funciones que siguen el patrón básico de defensa cibernética: **identificar, proteger, detectar, responder y recuperarse.** Proporciona un enfoque estructurado para identificar riesgos y activos de los que requieren protección, detectan amenazas, respondiendo a los riesgos incluso recuperando los activos en caso de un incidente de seguridad.

Un ejemplo bajo el patrón de "Proteger", el marco contiene una categoría que se conoce como PR.DS, ("Protect Data Security"), que incluye diferentes controles para proteger los datos en reposo (PR.DS-1), proteger los datos en tránsito (PR.DS-2), entre otras.

En esencia, el marco NIST organiza y estandariza las mejores prácticas de seguridad, facilitando su implementación en diversas industrias.

- *El Centro de Controles Críticos de Seguridad de Internet (CIS)*

Especialistas de ciberseguridad desarrollaron este marco a finales de la década de 2000 con el objetivo de proteger las empresas. Se compone de 20 controles que regularmente son actualizados por expertos de diferentes campos para adaptarse a las nuevas amenazas.

CIS funciona bien para organizaciones que desean dar pequeños pasos, su proceso de divide en tres fases progresivas: **básico, fundacional y organizacional,** lo que lo hace ideal para instituciones que buscan mejorar su seguridad. Además, es compatible con otros marcos como NIST e HIPAA, lo que facilita su integración en entornos con requisitos de cumplimiento específicos.

El marco CIS también proporciona puntos de referencia de seguridad, divididos en dos niveles:

1. **Nivel 1** – Configuraciones esenciales que garantizan seguridad sin afectar el rendimiento.
2. **Nivel 2** – Recomendaciones avanzadas que ofrecen mayor seguridad, aunque pueden impactar el rendimiento.

En general, CIS es una opción flexible y efectiva para mejorar la ciberseguridad sin requerir un gran nivel de inversión inicial.

- Los marcos de la Organización Internacional de Estándares (ISO) ISO/IEC 27001 y 27002

Es el estándar internacionalmente reconocido para la ciberseguridad, el marco establece las bases para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de una organización, el estándar ISO/IEC 270001 exige que las empresas gestionen de manera sistemática los riesgos de seguridad de la información, considerando amenazas y vulnerabilidades.

Es importante diseñar e implementar controles de seguridad de la información, que sean coherentes y efectivos para mitigar riesgos identificados, y el objetivo de estos controles es poder mitigar los riegos que fueron identificados, a partir de ahí, el marco sugiere que la organización adopte un proceso de gestión de riesgos que esté en curso.

Existen algunos otros marcos ya sea para una industria en específica o escenarios de seguridad.

- COBIT:
- HIPPA:
- LA NORMA GDPR de la UE

Los marcos de seguridad cibernética proporcionan una base para lograr una mejor postura de seguridad y evitar violaciones de datos. Poder adoptar un marco requiere dedicar tiempo y recursos al proyecto. El marco ofrece una forma organizada de darle seguridad a una organización y luego medir continuamente la efectividad de los controles de seguridad establecidos por el marco.

Ilustración 11: Diferencias entre la ISO 27001 y NIST CSF

ISO 27001 vs NIST CSF	ISO 27001	NIST CSF
Purpose	Designed as a formal standard that specifies compliance requirements	Designed as a guideline that offers best practices and additional resources
Requirements	Has 10 standard clauses that organizations must fulfill to build their ISMS	Has 6 functions that organizations can tailor to their cybersecurity programs
Controls	Has 93 controls grouped into 4 categories	Has 106 controls grouped into 22 categories
Compliance Process	Requires a full audit from a certification body	Involves self-assessment and does not require an external audit
Cost	The standard must be purchased for a fee	The framework can be accessed and utilized for free

Fuente: 6clicks (s.f).

Recuperado de https://www.6clicks.com/

3. Norma ISO/IEC 27002

> La norma ISO 27002 es un estándar internacional que proporciona directrices para la implementación de controles de seguridad de la información. A diferencia de la norma ISO 27001, que se centra en los requisitos para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI), la norma ISO 27002 actúa como un complemento a la norma ISO 27001. Un estándar que ofrece un conjunto detallado de directrices y mejores prácticas para implementar los controles de seguridad identificados en el Anexo A de la ISO 27001. Es una norma clave como recurso detallado para las organizaciones que buscan una guía sobre las mejores prácticas en seguridad de la información. (GlobalSuite, 2023, párrafo primero).

A partir de lo descrito, esta norma ISO 27002 es aplicable a todas las organizaciones, independientemente de su tamaño si es grande, mediana o pequeña empresa, tampoco el tipo o sector. Su objetivo es ayudar a las organizaciones en la elección e implementación de los diferentes controles de seguridad más adecuados, de acuerdo con los riesgos que enfrentan.

Dentro del documento oficial de la norma llamado “International Standard ISO/IEC 27002” “Seguridad de la información, ciberseguridad y protección de la intimidad – Controles de seguridad de la información”. tercera edición 2022-02, se presenta la versión actualizada la cual ha sido adaptada para enfrentar los retos actuales en la protección de la información y ha reducido el número de controles.

3.1 Controles

La estructura de la norma divide sus controles en 4 categorías principales.

3.1.1 Controles Organizacionales:

> El control expresa la política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal pertinente y las partes interesadas, y revisadas a intervalos planificados y si ocurren cambios significativos (27002, 2022).

El propósito principal de los 37 controles que los conforman es ofrecer un marco operativo para la protección de la información. Se enfocan en:

- Definición de estructuras de gobernabilidad y roles.
- Establecimiento de políticas claras.
- Fomento de una cultura de seguridad de la información.
- Asegurar el cumplimiento regulatorio.
- Gestión proactiva de riesgos.

3.1.2 Controles de Personas:

> Los controles de verificación de antecedentes de todos los candidatos a convertirse en personal deben realizarse antes de incorporarse a la organización y de forma continúa teniendo en cuenta las leyes, reglamentos y ética aplicables y ser proporcionales a los requisitos de la empresa, la clasificación de la información a la que se va a acceder y los riesgos percibidos. (27002, 2022).

Estos están conformados por 8 controles únicamente los cuales reconocen la importancia del factor humano en la seguridad de la información. Se centran en:

- Concientización y formación del personal.
- Establecimiento de procesos de reclutamiento seguros.
- Definición clara de responsabilidades en la contratación.
- Evaluaciones periódicas y disciplina en caso de incumplimientos.
- Protocolos de terminación de empleo que garantizan la continuidad de la seguridad.

3.1.3 Controles Físicos:

"Los procedimientos de funcionamiento de las instalaciones de tratamiento de la información deben estar documentados y disponibles al personal que las necesite" (27002, 2022).

La intención de estos 14 controles que los conforman es garantizar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información. Abordan:

- Salvaguarda de equipos y dispositivos.
- Protección de medios de almacenamiento.
- Seguridad de las instalaciones físicas.
- Medidas preventivas contra incidentes, ya sean naturales o intencionados.

3.1.4 Controles Tecnológicos:

"Debe diseñarse y aplicarse una protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras" (27002, 2022).

El propósito de los 34 controles que lo conforman es garantizar el ciclo de vida de la información, ayuda a las organizaciones a proteger su información de amenazas virtuales.

- Procesos seguros desde el diseño hasta la implementación de sistemas.
- Mantenimiento y configuración de redes.
- Monitoreo constante.
- Análisis y pruebas periódicas.
- Procedimientos de auditoría y recuperación en caso de incidentes.

A pesar de ofrecer 93 controles detallados, la norma ISO 27002:2022 enfatiza la adaptabilidad, permitiendo que las organizaciones escojan e implementen aquellos controles que mejor se alineen con sus necesidades. Es una guía, no un mandato, diseñada para ser lo más útil posible en la creación de sistemas de gestión de seguridad eficientes y efectivos.

Ilustración 12: División de controles

Fuentes: Global Trust Association (s.f).
Recuperado de https://globaltrustassociation.org/es/

3.2 Control de inteligencia de amenazas en ISO 27002:2022

El "control de inteligencia de amenazas" es uno de los nuevos controles de esta normativa, la cual es un componente crítico del programa de ciberseguridad de cualquier organización, esto permite a las organizaciones mantenerse actualizada sobre las amenazas emergentes.

La ISO/IEC 27002:2022 plantea que la información relativa a las amenazas de seguridad de la información debería ser obtenida y analizada para producir inteligencia de amenazas, con el fin de proveer de conocimiento a la organización del entorno de amenazas y tomar acciones apropiadas para su mitigación.

3.2.1 ¿En qué consiste la Inteligencia de Amenazas?

La Inteligencia de Amenazas se refiere al conjunto de acciones que una entidad lleva a cabo para recolectar y examinar datos acerca de los ataques presentes y potenciales amenazas que puedan impactar la seguridad de una organización y sus bienes.

Considerando lo anterior, podemos decir que es una medida de seguridad proactiva que previene ataques de seguridad y ahorra un costo económico importante para remediar un ataque o vulneración de la información.

3.2.2 ¿De qué manera es posible realizar la inteligencia de amenazas?

Una forma que podríamos utilizar para elaborar la inteligencia sobre amenazas es usando la medida denominada inteligencia de fuentes abiertas, que consiste en recolectar datos a partir de fuentes públicas y accesibles de forma gratuita.

Esto incluye, por ejemplo, sitios de interés de seguridad, medios de comunicación, redes sociales, así como los centros de análisis de la ciberseguridad que son patrocinados por el estado o empresas privadas.

Sin embargo, cosechar y analizar la gran cantidad de información disponible en internet sobre amenazas y ataques cibernéticos es una tarea muy ardua de realizar con estas herramientas de búsqueda, lo que requiere una cantidad considerable de tiempo y esfuerzo por parte de los profesionales de ciberseguridad, debido a esto, se ha desarrollado toda una industria de productos y servicios enfocados en ayudar a las organizaciones a producir y analizar informes o resúmenes de inteligencia sobre amenazas cibernéticas. Esto incluye productos de software, plataformas digitales, servicios en tiempo real y más.

3.2.3 Beneficios

La norma establece la necesidad de contar con un sistema de inteligencia de amenazas y ello tiene grandes beneficios, por ejemplo:

- Disminuye los riesgos en hackeos a bases de datos o centros de información sensible.
- Evitan las filtraciones de datos bloqueando direcciones IP sospechosas que podrían vulnerarlos.
- Reduce costos incluyendo elementos legales y multas además de los gastos de restablecimiento luego de un incidente de ciberseguridad.

Por todas estas razones anteriores es necesario poder implementar un correcto programa para la gestión de las amenazas a través de la inteligencia de amenazas.

3.3 Priorizar los controles tecnológicos basados en la ISO 27002

Recordemos que la ISO/IEC 27002 ofrece una amplia gama de controles de seguridad informática, el poder dar prioridad dentro de un departamento de tecnologías de información, dando un enfoque a los controles tecnológicos basados en la ISO/IEC 27002 podría ser un gran desafío, el cual requiere tener una dirección estructurada en el cual se consideren los riesgos, los recursos disponibles y cuáles son los objetivos de seguridad de la institución,

A continuación, se detallará una guía de procedimientos que nos ayudará poder lograrlo:

3.3.1 Identificar los activos y riesgos

Es importante poder identificar cuáles son los activos más críticos en el departamento de tecnologías de información, determinar los sistemas, aplicaciones, datos que son más valiosos y que requieren de mayor protección.

Es necesario también realizar un análisis de riegos para determinar las amenazas existentes y vulnerabilidades que puedan llegar afectar a los activos, en base con los riesgos clasificarlos según el impacto potencial y la probabilidad de ocurrencia.

Ilustración 13: Conceptos clave para análisis de riegos basado en activos

Fuente: Pirani (s.f).

Recuperado de https://www.piranirisk.com/

3.3.2 Madurez de la Organización

Se debe realizar un análisis actual de la infraestructura de departamento de TI con el objetivo de poder identificar las áreas de mejora o donde la protección de seguridad es más débil, enfocarlas para poder cerrar esas brechas.

Se debe considerar la complejidad de los controles, por lo que se recomienda implementar desde los controles más sencillos a los más complejos.

3.3.3 Selección de los controles tecnológicos de la ISO 27002

- 8.1 Dispositivos terminales de usuario: "Debe protegerse la información, procesada o accesible a través de los dispositivos de los usuarios." (27002, 2022, pág 81).
- 8.2 Derecho de acceso privilegiado: "La asignación y el uso de derechos de acceso privilegiados deben restringirse y gestionarse." (27002, 2022, pág 83).
- 8.5 Autenticación Segura: "Las tecnologías y procedimientos de autenticación segura deben aplicarse en función de las restricciones de acceso a la información y de la política específica del tema sobre control de acceso." (27002, 2022, pág 87).
- 8.7 Protección contra el malware: "La protección contra los programas maliciosos debe aplicarse y apoyarse en una concienciación adecuada de los usuarios." (27002, 2022, pág 90).
- 8.8 Gestión de vulnerabilidades técnicas: "Información sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas." (27002, 2022, pág 92).
- 8.10 Supresión de información: "La información almacenada en sistemas de información, dispositivos o cualquier otro medio de almacenamiento debe eliminarse cuando ya no sea necesaria." (27002, 2022, pág 97).

- 8.11 Enmascaramiento de datos: “El enmascaramiento de datos debe utilizarse de acuerdo con la política temática de la organización sobre control de acceso y otras políticas temáticas relacionadas, así como con los requisitos empresariales, teniendo en cuenta la legislación aplicable.” (27002, 2022, pág 98).
- 8.13 Respaldo de información: “Las copias de seguridad de la información, el software y los sistemas deben mantenerse y comprobarse periódicamente de acuerdo con la política específica acordada en materia de copias de seguridad.” (27002, 2022, pág 101).
- 8.17 Sincronización de relojes: “Los relojes de los sistemas de procesamiento de la información utilizados por la organización deben estar sincronizados con las fuentes de tiempo aprobadas.” (27002, 2022, pág 108).
- 8.19 Instalación de software en sistemas operativos: “Deben aplicarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.” (27002, 2022, pág 110).
- 8.20 Seguridad en las redes: “Las redes y los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información de los sistemas y aplicaciones.” (27002, 2022, pág 111).
- 8.21 Seguridad de los servicios de red: “Deben identificarse, aplicarse y controlarse los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.” (27002, 2022, pág 112).
- 8.22 Segregación de redes: “Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.” (27002, 2022, pág 113).

- 8.23 Filtrado Web: “El acceso a sitios web externos debe gestionarse para reducir la exposición a contenidos maliciosos.” (27002, 2022, pág 114).
- 8.25 Ciclo de vida del desarrollo seguro: “Deben establecerse y aplicarse normas para el desarrollo seguro de software y sistemas.” (27002, 2022, pág 117).
- 8.30 Desarrollo externalizado: “La organización debe dirigir, supervisar y revisar las actividades relacionadas con el sistema externalizado desarrollo.” (27002, 2022, pág 126).
- 8.31 Separación de los entornos de desarrollo, prueba y producción: “Los entornos de desarrollo, pruebas y producción deben estar separados y protegidos.” (27002, 2022, pág 127).

Ilustración 14: Controles tecnológicos ISO/IEC 27002

Fuente: Consultoría en Ciberseguridad

Recuperado de https://www.hkmexico.com/

3.3.4 Evaluar el Impacto y Viabilidad

Es importante realizar una priorización de aquellos controles que mitiguen los riegos con mayor impacto en la institución, así como una evaluación económica considerando el costo de implementación, tiempo y recursos humanos necesarios para poder cumplir con cada uno de los controles seleccionados.

Es importante también calcular el beneficio a corto y largo plazo que cada control aportará a la organización.

3.3.5 Establecer un Plan de implementación

Es posible afirmar que en este punto radica la necesidad más vital para asegurar el éxito de cualquier proyecto de seguridad de la información, una organización con un desarrollo de un plan de implementación adecuado y coherente puede proporcionar a las organizaciones la mejora radical de su postura de seguridad y la capacidad de cumplir con los requisitos de la ISO 27002. Algunas de las ventajas que se pueden mencionar son la mayor eficiencia que alinea los esfuerzos, la disminución de costos que evita la duplicación de esfuerzos y optimiza el uso de recursos y una gestión eficiente del tiempo lo que facilita el cumplimiento de los plazos establecidos y con una implementación efectiva de los controles de seguridad garantiza un aumento de la seguridad.

Partiendo de lo indicado podemos construir el plan de implementación de la siguiente manera:

- ✓ Fases de implementación: Dividir la implementación en fases, comenzando por los controles que aborden los riesgos más críticos.
- ✓ Cronograma: Definir plazos realistas para la implementación de cada control.

- ✓ Responsabilidades: Asignar roles y responsabilidades claras dentro del departamento de TI.

3.3.6 Integrar los controles en los procesos existentes

- ✓ Procedimientos y Políticas: Modificar las políticas de seguridad para incorporar los controles recientes.
- ✓ Automatización: Emplear instrumentos tecnológicos para automatizar controles como la administración de actualizaciones de seguridad, monitoreo de redes y detección de intrusiones.
- ✓ Capacitación: Formar al personal del departamento de TI en la implementación y mantenimiento de los controles.

3.4 Desarrollo de un plan de seguridad informática

En este sentido, en esta etapa, es crucial establecer un marco sólido y preventivo que garantice la protección de los activos digitales de cualquier entidad. Así, el plan de seguridad informática debería ser parte crucial de Ciberseguridad en cada organización para estar informado sobre las amenazas emergentes y ser proactiva.

Para desarrollar este plan, los siguientes pasos y puntos de vista, basados en ISO / IEC 27002 y otras fuentes, serían viables.

Análisis de la situación actual: Evaluación de la infraestructura tecnológica actual en busca de brechas y debilidades de seguridad.

Identificación de controles tecnológicos: Identificación de los controles tecnológicos de acuerdo con la norma ISO 27002, que mejorarán la detección de vulnerabilidades.

Priorización de controles tecnológicos: Se priorizan los controles tecnológicos identificados de acuerdo con la norma ISO 27002.

Uso seguro y aplicación de políticas: Asegurar el uso seguro y la aplicación de políticas de los recursos y activos bajo la norma ISO 27002.

Propuesta de implementación: Desarrollar una propuesta de implementación del plan de seguridad informática.

Fases de implementación: Dividir la implementación en fases, comenzando por los controles que aborden los riesgos más críticos.

Cronograma: Definir plazos realistas para la implementación de cada control.

Responsabilidades: Asignar roles y responsabilidades claras dentro del departamento de TI.

3.4.1 Actividades

Entre las actividades que podemos incluir dentro del plan estratégico de Seguridad Informática y que se relacionan con los controles seleccionados de la norme ISO 27002 tenemos.

3.4.2 Gestionar la seguridad de endpoint:

- Establecer bloqueo de sesión tras inactividad en PCs, móviles y sistemas críticos.
- Aplicar políticas de seguridad en USB, Bluetooth y puertos de red.
- Usar BitLocker, FileVault o cifrado en discos y dispositivos móviles.
- Implementar MDM (Mobile Device Management) para gestionar y bloquear equipos de forma remota.
- Evaluar Firewall de aplicaciones.
- Actualización de inventario de infraestructura crítica.

- Actualización y envío de indicadores de compromiso de ciberseguridad.
- Revisión sobre las conexiones de VPN del usuario final.
- Validar que exista un inventario de usuarios genéricos y de servicios, así como los controles aplicables.
- Evaluación del esquema de respaldos de la empresa.
- Validar el nivel de actualización de los elementos de infraestructura crítica.
- Validar que existan lineamientos establecidos para regular el acceso remoto
- Implementar VPN con MFA para conexiones remotas.
- Usar cifrado TLS/SSL para proteger el tráfico de datos.
- Registrar accesos remotos en SIEM/logs de seguridad.
- Validar los controles de seguridad implementados para el teletrabajo.
- Validar las medidas de protección física para los equipos de usuario final.
- Validar la seguridad en el borrado de información de equipos de usuario final, a su salida del sistema.
- Validar el cifrado de los equipos portátiles.
- Encriptar la información almacenada de acuerdo con su clasificación.

3.4.3 Gestionar la seguridad de la red y las conexiones.

- Configurar los sistemas operativos de forma segura.
- Hardening Servidores.
- Hardening Equipos de Usuario Final.
- Hardening Equipos de Seguridad.
- Hardening de equipos de telecomunicaciones.

- Garantizar que las políticas en los equipos de seguridad se encuentren alineadas con las necesidades del negocio. Revisión de los equipos de seguridad. Evaluar configuración, políticas y salud de los equipos.
- Encriptar la información en tránsito de acuerdo con su clasificación.
- Aplicación de pruebas de vulnerabilidad internas y externas.
- Verificar que los controles permitan que solo los dispositivos autorizados tengan acceso a la información corporativa.
- Validar si los proveedores externos que tienen conexión VPN se encuentran activos.
- Revisión de usuarios y perfiles en sistemas externos.
- Validar el funcionamiento de herramientas para la distribución de actualizaciones en servidores y usuarios finales.
- Elaborar un inventario de puertos de la infraestructura crítica.
- Verificar técnicamente que las VLANs y las ACLs se encuentran funcionando correctamente.
- Establecer y mantener una política para la seguridad de la conectividad con base en las evaluaciones de riesgo y los requisitos del negocio.
- Validar la aplicación de pruebas de penetración periódicas para determinar la idoneidad de la protección de la red.

3.4.4 Gestionar la identidad del usuario y el acceso lógico

- Realizar una revisión de los usuarios activos en el AD vs planilla.
- Validar el esquema de administración de derechos de acceso a los sistemas principales.
- Revisión de usuarios activos en infraestructura crítica.
- Validación de control de medios de removibles USB

-Utilización de dispositivos autorizados.

-Medios cifrados.

-Verificar que medios de almacenamiento no se hayan perdido.

- Validar que exista un registro de auditoría del acceso a la información dependiendo de su sensibilidad y de los requisitos regulatorios.
- Identificar de forma unívoca y por roles funcionales todas las actividades de procesamiento de información.
- Validar y gestionar activamente cuentas de usuario privilegiadas.
- Supervisar las acciones realizadas por las cuentas de usuario privilegiadas.
- Autenticar todo el acceso a activos de información de acuerdo con el rol del individuo o a las reglas del negocio.
- Verificar que sea posible la identificación de todos los usuarios en los sistemas principales de la organización.

3.4.5 Gestionar el acceso físico a los activos de TI

- Validar el esquema de revisión de logs de usuarios privilegiados.
- Aplicación de pruebas de conexión mediante herramientas como LogmeIn y Teamviewer.
- Evaluación física del centro de datos.
- Respaldo de configuración de infraestructura crítica.
- Emitir alertas de seguridad en tiempo real sobre modificaciones de la base de datos. Estas alertas deberán ser validadas por Auditoría Interna.
- Aplicación de pruebas de ingeniería social.
- Diseño y actualización de Diagrama de la Red.

- Validar si existen REDIRECT en el correo de Office365 a correos externos o no autorizados.
- Registrar a todos los visitantes al sitio, incluidos contratistas y proveedores.
- Concienciación de la seguridad de la información física de forma regular.
- Verificar perfiles de acceso de las instalaciones de TI.
- Garantizar que los perfiles de acceso permanezcan actualizados.
- Gestionar solicitudes para permitir el acceso debidamente autorizado a las instalaciones de cómputo.
- Requerir a los visitantes que estén acompañados en todo momento durante su estancia en las instalaciones.

3.4.6 Proteger contra software malicioso

- Revisar y evaluar la información sobre nuevas amenazas potenciales.
- Análisis y aplicación de alertas de ciberseguridad del MICITT.
- Validar que los equipos de usuario final y servidores se encuentren con herramientas de antimalware actualizado.
- Validar el filtrado de tráfico hacia internet de las estaciones de usuario final y servidores.
- Revisar los perfiles de navegación en equipos de usuario final y servidores.
- Validar que los controles de protección antimalware de Office365 estén funcionando de manera adecuada.
- Enviar mensajes de concientización sobre software malicioso.
- Validar que todo el personal se encuentre capacitado sobre software malicioso.
- Validar controles de acceso remoto para proveedores.

3.4.7 Gestionar documentos sensibles y dispositivos de salida

- Hay que asegurar que se han establecido controles criptográficos para proteger información sensible almacenada electrónicamente.
- Validar la asignación de privilegios a los documentos sensibles y formularios especiales, basado en el menor privilegio.
- Inventario de documentos sensibles y dispositivos de salida y realizar reconciliaciones periódicas.
- Establecer salvaguardas físicas adecuadas para documentos sensibles.

3.4.8 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad

- Identificar vulnerabilidades de seguridad de la información.
- Definir y comunicar escenarios de riesgo para que se puedan reconocer con facilidad y se pueda entender su probabilidad e impacto.
- Garantizar que se creen tiquetes relativos a incidentes de seguridad de forma oportuna cuando la monitorización identifique posibles incidentes.
- Revisar regularmente los logs de eventos para detectar posibles incidentes.
- Registrar eventos relacionados con la seguridad y conservar los registros durante el periodo de tiempo apropiado.

CAPÍTULO III: MARCO METODOLÓGICO

4.1 Tipo y enfoque de la investigación

En este capítulo se especificará el tipo y el enfoque de la investigación, identificando las fuentes y los participantes que integrarán el estudio. Asimismo, se especificarán las estrategias y recursos utilizados para la recopilación de datos, garantizando su adecuación y eficiencia. Por último, se elaborará el diseño general de la investigación, utilizando los recursos más idóneos para asegurar los objetivos definidos en el proyecto.

4.1.1 Tipo de investigación

La investigación actual se enmarca en un tipo de estudio exploratorio y descriptivo, ya que se realiza cuando se desea investigar un tema novedoso o del cual hay escasa información. Asimismo, es útil cuando un objeto de estudio no está completamente bien definido.

En este contexto, un estudio exploratorio y descriptivo es fundamental para la investigación, ya que facilita una mayor comprensión de los factores que incluyen en el fenómeno y sus interacciones. Este método ofrece una base firme para reconocer patrones causales y, en consecuencia, formular propuestas fundamentadas que aborden de manera eficaz las necesidades identificadas.

Definición de la investigación exploratoria e investigación descriptiva

- Investigación exploratoria
    - "La investigación exploratoria tiene el objetivo de investigar y analizar información específica que no ha sido profundamente estudiada. Es decir, se encarga de tener un primer acercamiento para que posteriormente, se pueda hacer una investigación más detallada". (Software, 2024).

- Investigación descriptiva
    - “Se enfoca en realizar un informe detallado sobre el fenómeno de estudio, sus características y configuración. No le importan ni las causas, ni las consecuencias de este, solamente quiere tener una visión clara para entender su naturaleza”. (Software, 2024).

4.1.2 Enfoque de la investigación

El método empleado para la investigación es cuantitativo, puesto que se pretende conseguir datos exactos a través de técnicas estadísticas; se centra en la medición y evaluación de controles de seguridad y riesgos.

Esto permite evidenciar y documentar de manera clara cuales controles de seguridad se cumplen, cuales se cumplen de manera parcial y cuales no se cumplen. Este método es esencial para reconocer patrones, evaluar indicadores clave y hacer elecciones fundamentales con datos fiables. En síntesis, asegura una compresión clara y minuciosa de la situación actual en la implementación de los controles tecnológicos de la norma ISO/IEC 27002.

¿Qué es la investigación cuantitativa?

> La investigación cuantitativa es un método estructurado de recopilación y análisis de información que se obtiene a través de diversas fuentes. Este proceso se lleva a cabo con el uso de herramientas estadísticas y matemáticas con el propósito de cuantificar el problema de investigación. (Software, 2024).

Dicho lo anterior la investigación cuantitativa presenta una visión lineal, lo que implica que los elementos que constituyen el problema deben ser claros, limitados y tener un inicio definido. También es fundamental identificar el tipo de relación que existe entre esos elementos.

Este enfoque cuantitativo se utiliza para obtener resultados medibles para poder solucionar los problemas que estén afectando de manera directa el funcionamiento de una empresa o que básicamente no se esté cumpliendo con algún proceso.

Para que haya metodología cuantitativa, es necesario que haya claridad desde el inicio hasta el final de los elementos investigativos, tratando los datos de forma estática y otorgándoles un valor numérico a través de la estadística, con el objetivo de realizar inferencias.

4.2 Fuentes y sujetos de información

En esta sección se definen las fuentes y los sujetos de información, elementos fundamentales para respaldar tanto la teoría como la práctica de la investigación, garantizando un desarrollo apropiado.

Habitualmente, al llevar a cabo una investigación, se nota la falta de algunos datos que, en su tiempo no fueron registrados; por eso surge la necesidad de establecer métodos que hagan más sencilla su recolección.

Para tratar esta problemática, se utilizan varias fuentes y se colabora con un grupo determinado de individuos. El uso de métodos y recursos asegura la recolección de información sea clara, breve y exacta, favoreciendo el éxito del proceso de investigación.

4.2.1 Fuentes Primarias

Los datos de las fuentes primarias son información original, ya que provienen directamente de las personas involucradas en la investigación. Con esta información, se pueden obtener detalles muy concretos sobre los problemas presentes en la organización. A continuación, se muestra la definición de la investigación primaria.

> La investigación primaria es el proceso sistemático de recopilación directa de datos originales a partir de individuos, fuentes o fenómenos para abordar preguntas u objetivos de investigación específicos. Este enfoque de primera mano implica el diseño y la aplicación de métodos de investigación como estudios y entrevistas para generar insights únicos e información adaptada al área de investigación específica del investigador. (Kurfess, 2023)

En este trabajo de investigación la principal herramienta para la obtención de la información fue una entrevista, observación y cuestionario con el encargado del Dpto. Tecnologías de Información y encargado del área de Soporte Técnico de Comercial de Seguros Corredora de Seguros S.A.

4.2.2 Fuentes Secundarias

> Los datos de las fuentes secundarias son información que ya ha sido recolectada por una entidad y no constituyen datos de primera mano. Para entender de forma más clara qué son los datos secundarios, Jonathan Kurfess lo define de la siguiente manera.
>
> La investigación secundaria implica el análisis de datos existentes recopilados por otros.
>
> La investigación secundaria es útil para crear contexto, identificar tendencias y obtener insights de estudios anteriores. Sin embargo, la investigación primaria te ofrece insights únicos y un conocimiento de primera mano de tu tema. (Kurfess, 2023).

En resumen, es posible examinar fuentes secundarias, aunque no hayan sido recolectadas para este proyecto, siempre que el origen sea fiable, con el propósito de evitar que la información sea incierta. Así, se contaría con información procesada y con datos de primera mano para el análisis.

4.2.3 Sujetos de Información

Los sujetos de información son todas las personas que deben ser tomadas en cuenta para obtener datos y poder recolectar la información necesaria para esta investigación. En este proyecto, los informantes el jefe del área de tecnologías de información y el encargado de soporte técnico, ya que son ellos quienes tienen acceso a la infraestructura y a los datos reales de la empresa.

Los sujetos consultados para la investigación son los siguientes:

Tabla 1: Sujetos de Información

Puesto laboral	Profesión u oficio	Experiencia	Relación con el tema
Jefe Departamento TI	Ingeniero en Sistemas y responsable del Dpto. TI	4 años	Encargado de los procesos
Encargado Soporte Técnico	Estudiante Ingeniería encargado del área de Infraestructura del Dpto. TI	3 años	Encargado de la operativa

Fuente: Elaboración propia

4.3 Técnicas y herramientas de recolección de datos

En esta sección se señalan las técnicas que utilizaremos para obtener la información, así como los métodos o herramientas que emplean los investigadores para recolectar y almacenar toda la información de diversas fuentes. Esta es la base de la indagación para el correcto desarrollo del proyecto. Con estas herramientas combinadas se pretende conseguir la máxima cantidad de información y datos requeridos.

4.3.1 Entrevista

Es una técnica de investigación cualitativa que implica tener una conversación ya sea estructurada o semiestructurada entre el investigador y los participantes involucrados, con el objetivo de poder obtener información detallada y en profundidad sobre algún tema específico y que esté relacionado con la investigación.

En este proyecto utilizando la entrevista como técnica inicial para comprender que tan maduro se encuentra el departamento de tecnologías de información con relación a los controles tecnológicos de la Norma ISO/IEC 27002 en Comercial de Seguros Corredora de Seguros S, A, al ser una entrevista un medio de interacción nos permite tener una mejor interpretación con respecto al tema en el momento de realizarla, así como un panorama mucho más claro, información más precisa y concisa.

4.3.2 Observación

La observación radica en saber seleccionar todo aquello que realmente queremos analizar, se suele decir que “saber observar es saber seleccionar”.

Para la observación lo primero es plantear previamente qué es lo que interesa observar, en definitiva, es haber seleccionado un objetivo claro de observación.

> “La forma más común de observación en el contexto de la recolección de datos consiste simplemente en observar los comportamientos o acciones de un sujeto en un entorno específico para comprenderlos y registrar lo observado”. (Software, 2024).

El tema de la Ciberseguridad requiere un contacto constante con la infraestructura crítica y no crítica de la organización, ya que siempre se debe velar por la seguridad.

Se realizó una observación para tener un panorama del cumplimiento y no cumplimiento de si existe un plan estratégico de seguridad informática centralizándose en los controles tecnológicos en el Dpto. TI y de qué manera tienen integrados los mismos.

4.3.3 Cuestionario

El cuestionario es un recurso que nos proporciona un marco durante la entrevista a los individuos, puesto que seguimos un orden y lógica que fue previamente diseñado para obtener la información. Sin embargo, también podemos hacer uso de los cuestionarios de manera virtual o en línea, que nos faciliten poder alcanzar a una mayor población de interés.

Los cuestionarios son una parte fundamental de las encuestas, y debido a que son baratos de crear y responder, son una opción muy accesible tanto para los investigadores como para sus corresponsables o encuestadores.

Para crear un buen cuestionario es necesario considerar varios elementos como las preguntas adecuadas, la organización del cuestionario, a quién está dirigido y el método de aplicación de este.

4.4 Variables de investigación

Las variables constituyen elementos esenciales de la investigación que nos facilitan la medición y el análisis de datos. Se pueden describir como atributos o cualidades que pueden tener diferentes valores, también son un factor muy importante porque nos dan una visión de cada uno de los resultados obtenidos de un proyecto.

A continuación, se crea una tabla en la que se pueden observar las diversas variables objeto de análisis.

Tabla 2: Variables de investigación 1

Objetivo específico 1
Analizar la situación actual de la infraestructura tecnológica existente de la entidad con la finalidad en la detección de brechas y vulnerabilidades de seguridad presentes.
Variable
Determinar la situación actual
Conceptualización
Se refiere en poder determinar el estado actual de la seguridad informática, y los diferentes puntos de vulnerabilidades que puedan existir.
Operacionalización
Porcentaje de cumplimiento de los controles tecnológico de la norma ISO/IEC 27002, así como el nivel de riesgo de las vulnerabilidades identificadas (alto, medio, bajo). Estado de actualización de los sistemas operativos y aplicaciones.
Instrumentalización

Análisis de documentos como la revisión de políticas de seguridad, diagramas de red, registros de incidentes, etc. Entrevistas con el personal del departamento de TI para poder comprender la configuración y los procesos de seguridad.

Fuente: Elaboración propia

Tabla 3: Variables de investigación 2

Objetivo específico 2
Identificar los controles tecnológicos que cumplen con la seguridad informática según lo dicta la norma ISO 27002 así como un mejoramiento de los que detectan vulnerabilidades.
Variable
Cumplimiento de controles tecnológicos ISO 27002
Conceptualización
Implica evaluar la implementación y efectividad de los controles tecnológicos de seguridad informática en la entidad. Además**,** proponer mejorar en los controles existentes que se utilizan para detectar vulnerabilidades en la infraestructura tecnológica.
Operacionalización
Porcentaje de controles tecnológicos implementados y efectivos, número de vulnerabilidades detectadas antes y después de la mejora de los controles.
Instrumentalización
Auditoria de seguridad basado en la evaluación de la implementación de los controles tecnológicos de la norma ISO/IEC 27002, entrevista con el encargado del área de infraestructura para entender la implementación y el funcionamiento de los controles.

Fuente: Elaboración propia

Tabla 4: Variables de investigación 3

Objetivo específico 3
Realizar una priorización de cada uno de los controles tecnológicos seleccionados de la norma ISO 27002, incorporando actividades dentro del plan estratégico de seguridad informática y un proceso de auditoría.
Variable
Priorización de controles tecnológicos ISO 27002, integrando en el plan estratégico y proceso de auditoria
Conceptualización
Se refiere a determinar la importancia relativa de los controles tecnológicos de la norma ISO 27002 en función de su impacto en la seguridad informática de la entidad.
Operacionalización
El nivel de prioridad asignado a cada control (alto, medio, bajo), los criterios utilizados para la priorización (riesgo, impacto, recursos), y actividades específicas incorporadas en el plan estratégico**.**
Instrumentalización
Análisis de riesgos: identificación y evaluación de amenazas y vulnerabilidades, matriz de priorización donde se asignan los niveles de prioridad a los controles y definir un documento las actividades y los recursos.

Fuente: Elaboración propia

Tabla 5: Variables de investigación 4

Objetivo específico 4
Desarrollar un plan de seguridad informática que permita a Comercial de Seguros Corredora de Seguros S.A el uso seguro y aplicación de políticas de los recursos y activos bajo la norma ISO 27002.
Variable
Plan de Seguridad Informática basado en ISO 27002
Conceptualización
Se refiere a la elaboración de un documento estratégico que defina las políticas, procedimientos y controles necesarios para proteger los recursos y activos de la información de la entidad, que estén alineados con la norma ISO/IEC 27002.
Operacionalización
Elaboración y aprobación del plan de seguridad informática.
Instrumentalización
Plantillas para planes de seguridad informática

Fuente: Elaboración propia

Tabla 6: Variables de investigación 5

Objetivo específico 5
Desarrollar una propuesta de implementación del plan de seguridad informática que permita a Comercial de Seguros Corredora de Seguros S.A el uso seguro y aplicación de políticas de los recursos y activos bajo la norma ISO 27002.
Variable
Propuesta de implementación del plan de seguridad informática
Conceptualización

Se enfoca en la creación de un plan detallado y práctico para la ejecución del plan de seguridad informática previamente desarrollado.
Operacionalización
Porcentaje de actividades completadas según el cronograma de trabajo.
Instrumentalización
Elaboración de cronograma, encuestas de satisfacción

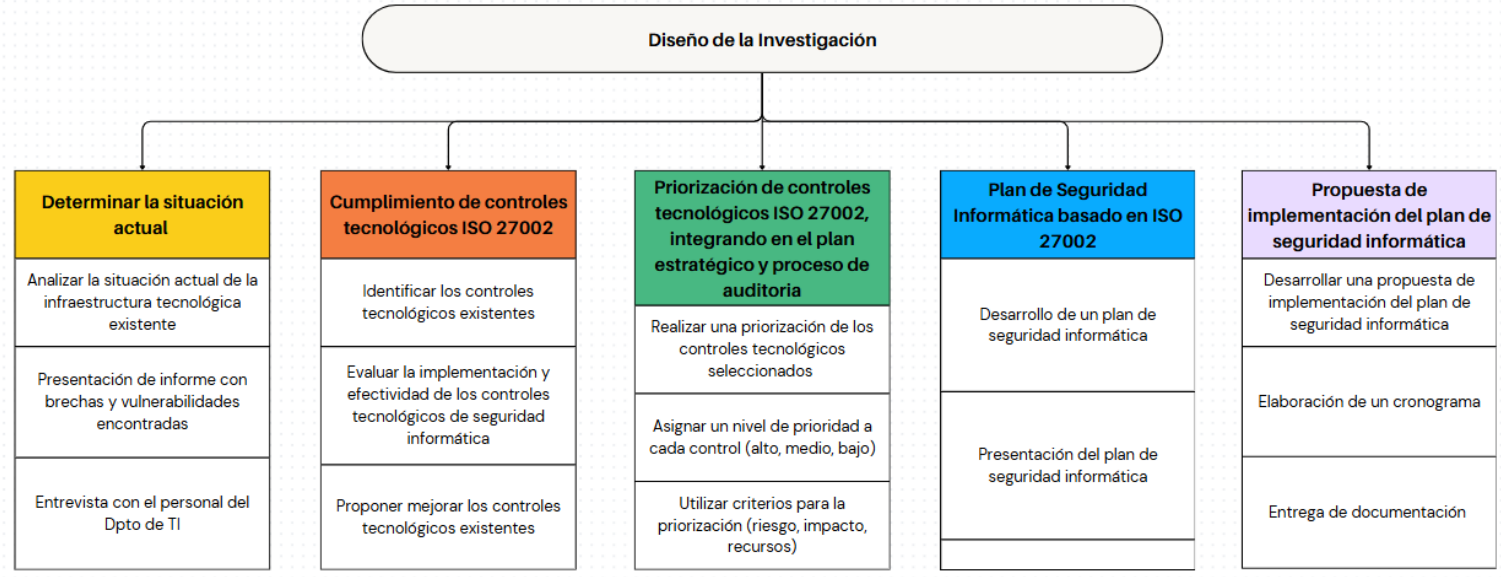
Fuente: Elaboración propia

4.5 Diseño de la investigación

En esta parte del proyecto se definen las etapas que componen el mismo, así también como se presenta cómo se llevará a cabo cada una de las fases de forma cronológica, con el fin de mantener una coherencia en el orden y la ejecución del proyecto.

Consiste en identificar, describir y explicar cómo implementar cada fase, lo que permite llevar una mejor administración y de manera controlada el proyecto, con lo anterior nos aseguramos del cumplimiento y objetivos establecidos.

Ilustración 15: Diseño de la Investigación



Fuente: Elaboración propia

4.5.1 Etapas del proyecto

- **Determinar la situación actual**

En esta primera etapa se buscar definir la problemática que se presenta en la organización Comercial de Seguros Corredora de Seguros S.A con respecto a la Ciberseguridad, poder realizar un análisis que permita detectar vulnerabilidades en los sistemas, configuraciones y procesos de seguridad. Así mismo facilitar la evaluación en el cumplimiento de estándares de seguridad como en este caso la norma ISO/IEC 27002.

En este punto también se incluyen la toma de decisiones informadas que proporcionen información precisa y actualizada para la toma de decisiones estratégicas en materia de Ciberseguridad, como también la priorización en los controles tecnológicos y recursos necesarios para mitigar los riesgos.

- **Cumplimiento de controles tecnológicos ISO 27002**

El objetivo en esta segunda etapa es poder realizar una evaluación del cumplimiento de los controles tecnológicos de seguridad informática según la norma ISO/IEC 27002, así mismo poder identificar y mejorar los controles existentes en la empresa para la detección de vulnerabilidades, evaluar su efectividad y buscar optimizar los mecanismos de estos controles dentro de la infraestructura tecnológica.

Con el cumplimiento de estos controles establece proteger la confidencialidad, integridad y disponibilidad de la información, lo que es crucial para evitar pérdidas de datos, fugas de información y otros incidentes de seguridad.

- **Priorización de controles tecnológicos ISO 27002, integrando en el plan estratégico y proceso de auditoria**

Esta parte es muy importante para maximizar la seguridad informática de una organización, muchas organizaciones tienen recursos limitados, por lo que priorizar permite enfocar aquellos recursos en los controles que ofrecen mayor protección contra los riesgos cibernéticos más significativos, además que se evita el desperdicio de tiempo y dinero en controles que tiene un impacto menor.

Es importante priorizar para abordar primero las vulnerabilidades y amenazas más críticas, lo que reduciría el riesgo general, permitiendo a la organización poder responder de manera más ágil y eficiente ante posibles incidentes de seguridad.

- **Plan de Seguridad Informática basado en ISO 27002**

El objetivo principal de esta etapa es que, mediante toda la información recopilada hasta este momento, poder elaborar un plan de seguridad informática basado en los controles tecnológicos de la norma ISO/IEC 27002 con el fin de poder aplicar mejores prácticas y mejorar la postura de seguridad en la organización, sin afectar la continuidad del negocio, operatividad y efectividad.

Dicho plan de seguridad informática debe ser presentado y aprobado por la jefatura del departamento de tecnologías de información con la finalidad de mantener un seguimiento y permitir al personal del Dpto. TI poder dar continuidad en el proceso de implementación, o los ajustes que conlleve.

- **Propuesta de implementación del plan de seguridad informática**

En esta fase examinaremos alternativas de implementación que se pueden ajustar a los requerimientos de la empresa.

Es fundamental comprender lo que necesita la empresa en este ámbito, ya que las pruebas pueden ser extensas y deben centrarse en herramientas de vigilancia, gestión de registros e indicadores de compromiso.

4.6 Matriz de coherencia

A continuación, la figura número 16 se presenta la matriz de coherencia elaborada según los objetivos del proyecto, dado que este debe cumplir con dichos objetivos.

Ilustración 16: Matriz de coherencia

Nombre del proyecto: AUDITORIA BASADA EN CIBERSEGURIDAD UTILIZANDO LA NORMA ISO/IEC 27002 PARA EL DESARROLLO DE UN PLAN ESTRATÉGICO DE SEGURIDAD INFORMÁTICA APLICANDO LOS CONTROLES TECNOLÓGICOS EN EL ÁREA DE INFRAESTRUCTURA DEL DEPARTAMENTO DE TI EN COMERCIAL DE SEGUROS CORREDORA DE SEGUROS, S.A EN EL PERÍODO 2025-2026 **Estudiante: Leonardo Solera Ovares**					
Objetivo	Entregable	Fase, parte o etapa de la metología del proyecto que posibilita la realización del entregable	Tecnicas metodos de recolección de información	Instrumentos	Temas relacionados para marco teórico
Desarrollar un plan estratégico de seguridad informática basado en los controles tecnológicos de la norma ISO 27002 permitiendo una reducción de los riesgos cibernéticos en el área de Infraestructura del Dpto. de TI en Comercial de Seguros Corredora de Seguros S.A y su continuidad del negocio durante el año 2025.					**Conceptos Fundamentales Seguridad de la Información, Ciberseguridad, Riesgos Cibernéticos.**
Analizar la situación actual de la infraestructura tecnológica existente de la entidad con la finalidad en la detección de brechas y vulnerabilidades de seguridad presentes.	Documento con el proceso actual identificando las vulnerabilidades en Ciberseguridad que tiene la organización	Identificación y diagnóstico	Reunión con el encargado del Dtpo.TI para el proceso actual	Microsoft Teams	**Conceptos Fundamentales Infraestructura Tecnológica, Amenazas, Vulnerabilidades, Riegos y Normativas.**
Identificar los controles tecnológicos que cumplen con la seguridad informática según lo dicta la norma ISO 27002 así como un mejoramiento de los que detectan vulnerabilidades.	Documento descriptivo del cumplimiento o no de cada uno de los controles tecnológicos basados en la ISO 27002.	Identificación de los controles tecnológicos	Entrevista con el encargado del Dpto. TI para analizar el cumplimiento o no de los controles tecnológicos	Herramientas de Office 365, Minutas de entrevistas	**Definición de la Norma ISO 27002, Controles de Seguridad, Relación entre la ISO 27002 y detección de vulnerabilidades.**
Realizar una priorización de cada uno de los controles tecnológicos seleccionados de la norma ISO 27002, incorporando actividades dentro del plan estratégico de seguridad informática y un proceso de auditoría.	Documento descriptivo con el nivel de priorización de cada control tecnológico de acuerdo a la metodología implentada.	Diseño de priorización	Análisis de cumplimiento y no cumplimiento	Metodología empleada, Matriz de riesgo	**Selección de controles tecnológicos, Alinear los controles de la ISO 27002 en el plan estratégico, utilizar un método de priorización de los controles.**
Desarrollar un plan de seguridad informática que permita a Comercial de Seguros Corredora de Seguros S.A el uso seguro y aplicación de políticas de los recursos y activos bajo la norma ISO 27002.	Desarrollo del plan de seguridad informática para los controles tecnologicos basados en la ISO 27002 que debe abarcar el Dpto. TI de la organización.	Desarrollo del plan estratégico	Reunión con especiastas en Ciberseguridad	Normativa ISO 27002 para determinar los controles tecnológicos de seguridad informática	**Concepto de un plan estratégico de seguridad informática, Desarrollo del plan de seguridad informática.**
Desarrollar una propuesta de implementación del plan de seguridad informática que permita a Comercial de Seguros Corredora de Seguros S.A el uso seguro y aplicación de políticas de los recursos y activos bajo la norma ISO 27002.	Desarrollo de documento con la propuesta de implementación del plan de seguridad informática para los controles tecnologicos basados en la ISO 27002.	Propuesta de Implementación	Análisis de los resultados del plan estratégico de seguridad informática	Guia de pasos para el cumplimiento de los controles	**Concepto e Implementación del plan de seguridad informática.**

Fuente: Elaboración propia

CAPÍTULO IV: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

En este capítulo se enfocará en el primer objetivo de este proyecto, el cual es analizar la situación actual de la infraestructura tecnológica existente de la organización, con el análisis obtendremos información sobre una mejor percepción de la empresa y los problemas existentes por falta de controles de seguridad, o malas prácticas.

El objetivo es proporcionar una información más detallada sobre el estado actual de la entidad y poder identificar de manera clara y precisa aquellas brechas o vulnerabilidades de seguridad presentes.

Para poder comprender este capítulo, el mismo se compone de 3 secciones:

- Diagnóstico Administrativo u Operativo.
- Diagnóstico Técnico
- Diagnóstico de Percepción

Con estos 3 diagnósticos se conseguirá información útil que permitirá mostrar un mejor detalle de lo existente, examinar sus características y lograr conclusiones entre lo anticipado y la realidad

5.1 Diagnóstico administrativo u operativo

Para comenzar este diagnóstico primer debemos comprender de qué trata esta sección, en la "Revista de Investigación Académica Sin Frontera" nos lo explica de la siguiente manera:

> Partir de un diagnóstico es una medida de control que permite llegar a un punto donde todos los procesos, eventos y documentos están justificados por sí mismos tanto los procedimientos como los requisitos son analizados a fondo para lograr un proceso administrativo eficiente. (García, 2022, p.1)

5.1.1 Procesos

Para establecer una línea base que permita evaluar la madurez actual de la organización en materia de gestión de seguridad de la información, se realizó un diagnóstico exhaustivo de los procesos administrativos y operativos existentes. Este análisis es fundamental para identificar las brechas entre el estado actual y los requisitos establecidos por la norma ISO/IEC 27001:2022 y los controles de la ISO/IEC 27002:2022.

El diagnóstico se llevó a cabo mediante:

- Entrevistas estructuradas con personal de infraestructura
- Revisión documental de procedimientos y políticas existentes
- Observación directa de prácticas operativas
- Análisis de la plataforma de gestión documental (intranet corporativa)

La organización cuenta con una estructura formal de gestión de procesos, donde se ha designado un responsable de procesos en la organización, algunas de sus funciones principales incluyen:

- Actualización continua.
- Gestión de la intranet corporativa.
- Coordinación con áreas.
- Capacitación y divulgación.

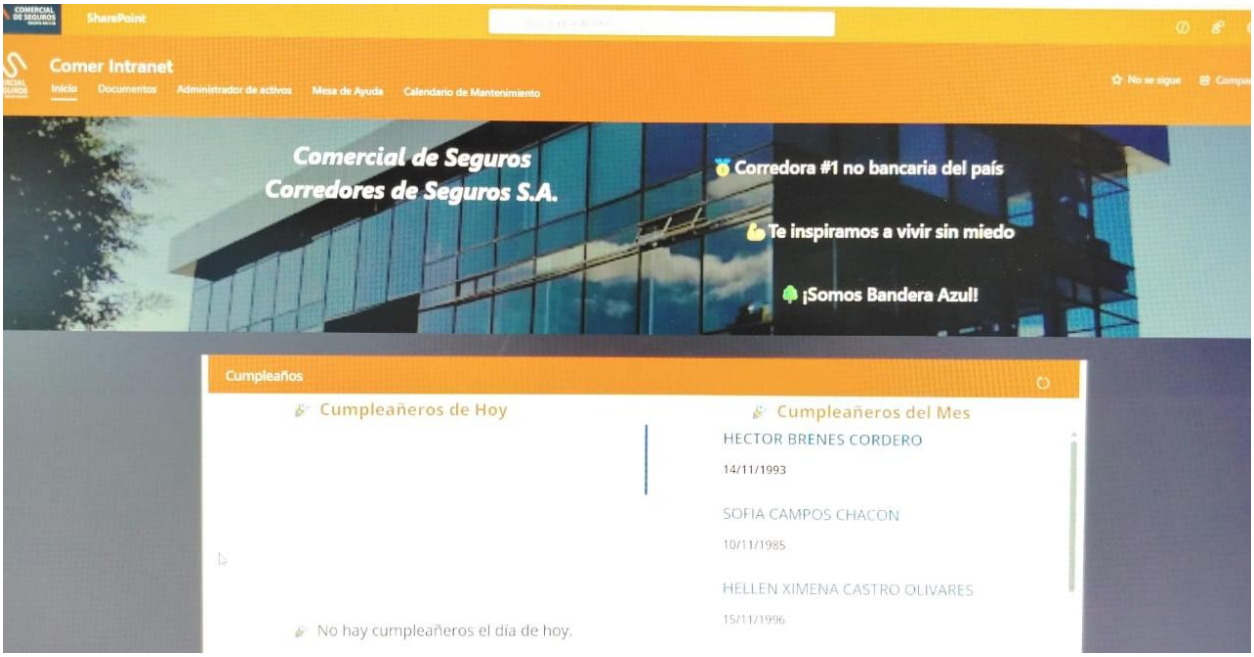
La organización también utiliza una **intranet corporativa** como repositorio centralizado de información organizacional. Esta plataforma digital funciona como el sistema de gestión del conocimiento donde se almacenan y publican:

- Documentación de procesos.
- Políticas organizacionales.
- Documentación de referencia.

Esta intranet opera bajo un modelo de acceso abierto interno, donde toda la información pública es de dominio público dentro de la organización y una sección que es segmentada por los diferentes departamentos y que únicamente tienen acceso aquellos los colaboradores que forman parte de su respectiva área, la autenticación requiere acceso con las credenciales de Active Directory, lo que garantiza que únicamente el personal interno autorizado puede ingresar a la plataforma.

Ejemplo de la intranet **Pública** donde se carga toda aquella información que es de conocimiento para todo el colaborador interno, esta información de políticas, proceso se comparte la sección de "Documentos".

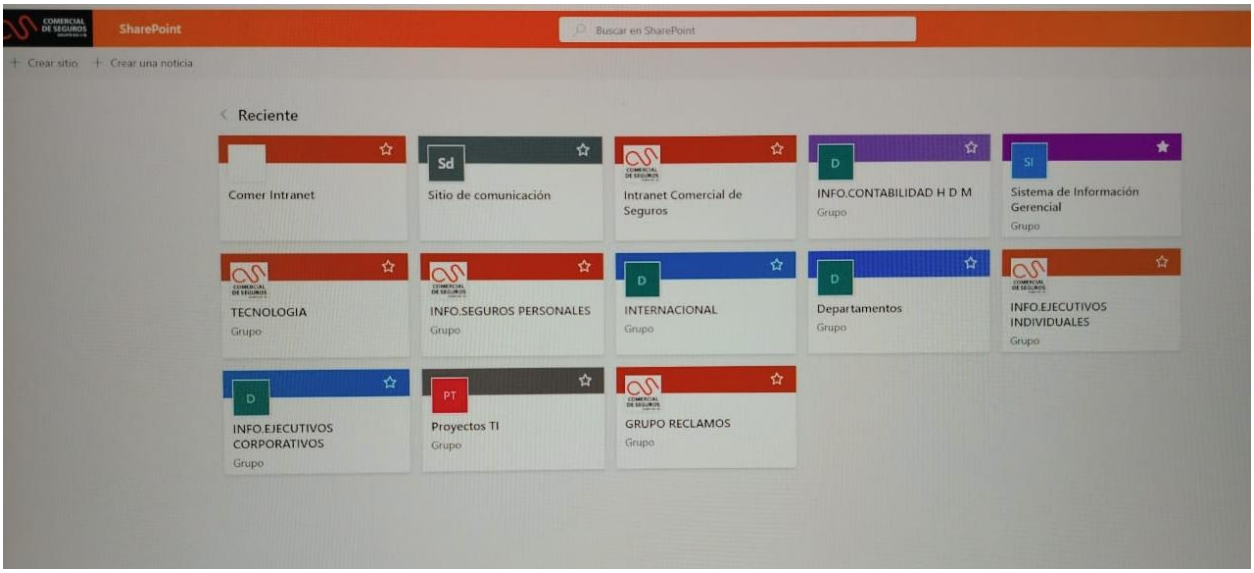
Ilustración 17: Intranet Pública Comercial de Seguros Corredores de Seguros.SA



Fuente: Elaboración propia

Ejemplo de la intranet **Privada** donde se encuentra toda aquella información segmentada por las diferentes áreas y con privilegios de acceso.

Ilustración 18: Intranet Privada Comercial de Seguros Corredores de Seguros.SA



Fuente: Elaboración propia

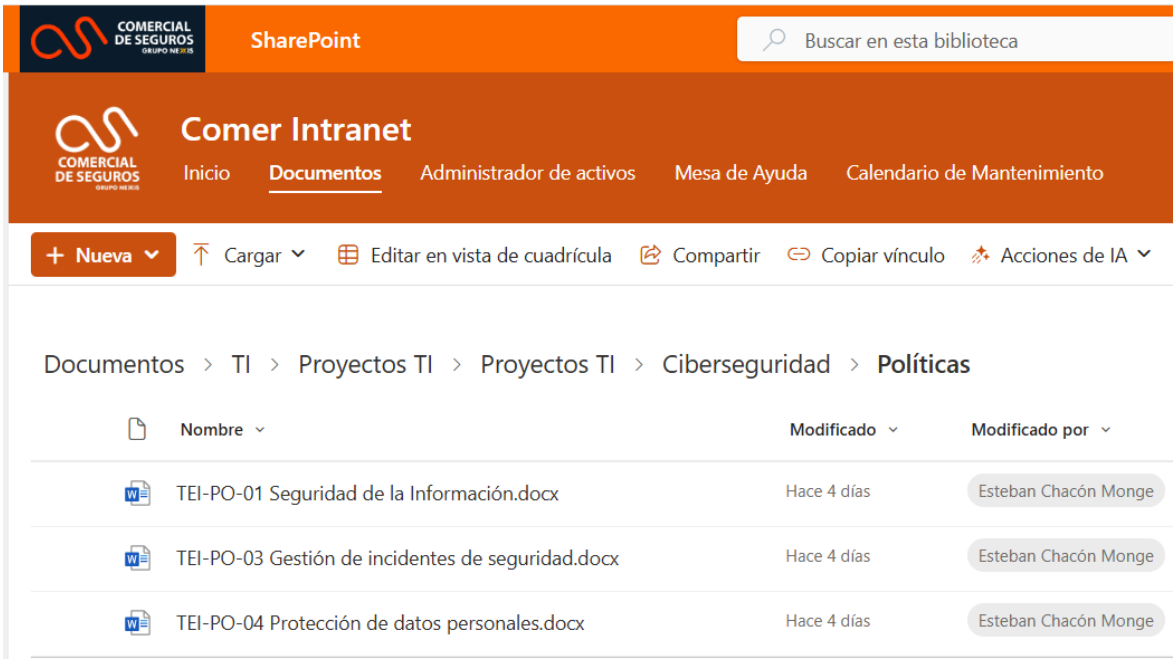
Actualmente la organización carece de documentación formal y políticas robustas en seguridad de la información, sin embargo, si cuentan dentro de la documentación de TI en Ciberseguridad algunas políticas y procesos tales como:

Políticas:

- ✓ TEP-PO-01 Seguridad de la información
- ✓ TEI-PO-03 Gestión de incidentes de seguridad
- ✓ TEI-PO-04 Protección de Datos Personales

Se adjunta evidencia:

Ilustración 19: Políticas de Ciberseguridad

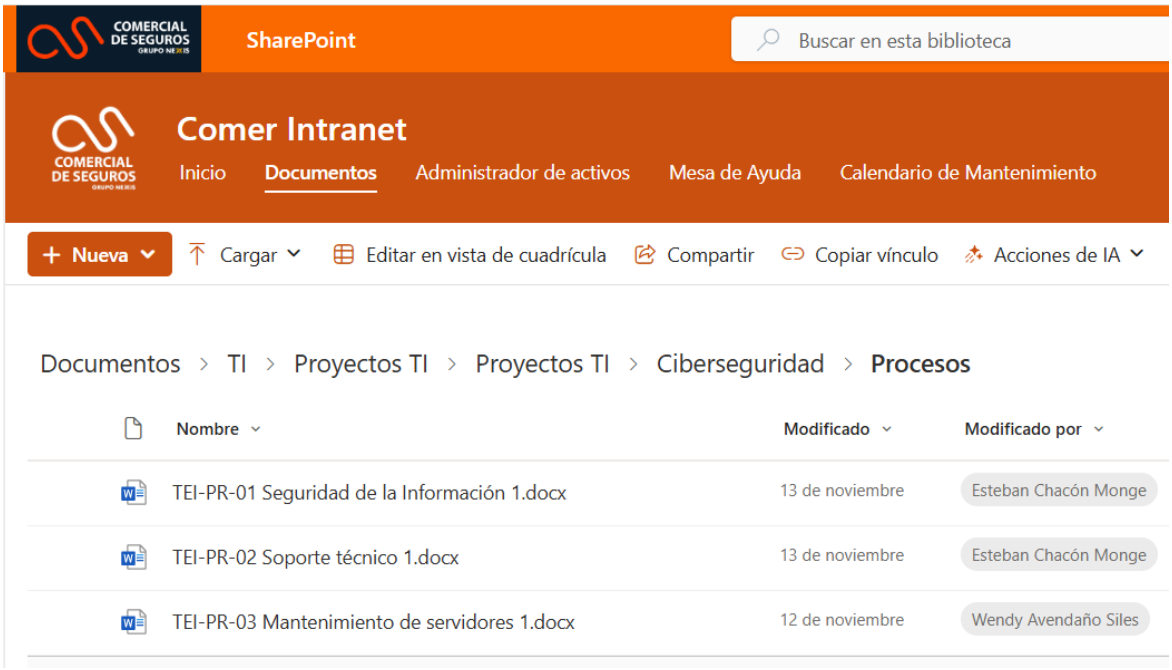


Fuente: Elaboración propia

Procesos:

- ✓ TEI-PR-01 Seguridad de la Información 1
- ✓ TEI-PR-02 Soporte técnico 1.
- ✓ TEI-PR-03 Mantenimiento de Servidores 1

Ilustración 20: Procesos de Ciberseguridad



Fuente: Elaboración propia

Para los dispositivos terminales de usuario final se cuenta con un inventario descriptivo en formato de Excel el cual lleva un registro detallado de cada dispositivo final asignado a los colaboradores. que incluye marca, modelo, serie, activo entre otra información.

Se adjunta ejemplo del documento en donde se muestra la información.

Ilustración 21: Inventario de activos

ACTIVOS INFORMATICOS COMERCIAL DE SEGUROS

#	MARCA	MODELO	SERIE	ACTIVO	NOMBRE DE EQUIPO	USUARIO	DEPARTAMENTO	FECHA DE COMPRA PORTATI	DAÑO EN VISAGAS
38	LENOVO	THINKBOOK 15 G2	MP25DLGC	*		BODEGA DE TI	INFORMATICA	12/10/2022	
49	CE2.0	Ethernet Service	*	*		EN RACK	INFORMATICA	*	
50	ECI	*	*	*		EN RACK	INFORMATICA	*	
72	NEXXT SOLUTIONS (8)	CL-130A	*	*		EN RACK	INFORMATICA	*	
47	Hitron (Modem)	CGN-1000	.251171039398	*		EN RACK	INFORMATICA	*	
48	PATTON (Modem)	RocketLink-G NTU	.70824009	*		EN RACK	INFORMATICA	*	
46	DINSTAR (Gateway)	MTG200	DA00-0030-1101-21	*		EN RACK	INFORMATICA	*	
51	Mikroyik router board	RB 3011 Ui AS-RM	E14C0D1E3296	*		EN RACK	INFORMATICA	*	
55	Fortigate	FG-100F	FG100FTK19004794	*		EN RACK	INFORMATICA	*	
45	Tesmart	HDMIKVMSwitch	Sin etiqueta	*		EN RACK	INFORMATICA	*	
121	**EQUIPO EXTERNO	*EQUIPO EXTERNO	*EQUIPO EXTERNO	*		DHIANCY CORDERO	INTERNACIONAL	*	
94	HDMI Matrix	*	*	*		BODEGA DE TI	INFORMATICA	*	
96	NAD	Stereo Receiver C 740	0257405428A	*		BODEGA DE TI	INFORMATICA	*	
76	TOSHIBA	Satellite C45-ASP4206FL	5D123325C	*		BODEGA DE TI	INFORMATICA	*	
38	DELL	(DellEMC)	TWORK1KTKST0016	**		EN RACK	INFORMATICA	*	
135	LENOVO	THINKPAD E470	PF0SDD60	ECO-002		JUAN CARLOS RODRIGUEZ	RT	*	
118	LENOVO	THINKPAD	PF16LT7L	ECO-006	CS-DIGI-CAROLIN	CAROLINA MORA	DIGITACION	*	
	LENOVO	THINKPAD E580	PF1C9XKW	ECO-009		DESECHO PROBLEMA DE PANTALLA	DESECHO	*	
98	HP	HP Pavilion 15 Notebook PC	5CD5143TYR	ECO-016		BODEGA DE TI	INFORMATICA	*	
90	DELL	Latitude E5530	FLSQTY1	ECO-021		BODEGA DE TI	INFORMATICA	*	
75	LENOVO	LENOVO Flex 2-15	WB15658722	ECO-024		BODEGA DE TI	INFORMATICA	*	
89	LENOVO	THINKPAD	*	ECO-028		BODEGA DE TI	INFORMATICA	*	
92	LENOVO	THINKPAD	PF-15J97N	ECO-029		BODEGA DE TI	INFORMATICA	*	
88	DELL	*	*	ECO-030		BODEGA DE TI	INFORMATICA	*	
	LENOVO	THINKPAD EDGE E540	CDSKTP0520	ECO-033		OFICINA DE TI (PARA RESPALDO DE CORREOS)	INFORMATICA	*	
131	LENOVO	THINKPAD E580	PF15JLOA	ECO-035		JOHANNA VALVERDE	RIEGOS DEL TRABAJO	*	
87	TOSHIBA	Satellite C55-B5214KL	9E201281P	ECO-040		BODEGA DE TI	INFORMATICA	*	
86	LENOVO	THINKPAD	*	ECO-048		BODEGA DE TI	INFORMATICA	*	
85	TOSHIBA	Satellite C55-C5219K	7F086716C	ECO-056		BODEGA DE TI	INFORMATICA	*	
84	LENOVO	LENOVO Flex 2-15	WB15659366	ECO-059		BODEGA DE TI	INFORMATICA	*	
74	LENOVO	LENOVO G510s Touch	CB28919564	ECO-061		BODEGA DE TI	INFORMATICA	*	
82	LENOVO	THINKPAD	*	ECO-064		BODEGA DE TI	INFORMATICA	*	

Fuente: Elaboración propia

Una brecha identificada es la falta de cifrado completo de los discos duros y no cuentan con protección física de ninguno de los dispositivos de usuario final. Por lo que dentro de la propuesta se recomienda de manera obligatoria el uso de candados de seguridad y el cifrado de todos los dispositivos tanto de usuario final, memorias USB, discos externos que utilicen dentro de la organización.

Para el control de acceso privilegiado se realizan revisiones esporádicas en algunos casos, pero sin registros completos, existe un control en la asignación de privilegios, pero sin ningún tipo de herramientas, tampoco se realizan revisiones formales de accesos privilegiados y presentan ausencia de registros centralizados de accesos. Dentro de la propuesta se incluyen recomendaciones y herramientas para su cumplimiento.

Con lo que respecta a la instalación de software o aplicativos en los equipos, es importante mencionar que únicamente el personal con privilegios de administrador elevados puede realizar este tipo de tareas.

Para el control de la autenticación segura se establece dentro de la política establecida **"TEP-PO-01 Seguridad de la información"** que hace hincapié al proceso **"TEI-PR-01 Seguridad de la Información 1"** en donde se mencionan los requisitos de complejidad que deben de cumplir para la implementación de contraseñas robustas.

Una de las brechas identificadas es la ausencia del MFA en sistemas críticos y cuentas administrativas, por lo que dentro de propuesta se incluyen recomendaciones para la implementación del doble factor de autenticación y alertas automatizadas de seguridad.

Para la protección contra el malware la organización cuenta con una plataforma de seguridad llamada **Sophos Intercept X** a pesar de ser una licencia empresarial se reporta que presenta muchas desventajas en los equipos, por ejemplo:

- Consumo de recursos: Los colaboradores se quejan de que el agente de manera muy frecuente consume bastante CPU y memoria en los equipos.
- Rendimiento percibido lento: Se mencionan reportes de congelamientos de Pc's tras alguna actualización de algún componente de Sophos.
- Dificultades con exclusiones: Algunos usuarios reportan que el agregar exclusiones por ejemplo carpetas o algún proceso, no funcionan como esperaban, lo que puede bloquear aplicaciones legítimas, de confianza y afectan los flujos de trabajo.
- Integración con ecosistemas externos: Al dentro del ecosistema Sophos, muchas veces no se logran integrar de manera correcta con herramientas de seguridad de terceros.

- Controles limitados en detección de software no autorizado y falta de revisiones periódicas del sistema.

Se estarán incluyendo más adelante dentro del capítulo V recomendaciones para este control.

Para la gestión de vulnerabilidades técnicas no cuentan con ningún programa de gestión para la aplicación de parches de seguridad, la falta de escaneos regulares y pruebas de penetración se efectuaron hace más de 3 años por lo que ya es recomendable realizar este proceso nuevamente. Se incluirán dentro de la propuesta diferentes recomendaciones para mitigar el riesgo al cumplimiento de este control.

Para el control de respaldo de información se efectúan backups de manera correcta mediante procesos automatizados ya establecidos, el cual utilizan la herramienta de Windows Server Backup para los respaldos de servidores de Active Directory, de los cuales se almacenan en un dispositivo NAS, para lo que son los servicios en la nube utilizan AWS Backup. Sin embargo, la empresa carece de procedimientos formales bien documentados para procesos de recuperación, la NAS local no cuenta con redundancia y el cifrado es insuficiente para los respaldos.

Se identificó una brecha con la documentación de la infraestructura de red, ya que la organización cuenta con un diagrama de red, pero el mismo se encuentra incompleto y no actualizado, con la segregación de redes se cumple de manera parcial por lo que dentro de la propuesta se incluirá algunas recomendaciones para reforzar este control en la segmentación formal y también la necesidad de reforzar controles en las redes inalámbricas.

A nivel de controles de filtrado web la empresa cumple con este control estableciendo diferentes niveles de navegación de acuerdo con el rol de cada uno de los colaboradores, sin embargo, se debe reforzar algunas funcionalidades avanzadas de filtrado.

La organización también cuenta con diferentes entornos de separación de desarrollo, pruebas y producción de manera correcta.

Se incluirá dentro de la propuesta una recomendación de herramientas para el acceso remoto seguro a proveedores ya que carecen de esta.

5.2 Diagnóstico técnico

Para llevar a cabo esta sección, primero necesitamos comprender cuál sería su objetivo:

En este caso consiste en un análisis detallado y sistemático de cada uno de los elementos y servicios de la infraestructura tecnológica vigente. Este procedimiento pretende reconocer las fortalezas, debilidades, oportunidades de mejora y posibles inconvenientes. La meta es comprender de qué manera la infraestructura tecnológica existente influye en la eficacia, la seguridad y los objetivos de empresa, permitiendo así la toma de decisiones fundamentadas para mejorar su rendimiento y prever inversiones futuras.

5.2.1 Infraestructura digital

Con el propósito de comprender el entorno tecnológico actual de la organización y disponer de una visión integral de su infraestructura digital, se realizó un levantamiento de información técnica que abarca servidores, sistemas operativos, conectividad, equipamiento de red, personal técnico y mecanismos de respaldo de información.

1. Servidores y Sistemas Operativos

La organización cuenta con un total de ocho (8) servidores, de los cuales siete (7) operan bajo el sistema **Windows Server 2022 Standard** y uno (1) utiliza **Linux**. Esta infraestructura permite la ejecución de los principales servicios institucionales, tales como:

- **Active Directory (AD)**, Servicio de directorio que gestiona la autenticación centralizada de usuarios, políticas de seguridad (GPOs), control de acceso y administración de recursos de red. Es el componente central de la infraestructura de identidad y representa un activo crítico.
- **Servidor de Base de Datos**, Aloja las bases de datos transaccionales que soportan el sistema CORE y otras aplicaciones empresariales. La disponibilidad e integridad de este servidor es fundamental para la continuidad operativa.
- **Azure**, Servicios de Azure integrados con el directorio activo local (Azure AD Connect - híbrido) y uso de Azure para servicios de colaboración (Microsoft 365, SharePoint, Exchange Online)
- **Sistema Core**, Ejecutan el sistema CORE y otras aplicaciones de negocio críticas que procesan información sensible de clientes y operaciones diarias.

2. Personal Técnico

El equipo de tecnología de la información está conformado por cinco (5) colaboradores, quienes se encargan de la administración, mantenimiento y soporte de los sistemas, servidores y servicios de red. Este recurso humano resulta fundamental para garantizar la disponibilidad, continuidad y seguridad operativa de la infraestructura tecnológica.

3. Conectividad a Internet

La organización dispone de dos enlaces de Internet provistos por **Telecable**, que garantizan redundancia y continuidad del servicio:

- **Enlace principal:** 600 Mbps por fibra óptica.
- **Enlace secundario (Backup):** 300 Mbps mediante antena inalámbrica.

Esta configuración permite mantener la conectividad incluso ante fallos del enlace principal.

4. Equipamiento de Red y Seguridad

En cuanto a la infraestructura de red, la empresa cuenta con:

- **1 Firewall Fortinet**, encargado de la seguridad perimetral y filtrado de tráfico.
- **2 Routers**, que facilitan la interconexión de redes internas y externas.
- **1 Switch Aruba**, utilizado para la distribución del tráfico interno.

Estos dispositivos conforman la base del esquema de comunicaciones internas y externas, asegurando un flujo eficiente y seguro de datos.

5. Respaldo y Recuperación

La organización mantiene políticas de respaldo tanto en infraestructura local como en la nube:

- Los servidores Windows utilizan **Windows Server Backup**, con almacenamiento en una **NAS** (Network Attached Storage).
- Los servicios en la nube cuentan con protección mediante **AWS Backup**, lo que permite mantener copias de seguridad automatizadas y seguras.

Este enfoque híbrido proporciona resiliencia ante pérdidas de información y contribuye a la continuidad operativa.

5.3 Diagnóstico de percepción

La percepción es el proceso mediante el cual los seres humanos interpretan y organizan la información que reciben del entorno. Se trata de decodificar los datos que son captados a través de los sentidos e interpretarlos para poder operar con ellos.

Para entender el cumplimiento o no de cada uno de los controles tecnológicos, se realizó una tabla con la siguiente información recolectada durante la entrevista.

Durante la recolección de información para este proyecto se utilizó la técnica de una entrevista de forma virtual, con el encargado del área de Infraestructura Tecnológica Oscar Esteban Chacon

Monge, en donde se expresó la necesidad del desarrollo de un plan de seguridad informática para los controles tecnológicos basados en la ISO 27002, el cual sería de gran ayuda para la organización poder identificar y entender todas aquellas brechas de seguridad y vulnerabilidades que requieran ser atendidas, la percepción del área ayuda a priorizar acciones y recursos para fortalecer la seguridad de manera alineada con los estándares internacionales.

Adicional con un plan de seguridad informática formalizado, la organización reconoce la necesidad de fomentar la conciencia y responsabilidad de todos los niveles de la empresa sobre la protección de sus activos tecnológicos.

Ilustración 22: Entrevista, cumplimiento de Controles Tecnológicos

Tabla de Evaluación de Cumplimiento de Controles Tecnológicos			
Control Evaluado			
8.1 Dispositivos terminales de usuario: Proteger la información frente a los riesgos introducidos por el uso de dispositivos de punto final de usuario	**SI**	**Parcialmente**	**No**
a. Existe un registro de dispositivos de punto final de usuario	X		
b. Requisitos de protección física (candado)			X
c. Restricción en la instalación de software	X		
d. Cifrado de equipo final y dispositivos de almacenamiento			X
8.2 Derechos de acceso privilegiado: Para garantizar que sólo los usuarios, componentes de software y servicios autorizados dispongan de derechos de accesos privilegiados.	**SI**	**Parcialmente**	**No**
a. Identificar usuarios que necesitan derechos de acceso privilegiados			X
b. Asignar derechos de acceso privilegiado a los usuarios según sea necesario	X		
c. Revisar periódicamente los accesos de las cuentas de usuario		X	
d. Registrar todos los accesos privilegiados			X
8.5 Autenticación Segura: Garantizar la autenticación segura de un usuario o una entidad cuando se le concede acceso a sistemas, aplicaciones y servicios.	**SI**	**Parcialmente**	**No**

a. Cuentan con políticas que exijan contraseñas robustas	X		
b. Cuentan con doble factor de autenticación para el acceso a los equipos		X	
c. Cuentan con alguna política que bloquee el usuario después de varios intentos erróneos	X		
d. Generar un evento de seguridad si se detecta un posible intento de violación de los controles de inicio de sesión			X
8.7 Protección contra el malware: Garantizar la protección de la información y otros activos asociados contra los programas maliciosos	**SI**	**Parcialmente**	**No**
a. Instalación y actualización de productos de seguridad	X		
b. Cuentan con controles que detecten el uso de software no autorizado		X	
c. Revisión periódica del software instalado en los elementos críticos			X
d. Aplican recomendaciones emitidas por entidades confiables (MICITT)			X
8.8 Gestión de las vulnerabilidades técnicas: Para evitar la explotación de vulnerabilidades técnicas	**SI**	**Parcialmente**	**No**
a. Se cuenta con un inventario de activos de hardware y software	X		
b. Se actualizan de manera periódica cada uno de los activos		X	
c. Se realizan pruebas de vulnerabilidades		X	
d. Se ejecutan pruebas de penetración		X	
8.10 Supresión de información: Para evitar la exposición innecesaria de información sensible y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información.	**SI**	**Parcialmente**	**No**
a. Se utiliza destructora de papel de corte cruzado para eliminar información física	X		
b. Se utiliza algún software para el borrado seguro			X
c. Se elimina información sensible de forma segura cuando ya no sea necesaria		X	
d. Se utilizan mecanismos de eliminación adecuados (desmagnetización de unidades de disco duro y otros soportes de almacenamiento magnético)			X
8.11 Enmascaramiento de datos: Limitar la exposición de datos sensibles, incluida la información de identificación personal, y cumplir los requisitos legales, estatutarios, reglamentarios y contractuales.	**SI**	**Parcialmente**	**No**
a. No conceder a todos los usuarios acceso a los datos	X		
b. Cuentan con mecanismos de ofuscación de datos		X	
c. Cuentan con acuerdos o restricciones sobre el uso de los datos tratados			X
d. Se lleva un registro del suministro y la recepción de los datos procesados		X	

8.13 Respaldo de información: Permitir la recuperación tras la pérdida de datos o sistemas.	**SI**	**Parcialmente**	**No**
a. Se realizan respaldos de información a los elementos críticos	X		
b. Se cuenta con procedimientos de restauración y recuperación de datos		X	
c. Los respaldos son almacenados en lugares seguros y protegidos		X	
d. Se protegen las copias de seguridad mediante cifrado			X
8.19 Instalación de software en sistemas operativos: Garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas	**SI**	**Parcialmente**	**No**
a. Se mantienen actualizadas las versiones de Windows	X		
b. Se instala software sólo después de haber realizado pruebas exhaustivas	X		
c. Se definen estrategias de reversión antes de aplicar cambios		X	
d. Se mantiene un registro de auditoría de todas las actualizaciones del software			X
8.20 Seguridad en las redes: Proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo contra el peligro a través de la red.	**SI**	**Parcialmente**	**No**
a. Se cuenta con un diagrama de red de la infraestructura		X	
b. Establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan por redes públicas,		X	
c. Detectar, restringir y autenticar la conexión de equipos y dispositivos a la red	X		
d. Se cuenta con herramientas de monitoreo de la red	X		
8.22 Segregación de redes: Dividir la red en fronteras de seguridad y controlar el tráfico entre ellas en función de la actividad empresarial. necesidades.	**SI**	**Parcialmente**	**No**
a. Cuentan con diferentes dominios de red independientes			X
b. Se utilizan mecanismos como VLANs	X		
c. Las redes inalámbricas cuentan con un tratamiento especial		X	
d. Se monitorean y registran los accesos de red, y se generan alertas ante actividades sospechosas o no autorizadas	X		
8.23 Filtrado web: Proteger los sistemas de ataques de programas maliciosos y evitar el acceso a sitios web no autorizados. recursos.	**SI**	**Parcialmente**	**No**
a. Cuentan con controles implementados para el filtrado web	X		
b. Se han establecido niveles de navegación web	X		

c. Utilizan equipos de seguridad para el control en la navegación		X	
d. Se capacita al personal para utilizar de manera correcta aquellos equipos que cuentan con mayores privilegios de navegación		X	
8.25 Ciclo de vida del desarrollo seguro: Garantizar que la seguridad de la información se diseñe y aplique dentro del ciclo de vida de desarrollo seguro de software y sistemas.	**SI**	**Parcialmente**	**No**
a. La organización ha establecido y documentado políticas y procedimientos para el desarrollo seguro de software y sistemas		X	
b. Se implementa la separación de los entornos de desarrollo, prueba y producción para prevenir accesos no autorizados	X		
c. Se aplican directrices de codificación segura adaptadas a cada lenguaje de programación utilizado en la organización		X	
d. Los desarrolladores reciben formación continua en prácticas de desarrollo seguro y están capacitados para identificar y corregir vulnerabilidades en el código		X	
8.30 Desarrollo externalizado: Garantizar que las medidas de seguridad de la información exigidas por la organización se aplican en el desarrollo de sistemas subcontratados.	**SI**	**Parcialmente**	**No**
a. Se han establecido acuerdos contractuales que incluyan requisitos específicos de seguridad de la información para los proveedores de desarrollo subcontratado	X		
b. La organización supervisa y revisa regularmente las actividades de desarrollo realizadas por proveedores externos	X		
c. Los acuerdos con proveedores externos contemplan derechos de auditoría para verificar el cumplimiento de las políticas de seguridad de la organización	X		
d. Se cuentan con herramientas de seguridad para la conexión de los proveedores externos a la organización		X	
8.31 Separación de los entornos de desarrollo, prueba y producción: Proteger el entorno de producción y los datos de los riesgos derivados de las actividades de desarrollo y prueba.	**SI**	**Parcialmente**	**No**
a. Se mantienen separados adecuadamente los sistemas de desarrollo, prueba y producción	X		
b. Se cuenta con ambientes de pruebas antes de aplicar algún cambio en producción	X		
c. Se realizan copias de seguridad de los diferentes entornos		X	
d. Se define un control de acceso en cada uno de los ambientes de desarrollo y producción			X

Con respecto a los resultados de la entrevista anterior, podemos observar que varios de los controles tecnológicos presentan debilidades, se analizarán cada uno de los puntos.

En el área de cumplimiento:

8.1 Dispositivos terminales de usuario: Se llevan registros y restricciones, aunque hay debilidades en cifrado y protección física.

8.5 Autenticación segura: Buen cumplimiento en políticas de contraseñas y bloqueo por intentos fallidos. Falta generar alertas de seguridad.

8.13 Respaldo de información: Se realizan respaldos, aunque con brechas en cifrado y procedimientos de restauración.

8.19 Instalación de software: Se aplican buenas prácticas previas a la instalación, pero faltan registros de auditoría.

8.30 Desarrollo externalizado: Todos los controles están en "Sí", excepto el uso de herramientas seguras para conexión de terceros.

En las áreas con cumplimiento parcial o limitado

8.2 Derechos de acceso privilegiado: Se asignan derechos, pero no se registran ni revisan adecuadamente los accesos.

8.7 Protección contra el malware: Sólo se cumple la instalación de productos, sin seguimiento ni cumplimiento de recomendaciones oficiales.

8.8 Gestión de vulnerabilidades técnicas: Falta ejecución sistemática de pruebas de vulnerabilidades y penetración.

8.10 Supresión de información: Se destruye físicamente la información, pero hay debilidades serias en el borrado seguro y eliminación digital.

8.11 Enmascaramiento de datos: Acceso está restringido, pero hay poca ofuscación, acuerdos y registros del uso de datos.

8.20 Seguridad en las redes: Se detectan y monitorean equipos, pero falta diagramado de red y controles para redes públicas.

8.22 Segregación de redes: Implementación limitada; no existen dominios independientes ni tratamiento adecuado a redes inalámbricas.

8.23 Filtrado web: Se filtra y controla navegación, pero hay carencias en capacitación y equipos de seguridad especializados.

8.25 Ciclo de vida del desarrollo seguro: Políticas implementadas parcialmente; falta formación, codificación segura y documentación.

8.31 Separación de entornos: Se mantiene separación básica, pero faltan copias de seguridad por entorno y controles de acceso diferenciados.

En resumen, podemos indicar que la organización cuenta con una seguridad razonable de controles tecnológicos, aunque muchas de las medidas están implementadas de manera parcial o no cumplen.

Al igual que el anterior diagnóstico, se llevó a cabo una entrevista en la que se formularon preguntas sobre el área de infraestructura digital del departamento de TI; a continuación, se presenta la información recopilada.

Ilustración 23: Entrevista, Evaluación de la Infraestructura Digital

Tabla de Evaluación de Infraestructura Digital			
¿La infraestructura física actualmente cuenta con equipos como servidores, switches, firewalls que sostienen las operaciones tecnológicas?	**SI**	**Parcialmente**	**No**
	X		
¿Realizan mantenimientos preventivos y correctivos a los equipos de red y servidores?	**SI**	**Parcialmente**	**No**
	X		
¿Existen políticas definidas para la renovación tecnológica de hardware y software para los equipos de infraestructura?	**SI**	**Parcialmente**	**No**
			X
¿Se encuentra documentada la arquitectura de la red con los flujos más críticos de comunicación interna y externa?	**SI**	**Parcialmente**	**No**
		X	
¿Existen ambientes segregados de desarrollo, prueba y producción dentro de la infraestructura de la organización?	**SI**	**Parcialmente**	**No**
	X		
¿Cuentan con herramientas para monitorear el rendimiento y la disponibilidad de los servicios de infraestructura?	**SI**	**Parcialmente**	**No**
		X	
¿Es escalable la infraestructura actual frente a un crecimiento esperado de la organización?	**SI**	**Parcialmente**	**No**
		X	
¿Se tienen establecidos procedimientos para la gestión de respaldos y recuperación de la información crítica desde la perspectiva de infraestructura?	**SI**	**Parcialmente**	**No**
			X
¿Cuentan con medidas de seguridad implementadas para proteger la infraestructura frente alguna amenaza interna o externa?	**SI**	**Parcialmente**	**No**
		X	

¿Se han identificado brechas de seguridad o puntos de falla en la infraestructura actual?	**SI**	**Parcialmente**	**No**
			X
¿Cuenta con algún enlace alterno de comunicación a internet?	**SI**	**Parcialmente**	**No**
			X
¿Se cuenta con alguna herramienta que balance las cargas de los equipos de la infraestructura crítica?	**SI**	**Parcialmente**	**No**
			X

Fuente: Elaboración Propia

Con la evaluación anterior de la infraestructura podemos revelar algunos aspectos importantes:

- La infraestructura física, incluyendo servidores, switches y firewalls, está presente y en parte mantenida, aunque no se especifica si los mantenimientos preventivos y correctivos son completamente efectivos.
- Existen políticas parciales para la renovación tecnológica y la documentación de la arquitectura de red, así como ambientes segregados para desarrollo, prueba y producción.
- Se cuenta con herramientas en algunos casos para monitorear rendimiento y disponibilidad, pero no de manera integral.
- La infraestructura es parcialmente escalable y se dispone de procedimientos para respaldos y recuperación de información, aunque estos no están completamente establecidos.
- En cuanto a seguridad, se han implementado medidas, pero aún hay brechas y puntos de falla identificados.
- No se dispone de un enlace alterno de internet ni de herramientas completas para balanceo de carga en los equipos de la infraestructura crítica.

Podríamos indicar que la organización si cuenta con una base sólida de infraestructura, pero es necesario fortalecer algunas políticas, documentación, monitoreo, brechas de seguridad y redundancia para mejorar su resiliencia y capacidad de crecimiento.

5.4 Brechas del diagnóstico

Este apartado se centra en comprender las carencias de la organización, considerando los diversos análisis que se llevaron a cabo en este capítulo. Es por esto por lo que en esta sección se ilustra una tabla en la comparación de la situación actual, las brechas y lo que se desea tener.

Ilustración 24: Brechas o conclusiones del diagnóstico

Brechas del Diagnóstico			
Aspecto	**Situación Actual**	**Brecha**	**Situación Deseada**
Políticas, normas y procedimientos	No se cuenta con políticas robustas ni procedimientos de seguridad de la información	Falta de políticas, normas y procedimientos	Capacitación e implementación de políticas y procedimientos de seguridad de la información
Dispositivos terminales de usuario	Registro de dispositivos y restricciones en uso, pero sin cifrado ni protección física adecuada.	Falta de cifrado y protección física robusta.	Registro completo, cifrado de datos y protección física eficaz en dispositivos terminales.
Derechos de acceso privilegiado	Identificación y revisión de accesos en algunos casos, pero sin registros de todos los accesos privilegiados.	No se registran todos los accesos y no se realiza revisión periódica de derechos.	Control, registro y revisión periódica de todos los accesos privilegiados.
Autenticación segura	Políticas de contraseñas robustas y bloqueo tras intentos fallidos; falta generación de alertas de seguridad.	Ausencia de alertas y doble factor en algunos casos.	Implementación de doble factor, alertas de seguridad y políticas estrictas de autenticación.
Protección contra malware	Instalación y actualización de seguridad en marcha, pero con controles limitados para software	Falta de controles en uso de software no autorizado y revisión periódica.	Sistemas actualizados, controles efectivos y revisiones periódicas para detectar malware.

	no autorizado y revisión periódica.		
Gestión de vulnerabilidades	Inventario y actualizaciones en proceso, pero sin pruebas regulares de vulnerabilidades o penetración.	Inexistencia de pruebas regulares y análisis de vulnerabilidades.	Inventario actualizado, pruebas de vulnerabilidades y penetración periódicas.
Respaldo de información	Respaldos realizados y procedimientos existentes, pero sin cifrado en copias de seguridad.	Copias no cifradas y procedimientos de restauración no completamente definidos.	Respaldos cifrados, procedimientos de recuperación claros y almacenados de forma segura.
Instalación de software en sistemas	Actualizaciones y pruebas previas, pero sin registros de auditoría.	Falta de registros de auditoría y control en actualizaciones.	Registros de auditoría, control estricto y pruebas documentadas en la instalación.
Seguridad en las redes	Diagrama de red y controles básicos, pero con monitoreo y segmentación limitada.	Necesidad de mejorar en segmentación, monitoreo avanzado y control de accesos.	Redes segmentadas, monitoreo en tiempo real y controles avanzados de seguridad en red.
Segregación de redes	Uso de VLANs y redes independientes, pero con monitoreo y registros insuficientes.	Mejorar en monitoreo y control del tráfico entre redes segregadas.	Monitoreo constante, registros y control estricto del tráfico entre segmentos.
Filtrado web	Controles de filtrado en marcha, pero con niveles limitados y capacitación del personal.	Mejoras en niveles de filtrado y en capacitación del personal.	Filtrado avanzado, capacitación continua y políticas claras de navegación.
Desarrollo seguro	Políticas y procedimientos establecidos, pero con brechas en formación continua y control en entornos de desarrollo.	Necesidad de mayor formación, control en ambientes y revisiones de seguridad.	Procesos integrados, formación continua y controles estrictos en desarrollo y pruebas.
Desarrollo externalizado y separación de entornos	Control adecuado en contratación, pero con deficiencias en supervisión y separación en algunos casos.	Mejorar en supervisión y control de entornos de desarrollo y producción.	Supervisión constante, separación efectiva y controles en entornos de desarrollo, prueba y producción.

Fuente: Elaboración Propia

CAPÍTULO V: DISEÑO Y DESARROLLO DEL PROYECTO

En este capítulo se detalla el diseño y desarrollo de las diferentes soluciones propuestas para abordar aquellas debilidades en los controles tecnológicos seleccionados de la norma ISO 27002 dentro de la empresa Comercial de Seguros Corredora de Seguros S.A. Basándonos en el análisis exhaustivo realizado, donde se diagnosticaron algunas brechas de cumplimiento, el principal objetivo es presentar las recomendaciones específicas y la metodología para su implementación.

Se establecerán las pautas para remediar cada deficiencia identificada, describiendo algunas acciones concretas, los recursos necesarios y pasos a seguir para fortalecer la postura de seguridad de la información de la empresa, buscando la conformidad con los estándares internacionales.

Se busca en este capítulo no solo corregir las falencias actuales, sino también establecer una base sólida para la mejora continua de los controles tecnológicos.

De acuerdo con el primer control tecnológico seleccionado se detectaron algunas debilidades encontradas durante el análisis realizado y ausencia de políticas robustas en el área de seguridad de la información, así como ausencia de personal especializado, por lo que se recomienda lo siguiente:

6.1 Políticas, normas y procedimientos

6.1.1 Definir un marco normativo

(Control ISO 27002:2022 - 5.1 - “Políticas de Seguridad de la Información”)

Una vez realizado el diagnóstico, se debe construir el marco documental de Seguridad de la Información conforme a la siguiente jerarquía lógica.

- ✓ Se debe establecer una política de Seguridad de la Información, el cual es un documento de alto nivel que declara el compromiso de la organización con la seguridad de la información.

- **Debe incluir:**
    - Objetivo y alcance (toda la infraestructura tecnológica y datos sensibles).
    - Principios de confidencialidad, integridad y disponibilidad.
    - Responsabilidades de usuarios, administradores y dirección.
    - Revisión anual y proceso de actualización.

✓ Entre las normas y estándares se debe especificar reglas para áreas clave, (uso de contraseñas robustas, cifrado, respaldos, dispositivos, entre otros).

- **Recomendación:**
    - **Contraseñas:** Una longitud mínima de 12 caracteres, combinando mayúsculas, minúsculas, números y símbolos; caducidad cada 30 días.
    - **Cifrado:** Uso obligatorio de algoritmos AES-256 para información sensible y TLS 1.3 para datos en tránsito.
    - **Respaldo:** Copias automáticas diarias y almacenamiento seguro con prueba de restauración mensual.
    - **Dispositivos móviles:** Implementación de MDM, bloqueo remoto y encriptación de almacenamiento.
    - **Actualizaciones:** Aplicación de parches críticos dentro de 48 horas de su publicación para todos los equipos de la infraestructura.

✓ Se debe construir procedimientos con las instrucciones detalladas de paso a paso para implementar las normas (por ejemplo, cómo hacer una copia de seguridad, cómo cifrar un equipo de usuario final, cómo aplicar parches de seguridad, entre muchos otros).

Nombre de cada uno de los procedimientos:

- “Procedimiento para crear copias de seguridad en servidores”.
- “Procedimiento para cifrar discos duros en equipos de usuario final”.
- “Procedimiento para gestionar accesos de nuevos empleados y eliminación de cuentas inactivas”.
- “Procedimiento para respuesta ante incidentes y recuperación ante desastres”.

6.1.2 Capacitación y sensibilización

(Control 6.3 - Concienciación, educación y formación en seguridad de la información)

Una vez aprobadas las políticas y procedimientos, se debe capacitar al personal de la organización sobre cada uno de sus roles y responsabilidades, realizar campañas de concientización y buenas prácticas y asegurar que todos firmen una declaración de aceptación de políticas.

6.2 Dispositivos terminales de usuario

6.2.1 Registro de dispositivos

(Control ISO 27002:2022 - 8.1 - “Dispositivos terminales de usuario”)

Se recomienda continuar con un registro actualizado de un inventario centralizado de todos los dispositivos autorizados propiedad de la organización como pc’ s, laptops, móviles entre otros.

Justificación:

Contar con un inventario de dispositivos permite mantener un control y trazabilidad sobre todos los equipos que acceden a la red corporativa.

Esto facilita para:

- Detectar accesos no autorizados o dispositivos desconocidos conectados al entorno.
- Aplicar políticas de seguridad coherentes (actualizaciones, antivirus, cifrado, etc.).
- Responder rápidamente ante incidentes, ya que se conoce qué equipo está comprometido y quién es su responsable.
- Cumplir con normas de seguridad y auditorías internas o externas, que exigen control sobre activos tecnológicos.

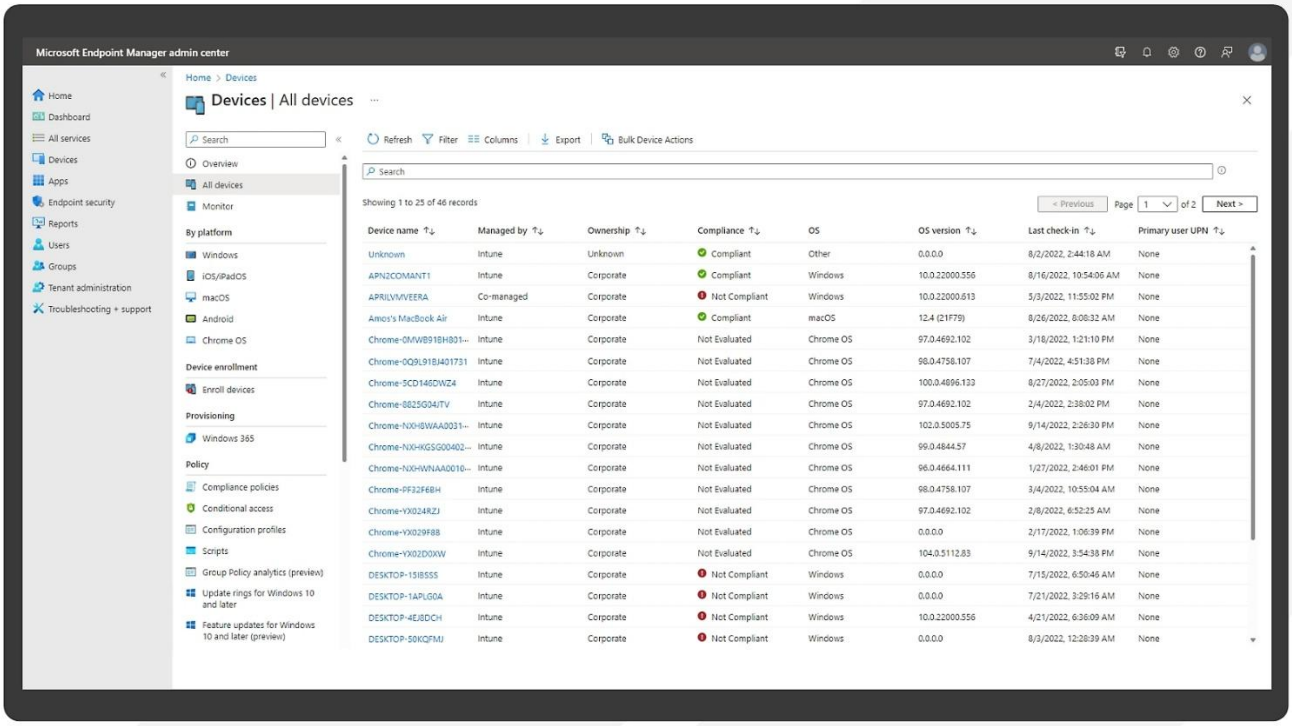
Entre las soluciones sugeridas podemos mencionar:

- Microsoft Intune: Herramienta que permite la administración remota, políticas de seguridad y control de cumplimiento.
- ManageEngine AssetExplorer: Solución que facilita la gestión del ciclo de vida de los activos y auditorías de manera automática.
- Lansweeper: Con esta herramienta se puede detectar y documentar todos aquellos dispositivos conectados a la red sin necesidad de ningún agente.
- GLPI (open source): Esta solución es gratuita, permite inventario, gestión de tickets y mantenimiento de equipos.

Tras analizar las diferentes opciones, se recomienda la implementación de **Microsoft Intune**, ya que ofrece mayor integración con servicios corporativos de Microsoft 365 y Azure, permite una administración centralizada, políticas de seguridad consistentes y soporte multiplataforma (Windows, macOS, Android, iOS).

Además, al ser una solución en la nube, reduce la carga operativa del equipo de TI y facilita el cumplimiento de estándares de seguridad, lo que la convierte en una opción robusta, escalable y alineada con entornos empresariales modernos.

Ilustración 25: Microsoft Intune



Fuente: Microsoft (s.f).

Recuperado de https://www.microsoft.com/

6.2.2 Protección física

(Control ISO 27002:2022 - 7.4 - “Monitoreo de seguridad física”)

Se debe de establecer normas para el almacenamiento físico seguro, implementando el uso obligatorio de candados de seguridad como los de tipo **Kensington**, y sensibilizar sobre la importancia en la protección en espacios abiertos o compartidos, también se recomienda sensores de apertura y movimiento en áreas críticas.

6.2.3 Restricción de instalación de software

(Control ISO 27002:2022 - 5.18 - “Derechos de acceso”)

Este control se cumple ya que únicamente el personal autorizado y con privilegios de administrador pueden efectuar cualquier tipo de instalación de software en los equipos corporativos, sin embargo, se recomienda realizar una revisión trimestral de los permisos y roles asignados a los usuarios con privilegios de instalación, con el fin de garantizar que continúen siendo válidos y de acuerdo con las funciones actuales del personal.

Es importante también utilizar herramientas de gestión que impidan instalaciones sin autorización como, por ejemplo:

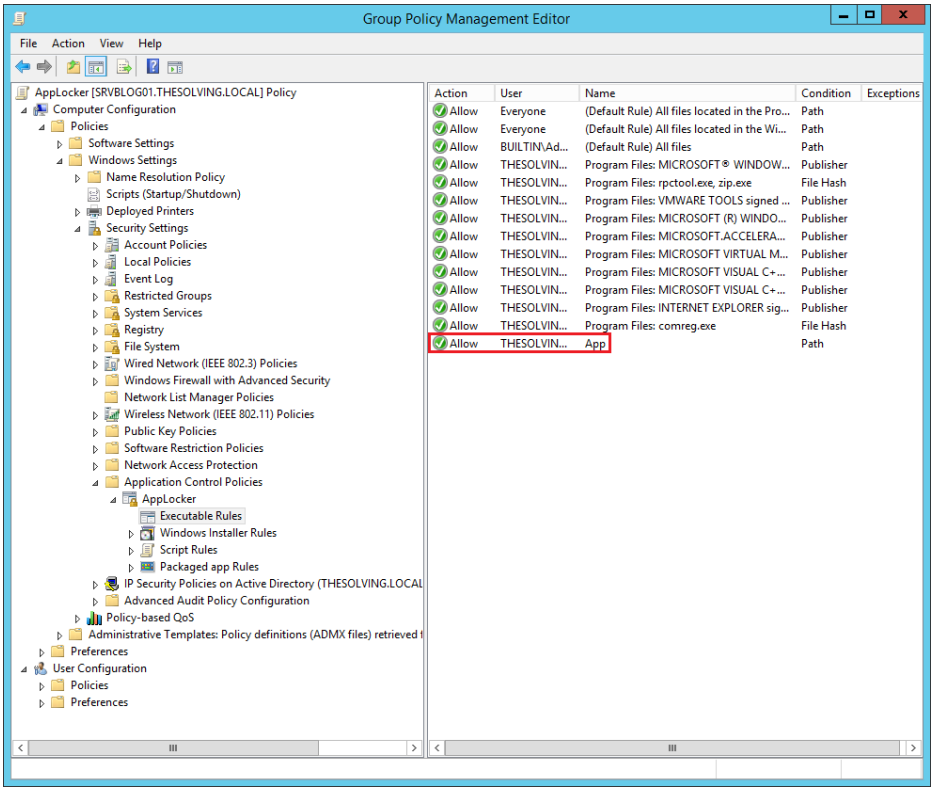
- Microsoft AppLocker (Windows): Esta solución se encuentra integrado nativamente en sistemas operativos Windows, permite definir políticas de ejecución según editor, ruta o hash del archivo, lo que facilita la administración en entornos con dominio Active Directory sin requerir software adicional, la organización cuenta con SO Windows y entornos con AD.
- FortiClient Application Control: Esta solución parte del ecosistema Fortinet, ideal para organizaciones que ya cuentan con dispositivos FortiGate, ya que permite aplicar

políticas de control de aplicaciones y monitorear cumplimiento desde una misma consola centralizada, actualmente la organización cuenta con Fortinet para los equipos de seguridad firewall.

- WatchGuard EPDR (control de aplicaciones no confiables): Esta consola combina protección antimalware con control avanzado de aplicaciones no confiables, ofreciendo visibilidad del comportamiento de software en tiempo real. Es útil en entornos que requieren detección proactiva y control granular de ejecución, actualmente en mi trabajo administro esta herramienta y es bastante robusto y cumple con diferentes productos de seguridad.

El objetivo principal es controlar instalaciones dentro de un entorno Windows con Active Directory, **Microsoft AppLocker** es la opción más directa y eficiente, ya que aprovecha las herramientas nativas del sistema y requiere mínima inversión adicional.

Ilustración 26: AppLocker



Fuente: Nanosytems (s.f).

Recuperado de https://www.thesolving.com/

6.2.4 Cifrado de equipos y almacenamiento

(Control ISO 27002:2022 - 5.33 - "Protección de registros")

Se recomienda implementar el cifrado completo del disco duro para todos los dispositivos de usuario final, cifrar memorias USB y discos externos utilizados en la organización debe ser de carácter obligatorio.

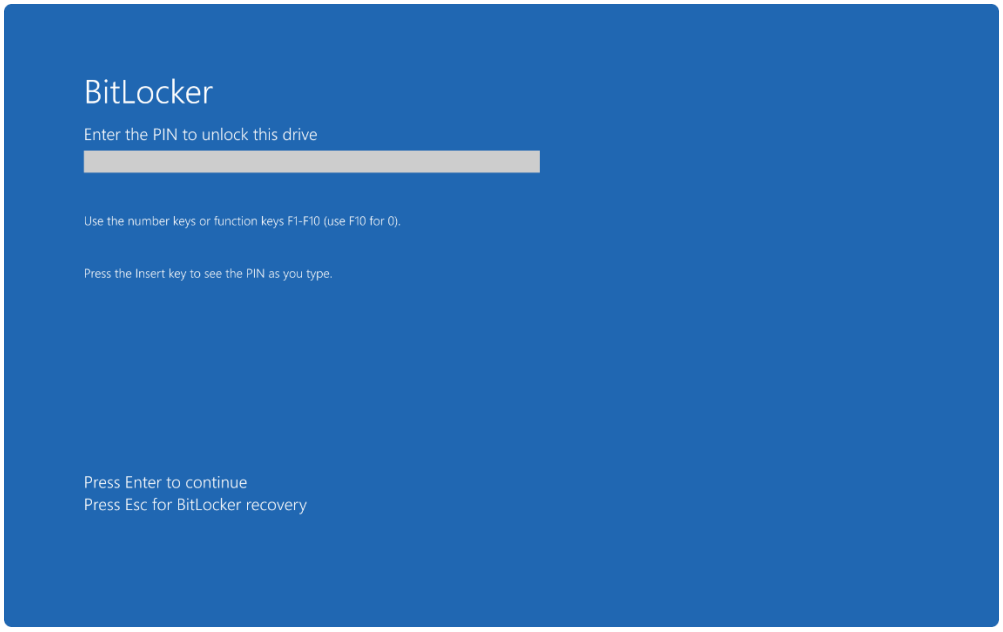
Entre las soluciones sugeridas tenemos:

- BitLocker (Windows): Su principal característica es integración nativa con Windows y Active Directory, permite el cifrado completo del disco duro sin software adicional.

- FileVault (macOS): Cifra automáticamente todo el disco del sistema en Macs, con protección integrada de la contraseña del usuario.
- VeraCrypt (software libre): Esta solución es de código abierto que permite cifrar discos completos o crear volúmenes cifrados, compatible con múltiples sistemas operativos.:
- Kingston IronKey (USB cifradas por hardware): Dispositivos USB con cifrado de hardware integrado y protección por PIN; no depende del sistema operativo para funcionar.

La organización tiene principalmente equipos Windows, por lo que la mejor opción sería **BitLocker**, porque combina integración nativa, administración centralizada y cumplimiento obligatorio del cifrado, simplificando la implementación masiva en todos los dispositivos.

Ilustración 27: BitLocker



Fuente: Microsoft (s.f).

Recuperado de https://learn.microsoft.com/

6.3 Derechos de acceso privilegiado

6.3.1 Identificar usuarios que necesitan privilegios

(Control ISO 27002:2022 - 5.18 - “Acceso a información y otros recursos”)

Se recomienda desarrollar un inventario detallado y actualizado de todas las cuentas privilegiadas (administradores, root, operadores, entre otros), una vez definido el inventario clasificar tipos de privilegios según sus funciones.

6.3.2 Asignar privilegios según la necesidad

(Control ISO 27002:2022 - 5.19 - “Gestión de privilegios de acceso”)

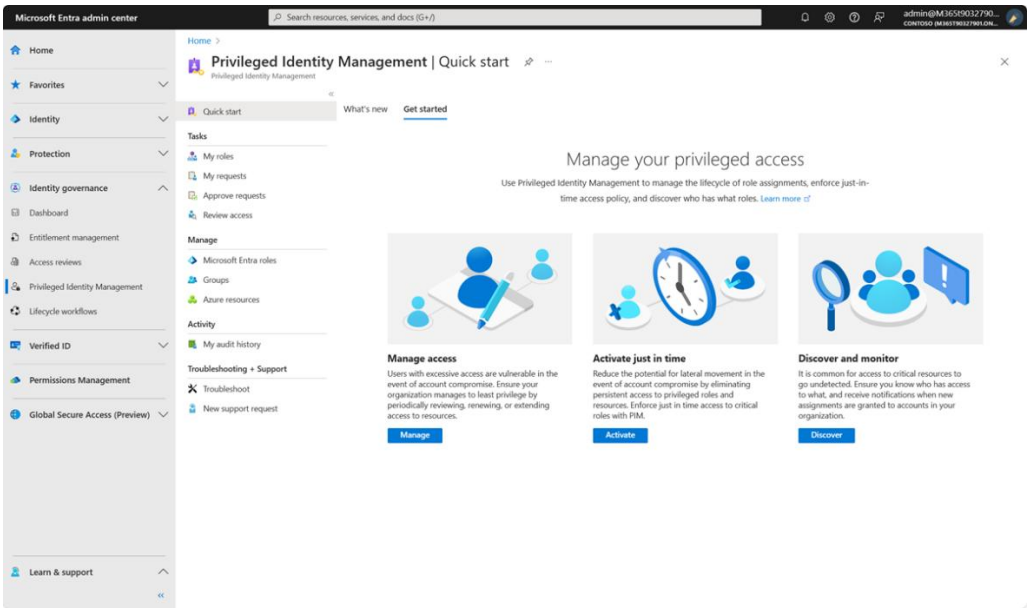
A pesar de que este control se cumple, se recomienda utilizar roles predefinidos con mínimos privilegios, además se podría valorar la opción de implementar la gestión de identidades y accesos (IAM) o alguna herramienta de PAM (Privileged Access Management).

De las cuales se podrían mencionar:

- CyberArk: Líder del mercado, ofrece una autenticación fuerte y rotación automática de contraseñas, es ideal para entornos que requieren máxima seguridad.
- BeyondTrust Password Safe: Proporciona una auditoria detallada y cumplimiento normativo, es útil para organizaciones con altos requerimientos regulatorios.
- ManageEngine PAM360: Solución accesible para medianas empresas, con buena relación costo-beneficio y funcionalidad completa.
- Azure Privileged Identity Management (PIM): Parte de Azure AD Premium, ideal para entornos Microsoft, gestiona privilegios just-in-time.

La organización ya opera en un entorno Microsoft con Active Directory y Azure. PIM permite gestionar privilegios de manera temporal ("just-in-time"), simplificando la administración y reduciendo riesgos de exposición de cuentas con permisos elevados.

Ilustración 28: Azure Privileged Identity Management



Fuente: Microsoft (s.f).

Recuperado de https://learn.microsoft.com

6.3.3 Revisión periódica

(Control ISO 27002:2022 - 5.20 – "Revisión de derechos de acceso")

Es recomendable realizar revisiones periódicas de los accesos privilegiados, ya una revisión de forma mensual o trimestral, según el riesgo y la criticidad de los sistemas. Además, se sugiere automatizar la generación de reportes de cambios de privilegios para facilitar el seguimiento y la auditoría.

6.3.4 Registro y auditoria de accesos

(Control ISO 27002:2022 - 8.15 – “Registro (logging) y 8.16 – Monitoreo de actividades”)

Se debe habilitar un registro centralizado (SIEM) de accesos privilegiados, en donde se activan los logs detallados de inicio de sesión, comandos ejecutados, cambios realizados.

Entre las principales herramientas para el registro y auditoría de accesos privilegiados les puedo mencionar:

- Splunk Enterprise Security
    - Recopila, analiza y correlaciona log’s en tiempo real.
    - Integración con herramientas PAM y Active Directory
    - Dashboards personalizados, alertas, análisis de comportamiento.
- Elastic Stack (ELK: Elasticsearch, Logstash, Kibana)
    - Solución flexible de código Abierto.
    - Recoge y visualiza log’s de Sistemas, firewalls, PAM.
    - Requiere configuración, pero altamente personalizable.
- Microsoft Sentinel (antes Azure Sentinel)
    - SIEM nativo de Azure.
    - Monitorea accesos en entornos de Microsoft 365, Azure AD, Windows Server.
    - Reglas de correlación automatizadas e integración con Defender.

6.4 Autenticación Segura

Control ISO 27002:2022 – 5.17 Información de autenticación

6.4.1 Políticas de contraseña robustas

(Control ISO 27002:2022 - 5.17 – “Autenticación de usuarios”)

A pesar de su cumplimiento, se recomienda aplicar políticas obligatorias que definan lo siguiente, alineadas con el Control 5.17 (Información de autenticación) y el control 5.18 (Derechos de acceso) de la norma ISO/IEC 27002:2022

- Longitud mínima de 12 caracteres, que incluyan mayúsculas, minúsculas, números y símbolos, control 5.17 – inciso "los requisitos de complejidad de la información de autenticación".
- Definir una periodicidad de cambio (se recomienda una vez al mes). Control 5.17 -inciso "procedimientos para cambiar o actualizar la información de autenticación".
- No reutilización de las últimas 5 contraseñas anteriores. Control 5.17 – inciso "restricciones sobre la reutilización de información de autenticación".

6.4.2 Doble factor de autenticación (MFA)

(Control ISO 27002:2022 - 5.17 - “Autenticación de usuarios”)

Se recomienda implementar un doble factor de autenticación (MFA) en aquellos equipos o sistemas críticos, y en cuentas de administradores. También en el correo electrónico, VPN, acceso remoto y aplicaciones en la nube.

Entre las herramientas recomendadas y para su valoración podemos mencionar.

- Microsoft Authenticator
- Google Authenticator
- AuthPoint (WatchGuard)

Se recomienda utilizar la herramienta de Microsoft Authenticator debido al ecosistema que integra con Microsoft y que utiliza la organización, la simplicidad de despliegue y cumplimiento del control.

Entre los beneficios es que va a venir a fortalecer la autenticación de cuentas privilegiadas y servicios críticos, reduciendo el riesgo de acceso no autorizado o compromiso de credenciales.

6.4.3 Bloqueo por intentos fallidos

(Control ISO 27002:2022 - 5.17 – "Autenticación de usuarios")

Este control se cumple de manera parcial, por lo que dentro de las recomendaciones podemos indicar lo siguiente:

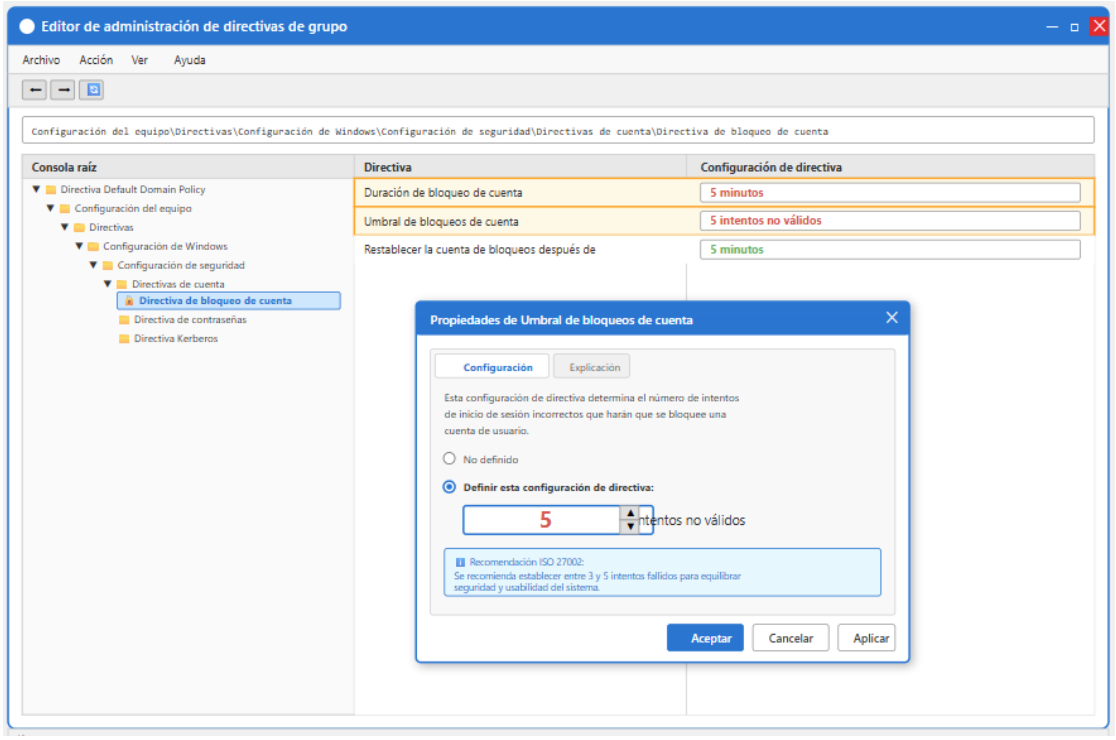
Para aquellos sistemas que utilizan Active Directory:

- Configurar una política para que el bloqueo automático de cuentas que sea después de 3 - 5 intentos fallidos.
- Definir un tiempo de duración de bloqueo automático (por ejemplo, 5 minutos) de inactividad del equipo.

Ejemplo para Windows (GPO)

Cuenta → Política de bloqueo → Límite de intentos = 5, Duración = 5 min

Ilustración 29: Administración directivas de grupo



Fuente: Elaboración propia

Para aplicaciones que NO utilizan Active Directory, pueden ser aplicaciones web propias, servicios cloud con autenticación independiente.

Identificar cada aplicación y su mecanismo de autenticación específico.

Implementar bloqueos de cuenta a nivel de aplicación mediante:

- Configuración en el código de la aplicación
- Parámetros de seguridad en la base de datos de usuarios
- Configuración nativa del servicio cloud (AWS IAM, Azure AD, Google Cloud Identity, etc.)

Documentar las políticas de bloqueo aplicadas en cada sistema.

6.4.4 Eventos de seguridad por intentos fallidos

(Control ISO 27002:2022 - 8.15 - “Registro de eventos”)

Dentro del control Autenticación Segura se identificó que no se cumple uno de los puntos dentro del control la cual es la generación de alertas de seguridad ante intentos fallidos.

Algunas de las recomendaciones que podríamos mencionar son:

- Activar la auditoría de eventos de seguridad (logs de fallos de inicio de sesión)
    - En Windows: Política de auditoría → "Logon Events".
    - En Linux: auditd o syslog + monitoreo con Wazuh o SIEM.
- Valorar adquirir alguna solución en donde se centralicen los registros como un SIEM.
    - Herramientas como Wazuh, Graylog, Splunk.
- Configurar alertas automáticas
    - Múltiples intentos fallidos desde una misma IP o cuenta.
    - Inicios de sesión desde ubicaciones no usuales.

6.5 Protección contra el malware

6.5.1 Instalación y actualización de productos de seguridad

(Control ISO/IEC 27002:2022 - 8.7 - “Protección contra el código malicioso”)

Durante la entrevista con el personal encargado de TI, se confirmó el cumplimiento del control. Sin embargo, la plataforma de seguridad que utilizan actualmente Sophos, aunque es efectiva en su función principal que es la protección de endpoint, presenta limitaciones en funcionalidades avanzadas como la autenticación multifactor, análisis de comportamiento, integración centralizada, entre otros. Por ello, se recomienda evaluar soluciones complementarias o considerar,

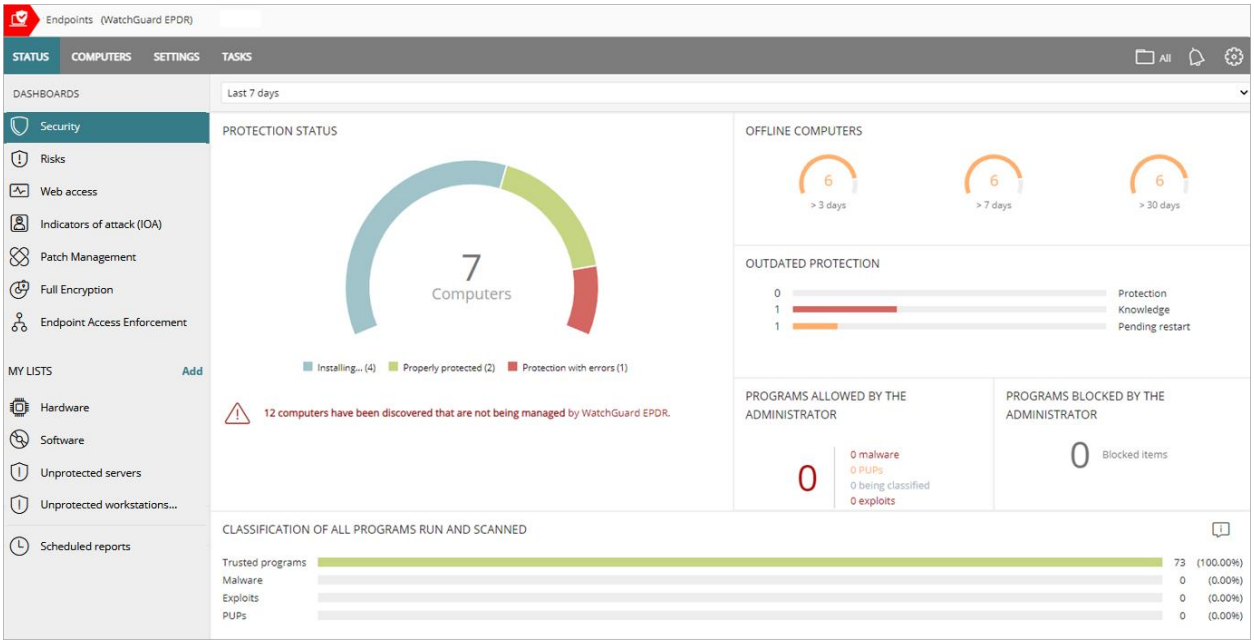
ya sea un upgrade a módulos más avanzados de Sophos (como Sophos XDR o Sophos Central) o explorar alternativas de nueva generación que refuercen dicho control.

Se menciona diferentes herramientas de protección y que son centralizadas como:

- Microsoft Defender for EndPoint: Esta es una plataforma empresarial de seguridad endpoint que forma parte del ecosistema Microsoft 365 Defender. Esta solución ofrece capacidades avanzadas de detección y respuesta (EDR - Endpoint Detection and Response), combinando inteligencia artificial y análisis de comportamiento para identificar amenazas en tiempo real.
- Sophos Intercept X: Esta es una solución de protección endpoint de nueva generación que combina técnicas tradicionales de antivirus con tecnologías avanzadas como deep learning y análisis de comportamiento para prevenir y detectar amenazas sofisticadas, incluido el ransomware.
- WatchGuard EPDR (Endpoint Protection Detection and Response).

Esta última herramienta mencionada de WatchGuard EPDR es una solución bastante robusta ya que es un antivirus de última generación, protección basada en comportamiento (EPP + EPDR), zero-trust application service (clasifica todo el software ejecutado en los endpoints), esta solución es ideal para bloquear malware avanzado, ransomware y amenazas sin archivo.

Ilustración 30: WatchGuard EPDR



Fuente: WatchGuard (s.f).

Recuperado de https://www.watchguard.com/

6.5.2 Controles para detectar software no autorizado

(Control ISO/IEC 27002:2022 - 8.9 - "Gestión de la instalación de software")

Recordemos que es de vital importancia contar con controles para la detección de software no autorizado por varias razones, que impactan directamente en la seguridad, la eficiencia operativa, el cumplimiento normativo. Sin ellos una organización se expone a riesgos significativos y evitables.

Existen herramientas para poder llevar un inventario automatizado de software instalado como, por ejemplo:

- ManageEngine EndPoint Central
- Wazuh
- OSQury

- SCCM

Entre las herramientas antes mencionadas se recomienda “ManageEngine EndPoint Central” ya que tiene capacidades robustas de inventario de software, el poder llevar un control estricto del inventario lo cual es fundamental para la seguridad, el cumplimiento y la gestión eficiente de los activos de TI en una organización.

6.5.3 Revisión periódica de software instalado

(Control ISO/IEC 27002:2022 - 8.9 - “Gestión de la instalación de software”)

Se identifica en la organización el NO cumplimiento sobre este control por lo que se recomienda lo siguiente:

- Establecer revisiones de manera trimestral del software en equipos críticos (como por ejemplo servidores, endpoints, activos de riesgo alto).
- Realizar una comparativa del software instalado contra el software permitido y aprobado por la organización.
- Documentar y reportar cualquier hallazgo encontrado al equipo de TI o Seguridad.

6.5.4 Aplicación de recomendaciones de entes confiables.

(Control ISO/IEC 27002:2022 - 8.8 - “Gestión de vulnerabilidades técnicas”)

El MICITT es una institución gubernamental encargada de diseñar, dirigir y coordinar la política pública en estas áreas clave para el desarrollo del país, por ende, les recomiendo suscribirse y dar seguimiento a alertas y boletines se seguridad que se comparten de manera mensual, dentro de esa valiosa información, se comparten por ejemplo diferentes campañas de ciberseguridad, grupos de ciber atacantes, indicadores de compromiso IoC para que el grupo técnico de cada organización tome acción ante las recomendaciones (por ejemplo, aplicar un parche crítico o bloquear una IP

maliciosa en los equipos de seguridad), de esa manera robustecer aún más la seguridad en sus empresas.

Se podría incluir este proceso como parte del plan de gestión de vulnerabilidades.

Se adjunta el sitio web para poder realizar la solicitud de inscripción y que incluyan a su empresa con el envío de la información URL: **MICITT (CSIRT-CR)**: https://www.csirt.go.cr/.

6.6 Gestión de las vulnerabilidades técnicas

6.6.1 Inventario de activos de hardware y software

(Control ISO/IEC 27002:2022 - 5.9 - "Inventario de información y otros activos asociados")

Este control tiene un cumplimiento parcial, por lo que es recomendable utilizar herramientas de descubrimiento automático de activos que registren, por ejemplo, dirección IP, sistema operativo, versiones de software, usuarios, entre otra información importante, inclusive poder clasificar los activos por criticidad y exposición.

Existen herramientas Open Source y soluciones comerciales que requieren de pago:

Open Source: GLPI, OCS Inventory

- **GLPI:** Es una solución de gestión de activos TI, y service desk que permite administrar el inventario completo de recursos tecnológicos de una organización. Entre sus principales ventajas es que es completamente gratuito y código abierto, interfaz web intuitiva, integración con el Active Directory, comunidad activa y plugins extensos.
- **OCS Inventory:** Esta herramienta se especializa en el descubrimiento y recopilación automática de inventario de hardware y software en la red. De igual forma que la solución

mencionada anteriormente es totalmente gratuita, agente ligeros y fáciles de desplegar, actualización automática de inventario son algunas de sus ventajas.

Comerciales: ManageEngine Asset Explorer, Lansweeper.

ManageEngine Asset Explorer: Esta solución permite el seguimiento completo del ciclo de vida de hardware y software empresarial.

Ventajas

- Integración nativa con todo el ecosistema ManageEngige
- Alertas proactivas de vencimientos y problemas
- Workflows automatizados de compras y contratos
- Soporte técnico profesional 24/7

Lansweeper: Es una herramienta de descubrimiento y gestión de activos de TI que ofrece capacidades avanzadas de inventario y auditoria.

Entre sus principales ventajas

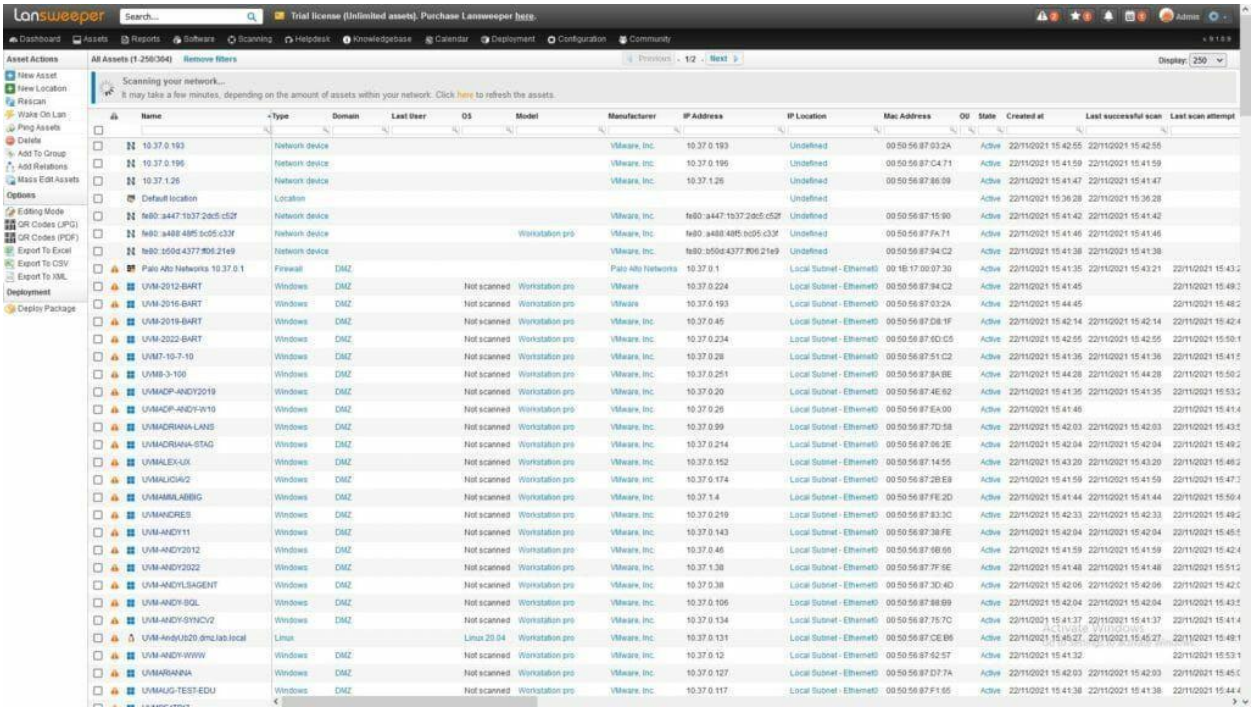
- No requiere instalar agentes
- Interfaz moderna y profesional
- Escaneo rápido y detallado
- Soporte técnico comercial
- Reportes de cumplimiento (ISO, PCI-DSS)

Para fortalecer la gestión de inventario de activos conforme a los controles 5.9 y 8.9 de la ISO 27002, se recomienda evaluar las siguientes soluciones anteriores, la selección dependerá de las

necesidades específicas de la organización, el presupuesto disponible y la complejidad de la infraestructura TI existente.

Mi recomendación para este control es la herramienta de Lansweeper, es la opción más ágil y de rápida implementación, es ideal para la organización que prioriza auditorías de cumplimiento y descubrimiento de activos sin la necesidad de instalar agente. También ofrece reportes predefinidos alineados con ISO 27001, lo que facilita las auditorías de seguridad.

Ilustración 31: Lansweeper



Fuente: Lansweeper (s.f).

Recuperado de https://invgate.com/

6.6.2 Actualización periódica de activos

(Control ISO/IEC 27002:2022 - 8.8 - “Gestión de vulnerabilidades técnicas”)

Este control es un pilar importante en la ciberseguridad y la gestión de TI de cualquier organización, y su omisión es una debilidad crítica. Esta práctica va más allá de solo tener el software o parches de seguridad al día; abarca la gestión continua de todo tipo de activos tecnológicos, desde software y firmware hasta hardware y configuraciones de red.

Se identifica que no realizar actualizaciones periódicas de activos es un factor de riesgo significativo que expone a la organización a brechas de seguridad, incumplimiento normativo, problemas de rendimiento y mayores costos operativos.

Recomendaciones para poder cumplir con este control:

- Definir un proceso formal de gestión de parches (path management).
- Automatizar las actualizaciones con soluciones centralizadas.
- Priorizar parches según severidad CVSS, criticidad del activo y exposición pública.

Algunas de las herramientas recomendadas:

- WSUS / Intune / SCCM: Son para entornos de Windows
- ManageEngige Patch Manager Plus
- WatchGuard (Patch Management)

Recomiendo esta última herramienta de WatchGuard ya que es un módulo crucial dentro de la suite de seguridad de endpoints de WatchGuard, que incluye diferentes productos de seguridad en una plataforma centralizada y fácil de administrar.

Esta solución está diseñada para automatizar y simplificar la gestión de vulnerabilidades en sistemas operativos y aplicaciones de terceros en las estaciones de trabajo y servidores de cualquier empresa (Windows, macOS y Linux). Los sistemas no solo están siendo monitoreados y respondiendo ante los diferentes ataques, sino que también estén proactivamente protegidos contra brechas conocidas a través de una buena gestión de parches de manera eficiente y centralizada.

6.6.3 Pruebas de vulnerabilidades

(Control ISO/IEC 27002:2022 - 8.8 - “Gestión de vulnerabilidades técnicas”)

De acuerdo con la entrevista que se mantuvo con el personal de infraestructura de la empresa, hace aproximadamente 3 años atrás fue la última vez que se realizaron pruebas de vulnerabilidades en la infraestructura de la organización y sus diferentes entornos.

Recordemos que estás pruebas de vulnerabilidades en los diferentes entornos del Dpto. TI, son un componente absolutamente crítico y no negociable de cualquier estrategia de ciberseguridad robusta. No son ejercicios que se realizan una única vez, sino un proceso continuo y sisemático.

Entre las recomendaciones a sugerir podemos indicar lo siguiente:

- Se deben de realizar escaneos de vulnerabilidades de forma trimestral.
- Se deben realizar escaneos al menos a los servidores más críticos de la organización como el del Active Directory, servidor de Base de Datos, servidor de Azure y al sistema de CORE, firewalls, aplicaciones web, dispositivos IoT, entornos de producción, entre otros.

Herramientas recomendadas:

- Open Source: OpenVAS, Wazuh con OSQuery, Nikto (para web).
- Comerciales: Nessus, ZAP, Qualys VMDR, Tenable.io.

Considerando el nivel de madurez actual del Departamento de TI y las capacidades técnicas de personal identificadas durante las entrevistas, se recomienda lo siguiente:

Dado que el equipo actual de TI no cuenta con experiencia especializada en análisis de vulnerabilidades y pruebas de penetración, se recomienda adquirir la contratación del servicio por parte de un proveedor o empresa certificada en seguridad ofensiva (OSCP, CEH, GPEN), el alcance de las pruebas debe ser de penetración completa (caja negra, caja gris) y mínimo 1 vez al año. El costo estimado ronda los 2 500 000 de colones en adelante según el alcance.

Una vez finalizadas las pruebas el proveedor debe hacer entrega de un informe ejecutivo, más el plan técnico de remediación priorizado.

Les comento lo siguiente para que lo tomen en consideración a futuro, si desean formar a alguno de sus técnicos en adquirir el conocimiento para realizar este tipo de pruebas de vulnerabilidades el costo ronda aproximadamente de la siguiente manera:

Costo: Adquiriendo la herramienta Nessus Profesional

Licencia anual $4,000 USD escaneo ilimitado de IP’s internas

La capacitación requerida de un curso avanzado de 16 horas, ronda entre $400 – 600 por técnico.

6.6.4 Pruebas de penetración

(Control ISO/IEC 27002:2022 - 8.29 - “Pruebas de seguridad de la información”)

Para este control se recomienda, primeramente, realizar el punto anterior, el análisis de vulnerabilidades en nuestro entorno, para poder identificar, clasificar y priorizar debilidades de seguridad en los sistemas, redes y aplicaciones.

De acuerdo con los informes que se emitan sobre los resultados, realizar el proceso de penetración es un proceso que se debe realizar de forma manual y semi – manual donde un “hacker ético” simula un ataque real a un sistema, red o aplicación.

El objetivo no es solo encontrar vulnerabilidades o brechas de seguridad, sino intentar explotarlas para determinar el impacto real y el nivel de acceso que un atacante podría obtener.

Entre las recomendaciones para las pruebas de penetración podemos indicar lo siguiente:

- Realizar pentests al menos 1 – 2 veces por año, o ante cambios mayores sobre la infraestructura existente.
- Se deben incluir pruebas tanto internas como externas en aplicaciones web, redes, accesos remotos, privilegios.
- Es posible la contratación de servicios profesionales con habilidades ofensivas (Red Team).
- Estas pruebas periódicas permiten evaluar la efectividad de los controles de seguridad implementados y detectar nuevas vulnerabilidades.

Pruebas ante eventos específicos

- **I**ncorporación de nuevos sistemas o aplicaciones: Antes de la puesta en producción de cualquier sistema nuevo, se debe realizar un pentest específico para validar su seguridad.
- Cambios arquitectónicos mayores: Migración a cloud, cambios en la infraestructura de red, implementación de nuevos servicios críticos.
- Actualizaciones críticas de aplicaciones: Después de upgrades mayores de versiones que modifiquen funcionalidades por ejemplo del core.
- Tras incidentes de seguridad: Para validar la remediación y asegurar que no existen vulnerabilidades residuales.
- Cambios en políticas de acceso: Implementación de nuevos métodos de autenticación o cambios en privilegios.

Herramientas y frameworks recomendadas:

- Herramientas: Metasploit, Burp Suite, Kali Linux, Cobalt Strike (profesional).
    - Metasploit Framework (explotación de vulnerabilidades)
    - Burp Suite Professional (aplicaciones web)
    - Kali Linux (distribución especializada)
    - Cobalt Strike (simulación de ataques avanzados - profesional)
- Frameworks: OWASP Testing Guide, MITRE ATT&CK, PTES.
    - OWASP Testing Guide (para aplicaciones web)
    - MITRE ATT&CK (simulación de tácticas y técnicas de atacantes)
    - PTES (Penetration Testing Execution Standard)
    - NIST SP 800-115 (guía de pruebas técnicas de seguridad)

Durante las entrevistas realizadas al personal de TI de la organización, se identificó que el equipo cuenta con experiencia en administración de sistemas Windows y Active Directory, tienen conocimientos básicos de redes y seguridad perimetral, pero en este punto no cuenta con experiencia práctica en pentesting ofensivo ni en el uso de herramientas especializadas como las antes mencionadas, tampoco poseen certificaciones en seguridad ofensiva (CEH, OSCP, GPEN).

De igual forma como el personal no está capacitado para realizar pruebas de penetración de forma efectiva, ni para implementar y utilizar las diferentes herramientas especializadas requeridas.

La recomendación al igual que en el punto anterior es la contratación de una empresa especializada para ejecutar dichas pruebas de penetración, ya que se requiere de conocimientos especializados y actualizados constantemente, son empresas que cuentan con certificaciones, seguro de responsabilidad y metodologías probadas.

Sin embargo y hago hincapié a que es únicamente una recomendación que la empresa pueda valorar más adelante es optar por un **"modelo híbrido"**

Justificación específica:

1. La organización actualmente NO cuenta con personal capacitado en pentesting
2. El riesgo de realizar pruebas sin conocimientos puede generar interrupciones o falsos positivos.
3. La contratación externa garantiza cumplimiento inmediato del control ISO 27002
4. La capacitación paralela permite desarrollar capacidades internas progresivamente

Plan de implementación recomendado:

Año 1 (Inmediato):

- Contratar empresa especializada para pentesting completo (prioridad ALTA)
- Iniciar capacitación de 1 persona en Security y CEH
- Implementar herramientas gratuitas de análisis de vulnerabilidades

Año 2:

- Segundo pentesting externo
- Personal capacitado realiza escaneos mensuales con OpenVAS/Nessus
- Evaluar capacitación avanzada (OSCP)

Año 3:

- Mantener pentesting externo anual
- Equipo interno realiza validaciones trimestrales
- Considerar Red Team interno básico

Ilustración 32: Recomendaciones generales para implementar todo el ciclo de gestión de vulnerabilidades

Fuente: Gigadefense (s.f).

Recuperado de https://gigadefense.com.mx/

6.7 Supresión de información

6.7.1 Uso de destructora de papel de corte cruzado

(Control ISO/IEC 27002:2022 - 8.10 - “Eliminación de información”)

A pesar del cumplimiento del control es importante reforzar y asegurarse de que todas las áreas que manejan información sensible cuenten con destructoras de tipo corte cruzado o micro corte.

Otra de las buenas prácticas es establecer una política de destrucción de documentos físicos con un calendario y responsables definidos, y así como aplicar controles para asegurar que ningún documento sensible se deseche sin ser destruido.

Ejemplo de equipo recomendado: **Modelo de referencia:** Fellowes Powershred 79Ci

Características Obligatorias:

- **Tipo de corte:** Corte cruzado (Cross-cut) P-4
- **Tamaño de partícula:** 4mm x 40mm o menor
- **Capacidad:** 10-15 hojas A4 simultáneamente
- **Capacidad del contenedor:** 20-30 litros
- **Ciclo de trabajo:** Uso continuo de 5-10 minutos
- **Destrucción adicional:** Tarjetas de crédito, CDs/DVDs, clips, grapas
- **Su costo aproximado** $200 **-** $ 800 USD según capacidad y marca

Ilustración 33: Powershred® 79Ci de Corte Cruzado con Tecnología 100% Anti-Atascos

Fuente: Fellowes (s.f).

Recuperado de https://www.fellowes.com/

Se recomienda la elaboración formal de la **"Política de Destrucción Segura de Documentos",** la misma debe establecer los lineamientos para la destrucción segura de documentos físicos que contengan información sensible, confidencial o de datos personales, garantizando que no puedan ser recuperados o reconstruidos por personas no autorizadas, lo anterior alineado con las mejores prácticas de la ISO 27002 para equipos de destrucción.

6.7.2 Uso de software para el borrado seguro de datos

(Control ISO/IEC 27002:2022 - 8.10 - "Eliminación de información")

Para el cumplimiento de este control se recomienda utilizar alguna herramienta o software especializado para el borrado seguro en discos duros, SSDs, USBs, memorias USB, otros medios de almacenamiento, aplicando estándares internacionales reconocidos como:

- **DoD 5220.22-M (Departamento de Defensa de EE.UU.)**
- **NIST 800-88 (National Institute of Standards and Technology)**

Estas herramientas deben utilizarse para el borrado seguro cuando los equipos sean dados de baja, reutilizados o transferidos algún colaborador.

Tabla 7: Herramientas recomendadas para el borrado seguro

Herramienta	Tipo	Comentario
DBAN (Darik's Boot and Nuke)	Gratuito	Para discos HDD. No recomendado para SSDs.
Blancco Drive Eraser	Comercial	Cumple con normativas internacionales (GDPR, HIPAA
Eraser	Gratuito (Windows)	Para eliminar archivos o particiones específicas.
Parted Magic	Comercial	Permite "secure erase" en SSDs y HDDs.
Linux shred / wipe	Gratuito (Linux)	Para borrar archivos o discos desde terminal.

Fuente: Elaboración Propia

Basándose en el análisis del entorno tecnológico, conocimientos del personal y necesidades identificadas, se recomienda implementar una estrategia combinada con las siguientes herramientas:

Eraser - Para uso rutinario en Windows: sitio de descarga https://eraser.heidi.ie/

- La organización opera principalmente en ambientes de Windows.
- Es una herramienta gratuita y de código abierto.
- Cumple con estándares DoD 5220.22-M.
- Permite borrado de archivos individuales, carpetas completas, discos completos.
- Permite también programar tareas automáticas de borrado.

Shred / wipe – Si se requiere borrar algún archivo o borrado de todo el servidor único de Linux que maneja la organización se recomienda utilizar esta herramienta para este entorno.

6.7.3 Eliminación segura cuando ya no es necesaria

(Control ISO/IEC 27002:2022 - 8.10 - "Eliminación de información")

Para este control se emiten las siguientes recomendaciones:

- Tener definido políticas claras de retención y destrucción de datos conforme a:
    - Legislación local (por ejemplo. Ley 8968 de Protección de Datos en Costa Rica).
    - Requisitos contractuales y regulatorios (auditoría, tributación, etc.).
- Automatizar el borrado tras cumplir con un tiempo de retención.
- Garantizar también que:
    - El borrado se realice tanto en backups, sistemas productivos y si se tienen repositorios en la nube.
    - Se genere un registro de todo el proceso de eliminación.

6.7.4 Mecanismos físicos adecuados (desmagnetización o destrucción)

(Control ISO/IEC 27002:2022 - 8.11 - “Eliminación de equipos”)

Para el cumplimiento de este control se recomienda aplicar métodos físicos de destrucción para los diferentes medios de almacenamiento que se encuentren fuera de uso:

- **Desmagnetización (degaussing)** para discos magnéticos.
- **Trituración física o perforación** de discos duros y SSDs.

Si no se cuenta con equipos especializados para ejecutar este tipo de tarea, es posible realizar la contratación de estos servicios de destrucción y equipo certificado.

6.8 Enmascaramiento de datos

Para este control es importante implementar diferentes medidas técnicas que reduzcan la exposición de información sensible o identificable (como datos personales, financieros, médicos, entre otros), en especial cuando se utilicen en entornos de desarrollo, pruebas, análisis o transferencia a terceros.

6.8.1 No conceder acceso total a todos los usuarios

(Control ISO/IEC 27002:2022 - 5.18 - “Acceso a información y otros activos asociados”)

Este control se cumple en la organización, sin embargo, es importante tener una retroalimentación de este, por lo que se recomienda:

- Implementar el principio de mínimo privilegio, asegurando que los usuarios tengan acceso únicamente a la información necesaria para realizar sus funciones.
- Implementar controles de acceso basados en roles (RBAC) o atributos (ABAC), que permitan la granularidad en los permisos.

- Separa los entornos de desarrollo, prueba y producción, empleando datos enmascarados o sintéticos que no sean de producción. Esto previene que individuos sin autorización tengan acceso a datos confidenciales en proceso de prueba o mantenimiento.

6.8.2 Mecanismos de ofuscación o enmascaramiento de datos

(Control ISO/IEC 27002:2022 - 8.11 - "Protección de datos en tránsito, almacenamiento y procesamiento")

En la organización no se cumple este control por lo que se recomienda implementar las siguientes técnicas:

- **Enmascaramiento estático**: reemplazo de datos sensibles por otros ficticios o irreversibles antes de moverlos a entornos no productivos.
- **Enmascaramiento dinámico**: se aplica en tiempo real según el perfil del usuario, sin modificar los datos en la base.
- **Tokenización**: Sustitución de valores sensibles por identificadores seguros.

Entre las herramientas recomendadas que se pueden utilizar se recomiendan las siguientes:

Tabla 8: Herramientas nativas recomendadas para enmascaramiento de datos MySQL

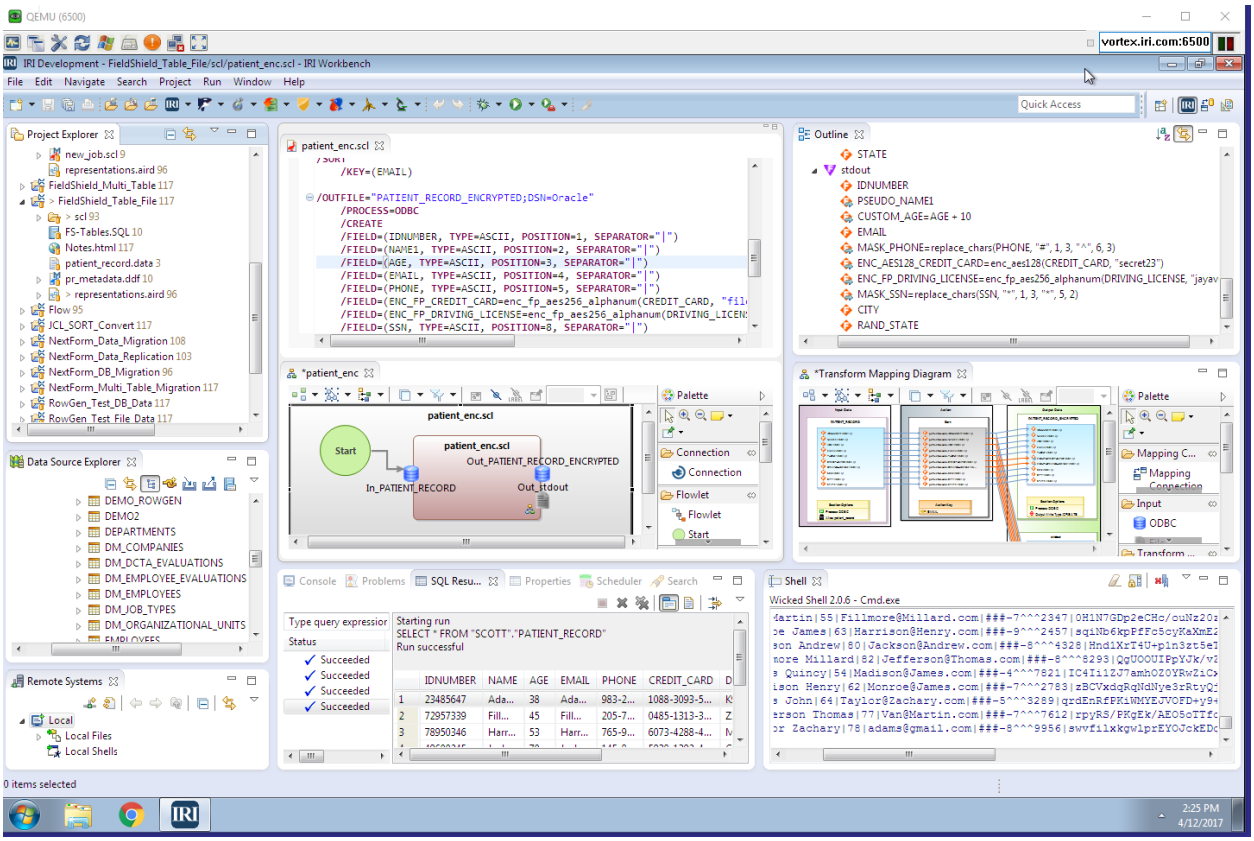
Herramienta	Tipo	Comentario
IRI Field	Comercial	Es recomendable para organizaciones que requieren una solución comercial accesible con soporte profesional
Redgate Data Masker	Comercial	Es una solución especializada para entornos Microsoft SQL Server, con excelente integración en el ecosistema Microsoft.
Microsoft SQL Server Data Masking	Comercial	ISu principal ventaja es la integración nativa y la simplicidad de implementación mediante comandos SQL estándar.

Fuente: Elaboración propia

Durante las entrevistas con el personal de TI, se confirmó que la organización utiliza MySQL como motor de base de datos principal para sus sistemas operativos y aplicaciones. Por lo tanto, las herramientas de enmascaramiento recomendadas deben ser completamente compatibles con MySQL.

Se recomienda IRI Field ya que es una herramienta comercial compatible con MySQL, su costo es accesible aproximadamente $995 anual en comparación otras alternativas Enterprise mucho más costosas, no requiere realizar cambios en infraestructura actual (MySQL), presenta una interfaz gráfica intuitiva adecuada para el nivel de conocimiento del personal, ayuda con el cumplimiento e ISO 27002 Control 5.33.

Ilustración 34: IRI Total Data Management



Fuente: IRI (s.f).

Recuperado de https://www.iri.com/

6.8.3 Acuerdos y restricciones sobre uso de datos tratados

(Control ISO/IEC 27002:2022 - 5.33 - “Protección de la información y privacidad en relaciones con terceros”)

En la actualidad, este control no se está llevando a cabo, por lo que se sugiere crear directrices formales y contractuales que aseguren la privacidad y el uso ético de los datos personales o sensibles administrados por la organización y por terceros.

Las acciones subsiguientes son consideradas de alta prioridad:

- Establecimiento de convenios de confidencialidad: Cualquier colaborador, contratista o proveedor que tenga acceso a información delicada deberá suscribir un acuerdo de confidencialidad (NDA) y aceptar las condiciones de uso exclusivo y eliminación segura posterior de los datos manejados.
- Incorporación de disposiciones contractuales con terceros: Los acuerdos deben incluir:
  - Uso de datos con propósito restringido.
  - Prohibición de copiar, reproducir o transferir sin autorización.
  - Responsabilidad de eliminación segura y privacidad después del servicio.
- Elaboración y difusión de normativas internas: Establecer y comunicar una Política Institucional sobre el Uso y Manejo Ético de la Información, que norme el acceso, tratamiento, conservación y eliminación de datos sensibles, conforme a la ISO/IEC 27002:2022 y la normativa nacional de protección de datos (Ley 8968).

Con estas acciones se pretende reforzar la responsabilidad, la trazabilidad y el cumplimiento normativo en la gestión de la información en la entidad.

6.8.4 Política de Registro y Trazabilidad del Suministro y Recepción de Datos Procesados

(Control ISO/IEC 27002:2022 - 8.15 - “Registro de eventos”)

La empresa actualmente no cuenta con mecanismos formales para rastrear y documentar el flujo de datos procesados, lo que genera riesgos en términos de responsabilidad, cumplimiento normativo y capacidad de respuesta ante incidentes de seguridad.

Para dar cumplimiento a este control, es fundamental implementar un sistema integral de trazabilidad que documente de forma exhaustiva el ciclo de vida de los datos dentro y fuera de la organización, este registro debe permitir identificar no solo los usuarios y sistemas involucrados, sino también los propósitos, momentos y condiciones bajo las cuales se realizan operaciones con datos sensibles o críticos, garantizando así transparencia, auditabilidad y cumplimiento de la ISO/IEC 27002:2022 y la Ley 8968 de Protección de Datos.

Las siguientes acciones se consideran prioritarias:

- Implementación de un sistema de trazabilidad de datos: Establecer mecanismos técnicos y procedimientos que registren de manera automatizada cada operación realizada con datos procesados, incluyendo, por ejemplo: quién accedió o procesó la información, cuando ocurrió el acceso, con qué propósito, desde qué sistema o aplicación, y en qué condiciones de seguridad.
- Adoptar herramientas especializadas de auditoría y linaje de datos (data lineage): Poder incorporar soluciones tecnológicas que faciliten el seguimiento del origen, transformación y destino de los datos a través de bases de datos, procesos ETL (Extract, Transform, Load), almacenamiento en la nube y aplicaciones empresariales.

- Generación de reportes y alertas automatizadas: Configurar el sistema de trazabilidad para que genere reportes de auditoría de forma mensual, y active alertas en tiempo real cuando se detecten transferencias de datos fuera del entorno autorizado, accesos inusuales o intentos de extracción masiva de información.

No solo para bases de datos, este sistema de trazabilidad debe aplicarse de manera integral:

- Bases de Datos
- Aplicaciones empresariales
- Sistemas de gestión documental
- Almacenamiento en la nube
- Servicios Web

Realmente a toda aquella plataforma que procese, almacene y transmita datos sensibles o críticos, con el objetivo de poder tener visibilidad completa del ciclo de vida de los datos sin importar en donde se encuentren o qué sistema los procese.

La periodicidad debe ser dual:

- ✓ **Reportes programados:** Mensualmente (o trimestralmente según la criticidad de los datos y requisitos regulatorios)
- ✓ **Alertas en tiempo real:** Inmediatas cuando se detecten anomalías, transferencias no autorizadas o accesos sospechosos.

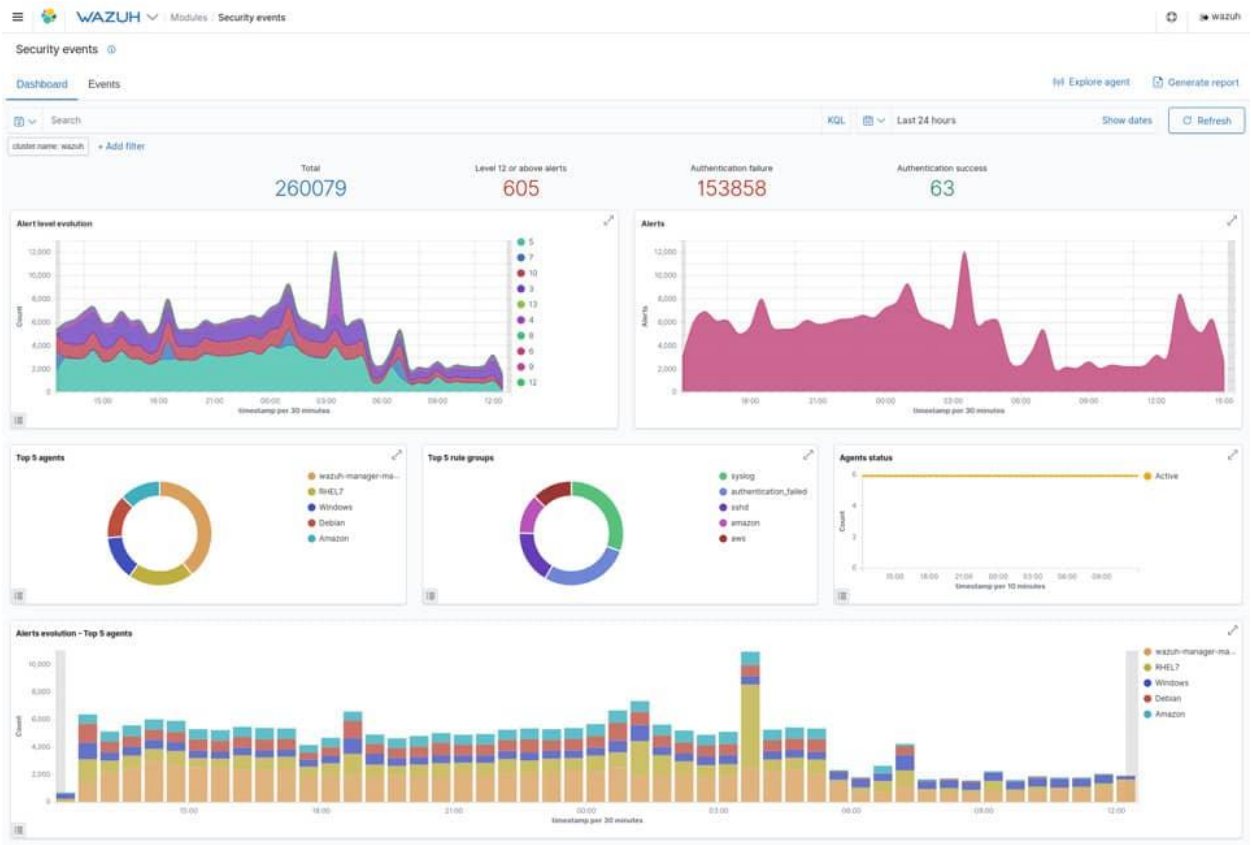
Entre algunas herramientas de apoyo podemos mencionar:

- **Microsoft Purview (antes Azure Data Catalog)**: Plataforma integral de gobernanza de datos que permite rastrear el uso, flujo y linaje de datos a través de diferentes sistemas y aplicaciones empresariales.
- **Talend Data Inventory / Governance**: Herramienta especializada en catalogación y trazabilidad de datos que facilita el descubrimiento, documentación y seguimiento del ciclo de vida de la información.
- **Splunk o Wazuh SIEM** Sistemas de gestión de información y eventos de seguridad que permiten monitorear en tiempo real la trazabilidad de accesos, transferencias de datos y actividades sospechosas en toda la infraestructura tecnológica.

Entre las herramientas antes mencionadas la opción más recomendable es **WAZUH** y les comento el porqué:

1. Cumple específicamente con el control 6.8.4 de registro y trazabilidad.
2. Es viable económicamente para cualquier organización.
3. Tiene un enfoque de seguridad que se alinea perfectamente con ISO 27002:2022.
4. Puedes incluir capturas de pantalla reales de su interfaz.
5. Es una solución moderna y ampliamente adoptada en la industria.

Ilustración 35: Wazuh



Fuente: Esgeeks (s.f).

Recuperado de https://esgeeks.com/wazuh-plataforma-seguridad-codigo-abierto/

6.9 Respaldo de información

6.9.1 Respaldos de información en elementos críticos

(Control ISO/IEC 27002:2022 - 8.13 - “Copia de seguridad de la información”)

De acuerdo con la entrevista realiza al encargado del área de infraestructura, este control se cumple realizando respaldos periódicos automatizados de servidores, bases de datos, aplicaciones empresariales, configuraciones de red, entre otros. No obstante, se identificó que actualmente no existe una clasificación formal de activos por criticidad que determine la frecuencia apropiada de

respaldo, ni procedimientos documentados para la verificación de integridad de los respaldos realizados.

Para fortalecer este control y garantizar la continuidad del negocio ante incidentes de seguridad, fallas técnicas o desastres, se recomienda implementar un esquema de respaldos diferenciado según la criticidad de los activos de información, alineado con la ISO/IEC 27002:2022 y considerando el Objetivo de Punto de Recuperación (RPO) y Objetivo de Tiempo de Recuperación (RTO) de cada sistema.

Con base en la información recopilada durante la auditoría y el análisis de los procesos críticos de la organización, se propone la siguiente periodicidad de respaldos:

Respaldos diarios (retención: 30 días)

- Bases de datos transaccionales críticas (ERP, sistemas financieros, facturación).
- Sistemas de correo electrónico corporativo.
- Aplicaciones que gestionan información de clientes o datos personales sensibles.
- Servidores de archivos con documentación operativa diaria.

Estos sistemas contienen información que cambia constantemente y cuya pérdida superior a 24 horas generaría un impacto operativo y financiero significativo para la organización.

Respaldos semanales (retención: 12 semanas)

- Bases de datos de soporte operativo (inventarios, control de activos, Help Desk).
- Sistemas de gestión de recursos humanos.
- Repositorios de proyectos y desarrollo.

Estos sistemas tienen actualizaciones menos frecuentes y un RPO de hasta 7 días es tolerable sin comprometer significativamente las operaciones.

Respaldos mensuales (retención: 12 meses)

- Configuraciones de red y equipos de infraestructura (switches, routers, firewalls).
- Bases de datos de consulta o reportería.
- Imágenes de sistemas operativos y software base.

Estos elementos tienen cambios poco frecuentes y su función es principalmente de consulta o respaldo de configuraciones que cambian esporádicamente.

6.9.2 Procedimientos de restauración y recuperación

(Control ISO/IEC 27002:2022 - 8.13 - "Copia de seguridad de la información")

En el diagnóstico realizado se detectó que, si bien la organización tiene sistemas automatizados de respaldo de información, no hay procedimientos formales documentados para la recuperación y restauración de sistemas críticos. Esta carencia constituye un peligro importante para la continuidad del negocio, ya que, si se concretan amenazas como ataques de ransomware, fallos de hardware, errores humanos, desastres naturales o corrupción de datos, la entidad podría enfrentar:

- Indisponibilidad prolongada de sistemas críticos
- Pérdida permanente de información
- Impacto financiero y reputacional
- Dependencia de conocimiento tácito

Este control es fundamental para cumplir con el objetivo del SGSI de garantizar la disponibilidad e integridad de la información, alineado con la ISO/IEC 27002:2022, y asegurar la resiliencia organizacional ante eventos disruptivos.

Para mitigar estos riesgos y fortalecer la capacidad de recuperación ante incidentes, se recomienda implementar las siguientes acciones prioritarias:

• **Documentación formal de procedimientos de restauración:** Desarrollar guías técnicas completas que expliquen de manera detallada el proceso para recuperar cada sistema, aplicación y base de datos esencial, que incluya:

- Origen del respaldo a emplear (lugar, servidor, tipo de almacenamiento)
- Secuencia precisa de procedimientos técnicos para la recuperación.
- Credenciales, autorizaciones y accesos necesarios
- Funciones y encargados de cada etapa del proceso
- Soporte técnico (proveedores, expertos internos)
- Estimaciones de tiempo para la recuperación según el sistema

• **Establecimiento de objetivos de recuperación:** Definir formalmente para cada sistema crítico:

RTO (Recovery Time Objective): Tiempo máximo aceptable de interrupción del servicio

- Sistemas críticos: RTO ≤ 4 horas
- Sistemas importantes: RTO ≤ 24 horas
- Sistemas de soporte: RTO ≤ 72 horas

RPO (Recovery Point Objective): Pérdida máxima aceptable de datos

- Sistemas transaccionales críticos: RPO ≤ 24 horas
- Sistemas operativos: RPO ≤ 7 días
- Sistemas de consulta: RPO ≤ 30 días

• **Pruebas periódicas de restauración:** Realizar ejercicios de recuperación al menos trimestralmente para validar:

- Integridad y completitud de los respaldos
- Funcionalidad de los procedimientos documentados
- Capacidad del personal para ejecutar la restauración
- Cumplimiento de los RTO y RPO establecidos

6.9.3 Almacenamiento seguro de respaldos

(Control ISO/IEC 27002:2022 - 8.13 - "Copia de seguridad de la información")

Durante el diagnóstico se identificó que este control tiene un cumplimiento parcial. Actualmente, la organización utiliza Windows Server Backup para los respaldos de servidores, los cuales se almacenan en un dispositivo NAS, y para los servicios en la nube se emplea AWS Backup. Si bien esta infraestructura proporciona una base funcional para la protección de datos, se detectaron las siguientes debilidades que incrementan el riesgo de pérdida permanente de información.

- Falta de redundancia geográfica: Los respaldos locales residen únicamente en el NAS dentro de las instalaciones, sin copias en ubicaciones alternas, lo que los expone a desastres

físicos (incendios, inundaciones, robos) que podrían destruir simultáneamente los sistemas productivos y sus respaldos.

- Ausencia del principio 3-2-1: No se cuenta con tres copias de los datos en medios diferentes, limitando las opciones de recuperación ante múltiples puntos de falla.
- Asegurarse que los respaldos o backups estén:
    - Protegidos con acceso restringido.
    - Fuera del dominio principal (ejemplo, algún entorno de red separado o almacenamiento inmutable).
    - No dejar los respaldos en el mismo servidor donde se originan los datos.
- Vulnerabilidad ante ransomware: Si el NAS está accesible desde la red principal y con credenciales administrativas compartidas, un ataque de ransomware podría cifrar tanto los servidores productivos como los respaldos almacenados en el NAS, eliminando toda posibilidad de recuperación.

Algunas soluciones que se pueden recomendar son:

- NAS con cifrado y control de acceso.
- Cloud backup Seguro (Azure, AWS, Wasabi).
- Cintas de respaldos protegidas físicamente.

Para ser más específicos la recomendación para la organización y considerando que ya cuenta con infraestructura de Windows Server Backup, NAS local y AWS Backup, la estrategia más costo-efectiva y técnicamente viable es

En los primeros 3 meses se debe realizar lo siguiente:

- Asegurar el NAS actual con las medidas de segregación, cifrado y control de acceso.
- Habilitar AWS Backup Vault Lock para inmutabilidad.
- Implementar replicación entre regiones de AWS.

Después de los 3 meses puede trabajar en:

- Extender AWS Backup para incluir servidores on-premises críticos mediante AWS Backup Gateway.
- Implementar monitoreo automatizado y alertas.
- Realizar pruebas trimestrales de restauración desde ambas fuentes (NAS y AWS).

Con estas recomendaciones la organización va a poder aprovechar la inversión tecnológica existente, fortalecer de manera significativa la postura de seguridad por ejemplo ante un ransomware o algún desastre, y cumplir con el principio 3-2-1, que garantice la disponibilidad y recuperabilidad de la información crítica conforme a los objetivos del SGSI y la ISO/IEC 27002:2022.

6.9.4 Copias de seguridad cifradas

(Control ISO/IEC 27002:2022 - 8.25 - “Cifrado”)

Por la falta del cumplimiento en este control se recomienda lo siguiente:

- Aplicar cifrado de extremo a extremo (E2EE) a:
    - Archivos antes de su respaldo.
    - Dispositivos de almacenamiento externo o servicios cloud.

- Usar algoritmos como AES-256 y almacenar las claves en un gestor seguro (HSM o Vault).

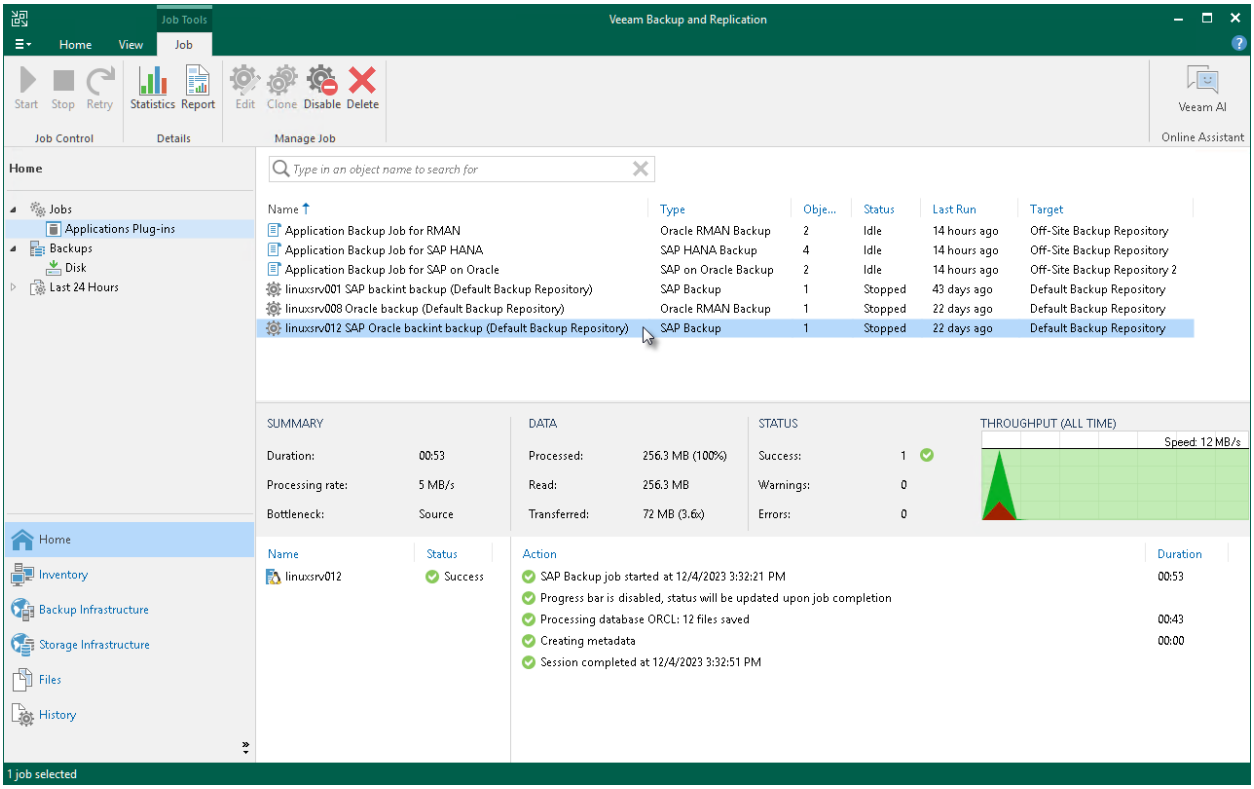
Algunas de las herramientas con cifrado integrado:

- Veeam Backup & Replication (incluye cifrado).
- Duplicati (open source).
- Acronis Cyber Protect.
- Restic, BorgBackup, Rclone (con soporte para cifrado al enviar a la nube).

Considerando el control anterior y que la organización ya utiliza Windows Server Backup + NAS +AWS Backup, se recomienda utilizar la herramienta de **Veeam Backup & Replication** por las siguientes razones:

Se integra perfecto con la infraestructura actual, es compatible de forma nativa con Windows Server (actualmente lo utilizan), se integra directamente con el NAS existente como repositorio de respaldo, también permite enviar copias cifradas a AWS (viene a complementar AWS Backup).

Ilustración 36: Veeam Backup & Replication



Fuente: Veeam Backup (s.f).

Recuperado de https://helpcenter.veeam.com/

6.10 Instalación de software en sistemas operativos

6.10.1 Se mantienen actualizadas las versiones de Windows

(Control ISO/IEC 27002:2022 - 8.8 - “Gestión de vulnerabilidades técnicas”)

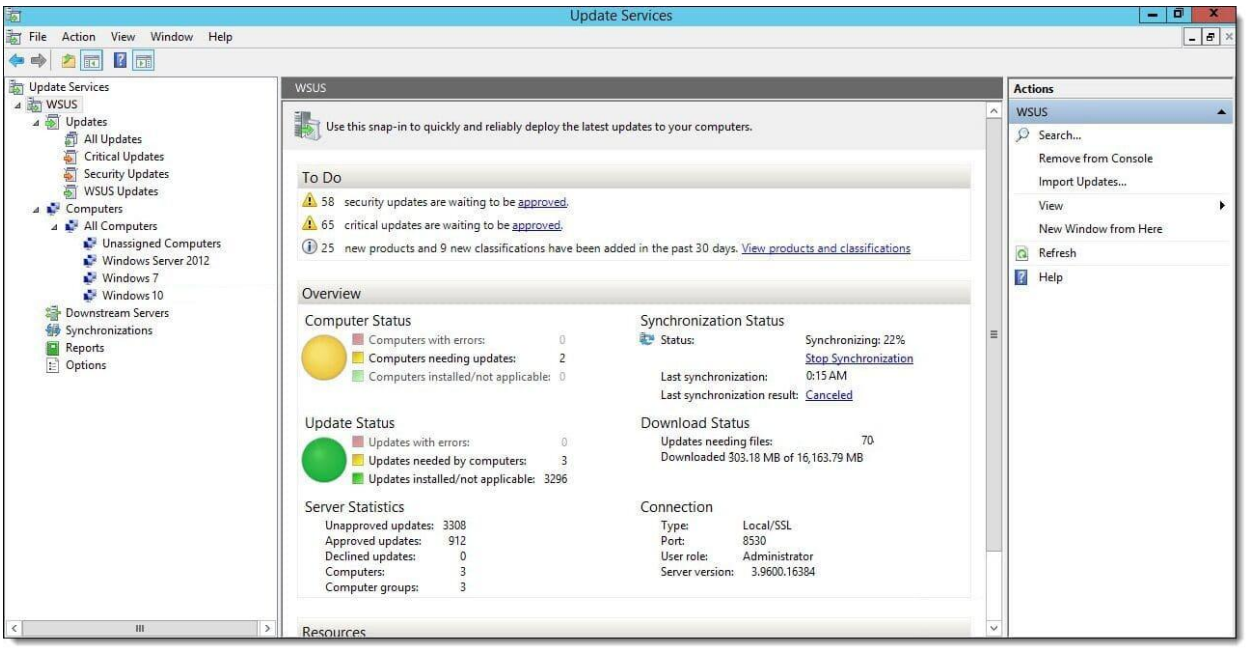
La empresa cumple con este control, sin embargo, se recomienda utilizar herramientas de gestión centralizada de parches como Microsoft Intune, Windows Server Update Services (WSUS), SCCM, ManageEngine Patch Manager.

El activar las actualizaciones de manera automática es otra de las recomendaciones, así como definir ventanas de mantenimiento programadas.

Monitorear todas aquellas versiones que se encuentren obsoletas o sin soporte.

Dado que la organización ya utiliza Windows Server y tienen Infraestructura On-Premises con Active Directory, buscan alguna solución sin costos adicionales de licenciamiento y no requieren gestión de dispositivos móviles la herramienta más viable que se les recomienda implementar es utilizar Windows Server Update Services (**WSUS**), ya que es suficiente para la gestión de parches.

Ilustración 37: WSUS



Fuente: WSUS (s.f).

Recuperado de https://learn.microsoft.com/

6.10.2 Instalar software solo después de pruebas exhaustivas

(Control ISO/IEC 27002:2022 - 8.32 - “Gestión de cambios”)

Como en el anterior control también se cumple este en la organización.

Para reforzar la continuidad del cumplimiento, se recomienda lo siguiente:

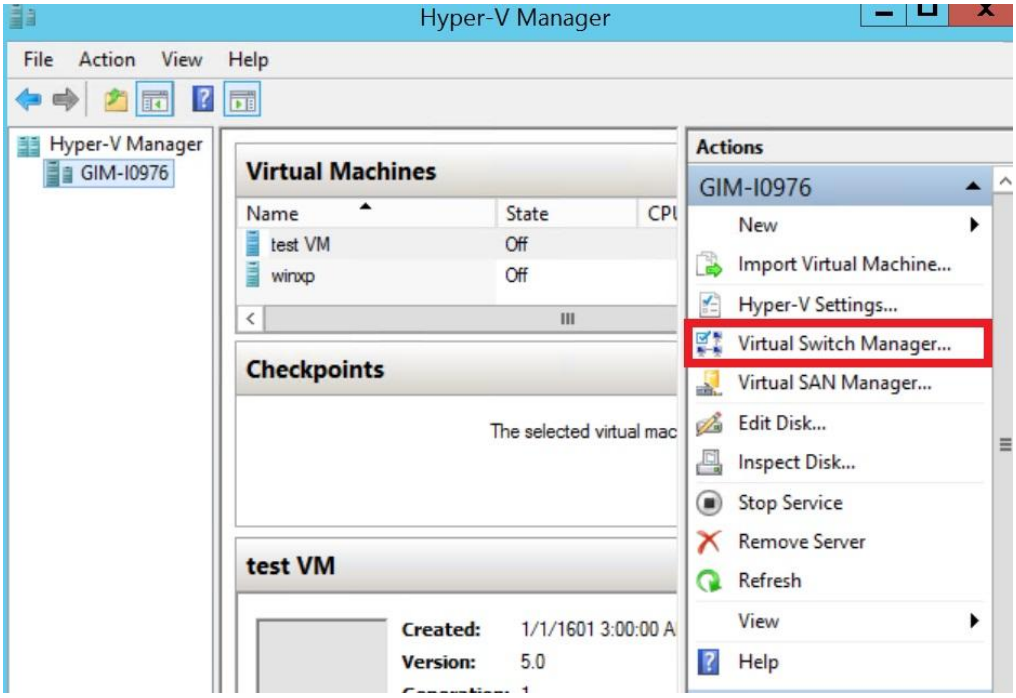
- ✓ Implementar una plataforma de pruebas previa a producción (pre-prod) donde, se simulen condiciones reales y se validen compatibilidades, desempeño y seguridad del software.
- ✓ Utilizar herramientas de virtualización o entornos de sandbox para pruebas.
- ✓ Mantener una bitácora de pruebas por cada instalación o actualización relevante.

Entre algunas herramientas útiles se pueden mencionar:

- ✓ VMware Workstation, VirtualBox, Docker, Hyper-V (para entornos aislados de prueba).
- ✓ TestRail o Jira para documentar resultados de validaciones funcionales y técnicas.

De acuerdo con que la empresa utiliza actualmente Windows Server, NAS, AWS Backup la recomendación emitida es utilizar Hyper-V que ya viene integrado de manera gratuita con Windows Server y funciona perfectamente con Active Directory, no tiene costo de licenciamiento extra, es posible crear puntos de restauración antes de pruebas y se pueden crear redes virtuales aisladas para crear un entorno aislado para pruebas.

Ilustración 38: Hyper-V



Fuente: Veeam (s.f).

Recuperado de https://www.veeam.com/

6.10.3 Se definen estrategias de reversión antes de aplicar cambios

(Control ISO/IEC 27002:2022 - 8.32 - "Gestión de cambios")

Ante la falta en el cumplimiento de este control se recomiendan lo siguiente:

Se debe definir en la política de cambios que todo cambio de software o actualización debe contar con:

- Un **backup previo** (imagen del sistema, base de datos o archivo de configuración).
- Un plan de **rollback documentado**.

Se pueden utilizar herramientas como:

- **Restaurar sistema (Windows Restore Point)**.
- **Veeam**, **Acronis**, **Clonezilla** para la creación de imágenes.
- **Snapshots en Hyper-V o VMware** si es virtualizado.

Documentar la reversión como parte del proceso de control de cambios.

6.10.4 Registro de auditoría de actualizaciones de software

(Control ISO/IEC 27002:2022 - 8.15 - “Registro de eventos”)

En la organización no se cumple este control por lo que se recomienda lo siguiente:

Activar y revisar los **logs del sistema** relacionados con instalaciones, actualizaciones y fallos:

- Visor de eventos de Windows (event logs).
- Sysmon + Wazuh o SIEM (Splunk, Graylog) para correlación avanzada.

Utilizar herramientas de gestión de configuración (CMDB) para registrar:

- Historial de software instalado.
- Parches aplicados, con fecha y responsable.

Generar reportes mensuales de cambios en sistemas operativos.

6.11 Seguridad en las redes

Es importante mencionar que para este control el objetivo fundamental es asegurar que la información que viaja a través de las redes de la organización esté protegida y que las mismas redes sean seguras.

De acuerdo con la documentación de red de la empresa la misma se encuentra incompleta y la protección de datos en redes públicas su cumplimiento es parcial.

6.11.1 Se cuenta con un diagrama de red de la infraestructura

(Control ISO/IEC 27002:2022 - 8.20 - “Seguridad de las redes”)

La empresa no tiene un diagrama de red completo ni actualizado, lo cual impide una gestión eficaz de la seguridad, dificulta la detección por ejemplo de dispositivos no autorizados, complica la resolución de problemas y retrasa la respuesta a incidentes.

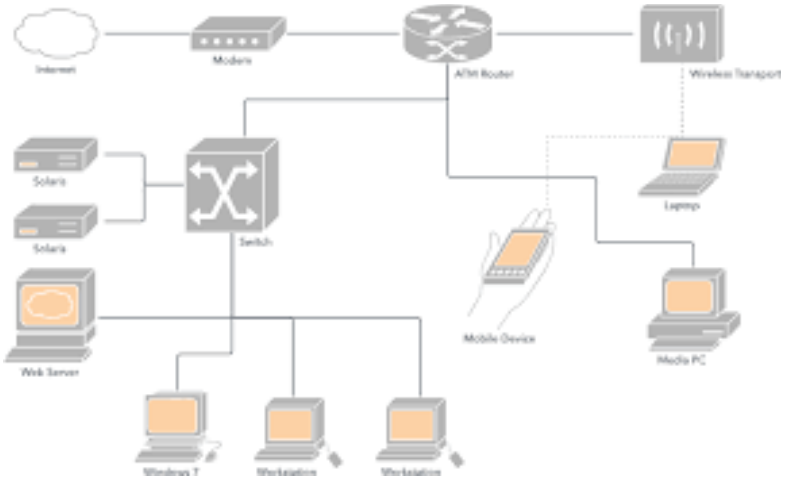
Para poder reforzar este control que se cumple de manera parcial en la organización es importante lo siguiente:

- Realizar un inventario de activos de red: En este punto se recomienda utilizar herramientas de escaneo de red como por ejemplo Nmap o Lansweeper, lo que ayuda a descubrir todos aquellos dispositivos conectados como servidores, routers, switches, firewalls, puntos de acceso Wi-fi, impresoras, entre otros.
- Se recomiendo crear o actualizar el diagrama tanto lógico como físico:
    - Diagrama Lógico: Se muestra toda la estructura de la red, incluyendo subredes, Vlan’s, direcciones IP, dominios, y equipos perimetrales (firewalls, IDS/IPS).
    - Diagrama Físico: Se muestra la ubicación física en donde se encuentran instalados los equipos (racks, centros de datos, oficinas) y la manera en que se interconectan.

- Entra algunas de las herramientas que se pueden utilizar:
    - Programas como Microsoft Visio
    - Lucidchart
    - Draw.io (gratuito)
- Una vez que se tenga creado el diagrama es recomendable que el equipo técnico valide en sitio para asegurar que coincide con la realidad.
- Se debe establecer un proceso de mantenimiento cada vez que se integre un nuevo equipo, o se modifique alguna subred o se reconfigure algun firewall, el diagrama debe estar siempre actualizado. Se podría asignar un responsable de mantenerlo al día.

Para la organización Lucidchart ofrece el mejor balance entre funcionalidad profesional, facilidad de uso, colaboración en equipo y costo razonable ($540 anual) y sería una inversión mínima considerando los beneficios.

Ilustración 39: Lucidchart



Fuente: Lucidchart (s.f).

Recuperado de https://www.lucidchart.com/

6.11.2 Se establecen controles para salvaguardar la confidencialidad e integridad de los datos

(Control ISO/IEC 27002:2022 - 8.20 - “Seguridad de las redes”)

Al igual que en el punto anterior se cumple de manera parcial en la organización.

Este es un riesgo muy alto. Si los datos viajan sin cifrar por redes públicas (como Internet), pueden ser interceptados (espionaje, robo de credenciales) o modificados (ataques de "man-in-the-middle").

Entre las soluciones recomendadas podemos indicar lo siguiente:

1. **Implementar Uso de VPN (Red Privada Virtual)**
    - Para todos los empleados que trabajen de forma remota o necesiten acceder a la red interna desde fuera de la oficina.
    - Para conectar sucursales o sitios entre sí (VPN site-to-site).
    - Asegurarse de que la VPN utilice protocolos y algoritmos de cifrado fuertes (ej. IPsec con AES-256, OpenVPN).
2. **Forzar Cifrado en Tránsito (TLS/SSL)**
    - HTTPS: Todas las aplicaciones y sitios web expuestos a Internet (portales de clientes, webmail, etc.) deben usar HTTPS (TLS 1.2 o superior) de forma obligatoria. Redirigir todo el tráfico HTTP a HTTPS.
    - Correo Electrónico: Configurar los servidores de correo para que usen cifrado en tránsito (STARTTLS, SMTPS, IMAPS).

- Transferencia de Archivos: Reemplazar el uso de FTP por protocolos seguros como SFTP (SSH File Transfer Protocol) o FTPS (FTP over SSL/TLS).

3. **Auditar Configuraciones de la Nube:** Si se utilizan servicios en la nube (IaaS, PaaS, SaaS), revisar y asegurar que todas las conexiones hacia y desde estos servicios estén debidamente cifradas.

6.11.3 Se detecta, restringe y autentica la conexión de equipos y dispositivos a la red

(Control ISO/IEC 27002:2022 - 8.21 - "Seguridad de los servicios de red")

Este control se cumple en la organización sin embargo es importante fortalecerlo con las siguientes recomendaciones:

- ✓ Implementar un NAC (Network Access Control): Una solución de NAC no solo autentica al usuario o dispositivo, sino que también puede verificar su "estado salud", de sus dispositivos antes de permitirle el acceso completo a la red.
- ✓ Segmentación de la Red y Microsegmentación: Dividir la red en segmentos (Vlans) para aislar diferentes tipos de tráfico.
- ✓ Seguridad en Puertos de Switch: Se pueden activar funciones como "port security" en los switches para limitar que direcciones MAC pueden conectarse a un puerto específico.
- ✓ Autenticación 802.1X: Implementar el estándar 802.1X para la autenticación basada en puerto, esto requiere que los usuarios/dispositivos se autentiquen antes de que el puerto de red se active.

6.11.4 Se cuenta con herramientas de monitoreo de la red

(Control ISO/IEC 27002:2022 - 8.16 - “Monitoreo de seguridad”)

Este punto también se cumple en la organización, de igual manera como en el control anterior siempre hay espacio para la mejora continua.

- ✓ Centralizar logs en un SIEM: Recolector de eventos de los logs de todas las herramientas de red (firewalls, routers, switches, VPN)
- ✓ Implementar IDS/IPS: Se puede considerar implementar un IPS que pueda no solo detectar, sino también bloquear activamente el tráfico malicioso en tiempo real.
- ✓ Análisis de flujo de red: Existen algunas herramientas que analizan los metadatos del tráfico de red.
- ✓ Definir alertas y planes de respuesta: Es importante configurara alertas significativas para eventos críticos, y tener un **plan de respuesta a incidentes** que defina quién hace qué cuando se dispara una alerta importante.

6.12 Segregación de redes

Para este control el objetivo es claro, el no tener una red “plana” en donde un atacante que compromete un solo dispositivo (como la computadora por ejemplo de una recepcionista) pueda ver y atacar directamente los servidores más críticos de la organización.

6.12.1 Cuentan con diferentes dominios de red independientes

(Control ISO/IEC 27002:2022 - 8.20 - “Seguridad de las redes”)

Acá es el problema principal, si no de definen dominios de red independientes (o zonas de seguridad), significa que la red es plana. Un atacante fácilmente puede realizar movimientos

laterales, escalando un incidente menor a un compromiso total de la red. El malware como por ejemplo un ransomware podría propagarse sin control.

Para el cumplimiento de este control se pueden emitir las siguientes recomendaciones:

- **Diseño de Áreas Seguras:** Como primer paso es conceptualizar, es necesario establecer áreas en función del grado de confianza y la función del negocio. Un modelo tradicional y altamente eficaz es:
  - DMZ (Zona Desmilitarizada): Para todos los servidores que deben ser accesibles a través de Internet como un servidor web o servidor de correo electrónico. Tiene que estar separada de la red interna.
  - Red de Producción/Servidores Críticos: Lugar donde se alojan las bases de datos, servidores de aplicaciones y controladores de dominio. El acceso a esta área debería ser el más limitado.
  - Red de Usuarios Empresariales: Espacio donde se enlazan las estaciones de trabajo y laptops de los empleados.
  - Red de Invitados (Guest): Es debe ser un aislamiento absoluto, únicamente con acceso a Internet.
  - Red de Administración: Una red aislada y altamente segura exclusivamente para que los administradores de sistemas controlen la infraestructura (routers, switches, firewalls).
  - Red de Desarrollo/Pruebas: Separada de producción para impedir que los fallos o experimentos impacten en el entorno real.
- **Implementación con Firewalls:** El firewall es la herramienta clave, se deben utilizar la capacidad de los firewalls de un switch de capa 3, en las fronteras de cada zona definida.

6.12.2 Se utilizan mecanismos como Vlans

(Control ISO/IEC 27002:2022 - 8.23 - “Filtrado de red”)

A pesar de que el control si se cumple en la organización, siempre se pueden mejorar.

La clave es auditar las reglas de enrutamiento y las ACLs entre las VLANs, asegurarse de que el tráfico entre ellas esté siendo filtrado por un firewall y que se aplique el principio de mínimo privilegio. No serviría de nada por ejemplo contar con una Vlan si una regla está configurada como “Allow any to any” porque permitiría que todo el tráfico pase libremente entre ellas.

Recomendaciones en este punto:

- Utilizar Private VLANs (PVLANs) para segmentar dispositivos en la misma VLAN, previniendo movimientos laterales indeseados entre subgrupos.
- Implementar ACLs y VACLs para regular el tráfico permitido entre VLANs y los protocolos que están limitados.
- Adoptar el principio de "mínimos privilegios", restringiendo de manera rigurosa la comunicación entre segmentos a lo que es absolutamente necesario.
- No utilizar la VLAN1 (todos los puertos por defecto) y desactivar DTP; aplicar etiquetado VLAN de manera explícita en trunks seguros.

6.12.3 Se cuenta con un tratamiento especial las redes inalámbricas

(Control ISO/IEC 27002:2022 - 8.22 - “Seguridad de las redes inalámbricas”)

En la organización este control se cumple de manera parcial por lo quiero comentar que las redes inalámbricas son por naturaleza un vector de ataque de alto riesgo debido a que su medio es

accesible para cualquiera que esté en el rango físico, tratarla como una red cableada normal es una seria una invitación a que un atacante cercano obtenga acceso directo a la red de la empresa.

Entre las recomendaciones podemos mencionar:

- **Segregación Inmediata**
  - La red Wi-Fi debe estar en una VLAN y subred distintas, totalmente aisladas de la red de servidores críticos y, de ser posible, también de la red de usuarios por cable.
  - El tráfico que proviene de la VLAN de Wi-Fi hacia otras áreas debe necesariamente transitar por un firewall y ser evaluado.
- **Establecer una Red para Visitantes (Wi-Fi para Invitados)**
  - Se debe contar con una red Wi-Fi para invitados que esté separada de la red corporativa.
  - Esta red necesita estar habilitada con "Aislamiento de Cliente", lo que evita que los dispositivos conectados puedan verse entre ellos.
  - Su única autorización debe ser conectarse a Internet. Ningún acceso a recursos internos.

- **Reforzar la Autenticación de la Red Inalámbrica Corporativa:**
  - Protocolo: Emplear WPA2/WPA3-Enterprise. Olvidar las contraseñas compartidas (PSK - Clave Precompartida).
  - Herramienta (Identificación): Configurar un servidor RADIUS, con 802.1X/RADIUS, cada usuario se identifica utilizando sus propias credenciales de dominio (nombre de usuario y contraseña), en lugar de una clave de Wi-Fi compartida.

6.12.4 Se monitorean y registran los accesos de red

(Control ISO/IEC 27002:2022 - 8.16 - “Monitoreo de seguridad”)

Este control se cumple en la organización, sin embargo, podemos fortalecerlo con las siguientes recomendaciones.

- Dirigir el Monitoreo hacia las Fronteras: Establecer el monitoreo y las notificaciones para que se enfoquen en el flujo que atraviesa las fronteras de seguridad establecidas.
    - Establecer alertar específicas de segregación: Se puede crear una notificación crítica si se identifica un intento de acceso desde la VLAN de invitados a la VLAN de Servidores.
    - Establecer una notificación de alta importancia si un equipo de la VLAN de usuarios intenta escanear puertos en la VLAN de Servidores.
- Utilizar alguna herramienta (Centralización): Redirigir todos los registros de los firewalls, switches y el servidor RADIUS hacia un sistema SIEM (Gestión de Información y Eventos de Seguridad). Esto posibilita relacionar eventos e identificar patrones de ataque que serían imperceptibles al revisar los registros de un solo dispositivo.

6.13 Filtrado Web

6.13.1 Se cuentan con controles implementados para el filtrado web

6.13.2 Se han establecido niveles de navegación web

(Control ISO/IEC 27002:2022 - 8.23 - “Filtrado de red”)

A pesar de que estos dos controles se cumplen en la organización se recomienda establecer un proceso formal de revisión trimestral o semestral de las políticas de filtrado web así también como cada uno de los niveles de navegación web.

Recomendaciones para la continuidad y monitoreo

¿Cómo lograrlo?

- ✓ Verificar al menos trimestralmente si los niveles de filtrado siguen alineados con los roles y riesgos actuales del negocio.
- ✓ Analizar los log's de tráfico bloqueados y permitidos para revisar sitios que estén siendo bloqueado por error (falsos positivos) y realizar los ajustes. Así también en busca de anomalías, como por ejemplo ¿Por qué un servidor está intentando acceder algo Google Drive, Dropbox, OneDrive entre otros?
- ✓ Documentar todos los cambios o modificaciones en la política del firewall, y llevar un registro de todos los cambios que se realicen en las diferentes reglas y roles del firewall.
- ✓ De ser posible integrar todos los eventos de filtrado en un SIEM para la correlación con otros eventos de seguridad. Algunas de las herramientas recomendadas para un SIEM podrían ser Splunk, QRadar (IBM), Microsoft Sentinel, Wazuh (Open Source).
- ✓ Utilizar herramientas nativas del NGFW/SWG o crear algún tipo de dashboards personalizados en el SIEM para tener una mejor visibilidad de la actividad web en tiempo real.

  Otras de las herramientas recomendadas:

  OpenDNS (Cisco Umbrella): Seguridad DNS y control de contenidos.

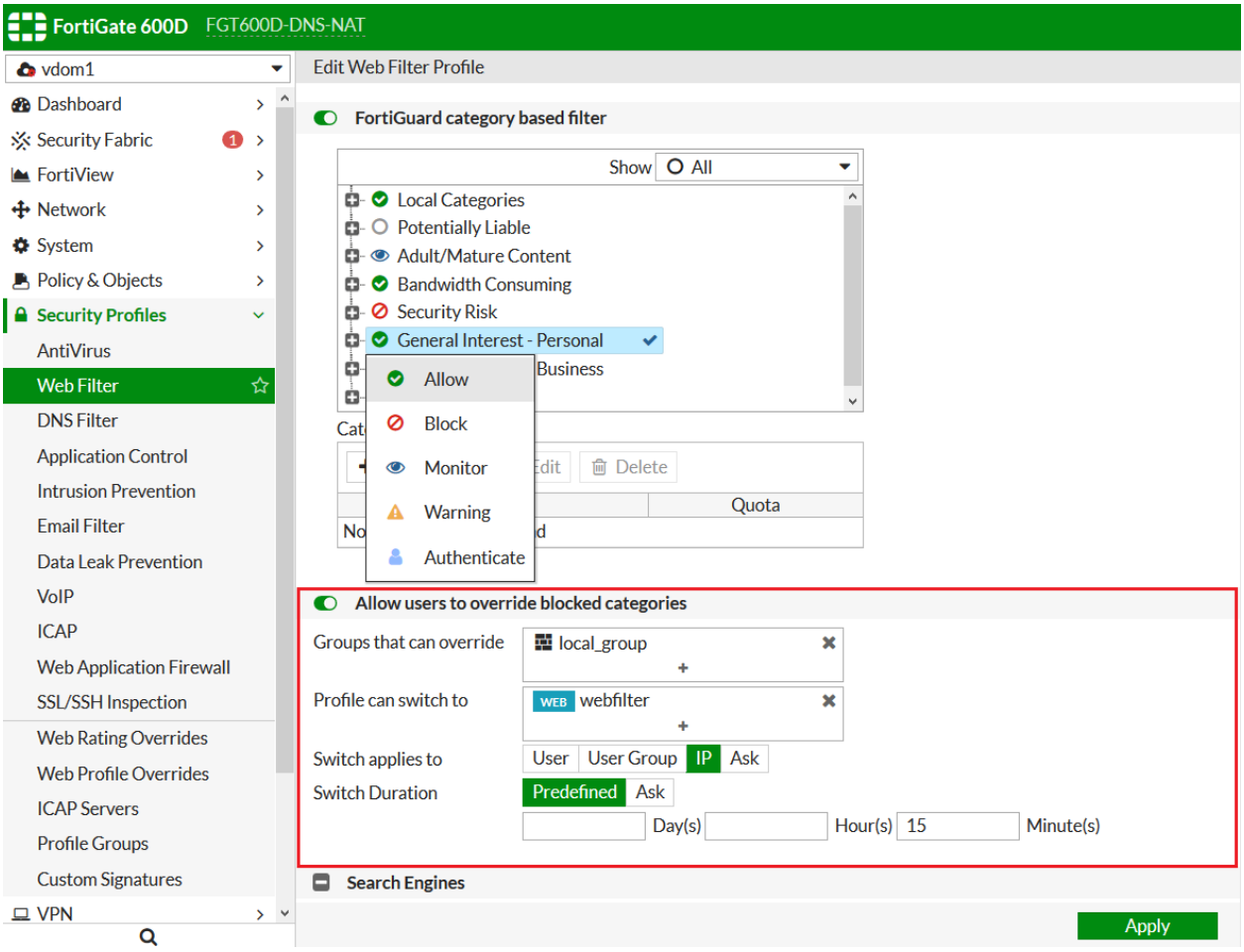
  Zscaler Internet Access: Filtrado en la nube con políticas por usuario y dispositivo.

  Microsoft Defender for Endpoint / ATP: Incluye capacidades de filtrado web.

FortiGuard Web Filtering (Fortinet) o Web Filtering de Palo Alto: Si ya cuentan con appliances de seguridad.

La recomendación para este control es utilizar FortiGuard Web Filtering ya que se integra de manera nativa con el firewall que poseen actualmente y sin costo alguno, para empezar a generar visibilidad de tráfico web en tiempo real.

Ilustración 40: FortiGuard Web Filtering



Fuente: FortiGuard (s.f).

Recuperado de https://docs.fortinet.com/

6.13.3 Equipos de seguridad

(Control ISO/IEC 27002:2022 - 8.20 “Seguridad de las redes”)

El cumplimiento de este control en la organización es parcial, por lo que emitiremos algunas recomendaciones a seguir para mejorar o remediar este.

- Es vital mantener la implementación de un firewall de nueva generación (NGFW), que incluyan funcionalidades de filtrado web, inspección SSL y control de aplicaciones. El cual también debe incluirse en el programa de gestión de vulnerabilidades de la organización, ya que el propio equipo de seguridad puede ser un punto de fallo si no se mantiene actualizado.
- Appliance dedicado de seguridad web (SWG): Como por ejemplo Blue Coat ProxySG, Squid Proxy + SquidGuard (esto para entornos más pequeños o controlados).
- Se recomienda aplicar reglas por grupos, ubicación o tipo de dispositivos con autenticación del usuario.
- Realizar bloqueos de dominios maliciosos (DNS sinkhole), que viene a ser un complemento para bloquear todos aquellos intentos de conexión a C2s.
- Se recomienda también realizar pruebas periódicas para validar que las reglas establecidas de bloqueo funcionen de manera correcta, por ejemplo, realizar pruebas manuales desde algún equipo de usuario final en cada segmento de red, intentar acceder a sitios web que deberían estar bloqueados según la política de ese segmento. Documentar los resultados.
- Utilizar sitios web diseñados específicamente para probar los filtros web, como por ejemplo testmyids.com o los proporcionados por los propios fabricantes.
- De ser posible incluir como objetivo en las pruebas de penetración internar el intento de evadir los controles de filtrado web.

6.13.4 Capacitación al personal

(Control ISO/IEC 27002:2022 - 6.3 - “Concienciación, educación y formación en seguridad de la información”)

Es importante mantener un constante reforzamiento en la concienciación de la seguridad en la navegación web para todo el personal con privilegios más elevados, no es solo una buena práctica, sino más bien una necesidad crítica para proteger los activos más valiosos de la empresa y garantizar su continuidad operativa y reputación.

¿Cómo lograr esta conciencia?

- **Capacitación continua y personalizada:** No es suficiente con solo una sesión de capacitación. Las amenazas cambian, y el personal con privilegios debe mantenerse al día con las tácticas de ataque más recientes. La formación tiene que ser práctica, incluyendo ejemplos auténticos y simulaciones de ciberataques (como intentos de phishing).
- **Políticas claras y aplicables:** Implementar normas rigurosas respecto al uso de internet, descargas, acceso a páginas web, uso de redes sociales y administración de contraseñas, y garantizar que el personal autorizado las comprenda y respete.
- **Principio de mínimo privilegio:** Garantizar que el personal cuente únicamente con los permisos necesarios para llevar a cabo su labor y nada adicional. Esto minimiza el daño posible en caso de una violación.
- **Monitore y auditorias:** Instalar sistemas de vigilancia para identificar acciones inusuales y llevar a cabo auditorías periódicas sobre los accesos y el comportamiento en línea del personal con privilegios.

- **Cultura de seguridad:** Promover una cultura en la que la seguridad es una responsabilidad compartida, y donde los trabajadores se sientan a gusto al informar sobre posibles incidentes o irregularidades sin temor a represalias. Existen herramientas como KnowBe4, Infosec IQ, LMS corporativo.

6.14 Ciclo de vida del desarrollo seguro

6.14.1 Políticas y procedimientos de desarrollo seguro

(Control ISO/IEC 27002:2022 - 8.25 - "Desarrollo seguro del software y los sistemas")

En este punto existe una carencia de políticas y procedimientos que no se encuentran bien documentados, esto le podemos llamar un fallo de gobierno. Sin embargo, no tener un marco bien definido cualquier esfuerzo de seguridad será inconsistente y no auditable.

La seguridad depende de las buenas intenciones de individuos, no de un proceso institucionalizado.

Recomendaciones:

Se debe establecer y formalizar una política de desarrollo seguro y los procedimientos asociados.

Pasos y algunas herramientas:

- Adoptar un Marco de Referencia: Se trata de ajustar la política actual en marcos reconocidos.

  Herramientas/Marco

  - OWASP SAMM (Software Assurance Maturity Model): Es un modelo de madurez excelente que te ayuda a evaluar tu estado actual y a planificar mejoras incrementales en cinco áreas de negocio: Gobierno, Diseño, Implementación, Verificación y Operaciones.

- NIST SSDF (Secure Software Development Framework): Un marco muy completo del gobierno de EE. UU. que proporciona un conjunto de prácticas de alto nivel para un desarrollo seguro.
- Microsoft SDL (Security Development Lifecycle): Un proceso muy maduro y bien documentado que ha sido probado en uno de los entornos de desarrollo más grandes del mundo.

- Documentar la Política: Se debe crear un documento formal que sea aprobado por la dirección:

  Contenido Clave de la Política

  - Propósito y Alcance: A qué desarrollos aplica.
  - Roles y Responsabilidades: Quién es el "Campeón de Seguridad" (Security Champion), responsabilidades de los desarrolladores, arquitectos, etc.
  - Requisitos Obligatorios: Mandatos como "Toda nueva aplicación debe pasar por un análisis de código estático antes del despliegue", "Se prohíbe el uso de librerías con vulnerabilidades conocidas".
  - Referencias: Enlaces a las guías de codificación segura, procedimientos de prueba, etc.

6.14.2 Separación de entornos

(Control ISO/IEC 27002:2022 - 8.31 - “Separación de los entornos de desarrollo, prueba y producción”)

Este es un pilar fundamental y se cumple en la empresa, es un excelente punto de partida que reduce significativamente el riesgo de cambios no autorizados y la exposición de los datos.

Como en los controles anteriores y de cumplimiento siempre es bueno reforzar cada control a pesar de que se cumplan en la empresa para la continuidad, por lo que recomendamos lo siguiente:

- Fortalecer el control de acceso entre ambientes utilizando principios de mínimo privilegio.
- Realizar segmentación de red para impedir que los entornos se comuniquen de manera directa.
- Realizar auditorías periódicas para asegurarse de que no existan datos reales en entornos de prueba o desarrollo.
- Automatizar la provisión de entornos para prevenir configuraciones manuales no segura.

Algunas de las herramientas recomendadas podemos mencionar:

- Terraform + Ansible: Aprovisionamiento y configuración segura.
- HashiCorp Vault: Separa y controla credenciales por entorno.
- AWS Organizations, Azure Dev/Test Labs, o Google Cloud Projects: Segmenta entornos en la nube.
- Jenkins: Con pipelines diferenciados por entorno y revisión de acceso.

Se recomienda adquirir Terraform + Ansiblel le permiten reforzar la separación de entornos mediante automatización, configuración segura e infraestructura como código, reduciendo errores manuales y garantizando consistencia.

Favorece a la consistencia y trazabilidad en las implementaciones, asegurando que todos los entornos sean creados bajo los mismos estándares de seguridad.

6.14.3 Directrices de codificación segura

(Control ISO/IEC 27002:2022 - 8.28 - “Principios de codificación segura”)

No hay en la organización directrices de codificación segura por lo que se recomienda crear y mantener guías de codificación segura específicas para los lenguajes y frameworks que utiliza la empresa.

¿De qué manera y con que herramientas poder realizarlo?

No escribas todo desde cero, sino más bien se deben de utilizar guías ya existentes y ajustarlas a guías de expertos.

Herramientas:

- OWASP Secure Coding Practices-Quick Reference Guide: Un excelente punto de partida, agnóstico al lenguaje.
- OWASP Cheat Sheet Series: Guías detalladas y prácticas para prevenir vulnerabilidades específicas (ej: "SQL Injection Prevention Cheat Sheet", "Cross-Site Scripting (XSS) Prevention Cheat Sheet"). Son extremadamente útiles.
- Guías Específicas del Lenguaje: Buscar guías como "SEI CERT Oracle Coding Standard for Java" o guías de seguridad para frameworks como Django, Ruby on Rails, etc.

Automatizar la verificación de estándares mediante la implementación de herramientas que analicen el código fuente en busca de patrones que violen estas directrices.

Herramientas:

- Comerciales: Veracode, Checkmarx, SonarQube (tiene versión gratuita y de pago).
- Open Source: SonarLint (plugin para el IDE del desarrollador), Snyk Code (tiene un plan gratuito generoso), Bandit (para Python), Brakeman (para Ruby on Rails).

Integrar estas herramientas directamente en el pipeline de CI/CD (con Jenkins, GitLab CI, GitHub Actions) para que se ejecuten automáticamente con cada cambio de código.

6.14.4 Formación continua en desarrollo seguro

(Control ISO/IEC 27002:2022 - 6.3 - "Concienciación, educación y formación en seguridad de la información")

La recomendación para el cumplimiento de este control es la implementación de un programa de formación continuo y práctico para todo el equipo de desarrollo, así también fomentar una cultura de seguridad.

¿Cómo hacerlo?

- Realizar un plan anual de formación en desarrollo seguro y en los 10 principales riesgos de OWASP.
- Llevar a cabo talleres prácticos y CTFs internos (Capture The Flag) enfocados en vulnerabilidades.
- Incorporar capacitación dentro del proceso de inducción para nuevos programadores.
- Evaluar la efectividad mediante evaluaciones o revisiones de código posteriores

Algunas de las plataformas y recursos recomendados podemos mencionar los siguientes:

- Secure Code Warrior, HackEDU (Now Security Journey): Plataformas de formación práctica.
- OWASP WebGoat, Juice Shop, Damn Vulnerable Web App (DVWA): Laboratorios para entrenar.
- TryHackMe, PortSwigger Academy, Cybrary: Plataformas para formación técnica.
- LMS corporativo con contenidos sobre codificación segura.

6.15 Desarrollo externalizado

6.15.1 Acuerdos contractuales con requisitos de seguridad

(Control ISO/IEC 27002:2022 - 5.19 - “Acuerdos con los proveedores”)

Este control se cumple en la empresa si embargo se recomienda dar continuidad estableciendo un proceso de revisión anual del anexo de seguridad en los contratos. Las amenazas y las tecnologías cambian, el contrato no debe ser estático.

Una de las acciones a tomar es añadir una cláusula que obligue a una revisión anual. Incluir nuevos requisitos a medida que la organización madure su propia seguridad (por ejemplo: es exigir que el proveedor realice análisis SAST a su código).

6.15.2 Supervisión regular de actividades de desarrollo subcontratado

(Control ISO/IEC 27002:2022 - 5.20 - “Gestión de la seguridad de la información en la cadena de suministro”)

Como en el control anterior, este punto también se cumple en la organización, para dar continuidad se recomienda automatizar la supervisión y definir indicadores clave de rendimiento (KPIs) y de Riesgo (KRIs).

¿Qué acciones se podrían tomar?

- Registros de Acceso: Establecer notificaciones automáticas (en el SIEM o la herramienta de acceso) para comportamientos sospechosos: conexiones en horarios no laborales, intentos de acceso a sistemas prohibidos, descargas masivas de información.
- Revisión del Código: Si el proveedor proporciona código, este debe someterse a las mismas herramientas de análisis estático (SAST) que el código interno antes de ser admitido en el repositorio de la organización.
- Métricas: Evaluar y comunicar acerca de: "Cantidad de vulnerabilidades graves detectadas en el código del proveedor", "Cantidad de intentos de acceso no permitidos interceptados".

6.15.3 Cláusulas de derecho de auditoría en contratos

(Control ISO/IEC 27002:2022 - 5.19 - “Acuerdos con los proveedores”)

Es recomendable para su continuidad en este control poder ejercer el derecho de auditoría, el tener el derecho, pero no usarlo tiene poco valor para la empresa.

Acción que se recomienda:

- Organizar Auditorías: Llevar a cabo una auditoría al menos anualmente o cada vez que se firme un contrato relevante.
- Tipo de Auditoría: Puede consistir en un cuestionario básico de seguridad, en la petición de informes de sus auditorías anteriores (por ejemplo, SOC 2, ISO 27001) o, si el riesgo es significativo, en una auditoría técnica más exhaustiva.
- Manejar los Resultados: Abordar los resultados de la auditoría del proveedor como cualquier otro peligro de seguridad, designando responsables y plazos de corrección

6.15.4 Herramientas de seguridad para la conexión de proveedores externos

(Control ISO/IEC 27002:2022 - 8.21 - "Seguridad de los servicios de red")

Este control no se cumple en la organización, no se cuentan con herramientas de seguridad para la conexión, lo cual es una brecha técnica de alto riegos, significa que, a pesar de tener buenos contratos, la conexión real del proveedor a los recursos de la empresa es insegura. Es como tener una puerta blindada (el contrato) pero dejarla abierta y sin cerradura (la conexión). Con este podemos mencionar que anula en gran medida la efectividad de los otros controles.

A continuación, se indicarán algunas recomendaciones, herramientas y tecnologías a considerar:

Primeramente, como recomendación se debe de implementar una solución de acceso remoto seguro dedicada para proveedores externos. El objetivo es proporcionar un acceso granular, auditado y basado en el principio mínimo privilegio. Nunca se debe dar a un proveedor una VPN "general" que le dé acceso a toda la red interna de la organización.

VPN de Acceso Remoto: Utilizar la funcionalidad de VPN de acceso remoto del Firewall de nueva generación (NGFW) existente.

¿Como poder cumplir con este control?

- ✓ Autenticación Robusta: Solicitar Autenticación Multifactor (MFA) para todos los accesos de proveedores. Esto no es innegociable.
- ✓ Políticas de Firewall Específicas: Formar un grupo de usuarios para cada proveedor ("Proveedor_A", "Proveedor_B") y establecer reglas de firewall que les den acceso únicamente a los servidores y puertos esenciales para sus labores. Bloquear todo lo restante.
- ✓ Verificación del Host / Evaluación de Postura: Configurar la VPN para que valide que el dispositivo del proveedor y que cumpla con los estándares mínimos de seguridad (por ejemplo: posee antivirus actualizado, firewall local activado) antes de autorizar la conexión.

  Herramientas: Funcionalidades nativas por ejemplo de WatchGuard, Fortinet, Palo Alto.

Zero Trust Network Access: Esta es la evolución de la VPN, en lugar de dar acceso a la "red", ZTNA da acceso a aplicaciones específicas, y valida la identidad y la seguridad del dispositivo en cada solicitud. El proveedor nunca está "dentro" de la red.

¿Como cumple el control?

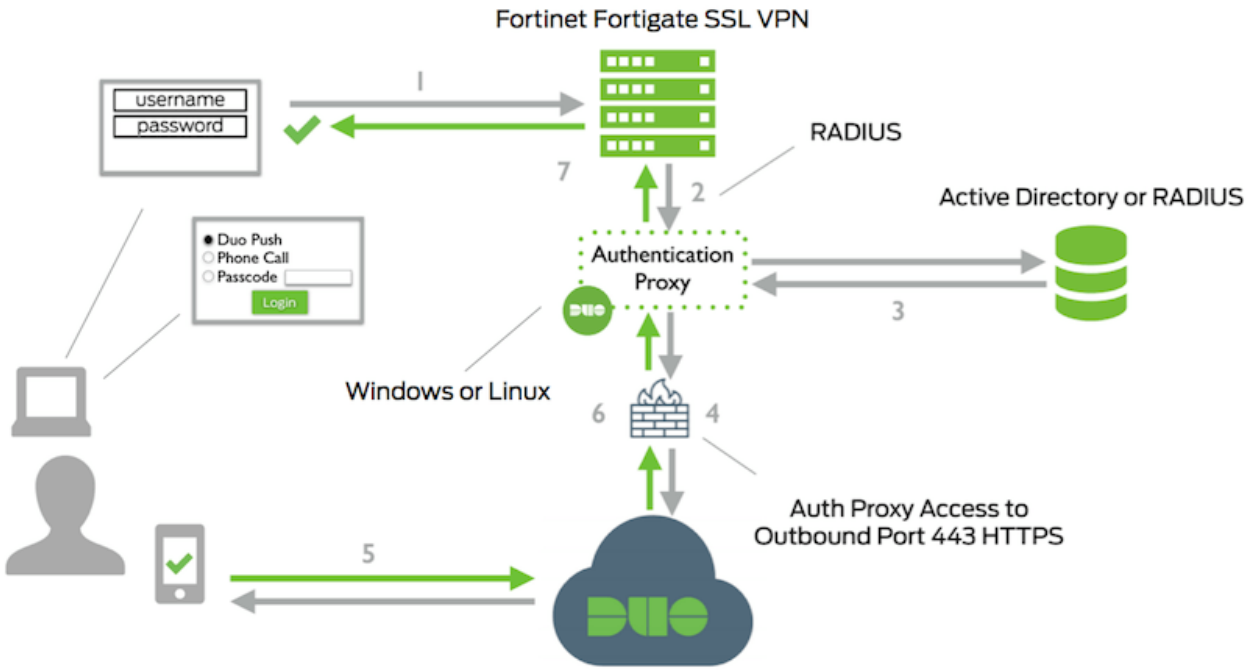
- ✓ Mínimo Privilegio por Defecto: Los proveedores solo tienen acceso a las aplicaciones que se les ha autorizado, el restante de la red les resulta invisible.
- ✓ Seguridad Avanzada: Reducción del área vulnerable, si el equipo de un proveedor resulta comprometido, el daño se restringe a las aplicaciones a las que tenía acceso, no a toda la red.
- ✓ Experiencia de Usuario Optimizada: Usualmente más sencilla y veloz que una VPN convencional.

Herramientas: Zscaler Private Access, Netskope Private Access, Cloudflare Access.

Para este control la herramienta recomendada Fortinet ZTNA / FortiGate VPN SSL con MFA y segmentación de acceso, y el motivo es porque esta herramienta se integra con la infraestructura ya existente, ofrece control granular, autenticación robusta y registro de accesos.

Reduce drásticamente el riesgo de acceso no autorizado de proveedores, cumpliendo con el control 8.21 “Seguridad de los servicios de red” de la ISO 27002:2022 y reforzando la postura de seguridad perimetral.

Ilustración 41: Fortinet Fortigate SSL VPN



Fuente: Fortinet (s.f).

Recuperado de https://duo.com/docs/fortinet

6.16 Separación de los entornos de desarrollo, prueba y producción

6.16.1 Separación adecuada entre entornos

6.16.2 Uso de ambientes de prueba antes de producción

(Control ISO/IEC 27002:2022 - 8.31 - “Separación de los entornos de desarrollo, prueba y producción”)

Para estos dos puntos de controles es fundamental su cumplimiento en la organización ya que tienen la base estructural, los entornos existen de forma aislada.

Esto indica que tienen un proceso para validar cambios antes de desplegarlos en un ambiente de producción, lo cual reduce el riesgo de introducir errores en este ambiente productivo.

El objetivo es mantenerla y auditarla

Para dar continuidad con el control 6.16.1 se recomienda auditar periódicamente la segmentación de red para asegurar que no hay “fugas” entre los entornos.

Existe algunas recomendaciones de como poder realizarlo:

- ✓ Evaluación de Reglas de Firewall: Cada tres meses, examinar las reglas del firewall que regulan el flujo de datos entre la VLAN de Desarrollo, Pruebas y Producción. No debe existir ninguna norma que autorice el tráfico directo, excepto para el pipeline de CI/CD.
- ✓ Pruebas de Penetración: Incluir dentro del alcance de las pruebas de penetración internas el esfuerzo por moverse de un entorno a otro (por ejemplo: desde un servidor de desarrollo vulnerado, intentar acceder a producción).

Para el control 6.16.2 es recomendable implementar el uso de datos de pruebas sanitizados y evitar el uso de datos de producción reales en los entornos de prueba, porque es necesario los datos para

las pruebas, crear un proceso documentado y automatizado que copie los datos de producción y los anonimice o enmascare antes de cargarlos en el entorno de pruebas. Esto protege los datos sensibles si el entorno de pruebas (que suele ser menos seguro) sea comprometido.

Para el enmascaramiento de datos existen herramientas específicas, o en muchas ocasiones se pueden crear scripts personalizados.

6.16.3 Copias de seguridad de los entornos

(Control ISO/IEC 27002:2022 - 8.13 - "Copia de seguridad de la información")

El cumplimiento parcial de este control, si es una debilidad grave de resiliencia. Si el entorno de desarrollo o prueba se corrompe (por un error humano, un ataque de ransomware, entre otros), podrían perderse semanas o meses de trabajo. Las copias de seguridad de producción son vitales para el negocio, pero las de desarrollo son vitales para la continuidad del desarrollo.

Entonces como recomendación es el implementar y automatizar una política de copias de seguridad para todos los entornos, ajustando la frecuencia y retención según la criticidad de cada uno.

1. Definir la política de backup:
    a. Determinar el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO) para cada entorno.
    b. Ejemplo de la política:
        - Producción: Respaldos completos cada día, incrementales cada hora. Retención de 30 días, con copias cada mes durante 1 año.
        - Desarrollo/Pruebas: Copias de seguridad completas cada semana, incrementales cada día. Retención por 15 días.

c. No olvidar realizar backups de los repositorios de código fuente. Existen plataformas como GitHub/GitLab que ofrecen sus propias soluciones, pero tener una copia externa es una buena práctica.

2. Implementar la solución de backup:
    - Para máquinas virtuales (VMs): Veem Backup & Replication, Cohesity, Rubrik. Son pioneros en el mercado y sumamente sencillos de automatizar.
    - Para Bases de Datos: Emplear las herramientas integradas de la base de datos (por ejemplo: Planes de Mantenimiento de SQL Server, pg_dump para PostgreSQL) o alternativas de respaldo que se acoplen a ellas.
    - Para Repositorios Git: Rewind (anteriormente BackHub) para GitHub, o scripts específicos que duplican los repositorios a un almacenamiento protegido.
3. Probar las restauraciones: Se recomienda realizar estas pruebas de restauración de manera periódica para asegurar que los backups sean válidos y que el proceso de recuperación sea efectivo y funcione de manera correcta.

6.16.4 Control de acceso en desarrollo y producción

(Control ISO/IEC 27002:2022 - 5.18 - “Acceso a la información”)

En la organización no existe un control de acceso definido para cada ambiente, esta es la brecha de seguridad más crítica, sin control de acceso, la separación de los diferentes entornos pierde gran parte de su valor.

Significa que un desarrollador podría tener acceso a producción, o un operador de sistemas podría modificar código en desarrollo. Esto abre la puerta a fraudes, sabotajes y errores catastróficos.

La recomendación para poder remediar este control es la implementación de un control de acceso basado en roles, estricto para cada entorno, siguiente el principio de mínimo privilegio, nadie debe tener acceso a un entorno que no sea absolutamente necesario para su función.

1. Definir Roles y una matriz de acceso: Se puede crear un documento que defina los roles (por ejemplo, el "Desarrollador", "QA", "Operador de TI", "DBA") y á que entornos y con qué nivel de privilegios puede acceder cada rol.

Tabla 9. Definición de Roles

ROL	Entorno Desarrollo	Entorno Pruebas	Entorno Producción
Desarrollador	Lectura/Escritura (Código)	Solo Lectura	Sin Acceso
QA	Sin Acceso	Lectura/Escritura	Sin Acceso
Operador de TI	Solo Lectura (Logs)	Solo Lectura (Logs)	Lectura/Escritura
DBA	Sin Acceso	Lectura/Escritura	Lectura/Escritura

Fuente: Elaboración Propia

2. Implementar técnicamente el control de acceso:
    - Active Directory (AD) / Azure AD: Establecer grupos de seguridad para cada combinación de rol y entorno (por ejemplo: G_Desarrollo_Acceso_Lectura, G_Produccion_Acceso_Escritura). Asignar usuarios a estos grupos y utilizar los grupos para otorgar permisos en los servidores y aplicaciones.
    - Gestión de Acceso Privilegiado (PAM): Para acceder a producción, utilizar una herramienta PAM es el estándar ideal, implementa la autenticación de múltiples factores (MFA), registra las sesiones y maneja las credenciales de manera segura. Herramientas como CyberArk, Delinea o Teleport (código abierto).

- Secretos de CI/CD: El pipeline de implementación automática (por ejemplo: Jenkins, GitLab CI) necesita contar con sus propias credenciales para realizar despliegues en producción, distintas de cualquier usuario humano, utilizar un repositorio de secretos como HashiCorp Vault o las características integradas de la plataforma de CI/CD.

6.17 Desarrollo de la propuesta de implementación del plan de seguridad informática

Para este apartado del documento y de acuerdo con todo el análisis realizado durante el proceso del proyecto, para hacerlo más digerible y transformarlo en un plan de acción, se ha creado una tabla en donde se consolida cada uno de los controles tratados en el cual resume el estado actual, se propone una acción y, lo más importante se sugiere una herramienta o solución especifica recomendada basada en las opciones del capítulo V y las mejores prácticas. También se añadió una columna de prioridad para ayudar a enfocar los esfuerzos iniciales.

Ilustración 42: Plan de Seguridad Informática para los Controles Tecnológicos basados en la ISO27002

Desarrollo de la propuesta de implementación del plan de seguridad informática

Proyecto Final de Tesis

Año 2025 - 2026

N°	Control Tecnológico	Estado Actual	Recomendación	Herramienta/Solución Recomendada	Prioridad Sugerida
6.1	Políticas, Normas y Procedimientos	No se cumple por la ausencia de marco normativo robusto	Elaborar y formalizar el marco documental de seguridad de la información	Desarrollar una Política de Seguridad, normas específicas (uso de contraseñas, respaldos) y procedimientos detallados.	Alta
6.2	Dispositivos Terminales de Usuario	Cumplimiento Parcial	Centralizar el inventario, implementar cifrado de disco y control de aplicaciones.	**Microsoft Intune**	Alta
6.3	Derechos de Acceso Privilegiado	Cumplimiento Parcial pero necesitan PAM y auditoria	Implementar una solución de Gestión de Acceso Privilegiado (PAM) y centralizar los registros.	**Azure Privileged Identity Management**	Alta
6.4	Autenticación Segura	Cumplimiento Parcial requieren implementar MFA y politicas mas robustas	Implementar Doble Factor de Autenticación (MFA) de forma obligatoria y robustecer la política de contraseñas.	**Microsoft Authenticator**	Alta
6.5	Proteccion contra el Malware	Cumplimiento Parcial no cuentan con software robusto y sin detección	Implementar una solución de EDR (Endpoint Detection and Response) y un control de inventario de software.	**WatchGuard EPDR**	Alta
6.6	Gestión de Vulnerabilidades técnicas	No se cumple, no cuentan con escaneos ni parches formales	Establecer un proceso formal de gestión de parches y realizar escaneos de vulnerabilidades periódicos.	**WSUS**	Alta
6.7	Supresión de Información	Cumpimiento Parcial	Implementar políticas y herramientas de borrado seguro para discos duros y SSDs.	**Eraser (Windows) / ShredWipe (Linux)**	Media

6.8	Enmascarmiento de Datos	No se cumple	Implementar técnicas de enmascaramiento de datos para entornos no productivos (desarrollo, pruebas).	**IRI Total Data Management**	Media
6.9	Respaldo de Información	Cumplimiento Parcial ya que el almacenamiento y cifrado es débil	Aplicar la regla 3-2-1, asegurar el almacenamiento y cifrar las copias de seguridad de extremo a extremo	**Veeam Backup & Replication**	Alta
6.10	Instalación de Software SO	No se cumple por la falta de estrategia de reversión y auditoría	Definir y documentar planes de *rollback* y activar la auditoría de instalación de software	**Hyper-V / Sysmon + SIEM** para auditoría.	Media
6.11	Seguridad en las Redes	Cumpliento Parcial por el diagrama incomplento y cifrado débil	Crear y mantener un diagrama de red actualizado y forzar el cifrado en tránsito para todo el tráfico.	**Lucidchart** para diagramas. **VPN del NGFW** y forzar TLS 1.2+ en todos los servicios.	Alta
6.12	Segregación de Redes	No se cumple, presentan una red plana	Diseñar e implementar una arquitectura de red segmentada (VLANs) con zonas de seguridad.	**Configuración de NGFW y Switches de Capa 3:** Usar la capacidad de los equipos existentes para crear VLANs y ACLs.	Alta
6.13	Filtrado Web	Cumplimiento Parcial	Mejorar el filtrado de contenidos web y bloquear dominios maliciosos a nivel de DNS.	**FortiGuard Web Filtering**	Media
6.14	Ciclo de Vida del Desarrollo Seguro	No se cumple	Adoptar un marco de desarrollo seguro (ej. OWASP SAMM) e integrar herramientas de análisis de código (SAST).	**SonarQube**	Media
6.15	Desarrollo Externalizado	Cumplimiento Parcial presenta una brecha técnica grave	Implementar una solución de acceso remoto seguro y granular para proveedores, eliminando VPNs generales.	**Fortinet Fortigate SSL VPN**	Alta
6.16	Separación de Entornos de Desarrollo, Prueba y Producción	Cumplimiento Parcial por la falta de control en los accesos	Implementar un control de acceso estricto basado en roles (RBAC) entre los diferentes entornos.	**Grupos de Active Directory / Azure AD:** Para definir permisos granulares por rol y entorno	Alta

Fuente: Elaboración Propia

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.18.1 Conclusiones

Para el objetivo número 1 de acuerdo con la matriz de coherencia, se centra en analizar la situación actual de la organización la cual ha sido alcanzado con éxito en su 100 porciento.

El diagnóstico no solo ha identificado brechas y vulnerabilidades claras, sino que también ha revelado una percepción interna favorable hacia la necesidad de un cambio, reconociendo que un plan formal de seguridad es indispensable.

De acuerdo con el capítulo IV del proyecto “DIAGNÓSTICO DE LA SITUACIÓN ACTUAL”, este proporciona una base sólida y una justificación irrefutable para las soluciones y el plan de implementación que se propondrán en los capítulos posteriores, sirviendo como hoja de ruta para elevar la postura de seguridad de la organización de un estado reactivo a uno resiliente y proactivo.

Para el objetivo número 2 el cual es identificar el cumplimiento o no de los controles tecnológicos de seguridad informática según lo dicta la norma ISO 27002, se alcanzó nuevamente con éxito al 100 por ciento. En esta ocasión se procedió con la recolección de la información mediante una entrevista realizada al encargado del Dpto. TI y encargado del área de Infraestructura Tecnológica de la empresa, la cual se realizó mediante una serie de preguntas a modo de cuestionario.

Para los objetivos 3 y 4 al igual que los anteriores su cumplimiento fue satisfactorio en su 100 porciento, ya que dentro del capítulo V “DISEÑO Y DESARROLLO DEL PROYECTO” la implementación íntegra de las soluciones propuestas en este capítulo representa el cumplimiento exitoso y completo de los objetivos estratégicos de este proyecto, transformando fundamentalmente la postura de seguridad de Comercial de Seguros Corredora de Seguros S.A. y alineándola con las mejores prácticas de la norma ISO 27002.

Al tratar de manera sistemática cada una de las brechas detectadas en el diagnóstico, la organización no solo soluciona sus vulnerabilidades presentes, sino que crea un ecosistema de seguridad sólido, resistente y listo para el futuro.

Por último, en el punto 6.17 “Desarrollo de la propuesta de implementación del plan de seguridad informática” este apartado materializa el objetivo final del proyecto al entregar un plan de seguridad que es a la vez comprensivo, práctico y priorizado. La tabla consolidada no es únicamente un resultado de la investigación, sino un instrumento de gestión estratégica creado para orientar la toma de decisiones, respaldar inversiones y sincronizar los esfuerzos de remediación. Con esta iniciativa, la entidad cuenta con una ruta clara para avanzar del diagnóstico a la implementación, garantizando que cada acción emprendida esté acorde con las mejores prácticas de la norma ISO 27002 y se centre en salvaguardar de manera efectiva sus activos informáticos.

6.18.2 Recomendaciones

Basado en el éxito total de todos los objetivos del proyecto y el sólido plan de acción desarrollado, se emiten las siguientes recomendaciones estratégicas dirigidas a la alta dirección y al equipo del Dpto. TI de Comercial de Seguros Corredora de Seguros S.A.

1. El proyecto ha demostrado la existencia de brechas críticas y ha proporcionado un plan priorizado para remediarlas. La recomendación más urgente es que la alta dirección apruebe formalmente el Plan de Seguridad Informática (Ilustración 18) y asigne los recursos (presupuestarios y humanos) necesarios para su ejecución, comenzando de inmediato con las iniciativas de prioridad "Alta". Sin este compromiso directivo, el plan corre el riesgo de quedar solo en papel.

2. Para capitalizar la "percepción interna favorable hacia el cambio", se recomienda formalizar un Comité de Seguridad de la Información. Este comité, compuesto por representantes de la dirección, TI, áreas de negocio clave (como operaciones y legal) y, si es posible, un asesor externo, será responsable de supervisar la implementación del plan, revisar el progreso, resolver impedimentos y asegurar que la seguridad se mantenga como una prioridad estratégica a largo plazo.

3. No se debe intentar abordar todo al mismo tiempo. La recomendación es ejecutar el plan de implementación de manera disciplinada y por fases, siguiendo estrictamente la priorización definida.

4. El plan de seguridad no debe ser visto como un proyecto con un inicio y un fin. Se recomienda institucionalizar un ciclo de mejora continua (Planificar, Hacer, Verificar, Actuar).

5. Aprovechando que ya se ha identificado la necesidad, se debe lanzar un programa continuo de capacitación y concienciación en seguridad para todos los empleados. Esto debe incluir simulaciones de phishing, comunicados sobre nuevas amenazas y formación específica según los roles. El objetivo es que cada miembro de la organización entienda que la seguridad es una responsabilidad compartida.

REFERENCIA BIBLIOGRÁFICAS

27002, N. I. (2022). *Seguridad de la información, ciberseguridad y protección de la intimidad - Controles de seguridad de la información*. Suiza: ISO/IEC 2022.

Amazon Web Services. (30 de Setiembre de 2022). *Que es la infraestructura de TI*. Obtenido de AWS: https://aws.amazon.com/es/what-is/it-infrastructure/#:~:text=La%20infraestructura%20de%20TI%20es%20el%20conjunto%20de%20software%2C%20hardware,la%20eficiencia%20general%20del%20sistema.

Ambit-bst. (22 de febrero de 2022). *Diferencias entre amenaza, vulnerabilidad y riesgo*. Obtenido de Ambit BST: https://www.ambit-bst.com/blog/diferencias-entre-amenaza-vulnerabilidad-y-riesgo

Corletti Estrada, A. (2020). *Ciberseguridad*. darFE.es.

Fortinet. (2025). *Tríada CIA: confidencialidad, integridad y disponibilidad*. Obtenido de Fortinet: https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

García, L. G. (2022). *Revista de Investigación Académica sin Frontera*. Mexico: Revistas Unison.

GlobalSuite. (17 de octubre de 2023). *Introducción a la norma ISO/27002*. Obtenido de GlobalSuite: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27002-y-para-que-sirve/#:~:text=La%20norma%20ISO%2027002%20es%20aplicable%20a%20todas%20las%20organizaciones,con%20los%20riesgos%20que%20enfrentan.

Gutierrez, N. (27 de Abril de 2024). *Marcos de Ciberseguridad*. Obtenido de Prey: https://preyproject.com/es/blog/marcos-de-ciberseguridad-la-guia-definitiva

Hewlett Packard Enterprise. (20 de Diciembre de 2024). *Que es una amenaza de ciberseguridad*. Obtenido de Amenaza de ciberseguridad: https://www.hpe.com/lamerica/es/what-is/cybersecurity-threats.html#:~:text=Las%20amenazas%20de%20ciberseguridad%20pueden,denegaci%C3%B3n%20de%20servicio%20(DoS).

Kurfess, J. (21 de noviembre de 2023). *¿Qué es la investigación primaria? Tipos, métodos y ejemplos*. Obtenido de ¿Qué es la investigación primaria?

Servicenow. (3 de Octubre de 2023). *Que es el riesgo cibernético*. Obtenido de https://www.servicenow.com/latam/products/governance-risk-and-compliance/what-is-cyber-risk.html

Simplilearn. (13 de Agosto de 2024). *Vulnerabilidad en la seguridad*. Obtenido de Simplilearn: https://www.simplilearn.com/vulnerability-in-security-article

Software, Q. S. (24 de Abril de 2024). *Tipos de investigación y sus características*. Obtenido de Tipos de investigación y su clasificación: https://www.questionpro.com/blog/es/tipos-de-investigacion-de-mercados/#investigacion_exploratoria

Vega Briceño, E. (2021). *Seguridad de la Información*. Área de Innovación y Desarrollo, S.L.

CAPÍTULO VII: APÉNDICE Y ANEXOS

6.19.1 Apéndices

Apéndice número 1. Entrevista de situación actual de la infraestructura tecnológica existente en la organización.

Entrevista #1. Encargado del área de Infraestructura Tecnológica del Dpto. TI

Proyecto: Auditoria basada en ciberseguridad utilizando la norma iso/iec 27002 para el desarrollo de un plan estratégico de seguridad informática aplicando los controles tecnológicos en el área de infraestructura del departamento de ti en comercial de seguros corredora de seguros s.a, en el período 2025-2026

Organización: Comercial de Seguros Corredora de Seguros S.A

Fecha: 17 de abril del 2025

Aplicador de la entrevista: Leonardo Solera Ovares

Objetivo de la entrevista

Proporcionar una información más detallada sobre el estado actual de la empresa y poder identificar de manera clara aquellas brechas o vulnerabilidades de seguridad presentes.

Sección 1. Cumplimiento de Controles Tecnológicos

8.1 Dispositivos terminales de usuario: Proteger la información frente a los riesgos introducidos por el uso de dispositivos de punto final de usuario	**SI**	**Parcialmente**	**No**

a. Existe un registro de dispositivos de punto final de usuario

b. Requisitos de protección física (candado)

c. Restricción en la instalación de software

d. Cifrado de equipo final y dispositivos de almacenamiento

8.2 Derechos de acceso privilegiado: Para garantizar que sólo los usuarios, componentes de software y servicios autorizados dispongan de derechos de accesos privilegiados.	**SI**	**Parcialmente**	**No**

a. Identificar usuarios que necesitan derechos de acceso privilegiados

b. Asignar derechos de acceso privilegiado a los usuarios según sea necesario

c. Revisar periódicamente los accesos de las cuentas de usuario

d. Registrar todos los accesos privilegiados

8.5 Autenticación Segura: Garantizar la autenticación segura de un usuario o una entidad cuando se le concede acceso a sistemas, aplicaciones y servicios.	**SI**	**Parcialmente**	**No**

a. Cuentan con políticas que exijan contraseñas robustas

b. Cuentan con doble factor de autenticación para el acceso a los equipos

c. Cuentan con alguna política que bloquee el usuario después de varios intentos erróneos

d. Generar un evento de seguridad si se detecta un posible intento de violación de los controles de inicio de sesión

8.7 Protección contra el malware: Garantizar la protección de la información y otros activos asociados contra los programas maliciosos	**SI**	**Parcialmente**	**No**

a. Instalación y actualización de productos de seguridad

b. Cuentan con controles que detecten el uso de software no autorizado

c. Revisión periódica del software instalado en los elementos críticos

d. Aplican recomendaciones emitidas por entidades confiables (MICITT)

8.8 Gestión de las vulnerabilidades técnicas: Para evitar la explotación de vulnerabilidades técnicas	**SI**	**Parcialmente**	**No**

a. Se cuenta con un inventario de activos de hardware y software

b. Se actualizan de manera periódica cada uno de los activos

c. Se realizan pruebas de vulnerabilidades

d. Se ejecutan pruebas de penetración

8.10 Supresión de información: Para evitar la exposición innecesaria de información sensible y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información.	**SI**	**Parcialmente**	**No**

a. Se utiliza destructora de papel de corte cruzado para eliminar información física

b. Se utiliza algún software para el borrado seguro

c. Se elimina información sensible de forma segura cuando ya no sea necesaria

d. Se utilizan mecanismos de eliminación adecuados (desmagnetización de unidades de disco duro y otros soportes de almacenamiento magnético)

8.11 Enmascaramiento de datos: Limitar la exposición de datos sensibles, incluida la información de identificación personal, y cumplir los requisitos legales, estatutarios, reglamentarios y contractuales.	**SI**	**Parcialmente**	**No**

a. No conceder a todos los usuarios acceso a los datos

b. Cuentan con mecanismos de ofuscación de datos

c. Cuentan con acuerdos o restricciones sobre el uso de los datos tratados

d. Se lleva un registro del suministro y la recepción de los datos procesados

8.13 Respaldo de información: Permitir la recuperación tras la pérdida de datos o sistemas.	**SI**	**Parcialmente**	**No**

a. Se realizan respaldos de información a los elementos críticos

b. Se cuenta con procedimientos de restauración y recuperación de datos

c. Los respaldos son almacenados en lugares seguros y protegidos

d. Se protegen las copias de seguridad mediante cifrado

8.19 Instalación de software en sistemas operativos: Garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas	**SI**	**Parcialmente**	**No**

a. Se mantienen actualizadas las versiones de Windows

b. Se instala software sólo después de haber realizado pruebas exhaustivas

c. Se definen estrategias de reversión antes de aplicar cambios

d. Se mantiene un registro de auditoría de todas las actualizaciones del software

8.20 Seguridad en las redes: Proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo contra el peligro a través de la red.	**SI**	**Parcialmente**	**No**

a. Se cuenta con un diagrama de red de la infraestructura

b. Establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan por redes públicas,

c. Detectar, restringir y autenticar la conexión de equipos y dispositivos a la red

d. Se cuenta con herramientas de monitoreo de la red

8.22 Segregación de redes: Dividir la red en fronteras de seguridad y controlar el tráfico entre ellas en función de la actividad empresarial. necesidades.	**SI**	**Parcialmente**	**No**

a. Cuentan con diferentes dominios de red independientes

b. Se utilizan mecanismos como VLANs

c. Las redes inalámbricas cuentan con un tratamiento especial

d. Se monitorean y registran los accesos de red, y se generan alertas ante actividades sospechosas o no autorizadas

8.23 Filtrado web: Proteger los sistemas de ataques de programas maliciosos y evitar el acceso a sitios web no autorizados. recursos.	**SI**	**Parcialmente**	**No**

a. Cuentan con controles implementados para el filtrado web

b. Se han establecido niveles de navegación web

c. Utilizan equipos de seguridad para el control en la navegación

d. Se capacita al personal para utilizar de manera correcta aquellos equipos que cuentan con mayores privilegios de navegación

8.25 Ciclo de vida del desarrollo seguro: Garantizar que la seguridad de la información se diseñe y aplique dentro del ciclo de vida de desarrollo seguro de software y sistemas.	**SI**	**Parcialmente**	**No**

a. La organización ha establecido y documentado políticas y procedimientos para el desarrollo seguro de software y sistemas

b. Se implementa la separación de los entornos de desarrollo, prueba y producción para prevenir accesos no autorizados

c. Se aplican directrices de codificación segura adaptadas a cada lenguaje de programación utilizado en la organización

d. Los desarrolladores reciben formación continua en prácticas de desarrollo seguro y están capacitados para identificar y corregir vulnerabilidades en el código

8.30 Desarrollo externalizado: Garantizar que las medidas de seguridad de la información exigidas por la organización se aplican en el desarrollo de sistemas subcontratados.	**SI**	**Parcialmente**	**No**

a. Se han establecido acuerdos contractuales que incluyan requisitos específicos de seguridad de la información para los proveedores de desarrollo subcontratado.

b. La organización supervisa y revisa regularmente las actividades de desarrollo realizadas por proveedores externos.

c. Los acuerdos con proveedores externos contemplan derechos de auditoría para verificar el cumplimiento de las políticas de seguridad de la organización.

d. Se cuentan con herramientas de seguridad para la conexión de los proveedores externos a la organización.

8.31 Separación de los entornos de desarrollo, prueba y producción: Proteger el entorno de producción y los datos de los riesgos derivados de las actividades de desarrollo y prueba.	**SI**	**Parcialmente**	**No**

a. Se mantienen separados adecuadamente los sistemas de desarrollo, prueba y producción.

b. Se cuenta con ambientes de pruebas antes de aplicar algún cambio en producción.

c. Se realizan copias de seguridad de los diferentes entornos.

d. Se define un control de acceso en cada uno de los ambientes de desarrollo y producción.

Apéndice número 2. Entrevista para la evaluación de la Infraestructura Digital

Entrevista #2. Encargado del área de Infraestructura Tecnológica y encargado del Dpto. TI

Proyecto: Auditoria basada en ciberseguridad utilizando la norma iso/iec 27002 para el desarrollo de un plan estratégico de seguridad informática aplicando los controles tecnológicos en el área de infraestructura del departamento de ti en comercial de seguros corredora de seguros s.a, en el período 2025-2026

Organización: Comercial de Seguros Corredora de Seguros S.A

Fecha: 24 de abril del 2025

Aplicador de la entrevista: Leonardo Solera Ovares

Objetivo de la entrevista

Consiste en un análisis detallado y sistemático de cada uno de los elementos y servicios de la infraestructura tecnológica vigente. Este procedimiento pretende reconocer las fortalezas, debilidades, oportunidades de mejora y posibles inconvenientes. La meta es comprender de qué manera la infraestructura tecnológica existente influye en la eficacia, la seguridad y los objetivos de empresa, permitiendo así la toma de decisiones fundamentadas para mejorar su rendimiento y prever inversiones futuras.

¿La infraestructura física actualmente cuenta con equipos como servidores, switches, firewalls que sostienen las operaciones tecnológicas?	**SI**	**Parcialmente**	**No**
¿Realizan mantenimientos preventivos y correctivos a los equipos de red y servidores?	**SI**	**Parcialmente**	**No**
¿Existen políticas definidas para la renovación tecnológica de hardware y software para los equipos de infraestructura?	**SI**	**Parcialmente**	**No**
¿Se encuentra documentada la arquitectura de la red con los flujos más críticos de comunicación interna y externa?	**SI**	**Parcialmente**	**No**
¿Existen ambientes segregados de desarrollo, prueba y producción dentro de la infraestructura de la organización?	**SI**	**Parcialmente**	**No**
¿Cuentan con herramientas para monitorear el rendimiento y la disponibilidad de los servicios de infraestructura?	**SI**	**Parcialmente**	**No**
¿Es escalable la infraestructura actual frente a un crecimiento esperado de la organización?	**SI**	**Parcialmente**	**No**

¿Se tienen establecidos procedimientos para la gestión de respaldos y recuperación de la información crítica desde la perspectiva de infraestructura?	**SI**	**Parcialmente**	**No**
¿Cuentan con medidas de seguridad implementadas para proteger la infraestructura frente alguna amenaza interna o externa?	**SI**	**Parcialmente**	**No**
¿Se han identificado brechas de seguridad o puntos de falla en la infraestructura actual?	**SI**	**Parcialmente**	**No**
¿Cuenta con algún enlace alterno de comunicación a internet?	**SI**	**Parcialmente**	**No**
¿Se cuenta con alguna herramienta que balance las cargas de los equipos de la infraestructura crítica?	**SI**	**Parcialmente**	**No**

Apéndice número 3. Entrevista de percepción para conocer las expectativas del desarrollo

Entrevista #3. Encargado del área de Infraestructura Tecnológica

Proyecto: Auditoria basada en ciberseguridad utilizando la norma iso/iec 27002 para el desarrollo de un plan estratégico de seguridad informática aplicando los controles tecnológicos en el área de infraestructura del departamento de ti en comercial de seguros corredora de seguros s.a, en el período 2025-2026

Organización: Comercial de Seguros Corredora de Seguros S.A

Fecha: 28 de abril del 2025

Aplicador de la entrevista: Leonardo Solera Ovares

Objetivo de la entrevista

Consiste en comprender las carencias de la organización, considerando los diversos análisis que se llevaron en el capítulo IV, este apartado ilustra una tabla en la comparación de la situación actual, las brechas y lo que se desea tener.

Aspecto	Situación Actual	Brecha	Situación Deseada
Políticas, normas y procedimientos	No se cuenta con políticas robustas ni procedimientos de seguridad de la información	Falta de políticas, normas y procedimientos	Capacitación e implementación de políticas y procedimientos de seguridad de la información
Dispositivos terminales de usuario	Registro de dispositivos y restricciones en uso, pero sin cifrado ni protección física adecuada.	Falta de cifrado y protección física robusta.	Registro completo, cifrado de datos y protección física eficaz en dispositivos terminales.
Derechos de acceso privilegiado	Identificación y revisión de accesos en algunos casos, pero sin registros de todos los accesos privilegiados.	No se registran todos los accesos y no se realiza revisión periódica de derechos.	Control, registro y revisión periódica de todos los accesos privilegiados.
Autenticación segura	Políticas de contraseñas robustas y bloqueo tras intentos fallidos; falta generación de alertas de seguridad.	Ausencia de alertas y doble factor en algunos casos.	Implementación de doble factor, alertas de seguridad y políticas estrictas de autenticación.
Protección contra malware	Instalación y actualización de seguridad en marcha, pero con controles limitados para software no autorizado y revisión periódica.	Falta de controles en uso de software no autorizado y revisión periódica.	Sistemas actualizados, controles efectivos y revisiones periódicas para detectar malware.
Gestión de vulnerabilidades	Inventario y actualizaciones en proceso, pero sin pruebas regulares de vulnerabilidades o penetración.	Inexistencia de pruebas regulares y análisis de vulnerabilidades.	Inventario actualizado, pruebas de vulnerabilidades y penetración periódicas.

Respaldo de información	Respaldos realizados y procedimientos existentes, pero sin cifrado en copias de seguridad.	Copias no cifradas y procedimientos de restauración no completamente definidos.	Respaldos cifrados, procedimientos de recuperación claros y almacenados de forma segura.
Instalación de software en sistemas	Actualizaciones y pruebas previas, pero sin registros de auditoría.	Falta de registros de auditoría y control en actualizaciones.	Registros de auditoría, control estricto y pruebas documentadas en la instalación.
Seguridad en las redes	Diagrama de red y controles básicos, pero con monitoreo y segmentación limitada.	Necesidad de mejorar en segmentación, monitoreo avanzado y control de accesos.	Redes segmentadas, monitoreo en tiempo real y controles avanzados de seguridad en red.
Segregación de redes	Uso de VLANs y redes independientes, pero con monitoreo y registros insuficientes.	Mejorar en monitoreo y control del tráfico entre redes segregadas.	Monitoreo constante, registros y control estricto del tráfico entre segmentos.
Filtrado web	Controles de filtrado en marcha, pero con niveles limitados y capacitación del personal.	Mejoras en niveles de filtrado y en capacitación del personal.	Filtrado avanzado, capacitación continua y políticas claras de navegación.
Desarrollo seguro	Políticas y procedimientos establecidos, pero con brechas en formación continua y control en entornos de desarrollo.	Necesidad de mayor formación, control en ambientes y revisiones de seguridad.	Procesos integrados, formación continua y controles estrictos en desarrollo y pruebas.
Desarrollo externalizado y separación de entornos	Control adecuado en contratación, pero con deficiencias en supervisión y separación en algunos casos.	Mejorar en supervisión y control de entornos de desarrollo y producción.	Supervisión constante, separación efectiva y controles en entornos de desarrollo, prueba y producción.

6.19.2 Anexos

Anexo. Cronograma de actividades

Ilustración 43. Cronograma de actividades, duración de Tesis

AUDITORIA BASADA EN CIBERSEGURIDAD UTILIZANDO LA NORMA ISO/IEC 27002 PARA EL DESARROLLO DE UN PLAN ESTRATÉGICO DE SEGURIDAD INFORMÁTICA APLICANDO LOS CONTROLES TECNOLÓGICOS EN EL ÁREA DE INFRAESTRUCTURA DEL DEPARTAMENTO DE TI EN COMERCIAL DE SEGUROS CORREDORA DE SEGUROS, S.A EN EL PERÍODO 2025-2026

ACTIVIDADES	Meses	Enero				Febrero				Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiembre	
	Semanas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
Entrega del anteproyecto																																			
Aprobación del anteproyecto y asignación de tutor																																			
Desarrollo del Capitulo I: Planteamiento del Problema																																			
Entrega del capitulo I y matriz de coherencia																																			
Revisión y aprobación de capitulo I por parte del tutor																																			
Desarrollo del Capitulo II: Marco Teórico																																			
Búsqueda de conceptos																																			
Recolección de la información																																			
Realización del marco teórico																																			
Entrega del capitulo II																																			
Revisión y aprobación de capitulo II por parte del tutor																																			
Desarrollo del Capitulo III: Marco Metodológico																																			
Analizar el enfoque de la investigación																																			
Recolectar la información necesaria a cerca del proyecto																																			
Entrega del capitulo III																																			
Revisión y aprobación de capitulo III por parte del tutor																																			
Desarrollo del Capitulo IV: Diagnóstico																																			
Identificación y recolección de datos de la situación actual																																			
Analizar las necesidades del cliente																																			
Definir los resultados actuales para determinar ejecución del proyecto																																			
Entrega del capitulo IV																																			
Revisión y aprobación de capitulo IV por parte del tutor																																			
Desarrollo del Capitulo V: Diseño y Desarrollo del Proyecto																																			
Desarrollo el plan estratégico de seguridad informática																																			
Desarrollo de la propuesta de implementación para plan estratégico																																			
Entrega del capitulo V																																			
Revisión y aprobación de capitulo V por parte del tutor																																			
Desarrollo del Capitulo VI: Conclusiones y recomendaciones																																			
Análisis de desempeño y conclusiones																																			
Redacción sobre las recomendaciones																																			
Entrega del capitulo VI																																			
Revisión y aprobación de capitulo VI por parte del tutor																																			

Fuentes: Elaboración Propia

Ilustración 44. Cronograma de actividades, Capítulo I.

ACTIVIDADES	Meses	Enero				Febrero			
	Semanas	1	2	3	4	5	6	7	8
Entrega del anteproyecto									
Aprobación del anteproyecto y asignación de tutor									
Desarrollo del Capitulo I: Planteamiento del Problema									
Entrega del capitulo I y matriz de coherencia									
Revisión y aprobación de capitulo I por parte del tutor									

Fuentes: Elaboración Propia

Ilustración 45. Cronograma de actividades, Capítulo II.

ACTIVIDADES	Meses	Febrero				Marzo			
	Semanas	5	6	7	8	9	10	11	12
Desarrollo del Capitulo II: Marco Teórico									
Búsqueda de conceptos									
Recolección de la información									
Realización del marco teórico									
Entrega del capitulo II									
Revisión y aprobación de capitulo II por parte del tutor									

Fuentes: Elaboración Propia

Ilustración 46. Cronograma de actividades, Capítulo III.

ACTIVIDADES	Meses	Marzo			
	Semanas	9	10	11	12
Desarrollo del Capitulo III: Marco Metodológico					
Analizar el enfoque de la investigación					
Recolectar la información necesaria a cerca del proyecto					
Entrega del capitulo III					
Revisión y aprobación de capitulo III por parte del tutor					

Fuentes: Elaboración Propia

Ilustración 47. Cronograma de actividades, Capítulo IV.

ACTIVIDADES	Meses	Abril				Mayo				Junio			
	Semanas	13	14	15	16	17	18	19	20	21	22	23	24
Desarrollo del Capitulo IV: Diagnóstico													
Identificación y recolección de datos de la situación actual													
Analizar las necesidades del cliente													
Definir los resultados actuales para determinar ejecución del proyecto													
Entrega del capitulo IV													
Revisión y aprobación de capitulo IV por parte del tutor													

Fuentes: Elaboración Propia

Ilustración 48. Cronograma de actividades, Capítulo V.

ACTIVIDADES	Meses	Junio				Julio				Agosto			
	Semanas	21	22	23	24	25	26	27	28	29	30	31	32
Desarrollo del Capitulo V: Diseño y Desarrollo del Proyecto													
Desarrollo el plan estratégico de seguridad informática													
Desarrollo de la propuesta de implementación para plan estratégico													
Entrega del capitulo V													
Revisión y aprobación de capitulo V por parte del tutor													

Fuentes: Elaboración Propia

Ilustración 49. Cronograma de actividades, Capítulo VI.

ACTIVIDADES	Meses	Agosto				Septiembre	
	Semanas	29	30	31	32	33	34
Desarrollo del Capitulo VI: Conclusiones y recomendaciones							
Análisis de desempeño y conclusiones							
Redacción sobre las recomendaciones							
Entrega del capitulo VI							
Revisión y aprobación de capitulo VI por parte del tutor							

Fuentes: Elaboración Propia