

**UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS**

**INGENIERÍA DE SISTEMAS DE INFORMACIÓN**

**CURSO: 1ASI0707 Gestión de Seguridad de la Información**

**ENUNCIADO DEL TRABAJO FINAL DEL CURSO**

**DOCENTE: Alfonso Raul Farje Tong**

**SECCIÓN: 3934**

**Integrantes:**

* **Martel Paez, Jhair Israel u202215562**
* **Caysedo Salvador, Fabrizio Michell u20211g109**
* **Caso Farfán, Jorge Stefano u202218675**
* **Verastegui Pajares, Mauricio u202017112**
* **Palomino Mayta, Luis Antonio u202017554**

2025

**Índice**

[**Resumen 3**](#_nv7juntu67jh)

[**Objetivo del Estudiante (Student Outcome) 3**](#_854h0hrgmn2h)

[**Capítulo 1: Presentación 3**](#_edwbstlbrof2)

[**Capítulo 2: Marco Teórico 8**](#_7rrke25sjjay)

[**Capítulo 3: Estado actual de las cláusulas de ISO 27002 10**](#_xjhxc8mvih6j)

[**Capítulo 4: Análisis de las causas de la inefectividad de los controles 17**](#_htabnxuav5v7)

[**Capítulo 5: Medidas propuestas para cubrir las brechas de seguridad 17**](#_pbadojjn6lj8)

[**Bibliografía 17**](#_s5czt5fagn5i)

# 

# 

# 

# 

# 

# **Resumen**

En el presente proyecto, se realizará un análisis de brechas de seguridad, un análisis sobre las causas de la inefectividad de los controles del "Anexo A" de la normativa ISO 27001 acerca de la empresa Servicentro Posben S.a.C. Asimismo, se aplicarán las directrices establecidas de la norma ya mencionada con la intención de implementar mejores prácticas en la gestión de seguridad de la información de la empresa.

# **Objetivo del Estudiante (Student Outcome)**

**ABET – EAC - Student Outcome 6:** La capacidad de adquirir y aplicar nuevos

conocimientos según sea necesario, utilizando estrategias de aprendizaje apropiadas.

**ABET – CAC - Student Outcome 6:** La capacidad para comprender y brindar soporte

para el uso, entrega y gestión de sistemas de información dentro de un entorno de

sistemas de información.

# **Capítulo 1: Presentación**

**Historia:**

El Grupo Posben inicia actividades por la década de 1960 por los esposos Felix Posadas Cabrera y Magda Benavides Rios, el Grupo Empresarial ha pasado por distintas industrias: Avicultura, construcción, agricultura, maquinarias, entre otras. Hoy, con sus 4 unidades de negocio, es uno de los Grupos Empresariales que lideran el desarrollo del interior del país y contribuyen con la empleabilidad y prosperidad de más de 200 familias en el sur del país.

En el año 1997, los fundadores identifican una oportunidad de negocio: Las Estaciones de Servicio para la comercialización de combustibles. Es así que en Mayo de 1998, y después de mucho esfuerzo y empuje, se constituye la primera Estación de Servicios del Grupo Posben en la ciudad de Ica: Estación de Servicios El Pacífico.

Visionariamente, los fundadores construyeron la Estación de Servicio Super grifo la Estancia, establecimiento ubicado estratégicamente de gran extensión cubriendo la necesidad de los transportistas de carga pesada y clientes agroindustriales que hasta ese momento no era atendida. Está asignada a la razón social Servicentro Posben S.a.C.

**Misión:**

La misión del Grupo Posben es promover el desarrollo del país y la prosperidad de nuestros colaboradores a través de la innovación y la orientación al cliente.

Con esta misión como base del Grupo Empresarial, la Misión de Super Grifo La Estancia es ser la mejor Estación de Servicios de Abastecimiento de Combustible y Servicios Adicionales en el país, generando una experiencia extraordinaria para nuestros clientes y brindando servicios y productos de alta calidad.

**Visión:**

Ser reconocida como la Estación referente a nivel nacional en calidad de atención, confiabilidad y servicio integral; e identificada como el mejor proveedor por nuestros clientes corporativos en términos de profesionalismo, cumplimiento y confiabilidad.

**Análisis FODA:**

| **FORTALEZA** | **DEBILIDADES** |
| --- | --- |
| * Producto de calidad garantizada y de prestigio en el mercado. * Seguridad comprobada en la cantidad que se expende. * Personal comprometido y alineado con los objetivos y metas establecidas por la empresa. * Ubicación estratégica de la Estación de Servicios. | * Procesos no automatizados. Inestabilidad de Energía Eléctrica. * Lentitud en la línea de comunicación – Internet. * Proceso deficiente para la autorización e instalación de tanque de combustible para ampliar la capacidad de almacenamiento. * La distancia geográfica limita conseguir personal operativo, administrativo y de seguridad. * Área de TI tercerizada. |
| **OPORTUNIDADES** | **AMENAZAS** |
| * Alta afluencia de unidades de carga pesada por la ruta de zona Sur y Norte. * Crecimiento del parque automotor en los últimos años. • * Ofrecer productos de calidad que protegen el motor de los vehículos. | * Desabastecimiento de combustible. * Implementación y funcionamiento de Estación de Servicio de Petroperú. * Estación de Servicio que ofrecen menores precios. * Complejidad y burocracia para obtener permiso de instalación de tanques o nuevos productos. * El precio internacional del petróleo afecta directamente los precios del mercado nacional. |

**Análisis PESTEL:**

**1. Político**

El sector político en el Perú influye directamente en la industria de los hidrocarburos, incluyendo la operación de estaciones de servicio. Las políticas energéticas impulsadas por el Estado, así como los subsidios o regulaciones sobre precios de combustibles, pueden generar impactos significativos en la rentabilidad del sector.

La estabilidad política es crucial para garantizar un entorno favorable a las inversiones en infraestructura energética. Cambios frecuentes en las políticas públicas, conflictos sociales o incertidumbre política pueden generar riesgos para la operación continua y eficiente de negocios como Super Grifo La Estancia.

**2. Económico**

El sector hidrocarburos es parte fundamental en el desarrollo del Perú, dentro de los cuales tenemos a los combustibles líquidos que se han vuelto cada vez más importantes en el desarrollo de la economía peruana. “La participación del sector en la economía peruana se refleja en cuatro variables económicas: Producto Bruto Interno (PBI), Valor Agregado Bruto (VAB), inversiones y Balanza Comercial de Hidrocarburos” (OSINERGMIN, 2015, p. 146).

El aumento del precio de los combustibles a nivel local se ve influenciado directamente por el aumento del precio internacional del petróleo. En el caso del gas licuado de petróleo, el aumento se da en función al marcador de referencia internacional de Mont Belvieu (BCRP, 2021b, p. 151-152).

“Respecto a los gasoholes, se registraron aumentos en los precios de paridad de importación.

El marcador internacional en este caso es el precio de la gasolina de la Costa del Golfo” (BCRP, 2021b, p. 151-152).

**3. Social**

“El Fondo de Inclusión Social Energético [FISE] que se crea con el propósito de llevar energía menos contaminante a las poblaciones más vulnerable de todo el país” (Ministerio de Desarrollo e Inclusión Social [MIDIS], 2015, párr. 7). Los recursos económicos del FISE entre otros, provienen de la producción e importación de combustibles. Con estos recursos el Ministerio de Energía y Minas puede llevar a cabo diversos proyectos energéticos, en beneficio de los peruanos.

El Fondo para la Estabilización de Precios de Combustibles [FEPC] “es un esquema para la estabilización de los precios al consumidor final, el objetivo es reducir la alta volatilidad de los precios internos con respecto a los precios internacionales, lo que incrementa el bienestar social” (OSINERGMIN, 2015, p. 94)

**4. Tecnológico**

Las estaciones de servicio o grifos utilizan la tecnología para mejorar la eficiencia, productividad, el control de inventarios y reducir riesgos.

Para medir los niveles de los tanques, los sistemas de tele medición automática destacan como una de las principales opciones y con resultados más precisos. La precisión no es la única ventaja de estos dispositivos electrónicos.

A continuación, enumeramos algunas de sus principales funciones:

• Control de las existencias en tiempo real.

• Detección de fugas.

• Informes automáticos.

La tecnología también nos brinda herramientas que permiten mejorar la gestión de las estaciones de servicio.

El mercado ofrece varias alternativas de software que permiten llevar un control de los turnos, controlar inventarios, cuentas por cobrar, cuentas por pagar y las ventas que se realizan por cada surtidor.

En otros países existe el autoservicio en el cual, los mismos clientes abastecen el combustible y pagan con tarjeta de crédito.

Debemos considerar este escenario para un futuro cercano y las aplicaciones móviles que están en constante innovación.

OSINERGMIN pone a disposición de los ciudadanos una aplicación móvil que permite encontrar estaciones de servicio cercanas a nuestra ubicación, con sus precios de venta.

**5. Ecológico**

La Asociación de Grifos y Estaciones de Servicio del Perú [AGESP] “desarrolla programas de Responsabilidad Social enfocados en el cuidado del medio ambiente, teniendo en cuenta el problema de calidad del aire de nuestra ciudad y el déficit de áreas verdes” (AGESP, 2021a, párr. 1, 3).

Para ayudar a reducir la contaminación ambiental, la AGESP ha promovido y participado en la plantación de árboles en la zona de Manchay. Esto se logró gracias a los aportes de los asociados, los cuales se hicieron cargo al 100% de todos los gastos.

**6. Legal**

En el Perú, existen diversas normativas sobre el procesamiento, comercialización y transporte de hidrocarburos líquidos (MINEM, s. f.), dentro las cuales, las referidas a la comercialización son:

• Ley N° 26221: Ley orgánica que norma las actividades de hidrocarburos en el territorio nacional.

• Decreto Supremo N° 052-93-EM: Reglamento de Seguridad para el Almacenamiento de Combustibles.

• Decreto Supremo N° 030-98-EM: Reglamento para la Comercialización de Combustibles Líquidos y Otros Productos para la Derivados de los Hidrocarburos. 38

• Decreto Supremo N° 054-93-EM: Reglamento de Seguridad para establecimientos de Venta al Público de Combustibles Derivados de Hidrocarburos.

• Decreto Supremo N° 039-2014: La Protección Ambiental en las Actividades de Hidrocarburos.

• Ley N° 27972: Ley Orgánica de Municipalidades.

Entre las principales instituciones que se encargan de velar por el cumplimiento de la normativa vigente, se encuentran la Dirección General de Hidrocarburos [DGH] que pertenece al Ministerio de Energía y Minas [MEM],

OSINERGMIN, INDECOPI, las municipalidades, gobiernos regionales y la Policía Nacional del Perú.

“Es el OSINERGMIN, una institución pública encargada de regular y supervisar que las empresas del sector eléctrico, hidrocarburos y minero cumpla las disposiciones legales de las actividades que desarrollan” (OSINERGMIN, s. f.-a, párr. 1).

Existe toda una base legal para la inscripción de un grifo o estación de servicios de acuerdo al Texto Único de Procedimientos Administrativos [TUPA] del OSINERGMIN.

Las municipalidades provinciales y distritales son las encargadas de otorgar las licencias de construcción y funcionamiento para estaciones de servicio, conforme a la Ley Orgánica de Municipalidades.

También existe la AGESP, “grupo privado sin fines de lucro que reúne a los

comerciantes minoristas, propietarios de grifos, estaciones de servicio, para velar por sus intereses, progreso y fortalecimiento y para representarlo ante las autoridades del gobierno y otras entidades sociales” (AGESP, 2021b, párr. 1, 2).

# **Capítulo 2: Marco Teórico**

* **Seguridad de la Información**

La seguridad de la información se refiere a un conjunto de normas y principios que buscan proteger la privacidad, la integridad y la disponibilidad de los datos en una organización. En un contexto altamente digital, salvaguardar la información vital se ha convertido en una prioridad estratégica, especialmente en industrias reguladas como la de hidrocarburos, donde la administración de datos delicados acerca de operaciones, clientes y acatamiento de normativas es permanente (Gkioulos et al., 2021).

Las amenazas a la protección de la información van desde ataques informáticos hasta fallos humanos o deficiencias en la infraestructura tecnológica. En este escenario, resulta esencial aplicar un método de administración integral para disminuir los riesgos vinculados (Rebollo et al., 2020).

* **Sistema de Gestión de Seguridad de la Información (SGSI)**

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un esquema organizado que facilita la administración sistemática de los riesgos asociados a la información. El SGSI se fundamenta en la mejora continua, facilitando la adaptación a amenazas emergentes, tecnologías y requerimientos de la organización.

Su implementación ayuda a:

* Alinear la seguridad con los objetivos de negocio.
* Cumplir requisitos legales y contractuales.
* Reducir incidentes de seguridad y mejorar la resiliencia operativa (Alrammal et al., 2021).

Esta perspectiva no solo resguarda activos tecnológicos, sino también procesos, individuos e infraestructuras vitales como las que se encuentran en estaciones de abastecimiento de combustible.

* **Norma ISO/IEC 27001**

La norma ISO/IEC 27001 es un estándar global que define las exigencias para instaurar, poner en marcha, conservar y perfeccionar un SGSI. Su enfoque centrado en riesgos facilita la identificación y manejo proactivo de las posibles amenazas a la seguridad de la información (Organización Internacional para la Normalización [ISO], 2022).

* Entre sus principales beneficios se encuentran:
* Aumento de la confianza de las partes interesadas.
* Mejora del cumplimiento regulatorio (especialmente importante en sectores críticos).
* Estandarización de controles técnicos y organizacionales.

La normativa fomenta la implementación del Ciclo PDCA (Planificar, Realizar, Comprobar, Actuar), lo que posibilita una administración dinámica de la seguridad y simplifica las auditorías tanto internas como externas.

**Normativas ISO/IEC 27002 y Regulaciones de Seguridad**

La norma adicional ISO/IEC 27002 ofrece un conjunto de controles de seguridad organizados en áreas como los controles organizacionales, físicos, de individuos y tecnológicos. En resumen, proporciona 93 controles categorizados en diversas cláusulas, los cuales funcionan como orientación para adaptar las políticas de seguridad de acuerdo al contexto de la organización (Caballero-Gómez et al., 2022).

Para un centro de servicios como Super Grifo La Estancia, estos controles adquieren importancia para asegurar la seguridad tanto de los sistemas de computación (por ejemplo, gestión automatizada de inventarios), como de los datos de clientes y proveedores, o la salvaguarda ante interrupciones en las operaciones.

* **Amenazas y Fallas de Seguridad Usualmente Presentes**

En entidades que requieren el manejo de datos para funcionar (como las estaciones de servicio que administran stocks de combustible, sistemas de facturación electrónica, entre otras), las amenazas más comunes comprenden:

* Accesos no autorizados a sistemas.
* Brechas de datos por fallas humanas.
* Ataques de malware en dispositivos conectados.
* Interrupciones en el servicio por falta de respaldo o energía.

La detección de estas brechas facilita la puesta en marcha de controles preventivos, correctivos y detectivos (Adedoyin et al., 2021), lo que resulta particularmente relevante en un contexto regulado por organismos como OSINERGMIN.

# **Capítulo 3: Estado actual de las cláusulas de ISO 27002**

| **Controles de seguridad de la información** | | | | | | | | | | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ISO 27002:2022** | | | | | | | | | | |  |
| Categoría | Código | Nombre de Control |  |  | Control | Preguntas | Responsable | Documento asociado | Comentario | % de Cumplimiento | ¿Cumple? |
| 5 | Controles organizacionales | | | | | | | | | |  |
| 1 | 5.01 | Políticas para la seguridad de la información |  |  | La política de seguridad de la información y políticas especificas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y conocidas tanto por el personal como por las partes interesadas pertinentes, además revisadas en intervalos planificados y cuando ocurran cambios significativos. | ¿Existe una política de seguridad de la información y políticas especificas?  ¿Las políticas han sido aprobadas, publicadas y comunicadas a todas las partes interesadas?  ¿Las políticas son revisados en intervalos planificados y cuando existe cambios significativos? ¿Cuando ha sido la ultima actualización? | Responsable de Seguridad de la Información |  | No se evidencia una política de seguridad de la información formalizada, aprobada por la dirección, comunicada al personal o revisada periódicamente.Sin este control, la organización carece de un marco base para gestionar riesgos y alinear prácticas de seguridad. | 0% | No |
| 2 | 5.02 | Roles y responsabilidades en seguridad de la información |  |  | Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización. | ¿Se ha establecido una estructura definida, aprobada y entendida para la implementación, operación y gestión de seguridad de la información?  ¿Se tiene definido las responsabilidades de la persona que asume el rol especifico de seguridad de la información?  ¿Tiene cada rol responsabilidad específica con respecto al riesgo y la seguridad de la información? | Recursos Humanos  Responsable de Seguridad de la Información |  | Existe una estructura de roles y responsabilidades en seguridad de la información poco clara, la asignación de tareas específicas es muy informal | 50% | Parcialmente |
| 3 | 5.03 | Segregación de funciones |  |  | Las funciones y responsabilidad en conflictos deben ser segregados. | ¿Se utiliza una matriz tipo RACI para mantener la identificación para cada tarea en los sistemas, aplicaciones? (Responsable | Accountable | Consulted | Informed)  ¿Existe una política que cubra la segregación de funciones?  ¿Se analizan los riesgos con respecto a la segregación de funciones?  ¿Se realiza un seguimiento regular de las actividades y los registros de auditoría? | Recursos Humanos  Responsable de Seguridad de la Información |  | Existe Riesgo, ya que no hay segregación, aumenta el fraude interno, errores no detectados y conflictos de interés.No existe política clara ni análisis de riesgos asociados. Se debe Implementar matriz RACI para roles clave. | 50% | Parcialmente |
| 4 | 5.04 | Responsabilidades de gestión |  |  | La dirección debe requerir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la establecida, las políticas y procedimientos específicos de la organización. | ¿Existe un programa de concientización y/o educación sobre la seguridad de la información dirigido a la gerencia? ¿Se realiza de manera regular y está a día?  ¿Los gerentes reciben el conocimiento y la capacitación apropiados específicamente sobre su rol y responsabilidad relacionados con la seguridad? | Recursos Humanos  Responsable de Seguridad de la Información |  | Falta que la dirección pueda realizar la implementación de la seguridad de la información. Implementar programa obligatorio de concienciación para gerentes. Realizar sesiones trimestrales de actualización para gerentes. Establecer KPIs de seguridad para la alta dirección | 50% | Parcialmente |
| 5 | 5.05 | Contacto con autoridades |  |  | La organización debe establecer y mantener contacto con las autoridades pertinentes. | ¿Cuenta con una lista de detalles de contacto para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias?  ¿Quién es el responsable de contactar a las autoridades y en qué punto de un incidente y/o evento se realiza este contacto y cómo?  ¿La lista es actual o cual es la ultima fecha de actualización?  ¿Existe un proceso de mantenimiento a lista? | Responsable de Seguridad de la Información |  | No existe registro formal de contactos con autoridades reguladoras. Falta protocolo definido para comunicación en incidentes. Retrasos en la notificación de incidentes críticos | 50% | Parcialmente |
| 6 | 5.06 | Contacto con grupos de interés especial |  |  | La organización debe establecer y mantener contacto con grupos especiales de interés u otros foros y asociaciones profesionales especializados en seguridad. | ¿Existe un contacto con grupos especiales de interés, foros y listas de correo profesional, tales como ISACA, ISC 2?  ¿Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias, vulnerabilidades recientemente descubiertas y disponibilidad de parches con los grupos de interés? | Responsable de Seguridad de la Información |  | No existen relaciones establecidas con comunidades profesionales de ciberseguridad. Pérdida de oportunidades para anticipar amenazas y adoptar mejores prácticas. Falta de actualización tecnológica. | 50% | Parcialmente |
| 7 | 5.07 | Inteligencia de amenazas |  |  | La información relacionada con las amenazas a la seguridad de la información debe ser recopilada y analizada para producir inteligencia sobre las amenazas. | ¿Se recopilan y analizan las amenazas relacionados a seguridad de la información?  ¿Se recibe la inteligencia de amenazas de foros y fuentes de intercambio de información? ¿Cuáles son?  ¿Se identifican y se documentan las amenazas, tanto internas como externas?  ¿Se analizan las amenazas para comprender los objetivos y métodos de ataque?  ¿Se determina el impacto de los eventos?  ¿Los datos de los eventos se recopilan y se correlacionan de múltiples fuentes?  ¿Se investigan las notificaciones de los sistemas de detección?  ¿Se comunica y comparte con personas relevantes las amenazas (por ejemplo tipos de atacantes o tipos de ataques?  ¿Se tiene una metodología y herramientas para llevar a cabo el proceso de inteligencia de amenazas? | Gestor de seguridad tecnológica  Responsable de Seguridad de la Información |  | No existe un proceso formalizado para recopilar, analizar y compartir inteligencia de amenazas. No se realiza análisis proactivo de TTPs (Tácticas, Técnicas y Procedimientos) de atacantes. Exposición a ataques conocidos que podrían prevenirse. | 50% | Parcialmente |
| 8 | 5.08 | Seguridad de la información en la gestión de proyectos |  |  | La seguridad de la información debe estar integrada en la gestión de proyectos. | ¿Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos, incluidos todos los tipos de proyectos relacionados con la información, los nuevos desarrollos y los cambios y/o mejoras en los sistemas, aplicaciones y procesos existentes? | Gestor de proyectos  Gestor de cambios  Responsable de Seguridad de la Información |  | No hay integración sistemática de seguridad en el ciclo de vida de proyectos. Falta de evaluación temprana de riesgos de seguridad en nuevos desarrollos o cambios. Falta de evaluación temprana de riesgos de seguridad en nuevos desarrollos o cambios. | 50% | Parcialmente |
| 9 | 5.09 | Inventario de información y otros activos asociados |  |  | Un inventario de información y otros activos asociados, incluidos los propietarios, debe ser desarrollado y mantenido. | ¿Existe un inventario de activos de la información?  ¿Contiene la siguiente información?  • Datos digitales  • Información impresa  • Software  • Infraestructura  • Servicios de información y proveedores de servicios  • Seguridad física  • Relaciones comerciales  • Las personas  ¿A quién pertenece el inventario?  ¿Cómo se mantiene actualizado el inventario?¿Cuando ha sido la ultima fecha de actualización?  ¿Se tiene una herramienta para realizar el inventario de activos?  ¿Los activos tienen propietario de riesgo?  ¿Los activos tienen responsable técnico?  ¿Cómo se asigna la propiedad poco después de crear o adquirir los activos críticos?  ¿Cómo se etiquetan los activos?  ¿Cómo se informa ante incidentes de seguridad de la información que los afectan? | Gestor de inventario  Responsable de Seguridad de la Información |  | No existe inventario centralizado de activos de información. Actualización inconsistente (sin fechas ni metodología documentada). Falta asignación clara de propietarios y responsables técnicos. Exposición desconocida: No se puede proteger lo que no está identificado. Respuesta lenta a incidentes: Falta datos para análisis forense. | 50% | Parcialmente |
| 10 | 5.10 | Uso aceptable de la información y otros activos asociados |  |  | Reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados debe ser identificada, documentada e implementada. | ¿Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios, etc.?  ¿Cubre el comportamiento del usuario en Internet y en las redes sociales?  ¿Se permite el uso personal de los activos de la empresa?  En caso afirmativo, ¿En qué medida y cómo se controla y/o asegura esto?  ¿Se describe de forma explícita lo qué constituye un uso inapropiado?  ¿Se distribuye esta información a toda la empresa?  ¿Están los niveles de clasificación adecuadamente asignados a los activos? | Responsable de Seguridad de la Información |  | Ausencia de política documentada sobre uso aceptable de activos (TI, datos, redes sociales). Falta de controles para uso personal de equipos corporativos. Clasificación inconsistente de activos según sensibilidad. Fugas de información por mal uso de recursos. Infecciones por malware (ej.: ransomware por descargas no autorizadas). | 50% | Parcialmente |
| 11 | 5.11 | Devolución de activos |  |  | El personal y otras partes interesadas, según sea apropiado, deben devolverse todos los activos de la organización en su posesión cuando cambien o terminen su empleo, contrato o acuerdo. | ¿Existe un procedimiento para recuperar los activos tras una baja o despido?  ¿Es un procedimiento automatizado o manual?  Si es manual, ¿Cómo se garantiza que no haya desvíos?  ¿Cómo se abordan los casos en los que los activos no han sido devueltos? | Gestor de inventario  Responsable de Seguridad de la Información |  | No existe un proceso formalizado para la recuperación de activos (equipos, credenciales, datos) al término de una relación laboral o contractual. Falta de automatización en la revocación de accesos y recuperación física de dispositivos. No hay protocolo para gestionar activos no devueltos (sanciones, bloqueos, acciones legales). | 50% | Parcialmente |
| 12 | 5.12 | Clasificación de la información |  |  | La información debe ser clasificada de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos de las partes interesadas pertinentes. | ¿Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la clasificación de la información?  ¿La clasificación se basa en los requisitos de confidencialidad, integridad y disponibilidad?  ¿El personal conoce los requisitos de seguridad correspondientes para el manejo de materiales clasificados? | Responsable de Seguridad de la Información |  | No existen políticas de revisión ni procedimiento de manera formalizada. Estos se basan en el criterio del administrador a cargo, coordinando con la directiva de la empresa. El resultado se lo comunican a los trabajadores por medio de correos en caso se amerite. | 60% | Parcialmente |
| 13 | 5.13 | Etiquetado de la información |  |  | Un conjunto de procedimientos apropiado para el etiquetado de información debe ser desarrollado e implementado en el esquema de clasificación de información adoptado por la organización. | ¿Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica?  ¿Está sincronizado con la política de clasificación de la información?  ¿Cómo se garantiza el correcto etiquetado?  ¿Cómo se garantiza que solo aquellos con permisos de acceso aprobados accedan a la información de la clasificación relevante?  ¿Cómo se garantiza que no haya acceso no autorizado?  ¿Se revisan los niveles de clasificación en intervalos predefinidos? | Responsable de Seguridad de la Información |  | No existe un procedimiento de etiquetado de manera formal. Este lo maneja el área de TI, el cual es un departamento que está tercerizado, y les brinda a los trabajadores claves de acceso dependiendo del rango del trabajador, para que así pueda los miembros de ciertas áreas específicas acceder a ciertos documentos. No hay un sistema que brinde alertas o intentos de accesos no deseados. | 70% | Parcialmente |
| 14 | 5.14 | Transferencia de la información |  |  | Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones para transferencia, dentro de la organización y entre la organización y otras partes. | ¿Existe un política sobre la transferencia de información?  ¿Existe un procedimiento para proteger la información en transito?  ¿Existe controles para asegura la trazabilidad de la información en tránsito?  ¿Se tienen pautas de retención y eliminación para todos los registros del negocio, incluidos los mensajes?  ¿Se implementa el uso de criptografías para la transferencia de la información?  ¿Existen un programa de concientización, capacitación y cumplimiento?  ¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos?  ¿Hay controles de seguridad adecuados para la mensajería electrónica (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)? | Seguridad Física  Responsable de Seguridad de la Información | Contrato del área de TI | No existe una política de sobre la transferencia de información. Sin embargo, el procedimiento de protección de información sí lo maneja el área de TI. Ellos implementan el uso de encriptación para la transferencia de información. No hay un programa de concientización, y las responsabilidades sobre la pérdida o divulgación depende del área que cometió la infracción. El área de TI se puede hacer responsable si es el caso, y se somete a las penalidades impuestas en el contrato, puesto que el un área tercerizada. | 70% | Parcialmente |
| 15 | 5.15 | Control de acceso |  |  | Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos del negocio y de seguridad de la información. | ¿Existe una política de control de acceso?  ¿Es consistente con la política de clasificación?  ¿Existe una segregación de responsabilidades en los sistemas, aplicaciones?  ¿Existe un proceso documentado de aprobación de acceso?  ¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión?  ¿Las conexiones inalámbrica y VPN son supervisado, controlados y autorizado?  ¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados?  ¿Cómo monitoriza la red para detectar acceso no autorizado?  ¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)? | Responsable de Seguridad de la Información |  | No tienen una política de control de acceso. En la entrevista, se menciona que la empresa contratada para el área de TI es la que maneja dichos datos, pero no se han difundido con la empresa encuestada. Existe un proceso de aprobación para acceso, pero no está documentado. En este sí se requiere que se involucre el propietario del sistema. Hay controles que maneja el área de TI, mayormente después de un evento. | 60% | Parcialmente |
| 16 | 5.16 | Gestión de identidad |  |  | El ciclo de vida completo de identidades debe ser gestionado. | ¿Existe un procedimiento o instructivo para la gestión de identidades?  ¿Se utiliza un ID de usuario únicos para cada usuario?  ¿Las cuentas se genera en función a una solicitud con aprobaciones y registros apropiados?  ¿Se deshabilitan los ID de usuario de forma inmediata tras una baja o despido?  ¿Existen una comunicación entre la administración de seguridad (gestor de accesos) y recursos humanos?  ¿Existe una revisión periódica para identificar y deshabilitar los ID de usuario redundantes?  ¿Se eliminan los ID deshabilitados después de confirmar que ya no son necesarios?  ¿Se reasignan los ID de usuarios dados de baja ? | Responsable de Seguridad de la Información |  | Existe un procedimiento para la gestión de identidades, pero no está formalizada. SÍ se utiliza un ID de usuario único para cada usuario. También se generan en función a una solicitud con aprobaciones y registros apropiados. Al hacer la revisión mensual, se verifica los usuarios que dejaron la empresa, y se deshabilitan sus ID correspondientes. Sí existe una comunicación entre administración de seguridad y recursos humanos, sin embargo, es para caso específicos. | 70% | Parcialmente |
| z | 5.17 | Información de autenticación |  |  | La asignación y gestión de la información de autenticación debe ser controlada por un proceso de gestión, incluyendo el asesoramiento al personal sobre el manejo adecuado de la información de autenticación. | ¿Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.?  ¿Se confirma la identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas?  ¿Se generan contraseñas temporales suficientemente fuertes?  ¿Se cambian las contraseñas por defecto de los fabricantes para los servidores, switch, router, etc.?  ¿Se almacena de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones?  ¿Cómo se asegura la confidencialidad de las credenciales de autenticación?  ¿Existe un proceso de cambio de contraseñas en caso de ser comprometida?  ¿Existen controles de seguridad relativas a las cuentas compartidas?  Los sistemas tiene configurado reglas tales como:  • Longitud mínima de la contraseña  • Evitan la reutilización de un número específico de contraseñas  • Imponen reglas de complejidad en la contraseña donde se incluye mayúsculas, minúsculas, números, símbolos, etc.  • Cambio forzado de contraseñas en el primer inicio de sesión  • Esconde la contraseña durante el inicio de sesión | Responsable de Seguridad de la Información |  | Se implementaron controles sobre la longitud mínima de la contraseña, reglas de complejidad. No se implementaron datos biométricos, contraseñas compartidas, cambio forzado en el primer uso. Si se confirma la identidad de los nuevos usuarios antes de proporcionarles contraseñas temporales nuevas. Las contraseñas temporales tienen la misma fortaleza que las contraseñas de personal en tiempo completo. Sí se cambian las contraseñas por defecto de los fabricantes para servidores, switch, router, etc. Si se almacena las contraseñas de forma cifrada y también existe proceso de cambio de contraseña. Su confidencialidad de las contraseñas se basa en los apartados de confidencialidad del contrato del personal. | 80% | Sí |
| 18 | 5.18 | Derechos de acceso |  |  | Los derechos de acceso a la información y otros activos asociados deben ser aprovisionados, revisados, modificados y removidos en concordancia con la política especifica de la organización y las reglas para el control de acceso. | ¿El acceso a sistemas y servicios de información se basa en las necesidades del negocio?  ¿Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones?  ¿Existe un registro documental de la solicitud y aprobación de acceso?  ¿Se hace una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones?  ¿Participan en dicha revisión los "propietarios" para verificar cambios en las funciones de los usuarios?  ¿Se revisan los derechos de acceso para usuarios con privilegios, con que frecuencia?  ¿Existe un proceso de ajuste de derechos de acceso?  ¿Se retira el acceso físico a las instalaciones y el acceso lógico a la red para los colaboradores, contratista al finaliza o cambiar de empleo?  En casos en los que se usan credenciales compartidas, ¿Se cambian las contraseñas cuando ocurren ceses o despidos de empleados que las usan? | Responsable de Seguridad de la Información |  | El acceso a sistemas y servicios de información se basa en las necesidades del negocio. Sin embargo, no existe una política de control de acceso a la cual se ajuste. Si existe un registro, el cual lo maneja el área de TI. Ellos también hacen una revisión documentada sobre los derechos de acceso de los usuarios. Tienen participación los propietarios en dichas revisiones, sin embargo, no es muy activa. | 80% | Sí |
| 19 | 5.19 | Seguridad de la información en las relaciones con los proveedores |  |  | Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de producto o servicios del proveedor. | ¿Existen políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con proveedores que involucran servicios de TI?  ¿Incluyen servicios de nube, logística, servicios públicos, recursos humanos, médicos, financieros, legales y otros servicios subcontratados de alto riesgo?  ¿Los contratos y acuerdos abordan lo siguiente?  • Riesgo de la información y los aspectos de seguridad, la métrica, el rendimiento, problemas, rutas de escalada  • Información y/o propiedad intelectual, obligaciones y limitaciones.  • Rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad de la información  • Requisitos legales y normativos, como el cumplimiento certificado de ISO 27001.  • Identificación de controles físicos y lógicos.  • Gestión de eventos, incidentes y desastres incluyendo evaluación, clasificación, priorización, notificación, escalado, gestión de respuesta y aspectos de continuidad del negocio  • Concientización de seguridad a los colaboradores  • Derecho de auditoría de seguridad por parte de la organización  ¿Existe una obligación contractual de cumplimento?  ¿Los proveedores de servicios externos son monitoreados y auditados para cumplir con los requisitos de seguridad? | Gestor de compras y administración  Responsable de Seguridad de la Información | Contrato del área de TI | Existe un contrato sobre la relación laboral entre la empresa propietaria y la empresa encargada de brindar servicios TI. Este sí incluye servicio de nube, logística, y otros servicios subcontratados. En estos si se aborda el riesgo de información y aspectos de seguridad, información y/o propiedad intelectual, obligaciones y limitaciones, rendición de cuentas y responsabilidades relacionadas con el riesgo y la seguridad informática, identificación de controles físicos y lógicos, gestión de eventos, incidentes, y desastres, derecho de auditoría de seguridad por parte de la organización, concientización de seguridad a los colaboradores. El contrato abarca la obligación contractual del cumplimiento de sus funciones. Si cuenta con un monitoreo constante para poder brindar seguridad y no ser vulnerados. | 80% | Sí |
| 20 | 5.20 | Directrices de seguridad de la información en los acuerdos con proveedores |  |  | Los requisitos de seguridad pertinentes deben establecerse y acordarse cada proveedor en función del tipo de relación con el proveedor. | ¿Los contratos con proveedores cubren lo siguiente?  • Gestión de las relaciones, incluyendo riesgos  • Cláusulas de confidencialidad  • Descripción de la información que se maneja y el método de acceder a dicha información  • Estructura de la clasificación de la información a usar  • Notificación de incidentes de seguridad  • Aspectos de continuidad del negocio  • Subcontratación y restricciones en las relaciones con otros proveedores  • Legajo de los antecedentes del personal que brinde el servicio (ej. Rendimiento, antecedentes, “robo de empleados”, etc.) | Gestor de compras y administración  Responsable de Seguridad de la Información | Contrato del área de TI | Cumple con cláusulas de confidencialidad, gestión de relaciones, incluyendo riesgos, aspectos de continuidad de negocio, subcontratación y restricciones en las relaciones con otros proveedores, legajo de los antecedentes del personal. Notificación de incidentes de seguridad. | 90% | Sí |
| 21 | 5.21 | Gestión de la seguridad de la información en la cadena de suministro de TIC |  |  | Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de las TIC. | ¿Cómo se validan los requisitos de seguridad a los productos o servicios adquiridos?  ¿Cómo se logra una capacidad de recuperación cuando los productos o servicios críticos son suministrados por terceros? | Gestor de compras y administración  Responsable de Seguridad de la Información |  | El área de TI le brinda a la empresa propietaria las especificaciones técnicas de los productos o servicios a adquirir. El ingeniero de sistemas valida que el equipo o software cumplan con los requerimientos de la empresa. No existe un plan contingente para ese tipo de situaciones, y en la entrevista se menciona que ese mismo hecho le ha generado problemas a la empresa. | 40% | No |
| 22 | 5.22 | Seguimiento, revisión y gestión de cambios de servicios de proveedores |  |  | La organización debe hacer seguimiento, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios. | ¿Existe una monitorización de servicios y quien responsable de esta actividad?  ¿Se llevan a cabo reuniones de revisión del servicio, con qué frecuencia?  ¿Se generan informes y / o métricas relacionadas al servicio proporcionado?  ¿Las reuniones abarcan riesgos, incidentes, políticas, cumplimiento e informes de auditoría?  ¿Existen cláusulas de penalización o de bonificación en el contrato relacionadas con el riesgo de la información?  ¿Cómo se comunican los cambios en los servicios relacionados con la información, servicios adicionales o cambios en la forma en que se prestan los servicios contratados?  ¿Cómo se comunican cambios en las políticas y requerimientos legales de la organización?  ¿Se actualizan los acuerdos relacionados con los cambios? | Gestor de compras y administración  Responsable de Seguridad de la Información | Contrato del área de TI | Sí existe. El área de TI es el encargado del inventario de todos los equipos con los que cuenta la empresa, y ellos se encargan de su monitorización. No se cuentan con mantenimientos preventivos, sino con mantenimientos correctivos en su mayoría. Si existen cláusulas de penalización en el contrato relacionadas con el riesgo de información. Por medio del staff de abogados se comunican los cambios en las políticas y requerimientos legales de la organización. Estos se notifican por medio del correo. | 60% | Parcialmente |
| 23 | 5.23 | Seguridad de la información para el uso de servicios en la nube |  |  | Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización | ¿Se tienen servicios en la nube, cuales son?  ¿Se tiene una política sobre uso de servicios en la nube? ¿Se ha comunicado?  ¿Se tiene definido un procesos de adquisición, uso, gestión y salida de los servicios en la nube?  ¿Se tiene definido las funciones y responsabilidades relacionadas con el uso y la gestión de los servicios en la nube?  ¿Qué controles de seguridad de la información gestiona el proveedor de  servicios en la nube y cuáles gestiona la organización como cliente del  servicio en la nube?  ¿Existe un procedimiento para el manejo de incidentes de seguridad de la información que se produzcan en relación con el uso de los servicios en la nube?  ¿Se monitorea, revisa y evalúa el uso continuo de los servicios en la nube para administrar riesgos de seguridad de la información?  ¿Existe un acuerdo de servicio en la nube debería abordar los requisitos de confidencialidad, integridad, disponibilidad y manejo de la información de la organización? | Tecnología de la Información  Responsable de Seguridad de la Información |  | Si, la empresa cuenta con servicios en la nube. Recientemente se migraron a microsoft 365, por lo que tienen acceso a servicios como onedrive, sharepoint, teams, entre otros. Al ser reciente, no se cuenta con una política sobre el uso de servicios en la nube, ni tampoco un proceso de adquisición o gestión de los servicios en la nube. En la entrevista se comentó que, al empresa estar creciendo, se requiere de un procedimiento para el manejo de incidentes de seguridad de la información en la nube. | 60% | Parcialmente |
| 24 | 5.24 | Planificación y preparación de la gestión de incidentes de seguridad de la información |  |  | La organización debe planificarse y preparar la gestión de los incidentes de seguridad de la información definiendo, estableciendo y comunicando los procesos, las funciones y las responsabilidades de gestión de incidentes de seguridad de la información. | ¿Existen políticas, procedimientos, instructivos para la gestión de incidentes?  ¿Se cuenta con plan de respuesta a incidentes?  ¿Se cuenta con un puntos de contacto para la notificación de incidentes, seguimiento y evaluación ?  ¿Se realizan el monitoreo, detección y reporte de eventos de seguridad?  ¿Se cuenta con algún método de recolección de evidencias y pruebas forenses digitales?  ¿Se realizan revisiones post-evento de seguridad?  ¿Se realiza un procesos de aprendizaje?  ¿Existen evidencias de la notificación de incidentes, registro, clasificación, asignación de resolución, la mitigación y la confirmación de cierre? | Gestor de seguridad tecnológica  Responsable de Seguridad de la Información |  | El procedimiento se basa en notificar al área de TI sobre el incidente. Se hace énfasis en su modelo de acción reactivo, no preventivo. Por ello también se cuenta con un punto de contacto para la notificación de incidentes. Los monitoreos no son tan seguidos, mayormente después de un incidente. También se realiza un proceso de aprendizaje después de un evento imprevisto. No se cuenta con ningún economato que permita tener eso en el inventario. | 60% | Parcialmente |
| 25 | 5.25 | Evaluación y decisión sobre los eventos de seguridad de información |  |  | La organización debe evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información. | ¿Qué tipos de eventos se espera que informen los empleados?  ¿A quién informa los eventos dentro de la organización?  ¿Cómo se evalúan estos eventos para decidir si califican como incidentes?  ¿Hay una escala de clasificación?  ¿Hay un proceso de clasificación y / o escalamiento para priorizar los incidentes? ¿En qué se basa? | Gestor de seguridad tecnológica  Responsable de Seguridad de la Información |  | Cuando existe un virus o un equipo que no esté funcionando de manera óptima. Estos se le informan al administrador de la empresa, la cual las deriva al área de TI. Se evalúa al criterio del administrador. No se presencia una escala de clasificación. | 60% | Parcialmente |
| 26 | 5.26 | Respuesta a incidentes de seguridad de la información |  |  | Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados. | ¿Cómo se recolecta, almacena y evalúa la evidencia respecto a los incidentes de seguridad de la información?  ¿Existe una matriz de escalamiento para usarlo según sea necesario?  ¿Existen medios para comunicar información de tales incidentes a las organizaciones internas y externas pertinentes?  ¿Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente? | Gestor de seguridad tecnológica  Responsable de Seguridad de la Información |  | Todos los meses se graban en discos duros la información. Cada cierre de mes para poder tener la data de seguridad en caso de tener un evento. El medio por el cual se comunica información de tales incidentes es un correo institucional. El tercerizado documenta las acciones tomadas por medio del correo tambien, | 70% | Parcialmente |
| 27 | 5.27 | Aprendizaje de los incidentes de seguridad de la información |  |  | El conocimiento obtenido de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información. | ¿Existe un proceso de evaluación para identificar incidentes de impacto recurrentes?  ¿Se aprovecha la información obtenida de la evaluación de incidentes para evitar recurrencias?  Además, ¿Se está utilizado para formación y concienciación?  ¿La organización cuenta con un proceso de gestión de incidentes? ¿En que nivel podrían indicar que se encuentra?  ¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad? | Gestor de seguridad tecnológica  Responsable de Seguridad de la Información |  | No se tiene un proceso de evaluación para identificar incidentes fijo. La empresa es más reactiva en ese aspecto, pero si se toman algunas medidas. Sin embargo, no es un proceso documentado. Sirve tambien para dar formación y concientización. El tercerizado tiene un proceso de gestión de incidentes, pero no ha sido comunicado en su totalidad con la gerencia. | 60% | Parcialmente |
| 28 | 5.28 | Recopilación de evidencias |  |  | La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información. | ¿La recolección de evidencias de hace de forma competente en la empresa o por terceros especializados y capacitados en esta área?  ¿Existe un gestor de incidentes de seguridad ?  ¿Quién decide emprender un análisis forense, y en qué criterio se base? | Gestor de seguridad tecnológica  Responsable de Seguridad de la Información |  | La recolecion de evidencias si se hace por un tercerizado especializado en el área. Si se tiene un gestor de incidestes de seguridad, el Ingeniero Javier. La gerencia se encarga de decidir si emprender un analisis forense según su criterio. | 100% | Sí |
| 29 | 5.29 | Seguridad de la información durante interrupciones |  |  | La organización debe planificar como mantener la seguridad de la información en un nivel adecuado durante la interrupción. | ¿Existe un plan de continuidad de negocio?  ¿Los planes tienen plazos definidos para restaurar servicios tras una interrupción?  ¿Se tiene equipos de recuperación / gestión de crisis / incidentes con conocimiento de los planes y tienen claro sus roles y responsabilidades?  ¿Los controles de seguridad son adecuados en los sitios de recuperación de desastres remotos? ¿Se ha realizado alguna verificación, cuando ha sido la ultima vez?  ¿Existe un método de pruebas del plan de continuidad?  ¿Con qué frecuencia se llevan a cabo dichas pruebas?  ¿Hay evidencia de las pruebas reales y sus resultados?  ¿Se han identificado deficiencias?, ¿Se han remediado? y ¿Se han vuelto a probar hasta que los resultados sean satisfactorios? | Responsable de Seguridad de la Información |  | Si existe un plan de continuidad de negocio. Tambien se cuentan con plazos definidos para retaurar servicios tras una una interrupción. El tercerizado es el encargado de los equipos de recuperació, gestión de crisis etc. Tambien tienen claro cuales son sus roles y responsabilidades. Los controles de seguridad si son adecuados en los sitios de recuperación de desastres remotos. Se comenta que la ultima verificación fue hace 1 año. La gerencia dezconoce si existe un método de pruehas de plan de continuidad. Se vuelve a presentar un deficit en la comunicación con su tercerizado. | 80% | Sí |
| 30 | 5.30 | Preparación de las TIC para la continuidad del negocio |  |  | La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC. | ¿Existe un plan de continuidad de las TIC, donde se incluyan los procedimientos de respuesta y recuperación?  ¿Existen un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos?  ¿Se tiene definido el tiempo de recuperación objetivo (RTO) y punto de recuperación objetivo (RPO)? | Responsable de Seguridad de la Información |  |  |  | No |
| 31 | 5.31 | Identificación de requerimientos legales, estatutarios, regulatorios y contractuales |  |  | Los requisitos legales, estatuarios, regulatorios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados. | ¿Existe una política acerca del cumplimiento de requisitos legales?  ¿Se mantiene un registro o base de datos de cumplimiento enumerando todas las obligaciones, expectativas legales, reglamentarias y contractuales aplicables?  ¿Hay una persona encargada de mantener, usar y controlar el registro?  ¿Cómo se logra y se garantiza el cumplimiento?  ¿Existen controles adecuados para cumplir con los requisitos? | Responsable Legal  Responsable de Seguridad de la Información |  | No existe una política acerca del cumplimiento de los requisitos legales. No hay un registro o base de datos de cumplimiento, sin embargo, se menciona acerca de un reglamento interno de trabajo. | 0% | No |
| 32 | 5.32 | Derechos de Propiedad Intelectual |  |  | La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual. | ¿Existen políticas y procedimientos respecto a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento? | Responsable Legal  Responsable de Seguridad de la Información |  | No se tiene una politica o procedimiento acerca de la addquisición y uso de licencias de propiedad intelectual o gestión de licencias. | 0% | No |
| 33 | 5.33 | Protección de registros |  |  | Los registros deben protegerse contra perdidas, destrucción, falsificación, acceso no autorizado y liberación no autorizada. | Existe una política que contemple lo siguiente: Clasificación, categorización, períodos de retención y medios de almacenamiento permitidos.  ¿Se almacenan las firmas digitales de forma segura? ¿Donde se almacenan?  ¿Se contempla la destrucción y/o eliminación de aquellos registros que ya no son útiles a la organización?  ¿Se verifica periódicamente la integridad de los registros?  ¿Se utilizan medios de almacenamiento de larga duración para el almacenamiento a largo plazo? | Gestor de seguridad tecnológica  Responsable de Seguridad de la Información |  | No se tiene una politica que contemple la clasificación, categorización, periodos de retención, y medios de almacenamiento permitidos. Si se almacena la firma digital, y cada persona lo tiene en su propio equipo. Se menciona que solo los miembros de la gerencia sueles tener la firma digital, puesto que son los que suelen usarla frecuentemente al momento de hacer acuerdos y contratos. No se completa la destrucción de registros si estos estan en el equipo, puesto que se menciona que, al momento en el un trabajador se desliga de la empresa, se aisla su correo institucional, inhabilitandolO, por lo que si se hace este proceso, pero solo en caso de la nube, no de forma local. No se revisa periodicamente la integridad de los registros. El medio de almacenamiento de larga duración sería el mismo servidor. | 60% | Parcialmente |
| 34 | 5.34 | Privacidad y protección de la información de identificación personas (IIP) |  |  | La organización debe identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la IIP de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales. | ¿Existe mecanismos para instruir al personal en el manejo de información de carácter personal?  ¿Existe un responsable de privacidad en la organización?  ¿El responsable conoce la información de carácter personal que es recopilado, procesado y almacenados por la organización?  ¿Cuáles son los controles de acceso a información de carácter personal?  ¿Cuál es el nivel de acceso y roles (de personal) que tienen acceso a estos activos? | Responsable de Protección de Datos Personales  Responsable de Seguridad de la Información |  | No existe un mecanismo para instruir al personas en el manejo de información de carácter personal. Se menciona que el Ingeniero Javier, de parte del tercerizado, se encarga de la privacidad de la organización. El responsable si conoce la inforamción decaracter personal que es recopilada, procesada y almacenada por la organización. Los controles se desconoce para gerencia, es un proceso del tercerizado. La gerencia y el tercerizado son los que tiene acceso a estos activos. | 50% | Parcialmente |
| 35 | 5.35 | Revisión independiente de la seguridad de la información |  |  | La organización debe realizar revisiones independientes y periódicas de la seguridad de la información, a cargo de personal interno sin conflictos de interés o por terceros, para evaluar la eficacia de los controles y el cumplimiento de políticas.. | ¿Los requisitos de auditoría de sistemas son planificados, autorizados, implementados y controlados para minimizar los riesgos?  ¿La alta dirección revisa y aprueba los resultados de estas auditorías?  ¿Con qué frecuencia se llevan a cabo estas revisiones?  ¿Se documentan los hallazgos de auditoría y los planes de acción ? | Gestor de auditoría  Responsable de Seguridad de la Información |  | Los requisitos de autoría de sistemas si son planificados, autorizados, implementados y controlados para la minimización de los riesgos. Los objetivos y el alcance de autoría si estan autorizados por la gerencia. Tambien se menciona que sí estan debidamente controladas el acceso a las herramientas de autoria del sistema de información. | 100% | Sí |
| 36 | 5.36 | Cumplimiento con políticas y estándares de seguridad de la información |  |  | Se debe verificar periódicamente que las actividades, procesos y sistemas cumplan con las políticas y estándares internos de seguridad de la información establecidos, aplicando controles, revisiones y acciones correctivas cuando sea necesario. | ¿Se hace una verificación del cumplimiento de las políticas y estándares de seguridad de la información? ¿Cada cuanto tiempo?¿Cuando fue la última ves?  ¿Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting regulares?  ¿Qué mecanismos existen para detectar incumplimientos (auditorías, revisiones, monitoreo)? | Gestor de auditoría  Responsable de Seguridad de la Información |  | No se realiza una verificación del cumplimiento de las políticas y estandares de seguridad de la información. Tampoco se realizan escaneo de vulnerabilidades de red o pruebas de Pentesling en general. | 0% | No |
| 37 | 5.37 | Procedimientos operativos documentados |  |  | La organización debe establecer, mantener y actualizar procedimientos operativos documentados para asegurar el uso correcto y coherente de los sistemas, así como la ejecución segura de tareas clave. | ¿Existen procedimientos operativos documentados para las actividades críticas?  ¿Cuándo se revisaron por última vez?  ¿Los roles y responsabilidades están bien definidos y se capacita adecuadamente al personal?  ¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)?  ¿Dónde se almacenan los documentos y quién tiene acceso a ellos? | Tecnología de la Información  Gestor de seguridad tecnológica  Responsable de Seguridad de la Información |  | No se tienen procedimientos documentados para las operaciones de TI, sistemas y gestión de redes, gestión de incidencias, administración de TI, seguridad de TI, seguridad física, gestión de cambios, etc. Si se tienen los roles definidos y se capacita al personal adecuadamente. Todos los cambios, configuraciones, versiones, capacidad, rendimiento, etc, lo toma en cuenta el area de TI tercerizado. | 70% | Parcialmente |
| 6 | Controles de personas | | | | | | | | | |  |
| 38 | 6.01 | Investigación de antecedentes |  |  | Se debe realizar investigaciones de antecedentes laborales y, cuando corresponda, verificaciones legales o penales, de todo el personal que tenga acceso a información sensible o sistemas críticos, antes de su contratación y según las leyes aplicables. | ¿La investigación de antecedentes lo realiza la empresa o se subcontrata a un tercero?  Si se subcontrata a un tercero, ¿Se ha revisado sus procesos ? ¿Se han considerado aceptables?  ¿Se hace contacto de referencias y una verificación de antecedentes, según corresponda durante el proceso de selección?  ¿Existen procesos de selección mejorados para los trabajadores con denominación de cargos críticos?  ¿Hay un proceso documentado que sea de propiedad y mantenido por recursos humanos? | Recursos Humanos |  | La investigación de antecedentes lo realiza el area de RR.HH. De la empresa. Si se realiza contacto de referencias y verificación de antecedentes. Tambien existen procesos documentados de pertenencia de RRHH. | 100% | Sí |
| 39 | 6.02 | Términos y condiciones del empleo |  |  | La organización debe definir, documentar y comunicar los términos y condiciones de empleo, incluyendo las responsabilidades relacionadas con la seguridad de la información, antes de que los empleados comiencen sus funciones. | ¿Todos los empleados, proveedores y terceros firman acuerdos de confidencialidad y no divulgación?  ¿Se comunican claramente los derechos y responsabilidades del empleado antes de su incorporación? | Recursos Humanos  Legal |  | Los proveedores no firman acuerdos de confidencialidad, pero el personal sí. | 90% | Sí |
| 40 | 6.03 | Concientización, educación y entrenamiento en seguridad de la información |  |  | El personal de la organización y las partes interesadas relevantes deben recibir la concienciación, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral. | ¿Todos los empleados, proveedores y terceros continuamente se someten a una capacitación de seguridad apropiada a su función dentro de la organización?  Y si es así ¿Con qué frecuencia se imparten sesiones de concientización o entrenamiento?  ¿Se evalúa la eficacia de la capacitación como cuestionarios, simulacros, etc?  ¿Se actualiza el contenido del programa con base en nuevas amenazas o incidentes? | Recursos Humanos  Seguridad de la información |  | Ni los empleados ni proveedores ni terceros se someten a una capacitación de seguridad apropiada a su función dentro de la organización | 0% | No |
| 41 | 6.04 | Proceso disciplinario |  |  | Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información. | ¿Existe un procedimiento disciplinario formal que permita a la organización tomar acciones contra empleados que han cometido una violación de seguridad de la información?  ¿Está comunicada a todos los empleados?  ¿Participa el área legal o de recursos humanos en la aplicación del proceso? | Recursos Humano  Legal |  | Existe un reglamento interno de trabajo, que tambien sirve la función de guia al momento de sancionar a un empleado. | 70% | Parcialmente |
| 42 | 6.05 | Responsabilidades después de la finalización o cambio de empleo |  |  | Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se definirán, aplicarán y comunicarán al personal pertinente y otras partes interesadas. | ¿Existe un proceso documentado para la finalización o cambio de tareas de los empleados?  ¿Se informa al ex empleado sobre sus obligaciones posteriores al empleo?  ¿Está la organización habilitada para forzar tareas de cumplimiento posterior a la salida del cargo?  ¿Se realiza un seguimiento para confirmar la eliminación de accesos remotos o cuentas? | Recursos Humanos |  | Los memorandums sirve como documento que se envia en el proceso de finalización o cambio de tareas a los empleados. Se le comunica solo al empleado afectado. La organización no está habilitada para forzar tareas de cumplimiento posterior a la salida del cargo. Unicamente se le da al empleado 48 horas, posterior a su notificación, para entregar todo el cargo formalmente. | 100% | Sí |
| 43 | 6.06 | Acuerdos de confidencialidad o no revelación |  |  | La organización requiere que empleados, contratistas y terceros firmen acuerdos de confidencialidad o no revelación para proteger la información sensible antes, durante y después de su relación contractual. | ¿Los empleados, contratistas y agentes firman contratos de confidencialidad o acuerdos de no-divulgación?  ¿Los acuerdos antes descritos están sujetos a revisiones regulares?  ¿Se mantienen registros de los acuerdos?  ¿Se revisan y actualizan periódicamente los formatos de los acuerdos?  ¿Aplican estos acuerdos a empleados, contratistas y terceros? | Recursos Humanos  Legal |  | Los empleados, contratistas y agentes si firman acuerdos de confidencialidad. También, dichos acuerdos están sujetos a revisiones regulares. También se mantienen registros de los acuerdos | 100% | Sí |
| 44 | 6.07 | Teletrabajo |  |  | Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización. | ¿Existe una política de teletrabajo?  Y si es así ¿Se proporciona capacitación sobre prácticas seguras de trabajo remoto?  ¿Está comunicada a todos los empleados? | Recursos Humanos |  | No se tiene política de teletrabajo | 0% | No |
| 45 | 6.08 | Reporte de eventos de seguridad de la información |  |  | La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna. | ¿Hay algún proceso para el oportuno reporte de eventos de seguridad de la información?  Y si es así ¿Se hace seguimiento a los eventos reportados hasta su resolución?  ¿Hay algún proceso para reportar vulnerabilidades en la seguridad de información que ya se hayan identificado?  ¿Todo el personal conoce cómo y a quién reportar un evento de seguridad? | Recursos Humanos |  | El proceso para el oportuno reporte de eventos de seguridad de la información es comunicar al área de TI al momento de un incidente. También se reporta la vulnerabilidades en la seguridad de información via email. | 70% | Parcialmente |
| 7 | Controles físicos | | | | | | | | | |  |
| 46 | 7.01 | Perímetro de seguridad física |  |  | Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados. | ¿Está claramente definido el perímetro de seguridad física de las instalaciones?  ¿Se controla el acceso físico mediante tarjetas, biometría u otros mecanismos?  ¿Se realizan inspecciones o rondas de seguridad periódicas? | Seguridad Física |  | Si hay un perímetro de seguridad designado para el área de servidores | 100% | Sí |
| 47 | 7.02 | Controles de entrada física |  |  | Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados. | ¿Las áreas seguras disponen de un debido sistema de control de entrada a fin de asegurar que solo el personal autorizado tenga acceso?  ¿Están separadas las áreas de carga y descarga?  ¿Se lleva un registro de visitas, incluyendo fecha, hora y persona anfitriona? | Seguridad Física |  | La áreas de seguridad no disponen de un debido sistema de control de entrada y salida. Tampoco están separadas de cargas y descargas | 0% | No |
| 48 | 7.03 | Seguridad de oficinas, despachos y recursos |  |  | Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones. | ¿Las oficinas, habitaciones y otras dependencias han sido diseñadas y configuradas teniendo la seguridad en consideración? | Seguridad Física |  | Las oficinas, habitaciones y otras dependencias no han sido diseñadas ni configuradas teniendo en cuenta la seguridad | 0% | No |
| 49 | 7.04 | Supervisión de la seguridad física |  |  | Los locales deberán ser monitoreados continuamente para el acceso físico no autorizado. | ¿Son monitoreados continuamente los accesos físicos no autorizados?  ¿Se aplican prácticas de escritorio limpio y pantalla bloqueada? | Seguridad Física  Seguridad de la información |  | Si son monitoreados con la camara interna de la empresa | 100% | Sí |
| 50 | 7.05 | Protección contra las amenazas físicas y ambientales |  |  | Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura. | ¿Se han diseñado medidas de protección física a fin de prevenir desastres naturales, ataques maliciosos o accidentes? | Seguridad Física  Seguridad de la información |  | Tienen ciertas medidas, pero el negocio es más reactivo | 50% | Parcialmente |
| 51 | 7.06 | Trabajar en áreas seguras |  |  | Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras. | ¿Existen las áreas seguras?  ¿En donde existan, las áreas seguras cuentan con políticas y procesos?  ¿Las políticas y procesos son monitoreados? | Seguridad Física  Seguridad de la información |  | Si existen las áreas seguras. Se encuentran ubicadas las políticas y procesos de defensa civil. Sin embargo, las políticas y procesos no están siendo monitoreadas. | 70% | Parcialmente |
| 52 | 7.07 | Escritorio limpio y pantalla limpia |  |  | Se deben definir y hacer cumplir adecuadamente las reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y las reglas de pantalla limpia para las instalaciones de procesamiento de información. | ¿Existe una política de escritorio/pantalla limpia?  ¿Está esto bien aplicado y es periódicamente supervisado? | Seguridad de la información |  | No hay una política de escritorio,/pantalla limpia | 0% | No |
| 53 | 7.08 | Ubicación y protección del equipamiento |  |  | El equipo se colocará de forma segura y protegida.  Reducir los riesgos de amenazas físicas y ambientales, y de accesos y daños no autorizados. | ¿Los riesgos ambientales son identificados y considerados cuando son seleccionadas las áreas de equipamiento?  ¿Se consideran los riesgos de acceso no autorizado / transeúntes cuando se sitúa el equipo? | TI- infraestructura  Seguridad de la información |  | Los riesgos ambientales son identificados y considerados cuando son seleccionadas las áreas de equipamiento. Sin embargo, no se consideran los riesgos de acceso no autorizado/transeúntes cuando se situa el equipo. | 50% | Parcialmente |
| 54 | 7.09 | Seguridad de los activos fuera de las instalaciones |  |  | Se protegerán los activos fuera del sitio.  Para evitar la pérdida, el daño, el robo o el compromiso de los dispositivos externos y la interrupción de las operaciones de la organización. | ¿Existe una política que cubra la seguridad de los activos fuera del sitio?  ¿Está esta política ampliamente comunicada? | TI- infraestructura  Seguridad de la información |  | La gerencia desconoce si habrá una política que cubra la seguridad de los activos como tal, pero se sabe que el Ingeniero Javier, responsable de TI tercerizado, tiene dicho activos identificados. | 60% | Parcialmente |
| 55 | 7.10 | Medios de almacenamiento |  |  | Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización. | ¿Hay alguna política que gobierne sobre las unidades removibles?  ¿Las políticas y procesos referentes al uso de unidades removibles son sociabilizadas con los empleados?  ¿Existe algún procedimiento formal que indique cómo deben ser desechadas las unidades removibles?  ¿Hay alguna política documentada y proceso que detalle cómo deben transportarse los medios físicos? | TI- infraestructura  Seguridad de la información |  | El área de TI tiene una política sobre las unidades removibles. Estas no son socializadas con los empleados. Se desconoce si habrá un procedimiento como deben ser desechadas las unidades removibles. Hay una política interna sobre cómo se deben transportar los medios físicos, sin embargo, no está documentada. | 70% | Parcialmente |
| 56 | 7.11 | Utilidades de apoyo |  |  | Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo. | ¿Existe algún sistema de UPS o generador de contingencia?  ¿Estos tienen pruebas en apropiados intervalos de tiempo? | Seguridad Física  TI- infraestructura  Seguridad de la información |  | Si existe un generador de contingencia, pues se graba toda la data en unos discos de contingencia. Se hacen pruebas mensuales a estos. | 100% | Sí |
| 57 | 7.12 | Seguridad del cableado |  |  | Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños. | ¿Tiene evaluaciones de riesgo sobre la localización de cables eléctricos y telecomunicaciones?  ¿Están estas localizaciones protegidas de interferencia, interceptación o daño? | TI- infraestructura |  | Si presentan evaluaciones de riesgo sobre la localización de cables eléctricos y telecomunicaciones. Estos están ubicados bajo el suelo, o canaleta y siempre con tubos corrugados. | 100% | Sí |
| 58 | 7.13 | Mantenimiento de equipos |  |  | El equipo se mantendrá correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información. | ¿Existe una programación rigurosa de mantenimiento al equipamiento? | TI- infraestructura |  | No existe una programación de mantenimiento al equipamiento. | 0% | No |
| 59 | 7.14 | Eliminación segura o reutilización de equipos |  |  | Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o  sobrescrito de forma segura antes de su eliminación o reutilización. | ¿Existe una política que indique como reutilizar los activos de información?  ¿Cuando se limpian los datos, ¿se verifica esto adecuadamente antes de su reutilización / eliminación? | TI- infraestructura  Seguridad de la información |  | No existe una política que indique cómo reutilizar los activos de información | 0% | No |
| 8 | Controles tecnológicos | | | | | | | | | |  |
| 60 | 8.01 | Dispositivos de punto final del usuario |  |  | Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario. | ¿Existe una política para dispositivos finales de usuario?  ¿Existen controles técnicos para asegurar el equipo que ha sido abandonado inadvertidamente? | TI- infraestructura  Seguridad de la información |  | No existe política para dispositivos finales de usuario. Pero sí existen controles técnicos para asegurar el equipo que ha sido abandonado inadvertidamente. Estos loss gestiona el área de TI | 50% | Parcialmente |
| 61 | 8.02 | Derechos de acceso privilegiado |  |  | La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará. | ¿Las cuentas con accesos privilegiados son administradas y controladas por separado? | Seguridad de la información |  | Las cuentas con accesos privilegiados sí son administradas y controladas por separado por el área de TI. El tercerizado los administra | 100% | Sí |
| 62 | 8.03 | Restricción del acceso a la información |  |  | El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso. | ¿El acceso a información y a funcionalidades de los aplicativos internos está siendo restringido con la política de control de accesos? | TI- infraestructura  Seguridad de la información |  | El acceso a información y a funcionalidad de los aplicativos sí está siendo restringido con la política de control de accesos. | 100% | Sí |
| 63 | 8.04 | Acceso al código fuente |  |  | El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente. | ¿El acceso al código fuente de os programas en desarrollo de la organización está protegido? ¿Qué controles aplican?  ¿Mediante que herramienta se gestiona el acceso a código fuente? ¿Qué medida de seguridad posee? | TI- Desarrollo |  | El acceso a código fuente de los programas en desarrollo está resguardado, el equipo de TI se encarga de eso | 80% | Sí |
| 64 | 8.05 | Autenticación segura |  |  | Las tecnologías y procedimientos de autenticación segura se implementarán en función de  las restricciones de acceso a la información y la política específica del tema sobre el control  de acceso. | ¿Donde la política de control de accesos lo requiera, el acceso es controlado por un procedimiento de autenticación seguro? | Seguridad de la información |  | Aunque se cuenta con el autenticador de Microsoft 365, el control de autenticación segura no se implementa de forma integral. No se evidencia el uso de autenticación multifactor (MFA) para accesos críticos, ni políticas escritas que definan los estándares mínimos de autenticación en todos los sistemas utilizados. | 70% | Parcialmente |
| 65 | 8.06 | Gestión de la capacidad |  |  | El uso de los recursos se controlará y ajustará de acuerdo con los requisitos de capacidad actuales y previstos. | ¿Existe un proceso de gestión de capacidad? | TI- infraestructura |  | El proceso actual de gestión de capacidad es reactivo, basado en notificaciones informales cuando el sistema reporta saturación. No se cuenta con herramientas de monitoreo proactivo ni umbrales de alerta para anticipar problemas de rendimiento. | 70% | Parcialmente |
| 66 | 8.07 | Protección contra malware |  |  | La protección contra el malware se implementará y respaldará mediante la concienciación adecuada del usuario. | ¿Existe un proceso para la detección de malware?  ¿Es conocida y concientizado al personal?  ¿Existen procesos para evitar la propagación de malware?  ¿Tiene la organización un proceso y la capacidad de recuperarse de una infección de malware? | TI- infraestructura  Seguridad de la información |  | No se cuenta con un proceso para la detección de malware. Se cuenta con una licencia de antivirus. Existen procesos para evitar la propagación de malware. No se realiza detección proactiva, ni se sensibiliza al personal sobre riesgos como phishing o ransomware. La falta de políticas de respuesta y contención incrementa la vulnerabilidad del sistema. | 50% | Parcialmente |
| 67 | 8.08 | Gestión de vulnerabilidades técnicas |  |  | Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas. | ¿Tiene la organización un medio para acceder a actualizaciones e información técnica actualizada sobre vulnerabilidades?  ¿Existe un proceso de gestión de riesgos y respuesta a cualquier nueva vulnerabilidad que es descubierta?  ¿La organización regularmente conduce revisiones de cumplimiento técnico sobre sus sistemas de información? | Seguridad Informática  TI- infraestructura  Seguridad de la información |  | Se identificó que no se realizan escaneos periódicos de vulnerabilidades, ni se efectúan revisiones de cumplimiento técnico. Aunque se accede a boletines técnicos y se cuenta con un proceso de respuesta reactivo, no se dispone de una estrategia sistemática de gestión. | 60% | Parcialmente |
| 68 | 8.09 | Gestión de la configuración |  |  | Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse. | ¿Existe evidencia documentada de las configuraciones de seguridad de los principales equipos, software y redes de la operación?  ¿Existen plantillas estándar de configuración segura de equipos ,software y redes?  ¿Se actualizan oportunamente las plantillas de configuración segura?  ¿Existe una revisión recurrente a las configuraciones de seguridad implementadas? | TI- infraestructura |  | Existe documentación sobre configuraciones de seguridad, así como plantillas estándar. Sin embargo, no se realizan auditorías periódicas que permitan validar la aplicación de dichas configuraciones. Esta falta de verificación abre la posibilidad a desviaciones no detectadas que comprometan la seguridad del entorno. | 70% | Parcialmente |
| 69 | 8.10 | Eliminación de la información |  |  | La información almacenada en los sistemas de información, dispositivos o en cualquier otro  medio de almacenamiento será eliminada cuando ya no sea necesaria. | ¿Existe un procedimiento de eliminación segura de información de equipos, aplicaciones, sistemas?  ¿Existe un registro de eliminación segura de información?  ¿Se tiene acuerdos contractuales con terceros sobre de borrado seguro de información que tuvieran acceso durante la prestación del servicio? | TI- infraestructura  Seguridad de la información  Legal |  | Este control está correctamente implementado. El procedimiento de eliminación segura está a cargo del proveedor de TI, quien también mantiene un registro formal y actúa conforme a cláusulas contractuales. | 100% | Sí |
| 70 | 8.11 | Enmascaramiento de datos |  |  | El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del  tema de la organización sobre el control de acceso y otras políticas relacionadas con  el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación  aplicable. | ¿Existe políticas de enmascaramiento de datos de información confidencial y/o datos personales?  ¿Existe un procedimiento de enmascaramiento de datos, seudonimización o anonimización? | TI- infraestructura  Seguridad de la información  Legal |  | Se han establecido políticas y procedimientos para el enmascaramiento de datos personales o confidenciales. Sin embargo, no se detalla si estas técnicas se aplican de forma automática o manual, ni si abarcan todos los entornos (producción, pruebas, backup). Dado el riesgo legal por tratamiento indebido de datos personales, es recomendable auditar el cumplimiento del Reglamento de Protección de Datos Personales y automatizar este control. | 80% | Sí |
| 71 | 8.12 | Prevención de la fuga de datos |  |  | Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible. | ¿Existe algún proceso por el cual la información deba ser clasificada en forma apropiada?  ¿Cuentan con alguna herramienta que bloquee la divulgación de información sensible o confidencial sin autorización?  ¿Qué controles aplican para la transferencia segura de información?  ¿Existen procedimientos de autorización para la divulgación de información sensible o confidencial? | TI- infraestructura  Seguridad de la información |  | Aunque existen controles básicos de clasificación y bloqueo de datos, no se han implementado herramientas específicas de DLP para la detección y prevención proactiva de fugas. Tampoco se aplican controles rigurosos en la transferencia de archivos ni alertas en tiempo real. | 60% | Parcialmente |
| 72 | 8.13 | Copias de seguridad de la información |  |  | Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del  tema acordado. | ¿Existe una política de copias de seguridad?  ¿La política de copias de seguridad de la organización cumplen con marcos de referencia legal?  ¿Las copias de seguridad se ejecutan conforme a la política?  ¿Se ejecutan pruebas a las copias de seguridad? | TI- infraestructura  Seguridad de la información |  | El control está correctamente ejecutado por el proveedor de TI. Se cumplen las políticas y marcos legales, y se realizan pruebas de restauración. No obstante, sería importante que la organización propietaria supervise estas pruebas y mantenga evidencia documentada, además de establecer criterios de RTO/RPO formales y almacenamientos off-site. | 100% | Sí |
| 73 | 8.14 | Redundancia de las instalaciones de procesamiento de información |  |  | Las instalaciones de procesamiento de información se implementarán con suficiente redundancia para cumplir con los requisitos de disponibilidad. | ¿Las dependencias que procesan información tienen suficiente redundancia como para cumplir los requerimientos de disponibilidad de la organización? | TI- infraestructura  Seguridad de la información |  | La redundancia está garantizada en la infraestructura crítica, lo cual fortalece la disponibilidad. Se recomienda documentar los procedimientos de failover y realizar simulacros de contingencia para asegurar que esta capacidad técnica pueda ser utilizada de manera efectiva ante fallas reales. | 100% | Sí |
| 74 | 8.15 | Gestión de eventos (Log) |  |  | Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallas y otros eventos relevantes. | ¿Los registros están protegidos contra manipulación indebida y acceso no autorizado?  ¿Los registros de eventos son mantenidos y revisados regularmente?  ¿Los registros de eventos de administradores y operadores están mantenidos, protegidos y revisados regularmente? | TI- infraestructura  Seguridad de la información |  | Si bien los registros están protegidos y almacenados, la revisión no es sistemática ni frecuente. La empresa actúa de forma reactiva ante incidentes, lo que limita su capacidad de detección temprana. | 60% | Parcialmente |
| 75 | 8.16 | Actividades de seguimiento |  |  | Las redes, los sistemas y las aplicaciones deberán ser monitoreados por comportamiento  anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información. | ¿Cuentan con sistema de monitoreo aplicado a trafico de red, sistemas, aplicaciones entrantes o salientes?  ¿Se monitorea el comportamiento anómalos en los sistemas, red o aplicaciones?  ¿Se revisa recurrentemente los registros de herramientas de seguridad (IDS, antivirus, FW)? | TI- infraestructura |  | El sistema de monitoreo cumple con los objetivos de supervisión del tráfico de red y comportamiento anómalo. Se revisan los logs de herramientas como antivirus, IDS y firewall. | 100% | Sí |
| 76 | 8.17 | Sincronización del reloj |  |  | Los relojes de los sistemas de procesamiento de información utilizados por la organización deben estar sincronizados con las fuentes de tiempo aprobadas. | ¿Están sincronizados todos los relojes de los equipos de la organización? | TI- infraestructura |  | Todos los relojes del sistema están sincronizados, lo cual asegura la consistencia temporal necesaria para la correlación de eventos y trazabilidad forense. | 100% | Sí |
| 77 | 8.18 | Uso de programas de utilidad privilegiados |  |  | El uso de programas utilitarios que pueden ser capaces de anular o sobrepasar los controles de los sistemas y aplicaciones deberá ser restringido y estrictamente controlado. | ¿El uso de programas de usuario capaces de modificar el sistema y los controles de las aplicaciones, está restringido y fuertemente controlado? |  |  | El uso de programas de utilidad privilegiados está debidamente restringido y controlado por el área de TI. Solo se recomenda establecer un procedimiento formal documentado que registre el acceso y uso de estas herramientas para permitir auditorías futuras y reforzar la trazabilidad. | 90% | Sí |
| 78 | 8.19 | Instalación de software en sistemas operacionales |  |  | Se debe implementar procedimientos y medidas para gestionar adecuadamente la instalación de software en sistemas operacionales | ¿Existen procedimientos para el control de la instalación de software sobre sistemas operacionales? |  |  | Existen procedimientos para controlar la instalación de software, lo que garantiza una gestión segura. Sería deseable complementar este control con la implementación de una lista blanca (whitelisting) de aplicaciones permitidas y un sistema de aprobación formal por parte de TI antes de cualquier instalación. | 90% | Sí |
| 79 | 8.20 | Controles de red |  |  | Las redes, así como los dispositivos de red deben ser asegurados, gestionados y controlados para proteger la información en los sistemas y aplicaciones. | ¿La red está adecuadamente administrada y controlada, con el fin de protegerla de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usa la red, incluida la información en tránsito? |  |  | La red se encuentra correctamente administrada y controlada, lo cual permite proteger la información en tránsito. No obstante, se recomienda documentar los controles implementados y realizar auditorías regulares sobre el tráfico y los dispositivos conectados. | 90% | Sí |
| 80 | 8.21 | Seguridad de los servicios de red |  |  | Los mecanismos de seguridad, los niveles de servicio, así como los requerimientos de las redes deben ser identificados, implementados y monitoreados. | ¿Las características de seguridad, los niveles de servicio, y los requerimientos de administración de todos los servicios de red, están identificados e incluidos en los acuerdos con los diferentes proveedores de servicios de red, bien sean internos o externos? |  |  | Los niveles de seguridad, servicios y requerimientos están incluidos en los acuerdos con proveedores. Se realiza una revisión anual de estos contratos para garantizar su alineación con los estándares actualizados de seguridad. | 100% | Sí |
| 81 | 8.22 | Segregación en redes |  |  | Los grupos de servicios de información, usuarios, y sistemas de información deben ser segregados (segmentados) en las redes de la organización.. | ¿Los controles para segregar / segmentar grupos de dispositivos de información, usuarios y sistemas de información son adecuados? (Ej. Servidores, computadores de usuario, redes de ocio, redes industriales, etc…) |  |  | La segmentación de redes está adecuadamente implementada, lo cual limita la propagación de amenazas. Se mantiene un mapa de red actualizado y realizan pruebas de penetración internas para validar el aislamiento entre segmentos. | 100% | Sí |
| 82 | 8.23 | Filtrado Web |  |  | El acceso a sitios web externos debe ser gestionado para reducir la exposición a contenido malicioso. | ¿Se cuenta con controles que restrinjan el acceso a páginas web con contenido malicioso? |  |  | No existen controles para restringir el acceso a contenido malicioso en sitios web, lo cual representa una amenaza directa. Este control es esencial en un entorno expuesto como el de un grifo. | 0% | No |
| 83 | 8.24 | Uso de Criptografía |  |  | Se debe definir e implementar reglas claras para el uso efectivo de la criptografía (cifrado), incluyendo la gestión de las llaves criptográficas. | ¿Se han definido e implementado reglas claras para el uso efectivo de criptografía (cifrado), incluyendo la gestión de llaves criptográficas? |  |  | Se han definido reglas para el uso de criptografía, lo cual permite proteger adecuadamente la información sensible. Están establecidos procedimientos de rotación periódica de claves y validan que los algoritmos criptográficos estén alineados con los estándares actuales. | 100% | Sí |
| 84 | 8.25 | Ciclo de vida de desarrollo seguro |  |  | Se deben establecer y aplicar reglas para el desarrollo seguro de las aplicaciones. | ¿Se cuenta con una metodología establecida para el desarrollo de sistemas?  ¿Se utilizan procedimientos de control de cambios formales para controlar la implementación de cambios?  ¿Se cuenta con procesos para gestionar las versiones del software?  ¿Las modificaciones de los paquetes de software, son desalentadas, limitadas a los cambios necesarios y todos los cambios son estrictamente controlados?  ¿El ambiente de desarrollo está adecuadamente protegido durante el ciclo completo de codificación? |  |  | El desarrollo está parcialmente asegurado por el tercerizado, y se cuenta con control de cambios. No obstante, el entorno no está protegido durante todo el ciclo de desarrollo. Se sugiere implementar entornos aislados y controlados, junto con políticas claras de codificación segura y pruebas de seguridad desde etapas tempranas. | 70% | Parcialmente |
| 85 | 8.26 | Requisitos de seguridad en aplicaciones |  |  | Los requerimientos de seguridad deben estar claramente definidos y aprobados al desarrollar o adquirir un nuevo sistema. | ¿Los requerimientos de seguridad de las aplicaciones se encuentran claramente definidos antes de iniciar el proceso de desarrollo o adquisición de alguna aplicación? |  |  | Los requerimientos de seguridad están claramente definidos antes del desarrollo o adquisición, lo cual demuestra una buena práctica. Formalizan un checklist de validación de seguridad para cada nuevo sistema adquirido o desarrollado. | 100% | Sí |
| 86 | 8.27 | Arquitectura y principios de ingeniería de sistemas seguros |  |  | Principios de ingeniería sistemas seguros deben ser establecidas, documentadas, mantenidas y aplicadas en toda actividad de desarrollo de sistemas. | ¿Se han establecido, documentados, mantenidos y aplicado procedimientos sobre cómo implementar medidas de seguridad en las técnicas de desarrollo? Así por ejemplo:  - Procedimientos seguros para el diseño y codificación (elaboración de código seguro)  - Procesos de diseño de mecanismos de autenticación difíciles vulnerar  - Procesos de estandarización de variables  - Procedimientos para el uso correcto de la criptografía, etc.. |  |  | Actualmente no se han establecido ni documentado principios de ingeniería segura, lo que representa una grave omisión. Se debe tenerr un marco mínimo que contemple diseño seguro y autenticación robusta si se desarrollan sistemas personalizados. | 0% | No |
| 87 | 8.28 | Codificación Segura |  |  | Principios de codificación segura deben ser aplicados al desarrollo de software | ¿Se han definido principios de codificación segura para el desarrollo de sistemas y procesos de cambio en los sistemas existentes? Es decir, conjuntos de reglas y pautas para reducir las vulnerabilidades y errores de seguridad durante el desarrollo |  |  | La empresa depende de las pautas del proveedor del nuevo ERP y no posee principios propios de codificación segura. Esto limita el control interno sobre la calidad del software. | 50% | Parcialmente |
| 88 | 8.29 | Pruebas de seguridad en el desarrollo y aceptación |  |  | Se debe implementar procesos de pruebas de seguridad en el ciclo de vida del desarrollo de los sistemas de información. | ¿Se prueban las funcionalidades de seguridad durante el desarrollo?  ¿Se programan pruebas de aceptación para sistemas nuevos o actualizados? |  |  | El proceso de pruebas de seguridad está implementado a través del proveedor, quien también programa las pruebas de aceptación. Se definen los criterios de aceptación y participan activamente en las pruebas, especialmente para funcionalidades críticas. | 100% | Sí |
| 89 | 8.30 | Desarrollo subcontratado |  |  | La organización debe dirigir, monitorear y revisar las actividades relativas al desarrollo de software tercerizado. | ¿El desarrollo de software realizado en outsourcing, está siendo supervisado y monitoreado por la organización? |  |  | El desarrollo tercerizado está supervisado por el área de TI, lo que garantiza el cumplimiento. Se mantienen registros formales de revisiones, hitos y entregables, así como la aplicación de penalidades contractuales ante incumplimientos de seguridad. | 100% | Sí |
| 90 | 8.31 | Separación de los entornos de desarrollo, prueba y producción |  |  | Los entornos de desarrollo, pruebas y producción deben encontrarse adecuadamente separados y asegurados. | ¿Los entornos de desarrollo, producción y pruebas están separadas para reducir los riesgos de accesos o cambios en los sistemas operativos no autorizados?  ¿ El acceso a cada uno de estos entornos es adecuadamente controlado? |  |  | Los entornos de desarrollo, prueba y producción están correctamente separados y controlados. Se implementó un monitoreo específico en los accesos a cada entorno y se estableció bitácoras de cambios. | 100% | Sí |
| 91 | 8.32 | Gestión del cambio |  |  | Se debe contar con procedimientos formales para la gestión de los cambios en infraestructura de procesamiento de datos, sistemas operativos y aplicaciones | ¿Se controlan los cambios a la infraestructura, sistemas operativos y aplicaciones?  ¿Se cuenta con procedimientos formales para el control de estos cambios? |  |  | Los cambios están gestionados por procedimientos formales bajo responsabilidad del ingeniero de TI. Se incorporó un análisis de impacto de seguridad previo a cada modificación significativa en los sistemas o infraestructura. | 100% | Sí |
| 92 | 8.33 | Información de prueba |  |  | La información o datos para las pruebas deben ser adecuadamente seleccionados, protegidos y gestionados. | ¿Los datos de prueba del sistema están seleccionados cuidadosamente, protegidos y controlados? |  |  | Todos los datos que posee el área de TI, contractualmente deben estar protegidos y controlados. | 100% | Sí |
| 93 | 8.34 | Protección de sistemas de información durante pruebas de auditoría |  |  | Se debe planificar y gestionar adecuadamente las pruebas de auditoría realizadas sobre los sistemas a fin de reducir el riesgo de afectar su operatividad. | ¿Los requerimientos y las actividades de auditoría sobre los sistemas, que involucran revisiones, son cuidadosamente planeados y acordados para minimizar el riesgo de impactar a los procesos del negocio? |  |  | Las auditorías son cuidadosamente planificadas y ejecutadas, lo que mitiga los riesgos operativos. Se deja evidencia documental de cada revisión y se asegura que los entornos auditados hayan sido restaurados a su estado previo, si fue alterado. | 100% | Sí |

# **Capítulo 4: Análisis de las causas de la inefectividad de los controles**

| **Código** | **Nombre de Control** | **Porcentaje de Cumplimiento** | **¿Cumple?** | **Análisis de las causas de la inefectividad** |
| --- | --- | --- | --- | --- |
| **5. Controles organizacionales** | | | | |
| 5.01 | Políticas para la seguridad de la información | 0% | No | No hay una regla escrita sobre cómo cuidar la información; tampoco se sabe lo vital que es en la empresa. |
| 5.02 | Roles y responsabilidades en seguridad de la información | 50% | Parcialmente | No tenemos quien se encargue de dar seguridad a los datos, sobre todo si lo hace una compañía externa. |
| 5.03 | Segregación de funciones | 50% | Parcialmente | Falla en separar las tareas, algunas importantes las hace un solo individuo. |
| 5.04 | Responsabilidades de gestión | 50% | Parcialmente | No están claramente definidos los responsables de la gestión de seguridad dentro de la organización. |
| 5.05 | Contacto con autoridades | 50% | Parcialmente | No se ha puest͏o a nadie ͏en ͏carg͏o de hab͏lar y planear con jefes en te͏mas de seguridad. |
| 5.06 | Contacto con grupos de interés especial | 50% | Parcialmente | No hay modo͏s clar͏os para c͏on͏ectar ͏con ͏grupos q͏ue les importa mucho la seguridad digital. |
| 5.07 | Inteligencia de amenazas | 50% | Parcialmente | No͏ existen forma͏s oficiales ͏para͏ notar y ͏actuar a͏ntepeligros nuevos. |
| 5.08 | Seguridad de la información en la gestión de proyectos | 50% | Parcialmente | No se incluye la segu͏ri͏dad de datos en el manejo de proyectos d͏esde q͏ue ͏se͏ planea. |
| 5.09 | Inventario de información y otros activos asociados | 50% | Parcialmente | El inventario de activos no está actualizado ni formalizado, lo que limita la gestión efectiva de los mismos. |
| 5.10 | Uso aceptable de la información y otros activos asociados | 50% | Parcialmente | No hay ͏un documen͏to de reglas claras sobre el uso adecuado de la información que se comunica a cada empleado. |
| 5.11 | Devolución de activos | 50% | Parcialmente | No existen͏ pasos f͏áciles ͏para ͏dar͏ atrás los bie͏nes cu͏ando un trabajador ͏se va de la empre͏sa. |
| 5.12 | Clasificación de la información | 60% | Parcialmente | Hay un método simple para organizar la información, pero no es total ni sabe todo el mundo. |
| 5.13 | Etiquetado de la información | 70% | Parcialmente | El nombrar información se ha͏ce a medias, por falta de enseñ͏anza y recursos para usarlo bien. |
| 5.14 | Transferencia de la información | 70% | Parcialmente | N͏o͏ hay reglas e͏scritas para as͏egurar que la información se mueva segura ͏entre lugares o con otros. |
| 5.15 | Control de acceso | 60% | Parcialmente | Los controles para entrar están un poco puestos, pero no cu͏bren todos los sistemas, ni están en papel. |
| 5.16 | Gestión de identidad | 70% | Parcialmente | Manejar qu͏ién pued͏e usar qué no tiene maneras fuertes͏; no hay au͏tomatizado ni seguimiento bueno. |
| 5.17 | Información de autenticación | 80% | Sí | Correctamente implementado; los derechos de acceso están bien definidos y controlados. |
| 5.18 | Derechos de acceso | 80% | Sí | Correctamente implementado; existen cláusulas y controles para la seguridad en la relación con proveedores. |
| 5.19 | Seguridad de la información en las relaciones con los proveedores | 80% | Sí | Correctamente implementado; existen cláusulas y controles para la seguridad en la relación con proveedores. |
| 5.20 | Directrices de seguridad de la información en los acuerdos con proveedores | 90% | Sí | Cumple con cláusulas de confidencialidad, gestión de relaciones, incluyendo riesgos en las relaciones con otros proveedores.. |
| 5.21 | Gestión de la seguridad de la información en la cadena de suministro de TIC | 40% | No | No existe un plan contingente para ese tipo de situaciones(validar que el equipo o software cumplan con los requerimientos de la empresa), este hecho le ha generado problemas. |
| 5.22 | Seguimiento, revisión y gestión de cambios de servicios de proveedores | 60% | Parcialmente | No se cuentan con mantenimientos preventivos, sino con mantenimientos correctivos en su mayoría. |
| 5.23 | Seguridad de la información para el uso de servicios en la nube | 60% | Parcialmente | No se cuenta con una política sobre el uso de servicios en la nube, ni tampoco un proceso de adquisición o gestión de los servicios en la nube. |
| 5.24 | Planificación y preparación de la gestión de incidentes de seguridad de la información | 60% | Parcialmente | Los monitoreos no son tan seguidos, mayormente después de un incidente. |
| 5.25 | Evaluación y decisión sobre los eventos de seguridad de información | 60% | Parcialmente | No se presencia una escala de clasificación. |
| 5.26 | Respuesta a incidentes de seguridad de la información | 70% | Parcialmente | Todos los meses se graban en discos duros la información. |
| 5.27 | Aprendizaje de los incidentes de seguridad de la información | 60% | Parcialmente | No se tiene un proceso de evaluación para identificar incidentes fijos. |
| 5.28 | Recopilación de evidencias | 100% | Si | La gerencia se encarga de decidir si emprender un análisis forense según su criterio. |
| 5.29 | Seguridad de la información durante interrupciones | 80% | Si | Si existe un plan de continuidad de negocio. También se cuentan con plazos definidos para restaurar servicios tras una una interrupción. |
| 5.30 | Preparación de las TIC para la continuidad del negocio | 60% | Parcialmente | Cuentan parcialmente con medidas preventivas, capacidades de recuperación y pruebas periódicas para garantizar que la organización pueda responder eficazmente a cualquier evento disruptivo. |
| 5.31 | Identificación de requerimientos legales, estatutarios, regulatorios y contractuales | 100% | Si | Logran identificar, documentar y cumplir con todas las normativas, leyes, regulaciones y obligaciones contractuales aplicables al proyecto o sistema en desarrollo. |
| 5.32 | Derechos de Propiedad Intelectual | 60% | Parcialmente | N͏o͏ hay reglas para as͏egurar el mal uso de los elementos tecnologicos que evite el uso indebido de softwares. |
| 5.33 | Protección de registros | 60% | Parcialmente | No se garantiza cómo se deben gestionar, almacenar y proteger los registros para asegurar su integridad, disponibilidad y confidencialidad. |
| 5.34 | Privacidad y protección de la información de identificación personas (IIP) | 60% | Parcialmente | No está especificada la implementación de medidas para garantizar que los datos personales recopilados, almacenados y procesados por una organización sean tratados de manera segura, ética y conforme a las leyes y regulaciones aplicables. |
| 5.35 | Revisión independiente de la seguridad de información | 100% | Si | Los requisitos de autoría de sistemas si son planificados y controlados para la minimización de riesgos. |
| 5.36 | Cumplimiento con políticas y estándares de seguridad de información | 0% | No | No se realiza una verificación del cumplimiento de las políticas y estándares ni escaneo de vulnerabilidad de red de la seguridad de información. |
| 5.37 | Procedimientos operativos documentados | 70% | Parcialmente | No se tienen procedimientos documentados para las operaciones de TI. |

| **Código** | **Nombre de Control** | **Porcentaje de Cumplimiento** | **¿Cumple?** | **Análisis de las causas de la inefectividad** |
| --- | --- | --- | --- | --- |
| **6.Controles de personas** | | | | |
| 6.01 | Investigación de antecedentes | 100% | Si | El área de recursos humanos se encarga correctamente de la verificación de antecedentes de empleados contratados. |
| 6.02 | Términos y condiciones del empleo | 90% | Si | Los proveedores no firman ningún tipo de acuerdo de confidencialidad, pero los empleados si. |
| 6.03 | Concientización, educación y entrenamiento en seguridad de la información | 0% | No | * No se ha acordado una asesoría hacia los empleados por términos de seguridad de información * La falta de concientización puede causar un gran riesgo respecto a la vulnerabilidad de la información |
| 6.04 | Procesos disciplinarios | 70% | Parcialmente | * Existe reglamento para que los empleados puedan también guiarse respecto a estos temas |
| 6.05 | Revisión de accesos después de desvinculación | 60% | Parcialmente | * El proceso de revocación de accesos tras la baja de un empleado no es inmediato y depende de una comunicación manual entre RR. HH. y el área de TI. * El retraso en la desactivación de cuentas crea una ventana de riesgo donde un ex empleado podría acceder a los sistemas. |
| 6.06 | Control sobre contratistas y terceros | 40% | Parcialmente | * Si bien existe un contrato con el proveedor principal de TI, no hay un proceso general para evaluar o gestionar los riesgos de seguridad asociados a otros contratistas o terceros * No se supervisa el acceso o las actividades de personal externo que pueda tener acceso a las instalaciones o a la red |
| 6.07 | Teletrabajo | 0% | No | No existe una política formal para el teletrabajo. El personal trabaja remotamente sin lineamientos ni controles de seguridad definidos. |
| 6.08 | Reporte de eventos de seguridad de la información | 70% | Parcialmente | Aunque hay un canal informal para reportar incidentes (correo o comunicación directa a TI), no existe un procedimiento formal ni seguimiento documentado. |

| **Código** | **Nombre de Control** | **Porcentaje de Cumplimiento** | **¿Cumple?** | **Análisis de las causas de la inefectividad** |
| --- | --- | --- | --- | --- |
| **7. Controles Técnicos** | | | | |
| 7.01 | Perímetro de seguridad física | 100% | Si | * Si se cumple con los perímetros de seguridad física designada para su área de servidores. |
| 7.02 | Controles de entrada física | 0% | No | * El área de seguridad no dispone de un control de seguridad óptimo en sus instalaciones. |
| 7.03 | Seguridad de oficinas, despachos y recursos | 0% | No | * Las instalaciones en su totalidad no han sido diseñadas ni configuradas teniendo en cuenta la seguridad. |
| 7.04 | Supervisión de la seguridad física | 100% | Si | * Son monitoreados con una cámara interna de la empresa |
| 7.05 | Protección contra las amenazas físicas y ambientales | 50% | Parcialmente | Hay medidas básicas, pero no se han implementado controles preventivos avanzados. Se actúa de forma reactiva. |
| 7.06 | Trabajar en áreas seguras | 70% | Parcialmente | Aunque existen áreas seguras, no se monitorean ni actualizan sus políticas. No hay verificación periódica. |
| 7.07 | Escritorio limpio y pantalla limpia | 0% | No | No hay políticas definidas ni controles aplicados. Riesgo alto de exposición de información por descuido. |
| 7.08 | Ubicación y protección del equipamiento | 50% | Parcialmente | No se considera el riesgo de acceso no autorizado. El entorno físico del equipo no está bien protegido. |
| 7.09 | Seguridad de los activos fuera de las instalaciones | 60% | Parcialmente | No se ha documentado una política. El control depende de prácticas informales del proveedor de TI. |
| 7.10 | Medios de almacenamiento | 70% | Parcialmente | No hay políticas socializadas ni procesos claros para la eliminación segura de medios removibles. |
| 7.11 | Utilidades de apoyo | 100% | Sí | Se realizan pruebas periódicas y existe respaldo eléctrico adecuado. Este control es eficaz. |
| 7.12 | Seguridad del cableado | 100% | Sí | Las evaluaciones de riesgo y la infraestructura del cableado están correctamente implementadas. |
| 7.13 | Mantenimiento de equipos | 0% | No | No se lleva una programación ni control de mantenimiento. Riesgo de fallas técnicas inesperadas. |
| 7.14 | Eliminación segura o reutilización de equipos | 0% | No | No existe una política o procedimiento para borrar datos antes de eliminar o reutilizar equipos. |

| **Código** | **Nombre de Control** | **Porcentaje de Cumplimiento** | **¿Cumple?** | **Análisis de las causas de la inefectividad** |
| --- | --- | --- | --- | --- |
| **8. Controles Tecnológicos** | | | | |
| 8.01 | Dispositivos de punto final del usuario | 50% | Parcialmente | No hay reglas escritas para ciudad computadoras y celulares. El control depende sólo del área de TI. |
| 8.02 | Derechos de acceso privilegiado | 100% | Sí | Este control se cumple porque el área de TI (tercerizada) administra correctamente los accesos especiales. |
| 8.03 | Restricción del acceso a la información | 100% | Sí | El control está bien aplicado y restringe el acceso según políticas. |
| 8.04 | Acceso al código fuente | 80% | Sí | El equipo de TI protege el código fuente, pero no hay detalle documentado del proceso o herramientas usadas. |
| 8.05 | Autenticación segura | 70% | Parcialmente | Se usa autenticador de Microsoft, pero no hay MFA ni políticas claras para todos los accesos sensibles. |
| 8.06 | Gestión de la capacidad | 70% | Parcialmente | Se actúa solo cuando el sistema ya reporta una saturación, basándose en notificaciones informales en lugar de utilizar herramientas de monitoreo proactivo. |
| 8.07 | Protección contra malware | 50% | Parcialmente | La protección se limita a tener una licencia de antivirus, pero no se realiza una detección proactiva. |
| 8.08 | Gestión de vulnerabilidades técnicas | 60% | Parcialmente | No se realizan escaneos periódicos de vulnerabilidades ni revisiones de cumplimiento técnico. Ausencia de una estrategia sistemática |
| 8.09 | Gestión de la configuración | 70% | Parcialmente | Falta de verificación y auditoría periódica. Si bien existen documentación y plantillas de configuración, no se realizan revisiones para validar que dichas configuraciones se apliquen correctamente |
| 8.10 | Eliminación de la información | 100% | Sí | El procedimiento está correctamente implementado y a cargo del proveedor de TI, quien mantiene un registro formal y actúa conforme a las cláusulas contractuales |
| 8.11 | Enmascaramiento de datos | 80% | Sí | Este control es mayormente efectivo. La leve inefectividad se debe a que no se detalla si las técnicas de enmascaramiento se aplican de forma automática o manual, ni si cubren todos los entornos necesarios (producción, pruebas, etc.) |
| 8.12 | Prevención de la fuga de datos | 60% | Parcialmente | Se depende de controles básicos de clasificación, pero no se han implementado herramientas específicas de Prevención de Pérdida de Datos (DLP) para una detección proactiva |
| 8.13 | Copias de seguridad de la información | 100% | Sí | El control es ejecutado correctamente por el proveedor de TI, cumpliendo con las políticas y realizando pruebas |
| 8.14 | Redundancia de las instalaciones de procesamiento de información | 100% | Sí | No se identifican causas de inefectividad, ya que la redundancia está garantizada en la infraestructura crítica |
| 8.15 | Gestión de eventos (Log) | 60% | Parcialmente | La revisión de los registros no es sistemática ni frecuente. La empresa actúa de forma reactiva solo después de los incidentes, lo que limita su capacidad para detectar amenazas de manera temprana |
| 8.16 | Actividades de seguimiento | 100% | Sí | El sistema de monitoreo cumple con sus objetivos de supervisión del tráfico y comportamiento anómalo. |
| 8.17 | Sincronización del reloj | 100% | Sí | No se identifican causas de inefectividad, ya que todos los relojes del sistema están correctamente sincronizados. |
| 8.18 | Uso de programas de utilidad privilegiados | 90% | Sí | Este control es altamente efectivo. La única causa de una posible inefectividad menor es la falta de un procedimiento formal documentado que registre el acceso y uso de estas herramientas |
| 8.19 | Instalación de software en sistemas operacionales | 90% | Sí | Es un control efectivo. La debilidad potencial es la ausencia de controles complementarios. Se recomienda implementar una lista blanca (whitelisting) de aplicaciones permitidas y aprobadas por el equipo de TI. |
| 8.20 | Controles de red | 100% | Sí | El control es efectivo, pero su eficacia a largo plazo podría verse reducida por la falta de documentación y auditorías regulares |
| 8.21 | Seguridad de los servicios de red | 100% | Sí | No se identifican causas de inefectividad en este control, ya que los acuerdos con proveedores sí contemplan los elementos clave. Sin embargo, debe mantenerse una supervisión continua para asegurar que los servicios se actualicen conforme a nuevos riesgos. |
| 8.22 | Segregación en redes | 100% | Sí | El control está correctamente aplicado, sin embargo, su efectividad puede verse reducida si no se actualiza el mapa de red ante cambios en la infraestructura o nuevos servicios. La ausencia de revisión continua puede provocar desalineación entre diseño y realidad operativa. |
| 8.23 | Filtrado Web | 0% | No | La inexistencia de controles de filtrado web responde a una falta de conciencia del riesgo asociado al uso libre de Internet en entornos operativos. Tampoco se ha priorizado este control en las políticas o requerimientos exigidos al proveedor de TI. |
| 8.24 | Uso de Criptografía | 100% | Sí | No hay fallas aparentes en este control, aunque su efectividad puede verse afectada si los responsables no realizan revisiones periódicas de algoritmos o no gestionan adecuadamente el ciclo de vida de las llaves criptográficas. |
| 8.25 | Ciclo de vida de desarrollo seguro | 70% | Parcialmente | La inefectividad surge por la falta de control de la empresa sobre el entorno de desarrollo, que está a cargo de un tercero. Al no tener supervisión completa, se generan brechas durante las etapas más tempranas del ciclo. |
| 8.26 | Requisitos de seguridad en aplicaciones | 100% | Sí | No se identifican fallas estructurales en este control, pero si los requerimientos definidos no se revisan ni actualizan frente a cambios tecnológicos, su utilidad podría disminuir con el tiempo. |
| 8.27 | Arquitectura y principios de ingeniería de sistemas seguros | 0% | No | La causa principal de inefectividad es la inexistencia total de documentación técnica o lineamientos propios. Esto se debe a una dependencia absoluta del proveedor y a la falta de capacidades internas en desarrollo seguro. |
| 8.28 | Codificación Segura | 50% | Parcialmente | El control no es eficaz porque la empresa no posee lineamientos propios ni evalúa la calidad del código entregado por terceros. La falta de verificación independiente impide garantizar seguridad en el código fuente. |
| 8.29 | Pruebas de seguridad en el desarrollo y aceptación | 100% | Sí | El control funciona correctamente, aunque su efectividad depende de la colaboración activa entre empresa y proveedor durante las validaciones de seguridad. |
| 8.30 | Desarrollo subcontratado | 100% | Sí | No se identifican causas directas de inefectividad. La organización ha asumido un rol de supervisión adecuado mediante cláusulas contractuales y seguimiento activo. |
| 8.31 | Separación de los entornos de desarrollo, prueba y producción | 100% | Sí | Aunque el control es efectivo, se debe vigilar que no se relajen las medidas de acceso entre entornos con el paso del tiempo o por presiones operativas. |
| 8.32 | Gestión del cambio | 100% | Sí | La gestión de cambios se realiza formalmente, pero su efectividad depende de que todos los cambios, por pequeños que sean, pasen por el mismo proceso. Saltar las validaciones puede comprometer la seguridad. |
| 8.33 | Información de prueba | 100% | Sí | No se identifican causas de inefectividad en este control, ya que los acuerdos con proveedores sí contemplan los elementos clave. Sin embargo, debe mantenerse una supervisión continua para asegurar que los servicios se actualicen conforme a nuevos riesgos. |
| 8.34 | Protección de sistemas de información durante pruebas de auditoría | 100% | Sí | El control está correctamente aplicado, sin embargo, su efectividad puede verse reducida si no se actualiza el mapa de red ante cambios en la infraestructura o nuevos servicios. La ausencia de revisión continua puede provocar desalineación entre diseño y realidad operativa. |

# 

# **Capítulo 5: Medidas propuestas para cubrir las brechas de seguridad**

El presente capítulo tiene como objetivo detallar las medidas propuestas para abordar las brechas de seguridad identificadas en el Capítulo 4. Cada medida está diseñada para mitigar las causas subyacentes de las ineficiencias, mejorar el cumplimiento de las políticas de seguridad, y garantizar la confidencialidad, integridad y disponibilidad de la información.

5.1.1 Fortalecimiento del control de acceso físico

Responsable: Área de TI (Tercerizado)

Tiempo estimado: 2 meses

Medidas:

* Implementar sistemas de control de acceso físico como tarjetas magnéticas, biometría o códigos de acceso para zonas críticas.
* Realizar auditorías trimestrales sobre el uso de accesos físicos y mantener registros detallados de ingresos y salidas.
* Instalar cámaras de vigilancia en puntos estratégicos, asegurando que todas las áreas sensibles estén monitoreadas 24/7.
* Capacitar al personal sobre la importancia de restringir el acceso físico a áreas no autorizadas y reportar incidentes sospechosos.

5.1.2 Supervisión y control de visitantes

Responsable: Seguridad

Tiempo estimado: 1 mes

* Establecer un registro digital de visitas, con identificación obligatoria y emisión de credenciales temporales.
* Asignar personal encargado de acompañar a los visitantes en las áreas restringidas.

5.2.2 Fortalecimiento de los roles y responsabilidades

Responsable: RRHH y Gerencia

Tiempo estimado: 1 meses

* Definir claramente los roles y responsabilidades en seguridad de la información, tanto para personal interno como proveedores.
* Asignar a un Responsable de Seguridad de la Información (RSI) que supervise el cumplimiento y las auditorías internas.
* Realizar sesiones de inducción y refuerzo sobre los roles específicos vinculados a la seguridad.

5.2.3 Gestión de activos de información

Responsable: Área de TI (Tercerizado)

Tiempo estimado: 2 meses

* Crear y mantener un inventario digitalizado de activos, que incluya hardware, software, bases de datos e información crítica.
* Clasificar los activos según su nivel de criticidad y sensibilidad.

5.2.4 Implementación de seguridad en los proyectos

Responsable: Área de TI (Tercerizado)

Tiempo estimado: 2 meses

* Incluir revisiones de seguridad desde las etapas iniciales de los proyectos tecnológicos y de infraestructura.
* Aplicar herramientas de análisis de riesgos durante la fase de diseño y desarrollo.
* Documentar las lecciones aprendidas al finalizar cada proyecto e incorporarlas en los procedimientos internos.

5.3.1 Medida: Crear un Programa de Concientización en Seguridad

Responsable: RRHH

Tiempo estimado: 1 mes

* Implementar un programa de capacitación continua y accesible para todo el personal.
* Realizar una charla de capacitación anual obligatoria enfocada en reconocer correos de *phishing* y en la importancia de no compartir contraseñas.
* Crear y distribuir una guía simple de una página con las reglas de seguridad más importantes (ej. bloquear el equipo al ausentarse, reportar equipos perdidos).

5.3.2 Medida: Fortalecer el Proceso de Desvinculación de Personal

Responsable: Área de TI (Tercerizado) y RRHH

Tiempo estimado: 1 mes

* Automatizar y formalizar la revocación de accesos.
* Implementar un *checklist* obligatorio que RR. HH. debe enviar al proveedor de TI inmediatamente después de confirmarse una baja, asegurando la desactivación de todas las cuentas (correo, sistemas) en un plazo no mayor a 24 horas

# 5.4.1 Medida: Fortalecer la Estrategia de Copias de Seguridad

Responsable: Área de TI (Tercerizado)

Tiempo estimado: 2 meses

# Garantizar la recuperabilidad de la información ante un desastre.

# Exigir en el contrato con el proveedor de TI la realización de pruebas de restauración semestrales, con un informe de resultados.

# Utilizar el almacenamiento de OneDrive o SharePoint (incluido en Microsoft 365) para guardar una segunda copia de la información más crítica.

# 5.4.2 Medida: Iniciar una Gestión Básica de Vulnerabilidades

Responsable: Área de TI (Tercerizado)

Tiempo estimado: 2 meses

# Identificar y corregir de forma proactiva las debilidades técnicas.

# Contratar un escaneo de vulnerabilidades externo anual para la infraestructura expuesta a internet.

# Solicitar al proveedor de TI un plan de aplicación de parches de seguridad críticos para servidores, con un plazo máximo de 30 días desde su publicación.

# 5.4.3 Medida: Mejorar la Seguridad de la Red

Responsable: Área de TI (Tercerizado)

Tiempo estimado: 2 meses

# Segmentar la red para contener posibles incidentes.

# Planificar la creación de una red separada para las cajas y surtidores (red transaccional), aislándola de la red administrativa general (oficinas).

# Realizar una auditoría anual de las reglas del firewall para eliminar reglas obsoletas o demasiado permisivas.

5.05 Contacto con autoridades

Responsable: Gerencia

Tiempo estimado: 2 meses

Medida: Fortalecer la relación y coordinación con entidades reguladoras y de supervisión.

* Establecer canales claros de comunicación con las autoridades
* Designar un responsable dentro de la organización como punto de contacto principal con las autoridades reguladoras.
* Realizar una evaluación anual del nivel de cumplimiento regulatorio mediante auditorías internas o externas certificadas.

5.06 Contacto con grupos de interés especial

Responsable: Gerencia

Tiempo estimado: 1 meses

Medida: Fortalecer la relación y comunicación con los grupos de interés especial para garantizar su participación activa y mitigar posibles conflictos o malentendidos.

* Identificar a los grupos de interés especial relevantes para el proyecto antes de su inicio.
* Planificar reuniones periódicas con estos grupos para recopilar retroalimentación, resolver inquietudes y mantenerlos informados sobre el progreso del proyecto.

5.07 Inteligencia de amenazas

Responsable: Área de TI (Tercerizado)

Tiempo estimado: 2 meses

* Establecer un equipo dedicado a la recolección, análisis y respuesta a datos relacionados con amenazas potenciales.
* Implementar herramientas de monitoreo en tiempo real (como SIEM - Security Information and Event Management) para recopilar información sobre actividades anómalas en sistemas y redes.
* Suscribirse a fuentes externas de inteligencia de amenazas (por ejemplo, feeds de ciberseguridad, informes de organismos reguladores como OSINERGMIN) para mantenerse actualizado sobre vulnerabilidades conocidas y nuevas tácticas utilizadas por actores maliciosos.

5.08 Seguridad de la información en la gestión de proyectos

Responsable: Área de TI (Tercerizado)

Tiempo estimado: 1 meses

* Integrar requisitos de seguridad de la información en el plan de gestión del proyecto desde su inicio.
* Realizar evaluaciones de riesgos de seguridad al inicio de cada fase del proyecto y actualizarlas según sea necesario.
* Implementar políticas de acceso controlado a la información crítica del proyecto, asegurando que solo el personal autorizado tenga acceso.

5.09 Inventario de información y otros activos asociados

Responsable: Área de TI (Tercerizado)

Tiempo estimado: 2 meses

* Identificar y clasificar todos los activos de información y recursos asociados, como documentos técnicos, bases de datos, código fuente, licencias de software y hardware.
* Asignar un propietario responsable para cada activo registrado, asegurando que haya claridad sobre quién gestiona y protege cada recurso.
* Implementar herramientas automatizadas para realizar un seguimiento continuo de los activos y detectar cualquier cambio no autorizado.

5.10 Uso aceptable de la información y otros activos asociados

Responsable: Área de TI (Tercerizado)

Tiempo estimado: 2 meses

* Desarrollar una política de uso aceptable que detalle qué está permitido y qué no está permitido con respecto a los activos del proyecto.
* Capacitar al equipo del proyecto sobre las reglas de uso aceptable y las consecuencias de violar estas políticas.
* Implementar herramientas de monitoreo para detectar actividades inapropiadas, como el acceso no autorizado a datos o el uso indebido de recursos tecnológicos.

5.11 Devolución de activos

Responsable: Área TI (tercerizado)

Tiempo estimado: 1 mes

* Crear un formulario estandarizado para registrar la devolución de activos, incluyendo detalles como el tipo de activo, su estado físico y la fecha de devolución.
* Asignar un responsable (por ejemplo, el jefe inmediato o el departamento de recursos humanos) para supervisar el proceso de devolución.
* Realizar inspecciones físicas de los activos devueltos para verificar su estado y detectar posibles daños o pérdidas.

5.12 Clasificación de la información

Responsable: Área TI (tercerizado)

Tiempo estimado: 2 mes

* Definir categorías de clasificación (por ejemplo, público, interno, confidencial, restringido) y establecer criterios claros para cada categoría.
* Capacitar al personal sobre cómo manejar la información según su clasificación y las consecuencias de violar estas políticas.
* Implementar herramientas tecnológicas para automatizar la clasificación y protección de datos, como etiquetado automático o cifrado basado en niveles de sensibilidad.

5.13 Etiquetado de la información

Responsable: Área TI (tercerizado)

Tiempo estimado: 1 mes

* Definir un estándar de etiquetado que incluya marcas visibles (como encabezados o pies de página) y metadatos digitales para documentos electrónicos.
* Capacitar al personal sobre cómo aplicar correctamente las etiquetas a los documentos, correos electrónicos y sistemas.
* Implementar herramientas automatizadas para etiquetar la información en sistemas digitales, como correo electrónico, bases de datos y plataformas de gestión documental.

5.14 Transferencia de la información

Responsable: Área TI (tercerizado)

Tiempo estimado: 1 mes

* Utilizar protocolos seguros de transferencia de datos, como HTTPS , SFTP o TLS , para proteger la información durante su transmisión.
* Implementar herramientas de cifrado para garantizar que los datos sean inaccesibles en caso de interceptación no autorizada.
* Documentar procedimientos claros para la transferencia de información crítica, incluyendo roles y responsabilidades de quienes participan en el proceso.

5.30 Preparación de las TIC para la continuidad del negocio

Responsable: Responsable de Seguridad de la Información

Tiempo estimado: 3 meses

Medidas:

* Elaborar e implementar un Plan de Continuidad del Negocio (BCP) enfocado en TIC.
* Establecer los parámetros RTO y RPO para sistemas críticos.
* Realizar pruebas semestrales de recuperación ante desastres.
* Incluir procedimientos para respaldo de información, restauración y roles de emergencia.

5.31 Identificación de requerimientos legales, estatutarios, regulatorios y contractuales

Responsable: Responsable Legal y Responsable de Seguridad de la Información

Tiempo estimado: 2 meses

Medidas:

* Crear una matriz legal que incluya requisitos regulatorios, contractuales y legales aplicables.
* Asignar un responsable para mantener y actualizar esta matriz.
* Elaborar una política de cumplimiento normativo vinculada al SGSI.

5.32 Derechos de Propiedad Intelectual

Responsable: Responsable Legal y Responsable de Seguridad de la Información

Tiempo estimado: 2 meses

Medidas:

* Desarrollar una política sobre propiedad intelectual y licenciamiento de software.
* Implementar controles para verificar el uso legal de software y activos digitales.
* Capacitar al personal sobre el uso adecuado de contenido licenciado.

5.33 Protección de registros

Responsable: Gestor de Seguridad Tecnológica y Responsable de Seguridad de la Información

Tiempo estimado: 3 meses

Medidas:

* Establecer una política de retención, clasificación y destrucción de registros.
* Implementar mecanismos de verificación de integridad y almacenamiento seguro.
* Establecer procedimientos para eliminación segura tanto en nube como en dispositivos locales.

5.34 Privacidad y protección de la IIP

Responsable: Responsable de Protección de Datos Personales y Responsable de Seguridad de la Información

Tiempo estimado: 2 meses

Medidas:

* Crear e implementar una política de privacidad de datos personales.
* Establecer controles de acceso y roles sobre los datos IIP.
* Capacitar al personal sobre el manejo adecuado de información personal.

5.35 Revisión independiente de la seguridad de la información

Responsable: Gestor de Auditoría y Responsable de Seguridad de la Información

Tiempo estimado: 1 mes

Medidas:

* Planificar auditorías anuales del SGSI con alcance definido por la alta dirección.
* Documentar hallazgos, acciones correctivas y evidencias de cumplimiento.
* Controlar el acceso a herramientas y registros de auditoría.

6.03 Concientización, educación y entrenamiento en seguridad

Responsable: Recursos Humanos y Seguridad de la Información

Tiempo estimado: 2 meses

Medidas:

* Diseñar un programa anual de capacitación en seguridad para todos los empleados.
* Realizar sesiones trimestrales por área enfocadas en amenazas reales y simulaciones.
* Incluir capacitación obligatoria al ingresar a la empresa.

6.04 Proceso disciplinario

Responsable: Recursos Humanos y Legal

Tiempo estimado: 1 mes

Medidas:

* Fortalecer el reglamento interno incluyendo faltas graves por incumplimiento de políticas de seguridad.
* Comunicarlo de forma clara a todos los empleados y en sesiones de onboarding.

6.07 Teletrabajo

Responsable: Recursos Humanos

Tiempo estimado: 1 mes

Medidas:

* Desarrollar e implementar una política formal de teletrabajo que contemple seguridad y acceso remoto.
* Comunicar la política a todo el personal y verificar cumplimiento periódicamente.

6.08 Reporte de eventos de seguridad

Responsable: Recursos Humanos y Seguridad de la Información

Tiempo estimado: 1 mes

Medidas:

* Establecer un canal formal y anónimo para el reporte de incidentes y vulnerabilidades.
* Capacitar al personal para reconocer eventos sospechosos y saber cómo reportarlos.
* Implementar registros y seguimiento a cada reporte realizado.

7.02 Controles de entrada física

Responsable: Seguridad Física

Tiempo estimado: 2 meses

Medidas:

* Instalar sistemas de acceso electrónico o biométrico en zonas sensibles.
* Separar físicamente las zonas de carga y descarga para evitar accesos no autorizados.
* Registrar todos los ingresos y egresos en oficinas seguras.

7.03 Seguridad de oficinas, despachos y recursos

Responsable: Seguridad Física

Tiempo estimado: 2 meses

Medidas:

* Rediseñar los espacios físicos para incorporar elementos de seguridad como cerraduras, control de acceso y señalética.
* Evaluar la ubicación de escritorios, puertas, ventanas y archivos para minimizar el riesgo de acceso no autorizado.
* Incluir la seguridad física como parte del onboarding al personal nuevo.

7.04 Supervisión de la seguridad física

Responsable: TI- infraestructura, Seguridad de la información

Tiempo estimado: 2 meses

Medidas:

* Establecer un procedimiento documentado para la revisión periódica de las grabaciones de las cámaras de seguridad.
* Implementar un registro de mantenimiento para asegurar que el sistema de cámaras internas funcione correctamente en todo momento.
* Realizar pruebas periódicas para verificar la cobertura y calidad de la vigilancia.

7.05 Protección contra las amenazas físicas y ambientales

Responsable: TI- infraestructura, Seguridad de la información

Tiempo estimado: 2 meses

Medidas:

* Realizar un análisis de riesgos formal para identificar y evaluar amenazas físicas y ambientales (terremotos, inundaciones, incendios, etc.).
* Diseñar e implementar medidas de protección preventivas en lugar de solo reaccionar a los incidentes.
* Establecer un plan formal de respuesta para desastres naturales o ataques maliciosos.

7.06 Trabajar en áreas seguras

Responsable: TI- infraestructura, Seguridad de la información

Tiempo estimado: 2 meses

Medidas:

* Implementar un proceso de monitoreo continuo para verificar el cumplimiento de las políticas y procesos en las áreas seguras.
* Realizar auditorías periódicas para asegurar que las medidas de seguridad se mantengan y actualicen.
* Reforzar la capacitación al personal sobre los procedimientos específicos para trabajar en estas áreas.

7.07 Escritorio limpio y pantalla limpia

Responsable: Seguridad de la información

Tiempo estimado: 2 meses

Medidas:

* Crear, documentar e implementar una política formal de "escritorio limpio y pantalla limpia" para documentos físicos y medios de almacenamiento extraíbles.
* Comunicar la política a todo el personal y supervisar periódicamente su cumplimiento para reducir el riesgo de exposición de información por descuido.

7.08 Ubicación y protección del equipamiento

Responsable: TI- infraestructura, Seguridad de la información

Tiempo estimado: 2 meses

Medidas:

* Reevaluar la ubicación física del equipamiento para incluir en el análisis el riesgo de acceso no autorizado por parte de transeúntes o personal no pertinente.
* Implementar controles físicos adicionales (ej. gabinetes con llave, áreas restringidas) para proteger equipos en zonas de paso.

7.09 Seguridad de los activos fuera de las instalaciones

Responsable: TI- infraestructura, Seguridad de la información

Tiempo estimado: 2 meses

Medidas:

* Desarrollar y documentar una política formal que cubra la seguridad de los activos fuera de las instalaciones (ej. laptops, dispositivos móviles).
* Comunicar dicha política a todo el personal relevante para que el control no dependa únicamente de prácticas informales del proveedor de TI.

7.10 Medios de almacenamiento

Responsable: TI- infraestructura, Seguridad de la información

Tiempo estimado: 2 meses

Medidas:

* Documentar formalmente la política interna sobre cómo se deben transportar los medios físicos.
* Crear y formalizar un procedimiento que indique cómo deben ser desechadas de forma segura las unidades de almacenamiento
* Socializar y capacitar a todos los empleados sobre las políticas y procesos referentes al uso, transporte y eliminación de unidades removibles.

7.13 Mantenimiento de equipos

Responsable: TI- infraestructura

Tiempo estimado: 3 meses

Medidas:

* Dado que no existe una programación de mantenimiento (cumplimiento del 0%), es crucial crear y documentar un programa de mantenimiento preventivo para todo el equipamiento.
* Establecer un calendario riguroso y asignar responsabilidades para la ejecución de las tareas de mantenimiento.
* Mantener un registro de todas las actividades de mantenimiento para evitar fallas técnicas inesperadas.

7.14 Eliminación segura o reutilización de equipos

Responsable: TI- infraestructura, Seguridad de la información

Tiempo estimado: 3 meses

Medidas:

* Aunque existen controles técnicos, la principal debilidad es la falta de una política formal. Por lo tanto, se debe desarrollar y comunicar una política para el uso seguro de los dispositivos finales del usuario.
* Esta política debe formalizar los controles técnicos que ya gestiona el área de TI y establecer reglas claras para los usuarios. Fuentes

8.01 Medida: Dispositivos de punto final del usuario  
Responsable: TI- infraestructura,Seguridad de la información   
Tiempo estimado: 2 meses

* Aunque existen controles técnicos, la principal debilidad es la falta de una política formal. Por lo tanto, se debe desarrollar y comunicar una política para el uso seguro de los dispositivos finales del usuario.
* Esta política debe formalizar los controles técnicos que ya gestiona el área de TI y establecer reglas claras para los usuarios.

8.05 Medida: Fortalecer la Autenticación Segura  
Responsable: Área de TI (Tercerizado)  
Tiempo estimado: 2 meses

* Establecer una política formal de autenticación que contemple MFA, requisitos de contraseña y reglas de renovación.
* Implementar autenticación multifactor en los accesos a sistemas críticos y cuentas privilegiadas.

8.06 Medida: Optimizar la Gestión de la Capacidad  
 Responsable: Área de TI (Tercerizado)  
 Tiempo estimado: 1 mes

* Instalar herramientas de monitoreo proactivo con alertas automáticas ante uso elevado de recursos.
* Elaborar un plan de contingencia y crecimiento de infraestructura basado en tendencias de uso.

8.07 Medida: Fortalecer la Protección contra Malware  
 Responsable: Área de TI (Tercerizado)  
 Tiempo estimado: 2 meses

* Implementar una solución EDR para la detección y respuesta ante amenazas en tiempo real.
* Desarrollar campañas internas de concientización sobre riesgos como phishing y malware.

8.08 Medida: Formalizar la Gestión de Vulnerabilidades Técnicas  
 Responsable: Área de TI (Tercerizado)  
 Tiempo estimado: 1 mes

* Contratar escaneos de vulnerabilidades trimestrales sobre los activos más críticos.
* Crear un procedimiento de parcheo con responsables y plazos definidos para cada criticidad.

8.09 Medida: Consolidar la Gestión de la Configuración  
 Responsable: Área de TI (Tercerizado)  
 Tiempo estimado: 1 mes

* Establecer plantillas estándar para configuración segura de servidores, redes y software.
* Realizar revisiones trimestrales para validar la consistencia entre configuraciones reales y documentadas.

8.12 Medida: Prevención de la fuga de datos  
 Responsable: Área de TI (Tercerizado)  
 Tiempo estimado: 2 meses

* Aplicar controles más rigurosos para la transferencia segura de información.
* Fortalecer los procedimientos de autorización para la divulgación de información confidencial.
* Configurar alertas en tiempo real para identificar posibles incidentes de fuga de datos de manera oportuna.

8.15 Medida: Mejorar la Gestión de Logs y Eventos  
 Responsable: Área de TI (Tercerizado)  
 Tiempo estimado: 2 meses

* Implementar un sistema SIEM que recolecte, almacene y analice los logs críticos.
* Definir un protocolo de revisión mensual con responsables y reporte de hallazgos.

8.23 Medida: Implementar Filtrado Web de Contenido Malicioso  
 Responsable: Área de TI (Tercerizado)  
 Tiempo estimado: 1 mes

* Incorporar una solución de filtrado web basada en categorías (proxy o firewall con listas negras).
* Configurar alertas y reportes ante intentos de acceso a sitios web bloqueados.

8.25 Medida: Asegurar el Ciclo de Vida del Desarrollo  
 Responsable: Proveedor de TI (Tercerizado)  
 Tiempo estimado: 2 meses

* Exigir el uso de entornos separados y controlados para desarrollo, prueba y producción.
* Integrar pruebas de seguridad automatizadas desde etapas tempranas del desarrollo.

8.27 Medida: Establecer Principios de Ingeniería Segura  
 Responsable: Proveedor de TI (Tercerizado)  
 Tiempo estimado: 3 meses

* Documentar lineamientos de arquitectura segura y mecanismos de autenticación robusta.
* Asegurar el uso adecuado de criptografía y validación de entradas en todos los desarrollos internos.

8.28 Medida: Adoptar Buenas Prácticas de Codificación Segura  
 Responsable: Proveedor de TI (Tercerizado)  
 Tiempo estimado: 1 mes

* Exigir al proveedor el uso de normas OWASP en los procesos de desarrollo.
* Establecer revisiones de código y pruebas de seguridad antes de pasar a producción.

# 

# **Conclusiones:**

**Cumplimiento Normativo y Sectorial:** La adopción de las medidas propuestas, basadas en la norma ISO 27002, permitirá a Servicentro Posben S.a.C. no solo alinearse con estándares internacionales, sino también fortalecer su cumplimiento con las exigentes regulaciones del sector de hidrocarburos en Perú, supervisadas por entidades como OSINERGMIN.

**Gestión de Riesgos Proactiva:** El análisis demuestra la necesidad crítica de evolucionar de un modelo de seguridad puramente reactivo a una gestión integral del riesgo. La implementación de controles como la gestión de vulnerabilidades y la inteligencia de amenazas permitirá a la empresa identificar, evaluar y mitigar riesgos de forma proactiva, protegiendo sus operaciones críticas y la información de sus clientes.

**Fortalecimiento de la Gobernanza de Seguridad:** La creación de políticas formales y la definición clara de roles y responsabilidades de seguridad, tanto para el personal interno como para el proveedor de TI, fortalecerán la estructura de gobernanza. Esto transforma la seguridad de una tarea informal y delegada a una función de negocio gestionada y supervisada.

**Cultura de Mejora Continua:** La integración de revisiones periódicas, como las auditorías de acceso, las pruebas de restauración de respaldos y el seguimiento formal de proveedores, establece un ciclo de mejora continua. Este enfoque asegura que los controles de seguridad se mantengan efectivos y se adapten a las nuevas amenazas y a la evolución del negocio.

**Sostenibilidad y Resiliencia del Negocio:** El fortalecimiento de la ciberseguridad es una inversión directa en la sostenibilidad y resiliencia de Servicentro Posben S.a.C. Al proteger sus activos de información y asegurar la continuidad operativa frente a incidentes, la empresa robustece su legado y su capacidad para mantener el liderazgo en un mercado competitivo.

# **Bibliografía**

Adedoyin, F. F., Adebayo, A. A., & Bekun, F. V. (2021). Cyber-risk and digital transformation in energy markets: Implications for developing economies. Energy Reports, 7, 6937–6945. <https://doi.org/10.1016/j.egyr.2021.09.007>

Agencia de Gestión de Servicios de Limpieza (AGESP). (2021). *Informe de Responsabilidad Social 2021*. <https://www.agesp.gob.pe/documentos/informe_responsabilidad_social_2021.pdf>

Alrammal, M., Al-Aqrabi, H., Hill, R., & Hussain, A. (2021). Framework for an ISO 27001-based information security management system (ISMS) for cloud computing. Procedia Computer Science, 184, 754–763. <https://doi.org/10.1016/j.procs.2021.03.095>

Banco Central de Reserva del Perú (BCRP). (2022). *Nota de estudios N.º 01-2022: Evolución reciente de los precios de los combustibles*. <https://www.bcrp.gob.pe/docs/Publicaciones/Notas-Estudios/2022/nota-de-estudios-01-2022.pdf>

Caballero-Gómez, J. A., López-Zambrano, L. I., & López-Samaniego, L. (2022). ISO 27001 y su adaptación en organizaciones públicas: una revisión sistemática. Revista Ibérica de Sistemas e Tecnologias de Informação, 43, 81–95. <https://doi.org/10.17013/risti.43.81-95>

Gkioulos, V., Kostopoulos, G., & Papaioannou, S. (2021). Information security management frameworks: A structured review. Computer Standards & Interfaces, 76, 103521. <https://doi.org/10.1016/j.csi.2021.103521>

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. <https://www.iso.org/standard/27001>

# OSINERGMIN. (2015). *La industria de los hidrocarburos líquidos en el Perú*. Organismo Supervisor de la Inversión en Energía y Minería. <https://www.osinergmin.gob.pe/seccion/centro_documental/Institucional/Estudios_Economicos/Libros/Libro-industria-hidrocarburos-liquidos-Peru.pdf>

Rebollo, O., Baldassarre, M. T., & Pascual-Espada, J. (2020). Risk management in ISO/IEC 27001: A systematic mapping study. Computer Standards & Interfaces, 68, 103401. <https://doi.org/10.1016/j.csi.2020.103401>