Legalidad y Protección de la Información

Caso 8

Empresa Telecomunicaciones del centro S.A.

Descripción General:

Telecomunicaciones del centro S.A. es una empresa de desarrollo de software con 200 empleados, ubicada en Aguascalientes, México. La empresa se especializa en soluciones de software personalizadas para clientes en diversas industrias, incluyendo finanzas, salud y educación.

Posterior a una auditoría de procesos, procedimientos, roles y tecnología el reporte presenta las siguientes eventualidades.

- Las políticas de seguridad de la información no están actualizadas y no se comunican adecuadamente a todos los empleados. La política de uso de dispositivos móviles no ha sido revisada en los últimos tres años, lo que deja brechas en la seguridad.

- No hay una clara definición de roles y responsabilidades en relación con la seguridad de la información. Los empleados no saben a quién reportar incidentes de seguridad, lo que retrasa la respuesta a estos incidentes.

- La empresa no realiza evaluaciones de riesgos periódicas ni tiene un proceso formal para gestionar los riesgos identificados. No se han identificado ni mitigado los riesgos asociados con el acceso remoto de los empleados.

- No se proporciona capacitación regular en seguridad de la información a los empleados. Los empleados no están al tanto de las últimas amenazas de phishing y cómo protegerse contra ellas.

- No se realizan verificaciones de antecedentes de manera consistente para todos los nuevos empleados. Un empleado con antecedentes de fraude fue contratado sin una verificación adecuada.

- La capacitación en seguridad de la información no es obligatoria para todos los empleados. Solo el personal de TI recibe capacitación en seguridad, dejando al resto de los empleados vulnerables a ataques.

- No hay un procedimiento claro para reportar y gestionar incidentes de seguridad. Los empleados no saben cómo reportar un incidente de seguridad, lo que resulta en una respuesta lenta y desorganizada.

- No se revocan de manera oportuna los accesos y privilegios de los empleados que dejan la empresa. Un ex-empleado aún tiene acceso a sistemas críticos semanas después de haber dejado la empresa.

- Las instalaciones no están adecuadamente protegidas contra accesos no autorizados. No hay controles de acceso físico en las áreas donde se almacenan datos sensibles.

- No hay planes de contingencia ni medidas de protección contra desastres naturales. No existen sistemas de respaldo para proteger los datos en caso de un incendio.

- El acceso a áreas sensibles no está restringido adecuadamente. Cualquier empleado puede acceder a la sala de servidores sin necesidad de autorización especial.

- No hay sistemas de monitoreo para detectar y responder a incidentes de seguridad física. No hay cámaras de vigilancia en las áreas críticas, lo que dificulta la identificación de accesos no autorizados.

- No se implementan controles de acceso adecuados para los sistemas y datos. Los empleados comparten contraseñas y no se utiliza autenticación multifactor (MFA).

- No se utilizan herramientas adecuadas para la detección y prevención de malware. No hay software antivirus instalado en todos los dispositivos de la empresa.

- Los datos sensibles no están cifrados, lo que pone en riesgo su confidencialidad e integridad. Los datos de los clientes se almacenan en texto plano en las bases de datos.

- No se implementan sistemas de monitoreo y registro para detectar y responder a incidentes de seguridad. No hay registros de eventos de seguridad, lo que dificulta la investigación de incidentes.

Reflexión

"Telecomunicaciones del centro S.A. enfrenta varios desafíos para cumplir con el estándar ISO/IEC 27001:2022. La empresa necesita actualizar sus políticas, definir roles y responsabilidades, implementar controles de acceso adecuados, y proporcionar capacitación continua en seguridad de la información para todos los empleados. Además, debe mejorar la seguridad física de sus instalaciones y adoptar tecnologías de protección y monitoreo más avanzadas".

ANEXOS

Rol Arquitecto de diseño de hardware y firmware (FPGA): Un arquitecto de diseño de hardware y firmware (FPGA) para un proyecto de ciencia de datos es responsable de diseñar y desarrollar sistemas FPGA personalizados que aceleran las cargas de trabajo de aprendizaje automático e inteligencia artificial, optimizando el rendimiento y la eficiencia energética para la ejecución de algoritmos complejos de ciencia de datos. En otras palabras, esta persona crea el "cerebro" físico de un sistema que permita procesar datos de manera rápida y eficiente, fundamental para aplicaciones de ciencia de datos como el reconocimiento de imágenes, el procesamiento del lenguaje natural y el aprendizaje profundo.

Desde el punto de vista de un arquitecto de diseño de hardware y firmware se analizaran las eventualidades presentadas por la Empresa Telecomunicaciones del centro S.A.

Eventualidad	Reflexión
Las políticas de seguridad de la información no están actualizadas y no se comunican adecuadamente a todos los empleados. La política de uso de dispositivos móviles no ha sido revisada en los últimos tres años, lo que deja brechas en la seguridad.	Se sugiere a Telecomunicaciones del centro S.A. el análisis de las cláusulas 8 "Controles tecnológicos" en especial el control 8.1 ya que los dispositivos móviles al ser un dispositivo de usuario final debe de contar con seguridad de todos sus datos propios o recabados. El dispositivo móvil debe de contar con un previo análisis de cumplimiento de los puntos de seguridad en análisis a vulnerabilidades según los controles 8.1 a 8.9.

No hay una clara definición de roles y responsabilidades en relación con la seguridad de la información. Los empleados no saben a quién reportar incidentes de seguridad, lo que retrasa la respuesta a estos incidentes.	Se sugiere a la empresa analizar el control 5.2 Roles y responsabilidades de seguridad de la información perteneciente a la cláusula 5 con un experto en la materia para en base a lo que estipule se puedan gestionar bien las personas que contaran con los privilegios adecuadamente como lo marca para el cumplimiento de las cláusulas 7 u 8 si se llegan a notar alguna vulnerabilidad en el proceso.
La empresa no realiza evaluaciones de riesgos periódicas ni tiene un proceso formal para gestionar los riesgos identificados. No se han identificado ni mitigado los riesgos asociados con el acceso remoto de los empleados.	Se recomienda a la empresa generar un esquema de cumplimiento para los equipos y usuarios que se conectan de manera remota para en base al cumplimiento de los controles 7.6,7.8 y en especial el 7.9 de la cláusula 7 “Controles físicos” se pueda generar un ambiente físico óptimo para poder laborar de forma segura en un ambiente remoto. También se sugiere que todo equipo que se conecte de manera remota se analice cuente con el cumplimiento de todos los puntos de control mencionados en la Cláusula 8”Controles tecnológicos”. También se tiene la necesidad de analizar con un experto el control 6.7 Trabajo remoto para su efectivo empleo.
No se proporciona capacitación regular en seguridad de la información a los empleados. Los empleados no están al tanto de las últimas amenazas de phishing y cómo protegerse contra ellas.	Se tiene la necesidad de recurrir a expertos en las cláusulas 6 “Controles de personas” para verificar con más detalle las necesidades para el uso adecuado de los controles 6.3 Concientización, educación y capacitación en seguridad de la información y mantener actualizados a los colaboradores sobre posibles amenazas que puedan surgir.
No se realizan verificaciones de antecedentes de manera consistente para todos los nuevos empleados. Un empleado con antecedentes de fraude fue contratado sin una verificación adecuada.	Se tiene la necesidad de recurrir a expertos en las cláusulas 6 “Controles de personas” para verificar con más detalle las necesidades para el uso adecuado de los controles 6.1 Poner en pantalla y 6.2Términos y condiciones de empleo.
La capacitación en seguridad de la información no es obligatoria para todos los empleados. Solo el personal de TI recibe capacitación en seguridad, dejando al resto de los empleados vulnerables a ataques.	Se tiene la necesidad de recurrir a expertos en las cláusulas 6 “Controles de personas” para verificar con más detalle las necesidades para el uso adecuado del control 6.3 Concientización, educación y capacitación en seguridad de la información según sean las necesidades de cada

	colaborador en base a el control 5.2 Roles y responsabilidades de seguridad de la información marcado en las cláusulas 5 “Controles organizacionales”.
No hay un procedimiento claro para reportar y gestionar incidentes de seguridad. Los empleados no saben cómo reportar un incidente de seguridad, lo que resulta en una respuesta lenta y desorganizada.	Se tiene la necesidad de recurrir a expertos en las cláusulas 5 “Controles organizacionales” para el adecuado empleo de los controles 5.2 Roles y responsabilidades de seguridad de la información, 5.3 Segregación de deberes, 5.4 Responsabilidades de gestión y 5.5 Contacto con autoridades
No se revocan de manera oportuna los accesos y privilegios de los empleados que dejan la empresa. Un ex-empleado aún tiene acceso a sistemas críticos semanas después de haber dejado la empresa.	Se sugiere estar al tanto de los ciclos utiles del personal para poder cumplir con el control 6.5 Responsabilidades después de la terminación o cambio de empleo para poder mantener solo al personal autorizado con el permiso de manipulación de los datos.
Las instalaciones no están adecuadamente protegidas contra accesos no autorizados. No hay controles de acceso físico en las áreas donde se almacenan datos sensibles.	En base a las Cláusulas 7 “Controles físicos” se sugiere generar un análisis de las posibles eventualidades de este entorno para poder generar un espacio que cuente con un lugar físico adecuado con bardas o rejas según se necesite para el cumplimiento del control 7.1, también un acceso controlado de manera segura con más de un punto proteccion a lo cual sugiero una cerradura física completamente mecánica con una llave controlada solo por las personas designadas a estos privilegios más una protección digital del mayor rango que sea posible y múltiples puntos de verificación como lo es un control de acceso biométrico como huella dactilar, reconocimiento facial o voz del emisor.
No hay planes de contingencia ni medidas de protección contra desastres naturales. No existen sistemas de respaldo para proteger los datos en caso de un incendio.	En base a las Cláusulas 7 “Controles físicos” se recomienda contar con un análisis previo de los requerimientos Eléctricos, o necesidades de controles de temperatura o protección a eventualidades climatológicas,para el cumplimiento del control 7.5 Protección contra amenazas físicas y ambientales para lo cual es necesario contar con no-brakes para respaldo de energía, gabinetes y racks de buena calidad y con aseguramientos y climas dedicados para este entorno.

El acceso a áreas sensibles no está restringido adecuadamente. Cualquier empleado puede acceder a la sala de servidores sin necesidad de autorización especial.	En base a las Cláusulas 7 “Controles físicos” se recomienda contar con un análisis previo de los posibles riesgos en el lugar de trabajo de la zona de los servidores, cuando menos se recomienda implementar un sistema de videovigilancia con aseguramiento de entradas con sistemas biométricos y alarmas de intrusión.
No hay sistemas de monitoreo para detectar y responder a incidentes de seguridad física. No hay cámaras de vigilancia en las áreas críticas, lo que dificulta la identificación de accesos no autorizados.	En base a las Cláusulas 7 “Controles físicos” en específico el control 7.4 Monitoreo de seguridad física se sugiere implementar un sistema de monitoreo moderno con una marca confiable para mantener un sistema actualizado con supervisión remota y cámaras ubicadas en lugares bien distribuidos buscan evitar los puntos muertos de vigilancia.
No se implementan controles de acceso adecuados para los sistemas y datos. Los empleados comparten contraseñas y no se utiliza autenticación multifactor (MFA).	En base a las Cláusulas 7 “Controles físicos” se recomienda para evitar los riesgos al saber que los empleados comparten sus contraseñas se sugiere el uso de tecnologías biométricas multi punto como lo son las que combinan la huella dactilar,reconocimiento facial, reconocimiento de voz,autenticación de iris, con contraseña cifrada.
No se utilizan herramientas adecuadas para la detección y prevención de malware. No hay software antivirus instalado en todos los dispositivos de la empresa.	Se tiene la necesidad de recurrir a expertos en las cláusulas 8 “Controles tecnológicos” para verificar con más detalle las necesidades para el uso adecuado de los controles 8.7 Protección contra malware y 8.8 Gestión de vulnerabilidades técnicas.
Los datos sensibles no están cifrados, lo que pone en riesgo su confidencialidad e integridad. Los datos de los clientes se almacenan en texto plano en las bases de datos.	Se tiene la necesidad de recurrir a expertos en las cláusulas 8 “Controles tecnológicos” para verificar con más detalle las necesidades para el uso adecuado de los controles 8.7 Protección contra malware y 8.8 Gestión de vulnerabilidades técnicas.
No se implementan sistemas de monitoreo y registro para detectar y responder a incidentes de seguridad. No hay registros de eventos de seguridad, lo que dificulta la investigación de	Se tiene la necesidad de recurrir a expertos en las cláusulas 8 “Controles tecnológicos” para verificar con más detalle las necesidades para el uso adecuado de los controles 8.28 Codificación segura y 8.27 Principios de arquitectura e

incidentes.	ingeniería de sistemas seguros.

CIO Andrea Graciela López Segura

Experiencia en estadísticas experimentales: Conocimiento en estadísticas, proporciona liderazgo estratégico en proyectos de ciencia de datos, diseñando y supervisando la implementación de modelos predictivos y analíticos que permiten a la organización tomar decisiones más informadas y basadas en datos.

Eventualidad	Reflexión
Políticas de seguridad de la información desactualizadas y no comunicadas adecuadamente	Se sugiere garantizar el cumplimiento de la cláusula 5.1 (Políticas de seguridad de la información). Esta cláusula requiere que las políticas se definan, publiquen y comuniquen. Se propone realizar revisiones periódicas de las políticas de seguridad, asegurando su actualización y comunicación a todos los niveles mediante capacitaciones y recordatorios frecuentes. Se sugiere garantizar el cumplimiento de la cláusula 8.1 (Dispositivos de punto final de usuario). Se requiere proteger la información almacenada y accesible a través de estos dispositivos. Se propone implementar revisiones anuales (preferentemente) de la política de uso de dispositivos móviles y asegurarse de que las medidas de seguridad estén actualizadas para mitigar riesgos Propuesta: Utiliza modelos predictivos para identificar qué áreas son más propensas a necesitar actualizaciones basadas en incidentes de seguridad previos y tendencias de ciberseguridad.
Falta de roles definidos en seguridad de la información	Se sugiere garantizar el cumplimiento de la cláusula 5.2 (Roles y responsabilidades de seguridad de la información). Es necesario que los roles de seguridad estén definidos. Se propone establecer una estructura organizacional clara donde los roles de seguridad estén asignados a personas específicas, lo que permite respuestas más rápidas y efectivas ante incidentes.
No se realizan evaluaciones de riesgos periódicas	Se sugiere garantizar el cumplimiento de las cláusulas 5.8 (Seguridad de la información en la gestión de proyectos) y 5.9 (Inventario de información y otros activos asociados). Se propone implementar evaluaciones de riesgos periódicas que identifiquen posibles vulnerabilidades en el acceso remoto, gestionando dichos riesgos mediante controles preventivos. Propuesta: implementar un sistema de monitoreo continuo con análisis predictivo para identificar riesgos emergentes en tiempo real. La modelación de datos te permitirá anticipar vulnerabilidades y proponer evaluaciones antes de que ocurran incidentes importantes.
Falta de capacitación regular en seguridad de la	Se sugiere garantizar el cumplimiento de la cláusula 6.3 (Concientización, educación y capacitación en seguridad de la

información	información). Desarrollar programas de capacitación regulares para todos los empleados, no solo el personal de TI, asegurando que todos estén preparados ante nuevas amenazas de seguridad de la información
No se realizan verificaciones de antecedentes de manera consistente para todos los nuevos empleados	Se sugiere garantizar el cumplimiento de la cláusula 6.1 (Poner en pantalla) Se propone asegurar que se implementen controles de verificación de antecedentes para todos los candidatos antes de su contratación, especialmente aquellos que accederán a información sensible. Propuesta: Crear un modelo predictivo basado en datos históricos sobre contrataciones, que identifique los perfiles de empleados con mayor probabilidad de causar problemas de seguridad.
Capacitación en seguridad no obligatoria para todos los empleados	Se sugiere garantizar el cumplimiento de la cláusula 6.3 (Concientización, educación y capacitación en seguridad de la información). Se propone asegurar que la capacitación adecuada y oportuna en seguridad de la información sea obligatoria para todos los empleados, y concientizarlos al respecto.
Falta de procedimiento claro para reportar incidentes	Se sugiere garantizar el cumplimiento de la cláusula 5.24 (Planificación y preparación de la gestión de incidentes de seguridad de la información). Se propone implementar procedimientos claros de reporte de incidentes y capacitar a los empleados sobre estos para asegurar una respuesta rápida y coordinada. Además, es crucial mantener una documentación de todos los incidentes ocurridos. Esta documentación no solo servirá para analizar las causas y consecuencias de cada incidente, sino que también permitirá desarrollar estrategias preventivas para evitar que se repitan en el futuro. En caso de que un incidente similar vuelva a ocurrir, contar con una estrategia predefinida permitirá una respuesta más rápida y efectiva, minimizando el impacto negativo en la organización. Propuesta: Los modelos predictivos pueden anticipar dónde es más probable que ocurran problemas y facilitar su resolución oportuna.
No se revocan de manera oportuna los accesos y privilegios de los empleados que dejan la empresa.	Se sugiere garantizar el cumplimiento de la cláusula 5.18 (Derechos de acceso). Se propone establecer procesos automáticos para la revocación de accesos tan pronto como un empleado deje la empresa, garantizando que no existan riesgos de acceso no autorizado. Y una revisión periódica, garantizando que se están revocando los accesos de manera oportuna.
Instalaciones sin controles de acceso físico adecuados	Se sugiere garantizar el cumplimiento de las cláusulas 7.1 (Perímetros físicos de seguridad) y 7.2 (Entrada física). Se propone implementar controles de acceso físico, como el uso de tarjetas o claves para restringir el acceso a áreas sensibles.

Sin planes de contingencia ni sistemas de respaldo	Se sugiere garantizar el cumplimiento de las cláusulas 5.30 (Preparación de las TIC para la continuidad del negocio) y 8.13 (Copia de seguridad de la información). Se propone implementar planes de contingencia y sistemas de respaldo periódicos que garanticen la recuperación de datos en caso de un desastre natural o fallo tecnológico.
Acceso a áreas sensibles sin restricciones	Se sugiere garantizar el cumplimiento de la cláusula 7.2 (Entrada física). Se propone implementar sistemas de control de acceso como tarjetas de identificación o biometría para asegurar que solo personal autorizado pueda acceder a estas áreas.
Sin sistemas de monitoreo para incidentes de seguridad física	Se sugiere garantizar el cumplimiento de la cláusula 7.4 (Monitoreo de seguridad física). Se propone instalar cámaras de vigilancia y sistemas de detección de accesos no autorizados en áreas críticas. Propuesta: integrar un monitoreo predictivo que analice datos de seguridad física y genere alertas tempranas sobre incidentes potenciales. Utiliza patrones históricos para predecir futuros accesos no autorizados.
Controles de acceso débiles (comparten contraseñas)	Se sugiere garantizar el cumplimiento de la cláusula 8.2 (Derechos de acceso privilegiado) y 8.5 (Autenticación segura). Se propone implementar autenticación multifactor (MFA) y establecer políticas estrictas de uso de contraseñas seguras.
Falta de herramientas para detección de malware	Se sugiere garantizar el cumplimiento de la cláusula 8.7 (Protección contra malware). Se propone implementar software antivirus y antimalware en todos los dispositivos de la empresa, con actualizaciones periódicas. Propuesta: realizar análisis predictivos para identificar patrones de actividad anormal en los sistemas, lo que permitirá detectar malware antes de que cause un daño significativo. Los modelos pueden basarse en datos de incidentes previos.
Datos sensibles no cifrados	Se sugiere garantizar el cumplimiento de la cláusula 8.24 (Uso de criptografía). Se propone implementar la encriptación de datos sensibles en todas las bases de datos y comunicaciones críticas.
Sin monitoreo y registro de incidentes de seguridad	Se sugiere garantizar el cumplimiento de la cláusula 8.15 (Inicio de sesión) y 8.16 (Actividades de seguimiento). Establecer un sistema de logs y monitoreo continuo para detectar y responder a incidentes de seguridad de manera proactiva. Propuesta: Desarrollar un sistema de análisis de logs y monitoreo predictivo que permita anticipar incidentes de seguridad. Con base en datos históricos, el sistema puede generar alertas sobre comportamientos anómalos.

Rol Arquitecto Tecnológico : Profesional encargado de diseñar y construir la infraestructura tecnológica necesaria para que los científicos de datos puedan llevar a cabo sus análisis y construir modelos de manera eficiente y escalable. Actúa como un puente entre los requisitos técnicos del proyecto y las capacidades de la organización.

Eventualidad	Reflexión
Las políticas de seguridad de la información no están actualizadas y no se comunican adecuadamente a todos los empleados. La política de uso de dispositivos móviles no ha sido revisada en los últimos tres años, lo que deja brechas en la seguridad.	Se recomienda aplicar medidas concernientes a la gestión de políticas de seguridad de información redactadas en ISO/CEI 27001:2022,Cláusula 5,5.1, donde la alta dirección define, aprueba y divulga diversas políticas, las cuales se revisan a intervalos definidos. Además aplicar la norma de control ISO/CEI 27001:2022,Cláusula 5,5.36 permite asegurar que las políticas sean conocidas y aplicadas por todo el personal.
No hay una clara definición de roles y responsabilidades en relación con la seguridad de la información. Los empleados no saben a quién reportar incidentes de seguridad, lo que retrasa la respuesta a estos incidentes.	Se recomienda realizar un análisis de riesgos y un plan de gestión de incidentes basado en la norma ISO/CEI 27001:2022,Cláusula 5,5.24 bajo el cuál se definan protocolos, procesos, roles y responsabilidades claras.
La empresa no realiza evaluaciones de riesgos periódicas ni tiene un proceso formal para gestionar los riesgos identificados. No se han identificado ni mitigado los riesgos asociados con el acceso remoto de los empleados.	Dado el contexto proporcionado referente a la falta de evaluación de riesgos se recomienda aplicar la norma de control ISO/CEI 27001:2022,Cláusula 8,8.8 que permite analizar, catalogar y evaluar todas las vulnerabilidades técnicas, las cuales se pueden ampliar a servicios provistos por proveedores ISO/CEI 27001:2022,Cláusula 5,5.19 e incluso a cadenas de suministros ISO/CEI 27001:2022,Cláusula 5,5.21. Referente al acceso para empleados remotos se recomienda aplicar la norma de control ISO/CEI 27001:2022,Cláusula 6,6.7 la cuál permite evaluar las necesidades y riesgos asociados a empleados remotos.
No se proporciona capacitación regular en seguridad de la información a los empleados. Los empleados no están al tanto	Se recomienda aplicar las medidas de control ISO/CEI 27001:2022,Cláusula 6,6.3 mediante la cuál permite a la empresa establecer medidas para la adecuada capacitación de empleados en materia de ciberseguridad según sea relevante para el correcto desempeño de sus funciones laborales.

de las últimas amenazas de phishing y cómo protegerse contra ellas.	
No se realizan verificaciones de antecedentes de manera consistente para todos los nuevos empleados. Un empleado con antecedentes de fraude fue contratado sin una verificación adecuada.	Se recomienda a la organización implementar las medidas descritas en ISO/CEI 27001:2022,Cláusula 6,6.1 mediante las cuales se establecen procesos claros que evalúan los antecedentes de todos los candidatos a integrarse a la organización.
La capacitación en seguridad de la información no es obligatoria para todos los empleados. Solo el personal de TI recibe capacitación en seguridad, dejando al resto de los empleados vulnerables a ataques.	Como se mencionó anteriormente es recomendable aplicar la norma ISO/CEI 27001:2022,Cláusula 6,6.3 mediante la cuál permite a la empresa establecer medidas para la adecuada capacitación de empleados en materia de ciberseguridad según sea relevante para el correcto desempeño de sus funciones laborales. Además se puede complementar con la medida ISO/CEI 27001:2022,Cláusula 8,8.7 la cuál está enfocada directamente a la capacitación referente a protección contra malware.
No hay un procedimiento claro para reportar y gestionar incidentes de seguridad. Los empleados no saben cómo reportar un incidente de seguridad, lo que resulta en una respuesta lenta y desorganizada.	Se recomienda definir y documentar procesos estandarizados para manejo de incidentes, fundamentado en la norma ISO/CEI 27001:2022,Cláusula 5,5.26 bajo el cuál se garantiza un protocolo que defina las acciones de manera clara y concisa que cada rol debe llevar a cabo.
No se revocan de manera oportuna los accesos y privilegios de los empleados que dejan la empresa. Un ex-empleado aún tiene acceso a sistemas críticos semanas después de haber dejado la empresa.	Es necesario aplicar medidas referentes a la norma ISO/CEI 27001:2022,Cláusula 8,8.3 referente a aplicar restricciones de acceso. Mediante la cual se aplican medidas específicas para administrar el control de información y otros activos. Complementado con la norma ISO/CEI 27001:2022,Cláusula 5,5.18, la cuál especifica reglas para revisar, modificar o eliminar accesos.

Las instalaciones no están adecuadamente protegidas contra accesos no autorizados. No hay controles de acceso físico en las áreas donde se almacenan datos sensibles.	Concerniente a accesos físicos las normas ISO/CEI 27001:2022,Cláusula 7,7.1 y ISO/CEI 27001:2022,Cláusula 7,7.2 donde se establecen recomendaciones referentes a la seguridad física y control de accesos.
No hay planes de contingencia ni medidas de protección contra desastres naturales. No existen sistemas de respaldo para proteger los datos en caso de un incendio.	Se recomienda aplicar las medidas de control de la norma ISO/CEI 27001:2022,Cláusula 7,7.5 la cuál recomienda diseñar e implementar medidas de control y protección contra amenazas físicas y ambientales.
El acceso a áreas sensibles no está restringido adecuadamente. Cualquier empleado puede acceder a la sala de servidores sin necesidad de autorización especial.	Como se mencionó anteriormente se recomienda aplicar las normas ISO/CEI 27001:2022,Cláusula 7,7.1, ISO/CEI 27001:2022,Cláusula 7,7.2 y ISO/CEI 27001:2022,Cláusula 7,7.3 las cuales establecen recomendaciones referentes a accesos físicos.
No hay sistemas de monitoreo para detectar y responder a incidentes de seguridad física. No hay cámaras de vigilancia en las áreas críticas, lo que dificulta la identificación de accesos no autorizados.	Se recomienda aplicar la norma ISO/CEI 27001:2022,Cláusula 7,7.4 bajo la cual se definen actividades para fortalecer la seguridad física y el control de accesos.
No se implementan controles de acceso adecuados para los sistemas y datos. Los empleados comparten contraseñas y no se utiliza autenticación multifactor (MFA).	Se recomienda aplicar la norma ISO/CEI 27001:2022,Cláusula 5,5.17 bajo la cuál se definen temas relacionados con la capacitación y asesoramiento sobre el manejo adecuado de la información de autenticación y la norma ISO/CEI 27001:2022,Cláusula 8,8.5 la cuál concierne los mecanismos de autenticación segura y control de accesos.
No se utilizan herramientas adecuadas para la detección y prevención de malware. No hay	Se enfatiza la previa recomendación de aplicar las medidas de control de la norma ISO/CEI 27001:2022,Cláusula 8,8.7 la cuál está enfocada directamente a la capacitación referente a protección contra malware.

software antivirus instalado en todos los dispositivos de la empresa.	
Los datos sensibles no están cifrados, lo que pone en riesgo su confidencialidad e integridad. Los datos de los clientes se almacenan en texto plano en las bases de datos	Se recomienda aplicar la norma ISO/CEI 27001:2022,Cláusula 8,8.11 mediante la cual se recomiendan técnicas de enmascaramiento de datos, lo cuál permite almacenar información sensible de manera segura, ya que el simple acceso no es suficiente para entender la información, como acompañamiento se pueden aplicar las normas de ISO/CEI 27001:2022,Cláusula 8,8.3 que filtre incluso el acceso a la información enmascarada.
No se implementan sistemas de monitoreo y registro para detectar y responder a incidentes de seguridad. No hay registros de eventos de seguridad, lo que dificulta la investigación de incidentes.	Se recomienda aplicar las normas de control propuestos en ISO/CEI 27001:2022,Cláusula 8,8.16 en acompañamiento de ISO/CEI 27001:2022,Cláusula 5,5.27 que en conjunto permiten detectar, monitorear y aprender de los incidentes de seguridad informática previos.

 Rol marco jurídico y de procesos Andrés Daniel Pérez Rodríguez

Marco jurídico y de procesos: "Un rol de BPM, al optimizar los procesos de negocio, garantiza que los datos utilizados en un proyecto de ciencia de datos sean precisos, relevantes y estén disponibles de manera oportuna. "Un marco legal jurídico asegura que el manejo y el uso de estos datos cumplen con las regulaciones existentes, protegiendo la privacidad y evitando riesgos legales".

Eventualidad	Clausula	Propuesta
Las políticas de seguridad de la información no están actualizadas y no se comunican adecuadamente a todos los empleados. La política de uso de dispositivos móviles no ha sido revisada en los últimos tres años, lo que deja brechas en la seguridad.	5.1 Políticas de seguridad de la información Control La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos. 6.3 Concientización, educación y capacitación en seguridad de la información Control El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, 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.	Revisión y actualización periódica de las políticas: - Implementar un ciclo de revisión regular, cada 3 meses o ante cambios tecnológicos o normativos. - Alinear las políticas de seguridad, incluyendo el uso de dispositivos móviles, con las mejores prácticas y amenazas emergentes. Comunicación efectiva a todos los empleados: - Hacer accesibles las políticas de seguridad mediante capacitaciones regulares, boletines informativos e intranet. - Verificar el reconocimiento de las políticas por parte de los empleados mediante firmas digitales o confirmaciones. Capacitación continua en

		seguridad de la información: - Proporcionar capacitación periódica en seguridad de la información, con énfasis en el uso seguro de dispositivos móviles. - Incluir simulacros de incidentes de seguridad para concienciar sobre posibles brechas de seguridad.
No hay una clara definición de roles y responsabilidades en relación con la seguridad de la información. Los empleados no saben a quién reportar incidentes de seguridad, lo que retrasa la respuesta a estos incidentes.	5.2 Roles y responsabilidades de seguridad de la información Control Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.	Definición de roles y responsabilidades: - Realizar un análisis organizacional para definir roles específicos relacionados con la seguridad de la información. - Asignar claramente estas responsabilidades a personas o equipos dentro de la empresa.
La empresa no realiza evaluaciones de riesgos periódicas ni tiene un proceso formal para gestionar los riesgos identificados. No se han identificado ni mitigado los riesgos asociados con el acceso remoto de los empleados.	5.27 Aprender de los incidentes de seguridad de la información Control El conocimiento obtenido de los incidentes de seguridad de la información se utilizará para fortalecer y mejorar los controles de seguridad de la información. 6.7 Trabajo remoto Control Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la	Evaluaciones periódicas de riesgos: - Establecer un proceso formal y continuo de evaluación de riesgos. - Identificar, analizar y priorizar los riesgos asociados a la seguridad de la información. - Enfocar el análisis en acceso remoto y

	que se acceda, procese o almacene fuera de las instalaciones de la organización. 7.9 Seguridad de los activos fuera de las instalaciones Control Se protegerán los activos fuera del sitio.	dispositivos móviles. - Revisar y actualizar el proceso periódicamente para adaptarse a las amenazas emergentes. Proceso de gestión de riesgos: - Definir un marco de gestión de riesgos alineado con la ISO/IEC 27005. - Incluir identificación, evaluación, tratamiento y monitoreo continuo de los riesgos. - Incorporar controles específicos para proteger el acceso remoto. - Definir roles claros en la mitigación de los riesgos. Trabajo remoto seguro: - Implementar políticas y tecnologías que aseguren el acceso remoto. - Usar VPNs, autenticación multifactor y cifrado de comunicaciones. Protección de dispositivos fuera de la oficina: - Asegurar la protección de dispositivos móviles y equipos fuera de las instalaciones. - Implementar cifrado de datos y políticas de uso de dispositivos personales

No se proporciona capacitación regular en seguridad de la información a los empleados. Los empleados no están al tanto de las últimas amenazas de phishing y cómo protegerse contra ellas.	6.3 Concientización, educación y capacitación en seguridad de la información Control El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, 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. 6.8 Informes de eventos de seguridad de la información Control 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.	Normatividad Interna: - Establecer una política que deslinde responsabilidades en caso de incumplimiento de las políticas de seguridad. - Definir claramente las consecuencias por negligencia en la protección de la información. - Incluir cláusulas de responsabilidad en los contratos laborales. Capacitación Obligatoria y Periódica: - Realizar capacitaciones anuales y actualizar políticas de seguridad. - Cubrir temas como amenazas emergentes (phishing), uso seguro de dispositivos móviles y procedimientos de reporte de incidentes. - Ofrecer capacitación específica según el

		rol del empleado. Firmas de Aceptación y Responsabilidad: - Después de cada capacitación, los empleados deben firmar un compromiso de cumplir con las políticas de seguridad. - Este documento debe reconocer la comprensión de responsabilidades y consecuencias por incumplimiento. Evaluaciones Periódicas: - Implementar evaluaciones periódicas de conocimiento mediante cuestionarios y simulaciones. - Asegurar que los empleados apliquen lo aprendido en la capacitación, como simulaciones de phishing.
No se realizan verificaciones de antecedentes de manera consistente para todos los nuevos empleados. Un empleado con antecedentes de fraude fue contratado sin una	6.1 Poner en pantalla Control Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal se llevarán a cabo antes de unirse a la	Implementar un proceso estándar de verificación de antecedentes para todos los nuevos empleados, independientemente de su nivel jerárquico o función, que incluya una revisión de

verificación adecuada.	organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.	antecedentes penales, crediticios y laborales. Este proceso debe ser documentado y revisado periódicamente para asegurar que se cumplan las normativas vigentes.
La capacitación en seguridad de la información no es obligatoria para todos los empleados. Solo el personal de TI recibe capacitación en seguridad, dejando al resto de los empleados vulnerables a ataques.	6.3 Concientización, educación y capacitación en seguridad de la información Control El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, 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. 5.1 Políticas de seguridad de la información Control La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.	Implementar un programa de capacitación obligatoria para todos los empleados, no solo para el personal de TI. Este programa debe incluir módulos que cubran los conceptos básicos de seguridad de la información, manejo seguro de datos, concientización sobre ataques comunes como phishing, y el uso adecuado de dispositivos móviles, especialmente considerando las brechas en la política actual de dispositivos. Actualización periódica: El programa debe ofrecer actualizaciones anuales para asegurarse de que todo el personal esté al día con las nuevas amenazas de ciberseguridad y cualquier cambio en las políticas internas. Medición y seguimiento: Realizar evaluaciones periódicas para medir el nivel de comprensión del personal sobre los temas de seguridad y ajustar el contenido de la capacitación en función de los resultados. Revisión de políticas de seguridad de dispositivos móviles: Dado que la política de dispositivos móviles no ha sido actualizada en tres años,

		es fundamental revisar y actualizar esta política para abordar riesgos actuales, y comunicarla de manera efectiva a todos los empleados. Se debe incluir en la capacitación, con módulos específicos sobre el uso seguro de dispositivos personales y corporativos
No hay un procedimiento claro para reportar y gestionar incidentes de seguridad. Los empleados no saben cómo reportar un incidente de seguridad, lo que resulta en una respuesta lenta y desorganizada.	5.1 Políticas de seguridad de la información Control La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos. 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información Control La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información. 5.26 Respuesta a incidentes de seguridad de la información Control Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados 6.8 Informes de eventos de	Actualización de políticas: Implementar un proceso de revisión y actualización anual de la política de seguridad de la información, y asegurarse de que se comunique a todos los empleados mediante capacitaciones regulares. Procedimiento claro para incidentes: Desarrollar e implementar un procedimiento claro y accesible para la gestión de incidentes de seguridad, incluyendo la designación de roles y responsabilidades específicas. Establecer un sistema de notificación centralizado y automatizado que permita el reporte ágil y eficiente de cualquier incidente. Capacitación en seguridad: Realizar capacitaciones periódicas a todo el personal para asegurarse de que entiendan cómo identificar y reportar incidentes de seguridad de manera oportuna y siguiendo los procedimientos establecidos. Simulacros y revisiones: Realizar simulacros de incidentes de seguridad regularmente para asegurar que los empleados conozcan el procedimiento y para

	seguridad de la información Control La organización debe proporcionar un mecanismo para que el personal informen eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.	identificar áreas de mejora en la respuesta organizacional.
No se revocan de manera oportuna los accesos y privilegios de los empleados que dejan la empresa. Un ex-empleado aún tiene acceso a sistemas críticos semanas después de haber dejado la empresa.	5.11 Devolución de activos Control El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo. 5.18 Derechos de acceso Control Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización. 6.5 Responsabilidades después de la terminación o cambio de empleo Control 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.	Revisar y actualizar los procedimientos de offboarding para que incluyan la revocación inmediata de todos los accesos a sistemas y redes internas. Implementar un sistema de monitoreo que asegure que no haya accesos activos de ex-empleados en los sistemas críticos después de su salida. Realizar auditorías regulares sobre los accesos y permisos de los empleados actuales y anteriores, verificando que los accesos no se mantengan más allá del periodo necesario. Incorporar un protocolo de devolución de dispositivos y activos tecnológicos que contengan información sensible, asegurándose de que toda la información confidencial se elimine antes de la entrega o reutilización del equipo.
Las instalaciones no están adecuadamente protegidas contra accesos no autorizados.	5.1 Políticas de seguridad de la información Control La política de seguridad de la	Actualizar y comunicar las políticas de seguridad: Se recomienda que las políticas de seguridad de la información,

No hay controles de acceso físico en las áreas donde se almacenan datos sensibles.	información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos. 6.3 Concientización, educación y capacitación en seguridad de la información Control El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, 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. 7.2 Entrada física Control Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados	especialmente la política de uso de dispositivos móviles, sean revisadas al menos una vez al año o tras cualquier cambio significativo en el entorno tecnológico o de amenazas. Además, debe implementarse un plan de comunicación eficaz, asegurando que todos los empleados comprendan las políticas y sepan cómo aplicarlas en su trabajo diario. Capacitación continua: Desarrollar un programa de capacitación anual que incluya sesiones sobre el uso seguro de dispositivos móviles, gestión de contraseñas y manejo de información sensible. Esto asegurará que los empleados estén informados y preparados para cumplir con las políticas de seguridad actualizadas. Mejora en la seguridad física: Implementar un sistema de control de acceso físico en las instalaciones, especialmente en las áreas donde se almacena información sensible. Esto puede incluir el uso de tarjetas de acceso, cámaras de vigilancia, y registro de visitantes, garantizando que solo personal autorizado pueda acceder a estas áreas. Monitoreo constante: Es necesario establecer mecanismos de monitoreo continuo de las instalaciones para detectar y responder a posibles accesos no autorizados, lo que también incluiría la implementación de alarmas y personal de seguridad especializado.

No hay planes de contingencia ni medidas de protección contra desastres naturales. No existen sistemas de respaldo para proteger los datos en caso de un incendio.	5.1 Políticas de seguridad de la información Control La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos 7.5 Protección contra amenazas físicas y ambientales. Control 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. 8.13 Copia de seguridad de la información Control 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 acordada.	Actualizar las políticas de seguridad de la información: Implementar un plan para revisar y actualizar las políticas de seguridad de la información, asegurando que se comuniquen adecuadamente a todos los empleados a través de capacitaciones regulares y accesibles en la intranet o a través de boletines. Realizar revisiones periódicas cada seis meses o después de cambios significativos en la infraestructura o en las normativas aplicables. Implementar un sistema de respaldo: Establecer un sistema de copias de seguridad automáticas que guarde los datos críticos en ubicaciones geográficamente separadas para protegerlos ante incendios o desastres naturales. Realizar pruebas periódicas de restauración de los datos para asegurar la funcionalidad de los sistemas de respaldo. Diseñar un plan de contingencia: Desarrollar un plan de contingencia y respuesta ante desastres naturales que incluya medidas de protección como detectores de incendios, sistemas de apagado automáticos y simulacros regulares para todo el personal. Además, se recomienda incluir revisiones anuales del plan para adaptarlo a nuevas amenazas o tecnologías emergentes.
El acceso a áreas sensibles no está restringido adecuadamente. Cualquier	5.1 Políticas de seguridad de la información Control La política de seguridad de la	Implementación de un sistema de control de acceso: Telecomunicaciones del Centro S.A. debe implementar un

empleado puede acceder a la sala de servidores sin necesidad de autorización especial.	información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos. 7.2 Entrada física Control Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.	sistema de control de acceso físico a las áreas sensibles, como la sala de servidores. Esto podría incluir el uso de tarjetas de acceso, autenticación biométrica o códigos de seguridad para garantizar que solo el personal autorizado pueda acceder. Además, debe haber un monitoreo regular de estos accesos mediante cámaras de seguridad y registros de acceso para identificar posibles anomalías o accesos no autorizados. Actualización de políticas de uso de dispositivos móviles: Las políticas deben actualizarse para abordar los riesgos asociados con el uso de dispositivos móviles en el entorno laboral. Estas políticas deben incluir medidas de seguridad como el cifrado de datos, la instalación de software de gestión de dispositivos móviles (MDM) y la restricción de acceso a información sensible desde dispositivos no seguros. Es esencial que estas políticas se comuniquen regularmente a todos los empleados y se asegure su comprensión y cumplimiento. Capacitación en concienciación de seguridad: Se debe implementar un programa continuo de capacitación y concienciación sobre seguridad de la información, que incluya la importancia de restringir el acceso físico a las áreas sensibles y las mejores prácticas para el manejo de dispositivos móviles. Esto ayudará a minimizar los

		riesgos y garantizar que todos los empleados estén al tanto de las políticas y procedimientos de seguridad.
No hay sistemas de monitoreo para detectar y responder a incidentes de seguridad física. No hay cámaras de vigilancia en las áreas críticas, lo que dificulta la identificación de accesos no autorizados.	5.1 Políticas de seguridad de la información Control La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos. 5.10 Uso aceptable de la información y otros activos asociados Control Se identificarán, documentarán e implementarán reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados. 7.4 Monitoreo de seguridad física Control Los locales deberán ser monitoreados continuamente para el acceso físico no autorizado.	Actualización de las políticas de seguridad de la información: Es fundamental realizar una revisión completa y actualización de las políticas de seguridad de la información, incluidas las relativas al uso de dispositivos móviles. Se deben establecer procesos regulares de revisión, por ejemplo, cada año, para asegurar que las políticas estén alineadas con las amenazas y tecnologías emergentes. Implementación de sistemas de monitoreo físico: Se deben instalar cámaras de vigilancia en las áreas críticas de la empresa. Además, la empresa debería implementar un sistema de monitoreo en tiempo real que permita detectar incidentes de seguridad física de manera inmediata, con la capacidad de generar alertas ante accesos no autorizados. Concientización y capacitación: Se debe reforzar la educación y capacitación del personal en cuanto a las políticas de seguridad, incluyendo el manejo seguro de dispositivos móviles y la importancia del reporte de incidentes. Esto permitirá que todo el personal esté alineado con las políticas y entienda su rol en la seguridad de la información.

No se implementan controles de acceso adecuados para los sistemas y datos. Los empleados comparten contraseñas y no se utiliza autenticación multifactor (MFA).	5.1 Políticas de seguridad de la información Control La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos. 5.17 Información de autenticación Control La asignación y gestión de la información de autenticación se controlará mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación. 6.3 Concientización, educación y capacitación en seguridad de la información Control El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, 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. 8.5 Autenticación segura Control Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la	Actualizar y Comunicar las Políticas: Revisar la política de uso de dispositivos móviles y actualizarla para cubrir las brechas de seguridad actuales. Esta actualización debe incluir la prohibición explícita de compartir contraseñas y la obligación de usar autenticación multifactor (MFA). Además, se debe comunicar adecuadamente a todo el personal para asegurar el cumplimiento. Implementar Autenticación Multifactor (MFA): Implementar el uso de autenticación multifactor (MFA) en todos los sistemas críticos para proteger el acceso a los datos sensibles de la empresa. Esto añadirá una capa adicional de seguridad en caso de que las credenciales de un empleado sean comprometidas. Capacitación Continua en Seguridad: Establecer un programa continuo de concientización y capacitación en seguridad de la información para educar a los empleados sobre las mejores prácticas de seguridad, incluyendo el manejo adecuado de contraseñas, los riesgos de compartirlas, y el uso seguro de dispositivos móviles en la empresa. Control de Acceso y Gestión de Contraseñas: Desarrollar una política estricta de gestión de contraseñas, incluyendo la implementación de un gestor de contraseñas corporativo que asegure que las contraseñas sean únicas y seguras.

	información y la política específica del tema sobre el control de acceso.	
No se utilizan herramientas adecuadas para la detección y prevención de malware. No hay software antivirus instalado en todos los dispositivos de la empresa.	5.1 Políticas de seguridad de la información Control La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos. 6.3 Concientización, educación y capacitación en seguridad de la información Control El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, 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. 8.7 Protección contra malware Control La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.	Actualización y comunicación de políticas: Desarrollar y revisar las políticas de seguridad de la información, incluidas las relativas al uso de dispositivos móviles y protección contra malware. Se recomienda que estas políticas sean comunicadas a todo el personal mediante capacitaciones regulares y manuales de buenas prácticas de seguridad. Implementación de un antivirus corporativo: Instalar software antivirus en todos los dispositivos de la empresa y establecer un sistema de actualizaciones automáticas. También se debe complementar con una solución de detección y prevención de malware (como un sistema de detección de intrusos) para mejorar la seguridad en los dispositivos móviles y equipos de escritorio. Capacitación continua en ciberseguridad: Establecer un programa de capacitación continua que incluya la concientización sobre malware, las mejores prácticas para el uso de dispositivos móviles y la implementación de medidas preventivas.
Los datos sensibles no están	5.1 Políticas de seguridad de la información	Actualizar y comunicar las políticas de seguridad: Se

cifrados, lo que pone en riesgo su confidencialidad e integridad. Los datos de los clientes se almacenan en texto plano en las bases de datos.	Control La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos. 6.3 Concientización, educación y capacitación en seguridad de la información Control El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, 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. 8.12 Prevención de fuga de datos Control 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. 8.24 Uso de criptografía Control Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas.	deben revisar y actualizar las políticas de seguridad de la información y de uso de dispositivos móviles, asegurándose de que sean comunicadas a todos los empleados. Esto puede incluir capacitaciones y la creación de un programa continuo de sensibilización en seguridad. Implementación de cifrado: Es crucial implementar inmediatamente la encriptación de los datos sensibles almacenados en las bases de datos para garantizar su confidencialidad e integridad. Esto incluye la gestión adecuada de claves criptográficas, como se menciona en la cláusula 8.24. Revisión periódica de políticas y medidas de seguridad: Establecer un calendario de revisiones periódicas para todas las políticas de seguridad de la información, incluyendo el uso de dispositivos móviles, para asegurar que se ajusten a las mejores prácticas y las regulaciones vigentes.
No se implementan sistemas de monitoreo y registro para	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la	Implementación de un Sistema de Monitoreo de Eventos de Seguridad: Instalar un sistema

detectar y responder a incidentes de seguridad. No hay registros de eventos de seguridad, lo que dificulta la investigación de incidentes.	información Control La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información. 5.25 Evaluación y decisión sobre eventos de seguridad de la información Control La organización debe evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información. 5.26 Respuesta a incidentes de seguridad de la información Control Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados. 5.27 Aprender de los incidentes de seguridad de la información Control El conocimiento obtenido de los incidentes de seguridad de la información se utilizará para fortalecer y mejorar los controles de seguridad de la información. 8.15 Inicio sesión Control Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallas y otros eventos relevantes. 8.16 Actividades de seguimiento Control Las redes, los sistemas y las	de monitoreo centralizado (SIEM) que permita registrar y analizar en tiempo real las actividades y eventos que ocurren en la red de la empresa, así como las actividades críticas de los sistemas. Este sistema ayudará a detectar incidentes de seguridad de manera temprana. Establecimiento de Procedimientos para la Gestión de Incidentes: Definir e implementar un plan de respuesta a incidentes de seguridad, que incluya roles y responsabilidades claras para todo el personal y procedimientos documentados para el manejo, escalamiento y mitigación de los incidentes. Capacitación al Personal: Proveer capacitaciones regulares a los empleados sobre la importancia de reportar incidentes de seguridad y cómo hacerlo de manera adecuada. Pruebas y Simulacros Regulares: Realizar simulacros de incidentes de seguridad para evaluar la eficacia del plan de respuesta y realizar ajustes según los resultados obtenidos.

	aplicaciones deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información.	

Rol: GHM - Omar Franco

Growth Hacking marketing: El growth hacking marketing proporciona un puente entre los descubrimientos de la ciencia de datos y la generación de valor real para un negocio, al optimizar la adquisición y retención de usuarios, y al maximizar el impacto de las soluciones de datos en el mercado.

Eventualidad	Reflexión
Políticas de seguridad no comunicadas adecuadamente.	5.2 Políticas de seguridad de la información. Se propone una campaña de concientización y entrenamiento personalizado, con herramientas de automatización para mejorar la segmentación y efectividad del mensaje.
Capacitación regular en seguridad de la información.	7.2 y 7.3 Competencia y Conciencia, respectivamente. Se sugiere usar análisis de datos para medir el impacto de la capacitación en la prevención de incidentes, ajustando la formación según los resultados obtenidos
Falta de sistemas de monitoreo y registro de eventos de seguridad.	9.1 Monitoreo, medición, análisis y evaluación. A.12.4 Registro de eventos y monitoreo

	Integrar Dashboards de monitoreo que permitan a los responsables de seguridad visualizar en tiempo real los riesgos y eventos críticos.
Datos no cifrados	A.8.3: Gestión de los medios de almacenamiento A.10 Encriptación o Criptografía Utilizar Growth Hacking para presentar esta mejora de seguridad como un valor agregado a los clientes, lo que podría fortalecer la confianza y la lealtad a la marca.
Acceso no controlado a áreas sensibles	A.9.1 Control de Acceso a la información A.9.4.2 Autenticación segura de usuarios Implementar herramientas de autenticación avanzada, como el MFA (Multi factor Authentication), y asegurarse de que estos cambios sean bien comunicados y aceptados por los empleados, con un enfoque en mejorar su experiencia de usuario.

Rol: Arquitecto de Visualizaciones Marco Antonio Rodríguez Rangel

Un rol de arquitecto de visualizaciones, al diseñar y optimizar la representación de datos, garantiza que la información presentada sea clara, precisa y relevante para la toma de decisiones. Además, asegura que los datos utilizados en las visualizaciones estén actualizados y sean accesibles en tiempo real para los usuarios.

Eventualidad	Cláusula ISO/IEC 27001:2022 Aplicable	Solución
Políticas de seguridad de la información desactualizadas y no comunicadas	5.1 Políticas de seguridad de la información	Definir, aprobar, publicar y revisar periódicamente las políticas de seguridad de la información, además de comunicar a todo el personal relevante.
Falta de definición de roles y responsabilidades en seguridad	5.2 Roles y responsabilidades de seguridad de la información	Definir y asignar roles y responsabilidades de seguridad de la información en función de las necesidades de la organización.
No se realizan evaluaciones de riesgos periódicas	5.24 Planificación y preparación para la gestión de incidentes 8.8 Gestión de vulnerabilidades técnicas	Establecer un proceso para realizar evaluaciones de riesgos periódicas y gestionar vulnerabilidades.
Capacitación en seguridad no proporcionada a todo el personal	6.3 Concientización, educación y capacitación en seguridad de la información	Proporcionar capacitación en seguridad de la información a todos los empleados, no solo al personal de TI.

Contratación sin verificaciones de antecedentes	6.1 Poner en pantalla	Realizar verificaciones de antecedentes para todos los candidatos antes de que se unan a la organización.
No se revocan los accesos de ex-empleados	5.18 Derechos de acceso	Gestionar y eliminar oportunamente los derechos de acceso de los empleados que dejan la organización.
Instalaciones no protegidas contra accesos no autorizados	7.1 Perímetros físicos de seguridad	Implementar perímetros de seguridad física para proteger las áreas que contienen información y activos críticos.
No existen planes de contingencia ni medidas de protección contra desastres	5.30 Preparación de las TIC para la continuidad del negocio	Planificar, mantener y probar la continuidad del negocio, incluyendo medidas de respaldo y protección.
Acceso no restringido a la sala de servidores	7.2 Entrada física	Establecer controles de acceso físico adecuados para las áreas seguras, incluyendo la sala de servidores.
Datos sensibles no cifrados	8.24 Uso de criptografía	Implementar reglas para el uso de criptografía y proteger la confidencialidad e integridad de los datos sensibles.

No hay un procedimiento claro para reportar incidentes de seguridad	5.24 Planificación y preparación para la gestión de incidentes	Definir y comunicar procedimientos para reportar y gestionar incidentes de seguridad.
Empleados no saben cómo reportar incidentes de seguridad	5.24 Planificación y preparación para la gestión de incidentes	Establecer y comunicar procedimientos para el reporte de incidentes y roles responsables.
No se utilizan controles de acceso adecuados para los sistemas y datos	5.15 Control de acceso	Implementar controles de acceso físicos y lógicos para proteger los sistemas y datos.
Los empleados comparten contraseñas y no se utiliza autenticación multifactor	8.5 Autenticación segura	Implementar autenticación multifactor (MFA) y políticas de uso adecuado de contraseñas.
No se implementan herramientas adecuadas de detección y prevención de malware	8.7 Protección contra malware	Instalar software antivirus y herramientas de detección de malware en todos los dispositivos.
No hay sistemas de monitoreo y registro para detectar incidentes de seguridad	8.16 Actividades de seguimiento	Implementar sistemas de monitoreo continuo para detectar incidentes de seguridad.
Un empleado con antecedentes de fraude fue contratado sin verificación adecuada	6.1 Poner en pantalla	Establecer un procedimiento formal de verificación de antecedentes antes de la contratación.

Empleados no están al tanto de las últimas amenazas de phishing	6.3 Concientización, educación y capacitación en seguridad de la información	Realizar capacitaciones regulares para educar a los empleados sobre las amenazas actuales de seguridad, como el phishing.
No hay cámaras de vigilancia en áreas críticas	7.4 Monitoreo de seguridad física	Instalar cámaras de vigilancia en áreas críticas para monitorear accesos no autorizados.
No se han identificado ni mitigado los riesgos asociados con el acceso remoto	8.7 Protección contra malware / 6.7 Trabajo remoto	Implementar medidas de seguridad para acceso remoto y mitigar riesgos asociados.