Capítulo 7

Buenas prácticas para la seguridad de información en las organizaciones aplicadas a una productora "Wedding joyce"

"Implementation of Best Practices for Information Security in Organizations: A Case Study of the 'Wedding Joyce' Production Company

Ibar Jacobo Rodríguez Villegas [1]
Héctor Guzmán Coutiño [2]

DOI: https://doi.org/10.61728/AE26001265

[1] Alumno de la maestría en Gestión de las Tecnologías de Información en las Organizaciones de la Facultad de Contaduría y Administración, zS23000606@estudiantes.uv.mx
[2] Miembro del Núcleo Académico Básico de la maestría en Gestión de las Tecnologías de Información en las Organizaciones de la Facultad de Contaduría y Administración de la Universidad Veracruzana. Correo electrónico de contacto: hguzman@uv.mx

Resumen

El presente proyecto está enfocado al desarrollo e implementación de buenas prácticas para la seguridad de información. Como ya sabemos, en la actualidad la integridad de datos en las pymes se ha convertido en uno de los activos más valiosos con los que se cuentan; de ellos depende si los clientes siguen con la empresa o si deciden cambiar de organización para el manejo de su información, imagen, finanzas, etc. Con esto se atenderán los principales problemas a los cuales se enfrentan día con día, por ejemplo, pérdida de datos, plagio de información o robo de identidad. La organización tiene como objetivo principal satisfacer las necesidades del cliente en el ámbito audiovisual y este proyecto de intervención tiene el fin de salvaguardar la integridad, confidencialidad y disponibilidad de los activos digitales de la organización.

Introducción

La seguridad de la información es un tema crítico en la actualidad debido al gran volumen de datos que se manejan en las organizaciones y al aumento de la ciberdelincuencia. Implementar buenas prácticas para la seguridad de la información es esencial para proteger los datos y garantizar la confidencialidad, integridad y disponibilidad de la información.

El objetivo general de este proyecto de intervención es atender la problemática que existe dentro de las instituciones, dependencias u organizaciones, con la aplicación de las buenas prácticas para garantizar la integridad de datos.

La seguridad de la información se ha convertido en un aspecto crucial en el entorno actual de tecnología y comunicaciones. La creciente dependencia de sistemas digitales y la constante amenaza de ciberataques demanda la implementación de buenas prácticas para proteger la integridad, confidencialidad y disponibilidad de la información sensible de una organización.

En muchas ocasiones estamos tan acostumbrados a la tecnología, ya que todos los días convivimos e interactuamos con ella, pero nunca se piensa en lo que pasaría si un día nos sucediera algo como robo de datos,

plagio de información, pérdida de acceso a datos con terceras personas o violación de confidencialidad de datos. Para ello se desarrollará el proyecto de intervención, para evitar todo este tipo de situaciones, en las que podamos tener algún problema y empezar a aplicar las buenas prácticas, tomar medidas de prevención como mantenimiento preventivo, mantenimiento correctivo, capacitación y evaluación de la estructura informática del personal para evitar un futuro problema con la empresa, ya sea que esta llegara a tener una auditoría informática o pérdida de datos de manera local o en la nube.

Es importante siempre estar en constante evaluación y actualización de las tecnologías de información (TI) y capacitación del recurso humano (colaboradores), para mantener la integridad de los datos e información que es importante para el sustento de cualquier persona moral y estar cerciorados de que es eficiente y eficaz.

Desarrollo de la propuesta

Como resultado del diagnóstico realizado a la empresa Wedding Joyce, se identificaron deficiencias en la gestión de la seguridad de la información, tales como la ausencia de políticas de protección de datos, falta de capacitación al personal y almacenamiento inseguro de información sensible. Por ello, se propone un conjunto de buenas prácticas orientadas a mejorar los niveles de confidencialidad, integridad y disponibilidad de la información en la organización.

Justificación

Las PYMES son un motor fundamental de la economía, pero muchas de ellas enfrentan desafíos significativos en términos de seguridad de la información debido a limitaciones de recursos, conocimientos técnicos y conciencia sobre riesgos cibernéticos. Abordar esta problemática es crucial por las siguientes razones:

Protección de datos sensibles

Se refieren a cualquier información que, si se divulga, se altera o se accede de manera no autorizada, podría causar un perjuicio significativo a la empresa, sus empleados, clientes o colaboradores: el acceso restringido, la formación en seguridad de datos para el personal y el cumplimiento de las regulaciones de privacidad pertinentes. Normalmente, en todas las empresas se firma un contrato de confidencialidad para evitar este tipo de inconvenientes.

Riesgos cibernéticos emergentes

Hace referencia a que sea divulgada información privada de la pyme, así quedando vulnerable ante la competencia.

Impacto en la reputación y la continuidad del negocio; es importante tener esto en cuenta, ya que la reputación es la que hablará por sí misma con el campo laboral.

Requisitos legales y regulatorios: En muchos países, hay leyes específicas que regulan la privacidad y la protección de datos, como la Ley de Protección de Datos Personales en México. Estas leyes pueden imponer requisitos adicionales sobre cómo se manejan y protegen los datos sensibles, poniendo como ejemplo la norma ISO 27001.

Fundamentación metodológica

La investigación se desarrolló bajo un enfoque cuantitativo y descriptivo, dado que se buscó medir el nivel de implementación de buenas prácticas de seguridad de información en la productora. Para ello, se diseñó un cuestionario basado en una escala Likert de 1 a 5, estructurado en cuatro categorías: Suficiencia, coherencia, relevancia y claridad.

El instrumento fue validado por cinco expertos en seguridad de información, seleccionados según criterios de experiencia y conocimiento en la materia, lo que garantizó la pertinencia y confiabilidad de los ítems. Posteriormente, se aplicaron análisis estadísticos descriptivos, incluyendo medias, desviaciones estándar y comparaciones entre categorías,

así como el cálculo del alfa de Cronbach para evaluar la consistencia interna del cuestionario.

Se destacan además las limitaciones del estudio, principalmente relacionadas con el tamaño de la muestra de expertos y la focalización en una sola organización. A pesar de ello, el diseño metodológico permitió obtener información relevante sobre el estado actual de las prácticas de seguridad y proporcionó un marco sólido para la formulación de recomendaciones futuras.

Fundamentación teórica

La seguridad de la información es la protección de los datos contra el acceso no autorizado, la divulgación, la modificación o la destrucción. Incluye la adopción de medidas técnicas, organizativas y de gestión para proteger y mantener en integridad la información.

De acuerdo con Bauer (2017), la política de seguridad de la información implementada por la organización para proteger su información puede ser uno de los temas que pueden generar controversia; la razón es que, a pesar de la existencia de esta información, la seguridad de la información es violada por factores humanos.

Como consecuencia, la seguridad de la información no solo se trata de tener nombres de usuario y contraseñas como lo hacemos en las organizaciones, sino de normativas y estrategias de privacidad y protección de datos que impongan obligaciones a la organización.

En primer lugar, se revisan los conceptos fundamentales de seguridad de la información, incluyendo las tres principales bases de una organización, empezando con confidencialidad, integridad y disponibilidad (CIA), la cual constituye la base sobre la cual se estructuran las prácticas organizacionales de protección de datos, conservando los activos intangibles y principios éticos.

Asimismo, se consideran normas internacionales como ISO 27001, la cual proporciona un marco estructurado para la gestión y control de la información. Dicha norma permite identificar procedimientos estandarizados y prácticas recomendadas que fortalecen la seguridad en entornos corporativos.

El análisis también incluye buenas prácticas organizacionales, como el control de accesos, la gestión de contraseñas, las copias de seguridad y la capacitación del personal. Se reconoce que, aunque estos elementos son teóricamente fundamentales, su implementación efectiva depende de factores culturales y de concienciación dentro de la organización; por ello es importante tener bien definido el marco legal y teórico, para fundamentar las bases de nuestras normas y cultura del ente.

Ciberseguridad

La ciberseguridad es un concepto más amplio que la seguridad de la información y abarca la protección de sistemas, redes y programas de ataques digitales. Se enfoca en proteger la información en todas las fases del ciclo de vida de los datos, incluidos los procesos de almacenamiento, transmisión y uso.

- Amenazas cibernéticas: La ciberseguridad se enfrenta a un amplio espectro de amenazas, como el malware, phishing, ransomware y ataques distribuidos de denegación de servicio (DDoS).
- Defensa en profundidad: Este enfoque estratégico implica la implementación de múltiples capas de seguridad (como firewalls, IDS/IPS, autenticación multifactor) para garantizar que, si un control falla, otros puedan proteger los activos críticos.

El marco teórico de la ciberseguridad implica también una adaptación constante a las nuevas amenazas y la necesidad de actualización continua de las políticas y herramientas de protección.

La ISO 27001 es la norma ISO que establece los requerimientos para implementar, mantener y mejorar un SGSI y en la actualidad es el único estándar aceptado a nivel internacional para la gestión de la seguridad de la información.

ISO/IEC 27001:2013 = NTP ISO/IEC 27001:2014. Permite reforzar la seguridad de la información y disminuir los riesgos de fraude, así como la pérdida o filtración de información. Algunos beneficios de la norma ISO/IEC 27001.

- Identificar los riesgos y establecer controles para gestionarlos o eliminarlos.

- Confidencialidad, asegurando que solo quienes estén autorizados puedan acceder a la información.
- Flexibilidad para adaptar los controles a todas las áreas de la empresa o solo a algunas seleccionadas.
- Conseguir que las partes interesadas y los clientes confíen en la protección de los datos.
- Demostrar conformidad y conseguir el estatus de proveedor preferente.

Alcanzar las expectativas demostrando conformidad. En las normas para la evaluación de la seguridad de la información se incluye dos partes:

ISO/IEC 27001:2013, describe los requisitos para la implementación y la documentación necesaria de un Sistema de Gestión de Seguridad de la Información (SGSI). Constituye:

- Tecnología de la Información.
- Técnicas de Seguridad.
- Sistemas de Gestión de Seguridad de la Información.
- Requisitos (Martín, 2021).

Privacidad de los datos

El concepto de privacidad de los datos tiene una base teórica que se centra en la protección de la información personal. En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) se erige como una de las principales normativas que regulan el uso de datos personales.

- Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición son esenciales en la gestión de datos personales. El marco teórico de la privacidad de datos establece que los individuos deben tener el control sobre su información personal.
- Consentimiento informado: Un principio clave es que las organizaciones deben obtener el consentimiento explícito de las personas antes de recopilar, usar o divulgar sus datos personales, garantizando la transparencia y el control sobre el uso de la información.

ISO 27001

La normativa ayuda a que las organizaciones conozcan el verdadero alcance de la seguridad de su información, así como a una gestión eficiente de los riesgos que afectan a su sistema. Confidencialidad, integridad y disponibilidad son los conceptos básicos en torno a los cuales orbitan las directrices de esta ISO (Gómez, 2006).

Este propone la gestión de seguridad de toda la información de la empresa, ya que el tener en riesgo la información de la empresa representa un alto nivel de amenaza, debido a que se puede llegar a tener pérdida financiera, pérdida de servicios esenciales de la red e incluso la reputación y confianza que se tenga con los clientes.

NIST

El Marco de ciberseguridad de NIST puede ayudar a una organización a comenzar o mejorar su programa de ciberseguridad. Construido de prácticas que se sabe que son efectivas, puede ayudar a las organizaciones a mejorar su postura de ciberseguridad. Promueve la comunicación entre las partes interesadas internas y externas sobre ciberseguridad (Mahn, 2021).

El marco se basa en cinco funciones principales: identificar, proteger, detectar, responder y recuperarse. La implementación de este marco nos ayudaría a identificar ciertas deficiencias internas y externas de las organizaciones, que pueden afectar el desempeño de sus objetivos.

COBIT

> Entre los lineamientos pertinentes se destaca el Control de Objetivos para la Información y la Tecnología relacionada, conocido por sus siglas en inglés como COBIT. Este es estándar de buenas prácticas para la gestión de los sistemas de información de las organizaciones que ofrece un marco de trabajo de procesos que presenta las actividades de manera lógica y alcanzable. Este estándar se encuentra mucho más enfocado al control que a la ejecución. (Sánchez, 2020)

Entonces, el COBIT es un estándar de buenas prácticas orientado a los negocios u organizaciones, al igual que a procesos, basado en controles e impulsos de mediciones, en los cuales se analizan los requerimientos del negocio, dirigiendo una investigación en TI, los cuales son ocupados por procesos de TI para posteriormente entregar la información recabada a la empresa que responderá a los requerimientos de la organización. Cada uno de los procesos que se llevan a cabo son actividades intuitivas lógicas que son alcanzables para las organizaciones con base en los requerimientos.

GTI

El gran problema del gobierno de TI es alinear los objetivos estratégicos de TI con los de la organización y entregar valor, para lograr beneficios comerciales mientras se optimizan los riesgos y los recursos (MARULANDA-ECHEVERRY y otros, 2017).

El impacto de las tecnologías de información en el mundo empresarial ha concitado un interés creciente por parte de la alta gerencia como elemento básico que debe ser gestionado eficientemente para sostener y aumentar la ventaja estratégica de las empresas (Zamora Sotelo, 2005). Es un patrón de comportamiento por parte de los grupos de interés de una organización, encargado del desarrollo estratégico, organizacional, cultural y de los procesos que aseguren que las TI soportan, amplían y desarrollan las estrategias y objetivos corporativos en el desarrollo de la creación de valor (Castro, 2010).

Principios básicos de la seguridad de información

- Integridad: Garantizar que la información sea precisa y completa, y que no sea alterada sin autorización, lo que propicie que la información sea certera y legítima.
- Disponibilidad: Asegurar que la información esté disponible para los usuarios autorizados cuando sea necesario, sin importar el lugar u hora.

Buenas prácticas en cuanto a seguridad de la información

Las buenas prácticas para la seguridad de la información incluyen la implementación de controles de acceso, la adopción de políticas y procedimientos de seguridad, la capacitación de los empleados en seguridad de la información, el uso de herramientas de seguridad como firewalls, antivirus y cifrado de datos, la monitorización y registro de actividades y la realización de auditorías de seguridad.

Características de las buenas prácticas

- Eficiencia: Las buenas prácticas deben ser efectivas para lograr el objetivo deseado con el menor recurso posible.
- Seguridad: En el ámbito de la seguridad de la información, las buenas prácticas protegen la confidencialidad, integridad y disponibilidad de los datos.
- Actualización: Deben ser revisadas y actualizadas regularmente para adaptarse a nuevos riesgos, tecnologías y estándares.
- Documentación: Las buenas prácticas deben estar bien documentadas para asegurar que todos los miembros de la organización las conozcan y puedan implementarlas correctamente.

Beneficios

- Reducción de riesgos: Minimiza la exposición a amenazas y vulnerabilidades mediante la aplicación de técnicas probadas.
- Confianza: Mejora la confianza de los clientes y socios al demostrar un compromiso con la protección de la información.
- Eficiencia operativa: Optimiza procesos y procedimientos, lo que puede llevar a una mayor eficiencia y menor costo operativo.
- Confidencialidad.
- Protección de la información contra el acceso no autorizado.
- Integridad.

Garantizar que la información sea legítima, precisa y completa, sin que esta haya sufrido algún cambio por agentes externos sin el rol encargado de modificarla.

Descripción de la propuesta

Buenas prácticas de seguridad gestión de accesos

- Control de accesos: Implementar políticas estrictas sobre quién puede acceder a la información y a qué nivel, dependiendo del rol asignado de la empresa, va a depender de los accesos que tenga a los diferentes tipos de información.
- Autenticación: Utilizar métodos de autenticación fuertes, como contraseñas seguras, autenticación multifactorial (MFA) y biometría.

Protección de datos

- Cifrado: Encriptar la información tanto en reposo como en tránsito para protegerla de accesos no autorizados.
- Respaldo: Realizar copias de seguridad periódicas de la información y almacenarlas en ubicaciones seguras; se puede decir que se realizará mantenimiento preventivo.

Seguridad de las Redes

- Firewall: Utilizar firewalls para proteger la red de accesos no autorizados.
- Monitorización: Implementar herramientas para monitorizar y detectar actividades sospechosas en la red.

Seguridad física

- Acceso físico: Restringir el acceso físico a las instalaciones donde se almacenan datos sensibles.

- Protección de equipos: Asegurar los dispositivos y equipos contra robos y daños.

Gestión de vulnerabilidades

- Actualizaciones y parches: Mantener sistemas y software actualizados con los últimos parches de seguridad.
- Auditorías: Realizar auditorías de seguridad regulares para identificar y corregir vulnerabilidades.

Formación y concienciación

- Capacitación: Formar a los empleados sobre las mejores prácticas de seguridad y la importancia de proteger la información.
- Simulacros: Realizar simulacros y pruebas de respuesta ante incidentes para preparar al personal en caso de una brecha de seguridad.

Políticas y procedimientos

- Políticas de seguridad: Desarrollar y mantener políticas de seguridad de la información claras y actualizadas.
- Procedimientos de respuesta a incidentes: Tener procedimientos definidos para la gestión y respuesta a incidentes de seguridad.

Evaluación y mejora continua

- Revisión periódica: Revisar y actualizar regularmente las políticas y prácticas de seguridad.
- Evaluaciones de riesgo: Realizar evaluaciones de riesgo para identificar y mitigar nuevos riesgos.

Plan de implementación

Tabla 1. *Elaboración propia*

Fase	Actividad	Responsable	Tiempo estimado
1	Diagnóstico técnico	Responsable TI	2 semanas
2	Desarrollo de políticas internas	Dirección administrativa	2 semanas
3	Capacitación al personal	Consultor externo	1 mes
4	Implementación de controles	Área de sistemas	3 semanas

Recursos necesarios

Según COBIT 4.1, los recursos de TI se dividen en cuatro categorías principales: Aplicaciones, Información, Infraestructura y Personas.

Dentro de los recursos en la productora se encuentran:

1. Aplicaciones

Software de edición y producción: Aplicaciones como Adobe Creative Cloud (Photoshop, Lightroom, Premiere Pro), Final Cut Pro u otros programas especializados para la edición y postproducción de imágenes y videos.

Plataformas de almacenamiento en la nube: Soluciones como Google Drive, Dropbox o servicios específicos para la industria que permiten el almacenamiento seguro y el acceso remoto a archivos y proyectos.

Servidores y almacenamiento local: Si la empresa opta por almacenamiento local, puede contar con servidores dedicados o unidades de almacenamiento en red (NAS) para guardar archivos y datos.

2. Información

- Almacenamiento: Almacenamiento centralizado para archivos de alta resolución, videos, proyectos en curso y recursos visuales. Puede incluir servidores locales o soluciones en la nube.

- Red y comunicaciones: Infraestructura de red que permite la comunicación fluida entre dispositivos y sistemas, garantizando la transferencia eficiente de archivos y datos.
- Sistemas de *backup* y recuperación: Estrategias y sistemas para realizar copias de seguridad regulares de datos críticos y procedimientos de recuperación en caso de fallos o pérdida de información.
- Seguridad de la información Soluciones de seguridad cibernética, incluyendo antivirus, acceso controlado y cifrado de datos sensibles para proteger la información de la empresa y la propiedad intelectual.

3. Infraestructura

- Equipos y dispositivos de producción: Cámaras, equipos de grabación de video, computadoras y software de edición necesarios para la creación y manipulación de contenido visual.
- Equipamiento fotográfico y de video: Cámaras (equipo Canon y Sony), lentes (diferentes obturaciones), iluminación, trípodes, micrófonos y otros equipos especializados para la captura de imágenes y grabación de video.
- Computadoras de alto rendimiento con especificaciones avanzadas para manejar la edición y procesamiento de archivos de alta resolución.
- Redes de alta velocidad y comunicaciones: Conexiones de red rápida y estable para transferir archivos grandes entre dispositivos y colaborar en tiempo real con miembros del equipo.
- Sistemas de seguridad informática: sistemas antivirus, medidas de encriptación y protocolos de seguridad para proteger los datos sensibles y mantener la integridad de la información.

4. Capital humano

- Colaboradores: Empleados y otros usuarios que utilizan los sistemas y aplicaciones de TI en sus actividades diarias.

Dentro de la productora, son los colaboradores involucrados dentro de la producción de material y la gestión de la información.

De la mano de los procesos de COBIT 4.1, las herramientas que pueden ser utilizadas para gestionar los recursos son: el plan estratégico, el presupuesto de TI, la descripción de puestos y el plan de desempeño y capacidad.

Beneficios esperados

La implementación de buenas prácticas en seguridad de la información en la empresa Wedding Joyce permitirá fortalecer la protección de los activos digitales mediante el aseguramiento de la confidencialidad, integridad y disponibilidad de la información. Este enfoque contribuirá a la reducción de riesgos asociados a accesos no autorizados, pérdida o alteración de datos sensibles, y permitirá establecer un marco normativo interno basado en estándares internacionales.

Asimismo, se promoverá una cultura organizacional orientada a la ciberseguridad mediante la capacitación del personal, lo que reducirá la vulnerabilidad humana y mejorará la respuesta ante incidentes. La formalización de políticas y procedimientos incrementará la eficiencia en la gestión tecnológica y administrativa, optimizando la toma de decisiones en contextos de riesgo.

Adicionalmente, la organización podrá proyectar una imagen institucional más confiable y profesional, lo que favorecerá su posicionamiento en el mercado y fortalecerá las relaciones con clientes y aliados estratégicos. En suma, la propuesta contribuirá a garantizar la continuidad operativa de la empresa, incrementando su resiliencia frente a amenazas tecnológicas y fortaleciendo su capacidad de adaptación en un entorno digital cada vez más exigente.

Enfoque y tipo de investigación

- Enfoque cuantitativo
- En la investigación existen diversos instrumentos para medir las variables de interés, pudiendo combinarse varias técnicas de recolección de datos; en este caso, se empleó el cuestionario como herramienta principal. Este instrumento permite recopilar información a través de un conjunto de preguntas estructuradas. En particular, se utilizó un cuestionario cerrado, en el cual las opciones de respuesta fueron previamente definidas, limitando a los participantes a seleccionar entre las alternativas establecidas para garantizar uniformidad y precisión en los datos obtenidos.

Elaboración del cuestionario

Para la elaboración del cuestionario se realizó primero un análisis para determinar la herramienta más adecuada al enfoque cuantitativo del estudio, concluyendo que el cuestionario cerrado con escala de Likert era el más pertinente. Este tipo de instrumento permite obtener respuestas estructuradas, representando distintos grados de acuerdo o desacuerdo ante afirmaciones relacionadas con el tema investigado.

El propósito principal fue recopilar información cuantitativa sobre las percepciones y actitudes de los participantes respecto a las buenas prácticas de seguridad de la información dentro de la organización Wedding Joyce. A partir de una adecuada operacionalización de variables, se diseñaron ítems que permitieron identificar niveles de cumplimiento y posibles deficiencias en la implementación de dichas prácticas, buscando fortalecer la protección de los datos y la confianza con clientes y socios.

Antes de su aplicación, el instrumento fue sometido a validación por juicio de expertos, contando con la revisión de cinco profesionales del área de sistemas, quienes evaluaron los criterios de suficiencia, coherencia, relevancia y claridad. Tras incorporar sus observaciones, se procedió a validar estadísticamente la consistencia del cuestionario mediante el coeficiente Kappa de Fleiss, asegurando la confiabilidad del instrumento para su aplicación.

El coeficiente kappa se construye en base a un cuociente, el cual incluye en su numerador la diferencia entre la sumatoria de las concordancias observadas y la sumatoria de las concordancias atribuibles al azar, mientras que su denominador incluye la diferencia entre el total de observaciones y la sumatoria de las concordancias atribuibles al azar (CERDA L, 2008).

Los coeficientes Kappa oscilan entre 0 y 1, donde 0 indica desacuerdo total y 1 representa el máximo nivel de acuerdo. Su interpretación se clasifica como: pobre (0–0.20), débil (0.21–0.40), moderado (0.41–0.60), bueno (0.61–0.80) y muy bueno (0.81–1.00). En esta investigación se obtuvo un valor de 0.59, lo que refleja una concordancia moderada entre los jueces. Esto indica que el instrumento presentaba buena coherencia y fundamentos adecuados, requiriendo únicamente ajustes menores según las observaciones de los expertos antes de su validación final y aplicación.

Resultados

El mapa de calor refleja las respuestas de cinco participantes a los 30 ítems del instrumento, donde los tonos rojos indican puntuaciones bajas y los verdes, altas. Se observa que las puntuaciones más bajas se concentran en la dimensión "Beneficios de la implementación de buenas prácticas", especialmente en los participantes 1, 2 y 5. En particular, la persona 2 mostró respuestas que oscilan entre "algunas veces sí", "la mayoría de las veces no" y "nunca", lo que evidencia la necesidad de reforzar el conocimiento sobre seguridad de la información.

Estos resultados sugieren que es necesario fortalecer las acciones de capacitación y concientización para minimizar riesgos tanto en entornos físicos como virtuales, así como promover la confianza entre colaboradores y clientes mediante la mejora continua de los procesos operativos.

En relación con los objetivos de la investigación, los hallazgos muestran que la implementación de buenas prácticas en la organización aún es débil, pero representa un área de oportunidad para optimizar la seguridad de la información dentro de la productora audiovisual. La escala Likert utilizada permitió identificar con claridad los niveles de cumplimiento y las áreas donde se deben enfocar los esfuerzos de mejora, aportando información útil para la toma de decisiones estratégicas.

Conclusión

Se puede decir que la información se ha convertido en uno de los aspectos más críticos dentro de las organizaciones en la actualidad, especialmente debido al aumento exponencial del uso de tecnologías digitales y la creciente amenaza de ataques cibernéticos. El manejo del volumen masivo de datos, tanto a nivel interno como externo, demanda que las organizaciones implementen medidas efectivas para proteger sus recursos informáticos. En este contexto, la implementación de buenas prácticas para la seguridad de la información no solo es una recomendación, sino una necesidad primordial para garantizar la integridad, confidencialidad y disponibilidad de la información crítica.

A lo largo de este proyecto de intervención, se ha evidenciado que la protección de la información no es un tema aislado, sino que está directamente vinculado con el funcionamiento eficiente de la organización. Esto se debe a que, ante la pérdida o robo de información, la operación general de la institución puede verse gravemente afectada, causando tanto daños operacionales como reputacionales. En este sentido, las buenas prácticas en seguridad informática se convierten en un pilar fundamental para la prevención de incidentes que puedan comprometer la estabilidad de una organización.

Referencias

Bauer, S., & Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *48*(3), 44–68. https://doi.org/10.1145/3130515.3130519

Castro, M. (2010). El nuevo estándar ISO para la gestión del riesgo.

Correa Sánchez, J. (2020). *Manual de buenas prácticas en seguridad de la información para entornos hospitalarios.* Universidad EIA.

Echeverry López Trujillo, C. E., & Valencia-Duque. (2017). Gobierno y gestión de TI en las entidades públicas.

Gil, Y. C. *Implementación del marco de trabajo para la ciberseguridad NIST CSF desde la perspectiva de COBIT 5.*

Gómez, E. A. (2006). *Nueva norma ISO 27001*.

Mahn, A., Marron, J., Quinn, S., & Topper, D. (2021). *Primeros pasos de NIST.*

Martín, T. de la R. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001. *Revista Universidad y Sociedad*, *13*(5), 495–506. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495

Zamora Sotelo, C. (2005). *COBIT, ITIL and ISO 17799*.