TRABAJO DE GRADO
Opción Seminario.

Ciberseguridad Organizacional para Diario Actualidad Digital S.A.S.: Análisis de Riesgos, Controles y Continuidad del Negocio

Corporación Universitaria Remington.
Facultad de Ingenierías
Ingeniería de Sistemas

Estudiante:

Gian Marco Palma Guzmán
Ingeniería de Sistemas

Jorge Leonardo Ramírez Restrepo
Docente del seminario
Seminario

2026

Dedicatoria

Dedico este trabajo, ante todo, a Dios, por ser mi guía en cada paso, por darme la fuerza necesaria en los momentos difíciles y por permitirme llegar hasta el final de esta etapa académica con éxito. A mi familia, porque su amor y comprensión fueron el sostén que me impulsó a no rendirme, y cuya motivación constante se convirtió en la base de este logro. Dedico también este esfuerzo a mis amigos, quienes con su compañía y palabras de aliento hicieron que este camino de formación fuera más ligero de recorrer. Este trabajo representa, en esencia, el resultado del esfuerzo, la perseverancia y el cariño de todas las personas que han acompañado mi vida académica y personal.

Con cariño: Gian Marco Palma Guzmán

Agradecimientos

Expreso mi agradecimiento, en primer lugar, a Dios, por ser mi fuente de sabiduría y fortaleza a lo largo de este camino, y por hacer posible que culminara con éxito este proceso. Agradezco también a la Corporación Universitaria Remington, por haberme brindado el conocimiento, los recursos y los espacios necesarios que hicieron posible mi aprendizaje. Por último, agradezco a mi familia, por su respaldo incondicional, su paciencia y su colaboración, cuya confianza y ánimo fueron fundamentales para alcanzar este logro académico.

Con gratitud: Gian Marco Palma Guzmán.

Tabla de Contenidos

1 Resumen

La transformación digital ha incrementado la dependencia de las organizaciones respecto a las tecnologías de la información, generando nuevos desafíos relacionados con la protección de los activos de información y la continuidad de las operaciones. En este contexto, el presente informe técnico analiza la situación de ciberseguridad de Diario Actualidad Digital S.A.S., un medio de comunicación regional que desarrolla gran parte de sus actividades mediante plataformas digitales, sistemas de gestión de contenidos, servicios en la nube y herramientas de comunicación electrónica.

El análisis se desarrolló con el propósito de identificar los activos de información más relevantes, reconocer las amenazas y vulnerabilidades que afectan la organización, valorar los riesgos asociados y proponer políticas, controles y estrategias orientadas a fortalecer la seguridad de la información y la continuidad del negocio. Para ello, se tomaron como referencia estándares internacionales y normativa vigente en materia de ciberseguridad, entre ellos la ISO/IEC 27001:2022, la ISO/IEC 27002:2022, la ISO 22301:2019, el NIST Cybersecurity Framework 2.0 y la legislación colombiana aplicable.

Como resultado del análisis se identificaron debilidades relacionadas con el uso de correos electrónicos personales para compartir información institucional, la utilización de credenciales compartidas para acceder al sistema de gestión de contenidos, la ausencia de autenticación multifactor, deficiencias en la gestión de privilegios de acceso, falta de programas permanentes de concienciación en ciberseguridad y la inexistencia de procedimientos formales para la gestión de incidentes. Estas situaciones incrementan la probabilidad de materialización de riesgos que pueden comprometer la confidencialidad, integridad y disponibilidad de la información.

Finalmente, el informe presenta un conjunto de recomendaciones orientadas a

fortalecer la gestión de riesgos, mejorar la protección de los activos de información, promover una cultura organizacional de ciberseguridad e implementar controles alineados con las buenas prácticas internacionales, contribuyendo así al fortalecimiento de la seguridad de la información y la continuidad operativa de la organización.

2 Palabras clave

Ciberseguridad organizacional, gestión de riesgos, activos de información, seguridad de la información, continuidad del negocio.

3 Marco conceptual y normativo

3.1 Conceptos fundamentales de ciberseguridad

El acelerado proceso de transformación digital ha generado importantes cambios en la manera en que las organizaciones administran su información, prestan sus servicios y desarrollan sus procesos internos. Actualmente, la mayoría de las empresas dependen de plataformas tecnológicas, aplicaciones web, servicios en la nube y sistemas de información para garantizar la continuidad de sus operaciones. No obstante, esta dependencia tecnológica también ha incrementado la exposición a amenazas cibernéticas que pueden comprometer la disponibilidad de los servicios, la integridad de la información y la privacidad de los datos. En este contexto, la ciberseguridad se ha consolidado como un componente estratégico para proteger los activos de información y garantizar la continuidad del negocio.

La ciberseguridad puede entenderse como el conjunto de políticas, procesos, tecnologías y prácticas orientadas a proteger los sistemas informáticos, las redes, las aplicaciones y la información frente a ataques cibernéticos, accesos no autorizados o cualquier evento que pueda afectar su funcionamiento normal. Su propósito no consiste únicamente en evitar incidentes de seguridad, sino también en desarrollar capacidades para identificarlos, responder de manera oportuna y recuperar la operación cuando estos ocurran. El NIST Cybersecurity Framework 2.0 establece que una estrategia efectiva de ciberseguridad debe contemplar funciones relacionadas con la gobernanza, la identificación de riesgos, la protección de los activos, la detección de amenazas, la respuesta ante incidentes y la recuperación de los servicios (National Institute of Standards and Technology [NIST], 2024).

En el caso de Diario Actualidad Digital S.A.S., la ciberseguridad adquiere una importancia especial debido a que gran parte de su operación depende de plataformas digitales. La publicación de noticias, la administración de suscriptores, la gestión del contenido periodístico y la comunicación entre los colaboradores se realizan mediante herramientas tecnológicas que requieren altos niveles de protección. Un incidente de seguridad podría afectar no solo la disponibilidad de la información, sino también la credibilidad del medio de comunicación y la confianza de sus lectores.

Relacionado con este concepto se encuentra la seguridad de la información, la cual busca proteger toda la información de la organización, independientemente del formato en que se encuentre almacenada o del medio utilizado para transmitirla. La norma ISO/IEC 27001:2022 define la seguridad de la información como un proceso de gestión basado en riesgos que permite establecer políticas, procedimientos y controles orientados a preservar el valor de la información y apoyar el cumplimiento de los objetivos organizacionales (International Organization for Standardization [ISO], 2022). A diferencia de la ciberseguridad, cuyo enfoque principal se orienta hacia la protección del entorno digital, la seguridad de la información abarca cualquier tipo de información, ya sea física o digital.

La seguridad de la información se fundamenta en tres principios esenciales conocidos como la triada CIA: confidencialidad, integridad y disponibilidad. Estos principios representan la base sobre la cual se diseñan las estrategias de protección de la información en cualquier organización.

La confidencialidad garantiza que únicamente las personas autorizadas puedan acceder a determinada información. Este principio busca prevenir la divulgación no autorizada de datos sensibles, evitando que terceros obtengan acceso a información

estratégica o confidencial. En el caso de Diario Actualidad Digital S.A.S., la confidencialidad resulta indispensable para proteger investigaciones periodísticas, fuentes de información, contratos comerciales, datos personales de los suscriptores y documentos internos. La utilización de correos electrónicos personales para compartir archivos o el uso compartido de credenciales representa una amenaza directa contra este principio, ya que facilita la fuga de información y dificulta el control sobre quién accede realmente a los datos.

La integridad hace referencia a la conservación de la exactitud, consistencia y confiabilidad de la información durante todo su ciclo de vida. Un sistema mantiene su integridad cuando los datos no son modificados, eliminados o alterados sin autorización. Para un medio de comunicación, este principio es especialmente relevante, ya que cualquier modificación indebida del contenido periodístico podría afectar la credibilidad institucional, generar desinformación o incluso ocasionar consecuencias legales. En consecuencia, resulta indispensable implementar mecanismos que permitan verificar la autenticidad de la información y mantener registros que faciliten la trazabilidad de las modificaciones realizadas.

Por su parte, la disponibilidad consiste en garantizar que la información, los sistemas y los servicios tecnológicos permanezcan accesibles para los usuarios autorizados cuando estos los requieran. Este principio cobra especial importancia en organizaciones cuya operación depende completamente de plataformas digitales, como ocurre con Diario Actualidad Digital S.A.S. Una interrupción del portal web, una falla en los servidores o un ataque de ransomware podrían impedir la publicación de noticias y afectar directamente la continuidad del servicio informativo. Por esta razón, la implementación de estrategias de respaldo, redundancia tecnológica y planes de

continuidad del negocio constituye una práctica indispensable para minimizar el impacto de posibles incidentes (ISO, 2019).

Otro concepto fundamental dentro de la gestión de la ciberseguridad corresponde a los activos de información. De acuerdo con la ISO/IEC 27001, un activo de información es cualquier recurso que posee valor para la organización y cuya pérdida, alteración o indisponibilidad puede afectar el cumplimiento de los objetivos institucionales (ISO, 2022). Estos activos no se limitan únicamente a los equipos informáticos, sino que también incluyen información, aplicaciones, bases de datos, infraestructura tecnológica, servicios en la nube, procesos, documentación y talento humano. En el caso de estudio, activos como el sistema de gestión de contenidos (CMS), la base de datos de suscriptores, los servidores virtuales, el correo institucional y las investigaciones periodísticas representan recursos críticos que requieren medidas de protección acordes con su nivel de importancia.

La protección de estos activos exige comprender el concepto de amenaza, entendido como cualquier evento, circunstancia o actor con la capacidad de ocasionar un impacto negativo sobre la organización. Las amenazas pueden tener origen humano, tecnológico o natural y pueden manifestarse mediante ataques de malware, ransomware, phishing, ingeniería social, accesos no autorizados, errores operativos, fallas de infraestructura o desastres naturales (NIST, 2024). La existencia de una amenaza no implica necesariamente que ocurra un incidente; sin embargo, cuando coincide con una vulnerabilidad, aumenta significativamente la probabilidad de que se materialice un riesgo.

Las vulnerabilidades representan precisamente aquellas debilidades presentes en los procesos, tecnologías o personas que pueden ser aprovechadas por una amenaza para

comprometer la seguridad de la información. Estas debilidades pueden originarse por configuraciones incorrectas, ausencia de controles, errores humanos, falta de capacitación o incumplimiento de políticas organizacionales. En Diario Actualidad Digital S.A.S. se identifican vulnerabilidades como el uso compartido de credenciales para acceder al CMS, la ausencia de autenticación multifactor, el empleo de dispositivos personales para acceder a información institucional, la utilización de correos electrónicos personales y la inexistencia de programas permanentes de concienciación en ciberseguridad. Estas condiciones incrementan la superficie de ataque y favorecen la ocurrencia de incidentes de seguridad.

La interacción entre amenazas y vulnerabilidades da lugar al concepto de riesgo. Desde la perspectiva de la ISO/IEC 27001, un riesgo corresponde a la posibilidad de que una amenaza aproveche una vulnerabilidad y genere consecuencias que afecten la confidencialidad, la integridad o la disponibilidad de los activos de información (ISO, 2022). La gestión del riesgo constituye uno de los pilares fundamentales de un Sistema de Gestión de Seguridad de la Información, ya que permite identificar los activos críticos, evaluar los posibles escenarios de ataque, estimar el impacto de un incidente y priorizar la implementación de medidas de tratamiento. En organizaciones con una alta dependencia tecnológica, como el caso analizado, una adecuada gestión del riesgo facilita la toma de decisiones y optimiza la asignación de recursos destinados a la protección de la información.

Finalmente, los controles de seguridad comprenden el conjunto de políticas, procedimientos, mecanismos técnicos y medidas administrativas implementadas para reducir la probabilidad de materialización de los riesgos identificados. La norma ISO/IEC 27002:2022 establece un amplio catálogo de controles relacionados con la

gestión de identidades, autenticación multifactor, protección de dispositivos, gestión de vulnerabilidades, cifrado de la información, monitoreo de eventos, copias de seguridad, continuidad del negocio y capacitación del personal (ISO, 2022). La aplicación de estos controles permitiría a Diario Actualidad Digital S.A.S. fortalecer su postura de seguridad, reducir las debilidades identificadas durante el análisis del caso y mejorar su capacidad de prevención y respuesta frente a incidentes cibernéticos.

En conclusión, los conceptos de ciberseguridad, seguridad de la información, confidencialidad, integridad, disponibilidad, activos de información, amenazas, vulnerabilidades, riesgos y controles de seguridad constituyen el fundamento teórico sobre el cual se desarrolla el presente informe técnico. Su adecuada comprensión permite analizar de manera integral la situación de Diario Actualidad Digital S.A.S., identificar las condiciones que pueden comprometer la seguridad de sus activos de información y proponer estrategias orientadas a fortalecer la protección de los recursos tecnológicos, garantizar la continuidad del negocio y cumplir con las buenas prácticas establecidas por los estándares internacionales y la normativa colombiana vigente.

3.2 Marco normativo

La ciberseguridad y la seguridad de la información se apoyan en normas, estándares y disposiciones legales que orientan a las organizaciones en la protección de sus activos de información. En el caso de Diario Actualidad Digital S.A.S., la aplicación de estos lineamientos resulta fundamental debido a la gran cantidad de información periodística, datos personales y recursos tecnológicos que hacen parte de su operación diaria. La adopción de estas normas no solo fortalece la protección de la información, sino que también permite gestionar los riesgos, garantizar la continuidad del negocio y cumplir con la legislación colombiana vigente (International Organization for Standardization [ISO], 2022).

Tabla 1. Normatividad aplicable

Norma o estándar	***Propósito***	***Aplicabilidad en la organización***
ISO/IEC 27001:2022	Implementar un SGSI basado en riesgos.	Protege los activos de información mediante políticas y controles de seguridad.
ISO/IEC 27002:2022	Proporcionar buenas prácticas y controles de seguridad.	Fortalece la gestión de accesos, contraseñas y protección de la información.
ISO 22301:2019	Establecer un sistema de continuidad del negocio.	Garantiza la continuidad de los servicios ante incidentes o desastres.
NIST Cybersecurity Framework (CSF) 2.0	Gestionar riesgos de ciberseguridad.	Mejora la identificación, protección, respuesta y recuperación frente a incidentes.
Ley 1581 de 2012	Regular la protección de datos personales.	Aplica al tratamiento de la información de suscriptores, empleados y usuarios.

Decreto 1377 de 2013	Reglamentar la Ley 1581 de 2012.	Define procedimientos para el tratamiento adecuado de datos personales.
Ley 1273 de 2009	Tipificar los delitos informáticos.	Protege la información y los sistemas frente a delitos cibernéticos.
CONPES 3995 de 2020	Fortalecer la confianza y seguridad digital.	Promueve la gestión del riesgo digital y la ciberseguridad organizacional.

3.3 Importancia de las normas para la organización

Las normas y estándares presentados constituyen una guía para que Diario Actualidad Digital S.A.S. fortalezca su gestión de la seguridad de la información y reduzca los riesgos asociados al uso de las tecnologías de la información. La implementación de la ISO/IEC 27001:2022 permitirá establecer un Sistema de Gestión de Seguridad de la Información basado en la mejora continua, facilitando la identificación de riesgos y la implementación de controles adecuados para proteger los activos de información (ISO, 2022).

Por otra parte, la ISO/IEC 27002:2022 complementa este proceso al ofrecer un conjunto de controles que pueden aplicarse para fortalecer aspectos como la gestión de accesos, el uso adecuado de contraseñas, la protección de los equipos, la seguridad en el correo electrónico y la administración de copias de seguridad, situaciones que presentan debilidades en el caso analizado (ISO, 2022).

Asimismo, la ISO 22301:2019 resulta especialmente importante para la organización porque permite diseñar estrategias de continuidad del negocio que

garanticen la disponibilidad de los servicios periodísticos ante posibles incidentes de ciberseguridad, fallas tecnológicas o desastres que puedan afectar la operación (ISO, 2019).

Desde la perspectiva de la gestión del riesgo, el Marco de Ciberseguridad del NIST proporciona una metodología ampliamente reconocida para identificar, proteger, detectar, responder y recuperar los sistemas frente a amenazas informáticas. Su aplicación contribuiría a fortalecer la capacidad de respuesta del periódico frente a ataques como phishing, pérdida de dispositivos o accesos no autorizados, eventos que ya se evidencian en el caso de estudio (NIST, 2024).

En cuanto a la normativa colombiana, la Ley 1581 de 2012 y el Decreto 1377 de 2013 establecen las obligaciones relacionadas con el tratamiento de los datos personales, aspecto fundamental para una organización que administra información de suscriptores, empleados y anunciantes. De igual manera, la Ley 1273 de 2009 proporciona el respaldo jurídico para prevenir y sancionar los delitos informáticos que puedan comprometer la integridad de la infraestructura tecnológica y de la información institucional (Congreso de Colombia, 2009; Congreso de Colombia, 2012).

Finalmente, el CONPES 3995 de 2020 promueve la implementación de estrategias orientadas a fortalecer la confianza y la seguridad digital en Colombia, impulsando la adopción de buenas prácticas que permitan gestionar los riesgos tecnológicos y mejorar la resiliencia de las organizaciones frente a las amenazas cibernéticas (Departamento Nacional de Planeación [DNP], 2020).

4 Marco contextual

4.1 Descripción de la organización

Diario Actualidad Digital S.A.S. es un medio de comunicación regional con más de veinticinco años de experiencia en la producción y difusión de noticias. Aunque sus operaciones iniciaron como un periódico impreso, el avance de las tecnologías de la información y los cambios en los hábitos de consumo impulsaron un proceso de transformación digital que actualmente constituye el eje principal de su funcionamiento.

La organización desarrolla sus actividades en el sector de los medios de comunicación digitales, teniendo como propósito informar a la comunidad de manera objetiva, oportuna y responsable mediante el uso de plataformas digitales y herramientas tecnológicas innovadoras. Su visión está orientada a consolidarse como uno de los medios digitales más influyentes y confiables del país, garantizando la calidad de la información y la protección de sus activos digitales como parte de su estrategia de crecimiento y sostenibilidad.

En la actualidad, la empresa cuenta con aproximadamente ciento ochenta colaboradores, entre periodistas, fotógrafos, camarógrafos, diseñadores gráficos, desarrolladores web, especialistas en marketing digital, personal administrativo y directivos. Su estructura organizacional está conformada por las áreas de Dirección General, Dirección Editorial, Unidad de Investigación Periodística, Redacción de Noticias, Producción Audiovisual, Marketing Digital, Tecnología y Desarrollo Web, Gestión de Suscriptores, Talento Humano, Contabilidad y Finanzas, Servicio al Cliente y Gestión Comercial y Publicidad. Además, dispone de corresponsales que desarrollan sus funciones de manera remota desde diferentes municipios, lo que amplía la cobertura informativa y exige mecanismos seguros para el acceso y manejo de la información institucional.

Como resultado de su proceso de transformación digital, el periódico publica contenido de manera permanente a través de su portal web y de diferentes redes sociales, alcanzando aproximadamente 350.000 visitas mensuales y una comunidad superior a 500.000 seguidores. Sus principales fuentes de ingresos provienen de la publicidad digital, las suscripciones premium, los convenios institucionales y la publicación de contenido patrocinado, actividades que dependen del funcionamiento continuo de sus plataformas tecnológicas y de la disponibilidad de la información.

Para el desarrollo de sus operaciones, Diario Actualidad Digital S.A.S. administra información de alto valor, como investigaciones periodísticas, datos personales de sus usuarios, contratos comerciales y material audiovisual. Asimismo, dispone de una infraestructura tecnológica integrada por noventa computadores de escritorio, cuarenta y cinco computadores portátiles, treinta dispositivos móviles corporativos, servidores virtuales, plataformas de almacenamiento en la nube, sistemas de gestión documental, un sistema de gestión de contenidos (CMS), plataformas de videoconferencia, redes inalámbricas corporativas, correo electrónico institucional y sistemas automáticos de respaldo de la información. Todos estos recursos son administrados por el área de Tecnología y Desarrollo Web, responsable de garantizar la disponibilidad, el mantenimiento y la seguridad de los servicios tecnológicos que soportan la operación diaria de la organización.

El crecimiento tecnológico de la empresa ha fortalecido sus procesos periodísticos, administrativos y comerciales, permitiéndole ampliar su cobertura y mejorar la interacción con sus usuarios. Sin embargo, esta evolución también ha incrementado la dependencia de los sistemas de información y la exposición a amenazas cibernéticas, haciendo necesario implementar controles de seguridad que protejan la confidencialidad, integridad y disponibilidad de los activos de información y garanticen

la continuidad de las operaciones.

4.2 Problemática identificada

A partir del análisis del caso se evidencian diversas situaciones que representan un riesgo para la seguridad de la información de Diario Actualidad Digital S.A.S. Una de las principales debilidades corresponde al uso de cuentas personales de correo electrónico para compartir información relacionada con investigaciones periodísticas, lo que incrementa la posibilidad de pérdida o divulgación no autorizada de información confidencial.

De igual manera, se identificó que varios periodistas y editores utilizan credenciales compartidas para acceder al sistema de gestión de contenidos (CMS), situación que dificulta la trazabilidad de las acciones realizadas y aumenta el riesgo de accesos indebidos. A esto se suma la inexistencia de una política formal para la clasificación de la información y el uso de computadores personales por parte de algunos corresponsales para acceder a los sistemas institucionales.

También se observaron debilidades relacionadas con la gestión de accesos, ya que no todos los equipos cuentan con autenticación multifactor, las contraseñas no cumplen criterios mínimos de seguridad y aún existen usuarios con privilegios administrativos que ya no desempeñan funciones relacionadas con el área tecnológica. Estas condiciones pueden facilitar el acceso no autorizado a los sistemas de información y comprometer la integridad de los datos.

Por otra parte, aunque la organización realiza copias de seguridad diariamente, no existen evidencias recientes de pruebas de restauración que permitan verificar su efectividad. Además, no se cuenta con un procedimiento formal para la gestión de incidentes de ciberseguridad ni con programas permanentes de capacitación dirigidos al personal. En conjunto, estas situaciones reflejan la necesidad de fortalecer la cultura de

seguridad y de implementar controles alineados con estándares internacionales como la ISO/IEC 27001 (ISO, 2022)

5 Identificación y análisis de activos

La identificación de activos de información constituye una de las etapas más importantes dentro de la gestión de la seguridad de la información, ya que permite reconocer aquellos recursos que poseen valor para la organización y que requieren medidas de protección. Un activo de información no solo corresponde a los datos almacenados en los sistemas, sino también a las personas, los equipos, las aplicaciones, los servicios y la infraestructura tecnológica que hacen posible el funcionamiento de la empresa (International Organization for Standardization [ISO], 2022).

En el caso de Diario Actualidad Digital S.A.S., los activos de información son fundamentales para el desarrollo de las actividades periodísticas, administrativas y comerciales. La organización depende de plataformas digitales para investigar, producir y publicar noticias, gestionar las suscripciones de los usuarios y administrar la información interna. Por esta razón, la pérdida, alteración o indisponibilidad de alguno de estos activos podría afectar la continuidad del negocio, disminuir la confianza de los lectores e incluso generar consecuencias legales y económicas.

La identificación de los activos permite establecer cuáles recursos son más críticos para la organización y cuáles requieren un mayor nivel de protección. Esta valoración facilita posteriormente la identificación de amenazas, vulnerabilidades y riesgos, así como la implementación de controles de seguridad acordes con la importancia de cada activo. Para determinar la criticidad de los activos se tuvo en cuenta el impacto que tendría su pérdida, alteración o indisponibilidad sobre el funcionamiento del periódico digital.

Tabla 2. Inventario de activos

Activo	***Tipo***	***Descripción***	***Criticidad***
Sistema de Gestión de Contenidos (CMS)	Software	Plataforma para crear y publicar noticias.	Alta
Base de datos de suscriptores	Información	Almacena datos personales y de suscriptores.	Alta
Portal web institucional	Servicio	Medio principal de publicación de noticias.	Alta
Servidores virtuales	Infraestructura tecnológica	Soportan el portal web y los servicios digitales.	Alta
Correo electrónico corporativo	Servicio	Canal oficial de comunicación interna.	Alta
Plataforma de almacenamiento en la nube	Servicio	Almacena y comparte información institucional.	Alta

Equipos portátiles corporativos	Hardware	Equipos utilizados por periodistas y colaboradores.	Media
Periodistas y editores	Recurso humano	Elaboran y publican el contenido periodístico.	Alta
Sistema de respaldo de información	Software / Servicio	Realiza copias de seguridad de la información.	Alta
Redes sociales institucionales	Servicio digital	Difunden noticias e interactúan con la audiencia.	Alta

Los activos clasificados con criticidad alta representan los recursos esenciales para el funcionamiento de Diario Actualidad Digital S.A.S. Entre ellos se encuentra el Sistema de Gestión de Contenidos (CMS)**,** ya que es la plataforma desde la cual se administra y publica toda la información periodística. Si este sistema deja de estar disponible o es comprometido por un atacante, la organización no podría actualizar el contenido del portal web, afectando directamente la continuidad de sus operaciones.

Otro activo de gran importancia es la base de datos de suscriptores, debido a que almacena información personal, historial de pagos y preferencias de los usuarios. La pérdida o divulgación no autorizada de estos datos podría ocasionar sanciones por incumplimiento de la Ley 1581 de 2012, afectar la confianza de los clientes y generar un impacto negativo

sobre la reputación de la organización.

Asimismo, los servidores virtuales, el portal web institucional y la plataforma de almacenamiento en la nube son fundamentales porque soportan gran parte de la infraestructura tecnológica del periódico. Una falla o ataque dirigido contra estos activos podría provocar la interrupción del servicio, la pérdida de información y dificultades para desarrollar las actividades periodísticas.

El correo electrónico corporativo también representa un activo crítico, ya que constituye el principal medio de comunicación entre las diferentes áreas de la organización. En el caso de estudio se evidenció que algunos colaboradores utilizan cuentas personales para compartir información institucional, situación que incrementa el riesgo de fuga de información y ataques de phishing.

Por otra parte, los periodistas y editores son considerados activos de información porque poseen conocimiento especializado y son responsables de producir contenido de alto valor para la organización. Su experiencia, acceso a fuentes confidenciales y manejo de información sensible hacen que desempeñen un papel esencial dentro de los procesos del periódico.

Finalmente, aunque los equipos portátiles corporativos fueron clasificados con criticidad media, siguen siendo relevantes debido a que son utilizados por corresponsales y periodistas durante desplazamientos. El caso de estudio demuestra que la pérdida de uno de estos equipos puede comprometer información confidencial si no existen mecanismos adecuados de protección, como el cifrado de la información o la autenticación multifactor.

En conjunto, estos activos constituyen la base tecnológica, operativa y humana que permite el funcionamiento de Diario Actualidad Digital S.A.S. Por esta razón, la

organización debe priorizar su protección mediante políticas de seguridad, controles técnicos y procedimientos de gestión de riesgos que reduzcan la probabilidad de incidentes y garanticen la continuidad de sus operaciones.

6 Análisis de amenazas y vulnerabilidades

La identificación de amenazas y vulnerabilidades constituye una etapa esencial dentro de la gestión de riesgos en seguridad de la información, ya que permite reconocer los factores que pueden comprometer los activos críticos de una organización. Una amenaza es cualquier evento, acción o circunstancia con capacidad de causar un daño a un activo de información, mientras que una vulnerabilidad corresponde a una debilidad que puede ser aprovechada por una amenaza para materializar un incidente de seguridad (International Organization for Standardization [ISO], 2022).

En el caso de Diario Actualidad Digital S.A.S., el análisis realizado evidencia que la organización enfrenta diferentes amenazas derivadas tanto de factores tecnológicos como humanos. La transformación digital del periódico ha incrementado la dependencia de plataformas tecnológicas para la producción y publicación de noticias, lo que exige la implementación de controles que permitan proteger la información periodística, los datos personales de los suscriptores y los servicios digitales que soportan la operación diaria.

Las situaciones identificadas durante el diagnóstico inicial demuestran que existen debilidades relacionadas con la gestión de accesos, el manejo de la información, la capacitación del personal y la respuesta ante incidentes. Estas vulnerabilidades incrementan la probabilidad de que amenazas como el phishing, el acceso no autorizado, la pérdida de información o la interrupción de los servicios afecten la continuidad del negocio y la reputación de la organización.

Tabla 3. *Amenazas y vulnerabilidades*

Activo	***Amenaza***	***Vulnerabilidad***
Sistema de Gestión de Contenidos (CMS)	Acceso no autorizado y alteración de contenidos.	Credenciales compartidas entre usuarios.
Base de datos de suscriptores	Robo o fuga de información.	Falta de clasificación y protección de datos.
Portal web institucional	Ataques DDoS y pérdida de disponibilidad.	Ausencia de planes de continuidad e incidentes.
Servidores virtuales	Malware, ransomware y accesos no autorizados.	Falta de autenticación multifactor y controles de acceso.
Correo electrónico corporativo	Phishing y robo de credenciales.	Uso de cuentas personales y poca capacitación.
Plataforma de almacenamiento en la nube	Pérdida o divulgación de información confidencial.	Gestión inadecuada de permisos y almacenamiento inseguro.
Equipos portátiles corporativos	Robo o pérdida de dispositivos.	Falta de cifrado y protección avanzada.

Periodistas y editores	Ingeniería social y manipulación de información.	Escasa capacitación en ciberseguridad.
Sistema de respaldo de información	Pérdida definitiva de información.	No se realizan pruebas periódicas de restauración.
Redes sociales institucionales	Suplantación de identidad y publicaciones no autorizadas.	Controles de acceso insuficientes y ausencia de autenticación multifactor.

El análisis evidencia que las situaciones de mayor riesgo están relacionadas con la gestión de identidades y accesos. El uso compartido de credenciales dentro del Sistema de Gestión de Contenidos (CMS) dificulta la identificación de responsabilidades y facilita que personas no autorizadas puedan modificar o eliminar información publicada en el portal institucional. Esta situación representa un riesgo elevado debido al impacto que tendría sobre la credibilidad del medio de comunicación y la confianza de sus lectores.

Otro aspecto crítico corresponde al manejo del correo electrónico corporativo. El caso de estudio indica que algunos periodistas utilizan cuentas personales para intercambiar información relacionada con investigaciones periodísticas, además de existir antecedentes de intentos de phishing dirigidos a colaboradores de la organización. Estas condiciones aumentan significativamente la probabilidad de que un atacante obtenga credenciales institucionales o acceda a información confidencial mediante técnicas de ingeniería social.

La base de datos de suscriptores constituye uno de los activos más sensibles de la

organización, ya que contiene información personal y registros relacionados con pagos y preferencias de los usuarios. La ausencia de políticas claras para la clasificación de la información y el tratamiento de datos incrementa el riesgo de fuga de información y de incumplimiento de la Ley 1581 de 2012, lo que podría generar sanciones legales y afectar la reputación institucional.

También resulta preocupante la situación del sistema de respaldo de información. Aunque la organización realiza copias de seguridad diariamente, no existen evidencias de pruebas recientes que permitan verificar la correcta recuperación de la información. En caso de un ataque de ransomware, una falla tecnológica o un desastre, esta vulnerabilidad podría impedir la restauración de los datos críticos y afectar la continuidad del negocio.

Por otra parte, la falta de autenticación multifactor, la permanencia de usuarios con privilegios administrativos innecesarios y la ausencia de procedimientos documentados para responder a incidentes demuestran debilidades importantes en la gestión de la seguridad. Estas situaciones incrementan la probabilidad de accesos no autorizados y reducen la capacidad de la organización para detectar, contener y recuperar oportunamente un incidente de ciberseguridad.

Finalmente, el análisis permite concluir que el principal factor de riesgo no está relacionado únicamente con la tecnología, sino también con el componente humano. La falta de capacitación, el uso inadecuado de herramientas tecnológicas y el desconocimiento de buenas prácticas de seguridad facilitan la materialización de amenazas como el phishing, la pérdida de información y la divulgación de datos confidenciales. Por esta razón, además de implementar controles técnicos, será necesario fortalecer la cultura organizacional en materia de ciberseguridad mediante políticas, procedimientos y programas permanentes de sensibilización para todos los colaboradores.

7 Análisis y gestión de riesgos

La gestión de riesgos es un proceso fundamental dentro de la seguridad de la información, ya que permite identificar, evaluar y tratar aquellos eventos que pueden afectar el cumplimiento de los objetivos de una organización. En un entorno digital como el de Diario Actualidad Digital S.A.S., donde gran parte de las actividades dependen de plataformas tecnológicas y del manejo de información sensible, resulta indispensable conocer cuáles son los riesgos más relevantes para establecer controles que reduzcan su probabilidad de ocurrencia y minimicen su impacto.

El análisis realizado en este informe parte de la información obtenida durante el estudio del caso, donde se identificaron diversas amenazas y vulnerabilidades relacionadas con el uso de tecnologías de la información, la gestión de accesos, el manejo de datos personales y la cultura organizacional en materia de ciberseguridad. Estas situaciones evidencian que la organización enfrenta riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información, comprometiendo tanto la continuidad de sus operaciones como la confianza de sus usuarios.

La norma ISO/IEC 27001:2022 establece que la gestión de riesgos debe formar parte del Sistema de Gestión de Seguridad de la Información (SGSI), permitiendo a las organizaciones tomar decisiones basadas en el nivel de riesgo identificado y en la eficacia de los controles implementados (International Organization for Standardization [ISO], 2022). De igual manera, el Marco de Ciberseguridad del NIST propone que la identificación y evaluación de riesgos constituye una actividad permanente para fortalecer la capacidad de respuesta frente a incidentes de seguridad (National Institute of Standards and Technology [NIST], 2024).

Metodología de análisis

Para valorar los riesgos de Diario Actualidad Digital S.A.S. se utilizó una metodología cualitativa basada en la relación entre impacto **y** probabilidad, siguiendo las recomendaciones establecidas por la ISO/IEC 27005, la ISO/IEC 27001 y el NIST Cybersecurity Framework (ISO, 2022; NIST, 2024).

En primer lugar, se identificaron los activos más importantes de la organización y posteriormente se asociaron las amenazas y vulnerabilidades detectadas durante el diagnóstico inicial. A partir de esta información se realizó una valoración considerando dos criterios:

Impacto: corresponde a las consecuencias que tendría la materialización del riesgo sobre la organización. Se evaluó teniendo en cuenta aspectos como la interrupción de los servicios, las pérdidas económicas, el incumplimiento de obligaciones legales, el daño en la reputación y la afectación de la información institucional.

Probabilidad: hace referencia a la posibilidad de que el riesgo ocurra, considerando las vulnerabilidades presentes en la organización, la existencia de controles de seguridad y los antecedentes descritos en el caso de estudio.

Con base en estos dos criterios, el nivel de riesgo se clasificó como Alto, Medio o Bajo. Los riesgos con impacto y probabilidad altos fueron considerados prioritarios, debido a que requieren la implementación inmediata de controles de seguridad para reducir su nivel de exposición.

Tabla 4. Matriz de riesgos

Riesgo	***Impacto***	***Probabilidad***	***Nivel***
Acceso no autorizado al CMS por credenciales compartidas	Alto	Alto	Alto
Fuga de información de la base de datos de suscriptores	Alto	Alto	Alto
Ataque de phishing al correo corporativo	Alto	Alto	Alto
Interrupción del portal web por ataques DDoS	Alto	Medio	Alto
Pérdida de información por fallas en las copias de seguridad	Alto	Medio	Alto
Robo o pérdida de equipos portátiles	Medio	Medio	Medio
Acceso indebido por falta de autenticación multifactor	Alto	Alto	Alto

Publicación no autorizada en redes sociales	Medio	Medio	Medio
Alteración de información periodística por errores humanos	Alto	Medio	Alto
Incumplimiento de la Ley 1581 de 2012	Alto	Medio	Alto

La matriz de riesgos evidencia que la mayoría de los riesgos identificados presentan un nivel alto, debido a la importancia de los activos de información administrados por Diario Actualidad Digital S.A.S. y a las vulnerabilidades detectadas durante el análisis del caso. La valoración de cada riesgo se realizó considerando la relación entre la amenaza identificada, las debilidades existentes en la organización, la probabilidad de ocurrencia y el impacto que tendría sobre la confidencialidad, integridad y disponibilidad de la información.

El riesgo asociado al acceso no autorizado al Sistema de Gestión de Contenidos (CMS) mediante el uso de credenciales compartidas fue clasificado con un impacto alto y una probabilidad alta, debido a que esta práctica impide la correcta identificación de los usuarios, dificulta la trazabilidad de las acciones realizadas y facilita el acceso indebido al sistema. La materialización de este riesgo podría ocasionar la modificación o eliminación no autorizada de información periodística y afectar la continuidad de las

operaciones.

La fuga de información de la base de datos de suscriptores fue valorada con impacto alto y probabilidad media. El impacto es alto porque la base de datos contiene información personal, historial de pagos y otros datos sensibles cuya divulgación podría generar sanciones legales por incumplimiento de la Ley 1581 de 2012, además de afectar la confianza de los usuarios y la reputación institucional. La probabilidad se considera media porque, aunque existen mecanismos básicos de protección, aún se presentan debilidades relacionadas con la gestión de accesos y el manejo de la información.

El ataque de phishing dirigido al correo electrónico corporativo presenta un impacto alto y una probabilidad alta, debido a que en el caso de estudio ya se evidenció un intento de fraude mediante correo electrónico y se identificó la ausencia de programas permanentes de capacitación en ciberseguridad. Estas condiciones aumentan la posibilidad de compromiso de credenciales y de acceso no autorizado a los sistemas institucionales.

La interrupción del portal web por ataques de denegación de servicio (DDoS) fue clasificada con impacto alto y probabilidad media. El impacto es alto porque el portal web constituye el principal canal de difusión de noticias y de interacción con los usuarios. La probabilidad se considera media debido a que este tipo de ataques depende de factores externos, aunque puede reducirse mediante controles de protección perimetral y servicios especializados de mitigación.

La pérdida de información por fallas en las copias de seguridad fue valorada con impacto alto y probabilidad media. Aunque la organización realiza respaldos periódicos, la ausencia de pruebas de restauración impide garantizar que la información pueda

recuperarse de manera efectiva ante un incidente, lo que podría afectar la continuidad del negocio.

El riesgo de robo o pérdida de equipos portátiles con información institucional presenta un impacto medio y una probabilidad alta, debido a que estos dispositivos son utilizados por periodistas y corresponsales durante desplazamientos frecuentes. La falta de mecanismos como el cifrado de la información o la autenticación multifactor incrementa la posibilidad de acceso indebido a los datos almacenados.

La ausencia de autenticación multifactor fue clasificada con impacto alto y probabilidad alta, ya que los sistemas dependen principalmente del uso de contraseñas. Esta situación incrementa la exposición a ataques de fuerza bruta, robo de credenciales e ingeniería social, permitiendo accesos no autorizados a los recursos tecnológicos de la organización.

La publicación no autorizada en las redes sociales institucionales presenta un impacto medio y una probabilidad media. Aunque este riesgo no compromete directamente todos los sistemas de información, puede afectar la imagen institucional, generar desinformación y disminuir la confianza de la audiencia si no existen controles adecuados sobre las cuentas oficiales.

La alteración de la información periodística por errores humanos fue valorada con impacto medio y probabilidad alta. Esta valoración obedece a que la elaboración y publicación de contenidos depende de múltiples usuarios, por lo que la ausencia de procedimientos de validación y revisión puede ocasionar errores que afecten la calidad y credibilidad de la información publicada.

Finalmente, el incumplimiento de la Ley 1581 de 2012 por el tratamiento

inadecuado de datos personales fue clasificado con impacto alto y probabilidad media. El impacto es elevado debido a las posibles sanciones legales, económicas y reputacionales derivadas de una gestión inadecuada de la información personal de los suscriptores. La probabilidad se considera media porque la organización dispone de algunos controles, aunque todavía presenta oportunidades de mejora en la gestión de datos y en la aplicación de políticas de seguridad.

En conjunto, la valoración realizada demuestra que los riesgos con mayor prioridad corresponden a aquellos relacionados con la gestión de accesos, la protección de la información, el uso seguro del correo electrónico y la disponibilidad de los servicios tecnológicos. Estos resultados justifican la implementación de políticas, controles y mecanismos de monitoreo orientados a reducir la probabilidad de ocurrencia de los riesgos identificados y fortalecer la capacidad de respuesta de la organización frente a incidentes de ciberseguridad.

8 Políticas y controles de seguridad

La implementación de políticas y controles de seguridad constituye una de las estrategias más importantes para proteger los activos de información de una organización. Una política de seguridad establece las directrices que deben seguir los colaboradores para garantizar el uso adecuado de la información y de los recursos tecnológicos, mientras que los controles de seguridad son las medidas técnicas, físicas y administrativas que permiten reducir la probabilidad de que un riesgo se materialice.

En el caso de Diario Actualidad Digital S.A.S., el análisis realizado evidenció debilidades relacionadas con el manejo de credenciales, la protección de los datos personales, la gestión de accesos, el uso de dispositivos corporativos y la respuesta ante

incidentes. Estas situaciones hacen necesaria la implementación de políticas institucionales que definan responsabilidades, establezcan buenas prácticas y promuevan una cultura organizacional orientada a la seguridad de la información.

De acuerdo con la ISO/IEC 27001:2022, las organizaciones deben implementar políticas de seguridad como parte de su Sistema de Gestión de Seguridad de la Información (SGSI), garantizando que todos los colaboradores conozcan las responsabilidades asociadas con la protección de los activos de información (International Organization for Standardization [ISO], 2022). Asimismo, la ISO/IEC 27002:2022 recomienda la implementación de controles que permitan fortalecer la gestión de accesos, la protección de los datos y la continuidad de las operaciones.

Tabla 5. Políticas de seguridad

Política	***Objetivo***	***Riesgo asociado***
Política de gestión de contraseñas	Fortalecer la seguridad de las contraseñas.	Accesos no autorizados y robo de credenciales.
Política de control de accesos	Limitar el acceso según el rol del usuario.	Uso indebido de privilegios e información confidencial.
Política de clasificación de la información	Proteger la información según su nivel de sensibilidad.	Divulgación de información sensible.

Política de uso aceptable de recursos tecnológicos	Regular el uso de equipos, correo e Internet.	Fuga de información y uso inadecuado de recursos.
Política de copias de seguridad	Garantizar la disponibilidad y recuperación de la información.	Pérdida de información crítica.
Política de respuesta a incidentes	Definir acciones para atender incidentes de seguridad.	Respuesta tardía ante incidentes.
Política de capacitación en ciberseguridad	Sensibilizar al personal sobre buenas prácticas.	Errores humanos e ingeniería social.
Política de dispositivos móviles y trabajo remoto	Regular el acceso desde dispositivos externos.	Pérdida de dispositivos y accesos inseguros.

Controles propuestos

Tabla 6. Controles de seguridad

Riesgo	***Control***	***Justificación***
Acceso no autorizado al CMS	Implementar autenticación multifactor (MFA).	Reduce accesos no autorizados.
Uso compartido de credenciales	Asignar cuentas individuales y prohibir compartir credenciales.	Mejora la trazabilidad y la responsabilidad.
Ataques de phishing	Capacitación y simulaciones de phishing.	Disminuye los errores humanos.
Robo de credenciales	Implementar filtros antispam, SPF, DKIM y DMARC.	Protege el correo corporativo.
Fuga de información de suscriptores	Cifrado de datos y gestión de privilegios.	Protege la información confidencial.
Pérdida de información	Copias de seguridad y pruebas de restauración.	Garantiza la recuperación de la información.
Robo de equipos portátiles	Inventario, guayas de seguridad y almacenamiento seguro.	Reduce el riesgo de pérdida o hurto.

Acceso físico a servidores	Control de ingreso con biometría y videovigilancia.	Evita accesos no autorizados.
Incendios o fallas eléctricas	UPS, sistema contra incendios y control ambiental.	Protege la infraestructura tecnológica.
Respuesta ineficiente ante incidentes	Procedimiento formal de respuesta y asignación de responsables.	Reduce el impacto de los incidentes.

Las políticas y controles propuestos responden directamente a los riesgos identificados durante el análisis realizado para Diario Actualidad Digital S.A.S. En primer lugar, las políticas de seguridad proporcionan un marco de actuación para todos los colaboradores, estableciendo responsabilidades claras sobre el uso de los recursos tecnológicos, el tratamiento de la información y la gestión de incidentes. Esto favorece el cumplimiento de las normas internas y reduce la probabilidad de que los riesgos se materialicen por desconocimiento o incumplimiento de los procedimientos.

Los controles administrativos fortalecen la gestión organizacional mediante la definición de procedimientos, la capacitación del personal y la asignación de responsabilidades. En el caso analizado, estas medidas son fundamentales porque varios de los riesgos detectados están relacionados con el factor humano, como el uso compartido de credenciales, la falta de sensibilización frente al phishing y la ausencia de procedimientos para responder a incidentes de seguridad.

Por otra parte, los controles técnicos buscan proteger los sistemas y la información mediante herramientas tecnológicas. La implementación de autenticación multifactor, cifrado de bases de datos, copias de seguridad automatizadas y mecanismos de protección del correo electrónico permitirá reducir significativamente el riesgo de accesos no autorizados, pérdida de información y ataques cibernéticos.

Finalmente, los controles físicos complementan las medidas anteriores al proteger la infraestructura tecnológica frente a amenazas como robos, incendios, fallas eléctricas o accesos físicos no autorizados. La instalación de sistemas de videovigilancia, controles biométricos, UPS y equipos contra incendios contribuirá a garantizar la disponibilidad de los servicios y la continuidad de las operaciones.

En conjunto, la aplicación de estas políticas y controles permitirá fortalecer la seguridad de la información en Diario Actualidad Digital S.A.S., reducir la probabilidad de ocurrencia de incidentes, minimizar su impacto y avanzar hacia un modelo de gestión alineado con las buenas prácticas establecidas por la ISO/IEC 27001:2022 y la ISO/IEC 27002:2022. Además, estas medidas contribuirán al cumplimiento de la legislación colombiana en materia de protección de datos personales y seguridad de la información, incrementando la confianza de los usuarios y garantizando la continuidad de las actividades de la organización.

Las recomendaciones propuestas para Diario Actualidad Digital S.A.S. responden a las necesidades identificadas durante el análisis de activos, amenazas, vulnerabilidades y riesgos desarrollado en este informe. Su finalidad es fortalecer la seguridad de la información mediante la implementación de políticas, procedimientos y controles que permitan proteger los activos críticos de la organización, reducir la probabilidad de ocurrencia de incidentes y garantizar la continuidad de las operaciones.

La ISO/IEC 27001:2022 establece que las organizaciones deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la identificación y el tratamiento de los riesgos, promoviendo la mejora continua de los controles de seguridad (International Organization for Standardization [ISO], 2022).

Las políticas de seguridad propuestas constituyen la base para establecer responsabilidades claras sobre el uso de la información y de los recursos tecnológicos. Su implementación permitirá fortalecer la gestión organizacional, promover el cumplimiento de las normas internas y reducir riesgos relacionados con el acceso no autorizado, la divulgación de información confidencial y el incumplimiento de las disposiciones legales sobre protección de datos personales. Estas acciones se encuentran alineadas con las buenas prácticas definidas en la ISO/IEC 27002:2022, la cual proporciona directrices para la selección e implementación de controles de seguridad de la información (ISO, 2022).

De igual manera, los controles administrativos, técnicos y físicos complementan las políticas de seguridad al establecer mecanismos específicos para prevenir, detectar y responder ante posibles incidentes de ciberseguridad. Los controles administrativos fortalecen la gestión mediante procedimientos documentados, programas de capacitación y asignación de responsabilidades; los controles técnicos protegen los sistemas mediante herramientas como la autenticación multifactor, el cifrado de la información y el monitoreo continuo; mientras que los controles físicos buscan proteger la infraestructura tecnológica frente a amenazas como robos, incendios o accesos no autorizados. El NIST Cybersecurity Framework 2.0 destaca la importancia de combinar estos tipos de controles para fortalecer la capacidad de las organizaciones frente a los riesgos cibernéticos (National Institute of Standards and Technology [NIST], 2024).

Asimismo, la implementación de estas recomendaciones contribuirá al cumplimiento de la legislación colombiana en materia de protección de datos personales, especialmente lo establecido en la Ley 1581 de 2012, la cual exige a las organizaciones adoptar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información personal bajo su responsabilidad (Congreso de Colombia, 2012). Esto permitirá proteger adecuadamente los datos de los suscriptores y fortalecer la confianza de los usuarios en los servicios ofrecidos por la organización.

Finalmente, la aplicación de estas recomendaciones facilitará el desarrollo de procesos orientados a la gestión de incidentes y la continuidad del negocio, permitiendo que Diario Actualidad Digital S.A.S. responda de manera organizada ante eventos que puedan afectar sus operaciones. En este sentido, la ISO 22301:2019 resalta la importancia de establecer planes que permitan mantener la continuidad de los procesos críticos y reducir el impacto de posibles interrupciones en los servicios (ISO, 2019). Por esta razón, en el siguiente apartado se presenta una estrategia básica de gestión de incidentes y continuidad del negocio, como complemento de las políticas y controles de seguridad propuestos.

9 Gestión de incidentes y continuidad del negocio

La gestión de incidentes y la continuidad del negocio son procesos fundamentales dentro de la seguridad de la información, ya que permiten a las organizaciones responder de forma oportuna ante eventos que comprometan la confidencialidad, integridad y disponibilidad de los activos de información. En una empresa como Diario Actualidad Digital S.A.S., cuya operación depende de plataformas digitales para la publicación de noticias y la administración de suscriptores, un incidente

de ciberseguridad puede afectar significativamente la prestación de los servicios, la confianza de los usuarios y la reputación institucional.

Con base en los riesgos identificados en el presente informe, es necesario establecer una estrategia que permita responder de manera organizada frente a incidentes de seguridad y, al mismo tiempo, garantizar que las actividades esenciales de la organización continúen funcionando con el menor impacto posible. Estas acciones se encuentran alineadas con las recomendaciones de la ISO 22301:2019, la ISO/IEC 27001:2022 y el NIST Cybersecurity Framework 2.0, las cuales promueven la preparación, respuesta, recuperación y mejora continua frente a incidentes de seguridad (ISO, 2019; ISO, 2022; NIST, 2024).

10 Estrategia general de respuesta a incidentes

La estrategia de respuesta a incidentes tiene como finalidad minimizar las consecuencias de un evento de ciberseguridad mediante acciones previamente definidas. Para Diario Actualidad Digital S.A.S. es importante contar con procedimientos que permitan identificar rápidamente un incidente, contener sus efectos, eliminar la causa del problema y recuperar la operación normal en el menor tiempo posible.

Tabla 7. Incidentes potenciales

Incidente	***Descripción***	***Impacto***

Ataque de phishing	Robo de credenciales mediante correos fraudulentos.	Alto
Acceso no autorizado al CMS	Modificación o eliminación de contenido sin autorización.	Alto
Fuga de información de suscriptores	Exposición de datos personales de los usuarios.	Alto
Ataque de ransomware	Cifrado de sistemas y bloqueo del acceso a la información.	Alto
Caída del portal web	Interrupción del servicio por ataques o fallas.	Alto
Robo de equipos portátiles	Pérdida de dispositivos con información institucional.	Medio
Falla en las copias de seguridad	Imposibilidad de recuperar la información.	Alto

Publicación no autorizada en redes sociales	Difusión de contenido falso o no autorizado.	Medio

Tabla 8. Plan básico de respuesta

Fase	***Acción***
Preparación	Elaborar procedimientos de respuesta, definir responsables, mantener actualizados los respaldos y capacitar al personal en ciberseguridad.
Detección	Identificar el incidente mediante herramientas de monitoreo, registros de eventos o reportes realizados por los usuarios.
Contención	Aislar los sistemas afectados, bloquear cuentas comprometidas y evitar la propagación del incidente.
Erradicación	Eliminar el malware, corregir vulnerabilidades, actualizar los sistemas y restablecer configuraciones seguras.
Recuperación	Restaurar la información desde las copias de seguridad, verificar el funcionamiento de los servicios y habilitar nuevamente la operación.
Comunicación	Informar oportunamente a la dirección, a los usuarios afectados y, cuando corresponda, a las autoridades competentes.
Lecciones aprendidas	Documentar el incidente, analizar sus causas y actualizar políticas, procedimientos y controles para evitar que vuelva a ocurrir.

Ante la ocurrencia de un incidente de ciberseguridad, Diario Actualidad Digital S.A.S. deberá activar el plan de respuesta establecido, iniciando con la identificación y detección del incidente mediante herramientas de monitoreo, registros de eventos o reportes realizados por los usuarios. Posteriormente, se deberán aplicar las acciones de contención para evitar la propagación del incidente y reducir su impacto sobre los activos de información y los servicios críticos de la organización.

Una vez controlada la situación, será necesario eliminar la causa del incidente, corregir las vulnerabilidades identificadas y restaurar los sistemas afectados utilizando las copias de seguridad previamente verificadas. Antes de restablecer completamente la operación, deberá comprobarse la integridad de la información y el correcto funcionamiento de las plataformas tecnológicas.

Para garantizar la continuidad del negocio, la organización deberá priorizar la recuperación de los servicios esenciales, como el portal web institucional, el Sistema de Gestión de Contenidos (CMS), la base de datos de suscriptores y el correo electrónico corporativo. Asimismo, será indispensable mantener respaldos actualizados, realizar pruebas periódicas de restauración, definir responsables para la atención de incidentes y desarrollar programas permanentes de capacitación para el personal. Estas acciones permitirán reducir el tiempo de interrupción de los servicios, fortalecer la capacidad de respuesta institucional y asegurar la continuidad de las operaciones frente a eventos de ciberseguridad.

11 Conclusiones

El desarrollo del presente informe permitió identificar los principales activos de información, amenazas, vulnerabilidades y riesgos que enfrenta Diario Actualidad Digital S.A.S., evidenciando la necesidad de fortalecer la gestión de la seguridad de la información mediante la implementación de políticas, controles y procedimientos acordes con las necesidades de la organización. Asimismo, el análisis realizado permitió priorizar los riesgos más relevantes y proponer medidas orientadas a proteger los activos críticos, mejorar la capacidad de respuesta ante incidentes y favorecer la continuidad de las operaciones. En conjunto, la aplicación de los conceptos, metodologías y estándares estudiados durante el seminario permitió formular una propuesta de mejora alineada con los objetivos de la organización y con las buenas prácticas de la gestión de la seguridad de la información.

12 Referencias

Congreso de Colombia. (2009). *Ley 1273 de 2009, por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos"*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de Colombia. (2012). *Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Departamento Nacional de Planeación. (2020). *Documento CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital*. https://colaboracion.dnp.gov.co

Congreso de Colombia. (2013). *Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre protección de datos personales.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements*.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*.

International Organization for Standardization. (2022). *ISO/IEC 27005 Information security risk management*.

National Institute of Standards and Technology. (2024). *Cybersecurity Framework (CSF) 2.0*. https://www.nist.gov/cyberframework