TRABAJO DE GRADO
Opción Seminario.

Título del trabajo

Informe Técnico de Ciberseguridad Organizacional para Diario Actualidad Digital S.A.S.: Análisis de Riesgos, Vulnerabilidades y Estrategias de Protección de la Información

Corporación Universitaria Remington.

Nombre de la facultad: Ingenierías

Nombre del programa académico: Ingeniería de Sistemas

Nombres de los estudiantes autores del trabajo de grado.

Michael Taborda Duarte

Sebastián Salazar Contreras

Yerling Vargas Rivas

Jorge Leonardo Ramírez Restrepo - docente del seminario.

Seminario

2026

Tabla de Contenidos

Resumen

El presente informe técnico desarrolla un análisis de ciberseguridad para Diario Actualidad Digital S.A.S., un medio de comunicación regional que ha migrado la mayor parte de sus operaciones al entorno digital. La organización enfrenta debilidades en la gestión de la seguridad de la información, como el uso compartido de credenciales del Sistema de Gestión de Contenidos (CMS), la ausencia de autenticación multifactor, el uso de correos personales para investigaciones periodísticas y la falta de procedimientos documentados para la respuesta ante incidentes. Estas condiciones exponen activos críticos como la base de datos de suscriptores, el portal web y las investigaciones periodísticas a riesgos de acceso no autorizado, fuga de información e interrupción del servicio.

El objetivo del informe es identificar los principales activos de información, analizar las amenazas y vulnerabilidades, evaluar los riesgos asociados y proponer controles de seguridad que fortalezcan la postura de ciberseguridad de la organización. Para ello, se aplicó la metodología de gestión de riesgos de la norma ISO/IEC 27005:2022 y se tomaron como referencia los estándares ISO/IEC 27001:2022, ISO/IEC 27002:2022 y el Marco de Ciberseguridad del NIST.

Como resultados principales, se elaboró un inventario de activos con su nivel de criticidad, se identificaron nueve amenazas con sus respectivas vulnerabilidades, y se construyó una matriz de riesgos que prioriza aquellos de nivel alto. Con base en este

análisis, se formularon siete políticas de seguridad y siete controles técnicos y administrativos orientados a mitigar los riesgos detectados. Adicionalmente, se propuso un plan básico de respuesta a incidentes y un conjunto de recomendaciones para fortalecer la cultura organizacional en ciberseguridad, destacando la necesidad de capacitación continua y el compromiso de la alta dirección. El informe concluye que la implementación de estas medidas contribuirá a proteger la confidencialidad de las fuentes periodísticas, garantizar la disponibilidad del portal web y preservar la credibilidad del medio ante sus lectores y anunciantes.

Palabras clave

ciberseguridad organizacional, gestión de riesgos, activos de información, políticas de seguridad, controles de acceso.

Marco conceptual y normativo

El presente capítulo establece las bases teóricas y normativas que sustentan el desarrollo del informe técnico de ciberseguridad para Diario Actualidad Digital S.A.S. En esta sección se presentan los conceptos fundamentales relacionados con la seguridad de la información y la gestión de riesgos, los cuales permiten comprender la importancia de proteger los activos de información frente a las amenazas que pueden afectar la continuidad de las operaciones. Asimismo, se describen los principales estándares internacionales y la normativa colombiana aplicables al caso de estudio, los cuales sirven como guía para la identificación de riesgos, la implementación de protocolos de seguridad y el fortalecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI). El desarrollo de este marco conceptual y normativo proporciona el soporte técnico necesario para el análisis realizado en los capítulos posteriores y permite fundamentar las recomendaciones propuestas para mejorar la postura de ciberseguridad de la organización.

Conceptos fundamentales de ciberseguridad

La transformación digital ha permitido que las organizaciones optimicen sus procesos, amplíen la disponibilidad de sus servicios y mejoren la interacción con clientes y usuarios. Sin embargo, este avance tecnológico también ha incrementado la exposición a riesgos asociados con ataques informáticos, fuga de información, interrupción de servicios y otros incidentes que pueden afectar el funcionamiento de las organizaciones. Es en este escenario donde la ciberseguridad emerge como la respuesta estratégica a estas situaciones. Dado que su propósito principal consiste en prevenir, detectar, responder y

recuperar los servicios tecnológicos frente a incidentes de seguridad, minimizando su impacto sobre la organización (NIST, 2024).

De acuerdo con la norma ISO/IEC 27001:2022, la seguridad de la información tiene como finalidad preservar la confidencialidad, la integridad y la disponibilidad de la información, principios conocidos como la triada CIA, fundamentales para garantizar el correcto funcionamiento de cualquier organización.

La confidencialidad asegura que la información únicamente sea conocida por personas autorizadas, evitando el acceso, divulgación o utilización indebida de datos sensibles. Por otro lado, la integridad hace referencia a la protección de la información frente a modificaciones no autorizadas, garantizando que los datos permanezcan completos, exactos y confiables durante todo su ciclo de vida. El tercer principio corresponde a la disponibilidad, entendida como la capacidad de garantizar que la información y los servicios permanezcan accesibles cuando sean requeridos por los usuarios autorizados (ISO/IEC 27000, 2018).

Dentro de la gestión de la seguridad de la información, los activos de información representan todos aquellos recursos que poseen valor para la organización y que requieren protección. Estos activos incluyen bases de datos, aplicaciones, infraestructura tecnológica, servicios en la nube y otros recursos. La identificación y clasificación de estos activos constituye la base para desarrollar una adecuada gestión del riesgo (ISO/IEC 27005, 2022).

Dichos activos de información pueden verse afectados por diferentes amenazas, entendidas como cualquier circunstancia, evento o actor con capacidad para ocasionar un incidente de seguridad. Estas amenazas pueden ser de origen natural, tecnológico o humano e incluyen ataques de malware, ingeniería social, fallas técnicas, errores humanos, incendios (NIST, 2024). Sin embargo, para que una amenaza pueda materializarse normalmente debe aprovecharse de una vulnerabilidad, definida como una debilidad presente en un sistema, proceso o recurso que puede ser explotada para comprometer la seguridad de la información. Ejemplos de vulnerabilidades incluyen contraseñas débiles, ausencia de autenticación multifactor, software desactualizado, falta de políticas de seguridad (ISO/IEC 27002, 2022).

La interacción entre amenazas y vulnerabilidades da origen al riesgo, entendido como la posibilidad de que un evento afecte los objetivos de la organización. Según la ISO/IEC 27005:2022, el riesgo se determina considerando tanto la probabilidad de ocurrencia de una amenaza como el impacto que esta puede generar sobre los activos de información. Para disminuir la probabilidad de ocurrencia de incidentes y minimizar sus consecuencias, las organizaciones implementan controles de seguridad, los cuales pueden ser de carácter administrativo, técnico o físico. Entre los controles más utilizados se encuentran las políticas de seguridad de la información, la autenticación multifactor, el cifrado de datos, la gestión de copias de seguridad, el control de accesos, el monitoreo de eventos, la capacitación del personal y los procedimientos de respuesta ante incidentes. La

correcta aplicación de estos controles fortalece la protección de los activos críticos y contribuye a garantizar la continuidad del negocio (ISO/IEC 27002, 2022).

Marco normativo

La gestión de la seguridad de la información requiere la implementación de normas, estándares y obligaciones legales que permitan establecer bases para proteger los activos de información, gestionar los riesgos de ciberseguridad y garantizar el cumplimiento de las obligaciones legales. En el caso de Diario Actualidad Digital S.A.S., la adopción de estándares internacionales y de la normativa colombiana constituye un pilar fundamental para fortalecer la protección de la información, los datos personales de usuarios y la infraestructura tecnológica que soporta la operación del negocio.

Tabla 1. Normatividad aplicable.

Norma o estándar	***Propósito***	***Aplicabilidad en la organización***

ISO/IEC 27001:2022	Establecer los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).	Permite implementar un sistema de gestión que proteja la información periodística, los datos de suscriptores y los servicios digitales mediante la gestión de riesgos y la mejora continua.
ISO/IEC 27002:2022	Proporcionar un conjunto de controles de seguridad para proteger los activos de información.	Facilita la implementación de controles relacionados con la gestión de accesos, protección de credenciales, clasificación de la información, seguridad de dispositivos y control de usuarios.

ISO/IEC 27005:2022	Proporcionar directrices para la gestión de riesgos en seguridad de la información.	Permite identificar, analizar y tratar los riesgos asociados a los activos de información críticos de la organización, priorizando acciones de mitigación.
NIST Cybersecurity Framework 2.0	Orientar la gestión de riesgos de ciberseguridad mediante las funciones Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar.	Sirve como referencia para fortalecer la estrategia de ciberseguridad, mejorar la capacidad de respuesta ante incidentes y garantizar la continuidad de las operaciones.
Ley 1581 de 2012	Regular la protección de los datos personales y el tratamiento de la información de los titulares.	Aplica al tratamiento de la información personal de suscriptores, clientes, anunciantes, colaboradores y demás usuarios registrados en las plataformas digitales.

Decreto 1377 de 2013	Reglamentar parcialmente la Ley 1581 de 2012 en materia de protección de datos personales.	Establece procedimientos para la autorización, uso y administración de datos personales tratados por la organización.
Ley 1273 de 2009	Tipificar los delitos informáticos y proteger la información y los datos.	Brinda soporte jurídico frente a incidentes relacionados con acceso no autorizado, daño informático, fraude o interceptación de información digital.

La aplicación correcta de estos estándares y obligaciones legales permite a Diario Actualidad Digital S.A.S. construir un sistema de seguridad integral. Mientras la ISO/IEC 27001:2022 provee el marco de gestión y mejora continua, es decir, establece el qué hacer, la ISO/IEC 27002:2022 detalla los controles técnicos y administrativos específicos, es decir, el cómo hacerlo, dando respuesta directa a las debilidades detectadas, como el uso de contraseñas débiles y la ausencia de clasificación de la información (ISO/IEC 27001, 2022; ISO/IEC 27002, 2022). De manera complementaria, la ISO/IEC 27005:2022 y el NIST CSF 2.0 brindan a la organización una metodología para priorizar la inversión en seguridad, basada en la probabilidad e impacto de los riesgos, y establecen un ciclo de

respuesta y recuperación ante incidentes que resulta vital para la continuidad operativa de un medio digital (NIST, 2024).

En el ámbito jurídico, el cumplimiento de la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012) y del Decreto 1377 de 2013 (Presidencia de la República de Colombia, 2013) no solo evita sanciones, sino que fortalece la relación de confianza con los usuarios al garantizar el manejo adecuado de sus datos personales. Finalmente, la Ley 1273 de 2009 proporciona el respaldo legal necesario para actuar frente a delitos informáticos, disuadiendo conductas malintencionadas que puedan afectar la infraestructura tecnológica del periódico (Congreso de la República de Colombia, 2009). En conjunto, este marco normativo sienta las bases para que la organización transite hacia una cultura de ciberseguridad proactiva y resiliente.

Marco contextual

Descripción de la organización

Diario Actualidad Digital S.A.S. es un medio de comunicación regional con más de veinticinco años de trayectoria en la producción y difusión de información periodística. Inicialmente desarrolló sus actividades mediante la publicación de un periódico impreso; sin embargo, durante la última década ha llevado a cabo un proceso de transformación digital que le ha permitido migrar la mayor parte de sus operaciones hacia plataformas web y medios digitales, ampliando significativamente su cobertura y alcance informativo.

La organización desarrolla actividades económicas relacionadas con la producción, edición y difusión de contenidos periodísticos en áreas como política, economía, deportes, cultura, tecnología y acontecimientos de interés general. Su modelo de negocio se fundamenta en la generación de ingresos mediante publicidad digital, suscripciones premium, convenios institucionales y publicaciones patrocinadas, lo que exige mantener altos niveles de disponibilidad y confiabilidad de sus servicios digitales.

En cuanto a su estructura organizacional, Diario Actualidad Digital S.A.S. cuenta con aproximadamente 180 colaboradores distribuidos en diferentes dependencias, entre las que se destacan la Dirección General, Dirección Editorial, Unidad de Investigación Periodística, Redacción de Noticias, Marketing Digital, Talento Humano, Contabilidad y Finanzas, Servicio al Cliente y Gestión Comercial. Adicionalmente, dispone de corresponsales ubicados en diferentes municipios que desarrollan sus funciones mediante

trabajo remoto, lo cual incrementa la necesidad de implementar controles de seguridad adecuados para el acceso a la información institucional.

Los procesos principales de la organización comprenden la producción periodística, la gestión de fuentes de información mediante la interacción permanente con entidades gubernamentales, organizaciones privadas y ciudadanos; la administración de suscripciones digitales; la comercialización de espacios publicitarios y la producción de contenido audiovisual para diferentes plataformas digitales. Todos estos procesos dependen de la disponibilidad, integridad y confidencialidad de la información, convirtiéndose en elementos críticos para la continuidad del negocio.

Respecto a los recursos tecnológicos, la organización dispone de una infraestructura compuesta por 90 computadores de escritorio, 45 computadores portátiles y 30 dispositivos móviles corporativos. Asimismo, cuenta con un Sistema de Gestión de Contenidos (CMS), portal web institucional, plataforma de suscripciones digitales, correo electrónico corporativo, almacenamiento en la nube, servidores virtuales para aplicaciones web, sistema de gestión documental, plataforma de publicidad digital, herramientas de respaldo automático de información, redes inalámbricas corporativas, equipos de producción audiovisual y sistemas de monitoreo de redes sociales. Esta infraestructura es administrada por un equipo conformado por un jefe de tecnología, dos desarrolladores web, un administrador de infraestructura y dos analistas de soporte, responsables de garantizar el funcionamiento y la seguridad de los servicios tecnológicos.

El contexto de operación de Diario Actualidad Digital S.A.S. se caracteriza por un entorno altamente dinámico, donde la disponibilidad permanente de los servicios digitales y la protección de la información constituyen factores estratégicos para mantener la confianza de sus usuarios y preservar la reputación institucional. No obstante, el crecimiento acelerado de la organización, la incorporación de nuevas tecnologías, el trabajo remoto y la ausencia de algunos controles formales de seguridad incrementan su exposición a amenazas cibernéticas y justifican la necesidad de fortalecer la gestión de la seguridad de la información mediante la adopción de estándares y buenas prácticas internacionales.

Problemática identificada

Diario Actualidad Digital S.A.S. desarrolla la mayor parte de sus actividades mediante plataformas digitales, sistemas de información y servicios tecnológicos que soportan la producción, administración y difusión de contenido periodístico. Debido a esta dependencia de los recursos tecnológicos, la seguridad de la información se convierte en un factor estratégico para garantizar la continuidad de las operaciones, proteger los datos administrados por la organización y preservar la confianza de sus lectores, suscriptores, anunciantes y demás partes interesadas. No obstante, el diagnóstico realizado evidencia la existencia de diversas debilidades en la gestión de la seguridad de la información que incrementan la exposición de la organización a incidentes de ciberseguridad.

Entre las principales situaciones identificadas se encuentra el uso de cuentas personales de correo electrónico, falta de políticas formales de clasificación de

información, uso de credenciales compartidas, falta de MFA, contraseñas débiles y el acceso desde dispositivos no controlados. Estas condiciones reducen la capacidad de controlar el acceso a la información institucional, dificultan la trazabilidad de las acciones realizadas por los usuarios y aumentan el riesgo de divulgación, alteración o pérdida de información sensible, lo que incrementa la probabilidad de accesos no autorizados y compromiso de las cuentas institucionales.

El caso también evidencia deficiencias en la gestión de controles de seguridad y en la administración de los recursos tecnológicos. La permanencia de usuarios con privilegios obsoletos, la ausencia de procedimientos documentados, la falta de simulaciones periódicas de eventos de ciberseguridad y la inexistencia de pruebas recientes de recuperación de respaldos reflejan un nivel insuficiente de preparación para prevenir, detectar y responder oportunamente a incidentes que puedan afectar la disponibilidad de los servicios o comprometer la información institucional y continuidad del negocio.

Adicionalmente, los incidentes registrados durante los últimos años demuestran que varias de estas vulnerabilidades ya han tenido consecuencias reales para la organización. Ya se han presentado incidentes como intentos de phishing, interrupciones del portal, compromiso de redes sociales, pérdida de equipos y publicaciones no validadas. Estos acontecimientos evidencian que las amenazas no representan únicamente riesgos potenciales, sino situaciones que han impactado la operación y la reputación institucional.

Finalmente, la cultura organizacional constituye uno de los principales desafíos para el fortalecimiento de la seguridad de la información. El caso evidencia que algunos colaboradores priorizan la rapidez de publicación sobre la seguridad, consideran que las medidas de protección afectan la productividad y mantienen una confianza excesiva en los correos electrónicos. Esta combinación de debilidades técnicas, culturales y organizativas evidencia la necesidad de un análisis detallado que permita identificar riesgos, priorizar acciones y proponer controles adecuados para asegurar la información y la continuidad del negocio.

Identificación y análisis de activos

Inventario de activos

Los activos de información representan todos aquellos recursos que poseen valor para una organización y que son indispensables para el desarrollo de sus procesos misionales, estratégicos y de apoyo. Estos activos pueden estar constituidos por información, software, hardware, infraestructura tecnológica, servicios, personal y otros elementos que intervienen en el funcionamiento diario de la organización. La adecuada identificación de los activos constituye el punto de partida para la gestión de riesgos, ya que permite determinar cuáles recursos requieren mayores niveles de protección frente a amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

En el caso de Diario Actualidad Digital S.A.S., la operación depende casi en su totalidad del uso de tecnologías digitales para producir, administrar y publicar información periodística. La organización gestiona diariamente contenido informativo, bases de datos de suscriptores, contratos comerciales, plataformas web y recursos tecnológicos que soportan la prestación de sus servicios. Debido a esta dependencia tecnológica, cualquier afectación sobre estos activos puede generar pérdidas económicas, interrupción de los servicios, afectación reputacional e incumplimiento de obligaciones con clientes y aliados estratégicos.

El análisis de los activos permitió identificar aquellos recursos cuya pérdida, alteración, divulgación no autorizada o indisponibilidad tendría un mayor impacto sobre la continuidad del negocio. Para ello se consideró la importancia de cada activo dentro de los procesos organizacionales, el tipo de información que administra, su nivel de exposición a amenazas y el impacto que tendría un incidente de seguridad sobre la operación de la organización.

Los activos fueron clasificados considerando diferentes categorías, entre ellas activos de información, software, hardware, infraestructura tecnológica y servicios. Esta clasificación facilita la implementación de controles de seguridad acordes con las características de cada recurso y permite priorizar las acciones de protección sobre aquellos activos que soportan los procesos críticos del negocio.

A partir del análisis del caso de estudio, se identificó el siguiente inventario de activos de información considerados más relevantes para Diario Actualidad Digital S.A.S.

Tabla 2. Inventario de activos

Activo	***Tipo***	***Descripción***	***Criticidad***

Base de datos de suscriptores	Información	Contiene datos personales, historial de pagos y preferencias de los usuarios registrados.	Alta
Sistema de Gestión de Contenidos (CMS)	Software	Plataforma utilizada para crear, editar y publicar las noticias del periódico digital.	Alta
Portal web institucional	Servicio	Plataforma donde se publica toda la información periodística y mediante la cual acceden los lectores.	Alta

Información periodística e investigaciones	Información	Documentos, borradores, entrevistas y material periodístico utilizado para la elaboración de noticias.	Alta
Plataforma de correo corporativo	Servicio	Medio oficial de comunicación entre colaboradores y con fuentes externas.	Alta
Servidores virtuales	Infraestructura	Alojan el portal web, aplicaciones institucionales y servicios tecnológicos del periódico.	Alta

Sistema de respaldo de información	Software/Servicio	Permite realizar copias de seguridad y recuperar información ante incidentes.	Alta
Sistema de almacenamiento en la nube	Servicio	Repositorio para almacenar documentos institucionales y contenido multimedia.	Alta
Equipos de periodistas y corresponsales (portátiles)	Hardware	Computadores utilizados para elaborar noticias y acceder a los sistemas institucionales desde diferentes ubicaciones.	Media

Red WiFi corporativa	Infraestructura	Proporciona conectividad a los usuarios y dispositivos internos de la organización.	Media
Plataforma de gestión documental	Software	Administra documentos administrativos y operativos de la organización.	Media
Plataforma de publicidad digital	Software	Gestiona campañas publicitarias y contratos con anunciantes.	Media
Dispositivos móviles corporativos	Hardware	Equipos utilizados por periodistas y personal administrativo para labores institucionales.	Media

Equipos de producción audiovisual	Hardware	Recursos empleados para generar videos, entrevistas y transmisiones multimedia.	Media
Personal de Tecnología y Desarrollo Web	Recurso humano	Responsable de administrar la infraestructura tecnológica y garantizar la disponibilidad y seguridad de los servicios.	Alta

Justificación de los activos críticos

Dentro del inventario elaborado, los activos clasificados con criticidad alta representan los recursos más importantes para Diario Actualidad Digital S.A.S., debido a que soportan directamente los procesos estratégicos de la organización y permiten el desarrollo de su actividad principal. La base de datos de suscriptores constituye uno de los activos más sensibles, ya que almacena información personal y financiera cuya pérdida o

divulgación podría afectar la confianza de los usuarios, generar sanciones legales y ocasionar impactos económicos.

El Sistema de Gestión de Contenidos (CMS) y el portal web institucional son fundamentales para la operación del medio de comunicación, puesto que permiten la publicación y distribución de noticias. Una indisponibilidad o alteración de estos sistemas impediría la difusión de información y afectaría directamente la continuidad del negocio.

Por otra parte, la información periodística e investigaciones posee un alto valor estratégico debido a que contiene contenido exclusivo, fuentes confidenciales y material previo a su publicación. Su pérdida, modificación o divulgación no autorizada podría comprometer la credibilidad del medio y afectar su reputación.

Asimismo, los servidores virtuales, el correo corporativo, el sistema de respaldo y el almacenamiento en la nube constituyen la infraestructura tecnológica que soporta el funcionamiento de los servicios institucionales. Estos activos garantizan la disponibilidad de la información, la comunicación organizacional y la recuperación de los datos frente a incidentes de seguridad.

Finalmente, el equipo de Tecnología y Desarrollo Web también se considera un activo crítico, ya que posee el conocimiento técnico necesario para administrar la infraestructura, implementar controles de seguridad, atender incidentes y asegurar la continuidad de las operaciones. La adecuada protección de estos activos debe constituir

una prioridad dentro de la estrategia de ciberseguridad de la organización, pues cualquier afectación sobre ellos tendría consecuencias significativas para la operación, la reputación y la sostenibilidad del medio de comunicación.

Análisis de amenazas y vulnerabilidades

La identificación de amenazas y vulnerabilidades constituye una etapa fundamental dentro del proceso de gestión de riesgos en seguridad de la información, ya que permite reconocer los eventos que pueden comprometer los activos críticos de una organización y las debilidades que facilitan su materialización. En el caso de Diario Actualidad Digital S.A.S., la alta dependencia de plataformas digitales, servicios web y herramientas colaborativas hace que la organización se encuentre expuesta a diferentes riesgos de origen tecnológico, humano y organizacional.

El análisis realizado evidencia que varios de los activos identificados presentan vulnerabilidades asociadas principalmente a la ausencia de políticas de seguridad, controles insuficientes de acceso, prácticas inadecuadas por parte de los usuarios y deficiencias en la administración de la infraestructura tecnológica. Estas condiciones incrementan la probabilidad de incidentes que podrían afectar la confidencialidad, integridad y disponibilidad de la información, además de generar impactos sobre la continuidad de las operaciones y la reputación institucional.

Las amenazas identificadas incluyen ataques de ingeniería social, phishing, accesos no autorizados, pérdida de información, malware, interrupción de los servicios tecnológicos, errores humanos y filtración de información confidencial. La existencia de estas amenazas se encuentra respaldada por los incidentes ocurridos en la organización

durante los últimos años, lo que demuestra que algunos riesgos ya se han materializado y requieren la implementación de controles preventivos y correctivos.

Asimismo, el análisis permitió establecer que no todas las amenazas afectan de la misma manera a los activos de información. Algunos recursos, como el Sistema de Gestión de Contenidos (CMS), el portal web institucional, la base de datos de suscriptores y la información periodística, poseen una mayor exposición debido a que soportan los procesos misionales de la organización y concentran información estratégica cuyo compromiso podría ocasionar pérdidas económicas, afectaciones legales y daños a la imagen institucional.

Con base en la información suministrada en el caso de estudio, se identificaron las siguientes amenazas y vulnerabilidades asociadas a los principales activos de la organización.

Tabla 3. Amenazas y vulnerabilidades

Activo	***Amenaza***	***Vulnerabilidad***
Base de datos de suscriptores	Acceso no autorizado o fuga de información	No existe una política formal de clasificación de la información.

Sistema de Gestión de Contenidos (CMS)	Alteración o publicación no autorizada de contenido	Credenciales compartidas entre periodistas y editores.
Portal web institucional	Ataques de denegación de servicio (DoS/DDoS)	Dependencia del portal y ausencia de simulaciones periódicas de incidentes.
Información periodística e investigaciones	Divulgación o pérdida de información confidencial	Uso de correos electrónicos personales y almacenamiento en dispositivos externos personales.
Plataforma de correo corporativo	Phishing y robo de credenciales	Falta de autenticación multifactor en todos los usuarios y confianza excesiva en correos recibidos.
Servidores virtuales	Interrupción de los servicios o malware	Usuarios con privilegios administrativos innecesarios y controles insuficientes.

Sistema de respaldo de información	Pérdida permanente de información	No existen evidencias recientes de pruebas de recuperación de respaldos.
Computadores portátiles	Robo o pérdida del equipo	Uso de equipos fuera de las instalaciones y acceso remoto a sistemas institucionales.
Red WiFi corporativa	Intrusión o acceso no autorizado	Controles de acceso y autenticación insuficientes.

Del análisis realizado se concluye que los activos que representan un mayor nivel de riesgo son el Sistema de Gestión de Contenidos (CMS), el portal web institucional, la base de datos de suscriptores, la información periodística y la plataforma de correo corporativo. Estos recursos soportan directamente la actividad principal de Diario Actualidad Digital S.A.S., por lo que cualquier incidente que comprometa su funcionamiento tendría consecuencias significativas para la continuidad de las operaciones y la confianza de los usuarios.

Una de las situaciones más críticas corresponde al uso compartido de credenciales del CMS, ya que esta práctica dificulta la identificación de responsabilidades, incrementa

el riesgo de accesos no autorizados y facilita la modificación o publicación indebida de contenido. De igual forma, el uso de cuentas personales de correo electrónico y dispositivos externos para almacenar información periodística representa una amenaza para la confidencialidad de investigaciones y documentos sensibles, especialmente cuando contienen información reservada o proveniente de fuentes confidenciales.

Otro riesgo relevante se relaciona con los ataques de phishing dirigidos al correo corporativo, debido a que el caso evidencia antecedentes de intentos de captura de credenciales mediante mensajes fraudulentos. La ausencia de autenticación multifactor en todos los usuarios aumenta la probabilidad de que un atacante obtenga acceso a los sistemas institucionales utilizando credenciales comprometidas.

Asimismo, la falta de pruebas periódicas de recuperación de los respaldos constituye una vulnerabilidad importante, ya que la existencia de copias de seguridad no garantiza por sí sola la recuperación de la información ante un incidente. En caso de una falla tecnológica, un ataque de ransomware o un error humano, la organización podría enfrentar dificultades para restablecer sus servicios en el tiempo esperado.

Finalmente, la combinación de debilidades técnicas y factores humanos incrementa considerablemente el nivel de exposición de la organización frente a amenazas cibernéticas.

Análisis y gestión de riesgos

Metodología de análisis

Este estudio se realizó con el propósito de identificar los eventos que pueden afectar los activos de información de Diario Actualidad Digital S.A.S. y determinar el nivel de riesgo asociado a cada uno. Para esto, se partió del diagnóstico previo del caso de estudio, el inventario de activos, las amenazas identificadas y las vulnerabilidades detectadas.

Como referencia metodológica se tomó la norma ISO/IEC 27005:2022, la cual proporciona directrices para la gestión de riesgos de seguridad de la información dentro de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta metodología permite identificar los activos críticos, reconocer las amenazas y vulnerabilidades que pueden afectarlos y establecer el nivel de riesgo para priorizar las acciones de tratamiento (ISO/IEC 27005, 2022).

Dos criterios primordiales guiaron la evaluación impacto y probabilidad.

El impacto corresponde a las consecuencias que tendría la materialización de un riesgo sobre la organización. Para este estudio se clasificó en tres niveles:

- Alto: El incidente compromete la continuidad del negocio, genera pérdidas económicas importantes, afecta la reputación institucional o provoca la pérdida de información crítica.
- Medio: El incidente afecta parcialmente la operación, genera retrasos o pérdidas controlables.

- Bajo: El incidente tiene un impacto limitado y puede ser corregido sin afectar significativamente los procesos de la organización.

La probabilidad representa la posibilidad de que una amenaza aproveche una vulnerabilidad y se materialice. Para su valoración también se utilizaron tres niveles:

- Alta: Existen antecedentes del incidente, vulnerabilidades evidentes o una alta exposición del activo.
- Media: El riesgo puede materializarse, aunque existen algunos controles o la exposición es moderada.
- Baja: La ocurrencia del incidente es poco probable debido a la existencia de controles o a una baja exposición.

Finalmente, el nivel de riesgo se determinó combinando el impacto y la probabilidad de cada escenario identificado, con el fin de establecer cuáles riesgos requieren atención prioritaria y la implementación de controles de seguridad (ISO/IEC 27001, 2022). Este enfoque permite orientar las decisiones de la organización hacia la protección de los activos más importantes y fortalecer su capacidad para prevenir y responder ante incidentes de ciberseguridad (NIST, 2024).

Matriz de riesgos

Tabla 4. Matriz de riesgos

Activo	*Amenaza*	*Vulnerabilidad*	*Impacto*	*Probabilidad*	*Nivel*
Sistema de Gestión de Contenidos (CMS)	Acceso no autorizado	Compartición de credenciales entre periodistas y editores.	Alto	Alto	Alto
Base de datos de suscriptores	Fuga de información	Ausencia de una política de clasificación de la información.	Alto	Medio	Alto
Correo corporativo	Phishing	Falta de autenticación multifactor y capacitación insuficiente.	Alto	Alto	Alto

Información periodística	Divulgación de información confidencial	Uso de correos personales y almacenamiento en dispositivos personales.	Alto	Alto	Alto
Portal web institucional	Ataque DDoS	Falta de simulaciones y medidas preventivas documentadas.	Alto	Medio	Alto
Sistema de respaldo	Pérdida de información	No se realizan pruebas periódicas de restauración.	Alto	Medio	Alto
Servidores virtuales	Malware o ransomware	Actualización y control de privilegios insuficientes.	Alto	Medio	Alto

Computadores portátiles	Robo o pérdida del equipo	Uso fuera de las instalaciones sin controles suficientes.	Medio	Medio	Medio
Redes sociales institucionales	Acceso indebido	Gestión inadecuada de credenciales.	Medio	Alto	Alto
Red WiFi corporativa	Acceso no autorizado	Controles de acceso insuficientes.	Medio	Medio	Medio

El análisis de la matriz de riesgos evidencia que los riesgos con nivel alto requieren atención prioritaria, ya que afectan los activos que soportan los procesos estratégicos de Diario Actualidad Digital S.A.S. La materialización de estos riesgos podría comprometer la confidencialidad de la información periodística, la disponibilidad de los servicios digitales y la confianza de los usuarios.

El impacto se calificó como alto en los activos que sostienen directamente la operación del periódico: el CMS, el correo corporativo, la información periodística, la base de datos de suscriptores, el portal web, los servidores virtuales y el sistema de respaldo, ya que su compromiso afectaría de forma inmediata la continuidad de la operación, la

confidencialidad de las fuentes o la disponibilidad de los servicios digitales. Los computadores portátiles y la red WiFi corporativa se calificaron con impacto medio, dado que su afectación generaría inconvenientes operativos puntuales sin comprometer directamente la operación misional del medio.

La probabilidad se calificó como alta en aquellos escenarios donde ya existe evidencia de intentos o incidentes reales como los intentos de phishing al correo corporativo, la exposición de la información por uso de dispositivos personales, y el acceso indebido a redes sociales por el uso descuidado de credenciales, así como en el caso del CMS, donde la compartición de credenciales incrementa considerablemente la exposición. Los escenarios calificados con probabilidad media son de riesgos posibles, pero sin antecedentes confirmados dentro del caso de estudio, como el ataque DDoS al portal web, la pérdida de información del sistema de respaldo o el malware en servidores virtuales, donde existen algunos controles parciales que reducen la exposición.

El Sistema de Gestión de Contenidos (CMS), por ejemplo, representa uno de los mayores riesgos, debido a que un acceso no autorizado o el robo de credenciales podría derivar en modificaciones de contenido, fuga de datos o exposición de información sensible. La base de datos de suscriptores es otro activo crítico debido a que almacena los datos personales de los usuarios. En el caso del correo corporativo, el riesgo principal es el robo de credenciales mediante phishing, dado que este canal administra información crítica

para la organización. Cada uno de estos escenarios impactaría directamente la operación diaria del periódico y la confianza de sus lectores.

La información periodística por su parte representa un activo especialmente sensible del medio de comunicación. La utilización de correos personales y dispositivos no controlados incrementa el riesgo de pérdida o divulgación de investigaciones antes de su publicación, situación que puede comprometer la credibilidad del periódico y la protección de sus fuentes de información.

El portal web y su disponibilidad, así como el sistema de respaldo representan otro frente crítico que resulta esencial para garantizar la continuidad del servicio. Un ataque de denegación de servicio o la imposibilidad de recuperar la información después de un incidente podría interrumpir las operaciones y generar pérdidas económicas y reputacionales.

La acción más urgente es implementar autenticación multifactor en el correo corporativo y el CMS, ya que son las puertas de entrada más vulnerables según el diagnóstico. Paralelamente, deben establecerse pruebas periódicas de restauración de respaldos y un procedimiento formal de respuesta ante incidentes, para garantizar que la organización pueda recuperar sus servicios ante cualquier eventualidad.

Políticas y controles de seguridad

La implementación de políticas y controles de seguridad constituye una estrategia fundamental para reducir la probabilidad de materialización de los riesgos identificados en Diario Actualidad Digital S.A.S. Estas medidas permiten establecer lineamientos para el uso adecuado de los recursos tecnológicos, fortalecer la protección de los activos de información y mejorar la capacidad de la organización para prevenir, detectar y responder ante incidentes de ciberseguridad. Las políticas definen las responsabilidades y normas que deben cumplir los colaboradores, mientras que los controles representan las acciones específicas que permiten gestionar los riesgos identificados.

Políticas propuestas

Tabla 5. Políticas de seguridad

Política	***Objetivo***	***Riesgo asociado***
Política de Gestión de Usuarios y Contraseñas	Establecer requisitos para la creación, administración y actualización de credenciales de acceso.	Acceso no autorizado al Sistema de Gestión de Contenidos (CMS).

Política de Uso Seguro del Correo Electrónico	Regular el uso del correo corporativo y prevenir ataques de phishing e ingeniería social.	Robo de credenciales mediante phishing.
Política de Clasificación y Manejo de la Información	Definir criterios para clasificar y proteger la información según su nivel de sensibilidad.	Fuga de información periodística y acceso indebido a datos confidenciales.
Política de Copias de Seguridad	Garantizar la realización y verificación periódica de respaldos de la información institucional.	Pérdida de información por fallas en los respaldos.
Política de Gestión de Accesos y Privilegios	Controlar la asignación, modificación y revocación de permisos de acceso a los sistemas institucionales.	Uso indebido de privilegios administrativos.

Política para el Uso de Dispositivos Institucionales y Personales (BYOD)	Regular el acceso a los sistemas institucionales desde equipos corporativos y personales.	Acceso desde dispositivos personales y pérdida de información.
Política de Gestión de Incidentes de Seguridad	Establecer el procedimiento para identificar, reportar y atender incidentes de seguridad de la información.	Respuesta insuficiente ante incidentes de ciberseguridad.

Controles propuestos

Tabla 6. Controles de seguridad

Riesgo	***Control***	***Justificación***
Acceso no autorizado al CMS	Implementar autenticación multifactor y eliminar el uso compartido de credenciales.	Reduce la posibilidad de accesos no autorizados y mejora la trazabilidad de las acciones realizadas por los usuarios.

Robo de credenciales mediante phishing	Realizar campañas de capacitación y simulaciones periódicas de phishing.	Fortalece la capacidad de los colaboradores para identificar correos fraudulentos y disminuye el riesgo de compromiso de cuentas.
Fuga de información periodística	Restringir el uso de correos personales y cifrar la información confidencial.	Protege las investigaciones periodísticas y reduce el riesgo de divulgación no autorizada.
Pérdida de información	Ejecutar copias de seguridad automáticas y realizar pruebas periódicas de restauración.	Garantiza la disponibilidad y recuperación de la información ante incidentes.
Uso indebido de privilegios administrativos	Revisar periódicamente los permisos y aplicar el principio de mínimo privilegio.	Evita que usuarios mantengan accesos innecesarios y reduce el riesgo de modificaciones no autorizadas.

Interrupción del portal web	Implementar monitoreo continuo y mecanismos de protección contra ataques DDoS.	Favorece la disponibilidad del servicio y disminuye el impacto de ataques externos.
Robo o pérdida de computadores portátiles	Implementar cifrado de discos, inventario de equipos y mecanismos de bloqueo remoto.	Protege la información almacenada en los dispositivos y reduce el impacto ante pérdida o robo.

El diagnóstico de seguridad evidenció debilidades concretas en Diario Actualidad Digital S.A.S: uso compartido de credenciales del CMS, falta de autenticación multifactor, uso de correos personales para investigaciones y falta de procedimientos para responder ante incidentes. Este contexto genera que estén expuestos activos críticos como la base de datos de suscriptores, el portal web y las investigaciones periodísticas a riesgos de acceso no autorizado, pérdida o robo de información e interrupción del servicio. Por ello, las políticas y controles aquí propuestos buscan cerrar estas brechas, estableciendo un marco que no solo proteja los activos, sino que también promueva una cultura de seguridad entre los trabajadores.

Las políticas de gestión de usuarios, clasificación de la información, copias de seguridad y gestión de incidentes proporcionan un marco organizacional para controlar el

acceso a la información, proteger los datos sensibles y establecer procedimientos claros para la respuesta ante eventos de seguridad. De igual forma, la política para el uso de dispositivos institucionales y personales permitirá reducir los riesgos derivados del acceso a los sistemas desde equipos que no cuentan con los controles de seguridad requeridos.

Por su parte, los controles técnicos y administrativos complementan estas políticas mediante acciones específicas como la autenticación multifactor, la revisión periódica de privilegios, el monitoreo de los servicios, las campañas de capacitación y la ejecución de pruebas de restauración de respaldos. Estas medidas disminuyen la probabilidad de que las amenazas identificadas se materialicen y reducen el impacto que podrían generar sobre la operación de la organización.

En conjunto, estas políticas y controles protegen la confidencialidad de las fuentes periodísticas, la integridad de los contenidos publicados y la disponibilidad del portal web en todo momento. Más allá de cumplir con estándares técnicos, el uso y adopción de estas medidas representa una inversión estratégica que salvaguarda el activo más valioso del periódico: su credibilidad. Al demostrar un compromiso serio con la seguridad de la información, Diario Actualidad Digital S.A.S no solo reduce su exposición a incidentes, sino que también refuerza la confianza de sus lectores, suscriptores y anunciantes.

Gestión de incidentes y continuidad del negocio

La gestión de incidentes y la continuidad del negocio son componentes esenciales para garantizar la disponibilidad de los servicios y la protección de los activos de información frente a eventos que puedan afectar el funcionamiento de una organización. En Diario Actualidad Digital S.A.S., cuya operación depende principalmente de plataformas digitales, la capacidad para responder de manera oportuna a incidentes de seguridad resulta fundamental para minimizar las interrupciones del servicio, proteger la información periodística y mantener la confianza de los usuarios.

En el caso de Diario Actualidad Digital S.A.S., el estudio previo evidenció vulnerabilidades críticas: uso compartido de credenciales del CMS, falta de autenticación multifactor, uso de correos personales para investigaciones y falta de procedimientos documentados para la respuesta ante incidentes. Este contexto incrementa la probabilidad de que se materialicen eventos como ataques de phishing, accesos no autorizados o interrupciones del servicio, afectando directamente la publicación de noticias y la confianza de los lectores. Por ello, la organización debe contar con un plan estructurado que permita identificar, contener y recuperar los servicios afectados en el menor tiempo posible.

La continuidad del negocio busca asegurar que los procesos críticos continúen operando durante y después de un incidente de seguridad. Para lograrlo, es necesario definir responsabilidades, establecer mecanismos de comunicación, mantener copias de seguridad

verificadas y disponer de procedimientos de recuperación que permitan restablecer los servicios esenciales sin afectar significativamente la operación del medio de comunicación.

Tabla 7. Incidentes potenciales

Incidente	***Descripción***	***Impacto***
Acceso no autorizado al Sistema de Gestión de Contenidos (CMS)	Uso indebido de credenciales que permite modificar o publicar contenido sin autorización.	Alto
Ataque de phishing al correo corporativo	Captura de credenciales mediante correos electrónicos fraudulentos.	Alto
Fuga de información periodística	Divulgación no autorizada de investigaciones o documentos confidenciales.	Alto

Interrupción del portal web	Indisponibilidad del sitio web por fallas técnicas o ataques de denegación de servicio (DDoS).	Alto
Pérdida de información	Imposibilidad de recuperar información debido a fallas en los respaldos.	Alto
Robo o pérdida de computadores portátiles	Exposición de información institucional almacenada en los equipos.	Medio
Compromiso de cuentas oficiales en redes sociales	Acceso no autorizado a las cuentas institucionales y publicación de contenido no autorizado.	Medio

Tabla 8. Plan básico de respuesta

Fase	***Acción***
Identificación	Detectar el incidente, registrar la información inicial y notificar al área de tecnología.
Contención	Limitar el alcance del incidente mediante el aislamiento de sistemas o el bloqueo de accesos comprometidos.
Erradicación	Eliminar la causa del incidente, corregir vulnerabilidades y actualizar las medidas de seguridad.
Recuperación	Restaurar los servicios mediante copias de seguridad verificadas y validar el funcionamiento de los sistemas.
Comunicación	Informar a la dirección, usuarios afectados y demás partes interesadas cuando sea necesario.
Seguimiento	Documentar el incidente, analizar las causas y establecer acciones de mejora para evitar su repetición.

La continuidad operativa de Diario Actualidad Digital S.A.S. depende de la disponibilidad de cinco activos críticos: el CMS, el portal web, el correo corporativo, la base de datos de suscriptores y la infraestructura tecnológica que los soporta. El CMS y el portal web son esenciales para la publicación y distribución de noticias; sin ellos, el periódico no puede cumplir con su misión informativa. El correo corporativo es el canal principal de comunicación con fuentes y colaboradores, mientras que la base de datos de suscriptores contiene información personal y financiera cuya pérdida podría generar sanciones legales y pérdida de confianza.

En caso de presentarse un incidente de seguridad, la organización deberá activar el procedimiento de respuesta, priorizando la protección de los activos críticos y la recuperación de los servicios esenciales. Durante la fase inicial será necesario identificar el incidente, evaluar su alcance y aplicar medidas de contención para evitar que el problema se propague a otros sistemas. Posteriormente, el equipo de tecnología deberá eliminar la causa del incidente, restaurar la información mediante copias de seguridad previamente verificadas y validar el correcto funcionamiento de las plataformas antes de restablecer completamente la operación.

La comunicación constituye un elemento fundamental durante la gestión del incidente. La organización deberá mantener informada a la alta dirección y, cuando corresponda, comunicar oportunamente la situación a colaboradores, usuarios y demás

partes interesadas. Una comunicación clara y oportuna contribuye a reducir la incertidumbre y preservar la confianza en los servicios prestados.

Una vez restablecida la operación, será necesario documentar el incidente, identificar las causas que lo originaron y definir acciones de mejora para fortalecer los controles existentes. Entre estas acciones se incluyen la actualización de procedimientos, la revisión de privilegios de acceso, la capacitación del personal y la realización periódica de simulacros de respuesta a incidentes.

La implementación de estas medidas permitirá que Diario Actualidad Digital S.A.S no solo actúe de manera efectiva ante incidentes, sino que también mantenga su compromiso con la publicación oportuna y confiable de noticias. Al contar con un plan estructurado de gestión de incidentes y continuidad del negocio, el periódico protege su activo más valioso: la credibilidad ante sus lectores, anunciantes y aliados estratégicos. De esta manera, la organización podrá minimizar las interrupciones operativas, preservar la confianza de los usuarios y asegurar la sostenibilidad de su modelo de negocio en un entorno digital cada vez más exigente.

Cultura organizacional en ciberseguridad

La cultura organizacional en ciberseguridad hace referencia al conjunto de conocimientos, comportamientos y prácticas que adoptan los colaboradores para proteger la información y los recursos tecnológicos de la organización. Una cultura de seguridad sólida permite reducir los riesgos derivados de errores humanos, fortalecer el cumplimiento de las políticas internas y promover la responsabilidad compartida frente a la protección de los activos de información.

En Diario Actualidad Digital S.A.S. se identificaron diversas situaciones que evidencian la necesidad de fortalecer la cultura de ciberseguridad. Aunque la organización dispone de herramientas tecnológicas para apoyar sus procesos, persisten prácticas inadecuadas relacionadas con el manejo de credenciales, el uso de dispositivos personales y la ausencia de procedimientos estandarizados para la gestión de incidentes. Estas condiciones incrementan la exposición a amenazas como el phishing, el acceso no autorizado y la fuga de información.

Fortalecer la cultura organizacional requiere el compromiso de todos los niveles de la empresa. La alta dirección debe promover políticas claras y asignar los recursos necesarios para la gestión de la seguridad de la información, mientras que los colaboradores deben conocer y aplicar las buenas prácticas definidas por la organización. De esta manera,

la ciberseguridad deja de ser una responsabilidad exclusiva del área de tecnología y se convierte en un compromiso institucional.

Tabla 9. Hallazgos organizacionales

Situación observada	***Riesgo asociado***
Compartición de credenciales entre periodistas y editores.	Acceso no autorizado a los sistemas institucionales.
Uso de cuentas de correo personales para actividades laborales.	Fuga de información confidencial.
Falta de autenticación multifactor para todos los usuarios.	Robo de credenciales mediante phishing.
Uso de dispositivos personales para almacenar información institucional.	Pérdida o divulgación de información.
Ausencia de un procedimiento formal para la gestión de incidentes.	Respuesta tardía ante incidentes de seguridad.

Permanencia de privilegios administrativos innecesarios.	Uso indebido de permisos y modificaciones no autorizadas.
Copias de seguridad sin pruebas periódicas de restauración.	Pérdida de información y afectación de la continuidad del negocio.

Tabla 10. Recomendaciones de mejora

Hallazgo	***Recomendación***
Compartición de credenciales.	Asignar cuentas individuales y prohibir el uso compartido de usuarios y contraseñas.
Uso de correos personales.	Utilizar exclusivamente el correo corporativo para actividades institucionales.
Falta de autenticación multifactor.	Implementar autenticación multifactor para todos los accesos a sistemas críticos.

Uso de dispositivos personales.	Establecer controles para el acceso desde equipos personales y promover el uso de dispositivos institucionales.
Ausencia de procedimientos para incidentes.	Diseñar e implementar un procedimiento formal para la gestión y reporte de incidentes de seguridad.
Privilegios administrativos innecesarios.	Revisar periódicamente los permisos de acceso y aplicar el principio de mínimo privilegio.
Falta de pruebas de restauración de respaldos.	Programar pruebas periódicas de recuperación para verificar la disponibilidad de la información.

Las recomendaciones propuestas contribuirán al fortalecimiento de la cultura organizacional en ciberseguridad al promover comportamientos responsables y buenas prácticas en el uso de la información y de los recursos tecnológicos. La asignación de credenciales individuales, el uso exclusivo del correo corporativo y la implementación de autenticación multifactor permitirán mejorar el control de accesos y reducir la posibilidad de que usuarios no autorizados comprometan los sistemas de la organización.

Asimismo, la definición de procedimientos para la gestión de incidentes proporcionará a los colaboradores una guía clara sobre cómo actuar frente a eventos que puedan afectar la seguridad de la información. Esto facilitará una respuesta más rápida y coordinada, disminuyendo el impacto de los incidentes y favoreciendo la continuidad de las operaciones.

La revisión periódica de privilegios, el control sobre el uso de dispositivos personales y la verificación de las copias de seguridad fortalecerán la protección de los activos críticos y fomentarán el cumplimiento de las políticas internas. Estas acciones permitirán que los colaboradores comprendan la importancia de seguir los procedimientos establecidos y adopten una actitud preventiva frente a los riesgos de ciberseguridad.

Finalmente, el desarrollo de programas permanentes de capacitación y sensibilización permitirá consolidar una cultura organizacional basada en la prevención, la responsabilidad y la mejora continua. De esta manera, Diario Actualidad Digital S.A.S. estará en mejores condiciones para enfrentar las amenazas actuales, proteger la información institucional y garantizar la continuidad de sus procesos estratégicos.

Conclusiones

El diagnóstico realizado permitió evidenciar que la principal fuente de riesgo de Diario Actualidad Digital S.A.S. no proviene únicamente de la infraestructura tecnológica, sino de prácticas organizacionales arraigadas. Esto confirma que la seguridad de la información depende tanto de controles técnicos como de los hábitos y la cultura de los colaboradores, y que ambos frentes deben trabajarse de manera conjunta para obtener resultados reales.

La ausencia de autenticación multifactor en sistemas críticos como el CMS y el correo corporativo representa la vulnerabilidad más urgente de atender. Esto permite concluir que no todas las medidas de seguridad tienen el mismo nivel de prioridad, y que la organización debe enfocar sus primeros esfuerzos en cerrar las brechas que representan la puerta de entrada más probable para un atacante.

El ejercicio de identificación de activos evidenció que el valor de una organización periodística no reside únicamente en su infraestructura tecnológica, sino en sus bienes intangibles como la credibilidad del medio y la confidencialidad de sus fuentes. De esto se concluye que los controles de seguridad no deben limitarse a garantizar la disponibilidad de los servicios digitales, sino que también protejan de manera especial la información periodística sensible y los procesos de investigación previos a su publicación.

La aplicación de una metodología estructurada de análisis de riesgos, basada en la valoración conjunta del impacto y la probabilidad, facilita la toma de decisiones para priorizar la inversión en seguridad. Esto representa una lección clave, pues demuestra que la gestión de riesgos permite anticiparse a los incidentes en lugar de actuar únicamente de forma reactiva una vez que estos ya se han materializado.

La formulación de políticas y controles, aunque necesaria, no es suficiente por sí sola si no está acompañada de un cambio cultural dentro de la organización. El caso evidenció que varios colaboradores anteponen la rapidez de publicación a la seguridad de la información, lo que demuestra que la capacitación continua, la sensibilización y el compromiso visible de la alta dirección resultan indispensables para que las medidas técnicas propuestas se traduzcan en una protección efectiva.

Finalmente, el desarrollo de este trabajo permitió comprender que la gestión de incidentes y la continuidad del negocio deben planearse de forma proactiva y no como una respuesta improvisada ante escenarios imprevistos. Contar con un procedimiento documentado, probado periódicamente y conocido por todo el personal es lo que realmente marca la diferencia entre un incidente controlado a tiempo y una crisis que compromete la operación y la reputación institucional de Diario Actualidad Digital S.A.S.

Referencias

International Organization for Standardization. (2018). ISO/IEC 27000:2018 — Information technology — Security techniques — Information security management systems — Overview and vocabulary (5.ª ed.). ISO.

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

International Organization for Standardization. (2022). ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls (3.ª ed.). ISO.

International Organization for Standardization. (2022). ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks (4.ª ed.). ISO.

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Congreso de la República de Colombia. (2012). Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial.

Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial.

Congreso de la República de Colombia. (2009). Ley 1273 de 2009, por medio de la cual se modifica el Código Penal y se crea el bien jurídico de la protección de la información y de los datos. Diario Oficial.