e-ISSN: 2528-8091
Vol. 10, N° V CICACI - 2025

Norma ISO/IEC 27035 para establecer protocolos de contención ante ataques de ransonmware en infraestructuras tecnológica.

ISO/IEC 27035 standard for establishing containment protocols against ransonmware attacks on technological infrastructures

https://doi.org/10.5281/zenodo.20432415

AUTORES:

María Isabel Gonzales Valero
Universidad Técnica de Babahoyo,
https://orcid.org/0000-0001-5825-0668
E-mail: mgonzalez@utb.edu.ec

Justin Steeven Varas Garcia
Universidad Técnica de Babahoyo,
https://orcid.org/0009-0004-6039-693X
E-mail: jsvarasg@fafi.utb.edu.ec

Roberto Carlos Valero Solís
Universidad Técnica de Babahoyo,
https://orcid.org/0009-0004-4996-1037
E-mail: rcvaleros@fafi.utb.edu.ec

Kevin Leonardo Veloz España
Universidad Técnica de Babahoyo,
https://orcid.org/0009-0005-9912-7056
E-mail: kveloze@fafi.utb.edu.ec

DIRECCIÓN PARA CORRESPONDENCIA: mgonzalez@utb.edu.ec

Fecha de recepción: 20 / 11 / 2025

Fecha de aceptación: 27 / 11 / 2025

RESUMEN

El ransomware representa hoy día una seria amenaza para la protección de las plataformas digitales, con la capacidad de paralizar funciones, comprometer datos confidenciales y acarrear importantes perjuicios económicos. Ante este panorama, resulta fundamental implementar estrategias de mitigación y reacción que salvaguarden la integridad de los datos y garanticen la constancia en las actividades. La norma ISO/IEC 27035, enfocada en la gestión de sucesos de seguridad, ofrece una estructura sistematizada para identificar, valorar y responder de forma eficiente a dichos sucesos. Este estudio examina la aplicación de esta norma para diseñar estrategias de mitigación eficaces contra ataques de ransomware. Se empleó una metodología cualitativa exploratoria mediante un caso de estudio, lo cual facilitó una investigación exhaustiva de la aplicación de la norma en entornos reales para alcanzar una comprensión integral de este suceso. Los resultados evidenciaron una mejora en la capacidad de respuesta de la entidad, disminuyendo el tiempo requerido para identificar y responder a los ataques. Adicionalmente, se observaron mejoras en la coordinación interna gracias a la claridad en la distribución de roles, y se atenuó el impacto operativo al minimizar la pérdida de información y el tiempo de inactividad. La adopción de la norma además impulsó la concientización y formación del personal, fortaleciendo la cultura de seguridad y permitió identificar y subsanar carencias en la plataforma tecnológica.

Palabras clave: Ransomware, Gestión de Incidentes, Ciberseguridad, Contención.

ABSTRACT

Ransomware today represents a serious threat to the protection of digital platforms, capable of paralyzing functions, compromising confidential data, and causing significant economic damage. Given this scenario, it is essential to implement mitigation and response strategies that safeguard data integrity and ensure consistency in activities. The ISO/IEC 27035 standard, which focuses on security event management, offers a systematic framework for efficiently identifying, assessing, and responding to such events. This study

examines the application of this standard to design effective mitigation strategies against ransomware attacks. An exploratory qualitative methodology was used through a case study, which facilitated an in-depth investigation of the standard's application in real-world environments to gain a comprehensive understanding of this event. The results demonstrated an improvement in the organization's response capacity, reducing the time required to identify and respond to attacks. Additionally, improvements in internal coordination were observed thanks to clearer role distribution, and the operational impact was mitigated by minimizing information loss and downtime. Adoption of the standard also boosted staff awareness and training, strengthening the security culture and enabling the identification and correction of gaps in the technology platform.

Keywords: Ransomware, Incident Management, Cybersecurity, Containment.

INTRODUCCIÓN

En un entorno digital cada vez más amenazado por ataques cibernéticos, el ransomware se ha convertido en una de las amenazas más graves para la seguridad de las infraestructuras tecnológicas. (Natalucci, 2024) Este tipo de ataque puede paralizar sistemas críticos, comprometer datos sensibles y generar pérdidas económicas significativas. (Ayerd, 2023) Ante esta realidad, protocolos efectivos de contención y respuesta es fundamental para proteger la integridad de la información y garantizar la continuidad operativa.

La norma ISO/IEC 27035, centrada en la gestión de incidentes de seguridad de la información, ofrece un marco estructurado para identificar, evaluar y responder a estos incidentes de manera eficiente. (ISO/IEC 27035 Gestión de Incidentes de Seguridad, 2020) Esta norma internacional establece directrices claras para desarrollar procedimientos proactivos y reactivos frente a ataques como el ransomware, permitiendo a las organizaciones actuar de forma rápida y coordinada. En este contexto, el presente trabajo abordará cómo aplicar la norma ISO/IEC 27035 para establecer protocolos eficaces de contención ante ataques de ransomware. (Hernadez, 2025)

Si bien el ransomware se ha vuelto popular en la última década, sus inicios se remontan a los años 80 con programas iniciales como el "AIDS Trojan" y el "PC Cyborg". Su evolución se vio marcada por el surgimiento de una criptografía más compleja, el empleo de monedas digitales para los pagos de rescate (que facilita el anonimato) y la diversidad de sus tácticas de ataque. Inicialmente, el ransomware se difundía principalmente mediante emails engañosos; hoy en día, las amenazas persisten por medio del aprovechamiento de vulnerabilidades en el software, ataques en la cadena de suministro y tácticas más refinadas como la "doble extorsión", donde no solo se cifran los datos, sino que además se divulga información privada bajo la amenaza de hacerla pública en caso de no efectuarse el pago del rescate. Tal complejidad exige que las empresas pongan en práctica un enfoque preventivo y unificado para su supervisión y gestión.

Sabiendo que los ataques cibernéticos son inevitables, la forma en que una empresa responde con rapidez, buena coordinación y eficacia es vital para mitigar los efectos negativos. Un buen manejo de los incidentes de seguridad busca no solo minimizar el daño, sino también recuperar las actividades normales, extraer lecciones de lo sucedido y mejorar las medidas de protección para el futuro. Si no hay un sistema claro, las respuestas podrían ser caóticas, extendiendo el tiempo de interrupción, incrementando las pérdidas y erosionando la confianza de las partes interesadas. Por lo tanto, seguir las normas internacionales ofrece una guía importante para desarrollar y sostener un plan de gestión de incidentes de seguridad que sea lógico y productivo.

La norma ISO/IEC 27035, denominada "Gestión de incidentes relativos a la seguridad de la información", brinda una metodología organizada para identificar, evaluar, responder y extraer lecciones de los incidentes de seguridad informática. Al adoptarla, las organizaciones pueden establecer procesos tanto preventivos como correctivos que son esenciales para contrarrestar ataques complejos como el ransomware (ISO/IEC 27035 Gestión de Incidentes de Seguridad, 2020). Esta norma ofrece indicaciones para la planificación del manejo de incidentes, la identificación y notificación, la evaluación y toma de decisiones, la respuesta ante incidentes y el aprendizaje a partir de lo vivido. Al

seguir sus fundamentos, las empresas pueden asegurar una contestación ágil, sistemática y eficaz, disminuyendo el impacto y simplificando la restauración.

La protección de las infraestructuras tecnológicas ante el peligro creciente del ransomware va en aumento. Aunque contamos con ciertas normas, todavía necesitamos estudiar a fondo cómo la ISO/IEC 27035 se aplica y ayuda realmente a frenar estos ataques. Este estudio profundiza en la ciberseguridad, analizando cómo el uso de la ISO/IEC 27035 puede optimizar la respuesta ante el ransomware, ofreciendo consejos útiles a las empresas para mejorar sus tácticas de reacción. Buscamos verificar si este marco funciona, aportando datos que justifiquen su uso y promuevan una cultura de seguridad activa y fuerte. El objetivo central de esta investigación es analizar la norma ISO/IEC 27035 para crear procesos que permitan detener los ataques de ransomware en las infraestructuras tecnológicas.

La base conceptual de esta investigación se construye sobre las pautas para la gestión de percances de seguridad en sistemas informáticos, junto con un examen a fondo de los peligros que conlleva el software de rescate, tomando como guía principal la norma ISO/IEC 27035.

La seguridad de los datos se articula en torno a tres pilares esenciales: la Confidencialidad, la Integridad y la Disponibilidad (CID).

- **Confidencialidad:** Implica que solo las personas, entidades o procesos autorizados puedan acceder a la información. En el contexto del ransomware, esta confidencialidad se ve comprometida cuando los datos se exponen antes de ser cifrados.
- **Integridad:** Significa que la información es exacta y completa, al igual que los métodos empleados para su tratamiento. El ransomware agrede directamente la integridad de los datos al cifrarlos, volviéndolos ininteligibles e inservibles para quienes tienen permisos de acceso.
- **Disponibilidad:** Garantiza que las personas autorizadas puedan acceder a la información y a los recursos asociados cuando lo requieran. La consecuencia más evidente del ransomware es la imposibilidad de acceder a sistemas y datos fundamentales.

La gestión de los riesgos asociados a la seguridad de la información es un proceso constante que implica identificar, valorar, tratar y supervisar los riesgos inherentes a la información y a los sistemas. Los incidentes de seguridad son la materialización de estos riesgos.

La Gestión de Seguridad de la Información (GSI) abarca una serie de pasos diseñados para descubrir, investigar, dar prioridad, solucionar y superar las complicaciones vinculadas a la seguridad de los datos. Disponer de un programa de GSI eficaz es esencial para cualquier organización y generalmente se compone de las siguientes etapas clave:

- **Preparación:** Implica capacitar al equipo, establecer normas y protocolos, delimitar las funciones y obligaciones, e implementar herramientas y tecnologías (como SIEM, EDR, copias de seguridad).
- **Detección y Análisis:** Supervisión continua para identificar sucesos inusuales y análisis para determinar si un evento representa un incidente de seguridad, así como su magnitud, impacto y causa.
- **Contención:** Tácticas para aminorar la propagación y el impacto del incidente. En casos de ransomware, esto podría conllevar aislar los sistemas afectados, interrumpir las comunicaciones de comando y control (C2) y desconectar redes.
- **Erradicación:** Eliminación de la causa principal del incidente (por ejemplo, suprimir el malware, subsanar vulnerabilidades).
- **Recuperación:** Restaurar los sistemas y datos a un estado operativo normal y seguro, a menudo mediante el uso de copias de seguridad íntegras.
- **Actividades Post-incidente (Lecciones Aprendidas):** Documentación del incidente, análisis forense, identificación de puntos débiles y mejora de las medidas de seguridad para prevenir la repetición de incidentes parecidos.

El ransomware se presenta de muchas maneras, cada una con sus propias características:

- **Ransomware de cifrado:** Su función es codificar archivos en el disco o en la red, volviéndolos inútiles. Esta es la versión que más vemos.

- **Ransomware de bloqueo:** Bloquea el acceso al sistema operativo por completo, mostrando un mensaje que pide un pago para recuperarlo.
- **Doble extorsión/chantaje:** Cifra tus datos y, además, los sustrae, amenazando con publicarlos si no pagas lo que piden.
- **Ransomware como servicio (RaaS):** Modelos donde los creadores del ransomware dejan que otros usen su sistema a cambio de una parte del dinero que obtengan.
- **Phishing/Spear-phishing:** Emails con malas intenciones que traen links o archivos adjuntos peligrosos.
- **Aprovechamiento de debilidades:** Sacar partido de errores de seguridad en programas o sistemas (como VPNs, RDP).
- **Ataques de fuerza bruta a RDP:** Intentos de acertar las claves para entrar de forma remota.
- **Software pirata o ilegal:** Bajar programas que traen virus escondidos.
- **Ataque a la cadena de suministro:** Ataques pensados para proveedores de software o servicios que sirven para colarse en otras empresas.

La norma ISO/IEC 27035, integrada dentro del conjunto de estándares ISO/IEC 27000 (que abarca la ISO/IEC 27001 sobre sistemas de gestión de seguridad de la información), se dedica particularmente al manejo de sucesos de seguridad. Este estándar se organiza en distintos apartados, resaltando los siguientes:

- **ISO/IEC 27035-1:2016:** Aspectos básicos de la gestión de incidentes y la respuesta. Establece los fundamentos clave y el esquema para la gestión de incidentes, abarcando la definición de incidente, evento y la estructuración de un equipo de respuesta.
- **ISO/IEC 27035-2:2016:** Sugerencias para la planificación y la preparación ante incidentes. Considera la creación de normativas, procesos, planes, formación y sensibilización, así como la infraestructura indispensable.
- **Preparación y Diseño Estratégico:** Se trata de forjar una directriz de seguridad informática, repartiendo responsabilidades (como formar un equipo de respuesta

a incidentes, el CSIRT), delineando procesos claros, capacitando al personal, adoptando las herramientas correctas y pactando con socios externos. Si hablamos de ransomware, es crucial tener respaldos de seguridad fuera de línea y verificados, planes B listos y equipos de reacción bien entrenados.

- **Identificación y Aviso:** Implica un monitoreo constante de la actividad de seguridad (a través de registros, SIEM, EDR), detectando anomalías y avisando rápidamente sobre posibles problemas. En el caso del ransomware, detectarlo pronto es clave para detener su avance.
- **Análisis y Decisiones Clave:** Se busca determinar si un suceso es un incidente de seguridad real, ordenarlo por tipo e importancia, y decidir la mejor forma de actuar. Esto requiere medir la dimensión, el posible daño y la seriedad de un ataque de ransomware.
- **Actuación ante Incidentes:** Puesta en marcha de acciones planeadas para frenar, suprimir y reparar el daño. Si nos enfrentamos a un ransomware, esto puede significar aislar computadoras, cortar conexiones de red, quitar el software dañino y recuperar información desde las copias de seguridad.
- **Lecciones Aprendidas:** Revisión tras el incidente, registro de lo sucedido, identificación de lo que se aprendió y aplicación de mejoras para fortalecer la protección y perfeccionar la gestión de la seguridad informática a futuro. Este punto es vital para evitar que los ataques de ransomware se repitan.

La norma ISO/IEC 27035 no opera de forma aislada. Está intrínsecamente ligada a:

- **ISO/IEC 27001:** Este estándar es la piedra angular para instaurar, implementar, sostener y optimizar constantemente un Sistema de Gestión de la Seguridad de la Información (SGSI).
- **La ISO 27035:** actúa como un componente clave dentro del SGSI de la 27001.
- **ISO/IEC 27002:** Facilita un abanico de prácticas recomendadas para los controles vinculados a la seguridad de la información.

- **Marco de Ciberseguridad del NIST:** Se trata de un esquema opcional que se apoya en estándares, lineamientos y prácticas ya consolidadas, con el fin de apoyar a las organizaciones en la gestión y mitigación de los riesgos en ciberseguridad. Abarca funciones de Identificación, Protección, Detección, Respuesta y Recuperación, que se alinean con la ISO 27035.

METODOLOGÍA

La presente investigación se desarrolló bajo un enfoque cualitativo, utilizando como método una revisión bibliográfica y documental sistemática. Este enfoque es el más apropiado para el objetivo del estudio, que consiste en analizar y sintetizar el conocimiento existente sobre la aplicación de la norma ISO/IEC 27035 para la creación de protocolos de contención de ransomware. A diferencia de un estudio empírico, esta metodología no busca generar datos nuevos a partir de experimentos o interacciones directas, sino consolidar y estructurar la información disponible en fuentes académicas y especializadas para construir un argumento coherente y fundamentado.

El proceso de recolección de información se centró en la consulta de una variedad de fuentes de alta fiabilidad. Las principales fuentes incluyeron:

- **Estándares internacionales:** Principalmente la documentación oficial de la serie ISO/IEC 27000, con un enfoque específico en las directrices de la norma ISO/IEC 27035:2016 sobre la gestión de incidentes de seguridad.
- **Artículos científicos y académicos:** Publicaciones de revistas y conferencias especializadas en ciberseguridad, seguridad de la información y gestión de riesgos tecnológicos.
- **Informes de organismos de ciberseguridad:** Documentos y análisis publicados por entidades como el NIST (Instituto Nacional de Estándares y Tecnología de EE. UU.) y agencias de seguridad informática.
- **Literatura técnica y libros especializados:** Textos que abordan la naturaleza del ransomware, sus vectores de ataque y las estrategias de defensa y recuperación.

La búsqueda de información se guio por palabras clave como "ransomware", "gestión de incidentes", "ISO/IEC 27035", "protocolos de contención", "respuesta a incidentes" y "ciberseguridad". La selección de los documentos se basó en criterios de relevancia, actualidad y autoridad de la fuente.

El análisis de la información recopilada se realizó mediante una síntesis de contenido. Este proceso implicó la identificación de conceptos clave, la comparación de enfoques y la estructuración de los hallazgos en temas centrales. El análisis se enfocó en extraer los principios fundamentales de la norma, las fases del ciclo de vida de la gestión de incidentes y las mejores prácticas recomendadas por expertos para aplicarlas específicamente a la amenaza del ransomware. De esta manera, se construyó un marco teórico y práctico sólido, derivado exclusivamente de la literatura existente, para fundamentar las conclusiones y recomendaciones del estudio.

RESULTADOS

La revisión sistemática de la literatura especializada permite estructurar los hallazgos en tres áreas clave que, en conjunto, establecen el fundamento para el uso de la norma ISO/IEC 27035 como pilar en la lucha contra el ransomware.

La investigación documental confirma que el ransomware es una amenaza compleja y en constante evolución, cuyas características demandan una respuesta estructurada. La literatura describe su trayectoria desde ataques simples hasta tácticas sofisticadas como la "doble extorsión", donde los atacantes no solo cifran los datos, sino que amenazan con su publicación. Este tipo de ataque impacta directamente los tres pilares de la seguridad de la información: compromete la confidencialidad al acceder y robar datos, destruye la Integridad al cifrarlos y anula la Disponibilidad al bloquear el acceso a sistemas críticos. Los vectores de ataque documentados son variados, abarcando desde el phishing y la explotación de vulnerabilidades de software hasta ataques a la cadena de suministro, lo que demuestra que ninguna organización está exenta de riesgo.

El análisis de los marcos de trabajo de ciberseguridad revela un consenso en torno a la necesidad de una Gestión de Incidentes de Seguridad (GSI) formalizada. La literatura

establece que un programa de GSI eficaz se compone de un ciclo de vida bien definido, que generalmente incluye las fases de: Preparación, donde se establecen políticas, se forman equipos y se despliegan herramientas; Detección y Análisis, para identificar anomalías y confirmar incidentes; Contención, para limitar el daño y la propagación del ataque; Erradicación, para eliminar la causa raíz de la amenaza;

Recuperación, para restaurar la operación normal; y Actividades Post-incidente o "Lecciones Aprendidas", para mejorar las defensas futuras. Este ciclo de vida no es una mera sugerencia teórica, sino un modelo operativo validado y recomendado por expertos para pasar de una respuesta caótica e improvisada a una acción coordinada y eficaz.

La investigación identifica a la norma ISO/IEC 27035 como el estándar por excelencia para la gestión de incidentes. La norma no opera de forma aislada, sino que se integra en el ecosistema de la seguridad de la información, complementando a la ISO/IEC 27001 (que establece el sistema de gestión global) y a la ISO/IEC 27002 (que ofrece un catálogo de controles). Específicamente, la ISO/IEC 27035 detalla las fases del ciclo de vida de la gestión de incidentes, ofreciendo directrices claras para cada una. Por ejemplo, en la fase de:

Preparación, la norma insiste en la creación de un Equipo de Respuesta a Incidentes de Seguridad (CSIRT) y en la realización de simulacros.

Para la Contención de un ransomware, las acciones derivadas de la norma incluirían el aislamiento inmediato de los sistemas afectados.

La fase de Lecciones Aprendidas se presenta como un componente vital para la mejora continua y la prevención de futuros ataques similares.

Tabla 1: Datos Basados en la investigación

Aspecto Mejorado	**Descripción del Impacto**
Capacidad de Respuesta	Mejora en la capacidad de la entidad para responder a los ataques, con una disminución del tiempo requerido para identificar y reaccionar.

Coordinación Interna	Mejoras en la coordinación entre equipos y departamentos gracias a una distribución de roles más clara.
Impacto Operativo	Atenuación del impacto operativo, minimizando la pérdida de información y el tiempo de inactividad.
Concientización y Formación del Personal	Impulso en la concientización y formación del personal, lo que fortaleció la cultura de seguridad.
Identificación y Subsanación de Carencias	Permitió identificar y corregir deficiencias en la plataforma tecnológica.

Desarrollado por los autores

Tabla 2: Historial de casos de Ransomware en el Ecuador.

Fecha del Incidente	**Entidad/Organización Afectada**	**Tipo de Ciberataque**	**Impacto Clave / Detalles Relevantes**	**Fuente**
Abril 2019	Cancillería, Presidencia, Banco Central, Ministerios	Ciberataques (ej. DDoS)	Más de 40 millones de ataques por Anonymous tras caso Assange.	(Velásquez, 2019)
Septiembre 2019	Seis entidades públicas (incl. IESS, Registro Civil)	Filtración Masiva de Datos	Exposición de datos personales de 20 millones de ecuatorianos (incl. fallecidos) de un servidor no seguro de Novaestrat.	(Velásquez, 2019)
Febrero 2021	Banco Pichincha, Ministerio de Finanzas	Ciberataque (no especificado como	Interrupción de operaciones bancarias y afectación al	(Onofa, 2022)

Fecha del Incidente	Entidad/Organización Afectada	Tipo de Ciberataque	Impacto Clave / Detalles Relevantes	Fuente
		ransomware, pero disruptivo)	Ministerio de Finanzas.	
Octubre 2021	Banco Pichincha	Ciberataque (no especificado como ransomware, pero disruptivo)	Interrupción de operaciones, cajeros automáticos y banca en línea. Considerado uno de los mayores ataques globales del año.	(Onofa, 2022)
Marzo 2022	CIES (Centro de Inteligencia Estratégica)	Ciberataque	Compromiso de información procesada por CIES, subsistemas de inteligencia de Policía y FF.AA.	(Onofa, 2022)
Abril 2022	Municipio de Quito	Ransomware (BlackCat)	Afectación del 20% del contenido de la base de datos de la administración central.	(Onofa, 2022)
Octubre 2022	Comando Conjunto de las FF.AA. de Ecuador	Rumor de Ransomware (BlackCat)	Negado oficialmente, pero el grupo BlackCat lo añadió a su sitio de filtraciones, indicando una posible amenaza.	(Greig, 2022)

Desarrollado por los autores

Tabla 3: Impacto de la ISO/IEC 27035 y sus Indicadores de Rendimiento

Aspecto Mejorado	Descripción del Impacto	Indicadores Clave de Rendimiento (KPIs) Sugeridos	Fuente de KPI
Capacidad de Respuesta	Mejora en la capacidad de la entidad para responder a los ataques, con una disminución del tiempo requerido para identificar y reaccionar.	- Reducción del Tiempo Medio de Detección (MTTD) - Reducción del Tiempo Medio de Respuesta (MTTR)	(Lee, 2025)
Coordinación Interna	Mejoras en la coordinación entre equipos y departamentos gracias a una distribución de roles y responsabilidades más clara.	- Reducción del número de errores en la escalada de incidentes. - Cumplimiento de los Acuerdos de Nivel de Servicio (SLA) de comunicación interna durante un incidente.	(Panda, 2024)
Impacto Operativo	Atenuación del impacto operativo, minimizando la pérdida de información y el tiempo de inactividad de los servicios.	- Reducción del Tiempo Medio de Recuperación (MTTRc) - Disminución del costo financiero por incidente y del tiempo de inactividad del negocio.	(Lee, 2025)

Aspecto Mejorado	Descripción del Impacto	Indicadores Clave de Rendimiento (KPIs) Sugeridos	Fuente de KPI
Concientización y Formación	Impulso en la concientización y formación del personal, lo que fortaleció la cultura de seguridad en toda la organización.	- Aumento en la tasa de reporte de correos de phishing por parte de los empleados. - Disminución en la tasa de éxito de campañas de phishing simuladas.	(Sunil Chaudhary, 2022)
Identificación y Subsanación de Carencias	Permitió identificar y corregir de manera proactiva las deficiencias en la plataforma tecnológica y en los procesos de seguridad.	- Aumento en el porcentaje de parches de vulnerabilidades críticas aplicados dentro del plazo definido. - Reducción de incidentes recurrentes causados por la misma vulnerabilidad raíz.	(Hodge, 2025)

Desarrollado por los autores

DISCUSIÓN

La discusión de estos resultados documentales permite argumentar por qué la adopción de un marco formal como la ISO/IEC 27035 es una estrategia no solo beneficiosa, sino esencial en el contexto actual de ciber amenazas.

La naturaleza multifacética del ransomware, con sus tácticas de doble extorsión y sus diversos vectores de ataque, hace que las defensas puramente preventivas sean insuficientes. La literatura es clara al señalar que los ciberataques son inevitables. Por lo

tanto, la capacidad de una organización para responder y recuperarse se convierte en un diferenciador crítico.

La adopción de la ISO/IEC 27035 traslada a las organizaciones desde una postura reactiva e improvisada, caracterizada por la confusión y la demora, hacia un modelo proactivo y organizado. La estructura que provee la norma, con roles definidos y procesos claros, es precisamente la antítesis del caos que un ataque de ransomware busca generar. Al tener un plan de contención predefinido, se reduce drásticamente el tiempo que los atacantes tienen para moverse lateralmente y cifrar activos críticos, minimizando así el impacto operativo y financiero. Así mismo, la implementación de este estándar fomenta una transformación cultural profunda. La norma va más allá de los controles técnicos y enfatiza la importancia de la preparación y la concienciación del personal. Este enfoque convierte al "factor humano", a menudo citado como el eslabón más débil de la cadena de seguridad, en un activo de defensa. Un personal capacitado para reconocer intentos de phishing o para reportar actividades anómalas de manera temprana acelera la fase de "Detección y Aviso", lo que puede marcar la diferencia entre un incidente menor y un desastre a gran escala. Este fortalecimiento de la cultura de seguridad crea una resiliencia organizacional que perdura más allá de cualquier tecnología específica.

El principio de "Lecciones Aprendidas", consagrado en la norma, institucionaliza un ciclo de mejora continua. Cada incidente, o incluso cada simulacro, se convierte en una oportunidad para identificar debilidades estructurales, ya sea en la configuración tecnológica, en los procedimientos internos o en la capacitación del personal. Este proceso de retroalimentación asegura que la organización no solo se recupere del incidente actual, sino que fortalezca su postura de seguridad para el futuro.

Esta evidencia documental demuestra que la ISO/IEC 27035 no es un simple formalismo burocrático, sino una herramienta estratégica y práctica que dota a las organizaciones de la estructura, la disciplina y la cultura necesarias para gestionar eficazmente una de las ciber amenazas más críticas de nuestro tiempo.

CONCLUSIONES

La aplicación de la norma ISO/IEC 27035 demostró ser una herramienta eficaz para establecer protocolos de contención ante ataques de ransomware en infraestructuras tecnológicas. A través de la investigación realizada, se evidenció que una adecuada gestión de incidentes no solo mejora la capacidad de respuesta y recuperación, sino que también fortalece la seguridad organizacional en su conjunto. La integración de esta norma permite anticiparse a amenazas, minimizar impactos y fomentar una cultura preventiva en torno a la ciberseguridad.

La implementación de la norma ISO/IEC 27035 marca una evolución estratégica fundamental, permitiéndonos pasar de una ciberseguridad reactiva a una proactiva. Esta capacidad para anticipar las amenazas de ransomware, en lugar de solo responder a ellas, es crucial en el panorama actual.

Al adoptar este estándar, reducimos significativamente los impactos negativos de un ataque, protegiendo todo, desde la continuidad operativa y las finanzas hasta la reputación de nuestra marca. El marco de trabajo que establece, con roles claros y procedimientos definidos, elimina la confusión durante una crisis, lo que acelera de forma directa la capacidad de recuperación del negocio.

Más allá de los aspectos técnicos, la implementación de la norma ISO/IEC 27035 cultiva de forma orgánica una cultura de seguridad que permea toda la organización. La capacitación continua, pilar fundamental de la norma, transforma a los empleados en un componente activo de nuestra defensa.

Este enfoque colectivo genera un doble beneficio estratégico: por un lado, reduce las vulnerabilidades al integrar prácticas seguras en las rutinas diarias y, por otro, acelera la detección de incidentes gracias a una mayor vigilancia. En esencia, fortalece la resiliencia de la organización desde su base, su personal, para la mejora de los mismos.

e-ISSN: 2528-8091
Vol. 10, N° V CICACI - 2025

Bibliografía

Ayerd, A. (27 de Noviembre de 2023). *Ciberataques: ¿Cómo proteger a tu empresa?* Obtenido de Docu Ware: https://start.docuware.com/es/blog/ciberataques-proteger-empresa

Greig, J. (31 de Octubre de 2022). *Ecuador's military denies ransomware attack after website goes offline.* Obtenido de The Record: https://therecord.media/ecuadors-military-denies-ransomware-attack-after-website-goes-offline

Hernadez, S. (27 de Marzo de 2025). *Fortalece estrategias y Políticas de Ciberseguridad: ISO 27032:2023*. Obtenido de Global Suite: https://www.globalsuitesolutions.com/es/estrategias-politicas-de-ciberseguridad-iso-iec-27032-2023/

Hodge, S. (11 de Mayo de 2025). *Key Metrics to Measure the Effectiveness of Your Incident Response.* Obtenido de CyberRisklnsight: https://www.cyberriskinsight.com/cyber-incident/key-metrics-measure-effectiveness-incident/

ISO/IEC 27035 Gestión de Incidentes de Seguridad. (16 de Julio de 2020). Obtenido de Esginnova Group: https://www.pmg-ssi.com/2020/07/iso-iec-27035-gestion-de-incidentes-de-seguridad/

Lee, S. (11 de Junio de 2025). *Mastering Incident Response with KPLs.* Obtenido de Number Analytics: https://www.numberanalytics.com/blog/mastering-incident-response-with-kpis

Natalucci, F. (10 de Abril de 2024). *Las crecientes amenazas cibernéticas, una grave preocupación para la estabilidad financiera* . Obtenido de IFM Blog: https://www.imf.org/es/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

Onofa, M. (30 de Junio de 2022). *Ataques cibernéticos amenazan seguridad en Ecuador.* Obtenido de Dialogo Americas: https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-ecuador/

Panda, B. (8 de Octubre de 2024). *Why measure incident response metrics and KPIs?* Obtenido de Big Panda: https://www.bigpanda.io/blog/guide-to-incident-response-metrics-and-kpis/

Sunil Chaudhary, V. G. (23 de Mayo de 2022). *Developing metrics to assess the effectiveness of cybersecurity awareness program.* Obtenido de Journal of CyberSecurity: https://academic.oup.com/cybersecurity/article/8/1/tyac006/6590603

Velásquez, F. (9 de Octubre de 2019). *Cybercrime in Ecuador: An Asymmetrical Threat.* Obtenido de thesecuritydistillery: https://thesecuritydistillery.org/all-articles/cybercrime-in-ecuador-an-asymmetrical-threat