

<https://doi.org/10.69639/arandu.v13i3.2590>

Plataforma de gestión automatizada de incidentes de ciberseguridad orientada al fortalecimiento de la continuidad del negocio

Automated cybersecurity incident management platform aimed at strengthening business continuity

Gustavo Eduardo Fernández Villacrés

gustavo.fernandez@iste.edu.ec

<https://orcid.org/0000-0003-1028-1224>

Instituto Superior Tecnológico España
Ambato – Ecuador

Artículo recibido: 10 agosto 2026- Aceptado para publicación: 16 septiembre 2026

Conflictos de intereses: Ninguno que declarar.

RESUMEN

El presente trabajo investigativo surge del poco interés del sector empresarial de Tungurahua en cuanto a los incidentes de ciberseguridad y su relación con la continuidad del negocio. En Ecuador, la evidencia disponible demuestra una creciente exposición de las organizaciones a incidentes y vulnerabilidades de ciberseguridad; sin embargo, existe limitada evidencia empírica que cuantifique específicamente el efecto de estos incidentes sobre la continuidad operativa del sector empresarial. Se ha realizado una investigación de campo entre 235 empresas de Tungurahua, consultándoles sobre que están haciendo para la prevención de incidentes de ciberseguridad, además se ha diagnosticado sobre el nivel de incidencia en la continuidad del negocio, el estudio fue cuantitativo, transversal y correlacional, la técnica fue la encuesta y el instrumento el cuestionario. Se trabajó el cuestionario con una escala de Likert de 5 opciones, se validó el mismo mediante un alfa de Cronbach y mediante expertos. Los hallazgos importantes son que: no es prioritario para las empresas de Tungurahua la prevención de incidentes de ciberseguridad, además que los mismos no influyen mayormente en la continuidad del negocio, esto a pesar de que los problemas de ciberseguridad se acrecientan a nivel nacional, sobre todo en el sector de medianas y grandes empresas, por lo mencionado anteriormente, el trabajo investigativo se justifica plenamente. Finalmente se concluye que una gestión automatizada de incidentes de ciberseguridad fortalecería la seguridad de la información empresarial y esto elevaría el nivel de continuidad del negocio.

Palabras clave: incidentes, ciberseguridad, gestión automatizada, continuidad del negocio

ABSTRACT

This research stems from the business sector in Tungurahua showing little interest in cybersecurity incidents and their relationship to operational continuity. In Ecuador, available evidence indicates that organizations are increasingly exposed to cybersecurity incidents and vulnerabilities; however, there is limited empirical evidence specifically quantifying the impact of these incidents on the operational continuity of the business sector. Field research was conducted involving 235 companies in Tungurahua to assess their cybersecurity incident prevention measures and the impact of such incidents on their operational continuity. The study was quantitative, cross-sectional, and correlational in nature, utilizing surveys administered via questionnaires. A 5-point Likert scale was employed for the questionnaire, which was validated through Cronbach's alpha and expert review. Key findings indicate that preventing cybersecurity incidents is not a priority for companies in Tungurahua, nor do such incidents significantly impact operational continuity even though cybersecurity issues are escalating nationwide, particularly among medium-sized and large enterprises. Given these circumstances, this research is fully justified. Finally, the study concludes that automated cybersecurity incident management would strengthen corporate information security and enhance operational continuity.

Keywords: incidents, cybersecurity, automated management, operational continuity

Todo el contenido de la Revista Científica Internacional Arandu UTIC publicado en este sitio está disponible bajo licencia Creative Commons Attribution 4.0 International. 

INTRODUCCIÓN

La continuidad del negocio puede entenderse como la capacidad de una organización para mantener sus procesos y servicios esenciales durante una situación disruptiva y recuperar progresivamente sus operaciones hasta alcanzar condiciones normales de funcionamiento. Desde esta perspectiva, la continuidad no se limita a reaccionar ante una emergencia, sino que comprende actividades de planificación, prevención, respuesta, recuperación y mejora continua que permiten disminuir el impacto de los eventos que puedan afectar el funcionamiento empresarial. (Standardization International Organization for ISO 22301:2019, 2019)

La continuidad del negocio también puede conceptualizarse como la capacidad institucional para sostener las funciones, procesos y recursos considerados esenciales durante y después de una interrupción significativa. Bajo este enfoque, resulta fundamental que la empresa identifique previamente sus actividades críticas y establezca procedimientos que permitan mantenerlas o restablecerlas dentro de periodos aceptables. El National Institute of Standards and Technology señala que los planes de continuidad comprenden instrucciones y procedimientos previamente definidos para asegurar que los procesos esenciales de una organización puedan mantenerse durante una disrupción y continuar posteriormente hasta su recuperación (National Institute of Standards and Technology, 2010)

Desde una perspectiva asociada con la resiliencia, la continuidad del negocio representa la capacidad de una organización para absorber los efectos de una perturbación, mantener la prestación de operaciones críticas y recuperar oportunamente los niveles de funcionamiento requeridos. Este concepto reconoce que las empresas están expuestas a amenazas tecnológicas, humanas, naturales y organizacionales, por lo que su capacidad de continuidad depende tanto de la preparación previa como de la rapidez para responder y recuperarse. Galaitsi, S; et. al (2023) sostienen que la continuidad del negocio y la resiliencia operativa comparten el objetivo de preparar a las organizaciones para anticipar, responder y superar las interrupciones, especialmente aquellas que pueden comprometer sus operaciones críticas

La continuidad del negocio está recibiendo una atención cada vez mayor en todas las organizaciones a medida que aumenta la frecuencia de los incidentes informáticos que generan interrupciones como la pérdida de centros de datos, violaciones de datos o privacidad e incidentes relacionados con la seguridad de las tecnologías de la información o desastres naturales consecuencias de los cambios climáticos, razones por las cuales, surge la necesidad de contrarrestar las amenazas que pueden llegar a impactar a una organización, ocasionando un impacto alto en su nicho de negocio y en sus procesos (Rodriguez, 2020)

Según la norma ISO 27035, “Un incidente de seguridad de la información es indicado por un único o una serie de eventos indeseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar

la seguridad de la información”. (GUÍA TÉCNICA COLOMBIANA GTC-ISO/IEC 27035, 2012, pág. 3).

El estándar define formalmente un incidente como cualquier suceso que comprometa o ponga en peligro inminente la integridad, confidencialidad o disponibilidad de los datos o de los sistemas; o bien, toda acción que represente una transgresión real o una amenaza directa contra las políticas de seguridad y normativas de uso aceptable (Castellanos, 2015).

La gestión de incidentes de ciberseguridad comprende el conjunto estructurado de políticas, procesos y actividades operativas orientadas a identificar, analizar, contener y resolver eventos que amenacen con vulnerar la confidencialidad, integridad o disponibilidad de los activos de información de una organización. En las directrices globales publicadas por el National Institute of Standards and Technology (NIST), establecen que este proceso ha evolucionado de ser una práctica operativa intermitente para constituirse como un pilar fundamental y continuo de la gestión integral de riesgos tecnológicos, debiendo encontrarse acoplado orgánicamente a todas las operaciones del negocio. (National Institute of Standards and Technology, 2010).

La ISO/IEC 27001:2022 es una norma internacional que establece los requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Su propósito principal es ayudar a las organizaciones a identificar, evaluar y tratar los riesgos asociados con la información, mediante políticas, procedimientos y controles de seguridad. La norma se fundamenta en la protección de tres principios esenciales: confidencialidad, integridad y disponibilidad de la información, contribuyendo además a fortalecer la resiliencia frente a incidentes y amenazas de ciberseguridad. Puede ser aplicada en organizaciones públicas o privadas, independientemente de su tamaño o actividad económica. (International Organization for Standardization, & International Electrotechnical Commission, 2022).

La ISO/IEC 27035 es una norma internacional orientada a la gestión de incidentes de seguridad de la información, cuyo propósito es establecer un enfoque estructurado para preparar, identificar, reportar, evaluar, responder y aprender de los incidentes que puedan afectar los activos de información de una organización. Su aplicación permite fortalecer la capacidad institucional para actuar de manera oportuna frente a eventos de ciberseguridad, reducir sus impactos y mejorar progresivamente los procedimientos de respuesta. La norma promueve una gestión integral del incidente a lo largo de su ciclo de vida, incorporando actividades de planificación, detección, análisis, contención, tratamiento y revisión posterior. Además, resalta la importancia de definir responsabilidades, establecer mecanismos de comunicación y conservar evidencias que permitan comprender las causas del incidente y prevenir su recurrencia. (International Organization for Standardization, & International Electrotechnical Commission, 2023)

Las fases de la ISO/IEC 27035 para la gestión de incidentes de seguridad de la información pueden resumirse en cinco etapas principales:

- **Planificación y preparación:** se establecen políticas, procedimientos, responsabilidades, equipos de respuesta, canales de comunicación y recursos necesarios para atender incidentes.
- **Detección y reporte:** se identifican eventos o comportamientos anómalos y se registran o comunican aquellos que puedan constituir un incidente de seguridad de la información.
- **Evaluación y toma de decisiones:** se analiza el incidente, su naturaleza, nivel de gravedad, alcance e impacto, con el fin de determinar las acciones de respuesta más adecuadas.
- **Respuesta al incidente:** se ejecutan medidas de contención, mitigación, recuperación y, cuando corresponde, preservación de evidencias para reducir los efectos sobre la organización.
- **Lecciones aprendidas y mejora continua:** una vez controlado el incidente, se revisan sus causas, la efectividad de la respuesta y las oportunidades de mejora, con el propósito de prevenir recurrencias y fortalecer la gestión de futuros incidentes (International Organization for Standardization, & International Electrotechnical Commission, 2023)

Entre los **principales incidentes de ciberseguridad** tenemos:

- **Phishing.** Mediante un ataque de phishing, un atacante intenta obtener información confidencial, como cuentas de usuarios, datos bancarios y de tarjetas de crédito, y otras credenciales importantes. Como se mencionó anteriormente, el atacante puede usar medios electrónicos, como mensajes de texto o correos electrónicos, y hacerse pasar por un usuario u organización genuina para engañar al usuario final para que haga clic en un enlace o descargue un archivo adjunto. (Kisser, 2020).
- **El vishing** es una técnica de phishing que usa llamadas telefónicas para engañar a los usuarios. Cuando el teléfono ganó popularidad, la gente solo se comunicaba usándolo. Sin embargo, con el avance de la tecnología actual, se pueden hacer llamadas utilizando Voz sobre Protocolo de Internet VoIP, donde un atacante puede imitar organizaciones genuinas para robar información de un usuario. (Walker, 2019).
- **Malware.** Es un término general para diferentes tipos de software malicioso, como spyware, ransomware y virus. El malware es un código desarrollado por los atacantes para atacar un sistema y sus datos asociados o acceder a la red de un tercero. El medio utilizado para liberar malware suele ser el correo electrónico. El correo contiene enlaces o adjuntos que, cuando se hace clic en ellos o se descargan, provocan la ejecución del código malicioso. El programa maligno apareció a finales de la década de 1970, con la introducción del virus Creeper, que amenazaba a usuarios individuales y organizaciones. Desde entonces, el mundo ha visto miles de variantes de malware, todas con la misma intención: interrupción y destrucción de servicios. (Renales, 2024).

- El ransomware es un programa maligno a través del cual los atacantes cifran todos sus datos y exigen un rescate para descifrarlos. Al inicio, los atacantes solían atacar a usuarios individuales con ransomware, pero se dieron cuenta de los beneficios monetarios de atacar a instituciones más grandes, como bancos, hospitales, etc. El ransomware será discutido en profundidad más adelante. (Anchal, 2024).
- El spyware es un tipo de malware usado por los atacantes para espiar las actividades de una persona. Es utilizado mayoritariamente por personas en una relación sentimental para espiarse entre sí, pero los atacantes también utilizan spyware para entender la actividad de un objetivo y registrar sus pulsaciones de teclas. (Moreno, Respuesta a incidentes de ciberseguridad, 2024).
- Los datos y las redes informáticas son vulnerables a numerosos ciberataques, y algunos de ellos fueron discutidos anteriormente en el libro. Por lo tanto, cada empresa, sin importar su tamaño, infraestructura o industria, necesita tener implementadas medidas de seguridad de red. La arquitectura de la red evoluciona y se vuelve más compleja cada día. El entorno de amenazas también cambia constantemente y los atacantes intentan encontrar nuevos métodos para aprovechar vulnerabilidades de seguridad en el sistema. Existen vulnerabilidades en varios aspectos de la infraestructura de red, como datos, dispositivos, aplicaciones y usuarios. Dado esto, existen herramientas individuales disponibles que protegen estos aspectos. Puede usar estas herramientas para probar las aplicaciones para asegurarse de que la empresa cumpla con los términos de cumplimiento regulares. La seguridad de la red es de suma importancia, ya que incluso unos pocos minutos de inactividad pueden dañar la reputación y las finanzas de la organización. (Pavon, P; Romero, M, 2024).

La problemática de la inseguridad informática en el Ecuador puede resumirse en los siguientes aspectos:

El EcuCERT, administrado por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), reportó para el primer semestre de 2025 un total de 220.228 direcciones IP notificadas con incidentes o vulnerabilidades. Entre los principales eventos identificados se encontraron *scanners*, *sinkhole HTTP*, malware, filtraciones de contraseñas, correo malicioso y sitios comprometidos. Adicionalmente, se identificaron 12 víctimas de ransomware y siete víctimas de filtraciones de datos, con afectaciones en sectores como gobierno, comercio, finanzas, salud, educación, construcción, alimentos, electricidad, desarrollo de software e inmobiliario (Agencia de Regulación y Control de las Telecomunicaciones, EcuCERT, 2025).

En el ámbito territorial, Tungurahua también presenta exposición a riesgos de ciberseguridad. Un dato particularmente relevante es que EcuCERT ubicó a Ambato entre las cinco ciudades del Ecuador con mayor número de sistemas vulnerables detectados durante el

primer semestre de 2025, registrando 36 sistemas vulnerables, después de Quito (226), Guayaquil (119) y Cuenca (43). Este resultado constituye un indicador de exposición tecnológica y no debe interpretarse como que existieron exactamente 36 empresas atacadas; sin embargo, demuestra la presencia de infraestructura vulnerable dentro del entorno digital de la ciudad. (Agencia de Regulación y Control de las Telecomunicaciones, EcuCERT, 2025)

Esta situación resulta especialmente relevante para Tungurahua debido a su actividad comercial y productiva. A medida que las empresas de la provincia incorporan sistemas de facturación, plataformas de comercio electrónico, banca electrónica, redes sociales, sistemas administrativos, almacenamiento en la nube y mecanismos digitales de comunicación con clientes y proveedores, aumenta simultáneamente la necesidad de proteger dichos recursos. Una interrupción de estos servicios puede afectar procesos esenciales como ventas, facturación, atención al cliente, producción, inventarios, pagos, logística y comunicación interna, generando tiempos de inactividad y posibles pérdidas económicas.

En síntesis, la evidencia disponible permite establecer que la ciberseguridad y la continuidad operativa mantienen una relación estrecha en el contexto empresarial ecuatoriano. La creciente digitalización incrementa las oportunidades de productividad y competitividad, pero también amplía la superficie de exposición frente a amenazas informáticas. En Tungurahua, particularmente en Ambato, la identificación de sistemas vulnerables refuerza la necesidad de implementar mecanismos preventivos, procedimientos de gestión de incidentes, respaldos de información, planes de recuperación y estrategias de continuidad del negocio. En consecuencia, fortalecer la capacidad de prevención, respuesta y recuperación frente a incidentes de ciberseguridad constituye una condición relevante para reducir interrupciones operativas, proteger la información y garantizar la sostenibilidad de las empresas.

De lo mencionado anteriormente surge la presente **pregunta de investigación:**

¿Cómo garantizar la continuidad del negocio ante la presencia frecuente de incidentes de ciberseguridad?

Como respuesta a la pregunta, surge esta investigación cuyo objetivo general fue: “Proponer el desarrollo de una plataforma de gestión automatizada de incidentes de ciberseguridad, para que en base a su aplicación se fortalezca la seguridad y confidencialidad de la información y con ello se eleve la continuidad del negocio”.

Para lograr el objetivo general se proponen los siguientes objetivos específicos:

- Diagnosticar el nivel de gestión de los incidentes de ciberseguridad en el sector empresarial, considerando los mecanismos de detección, clasificación, respuesta y seguimiento implementados.
- Evaluar la continuidad del negocio de las empresas frente a incidentes de ciberseguridad, considerando aspectos como disponibilidad de los servicios, tiempo de interrupción, capacidad de recuperación y existencia de procedimientos de continuidad.

- Analizar metodológicamente la relación existente entre la prevención de incidentes de ciberseguridad y la continuidad del negocio.
- Diseñar una plataforma de gestión automatizado para el control de los incidentes de ciberseguridad.

Las hipótesis con las que se han trabajado en la presente investigación son:

H1: Si existe una relación estadísticamente significativa entre la gestión de incidentes de ciberseguridad y la continuidad del negocio de las empresas de Tungurahua

H0: No existe una relación estadísticamente significativa entre la gestión de incidentes de ciberseguridad y la continuidad del negocio de las empresas de Tungurahua

MATERIALES Y MÉTODOS

Se adoptó un paradigma investigativo de tipo cuantitativo, debido a que permitirán medir numéricamente las variables relacionadas con la gestión de incidentes de ciberseguridad y la continuidad del negocio de las empresas de Tungurahua.

El diseño investigativo fue de tipo no experimental, debido a que las variables fueron observadas en su contexto natural, sin manipulación deliberada por parte del investigador. Asimismo, será de corte transversal, porque la información será recolectada en un único momento durante el período de estudio.

El alcance de la investigación fue: descriptivo, correlacional y propositivo. Fue descriptivo porque permitió caracterizar el estado actual de la gestión de incidentes de ciberseguridad y de la continuidad operativa en las empresas. Es correlacional porque se analizó estadísticamente la asociación entre ambas variables. Finalmente, tiene un componente propositivo porque, a partir de los resultados obtenidos, se diseñó un modelo de gestión automatizada de incidentes de ciberseguridad.

La población estuvo compuesta por 235 empresas de Tungurahua, la unidad de análisis es cada empresa y los informantes son personas relacionadas con las áreas técnicas y operativas.

La muestra se calculó en base a la fórmula de poblaciones finitas de la siguiente manera:

$$n = \frac{NZ^2pq}{e^2(N-1) + Z^2pq}$$

Donde: N=235 Z=1.96 p=0.50 q=0.50 e=0.05

Se utilizó un **nivel de confianza del 95 %** y un **margen de error del 5 %**.

Sustituyendo los valores:

$$\begin{aligned} n &= \frac{235(1.96)^2(0.50)(0.50)}{(0.05)^2(235-1) + (1.96)^2(0.50)(0.50)} \\ n &= \frac{235(3.8416)(0.25)}{0.0025(234) + 3.8416(0.25)} \\ n &= \frac{225.694}{0.585 + 0.9604} \end{aligned}$$

$$n = \frac{225.694}{1.5454}$$

$$n = 146.04$$

Por tanto:

$$\boxed{n = 147 \text{ empresas}}$$

En cuanto a la modalidad de la investigación esta fue esencialmente de campo, porque la información se obtuvo directamente de las empresas de Tungurahua mediante la aplicación del cuestionario.

La técnica de recolección de datos fue la encuesta y el instrumento asociado fue el cuestionario. Se trabajó con un cuestionario con respuestas en la escala de Likert en 5 niveles que fueron: 1 Totalmente en desacuerdo, 2. En desacuerdo, 3. Ni de acuerdo ni en desacuerdo, 4. De acuerdo, 5. Totalmente de acuerdo.

La investigación trabaja con 2 variables que son:

- **Variable independiente:** Gestión automatizada de los incidentes de ciberseguridad, y
- **Variable dependiente:** Continuidad del negocio

El cuestionario definido en base a las variables es:

1. ¿La empresa cuenta con mecanismos que permiten mantener operativos sus sistemas y servicios tecnológicos esenciales ante un incidente de ciberseguridad?
2. ¿Cuándo ocurre un incidente de ciberseguridad, la empresa logra reducir el tiempo de interrupción de sus procesos y servicios críticos?
3. ¿La empresa dispone de procedimientos que permiten recuperar oportunamente sus sistemas, información y procesos después de un incidente de ciberseguridad?
4. ¿La empresa cuenta con planes de contingencia y continuidad que permiten mantener o restablecer sus operaciones frente a incidentes de ciberseguridad?
5. ¿La empresa utiliza herramientas tecnológicas que permiten detectar y generar alertas automáticas ante posibles incidentes de ciberseguridad?
6. ¿La empresa dispone de mecanismos automatizados que permiten clasificar, priorizar y responder oportunamente a los incidentes de ciberseguridad detectados?
7. ¿La empresa utiliza sistemas que registran y realizan seguimiento automático de los incidentes de ciberseguridad para facilitar su análisis y prevenir su recurrencia?

Prueba piloto. Se realizó una prueba piloto con la finalidad de validar el cuestionario, se trabajó con 15 empresas del mismo sector comercial y de tamaños similares, los resultados obtenidos fueron:

Tabla 1
Resultados prueba piloto

Empresas	P1	P2	P3	P4	P5	P6	P7	Sumatoria
1	1	1	1	1	1	1	1	7
2	1	1	1	1	1	1	1	7
3	1	2	1	1	1	1	1	8
4	2	1	2	1	1	1	1	9
5	1	2	1	1	1	2	1	9
6	1	2	1	2	1	2	2	11
7	1	2	1	1	2	1	1	9
8	3	4	2	4	5	2	2	22
9	1	2	1	1	3	1	1	10
10	2	1	4	2	4	2	2	17
11	1	1	1	1	1	1	1	7
12	2	1	2	1	2	2	1	11
13	1	1	1	3	1	1	1	9
14	1	1	1	3	2	1	1	10
15	1	1	1	3	2	1	1	10
Varianzas	0,381	0,695	0,686	1,067	1,552	0,238	0,171	16,257

Nota: Fuente investigación del autor

La confiabilidad del cuestionario se determinó mediante el coeficiente alfa de Cronbach a partir de una prueba piloto aplicada a 15 empresas con características similares a las unidades de estudio. El instrumento estuvo constituido por siete ítems valorados mediante una escala Likert de cinco niveles. Para el cálculo se obtuvo una suma de las varianzas individuales de los ítems de 4,790 y una varianza de la puntuación total de 16,257. Mediante la expresión

$$\alpha = \frac{k}{k-1} \left(1 - \frac{\sum s_i^2}{s_T^2} \right),$$

considerando siete ítems, se obtuvo un coeficiente de $\alpha = 0,823$. Este resultado evidencia una **buena consistencia interna del instrumento**, por lo que se consideró confiable para su aplicación en la muestra definitiva de la investigación.

Validez del contenido del cuestionario mediante expertos y coeficiente V de Aiken.

Se trabajó con 3 expertos los cuales valoraron 4 aspectos fundamentales que fueron:

1. Claridad, 2. Coherencia, 3. Pertinencia, y 4. Relevancia

Los parámetros de la calificación fueron:

1. No cumple, 2. Bajo nivel, 3. Nivel moderado, y 4. Alto nivel

Los resultados emitidos por los expertos son:

Tabla 2
Resultados de los expertos

Preguntas	Criterio	EXP 1	EXP 2	EXP3
P1	Claridad	3	4	3
P2	Claridad	4	4	4
P3	Claridad	4	4	4
P4	Claridad	4	4	3
P5	Claridad	4	3	4
P6	Claridad	3	4	4
P7	Claridad	3	4	3
P1	Coherencia	4	3	4
P2	Coherencia	4	3	4
P3	Coherencia	4	3	4
P4	Coherencia	4	3	4
P5	Coherencia	3	4	3
P6	Coherencia	4	4	4
P7	Coherencia	4	4	4
P1	Pertinencia	4	4	3
P2	Pertinencia	4	3	4
P3	Pertinencia	3	4	4
P4	Pertinencia	3	4	3
P5	Pertinencia	3	4	4
P6	Pertinencia	3	4	4
P7	Pertinencia	3	4	4
P1	Relevancia	3	4	3
P2	Relevancia	4	4	4
P3	Relevancia	4	4	4
P4	Relevancia	4	4	3
P5	Relevancia	4	3	4
P6	Relevancia	3	4	4
P7	Relevancia	3	4	3

Validez de contenido mediante juicio de expertos y V de Aiken. La validez de contenido del instrumento se determinó mediante el juicio de tres expertos, quienes evaluaron los siete ítems del cuestionario considerando cuatro criterios: claridad, coherencia, pertinencia y relevancia. La valoración se realizó utilizando una escala ordinal de cuatro categorías, donde 1 correspondió a

“no cumple”, 2 a “bajo nivel”, 3 a “nivel moderado” y 4 a “alto nivel”. Para cuantificar el grado de acuerdo entre los jueces se empleó el coeficiente V de Aiken mediante la expresión:

$$V = \frac{\sum s}{n(c-1)}, \text{ donde } s = r - l_o, n = 3 \text{ expertos, } c = 4 \text{ categorías y } l_o = 1.$$

Los resultados evidenciaron valores promedio por ítem comprendidos entre 0,833 y 0,944. P2 y P3 alcanzaron los mayores coeficientes, con $V=0,944$, seguidos de P6 con $V=0,917$; P4, P5 y P7 obtuvieron $V=0,861$, mientras que P1 registró $V=0,833$. Al analizar los criterios de forma global se obtuvieron coeficientes de 0,889 para claridad, 0,905 para coherencia, 0,873 para pertinencia y 0,889 para relevancia.

Finalmente, el coeficiente global de validez de contenido fue de V de Aiken = 0,889, resultado que evidencia un alto grado de acuerdo entre los expertos y una adecuada validez de contenido del instrumento. En consecuencia, los siete ítems fueron considerados pertinentes para su aplicación definitiva, aunque se recomendó realizar ajustes menores de redacción en aquellos criterios específicos que presentaron valores de 0,778.

Con el valor V de Aiken global = 0,889 y junto con el alfa de Cronbach = 0,823, el cuestionario presenta evidencia favorable tanto de validez de contenido como de confiabilidad interna.

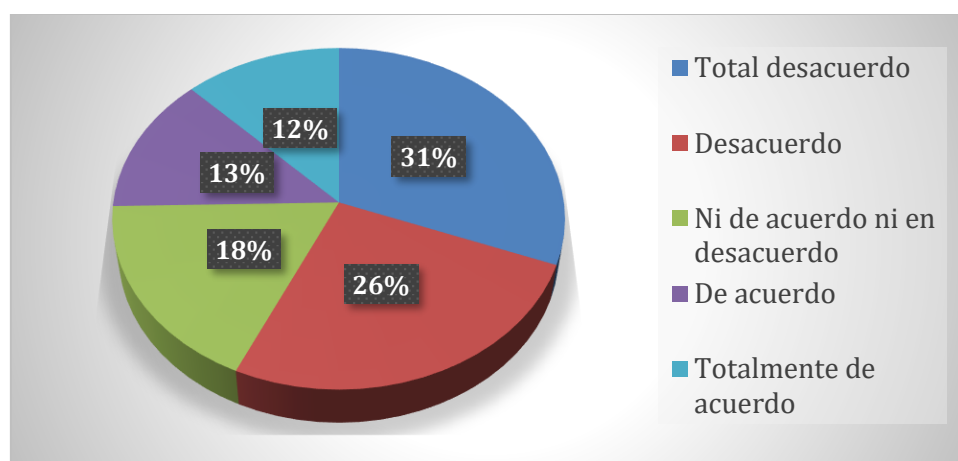
RESULTADOS Y DISCUSIÓN

Luego de la aplicación del instrumento a la muestra calculada se han obtenido los siguientes resultados:

Pregunta No 1. ¿La empresa cuenta con mecanismos que permiten mantener operativos sus sistemas y servicios tecnológicos esenciales ante un incidente de ciberseguridad?

Figura 1

Resultados de la pregunta 1



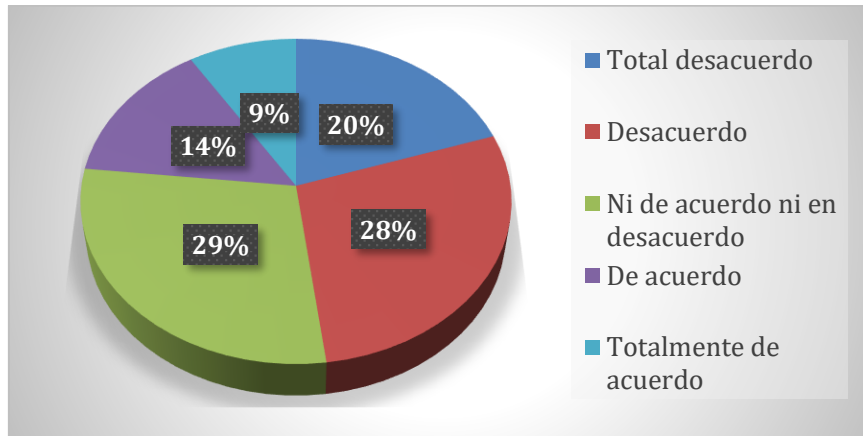
Análisis. El 31% señala que la empresa no cuenta para nada con mecanismos que permiten mantener operativos sus sistemas y servicios tecnológicos esenciales ante un incidente de ciberseguridad, un 26% lo ratifica solo al estar en desacuerdo, un 18% se manifiesta en forma

neutra, un 13% se señala que se cuenta con los mecanismos y un 12% ratifica totalmente que si se dispone.

Pregunta No 2 ¿Cuándo ocurre un incidente de ciberseguridad, la empresa logra reducir el tiempo de interrupción de sus procesos y servicios críticos?

Figura 2

Resultados de la pregunta 2

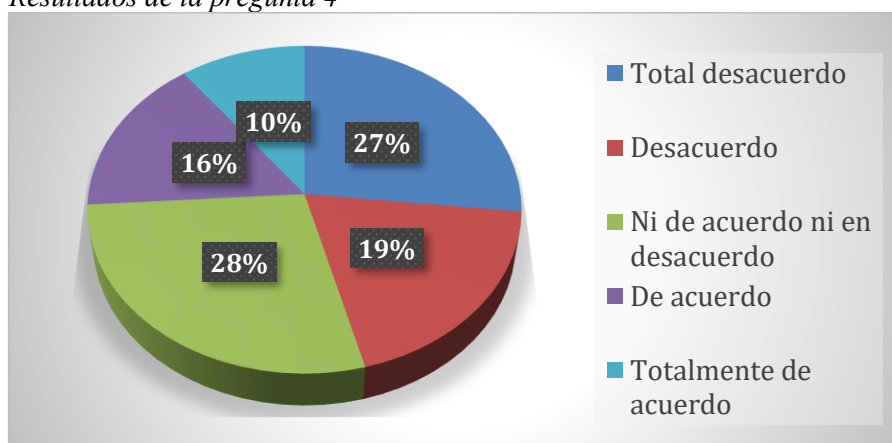


Análisis. Para el 20% de los investigados Cuándo ocurre un incidente de ciberseguridad, la empresa NO logra reducir el tiempo de interrupción de sus procesos y servicios críticos, el 28% lo ratifica mientras que el 29% lo hace en forma neutra, lo que indica el desconocimiento sobre la pregunta, un 14% se manifiesta favorablemente mientras que el 9% lo hace muy favorablemente.

Pregunta No 4 ¿La empresa cuenta con planes de contingencia y continuidad que permiten mantener o restablecer sus operaciones frente a incidentes de ciberseguridad?

Figura 3

Resultados de la pregunta 4

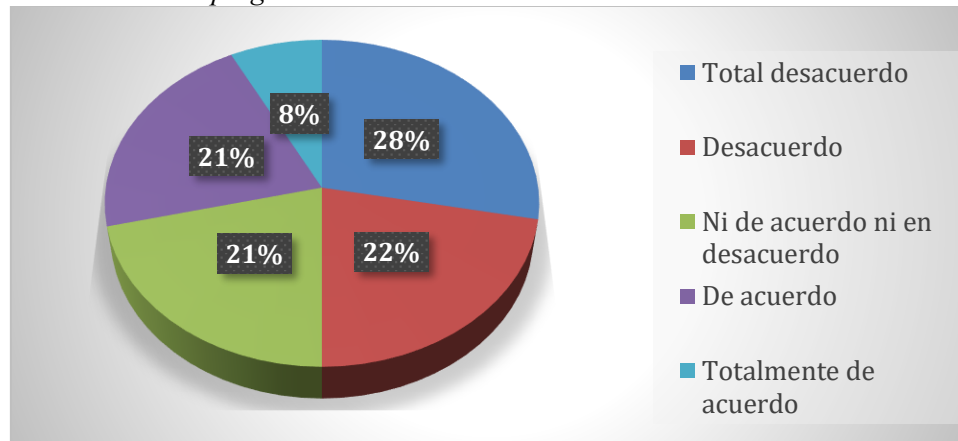


Análisis. El 27% asegura que la empresa NO cuenta con planes de contingencia y continuidad que permiten mantener o restablecer sus operaciones frente a incidentes de ciberseguridad, el 19% ratifica dicho criterio. El 28% se manifiesta en forma neutra lo cual indica

el desconocimiento sobre la pregunta, el 16% indica que si se cuenta con los planes y el 10% lo ratifica plenamente.

Pregunta No 5 ¿La empresa utiliza herramientas tecnológicas que permiten detectar y generar alertas automáticas ante posibles incidentes de ciberseguridad?

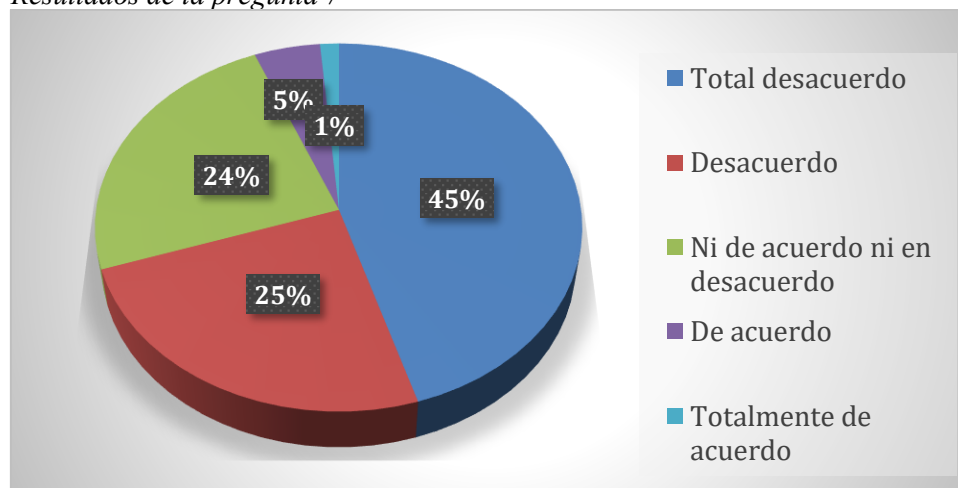
Figura 4
Resultados de la pregunta 5



Análisis. El 28% afirman totalmente que la empresa NO utiliza herramientas tecnológicas que permiten detectar y generar alertas automáticas ante posibles incidentes de ciberseguridad, un 22% lo ratifican al estar de acuerdo, un 21% se manifiesta de forma neutra, lo cual indica el desconocimiento sobre la pregunta, el 21% manifiesta que la empresa si utiliza y el 8% lo ratifica al estar totalmente de acuerdo.

Pregunta No 7 ¿La empresa utiliza sistemas que registran y realizan seguimiento automático de los incidentes de ciberseguridad para facilitar su análisis y prevenir su recurrencia?

Figura 5
Resultados de la pregunta 7



Análisis. Mayoritariamente un 45% afirma que la empresa NO utiliza sistemas que registran y realizan seguimiento automático de los incidentes de ciberseguridad para facilitar su análisis y prevenir su recurrencia, un 25% ratifican la negativa y un 24% se manifiesta de forma neutra. Apenas un 5% se expresa de forma afirmativa y un 1% lo ratifica totalmente

DISCUSIÓN

Los resultados obtenidos muestran una realidad que merece atención en el sector empresarial de Tungurahua: aunque las organizaciones dependen cada vez más de sistemas tecnológicos para desarrollar sus actividades, una proporción importante todavía no dispone de mecanismos suficientes para afrontar de manera organizada los incidentes de ciberseguridad. Este hallazgo permite advertir que la transformación digital de las empresas no necesariamente ha avanzado al mismo ritmo que la incorporación de medidas de protección, respuesta y recuperación. En otras palabras, utilizar más tecnología no significa necesariamente estar mejor preparado para enfrentar una interrupción provocada por un incidente informático.

Esta situación se evidencia inicialmente en los resultados relacionados con la continuidad operativa. El 57 % de los participantes manifestó una posición desfavorable respecto a la existencia de mecanismos que permitan mantener operativos los sistemas y servicios tecnológicos esenciales ante un incidente de ciberseguridad, mientras únicamente el 25 % presentó una valoración favorable. Estos datos sugieren que una parte considerable de las empresas todavía presenta debilidades para mantener sus funciones críticas cuando ocurre un evento que compromete sus recursos tecnológicos.

El resultado coincide con los planteamientos del Instituto Nacional de Ciberseguridad de España INCIBE (2024), que considera que la continuidad del negocio requiere diseñar, implantar y probar previamente un plan que permita recuperar la operación empresarial dentro de un período razonable. Desde esta perspectiva, la continuidad no puede depender únicamente de la reacción del personal cuando el problema ya se ha producido; requiere identificar procesos críticos, establecer responsabilidades y disponer de mecanismos tecnológicos y organizativos de recuperación.

Esta necesidad adquiere especial importancia al analizar la capacidad de las empresas estudiadas para reducir los períodos de interrupción. Los resultados muestran que el 48 % presenta una valoración desfavorable respecto a la capacidad de reducir el tiempo de interrupción de procesos y servicios críticos, mientras el 29 % mantiene una posición neutral y solamente el 23 % responde favorablemente. El predominio de respuestas negativas y neutrales permite inferir que la capacidad de recuperación todavía no constituye una práctica suficientemente consolidada en las organizaciones estudiadas.

Este hallazgo tiene implicaciones que van más allá del área informática. Cuando un sistema tecnológico deja de funcionar, el efecto puede extenderse a facturación, ventas, inventarios, comunicación, atención al cliente, pagos y otras actividades esenciales. El propio contexto analizado en el artículo muestra que la creciente incorporación de comercio electrónico, banca electrónica, almacenamiento en la nube y sistemas administrativos incrementa la dependencia tecnológica de las empresas de Tungurahua. Por ello, gestionar adecuadamente un

incidente de ciberseguridad debe comprenderse también como una acción dirigida a proteger la continuidad del negocio.

Un comportamiento similar se observa respecto a los planes de contingencia y continuidad. El 46 % de los participantes señala que sus empresas no cuentan adecuadamente con estos instrumentos, frente al 26 % que presenta respuestas favorables; adicionalmente, el 28 % adopta una posición neutral. Este resultado es particularmente relevante porque evidencia que las debilidades encontradas no son exclusivamente tecnológicas. También existe una dimensión organizacional relacionada con la planificación y preparación previa frente a posibles interrupciones.

En este sentido, INCIBE (Instituto Nacional de Ciberseguridad, 2024) plantea que un plan de continuidad debe permitir recuperar la operatividad habitual de una empresa en un tiempo razonable y contempla controles relacionados con procesos, tecnología y personas. Esta visión permite interpretar los resultados de Tungurahua desde una perspectiva integral: adquirir herramientas informáticas es importante, pero resulta insuficiente cuando no existen procedimientos, responsables, protocolos de recuperación y una cultura organizacional que permita actuar coordinadamente frente a un incidente.

Los hallazgos correspondientes a la variable gestión automatizada de incidentes de ciberseguridad profundizan esta problemática. En cuanto al uso de herramientas para detectar y generar alertas automáticas, el 50 % presenta una posición desfavorable, el 21 % se mantiene neutral y únicamente el 29 % responde favorablemente. Este comportamiento permite señalar que la automatización todavía tiene una presencia limitada dentro de las empresas analizadas.

La detección temprana constituye precisamente uno de los puntos en los que la automatización puede generar mayor valor. Un sistema que identifica comportamientos anómalos genera alertas, registra los eventos y facilita su clasificación disminuye la dependencia exclusiva de la intervención manual. Esto no significa sustituir al responsable de seguridad, sino proporcionarle información oportuna para tomar decisiones con mayor rapidez. La importancia de fortalecer estas capacidades también es reconocida institucionalmente por INCIBE (2021), cuyo Plan Estratégico 2021-2025 contempla expresamente el fortalecimiento de las capacidades de ciberseguridad de las empresas, con especial atención a las pymes, junto con acciones de sensibilización, formación y generación de conocimiento.

Uno de los resultados más significativos del estudio aparece en el registro y seguimiento automático de incidentes. El 45 % de los participantes se muestra totalmente en desacuerdo con que su empresa utilice sistemas para registrar y realizar seguimiento automático, y otro 25 % manifiesta desacuerdo. Esto significa que el 70 % presenta una valoración negativa; solamente el 6 % responde favorablemente. Este hallazgo constituye una de las evidencias más claras de la brecha existente entre la exposición empresarial a las amenazas digitales y el nivel de automatización utilizado para administrarlas.

Los resultados adquieren mayor relevancia cuando se contrastan con el contexto ecuatoriano. El EcuCERT tiene entre sus funciones la prevención y resolución de incidentes de seguridad informática, la coordinación de la respuesta, el manejo de vulnerabilidades y la emisión de alertas y comunicaciones tempranas (ARCOTEL, 2026). Esto evidencia que la gestión de incidentes se concibe institucionalmente como un proceso que integra componentes preventivos y reactivos, enfoque que debería trasladarse progresivamente al ámbito empresarial.

Además, los datos nacionales incluidos en el propio artículo evidencian que el problema no es hipotético. Para el primer semestre de 2025 se reportaron 220.228 direcciones IP notificadas con incidentes o vulnerabilidades, además de eventos relacionados con malware, filtraciones de contraseñas, correo malicioso, ransomware y filtraciones de datos. En el ámbito territorial, Ambato fue ubicada entre las cinco ciudades del país con mayor número de sistemas vulnerables detectados, con 36 sistemas identificados.

La coexistencia de estos dos escenarios resulta especialmente significativa: por un lado, existe una exposición objetiva a amenazas y vulnerabilidades; por otro, los resultados de la investigación muestran limitaciones en mecanismos de continuidad, planes de contingencia, detección automatizada y seguimiento de incidentes. Esta aparente contradicción permite sostener que el principal desafío no consiste únicamente en reconocer que existen amenazas informáticas, sino en convertir ese reconocimiento en capacidades concretas de prevención, detección, respuesta y recuperación.

Desde una perspectiva empresarial, los hallazgos permiten comprender que la ciberseguridad y la continuidad del negocio no deberían gestionarse como ámbitos independientes. La continuidad busca mantener o recuperar los procesos esenciales frente a una interrupción, mientras la gestión de incidentes procura identificar, contener, responder y aprender de los eventos de seguridad. En la práctica, ambas capacidades convergen: cuanto antes se detecte y gestione adecuadamente un incidente, mayores posibilidades existen de reducir su propagación y recuperar los servicios afectados.

Esta interpretación guarda relación con el enfoque del INCIBE (2024), que incorpora dentro de sus recursos para empresas tanto la gestión de incidentes como la contingencia y continuidad, reconociéndolas como componentes complementarios de la protección empresarial. De esta manera, los resultados encontrados en Tungurahua respaldan la conveniencia de pasar de un modelo predominantemente reactivo hacia uno preventivo y progresivamente automatizado.

En consecuencia, la principal contribución práctica del estudio se encuentra en la necesidad de diseñar un modelo de gestión automatizada adaptado a la realidad empresarial de Tungurahua. El propio artículo establece como objetivo proponer un modelo que contribuya a proteger la seguridad y confidencialidad de la información y elevar la continuidad operativa, incorporando detección, clasificación, respuesta y seguimiento. Los resultados obtenidos

proporcionan una justificación empírica para esta propuesta, especialmente por las debilidades identificadas en detección automática y seguimiento de incidentes.

Un modelo de estas características debería priorizar soluciones realistas para las empresas del entorno, evitando asumir que todas disponen de grandes departamentos de tecnologías de la información. La automatización puede incorporarse progresivamente mediante alertas centralizadas, clasificación de incidentes según criticidad, asignación automática de responsables, registro de evidencias, protocolos de escalamiento, respaldo de información, monitoreo de tiempos de respuesta y generación de reportes posteriores al incidente. Su propósito no sería simplemente incorporar más tecnología, sino reducir el tiempo entre la detección del incidente, la toma de decisiones y la recuperación de las operaciones.

En conjunto, los resultados permiten concluir que existe una brecha entre las necesidades actuales de ciberseguridad y el nivel de preparación observado en una parte importante de las empresas investigadas. Esta brecha resulta particularmente preocupante en un contexto de creciente digitalización y exposición a amenazas. Por ello, la gestión automatizada de incidentes debe entenderse como una herramienta para fortalecer la capacidad organizacional de anticiparse, responder y recuperarse, y no exclusivamente como una solución informática.

Finalmente, los hallazgos respaldan el componente propositivo de la investigación, pero conviene mantener prudencia al establecer relaciones causales. Al tratarse de un estudio no experimental, transversal y correlacional, sus resultados permiten identificar asociaciones y necesidades empresariales, pero no demostrar por sí solos que la automatización cause directamente una mejora de la continuidad operativa. En futuras investigaciones sería pertinente evaluar el modelo propuesto mediante una implementación piloto y comparar indicadores como tiempo medio de detección, tiempo de respuesta, duración de las interrupciones, porcentaje de recuperación de servicios y recurrencia de incidentes antes y después de su aplicación.

CONCLUSIONES

Luego de la investigación se han obtenido las siguientes conclusiones

La investigación evidenció que una parte importante de las empresas de Tungurahua presenta debilidades en su capacidad para mantener la continuidad operativa frente a incidentes de ciberseguridad. El 57 % manifestó una valoración desfavorable respecto a la existencia de mecanismos para mantener operativos sus sistemas y servicios tecnológicos, mientras que el 48 % indicó dificultades para reducir los tiempos de interrupción. Estos resultados muestran que la preparación empresarial frente a eventos disruptivos todavía es limitada.

Se identificó una insuficiente planificación para afrontar incidentes tecnológicos, debido a que el 46 % de los participantes señaló que sus empresas no cuentan adecuadamente con planes de contingencia y continuidad. Esta situación demuestra que las limitaciones existentes no son únicamente de carácter tecnológico, sino también organizacional, ya que se requieren

procedimientos, responsables, protocolos y mecanismos de recuperación previamente establecidos.

La gestión automatizada de incidentes de ciberseguridad presenta un nivel de implementación todavía reducido en las empresas estudiadas. El 50 % de los encuestados manifestó una valoración desfavorable respecto al uso de herramientas para detectar y generar alertas automáticas, mientras que el 70 % señaló que sus organizaciones no utilizan sistemas adecuados para registrar y realizar seguimiento automático de los incidentes. Estos resultados evidencian una brecha importante entre la creciente dependencia tecnológica de las empresas y su capacidad para responder de manera automatizada ante amenazas digitales.

Los hallazgos permiten establecer que la ciberseguridad y la continuidad del negocio deben abordarse de manera integrada, debido a que la capacidad para detectar, clasificar, responder y realizar seguimiento oportuno de un incidente influye en la posibilidad de reducir su impacto y recuperar los servicios afectados.

Los resultados justifican la propuesta de desarrollo de una plataforma de gestión automatizada de incidentes de ciberseguridad adaptado a la realidad empresarial de Tungurahua, orientado a integrar mecanismos de detección, clasificación, respuesta, seguimiento, registro de evidencias y recuperación operativa. Su implementación permitiría fortalecer la seguridad de la información y mejorar la capacidad de las organizaciones para anticiparse, responder y recuperarse frente a incidentes, aunque por el carácter no experimental, transversal y correlacional del estudio, su impacto deberá ser comprobado posteriormente mediante una implementación piloto.

REFERENCIAS

- Agencia de Regulación y Control de las Telecomunicaciones, EcuCERT. (2025). *Estado de la ciberseguridad: Primer semestre 2025*. ARCOTEL. Ecuador. Quito-Ecuador: Arcotel.
- Anchal, M. (2024). *Propuesta de gestión de incidentes de seguridad, mediante la integración de inteligencia*. Quito-Ecuador: Universidad Tecnológica Israel.
- Castellanos, L. (2015). *Seguridad en Informática*. Caracas - Venezuela: Ediciones Venezuela.
- Colombia, G. d. (20 de Diciembre de 2016). *Ministerio de Tecnologías de Colombia*. *Mintic.gob.com*. Recuperado el 8 de Septiembre de 2026, de <https://www.bing.com/ck/a?!&&p=891c2c79d9131f86e8f92dfa1c9c9fc02ba2e5696dd3a5a55aada3607408bff4JmltdHM9MTc4ODczOTIwMA&ptn=3&ver=2&hsh=4&fclid=107d88f7-f9c1-6932-2ec7-9e49fdc16f05&psq=Gu%3%ada+para+la+Gesti%3%b3n+y+Clasificaci%3%b3n+de+Incidentes+de+Seg>
- Cossio, F. (2017). *DISEÑO DE UN MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE UN SGSI*. Bogotá- Colombia: POLITÉCNICO GRANCOLOMBIANO FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS.
- Galaitis, S; et. al. (2023). *Business continuity management, operational resilience, and organizational resilience: Commonalities, distinctions, and synthesis*. *International Journal of Disaster Risk Science*, 14(5), 713–721. <https://doi.org/10.1007/s13753-023-00494-x>.
- Instituto Nacional de Ciberseguridad, I. (2024). *Instituto Nacional de Ciberseguridad [INCIBE]*. (2024). *Protege tu empresa: recursos de ciberseguridad para el sector empresarial*. . *Recursos empresariales de INCIBE*. Madrid - España: INCIBE.
- Instituto Nacional de Estadística y Censos, INEC. (2026). *Principales resultados de la Encuesta Estructural Empresarial 2024*. INEC. Quito-Ecuador: INEC.
- International Organization for Standardization, & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements (3rd ed.)*. ISO. New York: ISO.
- International Organization for Standardization, & International Electrotechnical Commission. (2023). *ISO/IEC 27035-1:2023 Information technology—Information security incident management—Part 1: Principles and process*. ISO. New York: ISO.
- Kisser, Q. (2020). *Ciberseguridad*. Bogota-Colombia: Ra-Ma.
- Leon, V; Tirado, V. (2026). *Optimización de la gestión de incidentes de ciberseguridad con validación de usuario mediante un flujo automatizado de notificación y control de estados*. Lima-Peru: Universidad peruana de Ciencias Aplicadas.

- Mona, L; Uribe, A. (2015). *Sistema de gestión de incidentes de seguridad informática*. Medellín - Colombia: Universidad de San Buena Ventura.
- Moreno, M. (2022). *Gestión de incidentes de ciberseguridad*. Madrid-España: Ra-Ma.
- Moreno, M. (2024). *Respuesta a incidentes de ciberseguridad*. Madrid- España: Ra-Ma.
- National Institute of Standards and Technology, I. (2010). *Contingency planning guide for federal information systems (NIST Special Publication 800-34 Rev. 1)*. U.S. Department of Commerce. New York: ISO.
- Orosia, M. (2022). *Desarrollo de una metodología para la gestión de incidentes de ciberseguridad*. Cataluña-España: Universidad Oberta de Cataluña.
- Pavon, C; Flores, M. (2022). *Mejorar un modelo de gestión de incidentes de seguridad estándar, mediante el uso de una base de conocimiento de ataques a servicios web en ambientes IoT*. Medellín - Colombia: Instituto Tecnológico Metropolitano.
- Pavon, P; Romero, M. (2024). *Incidentes de ciberseguridad*. M'xico-M'xico: Paraninfo.
- Ramirez, L. (15 de Diciembre de 2025). *ISO 27001: UNA PROPUESTA DE GUÍA PARA SU*. Recuperado el 7 de septiembre de 2016, de <https://www.bing.com/ck/a?!&&p=22a232a27cc6624d152a0062da8bfa39d9fbb25d8721fe34226d8e8456afc45JmltdHM9MTc4ODczOTIwMA&ptn=3&ver=2&hsh=4&fclid=107d88f7-f9c1-6932-2ec7-9e49fdc16f05&psq=ISO+27001%3a+UNA+PROPUESTA+DE+GU%c3%8dA+PARA+SU+IMPLEMENTACI%c3%93N%e2%8>
- Renales, R. (2024). *Respuesta a Incidentes de Ciberseguridad: Estrategias y Técnicas para la Gestión Efectiva de Crisis Digitales*. Madrid-España: Kindle.
- Rodriguez, C. (2020). *La importancia de un plan de continuidad del negocio*. Bogota-Colombia: Universidad Piloto de Colombia – Especialización Seguridad Informática .
- Rodríguez, O. (12 de Octubre de 2017). *Universidad Piloto de Colombia. Rodríguez Pinilla Oscar Javier. Continuidad del negocio*. Recuperado el 9 de Septiembre de 2026, de <https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2644/Trabajo%20de%20grado.pdf?sequence=1>
- Standardization International Organization for ISO 22301:2019, I. (2019). *Security and resilience. Business continuity management systems. Requirements*. ISO. ISO.
- Vásquez, H. (11 de Abril de 2012). *Diseño de un plan de continuidad operativa para los principales servicios de tecnología de la información de la sede principal del RENIEC basado en la norma ISO/IEC 27031:201*. Recuperado el 12 de Septiembre de 2026, de <http://hdl.handle.net/10757/65644>
- Walker, B. (2019). *Ciberseguridad Guía completa para principiantes aprende los conceptos básicos y los métodos eficaces de la ciberseguridad*. New -York: Kindle.