DEPÓSITO LEGAL ZU2020000153
ISSN 0041-8811
E-ISSN 2665-0428

Revista de la Universidad del Zulia

Fundada en 1947
por el Dr. Jesús Enrique Lossada

Ciencias del Agro, Ingeniería y Tecnología

Año 17 N° 48
Enero - Abril 2026
Tercera Época
Maracaibo-Venezuela

Análisis de delitos informáticos a través de la Matriz de Riesgos y Diagrama de Calor de Auditoría

Lina Yuliana Moreno Beltrán*
Gianella Granados Mayorga**
Jean Fernanda Gálvez Sabogal***

RESUMEN

El presente estudio tiene como objetivo analizar la utilidad de la matriz de riesgos y el diagrama de calor de auditoría como herramientas para la identificación, evaluación y gestión de los delitos informáticos en instituciones publicas colombianas. La metodología empleada se basa en un enfoque estructurado que comprende la definición del problema, la identificación de amenazas cibernéticas (como fraude, robo de información y accesos no autorizados), la evaluación de su probabilidad e impacto mediante una matriz de riesgos y su representación visual a través de un diagrama de calor. El análisis se desarrolla en alcaldías de los municipios de Fusagasugá, Pasca, Granada, Silvania y Tibacuy, tomando como marco de referencia la normativa colombiana vigente, especialmente la ley 1273 de 2009, la ley 1581 de 2012 y el decreto 1078 de 2025, así como buenas prácticas de seguridad de la información. Como resultados, se espera priorizar los riesgos críticos, fortalecer los sistemas de control interno, facilitar la toma de decisiones preventivas y correctivas, asegurar el cumplimiento normativo y promover una cultura de ciberseguridad que reduzca vulnerabilidades y mejore la protección de los activos digitales del sector público.

PALABRAS CLAVE: Ciberseguridad, Delitos informáticos, Diagrama de calor, Gestión de riesgos, Matriz de riesgos.

*Estudiante de décimo semestre de Contaduría Pública, Universidad de Cundinamarca, Fusagasugá – Cundinamarca, Colombia. ORCID: https://orcid.org/0009-0005-8525-0088. E-mail: lyulianamoreno@ucundinamarca.edu.co

**Estudiante de décimo semestre de Contaduría Pública, Universidad de Cundinamarca, Fusagasugá – Cundinamarca, Colombia. ORCID: https://orcid.org/0009-0006-8107-132X

***Docente del Programa de Contaduría Pública, Universidad de Cundinamarca, Fusagasugá – Cundinamarca, Colombia. ORCID: https://orcid.org/0000-0002-6371-3273

Recibido: 01/10/2025 Aceptado: 03/12/2025

Analysis of Cybercrimes Through the Risk Matrix and Audit Heat Diagram

ABSTRACT

This study aims to analyze the usefulness of the risk matrix and the audit heat map as tools for identifying, assessing, and managing cybercrime in Colombian public institutions. The methodology employed is based on a structured approach that includes defining the problem, identifying cyber threats (such as fraud, data theft, and unauthorized access), assessing their probability and impact using a risk matrix, and visually representing them through a heat map. The analysis is conducted in the municipalities of Fusagasugá, Pasca, Granada, Silvania, and Tibacuy, using current Colombian regulations as a framework, particularly Law 1273 of 2009, Law 1581 of 2012, and Decree 1078 of 2025, as well as information security best practices. As a result, it is expected to prioritize critical risks, strengthen internal control systems, facilitate preventive and corrective decision-making, ensure regulatory compliance, and promote a cybersecurity culture that reduces vulnerabilities and improves the protection of public sector digital assets.

PALABRAS CLAVE: Computer crimes, Cybersecurity, Heat diagram, Risk management, Risk matrix.

Introducción

En la actualidad, los crímenes en línea se han establecido como una de las preocupaciones más relevantes en el ámbito digital, afectando tanto a particulares como a entidades en todo el mundo. El rápido avance tecnológico y la creciente dependencia en los sistemas digitales han facilitado el aumento de actividades delictivas en la web, tales como el fraude en línea, el robo de datos confidenciales y los ataques de ransomware. Ante esta situación, la evaluación sistemática de riesgos se convierte en un elemento crucial para crear e implementar planes de seguridad eficaces. Dentro de este panorama, herramientas como la matriz de riesgos y el diagrama de calor de auditoría juegan un papel vital.

La matriz de riesgos es un recurso fundamental para detectar, analizar y clasificar los peligros vinculados a los delitos en internet, teniendo en cuenta tanto la probabilidad de que ocurran como el impacto posible de cada amenaza. Por otro lado, el diagrama de calor de auditoría proporciona una visualización clara de los resultados recolectados en la matriz, lo que

facilita su comprensión y permite identificar rápidamente las áreas críticas que necesitan atención urgente o intervenciones preventivas. Estas herramientas son esenciales para los expertos en ciberseguridad y auditoría, ya que ofrecen un marco metodológico claro que ayuda en la priorización de acciones correctivas y preventivas frente a amenazas digitales.

Este análisis tiene como objetivo explorar la utilización de la matriz de riesgos y del diagrama de calor de auditoría como herramientas efectivas para la identificación y gestión de delitos informáticos. Durante el estudio, se investigará cómo estas metodologías ayudan a lograr una comprensión más completa de los riesgos cibernéticos, favoreciendo una toma de decisiones bien fundamentada y la protección total de los recursos tecnológicos de las organizaciones.

1. Metodología

El análisis de delitos informáticos utilizando la matriz de riesgos y el diagrama de calor de auditoría se basa en una metodología estructurada que permite identificar, evaluar y gestionar los riesgos asociados a las amenazas cibernéticas. Este enfoque proporciona una comprensión integral de los factores de riesgo y facilita la toma de decisiones informadas en la protección de los activos tecnológicos. A continuación, se describe el marco metodológico que guiará el análisis.

1.1. Definición del problema y objetivos del análisis

El primer paso en el proceso es la definición clara del problema que se desea abordar: los delitos informáticos, los cuales pueden manifestarse de diversas formas, como el robo de datos, fraudes electrónicos, malware, ataques de denegación de servicio, entre otros. El objetivo principal de este análisis es identificar y evaluar los riesgos asociados a estos delitos, y proponer medidas de mitigación. Para ello, se utilizarán la matriz de riesgos y el diagrama de calor, que permitirán priorizar las amenazas y establecer acciones correctivas adecuadas.

1.2. Selección de la muestra y marco de referencia

El siguiente paso es la selección de la muestra la cual es intencionada para las alcaldías de los municipios Fusagasugá, Pasca, Granada, Silvania y Tibacuy, que puede incluir una organización específica que se desarrollara en Excel. El marco de referencia contiene normativas

legales vigentes en materia de seguridad informática, como la Ley de Protección de Datos Personales, así como las mejores prácticas en auditoría de seguridad de la información. En Colombia, la normativa relacionada con la seguridad de la información en las instituciones públicas está regida por un conjunto de leyes, decretos y directrices que buscan garantizar la protección, confidencialidad, integridad y disponibilidad de los datos manejados por las entidades del Estado. Estas regulaciones son fundamentales para fortalecer la confianza pública en los servicios digitales del gobierno y proteger los datos sensibles de los ciudadanos. A continuación, se presenta una descripción de las principales normativas que rigen la seguridad de la información en el sector público en Colombia.

2. Parámetros legales

En Colombia, las normativas vigentes en el país regulan la protección de la información y la ciberseguridad con el objetivo de asegurar la integridad, confidencialidad y transparencia en el manejo de datos, tanto en instituciones públicas como en empresas privadas. Dentro de las normativas pertinentes se encuentran la Ley 1581 de 2012, la cual establece las pautas para salvaguardar los datos personales; la Ley 1273 de 2009, que se centra en la clasificación y penalización de los delitos informáticos; y el Decreto 1078 de 2015, que establece la Política de Seguridad Digital para el Estado. Estas normas legales fortalecen los pilares de legalidad, calidad y seguridad en el tratamiento de la información, y además obligan a las entidades públicas a aplicar medidas técnicas y organizativas para prevenir accesos no autorizados, reducir riesgos cibernéticos y promover una cultura de seguridad informática en línea con estándares internacionales como la norma ISO/IEC 27001.

- **Ley 1581 de 2012: Ley de Protección de Datos Personales**

Esta ley requiere que las entidades públicas tomen las medidas adecuadas para garantizar la protección de la información personal de los ciudadanos. El objetivo es garantizar que los datos personales se manejen de manera transparente y segura, cumpliendo con principios fundamentales como la legalidad, la calidad de los datos y la seguridad.

Específicamente, las instituciones públicas deben crear políticas de seguridad que aseguren la confidencialidad y el acceso restringido a los datos personales que gestionan,

estableciendo procedimientos claros para la recopilación, almacenamiento, uso y eliminación de dichos datos. Congreso de la República de Colombia. (2012).

- **Ley 1273 de 2009: Ley sobre Delitos Informáticos**

Para las instituciones públicas, esta ley implica la obligación de implementar medidas técnicas y organizacionales adecuadas para prevenir el acceso no autorizado a los sistemas de información y la protección contra ataques cibernéticos. establece reglas sobre los delitos informáticos y el uso indebido de los sistemas de información de Colombia. Esta ley abarca delitos que pueden afectar tanto a entidades privadas como públicas, tales como el acceso no autorizado a sistemas de información, la alteración de datos, el fraude electrónico y el ciber espionaje. La ley impone penas penales a quienes cometan delitos relacionados con la información, como aquellos que intenten acceder ilegalmente a datos gubernamentales o manipular información razonable. (Congreso de la República de Colombia, 2009).

- **Decreto 1078 de 2015: Política de Seguridad Digital para el Estado**

El Decreto 1078 de 2015 es uno de los principales marcos legislativos para gestionar la seguridad digital en el sector público. Para garantizar la protección de las actividades de información del estado contra las amenazas cibernéticas, este decreto establece el desarrollo de una política de seguridad digital para las entidades públicas. De acuerdo con estándares internacionales como ISO/IEC 27001, la normativa ordena que cada entidad pública desarrolle y ejecute un sistema para gestionar la seguridad de la información.

Además, el Decreto establece la creación de un Comité de Seguridad de la Información dentro de las entidades públicas, que se encargará de la definición de políticas, la gestión de incidentes de seguridad y la capacitación del personal en prácticas de ciberseguridad. (Presidencia de la República de Colombia, 2015).

3. Resultados esperados

Las instituciones públicas en Colombia deben cumplir con un conjunto robusto de normativas en materia de seguridad de la información que buscan proteger tanto los datos de los ciudadanos como los activos tecnológicos del Estado. La implementación efectiva de estas normativas requiere de políticas claras, la adopción de estándares internacionales de seguridad,

y la capacitación continua del personal en ciberseguridad. En un contexto donde las amenazas cibernéticas están en constante evolución, es fundamental que el sector público mantenga una postura proactiva en la gestión de la seguridad de la información, asegurando la confianza y la transparencia en la administración pública.

4. Resultados

4.1. Delitos Informáticos a través de la Matriz de Riesgos y Diagrama de Calor de Auditoría

Las alcaldías en la región del Sumapaz, Colombia, se encuentran frente a un panorama desafiante en cuanto a seguridad informática, lo que las expone a riesgos que ponen en peligro la continuidad de sus operaciones y la confianza de los ciudadanos. Dentro de los principales riesgos, se destacan los ataques de ransomware, los cuales consisten en encriptar los datos y solicitar un rescate a cambio de su liberación, lo que podría resultar en la paralización de servicios esenciales. Además, el fraude de identidad y el phishing son un riesgo creciente, ya que permiten acceder de manera no autorizada a datos confidenciales a través de estrategias de manipulación psicológica. Estos problemas se agravan debido a la ausencia de políticas sólidas de seguridad y la capacitación limitada del personal.

Otro aspecto a considerar es la vulnerabilidad de la infraestructura tecnológica, la cual se manifiesta a través de sistemas desactualizados y configuraciones inseguras que podrían facilitar la aparición de brechas de seguridad. Asimismo, la intrusión no autorizada a sistemas es un peligro constante, motivado por contraseñas débiles y la falta de controles adecuados. Por último, la carencia de conciencia y formación en ciberseguridad intensifica los riesgos previamente señalados, al hacer que los empleados sean más propensos a ataques específicos y equivocaciones.

Estos riesgos no solamente inciden en la integridad y disponibilidad de los servicios públicos, sino que también impactan en la confianza de los ciudadanos y en el cumplimiento de las normativas de seguridad. Para hacer frente a estos desafíos, es esencial poner en marcha estrategias integrales que integren la modernización tecnológica, la formación constante y el

refuerzo de las políticas de seguridad cibernética, con el propósito de reducir sus efectos y garantizar la salvaguarda de los intereses de la ciudadanía.

Ahora bien, de acuerdo con lo anterior, el análisis de delitos informáticos utilizando la matriz de riesgos y el diagrama de calor de auditoría proporciona un diagnóstico detallado del estado de seguridad de los sistemas y las amenazas cibernéticas que enfrenta una organización. A continuación, se presenta cómo se lleva a cabo este análisis, incluyendo la identificación, ponderación y clasificación de los riesgos para ofrecer un diagnóstico general.

4.2. Identificación de los Riesgos de Seguridad

Las alcaldías de la región del Sumapaz, en Colombia, enfrentan desafíos significativos en términos de seguridad informática, exponiéndose a riesgos que comprometen tanto la continuidad operativa como la confianza de los ciudadanos. Entre los principales riesgos se destacan los ataques de ransomware, que implican el cifrado de datos esenciales para extorsionar a las entidades gubernamentales mediante la exigencia de un rescate. Este problema se ve exacerbado por la falta de políticas robustas de respaldo de datos y la presencia de sistemas tecnológicos desactualizados. Asimismo, el phishing y la suplantación de identidad se han convertido en amenazas comunes, debido a la falta de capacitación del personal para identificar correos fraudulentos o enlaces maliciosos, lo cual facilita el acceso no autorizado a información confidencial (Cámara Colombiana de Informática y Telecomunicaciones, 2022; Ministerio TIC, 2021).

Otro riesgo crítico es la vulnerabilidad en la infraestructura tecnológica, la cual incluye el uso de hardware y software obsoletos que no cumplen con los estándares de seguridad modernos. Esto crea brechas que pueden ser explotadas por ciberdelincuentes, afectando tanto la integridad de los sistemas como la disponibilidad de los servicios. Además, el acceso no autorizado a los sistemas representa una amenaza significativa, impulsado principalmente por la utilización de contraseñas débiles y la carencia de controles efectivos de seguridad. Estas falencias incrementan la exposición de las alcaldías a ciberataques, comprometiendo la información sensible y los procesos administrativos (Ministerio TIC, 2021; Cámara Colombiana de Informática y Telecomunicaciones, 2022).

Finalmente, la falta de concientización y capacitación en ciberseguridad constituye un riesgo transversal que agrava todos los escenarios anteriores. La ausencia de programas formativos regulares deja al personal vulnerable ante amenazas como el phishing y el ransomware. Esto resalta la necesidad de adoptar medidas preventivas, como capacitaciones continuas, simulacros de ciberseguridad, y la implementación de políticas claras para fortalecer la defensa informática. Abordar estos riesgos de manera integral no solo protegerá los sistemas, sino que también garantizará la confianza ciudadana en la gestión gubernamental (Cámara Colombiana de Informática y Telecomunicaciones, 2022; Ministerio TIC, 2021).

En primer lugar, se identificó los principales riesgos de seguridad informática que pueden estar afectando a la organización. Los riesgos se clasifican en diferentes categorías, tales como:

- **Riesgos técnicos**: Falta de actualizaciones de software, vulnerabilidades de seguridad en aplicaciones o sistemas, ataques de malware, errores de configuración de servidores y redes.
- **Riesgos operacionales**: Uso indebido de privilegios por parte del personal, acceso no autorizado a información confidencial, negligencia en la gestión de contraseñas, falta de formación del personal.
- **Riesgos externos**: Phishing, ataques de denegación de servicio, robo de identidad, espionaje cibernético, ransomware.
- **Riesgos legales y regulatorios**: Incumplimiento de normativas de protección de datos, violación de la privacidad de los usuarios, exposición de información sensible debido a fallos en la seguridad.

4.3. Ponderación de los Riesgos en la Matriz de Riesgos

Los riesgos identificados, de cada uno de ellos es ponderado en función de su probabilidad de ocurrencia y el impacto potencial que tendría si se materializara. Para esto, se asignan valores que permiten clasificar los riesgos en una escala. Por lo general, la escala de ponderación va de 1 a 5, donde:

- **Probabilidad de ocurrencia**:
  - 1 = Muy baja
  - 2 = Baja

- 3 = Media
- 4 = Alta
- 5 = Muy alta

- **Impacto**:
  - 1 = Bajo
  - 2 = Moderado
  - 3 = Significativo
  - 4 = Alto
  - 5 = Crítico

Tabla 1: *Matriz de ponderación.*

RIESGOS	CAUSAS	CONSECUENCIAS	IMPACTO	ACCIONES PREVENTIVAS	ACCIONES CORRECTIVAS	RUBRO
Ataques de Ransomware: Este tipo de malware cifra los datos de la entidad, exigiendo un rescate para su liberación. En Colombia, los ataques cibernéticos aumentaron un 30% en 2021 en comparación con el año anterior, afectando tanto a empresas como a entidades gubernamentales (Cámara Colombiana de Informática y Telecomunicaciones, 2022).	Falta de políticas de respaldo de datos, lo que dificulta la recuperación en caso de ataque.	Uso de software no actualizado con vulnerabilidades conocidas. Falta de segmentación en las redes internas, lo que facilita la propagación del ransomware. Descarga de archivos adjuntos sospechosos o enlaces maliciosos en correos electrónicos. -Ausencia de soluciones de detección y respuesta frente a amenazas avanzadas.	Alto: Puede interrumpir operaciones clave y generar pérdida de confianza en los ciudadanos.	Implementar políticas de respaldo periódico y almacenamiento o fuera de línea. Actualizar regularmente software y sistemas operativos. Instalar herramientas de detección de amenazas avanzadas.	Restaurar datos desde copias de seguridad. Contratar expertos en ciberseguridad para eliminar el ransomware. Notificar a las autoridades correspondientes y a los ciudadanos afectados.	Costo Seguridad informática, capacitación.
Phishing y Suplantación de Identidad: Mediante correos electrónicos o mensajes fraudulentos, los	Ausencia de capacitación para los empleados sobre cómo identificar	Uso de cuentas de correo electrónico no seguras. Ausencia de doble factor de	Medio-Alto: Genera problemas de credibilidad y posibles	Capacitar al personal sobre cómo identificar correos y	Revocar credenciales comprometidas inmediatamente. Notificar a los usuarios	Gasto Capacitación, infraestructura tecnológica.

atacantes obtienen información confidencial. La capacitación en temas como phishing es esencial para mitigar este riesgo (Gobierno Digital, 2021).	correos fraudulentos.	autenticación en accesos importantes. Falta de monitoreo activo de intentos de suplantación de identidad. Propagación de sitios web falsos que imitan plataformas legítimas.	sanciones legales.	enlaces fraudulentos. Implementar doble factor de autenticación (2FA). Monitorear y bloquear dominios fraudulentos.	afectados y recomendar cambio de contraseñas. Configurar filtros más estrictos en los sistemas de correo.	
Acceso No Autorizado a Sistemas: La falta de controles de acceso robustos puede permitir que personas no autorizadas manipulen o sustraigan información sensible. En 2020, se reportaron más de 32.000 denuncias relacionadas con ciberataques en Colombia, de las cuales 12.000 correspondieron a hurto por medios informáticos (Gobierno Digital, 2021).	Contraseñas débiles o compartidas entre múltiples usuarios	Sistemas obsoletos sin parches de seguridad aplicados. Configuraciones incorrectas en permisos y privilegios de usuarios. Uso de redes Wi-Fi públicas o no seguras para acceder a sistemas sensibles. Falta de registros y auditorías periódicas de accesos.	Alto: Riesgo significativo para la seguridad y la continuidad operativa.	Establecer contraseñas robustas y políticas de cambio periódico. Limitar los accesos según roles específicos. Realizar auditorías periódicas de accesos.	Revocar accesos sospechosos. Realizar análisis forense para determinar el alcance del acceso. Reconfigurar sistemas de permisos.	Seguridad, auditoría.
Vulnerabilidades en Infraestructura Tecnológica: Sistemas desactualizados o mal configurados pueden ser explotados por ciberdelincuentes. En 2021, se registraron siete billones de intentos de ataques cibernéticos en Colombia, evidenciando la magnitud de la amenaza (Cámara Colombiana de Informática y Telecomunicaciones, 2022).	Uso de hardware y software antiguos, sin soporte técnico.	Falta de inversión en la actualización de la infraestructura tecnológica. Configuraciones predeterminadas sin ajustes a las necesidades de seguridad. Ausencia de auditorías regulares de seguridad en la infraestructura. Escaso mantenimiento preventivo de equipos y redes.	Medio-Alto: Incrementa la susceptibilidad a otros ataques.	Invertir en la actualización de equipos y software. Realizar mantenimientos periódicos. Configurar correctamente los sistemas según estándares de seguridad.	Reparar vulnerabilidades detectadas de manera inmediata. Sustituir hardware obsoleto. Implementar configuraciones más seguras en sistemas críticos.	Inversión en tecnología, mantenimiento.

Falta de Concientización y Capacitación en Ciberseguridad: La ausencia de programas de formación para el personal incrementa la susceptibilidad a incidentes de seguridad. El Ministerio TIC y Asobancaria han implementado capacitaciones para alcaldías y gobernaciones con el fin de fortalecer la ciberseguridad en las entidades públicas (Ministerio TIC, 2021).	Escasa inversión en programas de formación técnica en ciberseguridad .	Falta de políticas organizacionales para fomentar una cultura de seguridad. Prioridad baja de la ciberseguridad en la agenda administrativa. Poca difusión de información sobre amenazas emergentes y mejores prácticas. Desconocimiento de las normativas y estándares de ciberseguridad aplicables.	Alto: Impacto significativo en la protección de la información y la reputación.	Implementar un programa continuo de capacitación en ciberseguridad. Realizar simulacros periódicos de incidentes cibernéticos. Difundir políticas claras sobre el uso seguro de recursos tecnológicos.	Evaluar incidentes para determinar puntos débiles en el conocimiento del personal. Reforzar las capacitaciones tras cada incidente. Contratar consultores externos para auditorías de ciberseguridad.	Capacitación, programas educativos.

Nota: La tabla muestra un análisis minucioso de los riesgos informáticos más relevantes que afrontan las entidades gubernamentales, específicamente las alcaldías del Sumapaz. Cada riesgo se detalla minuciosamente, incluyendo sus causas, consecuencias, nivel de impacto, medidas preventivas, acciones correctivas y área correspondiente. Entre los riesgos se encuentran posibles ataques de ransomware, phishing y suplantación de identidad, acceso sin autorización a los sistemas, vulnerabilidades en la infraestructura tecnológica, así como la carencia de conciencia y formación en ciberseguridad. Este análisis nos facilita la identificación de las áreas críticas y nos ayuda a definir estrategias eficaces para reducir su impacto.

Las causas pueden variar desde contraseñas poco seguras y redes sin segmentación adecuada, hasta la utilización de sistemas desactualizados y la carencia de formación, exponiendo a las organizaciones a serios incidentes en ciberseguridad. Las ramificaciones abarcan desde la interrupción de las operaciones hasta la pérdida de la confianza de la ciudadanía, pasando por posibles sanciones legales y serios riesgos para la seguridad en el funcionamiento. En cuanto al impacto, se observan niveles que van desde moderados hasta elevados, resaltando la importancia de adoptar medidas de forma inmediata.

Las medidas preventivas se centran en aspectos como respaldar los datos, mantener el software actualizado, aplicar el doble factor de autenticación, realizar auditorías de forma regular y brindar formación constante. Además, las acciones correctivas ofrecen soluciones ágiles como la recuperación de datos, la revocación de accesos comprometidos, la reparación de

vulnerabilidades y el fortalecimiento de programas educativos. Por último, en el análisis se resaltan aspectos concretos como seguridad informática, inversión en tecnología y formación, destacando la relevancia de asignar los recursos apropiados para abordar de manera completa estos riesgos.

Tabla 2: *Ponderación.*

Riesgo	Consecuencia (20-100)	Probabilidad (20-100)	Valoración Total	Ponderación
Ataques de Ransomware	80	90	85	Muy Alta
Phishing y Suplantación de Identidad	60	80	70	Alta
Acceso No Autorizado a Sistemas	70	70	70	Alta
Vulnerabilidades en Infraestructura Tecnológica	50	60	55	Media
Falta de Concientización y Capacitación	90	85	87.5	Muy Alta

Nota: La tabla muestra una valoración cuantitativa de los riesgos informáticos que las alcaldías del Sumapaz deben afrontar, organizados en términos de consecuencia, probabilidad, valoración total y ponderación. Cada posibilidad ha sido evaluada en una escala del 20 al 100 para mostrar tanto el impacto posible como la probabilidad de que ocurra, considerando una clasificación cualitativa que va desde "Moderada" hasta "Altísima", siguiendo la seriedad de cada situación. Los riesgos más críticos son los ataques de ransomware y la falta de concientización y capacitación en ciberseguridad, con una valoración total de 85 y 87. 5 respectivamente.

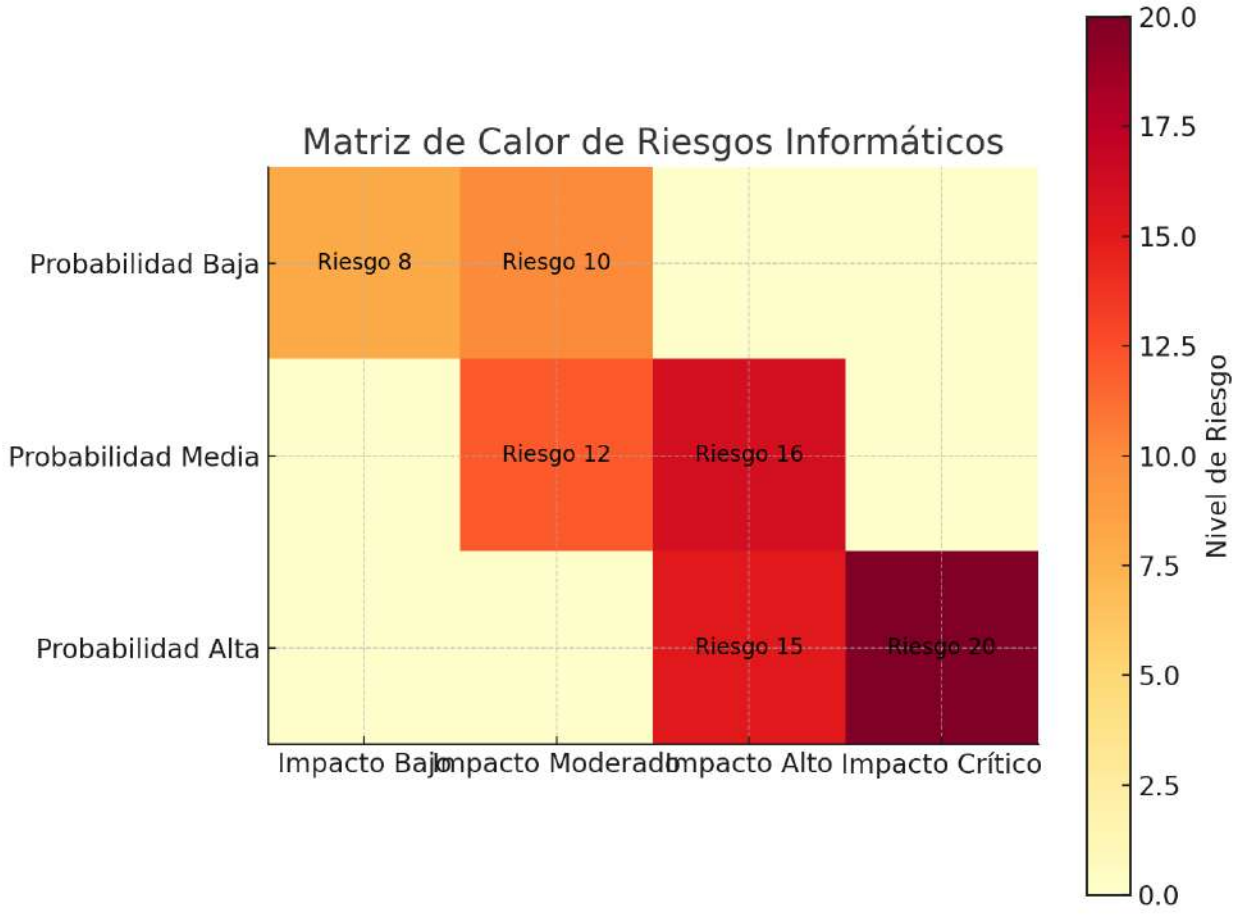
Ambos se clasifican como de Muy Alta prioridad debido a su potencial para interrumpir operaciones y comprometer fuertemente la seguridad. En cuanto a los riesgos asociados con el phishing, el acceso no autorizado a sistemas y las vulnerabilidades en la infraestructura tecnológica, se observan impactos que van de moderados a altos, con valoraciones de 70 (Alta) y 55 (Media) respectivamente. Esto sugiere la importancia de atenderlos mediante medidas correctivas específicas. En general, esta tabla se puede utilizar para priorizar intervenciones y asignar recursos de forma eficiente, resaltando la importancia de abordar primero los riesgos que tienen mayores impactos potenciales y probabilidades de ocurrencia.

DOI: https://doi.org/10.5281/zenodo.18215835

5. Construcción del Diagrama de Calor

Con la ponderación obtenida de la matriz de riesgos, se construyó un diagrama de calor. Este diagrama representa visualmente los riesgos según su probabilidad e impacto. Los riesgos más graves (con alta probabilidad y alto impacto) estarán en la zona roja, mientras que los de menor riesgo se ubicarán en la zona verde.

Figura 1: *Matriz de calor.*



- **Riesgo 1 (Robo de datos sensibles)**: Alta probabilidad (4) y alto impacto (5) → **Zona roja**.
- **Riesgo 2 (Ataques de ransomware)**: Media probabilidad (3) y alto impacto (5) → **Zona naranja**.
- **Riesgo 3 (Phishing a empleados)**: Alta probabilidad (4) y alto impacto (4) → **Zona naranja**.
- **Riesgo 4 (Acceso no autorizado a sistemas)**: Media probabilidad (3) y alto impacto (4) → **Zona amarilla**.

- **Riesgo 5 (Incumplimiento de normativas legales)**: Baja probabilidad (2) y alto impacto (5) → **Zona amarilla**.
- **Riesgo 6 (Vulnerabilidad en servidores)**: Baja probabilidad (2) y moderado impacto (4) → **Zona verde**.

6. Recomendaciones y mitigación de riesgos

A partir del análisis, se generarán recomendaciones específicas para mitigar los riesgos identificados. Las acciones a implementar dependerán de los resultados de la matriz de riesgos y el diagrama de calor. Estas medidas pueden incluir:

- Fortalecimiento de la seguridad de redes y sistemas.
- Uso de software de detección de intrusos.
- Políticas de acceso y control más estrictas.
- Planes de respuesta a incidentes.
- Formación continua del personal en ciberseguridad.

7. Informe sobre el análisis de delitos informáticos

Hemos auditado el análisis de riesgos y delitos informáticos presentado en el informe de auditoría, que incluye la identificación, evaluación y clasificación de riesgos a través de la **matriz de riesgos** y el **diagrama de calor** como herramientas clave. Este análisis comprende los datos obtenidos al 30 de octubre de 2024, con el objetivo de evaluar los riesgos asociados a los delitos informáticos y establecer las medidas de mitigación correspondientes.

8. Responsabilidad de los administradores

Los administradores son responsables de diseñar y supervisar el análisis de riesgos y delitos informáticos, garantizando que refleje fielmente el estado de la seguridad informática en las alcaldías de los municipios Fusagasugá, Pasca, Granada, Silvania y Tibacuy Esto incluye:

1. La implementación de controles internos adecuados para minimizar los riesgos asociados a los delitos informáticos.
2. La correcta identificación y priorización de amenazas mediante herramientas como la matriz de riesgos y el diagrama de calor.
3. La veracidad y claridad de la información presentada en el informe auditado.

Asimismo, los administradores son responsables de implementar las medidas necesarias para asegurar que los sistemas y procesos estén protegidos frente a posibles fraudes, accesos no autorizados o errores en los sistemas de información.

9. Responsabilidad del auditor

La responsabilidad del auditor es emitir una opinión independiente sobre el análisis de riesgos informáticos basado en la evidencia obtenida durante nuestra auditoría. La auditoría se desarrolló de conformidad con las normativas de auditoría aplicables en España. Esto incluye:

- Cumplir con los principios éticos exigidos.
- Planificar y ejecutar la auditoría de forma que se obtenga una **seguridad razonable** sobre si el análisis de riesgos está libre de incorrecciones materiales, ya sea por fraude o error.

10. Alcance de la auditoría

Una auditoría de este tipo requiere:

1. **Evaluar los procedimientos utilizados:** Verificar que la matriz de riesgos y el diagrama de calor reflejan adecuadamente la naturaleza, probabilidad y nivel de impacto de los delitos informáticos identificados.
2. **Valoración del control interno:** Analizar la eficacia de los controles internos relacionados con los sistemas de información para determinar si son adecuados para mitigar los riesgos asociados.
3. **Pruebas de evidencia:** Revisar documentación, informes y registros relevantes, así como realizar pruebas de validación del análisis de riesgos presentado.

Nuestra auditoría no incluye la validación de la eficacia operativa de los controles internos ni la implementación directa de medidas de mitigación.

Consideramos que la evidencia obtenida proporciona una base suficiente y adecuada para emitir nuestra opinión de auditoría.

Conclusión

El análisis realizado demuestra que la matriz de riesgo y el diagrama de calor de auditoría constituyen herramientas eficaces para la identificación evaluación y priorización de los delitos

informáticos en las instituciones públicas de la región del Sumapaz; los resultados evidencian que amenazas como el san ransomware y el phishing, la suplantación de identidad y el acceso no autorizado a los sistemas representa riesgos críticos intensificados por la obsolescencia tecnológica, la debilidad de los controles de seguridad y la limitada capacidad del personal. En este contexto, la integración de estrategias de mitigación resulta fundamental la actualización periódica de la infraestructura tecnológica, la implementación de políticas claras de seguridad de la información el fortalecimiento de los controles de acceso y la adopción de planes de respaldo y recuperación ante incidentes. Asimismo, la información continua y la concientización del talento humano se consolidan como un eje transversal para reducir vulnerabilidades operativas y técnicas. En conjunto, estas acciones permiten no sólo disminuir la probabilidad y el impacto de los riesgos identificados sino también asegurar el cumplimiento de la normativa colombiana vigente y fortalecer la confianza ciudadana promoviendo una gestión pública más segura transparente y alineada con la cultura integral de ciberseguridad.

En nuestra opinión, el análisis de riesgos de delitos informáticos realizado por investigadores de la ciberseguridad expresa, en todos los aspectos significativos, una imagen fiel de los riesgos informáticos a los que está expuesta la entidad al 31 de diciembre de 20X1. Además, las herramientas utilizadas (matriz de riesgos y diagrama de calor) están alineadas con las mejores prácticas internacionales para la gestión de riesgos.

Este análisis es coherente con las normas internas de seguridad informática de la entidad, así como con las normativas legales aplicables, incluyendo la **Ley 1273 de 2009** y la **Ley 1581 de 2012**.

Hemos verificado que la información adicional contenida en el informe de gestión de riesgos informáticos, presentado junto al análisis auditado, concuerda con la evidencia obtenida durante nuestra auditoría. Este informe incluye explicaciones sobre las políticas adoptadas para mitigar los riesgos identificados, la evolución del entorno tecnológico de la entidad y las medidas correctivas implementadas para garantizar la seguridad de los sistemas de información.

Nuestro trabajo como auditores se ha limitado a la verificación de la concordancia entre el informe de gestión y el análisis de riesgos auditado, y no incluye la evaluación de información adicional distinta de los registros contables y evidencias proporcionadas por la entidad.

Referencias

Congreso de la República de Colombia, 2009. *Ley 1273 de 2009: Ley sobre delitos informáticos*. Diario Oficial No. 47.706.

Cámara Colombiana de Informática y Telecomunicaciones. (2022, 29 de abril). *Ciberseguridad: diez acciones que su empresa debe implementar ahora mismo*. Recuperado de https://www.ccit.org.co/blog/ciberseguridad-diez-acciones-que-su-empresa-debe-implementar-ahora-mismo/

Cámara Colombiana de Informática y Telecomunicaciones. (2022, 6 de abril). *Entidades de gobierno en la mira de los ciberdelincuentes*. Recuperado de https://www.ccit.org.co/noticias/entidades-de-gobierno-en-la-mira-de-los-ciberdelincuentes/

Cámara Colombiana de Informática y Telecomunicaciones. (2022). *Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno*. Recuperado de https://www.ccit.org.co/wp-content/uploads/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno-safe-bp.pdf

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Ley sobre delitos informáticos*. Diario Oficial No. 47.706.

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Ley de protección de datos personales*. Diario Oficial No. 48.137.

Congreso de la República de Colombia. (2014). *Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública*. Diario Oficial No. 48.466.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021, 23 de marzo). *Ministerio TIC y Asobancaria abren convocatoria para capacitar en ciberseguridad a 250 Alcaldías y Gobernaciones*. Recuperado de https://gobiernodigital.mintic.gov.co/692/w3-article-162161.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021, 9 de abril). *Ante posibles ataques cibernéticos, alcaldías y gobernaciones se capacitarán gracias a convenio entre MinTIC y Asobancaria*. Recuperado de https://mintic.gov.co/portal/715/w3-article-162457.html

OpenAI. (2024). *Análisis de delitos informáticos a través de la matriz de riesgos y diagrama de calor de auditoría*. OpenAI.

Presidencia de la República de Colombia, 2015). *Decreto 1078 de 2015: Por el cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*. Diario Oficial No. 49.713.

Presidencia de la República de Colombia. (2018). *Directiva Presidencial 09 de 2018: Directrices para la implementación de la ciberseguridad en el Estado colombiano*.

Conflicto de interés

Los autores de este manuscrito declaran no tener ningún conflicto de interés.

Declaración ética

Los autores declaran que el proceso de investigación que dio lugar al presente manuscrito se desarrolló siguiendo criterios éticos, por lo que fueron empleadas en forma racional y profesional las herramientas tecnológicas asociadas a la generación del conocimiento.

Copyright

Licencia Creative Commons