**BANCO HIPOTECARIO DE LA VIVIENDA**
**AUDITORÍA INTERNA**

# Informe Final OP-SEG-001-2024

---

## AUDITORÍA SOBRE EL MONITOREO DE VULNERABILIDADES

24/02/2025

# RESUMEN EJECUTIVO

**Qué examinamos?**
El presente estudio se centró en la evaluación de la eficacia de las herramientas y procedimientos utilizados para identificar, controlar y mitigar vulnerabilidades en la infraestructura tecnológica, incluyendo hardware, software y redes. El periodo de análisis va del 01 de enero del 2024 al 30 de noviembre del 2024.

**Porqué es importante?**
La importancia de la revisión radica en la relevancia que tienen la infraestructura tecnológica del Banco para mantener la operativa diaria y la continuidad de las operaciones institucionales; así como para garantizar la seguridad de la información.

**Cómo lo auditamos?**
Con el fin de llevar a cabo esta revisión de manera exhaustiva, se aplicaron todos los principios aceptados, vigentes y pertinentes para la ejecución de auditorías relacionadas con vulnerabilidades tecnológicas. Este proceso incluyó desde la evaluación de la normativa interna y externa aplicable, hasta la ejecución de reuniones con los funcionarios involucrados en el proceso.

**Qué encontramos?**
Dentro del ámbito de las actividades de control susceptibles de mejora, se identificaron aspectos relacionados con los procedimientos internos destinados a controlar los incidentes de seguridad de TI, así como el monitoreo de vulnerabilidades. También se encontraron limitaciones en los controles destinados a administrar el portal Web institucional. Por último, se localizaron debilidades relacionadas con los reportes utilizados por el área de TI para controlar los principales insumos tecnológicos del Banco.

**Qué sigue?**
Se presentan a la Administración Activa una serie de observaciones dirigidas a impulsar la mejora continua en el proceso de implementación del proyecto Optimus que actualmente se está gestionando y desarrollando en el Banco con la colaboración de funcionarios internos y de un consorcio externo. Dada la significativa parte del proyecto aún por desarrollar, es crucial considerar las observaciones realizadas por la Auditoría Interna, detalladas en la sección de Recomendaciones de este documento.

# INDICE

# 1. INTRODUCCIÓN

## 1.1 Justificación de la auditoría

Este estudio forma parte del Plan Anual de Trabajo establecido por la Auditoría Interna para el año 2024, de conformidad con el Artículo 31 de la Ley 7052 del Sistema Financiero Nacional para la Vivienda, y el Artículo 22 de la Ley General de Control Interno N°8292, en los que se establece que la Auditoría Interna deberá velar y fiscalizar el uso adecuado de los recursos del BANHVI.

## 1.2 Objetivo

Evaluar la eficacia de las herramientas y procedimientos utilizados para identificar, controlar y mitigar vulnerabilidades en la infraestructura tecnológica, incluyendo hardware, software y redes.

## 1.3 Alcance

El estudio abarcó los controles vigentes y la documentación relacionada con la administración de vulnerabilidades tecnológicas del Banco, desde el 1 de enero del 2024 al 30 de noviembre del 2024.

Esta evaluación se realizó con el fin de verificar si las actividades asociadas con la administración de vulnerabilidades tecnológicas cumplen con el objetivo estratégico "*Desarrollar una estrategia de modernización tecnológica y de digitalización de procesos, que permitan la continuidad de operaciones, la suficiencia de la infraestructura, la seguridad y el control de la información, así como el soporte a la estrategia organizacional según las prioridades establecidas en el plan estratégico institucional*".

Se revisaron los procedimientos asociados a la administración de vulnerabilidades tecnológicas que son parte del proceso de Gestión de Servicios de TI.

## 1.4 Metodología de Trabajo

Se aplicó la metodología establecida en el Manual para el ejercicio de la práctica de la Auditoría Interna. También se aplicó el Manual de Normas Generales de Auditoría para el Sector Público emitido por la División de Fiscalización Operativa y Evaluativa. Otras normas y estándares utilizados fueron:

- ✓ Ley General de Control Interno.
- ✓ Normas Generales de Auditoria para el Sector Publico
- ✓ Normativa Interna vigente

- ✓ COBIT 2019
- ✓ INTE/ISO/IEC 27002:2016
- ✓ Norma 308 Comunicación de resultados.
- ✓ Reglamento de la Ley de Contratación Administrativa N°33411

Además, se aplicaron técnicas de auditoría comúnmente aceptadas como revisión documental relacionada con la evaluación, así como información adicional solicitada a los usuarios involucrados en el proceso.

Los resultados de las pruebas ejecutadas y demás documentos que respaldan el trabajo realizado, se mantienen como papeles de trabajo en el expediente electrónico de la Auditoría Interna. Las deficiencias detectadas de la presente revisión tanto en aspectos de control interno, administrativas y operativas, se detallan en la siguiente sección de Resultados de la Evaluación.

## 1.5 Comunicación preliminar de los resultados del estudio

La reunión de presentación de resultados de la revisión de auditoría (conferencia final) se realizó mediante reunión virtual el día 14 de enero del 2025, con la participación de los funcionarios del Departamento de TI.

El informe preliminar fue remitido al Departamento de TI mediante oficio BANHVI-AI-OF-177-2024 del 27 de diciembre 2025, con el objetivo de obtener sus apreciaciones y comentarios sobre el contenido de este en la reunión de cierre correspondientes. Se recibieron observaciones generales en dicha reunión, mismas que se valoraron para ser incluidas en el informe final.

# 2. RESULTADOS DE LA EVALUACIÓN

## 2.1 Procedimiento de monitoreo de vulnerabilidades

Como parte del estudio, se ejecutó una valoración del procedimiento "*PA-GTI-CTI-PR05 Monitoreo de Vulnerabilidades*", en el cual se localizaron ciertas deficiencias que podrían comprometer la capacidad de la institución para detectar, analizar y mitigar vulnerabilidades en su red de datos institucional de manera efectiva. Las mejoras localizadas como parte de este control incluyen las siguientes:

- ✓ Falta de una periodicidad claramente definida: el procedimiento no especifica la frecuencia con la que se deben realizar los escaneos de vulnerabilidades, lo que genera incertidumbre en la ejecución y puede resultar en largos periodos sin análisis. Esto no solo aumenta la exposición a amenazas, sino que también dificulta la priorización de acciones correctivas basadas en el riesgo.

- ✓ Ausencia de herramientas y metodologías documentadas: no se menciona el software específico aprobado para realizar los escaneos de vulnerabilidades ni los pasos técnicos necesarios para ejecutarlo. Esto deja a los encargados del proceso con interpretaciones abiertas sobre qué tecnología usar y cómo implementarla, reduciendo la consistencia y efectividad del monitoreo.

- ✓ Deficiencia en la gestión de resultados y registros: aunque se indica que los resultados del monitoreo de vulnerabilidades deben almacenarse en una ubicación específica, se verificó que la ruta de red detallada no existe, así como tampoco se encontraron evidencias de los reportes descritos. Esto representa un incumplimiento de las mejores prácticas para el manejo y trazabilidad de la información, imposibilitando posibles revisiones internas o externas, así como la evaluación de resultados.

- ✓ Desconexión con el sistema de gestión de riesgos: no se localizó una integración clara entre los resultados de los escaneos de vulnerabilidades y el plan de gestión de riesgos de la institución. Esto impide priorizar y tratar las vulnerabilidades de acuerdo con su criticidad y posible impacto en los activos del Banco.

- ✓ Falta de controles para garantizar la ejecución adecuada: el procedimiento no establece un mecanismo de supervisión o validación para asegurar que las tareas se realicen según lo planificado, en caso de que no se presenten vulnerabilidades al ejecutar el monitoreo.

- ✓ Desactualización en el contenido del procedimiento: se logró identificar que el procedimiento es del año 2019, y a la fecha de la revisión no parece estar alineado con los estándares internacionales y aplicables al Banco.

En los siguientes procesos del COBIT 2019 se pueden ubicar controles relacionados con el proceso de monitoreo de vulnerabilidades:

> *"**MEA01.03 Recopilar y procesar los datos de rendimiento y conformidad** Recopilar y procesar datos oportunos y precisos alineados con los enfoques de la empresa.*
>
> ***MEA01.05 Asegurar la implementación de acciones correctivas.***
> *Ayudar a las partes interesadas a identificar, iniciar y rastrear las acciones correctivas para abordar las anomalías.*
>
> ***MEA02.02 Revisar la eficacia de los controles del proceso de negocio.***
> *Revisar la operación de los controles, incluidas la supervisión y la evidencia de las pruebas, para asegurar que los controles de los procesos de negocio operan eficazmente. Incluir actividades para mantener evidencia de la operación efectiva de los controles mediante mecanismos, como pruebas periódicas, supervisión continua, evaluaciones independientes, centros de mando y control, y centros de operaciones de red. Estas evidencias garantizan al negocio que los controles cumplen con los requisitos relacionados con las responsabilidades de negocio, regulatorias y sociales."*

Dentro de las causas probables que generaron las debilidades de control localizadas en el procedimiento "*PA-GTI-CTI-PR05 Monitoreo de Vulnerabilidades*", se pueden mencionar las siguientes:

- ✓ Falta de planificación estratégica: no se ha implementado un marco estructurado para la gestión continua de vulnerabilidades.

- ✓ Suficiente capacitación: los responsables involucrados con el proceso podrían no estar completamente formados en las mejores prácticas basadas en estándares internacionales.

- ✓ Falta de supervisión: no se evidencia una revisión periódica del procedimiento para identificar y corregir deficiencias.

Algunos de los efectos relacionados con una limitada gestión en el área del monitoreo de vulnerabilidades, podrías ser los siguientes:

- ✓ Incremento del riesgo de ciberataques: la falta de un monitoreo adecuado puede permitir que vulnerabilidades críticas permanezcan sin resolver.

- ✓ Cumplimiento regulatorio comprometido: posible incumplimiento de normativas internas y externas relacionadas con la seguridad de la información.

- ✓ Impacto operativo y financiero: la falta de control puede derivar en interrupciones de los servicios, pérdida de datos sensibles y costos elevados para mitigar incidentes.

- ✓ Falta de trazabilidad: la carencia de registros confiables dificulta la realización de auditorías y análisis posteriores.

Adicionalmente, las debilidades localizadas indican una falta de madurez en la gestión del monitoreo de vulnerabilidades, lo que podría derivar en:

- Vulnerabilidades críticas que permanecen sin ser detectadas y explotadas por actores malintencionados.
- Pérdida de datos sensibles, interrupciones en la operación y daños a la reputación institucional.
- Ineficiencias operativas debido a la duplicación de esfuerzos o uso inconsistente de herramientas.
- Incumplimiento de normativas y estándares internacionales de seguridad de la información.

Este problema subraya la necesidad de realizar una revisión exhaustiva del procedimiento para alinearlo con las mejores prácticas internacionales y garantizar una implementación efectiva del monitoreo de vulnerabilidades.

## 2.2 Procedimiento sobre la Atención de Incidentes de Seguridad

En el proceso de revisión se identificaron varias debilidades relacionadas con el procedimiento "*PA-GTI-GSSTI-PR03 Atención de Incidentes de Seguridad de la Información*" que comprometen la efectividad del tratamiento de incidentes de seguridad. Estas debilidades están relacionadas con la clasificación, escalamiento, monitoreo y documentación de lecciones aprendidas, así como con la capacitación del personal.
Los aspectos puntuales que pueden presentar aspectos de mejora son:

- ✓ Clasificación y priorización de incidentes: El procedimiento no define un marco claro de clasificación y priorización basado en impacto y urgencia, lo que limita la capacidad de respuesta oportuna.

- ✓ Gestión del conocimiento: Aunque se menciona la base de datos de lecciones aprendidas, no existe un proceso formal de actualización y validación de esta información.

- ✓ Gestión de riesgos: No se establece una conexión explícita entre los incidentes registrados y la gestión de riesgos institucionales.

- ✓ Monitoreo y seguimiento: Carece de indicadores clave de desempeño (KPIs) para evaluar la efectividad de las acciones correctivas y el tratamiento de incidentes.

Con base en el marco COBIT 2019, específicamente los siguientes objetivos, se establece que la administración de proyectos y cronogramas debe garantizarse dentro de los parámetros establecidos para cumplir con los objetivos empresariales:

> *"**APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.***
> *Mantener un plan de seguridad de la información que describa cómo se debe manejar el riesgo de seguridad de la información y cómo se debe alinear con la estrategia y la arquitectura de la empresa. Asegurar que las recomendaciones para implementar mejoras a la seguridad se basen en casos de negocio aprobados, implementados como una parte integral del desarrollo de servicios y soluciones, y que operen como una parte integral de la operación del negocio.*
>
> ***BAI08.03 Utilizar y compartir conocimiento.***
> *Transmitir los recursos de conocimiento disponibles a las partes interesadas correspondientes y comunicar cómo estos recursos pueden utilizarse para abordar diferentes necesidades (p. ej., resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).*
> ***DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes.***
> *Identificar, registrar y clasificar las peticiones de servicio y los incidentes, y asignarles una prioridad de acuerdo con la criticidad para el negocio y los acuerdos de servicio."*

La norma INTE/ISO/IEC 27002:2016, enfocada en la gestión de la seguridad de la información, detalla en algunos de sus artículos con relación a este hallazgo lo siguiente:

> *"**12.1.2 Gestión de cambios***
> *Control*
> *Se deberían controlar los cambios de la organización, en los procesos de negocio, recursos de procesamiento de la organización y en los sistemas que afecten la seguridad de la información…*

*h) provisión de un proceso de cambio de emergencia para permitir la implementación rápida y controlada de los cambios necesarios para resolver un incidente (ver apartado 16.1)...*

***16.1.1 Responsabilidades y procedimientos***
*Control*
*Se deberían establecer responsabilidades y procedimientos de gestión para asegurarse de tener una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información."*

Como posible causa se encuentra que el procedimiento se diseñó sin considerar las mejores prácticas aplicables a la institución, así como tampoco se definieron roles claros para garantizar la actualización continua y la alineación con los estándares internacionales.

Algunos de los efectos de que no se incluyan este tipo de controles en la atención de incidentes de seguridad tecnológica se encuentran los siguientes:

- ✓ Tratamiento ineficiente de incidentes, lo que podría prolongar tiempos de respuesta.
- ✓ Incremento de la recurrencia de incidentes debido a la falta de aprendizaje institucional.
- ✓ Pérdida de confianza por parte de las partes interesadas debido a respuestas inadecuadas o tardías.
- ✓ Incumplimiento de requisitos normativos y estándares de la industria.

## 2.3 Aplicaciones Web Institucionales

Se identificó que las aplicaciones web de la institución (como el Portal Web y el Expediente Electrónico) no cuentan con un servicio de monitoreo activo ni con la implementación de un Web Application Firewall (WAF). Esto genera una exposición considerable a riesgos cibernéticos como ataques de inyección SQL, cross-site scripting (XSS), denegaciones de servicio (DoS) y otras posibles amenazas dirigidas específicamente a aplicaciones web. Además, la falta de estas medidas de seguridad limita la capacidad de respuesta ante incidentes, afectando la confidencialidad, integridad y disponibilidad de los datos.

Esta situación también implica que no se están monitoreando eventos o anomalías en el tráfico web, lo que aumenta las posibilidades de explotación de vulnerabilidades por actores malintencionados.

Algunos de los controles establecidos en el COBIT 2019 sobre este tipo de vulnerabilidades en sitios WEB son los siguientes:

> *"**EDM03.01 Evaluar la gestión de riesgos.***
> *Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las I&T en la empresa. Considerar si el apetito al riesgo de la empresa es apropiada, y que se identifique y gestione el riesgo para el valor de la empresa relacionado con el uso de I&T.*
>
> ***EDM03.03 Monitorizar la gestión de riesgos.***
> *Monitorizar r las metas y las métricas clave de los procesos de gestión de riesgos. Establecer cómo las desviaciones o los problemas se identificarán, se les dará seguimiento y se comunicarán para su solución.*
>
> ***APO12.01 Recopilar datos.***
> *Identificar y recopilar datos relevantes para habilitar una efectiva identificación, análisis y reporte de los riesgos relacionados con I&T.*
>
> ***APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI)**.*
> *Establecer y mantener un sistema de gestión de seguridad de la información (SGSI) que proporcione un enfoque estándar, formal y continuo para la gestión de la seguridad de la información, mediante la habilitación de tecnología segura y procesos de negocio alineados con los requisitos del negocio.*
>
> ***MEA01.01 Establecer un enfoque de supervisión.***
> *Involucrar a las partes interesadas a fin de establecer y mantener un enfoque de supervisión para definir los objetivos, el alcance y el método con los que medir la solución del negocio, la entrega de servicios y la contribución a los objetivos de la empresa. Integrar este enfoque con el sistema de gestión de rendimiento corporativo.*

En la INTE/ISO/IEC 27002:2016 también se localizan ciertos procesos referentes a la necesidad de controlar este tipo de servicios, como los siguientes:

> *"**13.1.1 Controles de red***
> *Control*
> *Se debería gestionar y controlar las redes para proteger la información en los sistemas y aplicaciones.*
>
> *Guía de implementación*
> *Los controles deberían ser implementarse para procurar la seguridad de la información en las redes y la protección de los servicios conectados de*

*accesos no autorizados. En particular, los siguientes ítems deberían ser considerados: …*
*c) deberían establecerse controles especiales para salvaguardar la confidencialidad y la integridad de los datos que circulan a través de redes públicas o inalámbricas así como para proteger los sistemas y aplicaciones conectados (ver apartados 10 y 13.2); podrían también ser requeridos controles especiales para mantener la disponibilidad de los servicios de red y de las computadoras conectadas…*

***13.1.2 Seguridad de los servicios de red***
*Control*
*Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red deberían ser identificados e incluidos en los acuerdos de servicios de red, ya sean servicios provistos internamente o subcontratados.*

***13.2.1 Políticas y procedimientos de transferencia de información***
*Control*
*Se deberían establecer políticas, procedimientos y controles formales para proteger la transferencia de información que se realice mediante el uso de todo tipo de recursos de comunicación.*

*Guía de implementación*
*Los procedimientos y controles a seguir cuando se usan recursos de comunicación para la transferencia de información deberían considerar los siguientes ítems:*
*a) los procedimientos diseñados para proteger la información transferida de la interceptación, el copiado, la modificación, la desviación y la destrucción;*
*b) los procedimientos para la detección y protección contra el código malicioso que pueda ser transmitido a través del uso de comunicaciones electrónicas (ver apartado 12.2.1)…"*

Una de las causas por las que no se cuenta con este tipo de controles, se debe a que no ha priorizado la asignación de recursos para la implementación de un sistema de monitoreo y protección específico para sus aplicaciones web, esto a pesar de que uno de estos servicios, el Expediente Electrónico, se implementó desde el año 2018 y es utilizado por todas las Entidades Autorizadas para la inclusión de los expedientes de bonos de casos individuales, una de las actividades esenciales del Banco.

El no contar con aplicaciones de seguridad que monitoreen estos servicios, generan algunos de los siguientes efectos:

- ✓ Las aplicaciones web pueden ser atacadas mediante técnicas como inyección SQL, Cross-Site Scripting (XSS) y exfiltración de datos, resultando en la exposición de información confidencial.

- ✓ Información personal de empleados o usuarios podría ser sustraída, lo que podría violar leyes de protección de datos.

- ✓ Ataques como denegaciones de servicio (DoS/DDoS) pueden inhabilitar las aplicaciones web, afectando su disponibilidad y causando interrupciones en los procesos institucionales.

- ✓ La falta de monitoreo continuo impide identificar y mitigar vulnerabilidades de manera proactiva, lo que puede llevar a brechas recurrentes.

- ✓ La institución puede enfrentarse a multas y sanciones debido al incumplimiento de regulaciones de seguridad de la información.

- ✓ Los atacantes podrían usar las aplicaciones comprometidas como puerta de entrada para acceder a otros sistemas internos de la institución.

- ✓ Sin monitoreo y respuesta adecuada, los atacantes pueden mantener accesos no autorizados a largo plazo, maximizando los daños.

- ✓ Servicios esenciales soportados por las aplicaciones web podrían detenerse, afectando a los usuarios y a la operación general.

## 2.4 Reportes de vulnerabilidades

Se identificó que el área de Soporte Técnico de TI realiza revisiones manuales diarias de los reportes generados por las herramientas de monitoreo de servicios tecnológicos, que incluyen Office 365, respaldos de OneDrive y correo electrónico (Acronis), respaldos locales y del Centro Alterno de Procesamiento (CPA), el estado de las SANs y los respaldos internos del Banco (utilizando VEEAM). Este proceso manual implica que el personal debe identificar y valorar cuáles eventos son falsos positivos o falsos negativos, lo cual aumenta la carga operativa y puede limitar la eficacia de las revisiones debido a otras responsabilidades del personal asignado.

Como ejemplo de esta actividad, se muestra en el siguiente cuadro un reporte de eventos relacionados con la ciberseguridad del Banco, donde se denota para el mes de noviembre del 2024 un aumento exponencial en los ataques de Malware y de Spam:

*Imagen 1- Eventos de Ciberseguridad*

| Eventos Potenciales de Ciberseguridad 2024 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Categoría | ene-24 | feb-24 | mar-24 | abr-24 | may-24 | jun-24 | jul-24 | ago-24 | sep-24 | oct-24 | nov-24 |
| Criptominería | --- | --- | --- | --- | --- | --- | 93 | --- | --- | --- | --- |
| Dominios recientes | --- | --- | --- | --- | --- | --- | 43 | --- | --- | --- | --- |
| Malware (Software malicioso) | 43 | 58 | 15 | 50 | 138 | 140 | 110 | 179 | 411 | 306 | 33,579 |
| Software malicioso avanzado | --- | 1 | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DNS dinámicos | --- | --- | --- | --- | --- | --- | 3 | --- | --- | --- | --- |
| Phishing | 163 | 384 | 347 | 384 | 424 | 286 | 311 | 58 | 87 | 86 | 0 |
| Eventos de intrusión | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Spam | --- | --- | --- | --- | --- | --- | --- | 29 | 7 | 50 | 11,379 |
| Boletines y contenido de marketing | --- | --- | --- | --- | --- | --- | --- | 26 | 19 | 36 | 5,147 |
| **Total:** | **206** | **443** | **362** | **434** | **562** | **426** | **560** | **292** | **524** | **478** | **50105** |

*Fuente: Área de Soporte Técnico de TI*

En el COBIT 2019 se detallan ciertos controles referentes a la administración y control del monitoreo de servicios tecnológicos, entre los que destacan:

> "***APO12.03 Mantener un perfil de riesgo.***
> *Mantener un inventario de los riesgos conocidos y los atributos de riesgo, incluidos la frecuencia esperada, impacto potencial y respuestas. Documentar los recursos, capacidades y actividades de control actuales relacionados con elementos de riesgo.*
>
> ***DSS01.03 Monitorizar la infraestructura de I&T.***
> *Monitorizar la infraestructura de I&T y eventos relacionados. Almacenar suficiente información cronológica en los logs de operación que permita la reconstrucción y revisión de las secuencias temporales de las operaciones y otras actividades asociadas o que apoyan las operaciones.*"

En el estándar INTE/ISO/IEC 27002:2016 encontramos criterios adicionales relacionados con la administración de estos reportes de vulnerabilidades, tales como:

> "***12.4.1 Registro de Eventos***:
> *Control*
> *Se deberían generar, mantener y revisar periódicamente los registros de eventos de las actividades de los usuarios, las excepciones, las fallas y los eventos de seguridad de la información.*
>
> ***12.6.1 Gestión de vulnerabilidades técnicas***
> *Control*
> *Se debería obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información usados, se debería evaluar la*

*exposición de la organización a estas vulnerabilidades y tomar las medidas apropiadas para abordar el riesgo asociado.*

***18.2.3 Revisiones del cumplimiento técnico***

*Control*

*Los sistemas de información deberían ser revisados regularmente para el cumplimiento de las políticas y las normas de seguridad de la información de la organización.*

*Guía de implementación*

*El cumplimiento técnico debería revisarse preferentemente con la ayuda de herramientas automatizadas que generen un informe técnico para su posterior interpretación por parte de un especialista técnico. Alternativamente, un ingeniero de sistemas experimentado podría realizar revisiones manuales (con el apoyo de herramientas de software apropiadas, si es necesario).”*

Una de las razones por las que los reportes de las herramientas de monitoreo de servicios tecnológicos se administren de la forma indicada, se debe a que no se han implementado herramientas o procesos automatizados que permitan analizar y correlacionar los eventos registrados en los sistemas de monitoreo de manera eficiente.

Dentro de los efectos directos de lo indicado en este hallazgo, se detallan los siguientes:

- ✓ Mayor probabilidad de que incidentes críticos pasen desapercibidos debido a la dependencia de revisiones manuales.
- ✓ Retrasos en la respuesta a eventos debido al tiempo requerido para validar falsos positivos y negativos.
- ✓ La carga manual limita la disponibilidad del personal técnico para actividades estratégicas o de mayor valor añadido.
- ✓ Riesgo de fallos no detectados que afecten la continuidad de las operaciones del Banco, pudiendo derivar en pérdidas económicas significativas.
- ✓ Incumplimiento parcial de estándares internacionales o regulaciones nacionales relacionadas con la automatización del monitoreo y la supervisión de operaciones críticas.

## 3. CONCLUSIÓN

En la revisión sobre el monitoreo de vulnerabilidades tecnológicas, la Auditoría Interna pudo determinar la existencia de controles generales implementados por el Departamento de TI tanto para su administración, su operativa y su gestión.

No obstante, se localizaron algunos aspectos específicos que pueden ser mejorados con el desarrollo e implementación de controles adicionales tanto a nivel normativo, operativo y tecnológico; esto con el objetivo de ir incrementado paulatinamente la continuidad de los servicios tecnológicos y la seguridad de la información institucional resguardada interna y externamente.

El enfoque de la Auditoría Interna en este tipo de evaluaciones es actuar como un órgano asesor de la Administración Activa recalcando aspectos que pueden mejorar tanto en el control interno como en la operativa del proceso, todo con el fin de contribuir al logro de los objetivos establecidos para la mejora continua de la institución.

## 4. RECOMENDACIONES

En relación con los informes de la Auditoría Interna dirigidos a los titulares subordinados, la Ley General de Control Interno No. 8292 en su artículo 36 establece:

*"Artículo 36. —**Informes dirigidos a los titulares subordinados**. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*

*a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.*

*b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.*

c) *El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda."*

### *4.1* Genaro Fuentes Abarca, Jefatura de TI o quien ocupe su cargo

**Procedimiento de monitoreo de vulnerabilidades**

4.1.1 El procedimiento "*PA-GTI-CTI-PR05 Monitoreo de Vulnerabilidades*" debe ser revisado y actualizado para garantizar un enfoque más integral en la identificación, análisis y mitigación de los riesgos asociados a vulnerabilidades en la red de datos institucional. Esto es fundamental para proteger la continuidad operativa y asegurar la disponibilidad, confidencialidad e integridad de los servicios tecnológicos del Banco. Algunos de los puntos específicos de mejora pueden ser:

- ✓ Establecer una periodicidad definida: implementar un cronograma para la ejecución regular de escaneos de vulnerabilidades (ej., mensual o trimestral) basado en el nivel de riesgo de los activos.

- ✓ Especificar herramientas y procedimientos: documentar el software aprobado para el monitoreo de vulnerabilidades e incluir pasos detallados para su uso en el procedimiento, con el fin de evitar la dependencia de personal y concentración de conocimiento.

- ✓ Implementar una gestión de registros adecuada: asegurar que los resultados del monitoreo se almacenen en una ubicación verificada y accesible con las medidas de control necesarias, y que se revise periódicamente por el supervisor del área de soporte técnico.

- ✓ Desarrollar indicadores y métricas: definir indicadores clave de desempeño (KPIs) para evaluar el desempeño del proceso, como por ejemplo el tiempo promedio de resolución de vulnerabilidades y el porcentaje de sistemas, equipos o activos monitoreados.

- ✓ Alinear con la gestión de riesgos: integrar los resultados del monitoreo en el plan de gestión de riesgos, priorizando las vulnerabilidades críticas según su impacto potencial.

- ✓ Supervisión y mejora continua: realizar revisiones periódicas del procedimiento para garantizar su alineación con los estándares internacionales y adaptarlo a los cambios constantes en el entorno tecnológico.

Nivel de Riesgo: **Alto**

**Procedimiento sobre la atención de incidentes de seguridad**

4.1.2 El procedimiento "*PA-GTI-GSSTI-PR03 Atención de Incidentes de Seguridad de la Información*" debe ser actualizado con el objetivo de abordar de manera más integral los posibles riesgos que, de materializarse, podrían comprometer la continuidad de los servicios tecnológicos del Banco. Dentro de las áreas que tienen aspectos de mejoras se encuentran:

- ✓ Clasificación y Priorización de Incidentes: implementar un marco de clasificación basado en impacto y urgencia, conforme a los criterios de las mejores prácticas de la industria, por ejemplo, el APO13 y DSS02 del COBIT 2019 y la Sección 16 del ISO 27002:2016.

- ✓ Gestión del Conocimiento: establecer un proceso formal para actualizar y validar la base de conocimientos de lecciones aprendidas, pudiendo utilizar para esto los criterios del BAI08 de COBIT 2019.

- ✓ Gestión de Riesgos: actualizar el documento para que se pueda vincular los incidentes que se presenten con el mapa de riesgos institucional, usando el APO12 de COBIT 2019 como posible referente.

- ✓ Monitoreo y Medición: definir indicadores claves de rendimiento (KPIs) que sirvan para medir el tiempo de resolución, recurrencia y efectividad de las acciones correctivas; para lo que se podría utilizar el MEA01 de COBIT 2019. Algunos posibles ejemplos de este tipo de KPIs son:

  - Tiempo promedio de resolución de no conformidades
  - Porcentaje de incidentes críticos resueltos dentro del tiempo acordado
  - Tasa de recurrencia de incidentes similares
  - Tiempo promedio entre recurrencias
  - Porcentaje de acciones correctivas exitosas
  - Reducción en el impacto de los problemas tras las acciones correctivas

Nivel de Riesgo: **Alto**

**Aplicaciones Web Institucionales**

4.1.3 Se deben realizar las gestiones administrativas correspondientes con el fin de implementar un Web Application Firewall (WAF) para proteger las aplicaciones web como el Portal Web y el Expediente Electrónico, contra amenazas comunes y avanzadas.
Nivel de Riesgo: **Alto**

4.1.4 Debe evaluarse la factibilidad técnica, operativa y económica de configurar un sistema de monitoreo de eventos de seguridad que permita la detección temprana de ataques a las aplicaciones WEB y la respuesta a incidentes en tiempo real.
Nivel de Riesgo: **Alto**

**Reportes de Vulnerabilidades**

4.1.5 Debe realizarse un estudio de costo beneficio que determine la viabilidad de implementar sistemas avanzados que automatice el análisis y correlación de eventos en los servicios que son monitoreados por el Departamento de TI, como por ejemplo un Sistema de Gestión de Eventos e Información de Seguridad (SIEM), o en su defecto la contratación de un Centro de Control de la Red (CCR o NOC) o un Centro de Operaciones de Seguridad (SOC); que sean los responsable de diseñar, instalar, dar mantenimiento correctivo y preventivo a la operación (Gestión, Soporte y monitoreo) de redes de telecomunicaciones de datos, así como de monitorizar las redes en función de alarmas o condiciones que requieran atención especial para evitar impacto en el rendimiento de las redes o de los servicio ofrecidos por el área de TI.
Nivel de Riesgo: **Alto**

4.1.6 Con las herramientas o aplicaciones que actualmente utiliza el área de Soporte Técnico de TI, valorar la factibilidad de configurar alertas específicas que permitan distinguir automáticamente eventos críticos de falsos positivos o negativos, priorizando aquellos con mayor impacto potencial.
Nivel de Riesgo: **Alto**

**Estudio realizado por:**

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2025.02.24 14:45:42 -06'00'

**MATI. Jorge Ramirez Bolaños**
**Auditor Encargado**

GUSTAVO FLORES OVIEDO (FIRMA)

Firmado digitalmente por GUSTAVO FLORES OVIEDO (FIRMA)
Fecha: 2025.02.24 17:50:17 -06'00'

**Aprobado MBA Gustavo Flores Oviedo**
**Auditor Interno**