BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA

Informe Final OP-SEG-002-2024

AUDITORÍA OPERATIVA DE CIBERSEGURIDAD

19/12/2025

RESUMEN EJECUTIVO

Qué examinamos?
El presente estudio muestra los principales hallazgos relacionados con la contratación externa número 2024LD-000035-0016400001 denominado "*Servicio auditoría externa para realizar una evaluación de la gestión de la ciberseguridad en el BANHVI*". El periodo de análisis fue del 01 de enero del 2024 al 30 de junio del 2025.

Porqué es importante?
La ciberseguridad constituye un pilar fundamental para garantizar la continuidad operativa del BANHVI, la protección de su infraestructura tecnológica y la salvaguarda de la información institucional. La adecuada gestión de las vulnerabilidades permite reducir riesgos asociados a ataques externos e internos que podrían comprometer la disponibilidad, integridad y confidencialidad de los datos.

Cómo lo auditamos?
La revisión se desarrolló conforme a los estándares internacionales de ciberseguridad (CVE/CWE MITRE, NIST 800-115, CVSS, OWASP y PTES). Se analizaron los resultados obtenidos por la auditoría técnica externa contratada (White Jaguars), incluyendo pruebas de penetración interna y externa. La Auditoría Interna centró su análisis en los hallazgos clasificados con severidad **Crítica y Alta** durante el periodo del 1° de enero al 30 de noviembre de 2024.

Qué encontramos?
Las pruebas evidenciaron la existencia de controles generales en materia de ciberseguridad; sin embargo, se identificaron debilidades significativas relacionadas con:

- Vulnerabilidades críticas en servicios expuestos a Internet.
- Configuraciones inadecuadas y componentes tecnológicos desactualizados.
- Insuficiente protección en la capa de transporte y exposición de consolas administrativas.
- Riesgos de divulgación de información sensible en servidores corporativos.

Estas condiciones podrían facilitar ataques de intrusión o denegación de servicio, así como comprometer la reputación institucional y la continuidad de las operaciones.

Qué sigue?
Se presentan a la Administración Activa una serie de observaciones dirigidas a fortalecer los controles tecnológicos y operativos, priorizando la atención inmediata de las vulnerabilidades críticas y de alto riesgo señaladas. Además, deberá integrarse un proceso continuo de gestión de vulnerabilidades, actualizaciones y monitoreo de seguridad, alineado las mejores prácticas internacionales.

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

Realizar pruebas técnicas de ciberseguridad basado en las buenas prácticas de la industria y en la normativa aplicable al BAHNVI.

1.3 Alcance

El estudio abarcó las pruebas de penetración (Pentest) Externas e Internas detalladas en el cartel de contratación, abarcando las fechas desde el 01 de enero del 2024 al 30 de junio del 2025.

Esta evaluación se realizó con el fin de verificar si las actividades asociadas con la ciberseguridad del Banco 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*".

1.4 Metodología de Trabajo

La metodología utilizada para la revisión fue propia de la empresa externa contratada para la evaluación, misma que se detalla en los documentos anexos a este informe. Las pruebas realizadas poseen características muy específicas que las diferencian de otros tipos de evaluaciones de riesgo o auditorías, para lo cual se utilizaron los siguientes marcos de referencia para la ejecución, medición de riesgo y vinculación con vulnerabilidades conocidas, incluyendo y sin limitarse a:

- CVE / CWE MITRE
- NIST 800-115
- CVSS de FIRST
- OWASP con sus proyectos: WSTG, ASVS, TOP 10 WEB
- PTES: Penetration Testing Execution Standard

Tomando en cuenta la totalidad de hallazgos localizados por la auditoría externa (374 en total), así como los hallazgos que representan mayor riesgo a nivel institucional, en este informe se presentan únicamente los resultados que tuvieron una severidad Crítica y Alta en ambas pruebas, con la finalidad de darles un seguimiento más detallado y oportuno por parte de la Auditoría Interna. El resto de los hallazgos se pueden ubicar en los documentos anexos a este informe remitidos por el consultor externo, detallando la totalidad de los resultados de las pruebas de penetración interna y las pruebas de penetración externa.

1.5 Comunicación preliminar de los resultados del estudio

El informe preliminar fue remitido al Departamento de TI mediante oficio BANHVI-AI-OF-177-2025 del 10 de diciembre 2025, con el objetivo de obtener comentarios y apreciaciones sobre el contenido de tal informe en la reunión de cierre correspondiente.

Por medio de correo electrónico remitido el 19 de diciembre del 2025 por la jefatura del Departamento de TI, se indica estar de acuerdo con los resultados de la auditoría, tomando en cuenta que el 27 de noviembre se reunieron con el consultor externo y la Auditoría Interna para revisar y hacer observaciones al informe preliminar, realizando para el documento final los ajustes correspondientes según lo solicitado por el Departamento de TI.

2. RESULTADOS DE LA EVALUACIÓN

Este documento contiene los resultados que se encontraron con severidad Crítica y Alta como parte de la ejecución de pruebas técnicas de seguridad realizadas por los especialistas en ciberseguridad de la empresa White Jaguars, ganadora de la licitación 2024LD-000035-0016400001.

Las pruebas de penetración ejecutadas tienen como objetivo detectar vulnerabilidades antes de que sean aprovechados por actores maliciosos. Los resultados brindan acciones puntuales que el BANHVI debe seguir para mitigar o reducir el riesgo.

Específicamente las pruebas ejecutadas fueron las siguientes:

Pentest Interno: Pruebas de seguridad realizadas a la infraestructura interna de la organización.

Pentest Externo: Pruebas de seguridad realizadas a la infraestructura externa de la organización que se encuentra expuesta en internet.

Los resultados se agruparon por los tipos de pruebas antes descritos y son detallados en los siguientes puntos.

2.1 Pruebas de Penetración Interna

En estas pruebas se detectaron 342 vulnerabilidades (vistas como hallazgos desde el punto de vista de la Auditoría). De estas, no se localizaron severidades Críticas y solo 1 vulnerabilidad de severidad alta. Las restantes 341 vulnerabilidades de severidades menores (detalladas en el informe anexo de la empresa consultora) pueden ser atendidas con un nivel de prioridad menor dando más énfasis a las de mayor severidad.

Imagen 1- Resumen Vulnerabilidades Pentest Interno

Severidad	Cant	Descripción
Crítico	0	Riesgo de severidad critica que puede involucrar impacto en la integridad de los datos sin ningún tipo de acceso permitido siendo alcanzable por cualquier atacante desde internet.
Alto	1	Riesgo alto de impacto en la reputación de la marca, en la confiabilidad de los datos en tránsito o la disponibilidad del servicio, su incumplimiento pone en riesgo certificaciones como PCI-DSS o de aceptación por parte de compromisos con terceros (convenios).
Medio	329	No representan un impacto directo para la confiabilidad, disponibilidad o integridad de los datos sin embargo podrían poner en riesgo la reputación de la marca o exponer a vulnerabilidades a sus usuarios.
Bajo	11	Buenas prácticas de seguridad que de no aplicarse pueden combinarse con otros factores para representar un riesgo para el cliente.
Info	1	Recomendaciones y prácticas adicionales para mejorar aspectos observados de forma opcional sin que requiera de una acción correctiva.

Fuente: Informe de Pruebas de Penetración y análisis de vulnerabilidades (White Jaguars)

2.1.1 Riesgos Altos

A. Componentes de Infraestructura desactualizados y vulnerables

Se localizaron sistemas utilizando componentes con vulnerabilidades conocidas que pueden reducir las defensas de las plataformas y permitir diversos ataques e impactos. Usualmente son vulnerables porque:

- ✓ No se conoce las versiones de todos los componentes que utiliza (tanto en el lado del cliente como en el servidor).
- ✓ El software es vulnerable, no soportado o desactualizado. Esto incluye al sistema operativo.
- ✓ No se realizan revisiones de vulnerabilidades regularmente y no se subscribe a boletines de seguridad de los componentes que utiliza.
- ✓ No corrige o actualiza la plataforma base, frameworks y dependencias de forma oportuna y basada en riesgo.
- ✓ Los desarrolladores de software no prueban la compatibilidad de las librerías actualizadas.

2.2 Pruebas de Penetración Externa

Relacionado con estas pruebas, se localizó un total de 32 vulnerabilidades. De estas, existe 1 vulnerabilidad de severidad crítica y se localizaron 9 vulnerabilidades de severidad alta. Las restantes 22 vulnerabilidades de severidades menores pueden

ser atendidas con un nivel de prioridad menor dando más énfasis a las de mayor severidad

Imagen 1- Resumen Vulnerabilidades Pentest Exerno

Severidad	Cant	Descripción
Crítico	1	Riesgo de severidad critica que puede involucrar impacto en la integridad de los datos sin ningún tipo de acceso permitido siendo alcanzable por cualquier atacante desde internet.
Alto	9	Riesgo alto de impacto en la reputación de la marca, en la confiabilidad de los datos en tránsito o la disponibilidad del servicio, su incumplimiento pone en riesgo certificaciones como PCI-DSS o de aceptación por parte de compromisos con terceros (convenios).
Medio	13	No representan un impacto directo para la confiabilidad, disponibilidad o integridad de los datos sin embargo podrían poner en riesgo la reputación de la marca o exponer a vulnerabilidades a sus usuarios.
Bajo	8	Buenas prácticas de seguridad que de no aplicarse pueden combinarse con otros factores para representar un riesgo para el cliente.
Info	1	Recomendaciones y prácticas adicionales para mejorar aspectos observados de forma opcional sin que requiera de una acción correctiva.

Fuente: Informe de Pruebas de Penetración y análisis de vulnerabilidades (White Jaguars)

2.2.1 Riesgos Críticos

A. SMTP Relay abierto

Se localizó un servidor de correo electrónico (SMTP) que está configurado para permitir que cualquier usuario en Internet envíe correos electrónicos a través de él, sin requerir autenticación.

Un SMTP Relay Attack ocurre cuando un actor malicioso explota un servidor SMTP mal configurado para enviar correos electrónicos no autorizados. Este tipo de ataque aprovecha la capacidad del servidor para reenviar correos electrónicos, permitiendo al atacante distribuir correos de spam o phishing sin necesidad de autenticación.

El servidor, comúnmente denominado Open Relay, se convierte inadvertidamente en una herramienta para spammers, lo que puede llevar a su inclusión en listas negras (blacklisting) y causar daños reputacionales a la organización afectada. Los atacantes pueden abusar de un servidor confiable para enviar correos maliciosos a víctimas internas o externas.

En el caso de los objetivos internos, los correos podrían incluso evadir los filtros de spam, ya que provienen de una fuente confiable, lo que incrementa significativamente las probabilidades de que el ataque tenga éxito.

2.2.2 Riesgos Altos

A. Transferencia de Zona DNS

Algunos servidores DNS externos pueden devolver una lista de direcciones IP y nombres de host válidos. Bajo ciertas condiciones, incluso puede ser posible obtener datos de la zona sobre la red interna de la organización.

Si un ataque tuviera éxito, el atacante obtiene información valiosa sobre la topología de la organización, incluyendo detalles sobre servidores específicos, su rol dentro de la estructura de TI, y posiblemente información sobre los sistemas operativos que se ejecutan en la red.

Este comportamiento depende de la configuración, por lo que puede ser necesario consultar múltiples servidores DNS mientras se intenta encontrar uno que permita transferencias de zona (Zone Transfers).

El mecanismo de Zone Transfer no ofrece autenticación, por lo que cualquier cliente puede solicitar a un servidor DNS una copia completa de la zona. Esto significa que, a menos que se implemente algún tipo de protección, un atacante puede obtener una lista de todos los hosts de un dominio, lo que le brinda múltiples vectores de ataque potenciales.

B. Protección insuficiente en la capa de transporte

Cuando la capa de transporte no está cifrada, todas las comunicaciones entre el servidor y el cliente son enviadas en texto plano lo cual permite que sea interceptado, inyectado y redirigido (también conocido como ataque de hombre en el medio MiTM).

Algunos de los posibles efectos que podrían generar esta situación son los siguientes:

- ✓ Posibles atacantes podrían interceptar las comunicaciones de forma pasiva, brindando acceso a datos sensibles que es transmitida como nombres de usuario y contraseñas.

- ✓ Los atacantes también podrían inyectar/remover contenido de las comunicaciones, permitiendo que se falsifique u omita información, inyectar código malicioso, o causar que el cliente acceda a contenido no confiable.

- ✓ Los atacantes también podrían redirigir la comunicación de forma que el servidor y el cliente ya no se estén comunicando entre sí y en su lugar interactuando con el atacante sin saberlo.

C. Servicio interno expuesto a Internet

Se localizaron servicios internos expuestos a Internet. Existen servicios considerados como sensibles porque:

- ✓ Pueden brindar acceso a datos restringidos o confidenciales.
- ✓ Están diseñados para ser consumidos solamente por sistemas internos.
- ✓ Poseen riesgos de diseño o vulnerabilidades conocidas.

No se debe exponer sistemas internos a internet porque pueden ser potencialmente alcanzados y atacados por actores no autorizados.

Algunos de los servicios internos que no deben estar expuestos son:

- ✓ Servicios de Bases de Datos (MySQL, MS SQL, Oracle, MongoDB, etc)
- ✓ Servicios de Escritorio Remoto (RDP, VNC, etc)
- ✓ Servicios de Directorio (Active Directory, LDAP, etc)
- ✓ Servicios de Recursos Compartidos (SMB, Samba, etc)
- ✓ Servicios administrativos (Telnet, SSH, consolas HTTP, etc)
- ✓ Servicios de respaldo.

Se debe tener en cuenta que servicios adicionales pueden entrar dentro de esta categoría según sea el análisis del profesional de seguridad durante la evaluación.

D. Consola de administración expuesta en Internet

Se detectó que la interfaz de Cisco AnyConnet Web VPN estaba expuesta a internet y la consola de administración "Exchange Admin Center" estaba accesible desde internet.

A pesar de que no es un riesgo inmediato, una consola administrativa expuesta puede hacer que sea significantemente fácil para atacantes el poder ingresar a los sistemas o inclusive obtener acceso a recursos internos, especialmente si los controles de acceso están limitados solamente a usuarios y contraseñas solamente.

Esta situación permite el uso de ataques por fuerza bruta, ingresar con credenciales por defecto o comprometidas, o en el caso de sistemas desactualizados, acceso al explotar vulnerabilidades. Inclusive en casos donde el URL de la consola de administración es difícil de adivinar, muchas herramientas son capaces de descubrirlos.

E. Divulgación de información en Microsoft Exchange Client Access Server

La dirección IP 201.195.230.180 se identificó como servidor de correo Microsoft Exchange expuesto en internet bajo en nombre de dominio correo.banhvi.fi.cr. Además, como parte de las pruebas de validación de la vulnerabilidad "CVE-2022-41040 - Server Side Request Forgery (SSRF) in Microsoft Exchange Server" se detectó la divulgación de información privada del servidor Exchange.

Esto permite que el Microsoft Exchange Client Access Server (CAS) se pueda ver afectado por una vulnerabilidad de divulgación de información.

Un atacante remoto no autenticado puede explotar esta vulnerabilidad para conocer la dirección IP interna del servidor.

El atacante puede enviar una solicitud GET manipulada al Web Server con un encabezado host vacío, lo que expone las direcciones IP internas del sistema subyacente en la respuesta del encabezado.

F. Algoritmos de intercambio de claves débiles SSH activados

El servidor SSH remoto está configurado para permitir algoritmos de intercambio de claves que se consideran débiles.

Esto se basa en el borrador del documento IETF Actualizaciones y recomendaciones del método de intercambio de claves (KEX) para Secure Shell (SSH).

Existe una guía sobre los algoritmos de intercambio de claves que DEBEN y NO DEBEN habilitarse. Entre estos se encuentran los siguientes:

- ✓ diffie-hellman-group-exchange-sha1
- ✓ diffie-hellman-group1-sha1
- ✓ gss-gex-sha1-*
- ✓ gss-grupo1-sha1-*
- ✓ gss-group14-sha1-*
- ✓ rsa1024-sha1

G. Configuración inadecuada de seguridad

Se localizaron múltiples servicios expuestos en un mismo servidor.

Según el principio de menor privilegio, cada recurso debe tener la menor cantidad de servicios y permisos para su funcionamiento adecuado.

Compartir múltiples servicios críticos en un mismo servidor incrementa el daño colateral que un servicio puede causar a los otros.

El recurso afectado podría ser vulnerable si:

- ✓ Falta una adecuada protección de seguridad en alguna parte del recurso o si los permisos en los servicios en la nube están configurados de manera incorrecta.
- ✓ Se encuentran habilitadas o instaladas características innecesarias (por ejemplo, puertos, servicios, páginas, cuentas o privilegios innecesarios).
- ✓ Las cuentas predeterminadas y sus contraseñas siguen habilitadas y sin cambios.
- ✓ El manejo de errores revela pistas u otros mensajes de error excesivamente informativos a los usuarios.
- ✓ En sistemas actualizados, las últimas características de seguridad están deshabilitadas o no configuradas de manera segura.
- ✓ Las configuraciones de seguridad en los servidores de aplicaciones, frameworks de aplicaciones (por ejemplo, Struts, Spring, ASP.NET), librerías, bases de datos, servicios, puertos, etc., no están configuradas con valores seguros.
- ✓ El software está desactualizado o es vulnerable.

H. ViewState sin cifrar

El parámetro ViewState no está cifrado en una o más páginas, permitiendo que la información almacenada en él sea visible y pueda ser leída y manipulada por cualquiera, ya que solo está codificada en Base64 y no encriptada con un algoritmo de seguridad. Adicionalmente se encuentran indicios de que se podría utilizar el ViewState para la realización de ataques de ejecución remota de comandos por medio de deserialización.

El ViewState es un parámetro específico del framework ASP.NET, utilizado como una especie de rastro de navegación cuando el usuario interactúa con la aplicación, preservando valores y controles entre diferentes páginas web. Presente en las páginas dentro del parámetro ViewState, todos los valores son serializados y codificados en Base64 en un campo oculto.

Además de la codificación en Base64, el ViewState también puede ser firmado con un MAC (Message Authentication Code) para garantizar la integridad y cifrado para garantizar la confidencialidad.

En algunos casos, ViewState puede ser utilizado para ataques de deserialización que podrían resultar en ejecución remota de comandos.

I. Componentes Web desactualizados y vulnerables

Los componentes Web como libreras, frameworks y otros módulos de software, se ejecutan con los mismos privilegios que la aplicación. Si un componente vulnerable es explotado, el ataque puede facilitar la perdida de datos o compromiso del servidor.

Las Aplicaciones y APIs utilizando componentes con vulnerabilidades conocidas pueden reducir las defensas de la aplicación y permitir diversos ataques e impactos. Es usualmente vulnerable si:

- ✓ No se conoce las versiones de todos los componentes que utiliza (tanto en el lado del cliente como en el servidor).
- ✓ El software es vulnerable, no soportado o desactualizado. Esto incluye al sistema operativo.
- ✓ Si no se realizan revisiones de vulnerabilidades regularmente y no se subscribe a boletines de seguridad de los componentes que utiliza.
- ✓ Si no corrige o actualiza la plataforma base, frameworks y dependencias de forma oportuna y basada en riesgo.
- ✓ Si los desarrolladores de software no prueban la compatibilidad de las libreras actualizadas.

3. CONCLUSIÓN

El proceso de auditoría permitió constatar que el BANHVI ha avanzado en la implementación de mecanismos de control para la gestión de la ciberseguridad; no obstante, los resultados evidencian que persisten riesgos relevantes derivados de configuraciones deficientes, exposición innecesaria de servicios y falta de actualización oportuna de componentes críticos.

Es indispensable que la Administración Activa adopte acciones correctivas inmediatas y sostenidas, orientadas a:

- ✓ Fortalecer la gobernanza de la ciberseguridad.
- ✓ Implementar controles de detección, respuesta y prevención de incidentes.
- ✓ Integrar las recomendaciones emitidas por la auditoría técnica externa en un plan de acción institucional con seguimiento formal.

En términos generales, los hallazgos reflejan un entorno tecnológico en desarrollo que requiere madurez operativa y técnica para alcanzar niveles de seguridad acordes con los estándares del sector financiero y las exigencias normativas vigentes.

La Auditoría Interna reafirma su compromiso de acompañar a la Administración en la mejora continua de los procesos de seguridad informática y la protección de los activos tecnológicos del BANHVI.

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 A Genaro Fuentes Abarca, Jefatura de TI o quien ocupe su cargo:

Pruebas de Penetración Interna

Riesgos Altos

4.1.1 Componentes de Infraestructura desactualizados y vulnerables

Se requiere actualizar los componentes desactualizados a la última versión disponible por parte del fabricante.
Si la actualización no es posible, debe considerar la implementación de controles compensatorios para mitigar el riesgo.

Como parte de algunas recomendaciones adicionales se debe evaluar o implementar un proceso de gestión de actualizaciones para:

- ✓ Remover dependencias no utilizadas, características, componentes, archivos y documentación que sean innecesarios.
- ✓ Mantener un inventario constante de versiones tanto de componentes utilizados en el lado del cliente (navegadores) como en el servidor (frameworks, librerías) y sus dependencias.
- ✓ Monitorear de forma constante las fuentes como CVE (Common Vulnerability and Exposures) y NVD (National Vulnerability Database) para detectar vulnerabilidades en componentes.
- ✓ Subscribirse a alertas por correo para recibir boletines de seguridad relacionados con los componentes que utiliza.
- ✓ Obtener componentes solamente desde las fuentes oficiales sobre enlaces seguros. Prefiera paquetes firmados para reducir las probabilidades de incluir componentes modificados o maliciosos.
- ✓ Monitorear las aplicaciones y componentes que no son mantenidos o que no crean parches de seguridad para versiones anteriores. Si la actualización no es posible, considere el uso de "Virtual patching" para monitorear, detectar y protegerse contra algún riesgo descubierto.

Adicionalmente, se debe implementar un plan continuo para monitorer, revisar, actualizar y administrar cambios configuración según el tiempo de vida de las aplicaciones o portafolio de productos.

Nivel de Riesgo: **Alto**

Pruebas de Penetración Externa

Riesgos Críticos

4.1.2 SMTP Relay abierto

Los servicios SMTP sin autenticación no deben estar expuestos a internet.

Es relevante adicionalmente que se consideren las siguientes recomendaciones adicionales:

1. Restringir el SMTP Relay:
Permitir solo direcciones IP o redes específicas: Configura el servidor de correo para que solo acepte y reenvíe correos desde direcciones IP o redes conocidas y confiables.
Restringir el reenvío a dominios específicos: Si es posible, configura el servidor para que solo reenvíe correos para tu propio dominio y otros dominios que autorices específicamente.

2. Implementar autenticación de correo electrónico:
SPF (Sender Policy Framework): Define qué servidores están autorizados para enviar correos en nombre de tu dominio.
DKIM (DomainKeys Identified Mail): Añade una firma digital a los correos salientes para verificar la identidad del remitente.
DMARC (Domain-based Message Authentication, Reporting, and Conformance): Proporciona instrucciones sobre cómo manejar correos que no superen las validaciones SPF o DKIM, como rechazarlos o ponerlos en cuarentena.

3. Asegurar las conexiones:
Usar cifrado TLS/SSL: Siempre cifra las conexiones de correo electrónico utilizando TLS/SSL para evitar la interceptación y garantizar la confidencialidad de los datos.
Considerar SMTPS (SMTP over SSL/TLS): Utiliza SMTPS para conexiones SMTP seguras, especialmente al conectarse desde redes públicas.

Nivel de Riesgo: **Alto**

Riesgos Altos

4.1.3 Transferencia de Zona DNS

Configurar todas las zonas DNS para que solo se permita la transferencia hacia direcciones IP específicas y permitidas.

Nivel de Riesgo: **Alto**

4.1.4 Protección insuficiente en la capa de transporte

- ✓ Implementar medidas de protección para el cifrado de las comunicaciones como el uso de la capa de transporte seguro SSL/TLS.
- ✓ No utilizar SMTP en puerto 25 sin cifrar y en su lugar forzar el uso de alternativas de SMTP sobre TLS que garantiza el cifrado en la capa de transporte.

Nivel de Riesgo: **Alto**

4.1.5 Servicio interno expuesto a Internet

- ✓ No exponer ningún servicio sensible hacia Internet configurando las reglas de control de acceso en el muro de fuego (Firewall).
- ✓ Se recomienda no exponer servicios FTP en internet, aunque estén cifrados debido al riesgo que representa la posibilidad de ataques por fuerza bruta.
- ✓ Si el servicio debe exponerse por decisión interna, se deben aplicar mecanismos de protección adicionales como el restringir el acceso por medio de listas de acceso que permitan una lista de direcciones IP permitidas (Whitelist).

Nivel de Riesgo: **Alto**

4.1.6 Consola de administración expuesta en Internet

- ✓ No exponer sobre internet ninguna consola de administración de dispositivos, software de terceros o portales de gestión internos.
- ✓ Estas interfaces deben ser alcanzables solo desde redes privadas o a través de conexiones VPN.
- ✓ Habilitar el acceso por listas blancas de direcciones IP solamente si las opciones mencionadas en el punto anterior no son posibles, sin embargo, tenga en cuenta que no es recomendado y no debe ser su primera opción considerada.
- ✓ Los clientes de Cisco AnyConnect pueden ser administrados por el personal de tecnología sin necesidad de exponer la interfaz de autenticación de Cisco que puede ser abusada en ataques de fuerza bruta.
- ✓ Restringir el acceso al ECP (Exchange Admin Center) para que no sea accesible desde internet.

Nivel de Riesgo: **Alto**

4.1.7 Divulgación de información en Microsoft Exchange Client Access Server

- ✓ Se deben aplicar los últimos parches y utilizar reglas para el bloqueo de información divulgada.
- ✓ Valorar la utilización de URLrewrite para rechazar solicitudes con encabezados Host vacíos y bloquear HTTP1.0.

Nivel de Riesgo: **Alto**

4.1.8 Algoritmos de intercambio de claves débiles SSH activados

Se debe deshabilitar todos los algoritmos de intercambio de claves que se consideran débiles.

Nivel de Riesgo: **Alto**

4.1.9 Configuración inadecuada de seguridad

Se debe implementar la utilización de servidores separados para el servicio DNS y el servidor Web.

Nivel de Riesgo: **Alto**

4.1.10 ViewState sin cifrar

Se debe utilizar los cifrados que provee ASP.NET para los parámetros ViewState con HMAC.

Nivel de Riesgo: **Alto**

4.1.11 Componentes Web desactualizados y vulnerables

Se deben actualizar los componentes desactualizados a la última versión disponible por parte del fabricante.

Si la actualización no es posible, debe considerarse la implementación de controles compensatorios para mitigar el riesgo.

Como parte de algunas recomendaciones adicionales se puede implementar un proceso de gestión de actualizaciones para:

- ✓ Remover dependencias no utilizadas, características, componentes, archivos y documentación que sean innecesarios.
- ✓ Mantener un inventario constante de versiones tanto de componentes utilizados en el lado del cliente (navegadores) como en el servidor (frameworks, librerías) y sus dependencias utilizando herramientas como OWASP Dependency Check, RetireJS, etc.

- ✓ Monitorear de forma constante las fuentes como CVE (Common Vulnerability and Exposures) y NVD (National Vulnerability Database) para detectar vulnerabilidades en componentes.
- ✓ Utilizar herramientas para el análisis de composición de software (SCA) para automatizar el proceso.
- ✓ Subscribirse a alertas por correo para recibir boletines de seguridad relacionados con los componentes que utiliza.
- ✓ Obtener componentes solamente desde las fuentes oficiales sobre enlaces seguros. Prefiera paquetes firmados para reducir las probabilidades de incluir componentes modificados o maliciosos.
- ✓ Monitorear las librerías y componentes que no son mantenidos o que no crean parches de seguridad para versiones anteriores. Si la actualización no es posible, considere el uso de "Virtual patching" para monitorear, detectar y protegerse contra algún riesgo descubierto.

Nivel de Riesgo: **Alto**

Estudio realizado por:

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2025.12.22 15:51:27 -06'00'

MATI. Jorge Ramirez Bolaños
Auditor Encargado

MAURICIO GONZALEZ ZUMBADO (FIRMA)

Firmado digitalmente por MAURICIO GONZALEZ ZUMBADO (FIRMA)
Fecha: 2025.12.22 17:08:59 -06'00'

Aprobado Lic. Mauricio González Zumbado
Auditor Interno a.i.