11 de diciembre de 2019
AI-707-2019

Señor
Alberto López Chaves
Gerente General

Asunto: Remisión de Informe AI-C-010-2019

Estimado señor:

Se remite el informe N° AI-C-10-2019, en el cual se consignan los resultados de la “Informe de la auditoría de cumplimiento sobre la seguridad de la red, bases de datos, configuraciones y web”

El día 6 de diciembre de 2019 la Auditoría Interna expuso los resultados, la conclusión y las recomendaciones obtenidas del estudio a la Gerencia y a los responsables de poner en práctica las recomendaciones.

Las recomendaciones se emiten al amparo del artículo 35 de la Ley Orgánica del Instituto, y a lo indicado en los artículos 22, 35 y 36 de la Ley Nº 8292 “Ley General de Control Interno”, que establecen un plazo de 10 días hábiles, para ordenar la implantación de las recomendaciones. Si discrepa de ellas, debe dentro ese plazo señalado elevar el informe a la Junta Directiva con las objeciones y soluciones alternas, con copia a la Auditoría Interna, para el análisis y resolución definitiva.

De aceptarse las recomendaciones, favor suministrar copia de las órdenes emitidas dentro de los próximos diez días hábiles, contados a partir del día siguiente al recibo del presente informe, para que los funcionarios responsables cumplan con lo recomendado por esta Auditoría Interna.

Favor enviar, dentro de los 15 días hábiles posteriores a la fecha en que instruyó la implementación de las recomendaciones, el plan de Implementación de las recomendaciones, que incluya de manera precisa las actividades necesarias, los responsables de desarrollarlas, las fechas y de requerirse los recursos.

Dado que ese plan es la base para verificar por parte de la Auditoría Interna la implementación de lo recomendado, se solicita comunicar cualquier modificación que a futuro se requiera previo al vencimiento de las fechas establecidas en el plan. Por último, respetuosamente se advierte sobre las posibles responsabilidades en que se puede incurrir por el incumplimiento injustificado de los deberes asignados según el artículo 39 de la Ley 8292.

Atentamente,

FERNANDO JOSE RIVERA SOLANO (FIRMA)

Firmado digitalmente por FERNANDO JOSE RIVERA SOLANO (FIRMA)
Fecha: 2019.12.11 17:05:35 -06'00'

Fernando Rivera Solano
Auditor Interno

C. Sra. Karen Hernández Bonilla
Departamento de TI
Sr. Saúl Ruiz Fernández
Dirección de Mercadeo

FRS / kbm

(506)2299.5800, San José Costa Rica
www.ict.go.cr / www.visitcostarica.com

INSTITUTO COSTARRICENSE DE TURISMO

AUDITORÍA
agregando valor a la gestión del ICT

AI-C-010-2019
Informe de la auditoría de cumplimiento sobre la seguridad de la red, bases de datos, configuraciones y web del Instituto Costarricense de Turismo.

Diciembre, 2019

esencial COSTA RICA

(506)2299.5800, San José Costa Rica
www.ict.go.cr / www.visitcostarica.com

INSTITUTO COSTARRICENSE DE TURISMO

Auditoría Interna

CONTENIDO

INSTITUTO COSTARRICENSE DE TURISMO

Auditoría Interna

RESUMEN EJECUTIVO DEL ESTUDIO

La realización de este estudio de auditoría tiene su origen en el Plan Anual de la Auditoría Interna 2019. Contiene los resultados del análisis de los sitios web, equipos pertenecientes a la red interna, infraestructura inalámbrica, configuraciones de equipos de bases de datos y de la suite de servicios de Office 365.
Del análisis realizado se han determinado oportunidades de mejora en los siguientes puntos:

- Vulnerabilidades y riesgos relacionados con el acceso no autorizado desde la infraestructura externa del ICT y a los sistemas críticos de la red interna como usuario interno o criminal cibernético, así como a la configuración de los puntos de acceso de la red inalámbrica institucional.

- La configuración de equipos que permitan reducir la superficie de ataque de los activos y sirva como configuración base de seguridad.

Producto de los resultados obtenidos se emite el presente con siete recomendaciones y además siete informes técnicos con 95 recomendaciones fortalecer la infraestructura tecnológica del ICT. Las principales recomendaciones son las siguientes:

- Fase Pruebas Externas: Definir controles basados en el principio de mínimo acceso, en los sitios web donde se revela información confidencial con el objetivo de que únicamente personas autorizadas puedan acceder a la misma.

- Fase Pruebas Internas: Desarrollar e implementar un procedimiento de gestión de parches de seguridad con el objetivo de mantener la infraestructura tecnológica actualizada

- Fase Pruebas Revisión de Configuraciones: Desarrollar e implementar un procedimiento de línea base de configuraciones de seguridad que aplique para todos los equipos de la infraestructura tecnológica de ICT con el objetivo de evitar configuraciones por defecto.

AI-C-010-2019

Informe de la auditoría de cumplimiento sobre la seguridad de la red, bases de datos, configuraciones y web del Instituto Costarricense de Turismo.

1. INTRODUCCIÓN

1.1 Origen del estudio

El estudio se originó en cumplimiento del Plan Anual de Trabajo 2019, ante la ausencia de evaluaciones por parte de la Administración y debido a la evolución de las técnicas de ataques cibernéticos, por lo que se planteó la necesidad de realizar pruebas de vulnerabilidades[1] para determinar la eficacia del control implementado en materia de seguridad informática, aunado a esto, el sistema de control interno institucional requiere contar con mecanismos efectivos de seguridad computacional que prevengan la intrusión no autorizada a los diferentes servicios y componentes de la plataforma tecnológica, que contribuyan a minimizar los riesgos que podrían afectar la continuidad del negocio, así como la confidencialidad, integridad y disponibilidad de la información.

Asimismo, existen en nuestro país legislación y normativa de protección de datos, como lo son el Código Penal, Ley de Información No Divulgada, Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales y Código de Trabajo que obligan a la entidad a asegurar sus sistemas.

[1] Una vulnerabilidad es una debilidad que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

1.2 Objetivos del estudio

Objetivo general

- Evaluar el estado general de la plataforma tecnológica con el fin de identificar oportunidades de mejora en sus componentes que puedan comprometer los principios de confidencialidad, integridad y/o disponibilidad de la información de la organización.

1.3 Alcance de la auditoría

A continuación, se presenta una serie de tablas que representan el alcance del proyecto de auditoría, según lo contratado a la empresa Deloitte.

Recursos a evaluar	Cantidad de sitios Web
• 9 IPs Públicas	• 3 sitios web
• 400 Direcciones IPS	• 4 Redes Inalámbricas
• 1 Aplicación interna	
• 22 instancias de bases de datos	• Office 365

Fases del proyecto

A continuación, se describe las fases de la la ejecución del análisis de seguridad, así como su alcance en términos de equipos evaluados y locación geográfica.

Tabla 4, Fases del análisis de seguridad

Fase	Descripción	Ubicación de las pruebas
Fase de pruebas externas (I)	Pruebas cuyo objetivo principal es identificar las vulnerabilidades y riesgos relacionados con la infraestructura externa del ICT.	Laboratorio de Cyber de Deloitte
Fase de pruebas internas (II)	Pruebas cuyo objetivo principal es identificar de las vulnerabilidades y riesgos relacionados con la infraestructura interna del ICT.	Sede Central y sedes regionales (Puntarenas y Liberia)
Fase de revisión de configuraciones (III)	Pruebas cuyo objetivo principal es analizar e identificar oportunidades de mejora en las configuraciones de bases de datos y correo electrónico basados en buenas prácticas de seguridad.	Sede Central

Metodología aplicada

Identificar posibles vulnerabilidades dentro de la red interna de la organización, partiendo desde una conexión a una punta de red dentro de las oficinas centrales del ICT y en las sedes regionales de Liberia y Puntarenas; siguiendo un enfoque “White Box” con el fin de evaluar si dichas vulnerabilidades podrían llegar a ser explotadas por un intruso o usuario malicioso obteniendo así información sensible o accesos privilegiados en los sistemas.

Mediante diferentes escenarios se simularon ataques a través de técnicas de evaluación e intrusión contra la red interna y sus componentes. Todo lo anterior, sin afectar el funcionamiento normal de los equipos ni su integridad.

Las fases del proyecto se ejecutaron entre el 5 y el 26 de septiembre en la sede central y en las sedes regionales entre el 25 y 28 de octubre del 2019.

Auditoría Interna

Para la ejecución de esta etapa se procedieron a utilizar las versiones más actualizadas de las siguientes herramientas y componentes asociados a éstas:

Herramientas utilizadas	
Herramienta	**Descripción**
Kali Linux	Es una distribución de Linux especializada en pruebas de penetración. Todos los paquetes distribuidos con este sistema operativo se encuentran personalizados para la realización de pruebas de penetración y de vulnerabilidades, escaneo de redes, entre otros.
Nmap	Es un escáner que permite identificar puertos abiertos en determinados equipos.
Nessus	Es una herramienta que permite la detección de vulnerabilidades en determinados equipos.
DNSEnum	Este escáner permite obtener información útil como rangos de IP y la enumeración de dominios registrados en un determinado servidor DNS.
OpenSSL	Es una herramienta que permite establecer conexiones utilizando los protocolos SSL o TLS.
XSS Me – SQL Inject Me	Es una suite de programas para la analizar las vulnerabilidades de Cross Site Script y SQL Injections.
Acunetix	Herramienta que analiza vulnerabilidades web.

Herramientas utilizadas	
Herramienta	**Descripción**
SCANSSL	Herramienta para realizar consultas a los certificados SSL.
BurpSuite	Herramienta utilizada como Web Proxie para analizar peticiones web de la aplicación.
Guía CIS	Estas guías elaboradas de CIS están dirigidas a los administradores de sistemas y de aplicaciones, especialistas en seguridad, auditores, HelpDesk, y el personal de despliegue de plataforma que planean desarrollar, implementar, evaluar o dar soluciones de seguridad para la incorporación de Microsoft Windows Server.

1.4 Normas técnicas de la auditoría

La auditoría se efectuó de conformidad con la normativa aplicable al ejercicio de la Auditoría Interna, las “Normas Generales de Auditoría para el Sector Público”, el “Manual para el Ejecución de los Servicios de la Auditoría Interna”, así como el Sistema de Gestión de Calidad de la Auditoría Interna y otra normativa conexa.

1.5 Marco normativo y buenas prácticas utilizadas.

El marco legal que se utilizó de referencia es el siguiente:

a. Normas Técnicas para la gestión y el control de las Tecnologías de Información (NTGCTI)

Buenas prácticas de la industria

a. National Institute of Standards and Technology (NIST) 800-115
b. National Institute of Standards and Technology (NIST) 800-97

c. Open Web Application Security Project (OWASP) Top 10
d. Center for Internet Security (CIS) Benchmarks.
e. White Paper “Conducting a Penetration Test on an Organization” del SANS Institute

1.6 Aspectos positivos que favorecieron la ejecución de la auditoría

La colaboración de los funcionarios del Departamento de TI que facilitó la labor ejecutada por la Auditoría Interna.

1.7 Limitaciones

- La red interna de ICT cuenta con 16 millones de direcciones IP utilizables por lo que, a la hora de realizar el escaneo de equipos, se escanearon únicamente los equipos incluidos en el alcance y no la totalidad de las direcciones IPs disponibles.
- Se analizaron equipos conectados a la red interna durante el periodo de las pruebas definido anteriormente, en caso de que computadoras no estuvieran conectadas a la red durante ese período no se incluyeron en el alcance.
- Durante las pruebas en las sedes regionales se ejecutaron comandos en computadoras que no contaban con permisos de administradores locales lo cual pudo limitar el alcance total del comando.

1.8 Comunicación verbal de los resultados de la auditoría

En reunión celebrada el día 6 de diciembre de 2019 en la Auditoría Interna, se expusieron los resultados, conclusiones y recomendaciones del presente informe ante los siguientes funcionarios: Alberto López Chaves, Gerente General y Karen Hernández Bonilla, Departamento de TI. Por parte de esta Auditoría Interna: Fernando Rivera Solano y Karen Barquero Murillo.

1.9 Análisis realizado de las observaciones recibidas de la Administración

No hubo observaciones por parte de la Administración que generaran cambios en los resultados del estudio.

1.10 Generalidades acerca del objeto auditado

Calificación de riesgo

Como forma de poder evaluar e informar los riesgos institucionales la calificación se basó en impacto y probabilidad de ataque de las múltiples vulnerabilidades identificadas. La siguiente tabla describe la forma de cómo se clasifican los riesgos:

Impacto	x	Probabilidad	=	Riesgo
Alto	x	Alta	=	Alto
Alto	x	Media	=	Alto
Alto	x	Baja	=	Medio
Medio	x	Alta	=	Medio
Medio	x	Media	=	Medio
Medio	x	Baja	=	Bajo
Bajo	x	Alta	=	Bajo
Bajo	x	Media	=	Bajo
Bajo	x	Baja	=	Bajo

Durante la ejecución de las pruebas de penetración externas, en las que se evaluó la infraestructura externa del ICT (sitio web, servidores, equipos de comunicación, entre otros) fueron ejecutadas pruebas haciendo uso de medios automatizados y manuales.

Auditoría Interna

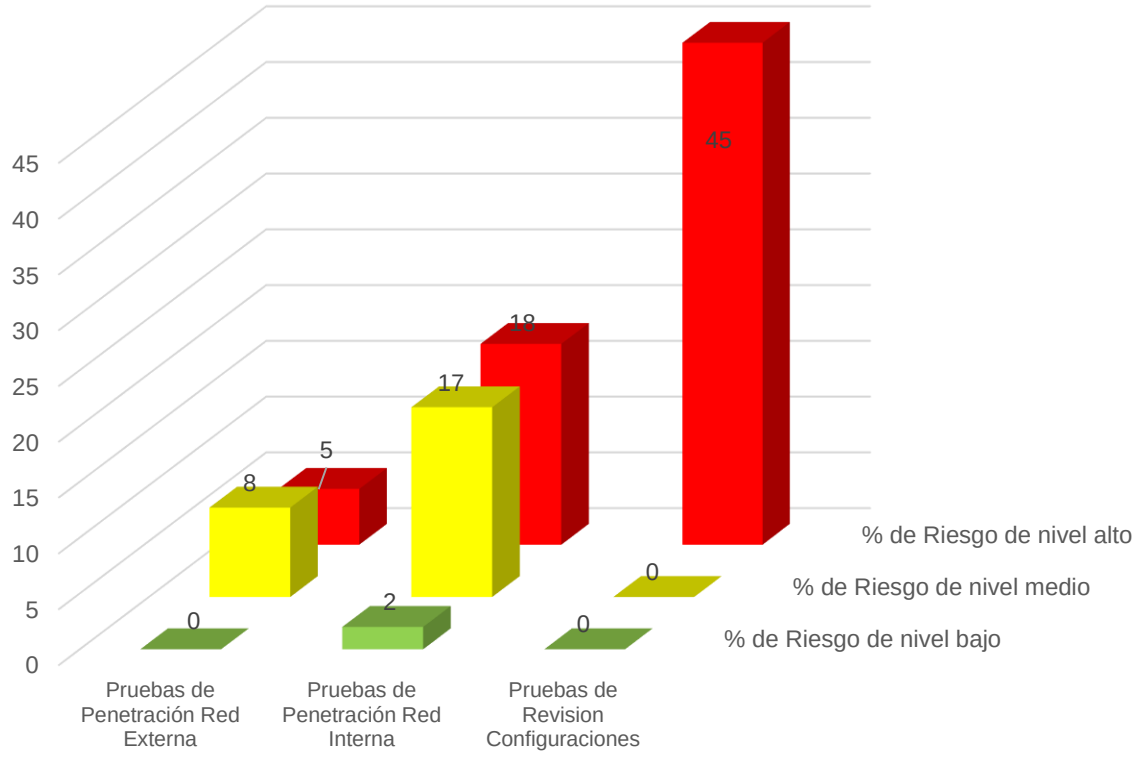
Durante la ejecución de la fase análisis de vulnerabilidades sobre la infraestructura tecnológica interna fueron ejecutadas pruebas para evaluar la seguridad de activos de información de la plataforma tecnológica donde figuran servidores, bases de datos, equipos de comunicación y equipos de usuario final. Además, se analizó el sistema integrado de recursos humanos, planillas y pagos (SIRH), que se encuentra en la red interna del instituto, utilizando la metodología mencionada anteriormente.

Durante la ejecución de la fase de revisión de configuraciones de seguridad se realizaron aproximadamente 110 pruebas para evaluar la seguridad de configuraciones de los equipos de bases de datos y correo electrónico de ICT.

2. RESUMEN DE LOS HALLAZGOS IDENTIFICADOS

Finalizada la ejecución del análisis de seguridad sobre las infraestructura externa, infraestructura interna, redes inalámbricas y revisión de configuraciones se pudo determinar que existe un total de 68 vulnerabilidades con nivel de criticidad alto, que podrían representar un riesgo a la infraestructura tecnológica de ICT, según el siguiente detalle:

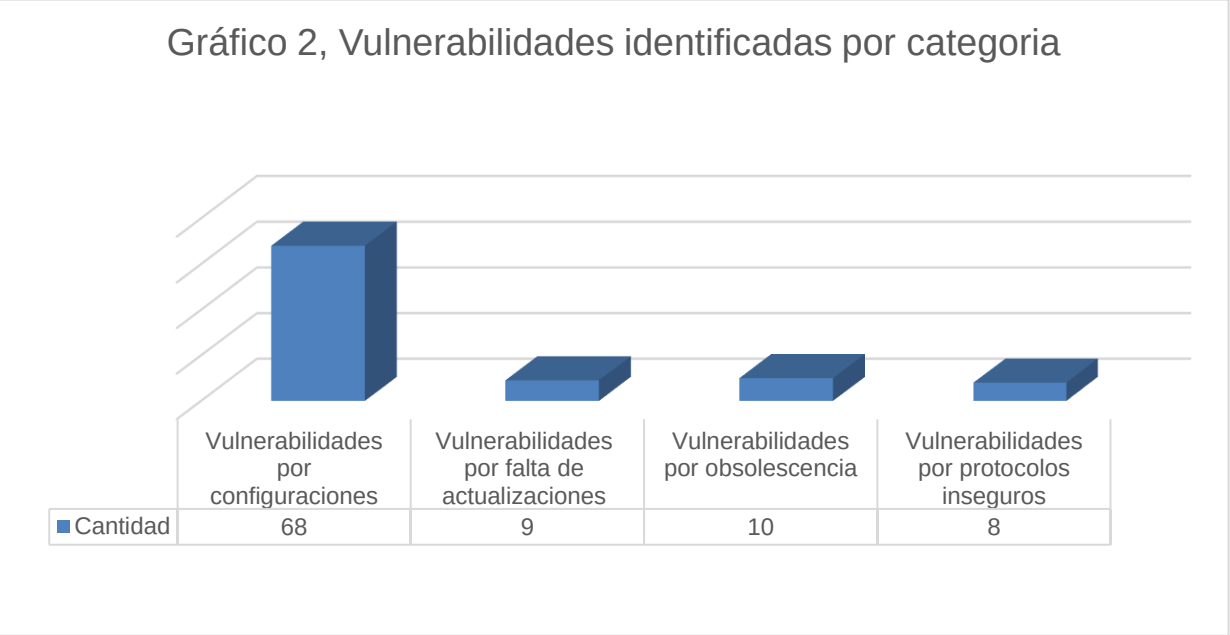
Gráfico 1, Debilidades identificadas y pruebas ejecutadas



Fuente: Elaboración propia, con base en la aplicación de las pruebas ejecutadas.

Por otra parte, se identificaron las siguientes categorías de vulnerabilidades:

- **Configuraciones:** se presentan cuando los parámetros de seguridad de los equipos se encuentran configurados de forma débil facilitando el riesgo de la seguridad de la información.
- **Falta de actualizaciones:** estas se presentan debido a que equipos o aplicaciones no cuentan los últimos parches de seguridad recomendados por el proveedor.
- **Obsolescencia:** aquellos equipos o aplicaciones que no se encuentran dentro del periodo de soporte del proveedor.
- **Protocolos inseguros:** se utilizan servicios que cuentan con vulnerabilidades que afectan la seguridad de la información.



Fuente: Elaboración propia, con base en la aplicación de las pruebas ejecutadas.

2.1 PRUEBAS EXTERNAS

A continuación, se presenta el resumen de los hallazgos presentes en la fase de ejecución de pruebas de penetración externas.

Nombre del hallazgo[2]	Descripción del hallazgo	Calificación del riesgo institucional
Configuraciones vulnerables	Se identificó que existen configuraciones de seguridad vulnerables que revelan información sensible y confidencial a cualquier persona desde internet, esta información implicaría un riesgo tanto de imagen como técnico para el ICT si esta información fuera utilizada por personas malintencionadas.	
Protocolos y Servicios inseguros	Se identificó que se utilizan protocolos y servicios que se consideran inseguros debido a que cuentan con vulnerabilidades conocidas o no cuentan con las medidas necesarias para asegurar que la información sensible y confidencial viaje en forma segura a través de desde internet.	
Versiones desactualizada	Se identificaron equipos expuestos a internet que no cuentan con actualizaciones de seguridad o utilizan versiones que cuentan con vulnerabilidades previamente identificadas. Debido a esto se podrían	

[2] Ver detalles en informes técnicos

Nombre del hallazgo[2]	Descripción del hallazgo	Calificación del riesgo institucional
	presentar ataques a los equipos y afectar la disponibilidad de los servicios	
Panel de administración web identificado	Un atacante al identificar la pantalla de autenticación para los usuarios del sistema, podría efectuar ataques de fuerza bruta o un ataque de diccionario (consiste en probar posibles usuarios y contraseñas genéricos o conocidos) sobre los campos de “login” y descifrar la contraseña ya que se identificó previamente el usuario de Administración.	🟠

Simbología:

🔴 **Alto:** Se refiere a vulnerabilidades en las cuales su explotación puede derivar en un compromiso total de la confidencialidad, integridad y/o disponibilidad del dispositivo en sí y eventualmente de otros componentes conectados; generalmente afecta a recursos críticos de la infraestructura, como servidores de bases de datos, o accesos a sistemas aplicativos y/o a dispositivos de control de tráfico de red.

🟠 **Medio:** Se refiere a vulnerabilidades cuya explotación puede derivar en el compromiso de algún atributo de seguridad, pudiendo afectar tanto a recursos críticos como no críticos de la infraestructura.

2.2 Pruebas Internas

A continuación, se presenta el resumen de los hallazgos presentes en la fase de ejecución de pruebas de penetración interna.

Auditoría Interna

Nombre del hallazgo[3]	Descripción del hallazgo	Calificación del riesgo institucional
Falta de Parches de Actualizaciones de Seguridad en equipos	Durante el análisis de seguridad realizado se identificó que ausencia de parches de seguridad considerados críticos en la infraestructura tecnológica que soporta la operativa de ICT.	
Equipos obsoletos sin soporte del fabricante	Además de identificaron equipos considerados obsoletos por sus propios fabricantes debido a que ya no existe ningún tipo actualización de seguridad hacia los mismo, esto significaría un riesgo inminente para ICT.	
Credenciales de autenticación en archivos de configuración interna	Un atacante podría conseguir la contraseña de la base de datos si logra obtener acceso al servidor donde se encuentra la aplicación. El servidor donde se encuentra la aplicación actualmente presenta múltiples vulnerabilidades por lo que un atacante podría explotar las mismas para ingresar al servidor.	
Protocolos y Servicios inseguros	Se identificó que se utilizan protocolos y servicios que se consideran inseguros debido a que cuentan con vulnerabilidades conocidas o no cuentan con las medidas necesarias para asegurar que la información	

[3] Ver detalles en los informes técnicos

(506)2299.5800, San José Costa Rica
www.ict.go.cr / www.visitcostarica.com

Nombre del hallazgo[3]	Descripción del hallazgo	Calificación del riesgo institucional
	sensible y confidencial viaje en forma segura a través de la red interna	
Equipo de red con carpetas compartidas públicas	Un usuario malicioso puede ingresar en estas carpetas compartidas y borrar, modificar o hasta sacar en algún dispositivo de almacenamiento información sensible de la organización poniendo en riesgo la integridad de la información, y al mismo tiempo ser víctimas de chantaje o de espionaje corporativo poniendo así en riesgo la entidad y los procesos.	
Falta de autenticación de doble factor	La aplicación SIRH no realiza una autenticación por medio de contraseña, debido a que se ingresa al sistema una vez que se haya autenticado el usuario en la estación de trabajo. Un usuario mal intencionado que obtenga credenciales validas de usuario puede ingresar la información personal del colaborador	

Simbología:

Alto: Se refiere a vulnerabilidades en las cuales su explotación puede derivar en un compromiso total de la confidencialidad, integridad y/o disponibilidad del dispositivo en sí y eventualmente de otros componentes conectados; generalmente

afecta a recursos críticos de la infraestructura, como servidores de bases de datos, o accesos a sistemas aplicativos y/o a dispositivos de control de tráfico de red.

🟠 **Medio:** Se refiere a vulnerabilidades cuya explotación puede derivar en el compromiso de algún atributo de seguridad, pudiendo afectar tanto a recursos críticos como no críticos de la infraestructura.

2.3 PRUEBAS DE CONFIGURACIONES DE SEGURIDAD

A continuación, se presenta el resumen de los hallazgos presentes en la fase de ejecución de pruebas de configuraciones de seguridad.

Nombre del hallazgo	Descripción del hallazgo	Calificación del riesgo institucional
Configuraciones por defecto	Se identificaron equipos que no cuentan con las configuraciones de seguridad según las buenas practicas definida por entes internacionales tanto para bases de datos como para el correo electrónico.	🔴

Simbología:

🔴 **Alto:** Se refiere a vulnerabilidades en las cuales su explotación puede derivar en un compromiso total de la confidencialidad, integridad y/o disponibilidad del dispositivo en sí y eventualmente de otros componentes conectados; generalmente afecta a recursos críticos de la infraestructura, como servidores de bases de datos, o accesos a sistemas aplicativos y/o a dispositivos de control de tráfico de red.

3. RECOMENDACIONES

Por lo indicado en los párrafos anteriores, se recomienda a la Gerencia, instruya al Departamento de Tecnología de Información, lo siguiente:

1. Diseñar e implementar un plan de acción aprobado por la Gerencia, para reemplazar los equipos y/o aplicaciones que se encuentran en estado de obsolescencia o próximos a caducar.
2. Analizar la factibilidad de implementar herramientas automatizadas para actualizar permanentemente el software institucional de conformidad con las políticas institucionales.
3. Diseñar e implementar conjuntamente con el Departamento de Recursos Humanos, un programa de concientización sobre la seguridad de la información, para que los colaboradores del ICT conozcan y se comprometan con las regulaciones correspondientes, con el fin de minimizar los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.
4. Definir, documentar y aplicar estándares de configuración de seguridad para los sistemas operativos y software autorizados
5. Diseñar un plan de capacitación continua para los colaboradores del Departamento de TI, que minimice la dependencia de terceros contratados en la implementación y el mantenimiento del software e infraestructura tecnológica.
6. Que la Gerencia, emita la instrucción mediante el comunicado correspondiente, para que el Departamento de TI, asuma el rol y responsabilidad que por competencia técnica le corresponde en todas las contrataciones con terceros, vigentes y futuras, de manera que se garantice razonablemente su congruencia con las políticas sobre calidad, seguridad y seguimiento, y además minimice la dependencia respecto de los servicios contratados a terceros.
7. Presentar a la Gerencia dentro del plazo que ésta establezca, un plan de acción para que, en coordinación con las unidades correspondientes, se

implementen las noventa y cinco (95) recomendaciones técnicas, contenidas en los siete informes específicos –adjuntos a este informe-, para minimizar las vulnerabilidades detectadas, **considerando que cada recomendación deberá ser validada en un entorno de prueba antes de ser implementada en el ambiente de producción.**

Las anteriores recomendaciones se emiten al amparo del artículo 35 de la Ley Orgánica del Instituto y a la competencia que facultan los artículos 22, 35 y 36 de la Ley General de Control Interno.

4. CONCLUSIÓN

La ciberseguridad[4] es un aspecto fundamental que la Institución debe enfrentar ante una nueva realidad donde todo está interconectado, por lo que las vulnerabilidades identificadas en el estudio podrían representan riesgos para la institución que de materializarse por acciones mal intencionadas, podrían afectar significativamente, entre otros aspectos, la calidad de los servicios, razón por la que los riesgos de ciberseguridad se deben gestionar, ya que entre más automatizada esté una organización, tiene mayor probabilidad que surjan este tipo de riesgos que los riesgos tradicionales.

Si bien es cierto, el Departamento de Tecnologías de Información, ha implementado algunas medidas para fortalecer la seguridad digital, se debe destacar la necesidad de herramientas automatizas, capacitación y administración de contratos con terceros con el fin de minimizar los riesgos por actualizaciones pendientes, software obsoleto, falta de doble autenticación en aplicaciones, equipos de red con carpetas compartidas públicas y contraseñas por defecto, divulgación de información sensible, servicio de bases de datos expuesto, portales de administración web y servicios inseguros, que de materializarse pueden afectar significativamente el cumplimiento de los objetivos institucionales.

Si bien, el informe presenta las recomendaciones para mitigar las vulnerabilidades encontradas, para mejorar la seguridad cibernética, más allá de protocolos y políticas para prevenir ataques, es necesaria una transformación cultural organizativa, sobre la mejor forma de llevar a cabo esos controles, sin desmejorar la eficiencia, por lo que se debe entender que la ciberseguridad no es un asunto solo de TI sino de la organización en su conjunto.

[4] La ciberseguridad busca proteger la información digital en los sistemas interconectados. Está comprendida dentro de la seguridad de la información