




AUDITORIA INTERNA

A-A-03/2018

OBSERVACIONES DE AUDITORIA DETALLADAS

Nombre del Informe	Gestión y Seguridad de Redes - Scotiabank Perú, CrediScotia Financiera y SCI
Línea de Negocios / Función de Soporte	International Banking
Ubicación	Perú
Nivel de Riesgo (Banco)	Moderado
Nivel de Riesgo (País/Subsidiaria)	Moderado
Fecha de Término de Trabajo de Campo:	[Q1/2018]
Fecha de Emisión de Informe	[Q1/2018]
Opinión de Auditoría	Satisfactorio 

CONFIDENCIAL

APO # 2017-237-81

OBSERVACIÓN DE AUDITORÍA #1

Nombre de la Auditoría	Gestión y Seguridad de Redes SBP, CSF y SCI
Título de la Observación	Configuración de seguridad y gestión de vulnerabilidades
Nivel de Riesgo (Unidad/Proceso)	Alto
Nivel de Riesgo (País/Subsidiaria)	Moderado
Nivel de Riesgo (Scotiabank)	Bajo

Observación(es)

Sobre el proceso de aseguramiento de la configuración de seguridad en los dispositivos de redes observamos lo siguiente:

1. En promedio, 10% del total de parámetros de los 47 dispositivos de redes seleccionados como muestra (14 firewalls, 21 switches, 12 routers) no están configurados de acuerdo a lo recomendado por el fabricante o lo establecido en los checklist de configuración. Algunos de los parámetros no configurados correctamente y que permiten mitigar riesgos de interceptación de datos y denegación de servicio, son los siguientes:

Tipo Dispositivo	Dynamic ARP Inspection (*)	Desactivar Proxy ARP	Deshabilitar servicios no seguros	Complejidad claves SNMP	IP SSH v2	SNMP v3 (*)
# Firewall	0	0	5	0	6	5
# Switch	21	3	5	0	4	19
# Router	0	8	11	12	12	3
# Dispositivos con excepciones	21	11	21	12	22	27
% Dispositivos con excepciones	45%	23%	45%	26%	47%	57%

(*) Configuración de seguridad recomendada por el fabricante

Cabe señalar que uno de los parámetros configurados correctamente en todos los dispositivos es el parámetro de "Access list" que permite el acceso al dispositivo a sólo los usuarios inscritos en una lista.

2. Las guías de aseguramiento aplicadas en los dispositivos de redes omiten algunas recomendaciones de seguridad del fabricante que mitigan riesgos de interceptación de datos e indisponibilidad de los equipos.

3. Sobre un total de 9 altas de dispositivos de redes instalados en 2017 (firewalls, switches, routers), observamos que no existe el detalle de la evidencia de la configuración de seguridad implementada previo a la puesta en producción.

4. No existe una certificación periódica que asegure el cumplimiento del hardening de seguridad de los dispositivos de redes.

5. Sobre el escaneo de vulnerabilidades en los dispositivos de red mediante la herramienta IP360 observamos lo siguiente:

- 52 dispositivos de red (4% del total) con score mayor a 3,000 no fueron informados a la unidad de CREO - Perú Infraestructura para la remediación de las vulnerabilidades.

- b. 289 dispositivos de red (22% del total), no son escaneados por la herramienta IP360 (4 firewalls y 285 switches). **(Observación identificada por la gerencia).**

Implicación / Riesgo

Operacional/ Tecnológico

Explotación de vulnerabilidades en los dispositivos de red que podría afectar la confidencialidad e integridad de la información transmitida en forma no cifrada, así como la disponibilidad de la infraestructura de comunicaciones.

Causa(s) Raíz

Fallas en el diseño / ejecución del control

Recomendación(es)

Para la Gerencia de Seguridad de Informática:

1. Coordinar con la Gerencia de CREO Perú - Infraestructura Perú el ajuste de las configuraciones de los dispositivos de redes observados.
2. Revisar, actualizar y aprobar los checklists de hardening por tecnología de dispositivo de red (firewall, router, switch), de modo que se incluya la activación de los parámetros críticos de seguridad.
3. Elaborar e implementar un procedimiento de aseguramiento de dispositivos de redes que asegure la verificación y evidencia de la configuración de seguridad cuando se conecten/instalen nuevos dispositivos de redes.
4. Elaborar e implementar un procedimiento de certificación anual del aseguramiento de los dispositivos de redes (firewall, router, switch).
5. Revisar los dispositivos de red observados, incluirlos en los reportes periódicos de vulnerabilidades remitidos a la Unidad de CREO Perú - Infraestructura y asegurarse que se efectúen los ajustes necesarios para obtener un score satisfactorio.
6. Implementar la inclusión de los dispositivos de red observados en el servicio de escaneo y reporte de la herramienta IP360.
7. Implementar un procedimiento de conciliación periódica del inventario de dispositivos de redes contra lo registrado en IP360.

Plan de Acción de la Gerencia

1. Se coordinará con CREO Perú - Infraestructura la corrección del aseguramiento de los equipos observados. Asimismo, se coordinará la implementación de una herramienta para el control del Hardening de los equipos de Comunicaciones.
2. Se revisará y actualizará plantilla de hardening de equipos de Comunicaciones incluyendo parámetros críticos de seguridad.
3. Se ampliará el procedimiento de verificación de las configuraciones de seguridad cuando se conecten o instalen dispositivos de redes, se formalizara checklist como documento de puesta en Producción.

4. Se ampliará el procedimiento de certificación para el aseguramiento de redes (Firewall, router, switch). Se realizará una certificación manual del Aseguramiento de los equipos en base a una muestra de dispositivos críticos y luego progresivamente sobre el resto de equipos.
5. Actualmente estos 52 equipos ya se encuentran siendo reportados a la unidad de CREO para la remediación de las vulnerabilidades en 2018-Q1. Asimismo, se coordinará con CREO Perú - Infraestructura el ajuste necesario sobre estos dispositivos para reducir el score de las vulnerabilidades detectadas.
6. Se coordinará con IS&C Canadá el escaneo de los 289 dispositivos de redes observados.
7. Se monitoreará semanalmente que las redes sean escaneadas, y se reportará oportunamente a Toronto si existe una falla.

Acciones Específicas / Evidencia requerida para el Cierre de la Observación

1. Evidencia de los ajustes en la configuración de los dispositivos de redes observados revisada por IS&C Perú.
2. Checklists de aseguramiento por tecnología de firewalls, switches, routers revisados por IS&C Perú.
3. Sobre una muestra de altas de dispositivos de redes.evidencia del hardening revisado por IS&C Perú.
4. Evidencia de la certificación del hardening sobre una muestra dispositivos de redes críticos revisado por IS&C Perú.
5. Reporte IP360 con score compliant sobre los 52 dispositivos de redes con vulnerabilidades.
6. Reporte IP360 con score compliant sobre los 289 dispositivos de redes no escaneados.
7. Reporte de revisión de dispositivos de redes en inventario contra lo escaneado por IP360.

Fecha Esperada de Solución de la Gerencia:

- 1, 2, 3, 7. Q2-2018
4, 5, 6. Q3-2018

Fecha Esperada de Solución de Auditoría:

- 1, 2, 3, 7. Q3-2018
4, 5, 6. Q4-2018

OBSERVACIÓN DE AUDITORÍA #2

Nombre de la Auditoría	Gestión y Seguridad de Redes SBP, CSF y SCI
Título de la Observación	Acceso lógico
Nivel de Riesgo (Unidad/Proceso)	Moderado
Nivel de Riesgo (País/Subsidiaria)	Moderado
Nivel de Riesgo (Scotiabank)	Bajo

Observación(es)

Sobre los controles de acceso lógico en los dispositivos de redes (firewalls, switchs, routers) observamos lo siguiente:

1. Existen 5 cuentas genéricas (cprime, prtg, cfadmin, btito, admseguridad) con acceso privilegiado en los dispositivos de redes cuyas contraseñas no son custodiadas en el sistema firecall (Xceedium). Asimismo, la contraseña del usuario privilegiado "usr_tacacs" del servidor TACACS (control de accesos) no es modificada periódicamente. No obstante el acceso a dispositivos de redes está restringido sólo a personal de soporte.
2. No existe segregación de funciones en el otorgamiento de accesos en los dispositivos de redes. Al respecto no se obtuvo evidencia de aprobación de los privilegios otorgados a una muestra de 9 cuentas creadas en la herramienta Cisco Secure ACS.
3. No se realiza una certificación periódica de las cuentas con acceso a los dispositivos de red (21) registradas en Cisco Secure ACS. Asimismo, no se certifican las cuentas de accesos en los routers administrados por los proveedores Telefónica y Claro.

Implicación / Riesgo

- Cambios no autorizados en la configuración de los dispositivos de red, lo que podría afectar la confidencialidad e integridad de la información transmitida, así como la disponibilidad de la infraestructura de comunicaciones.
- Acceso no autorizado a los recursos de la red.

Causa(s) Raíz

- No se priorizó el control de las cuentas de acceso
- Fallas en el diseño / ejecución del control

Recomendación(es)

1. Modificar y custodiar las contraseñas de las cuentas privilegiadas observadas en la herramienta firecall. Asimismo, en el caso de la cuenta usr_tacacs, configurar el vencimiento de la contraseña según los requerimientos de políticas de contraseña.
2. Formalizar e implementar un proceso para la gestión de acceso de cuentas de acceso a los dispositivos de red, cumpliendo la segregación de funciones (solicitante / ejecutor / verificador).
3. Formalizar e implementar un control para certificar las cuentas con acceso a los dispositivos de red, incluyendo los equipos routers administrados por terceros.

Plan de Acción de la Gerencia

1. Se modificarán las contraseñas y custodiarán las cuentas identificadas, a la fecha ya se viene trabajando el registro en bóveda. Asimismo, se coordinará con Comunicaciones la configuración de cuenta usr_tacacs.
2. Se asumirá la administración de los accesos a los equipos de comunicaciones y se realizará la segregación de funciones. Se formalizara procedimiento.
Q2
3. Se ha incluido en el proceso de certificación, la validación de las cuentas con accesos a los dispositivos de red.

Acciones Específicas / Evidencia requerida para el Cierre de la Observación

1. Evidencia de la custodia de las cuentas observadas en el software firecall.
2. Evidencia de una muestra de otorgamiento/modificación baja de accesos bajo el nuevo procedimiento.
3. Evidencia de la certificación de accesos en el software CISCO ACS y cuentas locales en dispositivos de redes.

Fecha Esperada de Solución de la Gerencia:

- 1, 2. Q2-2018
3. Q3-2018

Fecha Esperada de Solución de Auditoría:

- 1, 2 y 4. Q3-2018
3. Q4-2018

OBSERVACIÓN DE AUDITORÍA #3

Nombre de la Auditoría	Gestión y Seguridad de Redes SBP, CSF y SCI
Título de la Observación	Control de cambios
Nivel de Riesgo (Unidad/Proceso)	Moderado
Nivel de Riesgo (País/Subsidiaria)	Bajo
Nivel de Riesgo (Scotiabank)	Bajo

Observación(es)

1. No se verifica si los cambios efectuados en las reglas de los firewalls (14 en Producción) por personal de CREO Perú - Infraestructura correspondan a solicitudes aprobadas FPR (Firewall Port Request).

2. El procedimiento de control de cambios sobre las reglas de los firewalls no se encuentra normado. Asimismo, el procedimiento de control de cambios de infraestructura no está alineado al nuevo modelo del Service Now.

Implicación / Riesgo

Operacional / Tecnológico

- Cambios en las políticas de acceso no autorizadas.
- Cambios no autorizados en la infraestructura de comunicaciones.
- Desconocimiento de controles contemplados en normas/procedimientos.

Causa(s) Raíz

- Falta de un adecuado diseño de políticas y controles.

Recomendación(es)

Gerencia de Seguridad Informática:

1. Implementar un control de verificación de cambios en las políticas de firewalls empleando el log de eventos de los firewalls, antes del cierre de la solicitud FPR. Asimismo, asegurarse que todos los cambios en los firewalls sean ingresados como solicitudes FPR.
2. Actualizar el procedimiento de control de cambios de políticas de firewalls y el procedimiento de control de cambios de infraestructura de acuerdo al nuevo modelo/roles Service Now.

Plan de Acción de la Gerencia

1. Se realizará la validación de los cambios post impacto de los FPR.
2. Se actualizará y publicará el procedimiento de cambios en Firewall en coordinación con el equipo de Comunicaciones.
3. Se actualizará y publicará el procedimiento de Control de Cambios con la nueva herramienta que se viene utilizando hace unos meses Service Now en coordinación con Planeamiento de la producción.

Acciones Específicas / Evidencia requerida para el Cierre de la Observación

1. Evidencia de una muestra de verificaciones de FPR's sobre los cambios registrados en los logs.
2. Procedimiento de control de cambios de políticas de firewalls aprobado.
3. Procedimiento de control de cambios de infraestructura actualizado y aprobado.

Fecha Esperada de Solución de la Gerencia:

1, 2 y 3. Q2-2018

Fecha Esperada de Solución de Auditoría:

1, 2 y 3. Q3-2018

OBSERVACIÓN DE AUDITORÍA #4

Nombre de la Auditoría	Gestión y Seguridad de Redes SBP, CSF y SCI
Título de la Observación	Obsolescencia y upgrade de software y hardware
Nivel de Riesgo (Unidad/Proceso)	Moderado
Nivel de Riesgo (País/Subsidiaria)	Bajo
Nivel de Riesgo (Scotiabank)	Bajo

Observación(es)

Respecto al upgrade y obsolescencia de los dispositivos de redes identificamos lo siguiente:

1. 10 switches localizados en el Data Center de San Isidro no cuentan con soporte del fabricante **(identificado por la Gerencia)**.
2. El software Cisco Secure ACS 4.0, que gestiona la administración y auditoría de los dispositivos de redes no cuenta con soporte.
3. Los sistemas operativos de 14 firewalls y 158 switches no están actualizados con la última versión recomendada por el fabricante.

Implicación / Riesgo

Riesgo Operacional / Tecnológico

- Las vulnerabilidades de software sin soporte pueden ser aprovechadas a través de exploits, impactando la integridad y confidencialidad de la información.
- Impacto en la disponibilidad de servicios, ante fallas en los dispositivos y falta de soporte por parte del proveedor.

Causa(s) Raíz

- No se consideró una renovación oportuna de la infraestructura tecnológica.
- Fallas en la ejecución del control.

Recomendación(es)

Gerencia de CREO Perú - Infraestructura:

1. Reemplazar los switches que no cuentan con el soporte del fabricante.
2. Renovar el software que soporta la administración de los dispositivos de redes observados, de modo que se cuente con soporte vigente.
3. Actualizar el sistema operativo de los dispositivos identificados a versiones que mitiguen vulnerabilidades de seguridad.

Plan de Acción de la Gerencia

1. Los equipos serán reemplazados cuando culmine la migración a LATAM DCC. Mientras tanto se cuenta con equipos en el inventario en caso de contingencias.
2. Estamos esperando una solución estable del fabricante para su migración (ACS fue hasta el 2015 y ahora proponen el ISE que está en evaluación por Global Networks). Mientras tanto se tiene alta disponibilidad para garantizar la continuidad de servicio.
3. Se solicitará a la casa matriz la evaluación del upgrade de los OS observados y en base a ello se realizará el despliegue, dado que no se reciben instrucciones desde Febrero 2015.

Acciones Específicas / Evidencia requerida para el Cierre de la Observación

1. Evidencia del reemplazo de los switches sin soporte.
2. Renovación del software CISCO Secure a una versión con soporte.
3. Evidencia de upgrade de sistemas operativos en los dispositivos de redes.

Fecha Esperada de Solución de la Gerencia:

1. Q4-2018
2. Q3-2018
3. Q3-2018

Fecha Esperada de Solución de Auditoría:

1. Q4-2018
2. Q3-2018
3. Q3-2018

OBSERVACIÓN DE AUDITORÍA #5

Nombre de la Auditoría	Gestión y Seguridad de Redes SBP, CSF y SCI
Título de la Observación	Monitoreo de la capacidad y desempeño
Nivel de Riesgo (Unidad/Proceso)	Moderado
Nivel de Riesgo (País/Subsidiaria)	Bajo
Nivel de Riesgo (Scotiabank)	Bajo

Observación(es)

1. Si bien existe un monitoreo 24x7 sobre la performance y disponibilidad de los dispositivos de redes en los Data Centers, routers de agencias y enlaces críticos, observamos 855 switches (principalmente en Sedes, Agencias y Retailers), no configurados/incluidos en el software especializado de monitoreo.
2. No existe un proceso formal para la proyección periódica de la capacidad y crecimiento del uso de recursos de redes de comunicaciones (ancho de banda, memoria, procesador).

Implicación / Riesgo

Riesgo Operacional / Tecnológico

- Indisponibilidad prolongada de comunicaciones por fallas en dispositivos de redes no detectadas oportunamente.
- Falta de capacidad en los recursos debido a incrementos no contemplados.

Causa(s) Raíz

Fallas en el diseño del control.

Falta de un adecuado diseño de políticas y procesos.

Recomendación(es)

Gerencia de CREO Perú - Infraestructura:

1. Registrar en el software de monitoreo los dispositivos de redes observados.
2. Implementar un procedimiento de conciliación periódica entre los dispositivos de redes en producción contra los registrados en la herramienta de monitoreo, de modo que se asegure el monitoreo de los todos los dispositivos.
3. Definir e implementar un proceso formal y sostenible para analizar la información sobre el uso de recursos en la infraestructura de comunicaciones, pronosticar su crecimiento y generar un informe periódico sobre el rendimiento y la capacidad de la infraestructura de comunicaciones.

Plan de Acción de la Gerencia

1. Se registrará en la herramienta de monitoreo todos los switches de las Sedes de SBP, CSF y SCI. En el caso de las agencias y retailers, se monitorea la disponibilidad de equipos críticos a nivel de LAN de los routers, no obstante se incluirán los switches intermedios dependiendo de su criticidad e impacto en la operativa diaria.
2. Se implementará un procedimiento semestral de conciliación periódica entre los equipos instalados en producción contra lo registrado en el software de monitoreo.
3. Se elaborará un informe de capacidad mensual y forecasting semestral de las redes de SBP, CSF y SCI incluyendo los enlaces de comunicaciones.

Acciones Específicas / Evidencia requerida para el Cierre de la Observación

1. Reporte de dispositivos de redes observados registrados en el software de monitoreo.
2. Evidencia de conciliación de dispositivos en inventario contra aquellos registrados en el software de monitoreo.
3. Informe sobre el rendimiento y pronóstico de la capacidad de las redes de comunicaciones.

Fecha Esperada de Solución de la Gerencia:

1, 2 y 3. Q2-2018

Fecha Esperada de Solución de Auditoría:

1, 2 y 3. Q3-2018

OBSERVACIÓN DE AUDITORÍA #6

Nombre de la Auditoría	Gestión y Seguridad de Redes SBP, CSF y SCI
Título de la Observación	Contratos con terceros
Nivel de Riesgo (Unidad/Proceso)	Moderado
Nivel de Riesgo (País/Subsidiaria)	Bajo
Nivel de Riesgo (Scotiabank)	Bajo

Observación(es)

No existen contratos vigentes para los siguientes servicios:

1. Servicio de enlace de datos. (Telefónica del Perú)
2. Soporte a la infraestructura Cisco. (Logicalis)
3. Servicio de redes inalámbricas guest (wifi) en agencias.

Esta situación no permite ejercer legalmente derechos contractuales en aspectos como: confidencialidad de la información, continuidad de servicios, cláusulas de riesgo operacional, solución de controversias y/o niveles de servicio.

Implicación / Riesgo

Riesgo Operacional / Tecnológico

- Entrega de servicios no acorde a los requerimientos acordados.
- Indisponibilidad en los servicios debido a fallas no atendidas.

Causa(s) Raíz

- No se ha gestionado o culminado la renovación de los contratos.

Recomendación(es)

Gerencia de CREO Perú - Infraestructura:

Gestionar la firma de los contratos con los proveedores de servicios de comunicación y soporte con las cláusulas estándares del grupo.

Plan de Acción de la Gerencia

- 1 y 3. Los contratos de servicios de enlace de datos y redes inalámbricas están en proceso de renovación.
2. En coordinación con la Unidad de Contratos se elaborará el contrato de soporte con Logicalis.

Acciones Específicas / Evidencia requerida para el Cierre de la Observación

Contratos refrendados con los proveedores de servicios de comunicación y soporte identificados.

Fecha Esperada de Solución de la Gerencia:

1, 2 y 3. Q2-2018

Fecha Esperada de Solución de Auditoría

1, 2 y 3. Q2-2018

OBSERVACIÓN DE AUDITORÍA # 7

Nombre de la Auditoría	Gestión y Seguridad de Redes SBP, CSF y SCI
Título de la Observación	Copias de respaldo de eventos de seguridad y configuración
Nivel de Riesgo (Unidad/Proceso)	Moderado
Nivel de Riesgo (País/Subsidiaria)	Bajo
Nivel de Riesgo (Scotiabank)	Bajo

Observación(es)

En los procesos de respaldo de logs de seguridad y configuración de los dispositivos de red observamos lo siguiente:

1. No se respaldan los logs almacenados en los servidores TACACS, los cuales registran los eventos de seguridad y cambios en la configuración de los dispositivos de redes.
2. La configuración de 20 dispositivos de redes (50% de una muestra de 40), 1 firewall y 19 switches no ha sido respaldada durante el 2017. Asimismo el procedimiento de respaldo no define los dispositivos a ser respaldados, frecuencia y periodo de retención, así como los controles para su cumplimiento.

Implicación / Riesgo

1. Pérdida de información sobre eventos ocurridos en la infraestructura de red. Por ejemplo, para la detección e investigación de incidentes de seguridad.
2. Retraso en la recuperación de los dispositivos de red que no mantienen un adecuado proceso de respaldo.

Causa(s) Raíz

Fallas en el diseño / ejecución del control

Recomendación(es)

Gerencia de CREO Perú - Infraestructura:

1. Implementar el respaldo periódico de los log registrados en los servidores TACACS.
2. Elaborar un procedimiento de respaldo de la configuración de los dispositivos de red, que incluya la definición del alcance de los equipos considerados en el proceso, frecuencia, periodos de retención y controles en el proceso.

Plan de Acción de la Gerencia

1. Se implementará el respaldo periódico de los logs de eventos de los servidores TACACS y sobre la configuración de los equipos de redes observados.
2. Se implementará un procedimiento formal de backup que defina el alcance de dispositivos a respaldar, frecuencia y controles para su cumplimiento.

Acciones Específicas / Evidencia requerida para el Cierre de la Observación

1. Evidencia de copias de respaldo de los logs TACACS y configuración de equipos observados.
2. Procedimiento aprobado de copias de respaldo y retención de los dispositivos de redes.

Fecha Esperada de Solución de la Gerencia:

1, 2. Q2-2018

Fecha Esperada de Solución de Auditoría:

1, 2. Q3-2018