




INFORME DE AUDITORIA INTERNA

A-A-03/2018

Nombre del Informe	Administración y Seguridad de Redes de Scotiabank Perú, Crediscotia 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

RESUMEN EJECUTIVO

ANTECEDENTES


La infraestructura de la red permite la conectividad de los Data Centres, aplicaciones, servidores, dispositivos de seguridad y storage de Scotiabank Perú y subsidiarias. La infraestructura de red es clave para soportar los servicios de comunicaciones, como resultado, se requieren controles adecuados que aseguren la seguridad y operación de los servicios.

La Unidad de CREO Perú - Infraestructura es responsable del soporte de la infraestructura de comunicaciones, así como asegurar la disponibilidad y continuidad operativa de las redes. Asimismo, la Unidad de Seguridad y Control de información (IS&C Perú) proporciona funciones de seguridad y supervisión de riesgos, monitoreo de vulnerabilidades y aprobaciones de cambios en la infraestructura de redes.

OBJETIVO

El objetivo de esta auditoría fue emitir una opinión independiente sobre el diseño y efectividad operativa de los controles internos establecidos en la gestión y seguridad de las redes de Scotiabank Perú, CrediScotia Financiera y SCI.

CONCLUSION

En nuestra opinión, el diseño y efectividad operativa de los controles internos en los procesos de gestión y seguridad de la red de SBP, CSF y SCI son satisfactorios. 

Nuestra calificación está basada en lo siguiente:

- La estructura organizacional permite una adecuada segregación de las funciones en la administración y seguridad de las redes, el personal se encuentra capacitado y tiene conocimiento de sus responsabilidades.
- El diseño y arquitectura de la red está alineada con los estándares de BNS, asegurando una apropiada seguridad y continuidad de las comunicaciones.
- El control de inventario y borrado de datos de los dispositivos de redes es satisfactorio.
- Los cambios en infraestructura de redes son aprobados por un comité local y de ser el caso, por otro regional.
- La configuración de las reglas de los firewalls es apropiada y las vulnerabilidades identificadas en los dispositivos de redes son corregidas. Se utilizan herramientas de escaneo corporativas como el IP360 y se efectúan pruebas de penetración externas e interna (pentesting).
- El control de acceso en los dispositivos de redes está centralizado en servidores especializados de autenticación (TACACS¹).
- La capacidad y disponibilidad de la red es adecuada para soportar la operación transaccional de SBP, CSF y SCI. Asimismo, el software de monitoreo está configurado

¹ TACACS (Terminal Access Controller Access Control System) es un protocolo de autenticación que permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red.















para alertar eventos críticos de disponibilidad y desempeño de la red. Por otro lado, los incidentes en la red son analizados, priorizados y resueltos oportunamente.










- El acceso remoto VPN y las redes inalámbricas (WLAN) con conexión a la red interna se encuentran adecuadamente configurados y con accesos restringidos.
- Los equipos y enlaces de comunicaciones se encuentran implementados con un esquema de redundancia, lo que permite la alta disponibilidad de los servicios de datos en los centros de datos, sedes y agencias.
- El acceso físico y controles ambientales en las salas de los equipos de comunicaciones en los Centros de Datos Principal y Secundario, así como en las agencias principales, son apropiados.
- Existe una supervisión local y regional de la gestión y seguridad de la red.

A pesar de lo anterior, identificamos las siguientes debilidades de control:

- La configuración de algunos dispositivos de redes no está alineada con algunos estándares de seguridad. Asimismo, existen dispositivos que no se escanean con la herramienta corporativa IP360.
- Si bien el acceso a dispositivos de redes está restringido a personal de soporte, las cuentas privilegiadas no son custodiadas en el sistema firecall (Xceedium). Asimismo, el proceso de otorgamiento de accesos es administrado por la Unidad de Soporte de TI sin intervención de IS&C.
- Si bien los cambios en las reglas de los firewalls son autorizados, éstos no son verificados en forma posterior a fin de asegurar que sólo se efectuaron los cambios autorizados.

ALCANCE Y RESUMEN DE CALIFICACIONES

Alcance de Auditoría	Calificación Control Interno		Referencia a Observaciones de Auditoría
	Auditoría Actual Q1/2018	Auditoría Previa N/A*	
Calificación Total		N/A	
Ambiente de Control		N/A	
Estructura organizacional / roles y responsabilidades		N/A	
Estrategia y planes		N/A	
Políticas y procedimientos		N/A	
Cumplimiento Regulatorio		N/A	
Evaluación de riesgos de TI		N/A	
Actividades de Control		N/A	
Diseño y arquitectura de la red		N/A	
Obsolescencia – hardware y software		N/A	Observación # 4: Obsolescencia y upgrade de software y hardware
Gestión de activos		N/A	
Control de cambios		N/A	Observación # 3: Control de cambios
Gestión de configuración de seguridad y vulnerabilidades		N/A	Observación # 1: Configuración de seguridad y gestión de vulnerabilidades
Administración de accesos privilegiados		N/A	Observación # 2: Acceso lógico

Seguridad física y controles ambientales (Dispositivos de comunicaciones)		N/A	
WLAN (WI_FI)		N/A	
Acceso Remoto VPN		N/A	
Disponibilidad, rendimiento y gestión de la capacidad		N/A	Observación # 5: Monitoreo de la capacidad y desempeño
Respaldo, retención y rotación		N/A	Observación # 7: Copias de respaldo de eventos de seguridad y configuración
Continuidad y recuperación de desastres		N/A	
Gestión de terceros		N/A	Observación # 6: Gestión de terceros
Informes de gestión y reportes ejecutivos		N/A	
Supervisión de la Gerencia		N/A	

El periodo cubierto por la auditoría fue de octubre 2016 a octubre 2017.

Exclusiones al Alcance: Se excluyeron los procesos de administración de antivirus y web/mail filter, los cuales serán revisados en la próxima auditoría de Controles Generales de TI Grupo SBP en Q3-2018.

Ismael Mendoza,
Senior Audit Manager
Scotiabank Perú

Marcial Figueroa
IT Audit Director
Scotiabank Perú

Elbia Castillo
Vice President &
Auditor General
Scotiabank Perú

RESUMEN DE OBSERVACIONES

#	Descripción de la Observación	Nivel de Riesgo ²	Grupo Responsable del Cierre de la Observación	Fecha Esperada de Solución - Gerencia	Fecha Esperada de Solución - Auditoría	Acciones Específicas / Evidencia Requerida para el Cierre de la Observación
1	Configuración de seguridad y gestión de vulnerabilidades En promedio, 10% del total de parámetros de los 47 dispositivos de redes seleccionados como muestra evaluada, no están configurados de acuerdo a lo recomendado por el fabricante o lo establecido en los checklist de configuración y aproximadamente el 4% del total de dispositivos presentan un score de riesgo moderado/alto según el IP360. Asimismo 289 dispositivos de red (22% del total) no son escaneados (identificado por la Gerencia) y no existe una certificación periódica del hardening de seguridad.	Alto/ Moderado/ Bajo	Information Security and Control (Information Systems, Technology & Solutions)	Q3-2018	Q4-2018	<ul style="list-style-type: none"> Evidencia de los ajustes en la configuración de los dispositivos de redes observados. Checklists de aseguramiento por tecnología de firewalls, switches, routers aprobados. Evidencia de hardening sobre una muestra de altas de dispositivos de redes. Evidencia de la certificación del hardening sobre todo el stock de dispositivos de redes. Reporte IP360 con score compliant sobre los dispositivos de redes.
2	Acceso lógico Si bien el acceso a dispositivos de redes está restringido a personal de soporte, las cuentas privilegiadas no son custodiadas en el sistema firecall (Xceedium). Asimismo, no existe segregación de funciones en el otorgamiento de accesos en los	Moderado/ Moderado/ Bajo	Information Security and Control (Information Systems, Technology & Solutions)	Q3-2018	Q4-2018	<ul style="list-style-type: none"> Evidencia de la custodia de las cuentas privilegiadas en el software firecall. Evidencia de flujo de aprobación de accesos en dispositivos de redes. Certificación de accesos en el software CISCO ACS y cuentas locales en dispositivos de redes.

² Alto, Moderado, Bajo o No Aplica (NA). Las observaciones de Auditoría son reportadas como alto, moderado, bajo o NA basado en el juicio profesional del auditor y teniendo en cuenta la naturaleza, el alcance y el impacto de la observación. Las observaciones de auditoría se evalúan en el contexto de la unidad / proceso auditado, el país / subsidiaria (si es aplicable) y a nivel de Todo el Banco (Scotiabank).

#	Descripción de la Observación	Nivel de Riesgo ²	Grupo Responsable del Cierre de la Observación	Fecha Esperada de Solución - Gerencia	Fecha Esperada de Solución - Auditoría	Acciones Específicas / Evidencia Requerida para el Cierre de la Observación
	dispositivos de redes, ni tampoco una certificación periódica.					
3	Control de cambios Si bien los cambios a la reglas de los firewalls son autorizados, éstos no son verificados de manera posterior a fin de asegurar que sólo se efectuaron los cambios autorizados. Asimismo, los procedimientos de control de cambios de reglas de acceso de firewalls e infraestructura no están actualizados.	Moderado/ Bajo/ Bajo	Information Security and Control (Information Systems, Technology & Solutions)	Q2-2018	Q3-2018	<ul style="list-style-type: none"> Evidencia de una muestra de verificaciones de FPR (Firewall Port Request) sobre cambios registrados en los logs. Procedimiento de control de cambios de reglas de firewalls e infraestructura actualizado y aprobado.
4	Obsolescencia y upgrade de software y hardware 10 switches localizados en el Centro de Datos Principal no cuentan con soporte del fabricante (identificado por la Gerencia). Asimismo, la versión del software de administración de accesos de dispositivos de redes ya no es soportada. Por otro lado, los sistemas operativos de 14 firewalls y 158 switches no están actualizados.	Moderado/ Bajo/ Bajo	CREO Peru – Infraestructura (Infrastructure & Systems Latam)	Q4-2018	Q4-2018	<ul style="list-style-type: none"> Evidencia del reemplazo de los switches sin soporte. Renovación del software CISCO Secure a una versión con soporte. Evidencia de upgrade de sistemas operativos en los dispositivos de redes.
5	Monitoreo de la capacidad y desempeño Switches no críticos (principalmente en Sedes y Agencias) no se han considerado en el proceso de monitoreo en línea establecido. Asimismo, no existe un proceso formal para la proyección periódica de	Moderado/ Bajo/ Bajo	CREO Peru – Infraestructura (Infrastructure & Systems Latam)	Q2-2018	Q3-2018	<ul style="list-style-type: none"> Reporte de dispositivos de redes observados registrados en el software de monitoreo. Evidencia de conciliación de dispositivos en inventario contra aquellos registrados en el software de monitoreo. Informe sobre el rendimiento y

#	Descripción de la Observación	Nivel de Riesgo ²	Grupo Responsable del Cierre de la Observación	Fecha Esperada de Solución - Gerencia	Fecha Esperada de Solución - Auditoría	Acciones Específicas / Evidencia Requerida para el Cierre de la Observación
	la capacidad y crecimiento del uso de recursos de redes.					pronóstico de la capacidad de las redes de comunicaciones.
6	Gestión de terceros No se han formalizado/renovado contratos para los servicios de enlaces de datos (Telefónica del Perú) y soporte de la infraestructura Cisco (Logicallis).	Moderado/ Bajo/ Bajo	CREO Peru – Infraestructura (Infrastructure & Systems Latam)	Q2-2018	Q2-2018	<ul style="list-style-type: none"> Contratos refrendados con los proveedores de servicios de comunicaciones y soporte.
7	Copias de respaldo de eventos de seguridad y configuración Las bitácoras de auditoría en los servidores TACACS y las configuraciones de 20 dispositivos de redes, no tienen copias de respaldo.	Moderado/ Bajo/ Bajo	CREO Peru – Infraestructura (Infrastructure & Systems Latam)	Q2-2018	Q3-2018	<ul style="list-style-type: none"> Evidencia de copias de respaldo de los logs TACACS y la configuración de equipos observados. Procedimiento aprobado de copias de respaldo y retención de los dispositivos de redes.

OBSERVACIONES DE AUDITORÍA ABIERTAS

#	Descripción de la Observación	Grupo Responsable	Fecha Esperada de Solución
1	Ninguna		

OBSERVACIONES REGULATORIAS ABIERTAS

#	Descripción de la Observación	Regulador	Grupo Responsable	Fecha Esperada de Solución - Gerencia
	Ninguna			

PERFIL DEL NEGOCIO

Una red informática o red de datos permite que las computadoras personales, teléfonos, servidores, aplicaciones, impresoras y dispositivos intercambien información, incluso si no tienen una conexión directa entre ellos. Los siguientes dispositivos y aplicaciones soportan la conectividad con la red:

- Firewall: Es un dispositivo de red que controla la seguridad de la red y las reglas de acceso. Actualmente están operando firewalls Juniper y CISCO en alta disponibilidad, tanto en el perímetro, subsidiarias y extranet con proveedores.
- Switch: Es un dispositivo de red de computadora que conecta dispositivos en una red de computadora mediante el uso de conmutación de paquetes para recibir, procesar y reenviar datos al dispositivo de destino. Principalmente del fabricante CISCO.
- Router: Es un dispositivo electrónico que une varias redes de computadoras a través de conexiones alámbricas o inalámbricas. Los routers son administrados por Telefónica del Perú y Claro.
- MPLS (Multiprotocol Label Switching): Es una red administrada por terceros que proporciona conectividad de área amplia para vincular las redes de área local con las redes de agencias y retailers a nivel nacional, la casa matriz y subsidiarias a nivel internacional. Las redes MPLS contratadas por Scotiabank Perú son administradas por Telefónica del Perú y Claro.

Scotiabank Perú ha implementado una estructura de red redundante con una topología de anillo que mantiene la red en funcionamiento en caso de fallas en el funcionamiento de uno de los nodos. Los equipos de comunicaciones que soportan los enlaces de datos de la plataforma core principal y alterna están alojados en dos salas de comunicaciones: una en el Centro de Datos Principal ubicado en el San Isidro (Sede Derteano) y otra en el Centro de Datos Secundario ubicado en La Molina, subcontratado con el proveedor IBM.

Actualmente, Scotiabank Perú está trabajando en la consolidación de los centros de datos en México (Q2-2018) con la finalidad de mejorar la eficiencia operativa, la disponibilidad y el rendimiento de los sistemas.

ESTRUCTURA ORGANIZACIONAL

Las unidades de Seguridad y Control de la Información (IS&C Perú) y la Unidad de CREO Perú - Infraestructura. IS&C Perú son las encargadas de la seguridad y gestión de las redes de Scotiabank Perú. IS&C Perú reporta a la VP de Sistemas y CREO-Perú Infraestructura reporta a la VP de Infraestructura LATAM.

La Unidad de IS&C Perú brinda los servicios de administrar el acceso lógico en las plataformas de cómputo, el control de cambios en las aplicaciones e infraestructura del Grupo SBP, la aprobación de las reglas de acceso en los firewalls y el monitoreo de los niveles de seguridad de la información en la infraestructura y procesos de cómputo del Grupo Scotiabank Perú.

Por otro lado, la Unidad de CREO Perú Infraestructura es la encargada de mantener la conectividad de las agencias y oficinas administrativas, proveedores y entes reguladores, la conexión con entes financieros externos, como VISA, Banred, las redes de ATM'S, canales alternos de uso de clientes, así como con subsidiarias del Grupo Scotiabank.

LEYES Y REGULACIONES

- Ley general del Sistema Financiero y del Sistema de Seguros y orgánica de la Superintendencia de Banca y Seguros.
- Ley de Protección de Datos Personales.
- Reglamento de la Gestión Integral de Riesgos.
- Reglamento de Tarjetas de Crédito y Débito.
- Circular N° G-164-2012 Reporte de eventos de interrupción significativa de operaciones.
- Circular N° G- 139-2009 Gestión de la continuidad del negocio.
- Circular N° G-140-2009 Gestión de la seguridad de la información
- Medidas mínimas de seguridad para las entidades del sistema financiero.

SISTEMAS DE SOPORTE

- **PRTG**: gestión de estado de enlaces y consumo de equipos de comunicación y seguridad.
- **Cisco ACS**: seguridad de acceso a los equipos de seguridad.
- **Cisco Prime**: monitoreo y backup de equipos de comunicaciones Cisco.
- **IP360**: monitoreo de vulnerabilidades en los dispositivos de redes.

DEFINICIONES DE LA CALIFICACIÓN DE AUDITORÍA

Se utiliza una estructura de calificación de dos partes, para comunicar la opinión de Auditoría sobre los controles internos. El primer componente representa la evaluación de la *condición* de los controles al momento de la auditoría y el ‘Símbolo’ refleja la evaluación de la *dirección* de los controles internos. Las calificaciones son evaluadas al nivel de proceso/unidad que está siendo auditada.

Calificación	Símbolo	Calificación y Dirección	Descripción
Satisfactorio (S) El diseño y la operación de los controles internos son satisfactorios para administrar el riesgo. Sin embargo, se pueden haber identificado deficiencias de control interno de menor importancia.		Satisfactorio – Estable	La Gerencia tiene la intención y la capacidad de solucionar las observaciones de auditoría en un <i>tiempo razonable</i> ³ .
		Satisfactorio – Deteriorando	La Gerencia no ha identificado ni solucionado activamente las deficiencias de control interno y/o las observaciones de auditoría no han sido aceptadas o no se espera que sean corregidas en un <i>tiempo razonable</i> . Como consecuencia, se espera que los controles internos se deterioren.
Requiere Mejorar (RM) El diseño y/u operación de los controles internos requiere mejorar para administrar el riesgo.		Requiere Mejorar – Solución Oportuna	Las observaciones de la auditoría han sido, ya sea, identificadas por la propia Gerencia o han sido aceptadas por ésta. Se espera que las observaciones sean solucionadas en un <i>tiempo razonable</i> o que sean implementados controles compensatorios.
		Requiere Mejorar – Estable	Se espera que la Gerencia implemente nuestras recomendaciones, aun cuando existe alguna incertidumbre si los cambios puedan ser realizados en un <i>tiempo razonable</i> . Las observaciones previamente identificadas como solucionadas por la Gerencia, pueden haber sido identificadas nuevamente o permanecen abiertas.
		Requiere Mejorar – Deteriorando	La Gerencia no ha identificado ni solucionado activamente las deficiencias de control interno y/o las observaciones de auditoría no han sido aceptadas o no se espera que sean corregidas en un <i>tiempo razonable</i> . Como consecuencia, se espera que los controles internos se deterioren.
Insatisfactorio (I) El diseño y/u operación de los controles internos son insatisfactorios para administrar el riesgo, debido a la identificación de debilidades de control significativas que podrían tener un impacto material en el proceso/negocio.		Insatisfactorio – Solución Oportuna	Las observaciones de la auditoría han sido, ya sea, identificadas por la propia Gerencia o han sido aceptadas por ésta. Se espera que las observaciones sean solucionadas en un <i>tiempo razonable</i> o que sean implementados controles compensatorios.
		Insatisfactorio – Estable	Se espera que la Gerencia implemente nuestras recomendaciones, aun cuando existe alguna incertidumbre si los cambios puedan ser realizados en un <i>tiempo razonable</i> . Las observaciones previamente identificadas como solucionadas por la Gerencia, pueden haber sido identificadas nuevamente o permanecen abiertas.
		Insatisfactorio – Deteriorando	La Gerencia no ha identificado ni solucionado activamente las deficiencias de control interno y/o las observaciones de auditoría no han sido aceptadas o no se espera que sean corregidas en un <i>tiempo razonable</i> . Como consecuencia, se espera que los controles internos se deterioren.

³ Esto significa que la Gerencia solucionará la Observación dentro de 2 trimestres. Esto excluye el tiempo de pruebas de auditoría.

LISTA DE DISTRIBUCIÓN

Áreas Auditadas

Carrillo, Roberto - VP Infraestructura y Sistemas LATAM
Castro, Frankie - Gerente Principal Seguridad Informática
Landauro, Manuel - Director Global Security Services LATAM
McMillan, Phil - VP, Global Networks
Tortolini, Carlos - VP Tecnología De Información y Soluciones
Zamalloa, Giovanni - Peru Country Delivery Manager Director

Para Información

Battiato, Gaston - SVP, International Technology Systems
Cirinna, Samantha - VP, Global Security Operations Services
Deschamps, Ignacio - Group Head, International Banking & Digital Transformation
Hawkins, Steve - SVP, Global Technology Services & CISO
Lloyd, Heather - SVP, Office of the Chief Information Officer
Simpson, Barbara - VP & Head, International Operations
Viola, Ernesto - SVP & Chief Financial Officer, International Banking
Zerbs, Michael - Chief Technology Officer
International Offices Administration
Global Operational Risk
ITS Audit