Banco Hipotecario de la Vivienda

# Informe Final TI-HW-001-2018

## AUDITORÍA SOBRE LA ADMINISTRACIÓN DE LA RED DE DATOS INSTITUCIONAL

07/06/2018

# INDICE

## A. RESUMEN EJECUTIVO

*En esta auditoria se evaluaron los principales controles referentes a la administración de la red de datos institucional y sus componentes, valorando desde la parte documental hasta procesos operativos específicos de telecomunicaciones.*

*Al efectuar una revisión sobre la normativa interna del Departamento de TI que tenía relación directa con los servicios de red y sus componentes, se determinó la presencia de normativa vigente que se encontraban descontinuada y desactualizada.*

*Cuando se valoró el estado del cable de red ubicado en el rack de comunicaciones principal y el los ductos de cada piso, se localizó cierta cantidad de cables sin etiquetas ni certificación alguna. Además no se controla adecuadamente el acceso a tales ductos.*

*A nivel de inventarios de equipos de comunicación se revisó su ubicación y existencia según el detalle que es administrado por el área de Proveeduría, localizando equipos fuera de inventario, sin placas de activos o sin una ubicación precisa.*

*Relacionado con el mantenimiento y soporte de los equipos de comunicación, se encontró una debilidad con relación al seguimiento de la misma y ciertos controles que deberían existir para tener una mejora administración de los mismos.*

*Como parte de las pruebas de red ejecutadas, se ingresó de forma remota a las cuentas de correo de algunos funcionarios de la Auditoría Interna utilizando la plataforma Web del Banco, dando como resultado la posibilidad de bloquear cuentas de usuario al ingresar passwords incorrectos.*

*Para finalizar, se pudo determinar que no se realizan desde hace algunos años estudios de vulnerabilidad interna o externa sobre la red de datos institucional.*

*Los detalles de cada aspecto indicado en los párrafos anteriores, son ampliados a lo largo de este documento.*

# BANCO HIPOTECARIO DE LA VIVIENDA
# AUDITORÍA INTERNA

**Informe Final Nº TI-HW-001-2018**
**07 de Junio del 2018**

## AUDITORÍA SOBRE LA ADMINISTRACIÓN DE LA RED DE DATOS INSTITUCIONAL

## 1. INTRODUCCIÓN

### *1.1 Justificación de la auditoría*

Este estudio forma parte del Plan Anual de Trabajo de esta Auditoría Interna para el año 2018 y está fundamentado en el Artículo 31 de la Ley 7052 del Sistema Financiero Nacional para la Vivienda, en el Artículo 22 de la Ley 8292, Ley General de Control Interno, en los cuales se establece que la Auditoría Interna deberá velar y fiscalizar el uso adecuado de los recursos del BANHVI.

### *1.2 Objetivo*

Evaluar los controles existentes para administrar los servicios y la seguridad de la Red de Datos Institucional.

### *1.3 Alcance*

El estudio abarcó la documentación, información y procesos operativos vigentes al 31 de Marzo del 2018 relacionados con los controles sobre la red de datos del Banco.

### *1.4 Metodología de Trabajo*

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

- ✓ Reglamento SUGEF 14-17 – COBIT 5
- ✓ Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).
- ✓ Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE).
- ✓ Normas Generales de Auditoria para el Sector Publico
- ✓ Manual para el ejercicio de la práctica de la Auditoria Interna.
- ✓ Norma 308 Comunicación de resultados
- ✓ ISO-IEC-27002:2016 Tecnologías de la información Técnicas de seguridad – Códigos de buenas prácticas para controles de seguridad de la información

Además, se aplicaron técnicas de auditoría comúnmente aceptadas como entrevistas, revisión documental de la gestión administrativa y visitas de campo para la verificación del control interno.

Específicamente se ejecutaron entrevistas con ciertos funcionarios del área de Soporte Técnico del Departamento de TI, encargados de velar por la administración y la implementación de controles de la red de datos del Banco.

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

# 2. RESULTADOS DE LA EVALUACIÓN

## 2.1 Normativa sobre la Red Institucional

Al evaluar la normativa relacionada con el mantenimiento y control de la red de datos institucional, se localizaron ciertos procedimientos vigentes que se encuentran desactualizados o descontinuados, con fechas de creación entre el año 2013 y 2014. Se detallan seguidamente los documentos en cuestión:

- P-DTI-HRC-005 Administración de la Central Telefónica
- P-DTI- HRC-008 Revisión y pruebas de funcionamiento de Equipos de comunicación adquiridos
- P-DTI-HRC-016 Administración de la conectividad de red

Las Normas de Control Interno para el Sector Público de la Contraloría General de la República N-2-2009-CO-DFOE, detallan el en artículo 4, inciso c) lo siguiente:

> "***1.4 Responsabilidad del jerarca y los titulares subordinados sobre el SCI***
> *c. La emisión de instrucciones a fin de que las políticas, normas y procedimientos para el cumplimiento del SCI, estén debidamente documentados, oficializados y actualizados, y sean divulgados y puestos a disposición para su consulta."*

Además en el artículo 15 de la ley de Control Interno 8292, se detalla el siguiente enunciado:

> *"Artículo 15.—**Actividades de control**. Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*
>
> *a) Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones."*

El motivo por el que varios de los documentos evaluados se encontraban desactualizados, se debe a que por ser un tema que requiere de un especialista, la actividad debía ser ejecutada por el ex funcionario encargado de las telecomunicaciones, pero la misma no se ejecutó y no se le brindó el seguimiento correspondiente.

Como efectos de contar con la normativa actualizada, se crea dependencia del personal que sabe ejecutar las tareas sin utilizar el procedimiento, ampliando la posibilidad de omitir actividades específicas o controles operativos importantes para el correcto funcionamiento de la red de datos institucional.

## 2.2 Cableado y ductos de Red

En el proceso de auditoría, al evaluar el etiquetado del cableado de red que se localiza en el rack principal de comunicaciones ubicado en la sala de servidores, así como en los ductos de comunicación de cada uno de los siete pisos del Banco; se localizaron cables de datos que no se encuentran etiquetados ni certificados según el estándar implementado en la Institución.

Según los puntos 4, 5, 6 y 7 del procedimiento P-DTI-HRC-017 denominado "*Nuevas conexiones de Red*", se indica lo siguiente con relación a estos temas:

> *"4- Instala cables certificados que van desde el módulo de pared hasta el PC y el que va al Patch Panel y luego al puerto del Switch.*
>
> *5- Etiqueta el cable que va del Patch Panel al Switch con el código Internacional ya definido.*
>
> *6- Certifica la conexión, si corresponde, y la verifica*
>
> *7- Ejecuta el Procedimiento "Control del Inventario de Componentes de Red" y actualiza la Documentación de la Red en la siguiente dirección: G\Inf_inst_unidad\Dpto.Tecnologia de informacion\controles\area soporte\configuración\componentes de red\documentacion de la red de datos"*

De igual forma sobre este tema, en los puntos 2 y 3 del procedimiento P-DTI-HRC-019 que trata sobre la revisión del cableado y componentes de red, indica que una empresa certificada junto al ingeniero de soporte interno, serían los responsables de las siguientes actividades:

> *"2- Revisa y si fuera del caso, corrige la disposición de los cables.*
> *3- Revisa y si fuera del caso, corrige el estado de los componentes de la red."*

Referente a los ductos ubicados en cada uno de los pisos donde se encuentran los Switch de comunicación para cada área y que son administrados por el soporte técnico de TI, encontramos que a pesar de que las puertas normalmente se mantienen cerradas, el área de mantenimiento del Banco también tiene llaves para realizar trabajos esporádicos en la parte eléctrica; lo cual incrementa el riesgo de desconexiones de puntos de red o apagados de equipos de comunicaciones.

En el punto 5 de la práctica de gestión DSS01.05 del COBIT 5, relacionada con el proceso DSS01 sobre la gestión de operaciones, se detalla lo siguiente:

> *"**DSS01.05 Gestionar las instalaciones**.*
> *Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.*
> *(…)*
>
> *5. Asegurar que el cableado y el pathching físico (datos y telefonía) están estructurados y organizados. Las estructuras de cableado y de conductos debieran estar documentadas (p.ej. plano del edificio y diagramas de cableado)."*

Como principal razón para que se presenten cables de red en el estado indicado, tanto en el rack de la sala de servidores como en los distintos ductos del Banco, se atribuye a que en la institución se han realizado varios reacomodos internos en diferentes departamentos a nivel de cubículos y oficinas, siendo necesario tirar nuevos cables de datos; actividad que ha sido ejecutada por personal de mantenimiento del Banco o por el encargado de redes (exfuncionario que dejó de laborar desde el 26 de Octubre del 2017), sin que se haya contado con la participación de alguna empresa externa certificada para dicho fin.

Como posibles consecuencias de estas situaciones se pueden presentar problemas de seguridad en la información que viaja a través de la red, conexiones que no funcionen adecuadamente, dificultades al momento de dar mantenimientos a equipos de comunicación, dependencia del personal que ejecutó la tarea, entre otros.

## 2.3 Inventario de Equipos de Comunicación

Como parte de la revisión se realizó un inventario sobre los principales equipos de comunicaciones que se ubican en la sala de servidores de datos y en cada uno de los ductos de cableado ubicado en cada piso. En el siguiente cuadro se muestra un resumen de lo encontrado, con su debido detalle en el campo de la observación:

| RESULTADO INVENTARIO EQUIPO COMUNICACIÓN | | | |
|---|---|---|---|
| **N° ACTIVO** | **EQUIPO** | **UBICACIÓN** | **OBSERVACIÓN** |
| NA | Cisco Catalyst 2960 | Sala Servidores | Sin Número de Activo |
| NA | Patch Panel 48 puertos R2-PP3 | Sala Servidores | Sin Número de Activo |
| NA | Cisco Switch Catalyst 2960-S 24 puertos | Ducto Segundo Piso | Sin Número de Activo |
| NA | Switch 8 puertos Encore | Ducto Séptimo Piso | Sin Número de Activo |
| NA | Cisco Power Inyector | En los ductos de cada piso | Sin Número de Activo |
| 25-5320 | Cisco Switch Catalyst 2960-X | Sala Servidores | Desecho o Localizar, pero está en uso (*) |
| 25-4665 | Patch Panel 48 puertos PP2 48 puertos | Ducto Cuarto Piso | Taller Bodega, pero está en uso |
| 25-4313 | Patch Panel 48 puertos PP2 24 puertos | Ducto Quinto Piso | Desecho o Localizar, pero está en uso (*) |
| 25-4311 | Patch Panel 48 puertos PP1 48 puertos | Sala Servidores | Desecho o Localizar, pero está en uso (*) |
| 25-5857-01 | Switch de seguridad FTX2140W007 | Sala Servidores | No se encuentra en el inventario |
| 25-5857-02 | Switch de seguridad FTX2140W00B | Sala Servidores | No se encuentra en el inventario |
| 25-5857-02 | Cisco UCS C220 M4 | Sala Servidores | No se encuentra en el inventario |
| 25-4137 | Switch digital de 8 puertos para servidores | Sala UPS | Se mantiene en Inventario, pero ya se desechó |
| (*) Significa que el activo según el detalle de inventario fue desechado o no se ha ubicado como corresponde | | | |

También referente a estos activos, al revisar la documentación sobre el "*control de inventario de los componentes de red*" administrada por el Departamento de TI, se localizó que la misma no se actualiza desde el año 2013; esto según los archivos remitidos a la Auditoría Interna y el punto 7 del procedimiento P-DTI-HRC-017 sobre las nuevas conexiones de Red, el cual detalla:

> *"Ejecuta el Procedimiento "Control del Inventario de Componentes de Red" y actualiza la Documentación de la Red en la siguiente dirección: G\Inf_inst_unidad\Dpto.Tecnologia de informacion\controles\area soporte\configuración\componentes de red\documentacion de la red de datos"*

El artículo 4.3 del manual de Normas de control interno para el Sector Público (N-2-2009-CO-DFOR), detalla lo siguiente con relación a la conservación del patrimonio:

> ***"4.3 Protección y conservación del patrimonio***
> *El jerarca y los titulares subordinados, según sus competencias, deben establecer, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente la protección, custodia, inventario, correcto uso y control de los activos pertenecientes a la institución, incluyendo los derechos de propiedad intelectual. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de tales*

*activos y los riesgos relevantes a los cuales puedan verse expuestos, así como los requisitos indicados en la norma 4.2."*

En la práctica de gestión BAI09.01 del proceso del COBIT 5 BAI09 relacionado con la gestión de activos, se indica lo siguiente:

*"**BAI09.01 Identificar y registrar los activos actuales**.*
*Mantener un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios y garantizar su alineación con la gestión de la configuración y la administración financiera."*

Como posibles causas de las situaciones detectadas relacionadas con el inventario de los equipos de comunicación, se tiene el limitado control ofrecido por el ex funcionario de telecomunicaciones, así como la falta de seguimiento del área de Proveeduría en lo que a etiquetado se refiere.

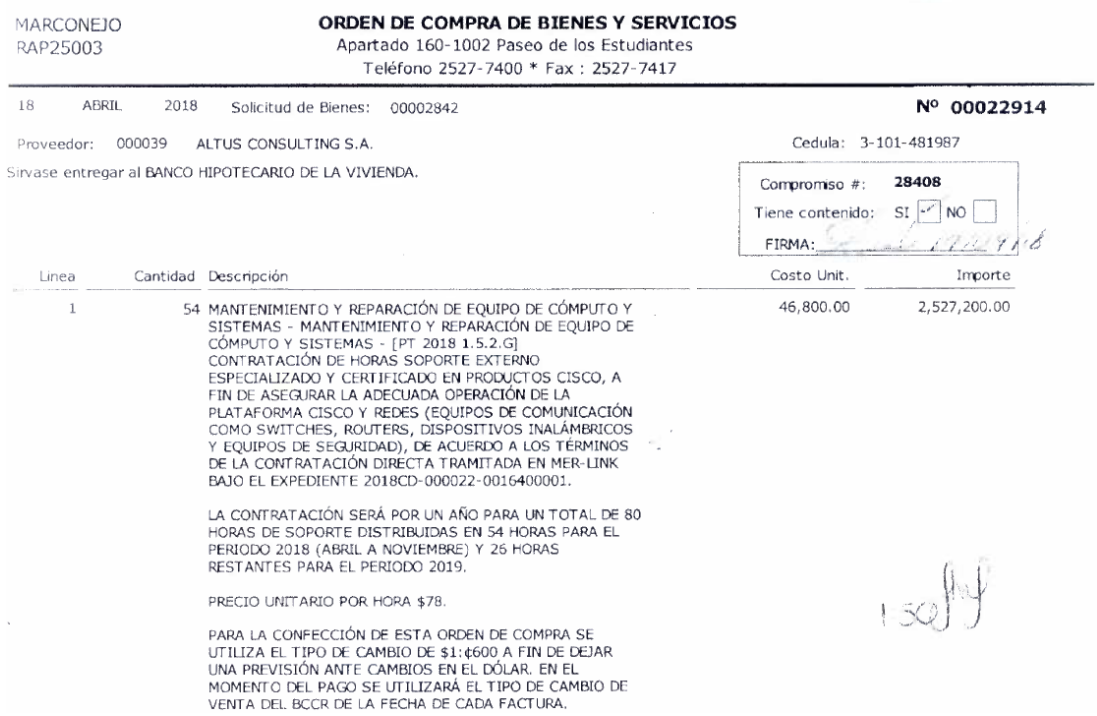
Se considera que dentro de las potenciales consecuencias de llevar un control de inventarios que no se apegue a la realidad de los equipos, están las posibles pérdidas económicas a nivel institucional, así como problemas de continuidad operativa al no poder ubicar algún equipo en una contingencia.

## 2.4 Mantenimiento sobre los Equipos de Comunicación

En el memorando DTI-ME-0019-2018 dirigido a la Gerencia General el 07 de febrero del 2018, el Departamento de TI solicita la aprobación del pago de soporte anual para la plataforma Cisco y los equipos de comunicación. Como parte de las condiciones técnicas detalladas en ese documento, se incluye una lista de 38 equipos de comunicación que deben ser parte del soporte anual; mismo que es aprobado por la Gerencia General según documento GG-ME-0115-2018 y que se logra completar según la orden de compra N°00022914. Se corroboró que el detalle de contratación y las condiciones generales y específicas fueron colocados debidamente en la página del SICOP (Sistema Integrado de Compras Públicas). Con respecto a este tema se encontraron las siguientes debilidades:

A) Al evaluar la lista de equipos detallada en dicho memorando versus el inventario de equipos facilitado por el área de Proveeduría, se determina que no se están incluyendo dentro de las horas de soporte todos los equipos de comunicaciones vigentes en el Banco.

   Se muestra seguidamente la orden de compra con la que canceló el mantenimiento actual de los equipos se comunicación:



MARCONEJO
RAP25003

**ORDEN DE COMPRA DE BIENES Y SERVICIOS**
Apartado 160-1002 Paseo de los Estudiantes
Teléfono 2527-7400 * Fax : 2527-7417

18 ABRIL 2018 Solicitud de Bienes: 00002842 **Nº 00022914**

Proveedor: 000039 ALTUS CONSULTING S.A. Cedula: 3-101-481987

Sirvase entregar al BANCO HIPOTECARIO DE LA VIVIENDA.

Compromiso #: 28408
Tiene contenido: SI [✓] NO [ ]
FIRMA:

| Linea | Cantidad | Descripción | Costo Unit. | Importe |
|---|---|---|---|---|
| 1 | 54 | MANTENIMIENTO Y REPARACIÓN DE EQUIPO DE CÓMPUTO Y SISTEMAS - MANTENIMIENTO Y REPARACIÓN DE EQUIPO DE CÓMPUTO Y SISTEMAS - [PT 2018 1.5.2.G] CONTRATACIÓN DE HORAS SOPORTE EXTERNO ESPECIALIZADO Y CERTIFICADO EN PRODUCTOS CISCO, A FIN DE ASEGURAR LA ADECUADA OPERACIÓN DE LA PLATAFORMA CISCO Y REDES (EQUIPOS DE COMUNICACIÓN COMO SWITCHES, ROUTERS, DISPOSITIVOS INALÁMBRICOS Y EQUIPOS DE SEGURIDAD), DE ACUERDO A LOS TÉRMINOS DE LA CONTRATACIÓN DIRECTA TRAMITADA EN MER-LINK BAJO EL EXPEDIENTE 2018CD-000022-0016400001.<br><br>LA CONTRATACIÓN SERÁ POR UN AÑO PARA UN TOTAL DE 80 HORAS DE SOPORTE DISTRIBUIDAS EN 54 HORAS PARA EL PERIODO 2018 (ABRIL A NOVIEMBRE) Y 26 HORAS RESTANTES PARA EL PERIODO 2019.<br><br>PRECIO UNITARIO POR HORA $78.<br><br>PARA LA CONFECCIÓN DE ESTA ORDEN DE COMPRA SE UTILIZA EL TIPO DE CAMBIO DE $1:¢600 A FIN DE DEJAR UNA PREVISIÓN ANTE CAMBIOS EN EL DÓLAR. EN EL MOMENTO DEL PAGO SE UTILIZARÁ EL TIPO DE CAMBIO DE VENTA DEL BCCR DE LA FECHA DE CADA FACTURA. | 46,800.00 | 2,527,200.00 |

B) Al revisar el detalle de los equipos que se incluyeron en el mantenimiento y soporte de acuerdo a la documentación remitida por el Departamento de TI en memorando DTI-ME-0019-2018; se localizó el Switch de Seguridad ASA5520-AIP10-K9 serie JMX0951K031, mismo que fue devuelto por el Departamento de TI al área de Proveeduría desde el 21 de febrero del 2018; esto por haberse cumplido su vida útil y por ende dejado de utilizar. Se presenta a continuación una sección de la lista de equipos donde se muestra el Switch indicado:

| N° | Dispositivo | Modelo | N° Serie |
|---|---|---|---|
| 1 | RUTEADOR DE SEGURIDAD | CISCO1841-SEC/K9 | FTX13088QHR |
| 2 | SWITCH ENLACES FIBRA | WS-C2960PD-8TT-L | FOC1321W36J |
| 3 | SWITCH ENLACE USUSARIOS | WS-C2960S-24TS-S | FOC1623Z4C2 |
| 4 | SWITCH ENLACE USUSARIOS | WS-C2960S-24TS-S | FOC1623Y24Y |
| 5 | SWITCH ENLACE USUSARIOS | WS-C2960S-24TS-S | FOC1623Z49N |
| 6 | SWITCH ENLACE USUSARIOS | WS-C2960S-24TS-S | FOC1623Z4DL |
| 7 | SWITCH ENLACE SERVIDORES | WS-C2960S-24TS-S | FOC1623W4LK |
| 8 | SWITCH ENLACE USUSARIOS | WS-C2960S-24TS-S | FOC1623Z4E2 |
| 9 | SWITCH ENLACE USUSARIOS | WS-C2960-24TS-S | FOC1623Z4CK |
| 10 | SWITCH ENLACE USUSARIOS | WS-C2960S-24TS-S | FOC1623Z4A3 |
| 11 | SWITCH ENLACE USUSARIOS | WS-C2960S-24TS-S | FOC1623W4PB |
| 12 | SWITCH ENLACE USUSARIOS | WS-C2960S-24TS-S | FOC1623W4LJ |
| 13 | SWITCH ENLACE USUSARIOS | WS-C2960S-24TS-S | FOC1623Z49S |
| 14 | SWITCH ENLACE USUSARIOS | WS-C2960S-24TS-S | FOC1623W3DP |
| 15 | SWITCH DE SEGURIDAD | ASA5520-AIP10-K9 | JMX0951K037 |
| 16 | MÓDULO IPS DE SEGURIDAD | ASA-SSM- AIP10-K9 | JAB095000BC |
| 17 | SWITCH DE SEGURIDAD | ASA5520-AIP10-K9 | JMX0951K031 |

C) Se detectó que el Sistema de Activos carece de cierta información necesaria para administrar correctamente los equipos tecnológicos, específicamente no cuenta con la información de la serie del equipo, la clasificación o tipo del mismo (servidor físico, computadora personal o portátil, Switch, Router, Patch Panel, etc.), así como la información sobre la garantía del activo (estado y fecha de vencimiento). En la siguiente pantalla se muestra parte de la información con la que cuenta el sistema:

RAF304 JORMORENO

**BANCO HIPOTECARIO DE LA VIVIENDA**
**SISTEMA DE ACTIVOS FIJOS**
**FUENTE DE FONDOS CUENTA GENERAL**

03/22/2018
Pag 38 de 63

Reporte de Depreciación Mensual de Activos por Cuenta de Depreciación
Mes-Año de Proceso: 03-2018

**Cuenta de Depreciación Acumulada 1790310033400010 Equipo De Comunicaciones**

| No Activo | Detalle del Activo | Fecha de Ingreso | Costo Original | Valor Residual | Vida Útil | % Dep | Depreciación Acum Anterior | Depreciación Mensual | Depreciación Acum Actual | Valor en libros actual |
|---|---|---|---|---|---|---|---|---|---|---|
| 25-5684 | SWITCH DE COMUNICACIÓN 8 PUERT | 09/11/2016 | 22,000.00 | 1.00 | 10 | 10 | 2,749.95 | 183.33 | 2,933.28 | 19,066.72 |
| 25-5685 | SWITCH DE COMUNICACIÓN 8 PUERT | 09/11/2016 | 22,000.00 | 1.00 | 10 | 10 | 2,749.95 | 183.33 | 2,933.28 | 19,066.72 |
| 25-5686 | SWITCH DE COMUNICACIÓN 8 PUERT | 09/11/2016 | 22,000.00 | 1.00 | 10 | 10 | 2,749.95 | 183.33 | 2,933.28 | 19,066.72 |
| 25-5687 | SWITCH DE COMUNICACIÓN 8 PUERT | 09/11/2016 | 22,000.00 | 1.00 | 10 | 10 | 2,749.95 | 183.33 | 2,933.28 | 19,066.72 |
| 25-5688 | SWITCH DE COMUNICACIÓN 8 PUERT | 09/11/2016 | 22,000.00 | 1.00 | 10 | 10 | 2,749.95 | 183.33 | 2,933.28 | 19,066.72 |
| 25-5689 | SWITCH DE COMUNICACIÓN 8 PUERT | 09/11/2016 | 22,000.00 | 1.00 | 10 | 10 | 2,749.95 | 183.33 | 2,933.28 | 19,066.72 |
| 25-5690 | SWITCH DE COMUNICACIÓN 8 PUERT | 09/11/2016 | 22,000.00 | 1.00 | 10 | 10 | 2,749.95 | 183.33 | 2,933.28 | 19,066.72 |
| 25-5691 | SWITCH DE COMUNICACIÓN 8 PUERT | 09/11/2016 | 22,000.00 | 1.00 | 10 | 10 | 2,749.95 | 183.33 | 2,933.28 | 19,066.72 |

El artículo 8.1.1 sobre el inventario de activos del ISO-IEC-27002:2016, detalla lo siguiente relacionado a la administración de activos:

> *"Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir la creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. La documentación debería mantenerse en inventarios dedicados o existentes según corresponda.*
>
> *El inventario de activos debería se exacto, actualizado, coherente y alineado con otros inventarios.*
>
> *Para cada uno de los activos identificados, deberían asignarse un propietario (ver apartado 8.1.2) y debería identificarse la clasificación (ver apartado 8.2)"*

Adicionalmente, en el punto 4 de la práctica de gestión DSS01.03 "*Supervisar la infraestructura de TI*" del COBIT 5, se indica lo siguiente:

> *"**DSS01.03 Supervisar la infraestructura de TI**.*
> *Supervisar la infraestructura de TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.*
> *(…)*

*2. Identificar y mantener una lista de activos de infraestructura que necesiten ser monitoreados en base a la criticidad del servicio y la relación entre los elementos de configuración y los servicios que de ellos dependen…"*

Según lo indicado por personal de soporte, el que no se incluyeran todos los equipos de comunicación en el contrato indicado así como la colocación de equipos fuera de uso, se debe a la carencia de una persona encargada del área de telecomunicaciones, lo que originó que se utilizara el listado de equipos de comunicación que se definieron en el mantenimiento del año 2017. Además, los campos que se requieren para controlar mejor los activos tecnológicos no se incluyeron en el sistema de Activos porque no fueron visto como necesarios cuando se elaboró la aplicación.

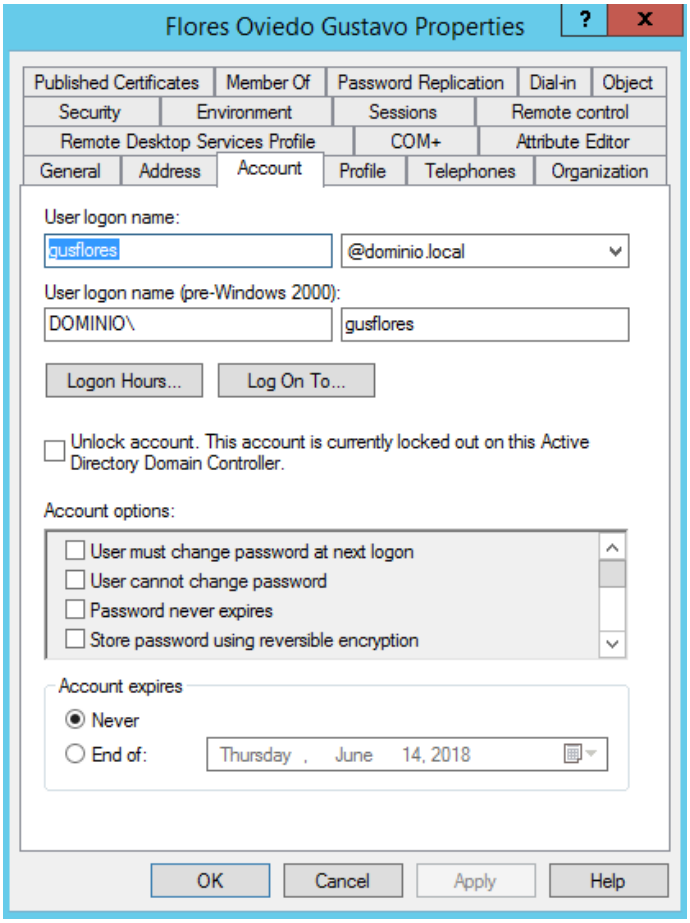
Como posibles riesgos de que no se incluyan y detallen todos los equipos de comunicación en los mantenimientos anuales, es que alguno de estos activos tenga un desperfecto y no sea atendido según el contrato vigente, viéndose afectada la operativa institucional y por ende, la continuidad del servicio interno y externo. Adicionalmente, el no contar con un detalle más específico a nivel del sistema de Activos, obliga a llevar un control manual sobre el seguimiento de los equipos y sus fechas de vencimiento de garantías, pudiendo omitirse activos de importancia en una actualización del contrato de mantenimiento.

## 2.5 Acceso remoto a los Servicios Internos

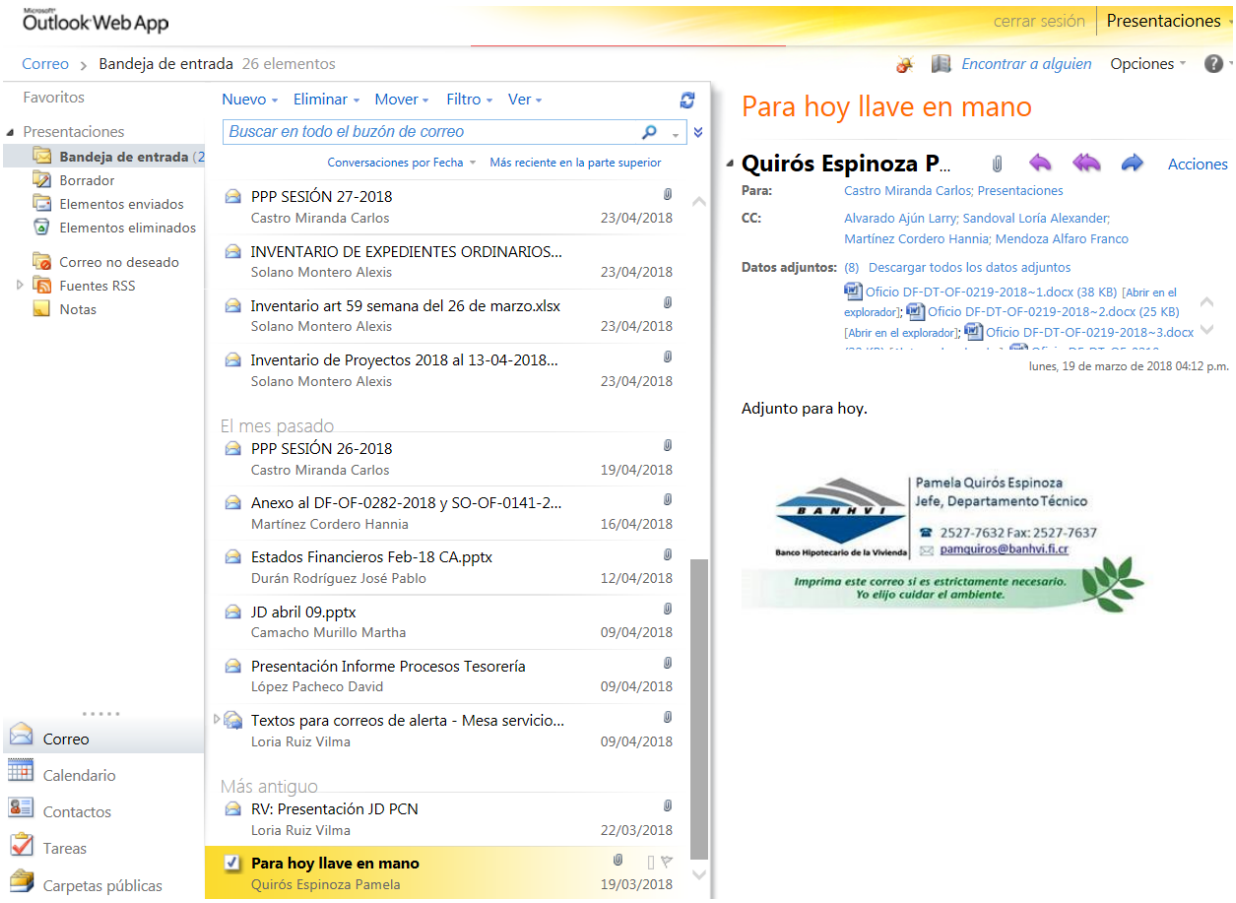
Evaluando algunos de los métodos actuales con los que se puede acceder a los recursos tecnológicos del Banco, en este caso, al correo electrónico, se realizaron pruebas que consistieron en ingresar a ciertas cuentas de correo por medio del link que ofrece la página web del Banhvi a los funcionarios activos (http://www.banhvi.fi.cr/perfiles/funcionario.aspx), para lo que se utilizaron algunos códigos de usuario de personal de la Auditoría Interna (incluido el Auditor Interno). Las pruebas consistieron además de ingresar a las respectivas cuentas, en tratar de bloquear al usuario con el uso de contraseñas de acceso incorrectas. Como resultado se obtuvo que todas las cuentas probadas fueron bloqueadas después de ingresar incorrectamente la clave de acceso en varias ocasiones, denegando así el respectivo acceso al equipo y por defecto a todos los recursos tecnológicos disponibles en la red institucional. Se aclara que después de cierto tiempo, la cuenta se desbloquea de forma automática.

Seguidamente se muestran como ejemplo algunas de las pantallas capturadas.


Microsoft
Outlook Web App
Seguridad ( mostrar explicación )
Es un equipo público o compartido
Es un equipo privado
Aviso: Al seleccionar esta opción, confirmas que este equipo cumple con la directiva de seguridad de la organización.
Usar Outlook Web App Light
Nombre de usuario: gusflores
Contraseña:
Iniciar sesión
El nombre de usuario o contraseña no son correctos. Vuelva a introducirlos.
Conectado a Microsoft Exchange
© 2010 Microsoft Corporation. Reservados todos los derechos.


Flores Oviedo Gustavo Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Security
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
Attribute Editor
General
Address
Account
Profile
Telephones
Organization
User logon name:
gusflores
@dominio.local
User logon name (pre-Windows 2000):
DOMINIO\
gusflores
Logon Hours...
Log On To...
Unlock account. This account is currently locked out on this Active Directory Domain Controller.
Account options:
User must change password at next logon
User cannot change password
Password never expires
Store password using reversible encryption
Account expires
Never
End of:
Thursday , June 14, 2018
OK
Cancel
Apply
Help

Adicional a las pruebas descritas se ejecutaron accesos remotos vía Web, se utilizó el usuario genérico de "*presentaciones*" utilizado en el Banco para realizar trabajos generales de escaneo o efectuar exposiciones por distintas áreas (incluida la Junta Directiva). Una vez que se ingresó con dicho usuario, se logró acceder a información de diferentes áreas tanto en la bandeja de Entrada como en la de Salida, todo sin ninguna restricción sobre la información contenida. Las siguientes son unas de las pantallas donde se observa parte de los correos y temas disponibles:




Según el artículo 13.1.1 sobre la sección de "*Gestión de seguridad de red*" del ISO-IEC-27002:2016, se indica lo siguiente referente a controles de red:

> *"13.1.1 Controles de red*
>
> *Los controles deberían ser implementados para procurar la seguridad de la información en las redes y la protección de los servicios conectados de accesos no autorizados. En particular, los siguientes ítems deberían ser considerados:*
> *(…)*
> *c) deberían establecerse controles especiales para salvaguardar la confidencialidad y la integridad de los datos que circulan a través de redes públicas o inalámbricas así como para proteger los sistemas y aplicaciones conectados (ver apartados 10 y 13.2); podrían también ser requeridos controles especiales para mantener la disponibilidad de los servicios de red y de las computadoras conectadas;*
> *(…)"*

El posible motivo de que se puedan bloquear usuarios de forma remota o acceder a información de diferentes áreas del Banco utilizando el usuario de "*Presentaciones*", se debe a que hasta la fecha de la auditoría no se había valorado esa posibilidad como un riesgo materializable en la institución.

Efectos directos de las dos situaciones detalladas, son la posible denegación del servicio a cualquiera de los funcionarios internos (Gerencia, Direcciones, Jefaturas, etc.) siendo necesario contar con personal de soporte técnico para desbloquear las cuentas; así como el acceso a información que puede ser confidencial o privada dentro de la operativa de ciertas áreas del Banco.

## 2.6 Monitoreo de Vulnerabilidades de Red

Como parte de las actividades de control realizadas por el Departamento de TI y según la normativa interna vigente (procedimiento P-DTI-HRC-025), se realizan de forma periódica estudios sobre las vulnerabilidades internas a la red de datos institucional. De acuerdo a la información recabada, se detectó que desde el 11 de julio del año 2013 se dejaron de efectuar este tipo de revisiones, a pesar de que según el procedimiento debían realizarse al menos una vez al año.

Referente también a este tipo de evaluación, no se encontró documentación que demuestre la ejecución de pruebas de vulnerabilidad o penetración a la red del Banco de forma externa, normalmente realizadas por empresas especializadas en el tema de seguridad.

Se muestra una muestra de la documentación interna obtenida referente a la revisión interna de vulnerabilidades de la red:

**Security assessment:**
**Severe Risk (One or more critical checks failed.)**

| | |
|---|---|
| **Computer name:** | DOMINIO\SRV-SP-07 |
| **IP address:** | 192.168.100.11 |
| **Security report name:** | DOMINIO - SRV-SP-07 (11-07-2013 10-35 a.m.) |
| **Scan date:** | 11/07/2013 10:35 a.m. |
| **Catalog synchronization date:** | |
| **Security update catalog:** | Microsoft Update |

**Security Updates**

| Score | Issue | Result |
|---|---|---|
| | Developer Tools, Runtimes, and Redistributables Security Updates | 1 security updates are missing.<br>**Security Updates**<br>Score ID Description Maximum Severity<br>Missing MS11-025 Security Update for Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package (KB2538242) Important |
| | Exchange Security Updates | 1 security updates are missing.<br>**Security Updates**<br>Score ID Description Maximum Severity<br>Missing MS13-012 Update Rollup 6 for Exchange Server 2010 Service Pack 2 (KB2746164) Critical<br>**Current Update Compliance**<br>Score ID Description Maximum Severity<br>Installed MS12-080 Update Rollup 5-v2 for Exchange Server 2010 Service Pack 2 (KB2785908) Critical |
| | Windows Security Updates | 15 security updates are missing. 2 service packs or update rollups are missing.<br>**Security Updates** |

El artículo 18.2.3 perteneciente a la sección 18.2 sobre revisiones de seguridad de la información, del ISO-IEC-27002:2016, detalla lo siguiente:

> ***"18.2.3 Revisiones del cumplimiento técnico***
>
> *La revisión de cumplimiento técnico comprende el examen de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. Este tipo de revisión de la conformidad requiere asistencia técnica especializada.*
>
> *La revisión del cumplimiento también comprende, por ejemplo, pruebas de penetración y evaluación de vulnerabilidades, las cuales podrían ser realizadas por expertos independientes contratados específicamente con este propósito. Esto puede resultar útil para la detección de vulnerabilidades en el sistema y para verificar qué tan efectivos son los controles en relación con la prevención de accesos no autorizados posibilitados por estas vulnerabilidades.*
>
> *Las pruebas de penetración y la evaluación de vulnerabilidades proporcionan una fotografía de un sistema en un estado y momento específico. La muestra se limita a esas porciones del sistema probado realmente durante el o los intentos de penetración. Las pruebas de penetración y evaluación de vulnerabilidades no son un sustituto para la evaluación de riesgo.*
>
> *La Norma ISO/IEC TR 27008 proporciona orientación específica con respecto a las revisiones de cumplimiento técnico."*

Como causa principal para que no se ejecuten estudios de vulnerabilidad internos a la red de datos, es que la normativa correspondiente se encuentra desactualizada, aunado a la carencia de personal técnico especializado en ese tipo de estudios. Relacionado con las pruebas de penetración externas, las mismas no se han efectuado porque no existe alguna política y procedimiento que obliguen su ejecución.

Al carecer de este tipo de revisiones internas y externas, se amplía la posibilidad de contar con debilidades de control lógicas o físicas sobre la red de datos institucional, pudiendo verse afectada directamente la información interna contenida en las bases de datos del Banco.

## 3. CONCLUSIÓN

La innovación constante de la tecnología ha venido a incidir directamente sobre la forma en que deben ser administrados y controlados los recursos tecnológicos del Banco; donde la red de datos institucional y sus componentes representa uno de los insumos de mayor relevancia para la adecuada prestación de servicios ofrecidos por el Departamento de TI.

En la ejecución de la auditoría se detectó la carencia de algunos controles relevantes para la correcta administración de los equipos de comunicación y la infraestructura que los soporta. Como parte de los aspectos que deben mejorarse se encuentra la normativa interna relacionada con el tema, una mayor vigilancia y seguimiento sobre el inventario y cableado de red, la actualización de los contratos actuales de mantenimiento y soporte sobre el hardware de comunicaciones, el incremento en los controles para los accesos remotos, así como la reactivación de actividades orientadas a valorar los posibles riesgos internos y externos de la red de datos.

La ejecución del trabajo fue realizado aplicando las técnicas de auditoria correspondientes, evaluando la operativa y la normativa vigente relacionada con la red de datos institucional y sus componentes

En la sección siguiente se explica con mucho más detalla las recomendaciones que según la Auditoría Interna deben implementarse para mejorar el proceso de continuidad de negocio, en una posible contingencia que afecte los recursos tecnológicos.

## 4. RECOMENDACIONES

En relación con los informes de la Auditoria 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."*

A continuación se presentan las recomendaciones de acuerdo al orden en que fueron expuestas en la sección de resultados. Todas las recomendaciones están dirigidas para su seguimiento e implementación hacia la Dirección FOSUVI.

## 4.1 Normativa sobre la Red Institucional

**Al Departamento de TI**

4.1.1 Actualizar según la realidad institucional las políticas y procedimientos detallados en el apartado 2.1 de la sección de resultados de este informe.

Nivel de Riesgo: **Medio**

## 4.2 Cableado y ductos de Red

**Al Departamento de TI**

4.2.1 Se debe efectuar un estudio de costo beneficio enfocado a valorar la factibilidad técnica y económica de contratar a una empresa externa para que certifique todos los nuevos puntos de conexión y las placas de pared que se han modificado o agregado a la red de datos institucional en los últimos años. De ser viable tal proyecto, debe realizarse una vez que se cuente en el Banco con el recurso interno capacitado en telecomunicaciones (que está en proceso de contratación al momento de la auditoría), para que sirva como contraparte interna a nivel de control de calidad.

Nivel de Riesgo: **Medio**

4.2.2 Deben etiquetarse el cableado de red correspondiente que esté ubicado en el rack de comunicaciones de la sala de servidores, así como el cable de cada uno de los ductos ubicados en cada piso del Banco y sus correspondientes placas de pared (de ser necesario). Junto a este trabajo debe actualizarse toda la documentación interna de la red con la que cuente el área de Soporte Técnico, para facilitar tanto el control de los insumos con los que se cuente, así como el mantenimiento respectivo.

Nivel de Riesgo: **Medio**

**A la Dirección Administrativa**

4.2.3 La administración y control de los ductos de comunicación debe ser una actividad realizada exclusivamente por el Departamento de TI, por lo que es necesario que se eliminen todas las llaves de acceso a dichos ductos por parte del área de mantenimiento del edificio. Siendo así, en lo sucesivo cada vez que se requiera efectuar un trabajo en algunos de los ductos de comunicación, debe ser coordinado con el área de Soporte de TI y supervisado en todo momento.

Nivel de Riesgo: **Medio**

### 4.3 Inventario de Equipos de Comunicación

**A la Dirección Administrativa**

4.3.1 Se debe etiquetar el equipo de comunicaciones que lo amerite (detallados en este informe) y actualizarlos o ubicarlos en el inventario administrado por Proveeduría según corresponda, evitando pérdidas o confusiones al momento de revisar tales activos.

Nivel de Riesgo: **Medio**

**Al Departamento de TI**

4.3.2 Renovar la documentación del "control de inventario de los componentes de red" que es utilizado por el Departamento de TI y de ser necesario actualizar el procedimiento P-DTI-HRC-017 "Nuevas conexiones de Red", de acuerdo a los insumos tecnológicos que se tengan para administrar los recursos de la red (hardware y software).

Nivel de Riesgo: **Medio**

### 4.4 Mantenimiento sobre los Equipos de Comunicación

**Al Departamento de TI**

4.4.1 Implementar un control enfocado a administrar la totalidad de equipos de comunicación que son incluidos como parte del soporte y mantenimiento anual con el proveedor externo, previendo que se incluyan dentro del contrato todos los equipos vigentes de la institución.

Nivel de Riesgo: **Medio**

4.4.2 Evaluar junto al área de Proveeduría, la posibilidad de elaborar un adendum al contrato vigente 2018CD-000022-00164-00001 con la empresa Altus Consulting, con el objetivo de que se incluyan la totalidad de equipos de comunicación que están vigentes y que deberían formar parte del soporte y mantenimiento anual con dicha empresa.

Nivel de Riesgo: **Medio**

**A la Dirección Administrativa**

4.4.3 Con la finalidad de que se controlen mejor los activos tecnológicos del Banco, debe gestionarse con el área de Desarrollo de Sistemas una mejora a la aplicación de Activo Fijo, para que se incorpore más información de control al sistema. A criterio de la Auditoría Interna debería incluirse al menos campos para administrar el número de serie del equipo, la clasificación o tipo del activo (servidor físico, computadora personal o portátil, Switch, Router, Patch Panel, etc.) e información sobre sobre su garantía (estado y fecha de vencimiento) cuando aún la tenga. Queda a criterio del área de Proveeduría solicitar más campos para controlar mejor su proceso.

Nivel de Riesgo: **Medio**

## 4.5 Acceso remoto a los Servicios Internos

**Al Departamento de TI**

4.5.1 Evaluar si dentro de las tecnologías disponibles hoy día en el mercado, existe alguna herramienta que le permita a los empleados que lo requieran, tener acceso remoto a los recursos de TI del Banco (correo, archivos, sistemas, computadoras, etc.), minimizando la posibilidad de que sean bloqueadas cualquiera de las cuentas lógicas de los funcionarios internos.

Nivel de Riesgo: **Medio**

4.5.2 Valorar la viabilidad técnica y operativa de que si una cuenta de usuario es bloquea de forma remota (vía WEB), no exista la opción de que se desbloquee automáticamente después de cierto tiempo, sino que se necesite de algún técnico de soporte interno para hacerlo o algún procedimiento especial. Esto con la finalidad de minimizar el riesgo de que estén probando posibles passwords para una cuenta específica por un número indefinido de veces. Adicional, si la cuenta es bloqueada de esta forma, debe quedar un registro en el área de TI y se debe comunicar al dueño de la cuenta para que este tome las medidas de seguridad que considere convenientes.

Nivel de Riesgo: **Bajo**

4.5.3 Debe evaluarse la posibilidad de que el usuario de “presentaciones” no deje ningún registro o material de la información que es enviada o recibida vía correo electrónico por medio de dicha cuenta. Al respecto debe valorarse los beneficios y contras de mantener activo ese usuario y de ser necesario, debe actualizarse la normativa sobre su utilización,

tomando en cuenta las medidas de seguridad y confidencialidad que sean necesarias.

Nivel de Riesgo: **Medio**

## 4.6 Monitoreo de Vulnerabilidades de Red

**Al Departamento de TI**

4.6.1 Actualizar y desarrollar la normativa interna necesaria y suficiente para que se realicen periódicamente pruebas internas de vulnerabilidad a la red de datos y pruebas de penetración de forma externa con personal técnico especialista en ese tipo de trabajos.

Nivel de Riesgo: **Alto**

4.6.2 Evaluar por medio de un estudio de costo beneficio, la viabilidad de contratar una empresa externa que verifique por medio de pruebas de penetración y evaluación de vulnerabilidades, las posibles debilidades o huecos de seguridad de los recursos tecnológicos utilizados por el Banco, así como la capacidad de la organización para identificar y responder a posibles incidentes de seguridad.

Nivel de Riesgo: **Alto**

MBA. Gustavo Flores Oviedo.
Auditor Interno.