Auditoría Interna

Informe Definitivo

Gestión de la disponibilidad y capacidad de la red de datos

AIRI-17-2020

Julio, 2020

Tabla de Contenido

I. Resumen Ejecutivo 3
II. Resumen de hallazgos 5
III. Observaciones y Recomendaciones 5
1. Los usuarios del Banco presentan problemas de navegación a Internet de forma recurrente 5
2. El monitoreo del tráfico de datos de red no genera un valor agregado 8
3. Ausencia de criterios para la definición justificada de la capacidad de los enlaces 10
4. El manejo actual de los enlaces alternos de microondas no garantiza una continuidad del servicio 13
IV. Equipo de Auditoria 15

I. Resumen Ejecutivo

Objetivo General	Evaluar la gestión de la capacidad y disponibilidad de la infraestructura de telecomunicaciones, incluyendo nube y comunicaciones unificadas, con la finalidad de determinar la efectividad en la atención de la demanda actual de servicios requeridos por el Banco.
Objetivos Específicos	✓ Verificar los controles establecidos por las áreas técnicas para mantener la disponibilidad de la red de datos en niveles óptimos de operación, con el fin de determinar si se asegura una prestación de los servicios de manera estable y continua. ✓ Evaluar la gestión de planificación de los recursos de TI relacionados con telecomunicaciones, con la finalidad de verificar si se soportan las necesidades del negocio y la demanda de nuevos modelos de operación, tales como servicios de nube y comunicaciones unificadas. ✓ Comprobar que se realiza un proceso de monitoreo de la disponibilidad y de la capacidad de los recursos de Telecomunicaciones, incluyendo la emisión de informes periódicos y de definición de acciones correctivas, con la finalidad de verificar que se mitiguen de forma oportuna aquellos riesgos que puedan afectar la entrega de servicios.
Alcance	El estudio comprendió la gestión de capacidad y disponibilidad de la red de datos en producción del Banco para el período de noviembre 2019 a mayo 2020.
Comunicación verbal de los resultados	El pasado 3 de julio del 2020, se efectuó la reunión de discusión de los resultados del estudio con la participación de los siguientes funcionarios de la Administración: Geoffrey Araya Gómez, jefe de la División de Operación de Servicios, Daniels Hidalgo Jiménez, jefe del Área de Seguridad Operativa Informática, Sergio Cambronero Montero, supervisor del Área de Redes y Telecomunicaciones, Jorge Alfaro Casas, jefe del Área de Monitoreo. Por su parte, la Auditoría Interna estuvo representada por Edgar Bolaños Jara, Carlos Araya Guzmán y Gerardo Zúñiga Hernández. Los puntos y recomendaciones que requirieron ajustes fueron realizados y se incorporaron, en lo que corresponde, los comentarios externados.

Conclusión

La gestión de las redes y de seguridad perimetral requiere de un mayor esfuerzo conjunto entre el Área Seguridad Operativa Informática y el Área de Redes y Telecomunicaciones, y de mejor comunicación para la atención oportuna y eficiente de los incidentes que provocan inestabilidad en los servicios y enlaces de red, elementos que al día de hoy no garantizan la entrega de un servicio estable al usuario.

Los incrementos de capacidades de la red, no son realizados bajo un análisis estructurado y estandarizado, basado en estadísticas y comportamientos de los enlaces, lo que ocasiona que se adquieran capacidades adicionales a las requeridas, asumiendo un costo adicional de manera innecesaria.

Se determinaron oportunidades de mejora en el servicio de monitoreo de la red, en cuanto a la necesidad de incorporar herramientas adicionales que permitan un monitoreo por servicios y con la posibilidad de obtener información estadística para la toma de decisiones, puesto que, en las condiciones actuales, el servicio recibido no agrega valor.

Aunque existen esfuerzos encaminados a una mejor atención de la capacidad y disponibilidad de los servicios de red, no es posible identificar, en función de los elementos anteriormente citados, si la capacidad y disponibilidad se desarrolla de forma adecuada, por la falta de análisis y soluciones a los problemas de navegación, carencias de herramientas y conocimiento para el monitoreo de patrones irregulares del tráfico , ausencia de criterios para definir capacidades de enlaces, en función tanto de la demanda actual como futura de necesidades y tendencias tecnológicas.

Calificación de riesgo y control

Muy bueno	Satisfactorio	Necesita Mejorar	Necesita mejorar significativamente	Insatisfactorio
		✓		

II. Resumen de hallazgos

Calificación de riesgo:	Alto	Medio	Bajo

Núm.	Hallazgo	Riesgo
1	Los usuarios del banco presentan problemas de navegación a Internet de forma recurrente	Alto
2	El monitoreo del tráfico de datos de red no genera un valor agregado	Medio
3	Ausencia de criterios para la definición justificada de la capacidad de los enlaces	Medio
4	El manejo actual de los enlaces alternos de microondas, no garantizan una continuidad del servicio	Medio

III. Observaciones y Recomendaciones

1. Los usuarios del Banco presentan problemas de navegación a Internet de forma recurrente

Pese a la implementación de las soluciones ForcePoint[1] como rol primario de salida de la navegación a Internet y VPN[2] de AnyConnect para el acceso remoto a la red del Banco, se determinó que se continúan presentando las siguientes situaciones, que muestran inestabilidad en el servicio de conexión a Internet:

- Mensaje que limita el uso de servicios: "Se requieren las credenciales del proxy (nombre de usuario y contraseña) http://ipv4.201.203.6.187.hybrid-web.global.blackspider.com:8081".
- Mensaje: "No se puede establecer la conexión con el Servidor Proxy".
- La aplicación de correo Outlook muestra un mensaje de error indicando que no puede establecerse la conexión o intenta conectarse al Microsoft Exchange y se mantiene desconectado.
- Mensaje: "The VPN connection failed due to unsuccesful domain name resolution".
- Mensaje: "AnyConnect was no able to establish a connection to the specified secure Gateway. Please try connection again".
- El Cisco AnyConnect da mensajes de conexiones y desconexiones de forma constante, durante algunos lapsos (*"Connected: www.remoto.bp.fi.cr" y "Reconnecting: www.remoto.bp.fi.cr"*).

[1] ForcePoint es una solución para reemplazar el proxy TMG (Microsoft ForeFront Threat Management Gateway 2010), el cual está fuera de soporte del fabricante desde abril 2020 y provocó saturación del servicio de Internet, debido a que manejaba más sesiones concurrentes de las que realmente podía gestionar.
2 El VPN AnyConnect de Cisco se reemplazó por el VPN CheckPoint de Symantec, el AnyConnect se implementó como parte de la solución de NAC para el control de acceso a la red.

Si bien, estos incidentes se presentan con mayor frecuencia desde mediados de marzo 2020, producto de la implementación del teletrabajo[3], debido a que se está haciendo un uso más intensivo del servicio de internet, por la migración de varias herramientas de trabajo a la nube de Office 365; esta auditoría ya había indicado al personal de la Dirección de Tecnología de Información, desde abril de 2019, la existencia de problemas para el acceso a Internet.

La inestabilidad en el servicio de Internet, también se ha producido por incidentes asociados con el enlace de navegación[4], tal y como se evidencia el 28 de febrero de 2020, donde según el informe preparado por RACSA, la afectación fue de 5 horas y 35 minutos y cuya resolución consistió en el reinicio de un equipo del proveedor para normalizar el tráfico.

La solución brindada a la fecha por el Grupo de Seguimiento a Problemas y por la mesa del Área de Atención al Cliente Interno, ha consistido en aplicar actualizaciones al Sistema Operativo Windows, y aplicaciones de Microsoft Office, desinstalar Check Point y desinstalar e instalar el AnyConnect y ForcePoint, reiniciar equipos o ejecutar comandos tales como: netsh winsock reset, gpupdate.exe /force y Outlook.exe /resetnavpane, este último cuando no abre la aplicación de correo, siendo medidas que no garantizan una solución permanente de los incidentes que se presentan.

Las situaciones anteriores se mantienen debido a lo siguiente:

- No se evidenció que los incidentes relacionados con el proxy y el VPN hayan sido analizados por el Grupo de Seguimiento a Problemas o de forma integral por la Dirección de Tecnología de Información y sus dependencias adscritas, únicamente se aplican las medidas de reinstalación y reinicio de equipos indicadas anteriormente.
- A la fecha, el área de Seguridad Operativa Informática no ha elevado los casos para su resolución por parte de los proveedores o fabricantes.
- No se han implementado esquemas de monitoreo en tiempo real o por medio de generación de reportes, que permitan determinar si las soluciones de ForcePoint y Cisco AnyConnect, presentan problemas de capacidad y desempeño. Esta situación también se presentó con la plataforma de proxy anterior TMG, lo que dificultó la identificación oportuna de los problemas de capacidad en conexiones concurrentes.
- Aún no se ha dado de baja a las plataformas de TMG y CheckPoint. Según el argumento del Área de Seguridad Operativa Informática, para dar de baja el TMG, ningún equipo de usuario final debe tener instalado el CheckPoint y según se evidenció, al menos 2100 computadoras se mantienen con ese agente instalado, pues solo se desinstala si el usuario reporta un incidente a la mesa de servicios del Área de Atención al Cliente Interno (AACI).

[3] Como una acción de la Administración para evitar el contagio por la crisis del COVID-19.

[4] Enlace de Navegación: Capacidad de 900 MBPS, por el cual pasa el tráfico asociado con las conexiones mediante VPN, la navegación por Internet accediendo a páginas web y también el acceso requerido hacia Office 365. El tráfico es generado por los usuarios del Banco según uno o varios de los servicios anteriores que consuman.

Lo anterior, es contrario a lo recomendado por el **Marco de Trabajo de Referencia para el Gobierno y Administración de la Tecnología de Información Empresarial COBIT 5**, en la siguiente práctica:

> ***DSS02.04 Investigar, diagnosticar y localizar incidentes.***
> *Identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución.*

Específicamente, la siguiente actividad:

> *Asignar incidentes a funciones especialistas si se necesita de un conocimiento más profundo, e implicar al nivel de gestión apropiado, cuando sea necesario.*

Una conexión inestable se traduce en problemas constantes de acceso a los recursos de la red del Banco y en un uso ineficiente de los servicios en la nube de Office 365, situación que afecta el desarrollo de las funciones diarias de los colaboradores del Banco, especialmente aquellos bajo la modalidad de teletrabajo, lo que genera un riesgo de incumplimiento en las metas de negocio, aspectos normativos e inclusive afectar la salud de los funcionarios (en la situación de pandemia actual), por la necesidad de trasladarse a las oficinas para obtener una conexión más estable a los recursos de red.

Recomendaciones
Para: Área de Seguridad Operativa Informática

1. Identificar, analizar y gestionar la solución de la causa raíz de los incidentes relacionados con ForcePoint y AnyConnect.

   Valorar la participación de los proveedores de ForcePoint y AnyConnect u otras áreas de TI para resolver las causas raíz de esos incidentes.

Fecha cumplimiento: 31/01/2021	**Nivel de Riesgo: Alto**	**TR: CI**

Para: División de Operación de Servicios

2. En conjunto con el Área de Atención al Cliente Interno, desarrollar e implementar un plan con responsables, fechas y actividades para gestionar la instalación de las herramientas ForcePoint y VPN de AnyConnect a todos los usuarios que actualmente mantienen en sus equipos de cómputo el agente de CheckPoint.

   Asegurar la desinstalación del agente de CheckPoint de Symantec de todos los equipos de usuario final.

Fecha cumplimiento: 17/08/2020	**Nivel de Riesgo: Alto**	**TR: CI**

3. En conjunto con el Área Seguridad Operativa Informática, realizar un análisis sobre el manejo de sesiones concurrentes asociado a las plataformas ForcePoint y VPN de AnyConnect, con el fin de determinar si la capacidad actual es suficiente para atender la demanda de servicios.

   Sobre los resultados obtenidos, ejecutar las acciones que corresponda para mejorar la capacidad de los servicios si corresponde.

Fecha cumplimiento: 31/01/2021 Nivel de Riesgo: Medio TR: CI

Para: Área de Monitoreo

4. Realizar un análisis para determinar la factibilidad de desarrollar esquemas de monitoreo de la capacidad y desempeño para las herramientas Cisco AnyConnect y ForcePoint, con la finalidad de mejorar la comprensión e identificación de problemas en su comportamiento y uso y para el manejo de alertas en los equipos de usuario final.

Fecha cumplimiento: 15/11/2020 Nivel de Riesgo: Medio TR: CI

2. El monitoreo del tráfico de datos de red no genera un valor agregado

La gestión de la red de datos carece de herramientas, infraestructura y conocimiento para ejecutar un monitoreo integral de los diferentes servicios que consumen recursos de red y que prevenga de eventos de saturación, especialmente en este momento, donde se realiza un uso más intensivo de comunicaciones unificadas y servicios de la nube de Office 365.

Al respecto, se determinó que las herramientas provistas por el Área de Redes y Telecomunicaciones al personal de GBM que realiza labores de monitoreo, no reflejan el comportamiento real de los enlaces, ni permiten identificar las causas que originan la saturación de la red. Por ejemplo: se evidenciaron casos en enlaces que operaron por niveles cercanos al 100% de su capacidad, sin poder determinarse el origen del alto consumo de recursos, al no poder identificarse de manera puntual, comportamientos de tráfico irregular en una o varias direcciones IP o dispositivos que presenten una mayor pérdida de paquetes[5].

Asimismo, los procesos de monitoreo con la verificación de pérdida de paquetes y estado de recursos (CPU, Memoria), en switches y routers solo están disponibles en tiempo real, pero no se cuenta con información histórica para la revisión de tendencias, lo que a su vez, se traduce en la solución y monitoreo del evento cuando

5 Una pérdida de paquetes, implica que los paquetes o datos que vienen desde un origen, no llegan a su destino y esto se traduce en la afectación de algún servicio(s) justamente por esta pérdida

este se presenta en determinado momento, pero sin poder determinar si el evento se presenta de manera recurrente a largo plazo en un mismo equipo, por falta de reportes que puedan recoger y generar estadísticas para análisis.

Estas situaciones se producen debido a que el Área de Redes y Telecomunicaciones carece de herramientas que permitan ejercer un monitoreo integral y ayuden a desarrollar una gestión preventiva del uso de recursos de red, por consiguiente el apoyo de personal externo de GBM en labores de monitoreo es limitado; además se asume que el Área de Monitoreo abarcará todas las actividades de monitoreo de las redes[6].

Sobre las mejoras en el monitoreo de la red, el **Marco de Trabajo de Referencia para el Gobierno y Administración de la Tecnología de Información Empresarial COBIT 5**, refiere a la siguiente práctica:

> ***BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.***
> *Abordar las desviaciones investigando y resolviendo las cuestiones identificadas relativas a disponibilidad, rendimiento y capacidad*

Específicamente, la siguiente actividad:

> *Identificar brechas de rendimiento y capacidad sobre la base de la monitorización del rendimiento actual y previsto…*

El monitoreo actual no agrega valor a la gestión integral de mejora de la capacidad y disponibilidad de la red, lo que limita la posibilidad de identificar de manera proactiva las causas de saturación en los enlaces y genera un desaprovechamiento de la inversión en recurso tercerizado.

Recomendaciones
Para: Área de Redes y Telecomunicaciones

5. Gestionar las acciones que corresponda para la puesta en uso de herramientas que permitan la generación de reportes sobre eventos dentro y fuera de los patrones habituales y que contribuyan a una mejor comprensión de las actividades recurrentes que afectan las redes.

Fecha cumplimiento: 31/10/2020	**Nivel de Riesgo: Medio**	**TR: CI**

6 El Área de Monitoreo está gestionando un proyecto que dentro de su implementación, considera el monitoreo de los Routers y Switches a nivel de CPU; RAM, Memoria, labores que son actualmente desarrolladas por GBM.

3. Ausencia de criterios para la definición justificada de la capacidad de los enlaces

En la revisión de la gestión de los enlaces de comunicaciones se identificaron las siguientes situaciones:

Capacidades distintas en enlaces de Oficinas comerciales: Las oficinas del Banco del mismo tipo, cuentan con enlaces de comunicación con anchos de banda distintos; al respecto, este Despacho no obtuvo evidencia que justifique tales diferencias ni los criterios para justificar los aumentos tramitados. Algunos de los casos identificados se muestran a continuación:

Cuadro No.1
Capacidad del enlace de Agencias y BP Totales

Oficina comercial	Capacidad del enlace primario
Agencia San Vito	4 Mbps
Agencia. Paseo Metrópoli	6 Mbps
Agencia. Paquera	4 Mbps
Agencia Monteverde	4 Mbps
Agencia Hatillo	8 Mbps
Agencia Nosara	4 Mbps
Agencia Peri Cartago	4 Mbps
Agencia Guácimo	4 Mbps
Agencia San Marcos de Tarrazú	4 Mbps
BP Total Cartago	30[7] MBPS
BP Total Heredia	30 MBPS
BP Total Puntarenas	30 MBPS
BP Total Alajuela	30 MBPS

Fuente: Creación propia a partir de información facilitada por el Área de Redes y Telecomunicaciones

Tampoco se identificaron los criterios para definir la capacidad del enlace que debe tener cada tipo de oficina, sin embargo, según se evidenció el consumo promedio inclusive en periodos de mayor transaccionalidad como: del 12 al 18 de agosto 2019 (día de la madre), del 1 al 15 de diciembre 2019 (pago de aguinaldos) y del 18 al 26 de enero 2020 (pago de salario escolar), no superó 1 MBPS.

Por el contrario, en el caso del enlace de Webbanking[8], para el período del 1 al 21 de diciembre de 2019, llegó a un punto máximo de 53,14 MBPS y del 18 al 26 de enero

[7] Posterior a la revisión del enlace, este pasó de una capacidad de 10 a 30 MBPS
[8] Se refiere al enlace que permite la conexión con los servicios de internet banking y app del Banco.

de 2020, registró como punto máximo, 43,15 MBPS, operando a más del 100%, ante la mayor utilización de canales digitales, como ha sido la tendencia.

Aumentos de capacidades en canales de servicio: El enlace de Webbanking (línea 1739-4529) se aumentó de 50 a 300 MBPS, justificado[9] en que existe una "saturación porque los clientes utilizan el acceso Web y la App Móvil del Banco, además, que los clientes realizan ahora los trámites de forma remota", no obstante, según los datos promedio del enlace de los últimos meses, el consumo de ancho de banda se encuentra muy por debajo de su capacidad, tal y como se muestra a continuación:

Cuadro No. 2
Comportamiento del enlace

Mes	Enlace de Recepción (MBPS)		Enlace de Transmisión (MBPS)	
	Promedio	Máximo	Promedio	Máximo
Marzo	1,84	2,76	13,58	22,76
Abril	2,09	4,19	20,51	47,27
Mayo	2,31	11,53	20,64	152,30

Fuente: Creación propia a partir de información facilitada por el Área de Redes y Telecomunicaciones desde la herramienta Cacti.

El costo mensual de los 300 MBPS es de $3.248,75 para un plazo contratado de 12 meses, mientras el costo mensual de 50 MBPS es de $1.865.

Del cuadro anterior se desprende para el enlace de 300 MBPS:

- El punto máximo a nivel del enlace de transmisión en mayo 2020 fue de 152,30 MBPS, siendo este el dato más cercano a la capacidad dada del enlace, aunque muy por encima de otros máximos, sin determinarse a que se debió ese "pico".
- El resto de los datos en el cuadro anterior, se alejan de la capacidad dada de 300 MBPS, lo que se traduce en una capacidad sobre estimada contratada.

Comunicaciones Unificadas y servicios en la nube: Actualmente se está desarrollando la tercera etapa de Comunicaciones Unificadas y se está dando un uso más intensivo de los servicios de nube de Office 365, ambas tendencias demandan un mayor consumo de recursos de red, especialmente en el uso de videoconferencias y salida a Internet, pese a ello, no se evidenció la existencia de estudios de capacidades para determinar el impacto en los enlaces de comunicación.

Al respecto, este despacho conoció que el Área de Redes y Telecomunicaciones está desarrollando algunas pruebas aprovechando una sustitución de Routers modelo ISR 4321 que cuentan con la tecnología denominada SD-WAN, la cual permite el traslado del tráfico desde el origen (una oficina) hasta Internet de forma directa, es decir, sin que el tráfico ingrese a la red interna del Banco; no obstante, pese a que con esta mejora se pueden mitigar problemas de saturación en los enlaces, se carece de un plan con actividades, responsables y fechas para su implementación.

[9] Oficio ART-59-2020 del 27 de marzo de 2020, del Área de Redes y Telecomunicaciones

El Área de Redes y Telecomunicaciones no aplica un proceso estructurado de análisis de la capacidad de los enlaces, aunado a limitaciones para realizar un monitoreo de servicios; razón por la cual, actualmente solo se verifica si se presenta un aumento del tráfico en los enlaces durante algún período no estandarizado y se tramita de oficio el incremento de capacidad de ancho de banda.

Al respecto, el **Marco de Trabajo de Referencia para el Gobierno y Administración de la Tecnología de Información Empresarial COBIT 5**, establece la siguiente práctica:

> ***BAI04.04 Supervisar y revisar la disponibilidad y la capacidad.***
> *Supervisar, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad. Identificar desviaciones respecto a las líneas de referencia establecidas. Revisar informes de análisis de tendencias identificando cualquier cuestión y variación significativa, iniciando acciones donde sea necesario y asegurando que se realiza el seguimiento de todas las cuestiones pendientes.*

Las situaciones identificadas no permiten determinar si los incrementos de capacidad en los enlaces son suficientes o por el contrario corresponden a erogaciones por capacidades no requeridas, lo que incrementa el riesgo de aumento de costos de operación injustificado en perjuicio de los intereses del Banco.

Recomendaciones
Para: Área Redes y Telecomunicaciones

6. Definir y aplicar, dentro de la Normativa de Monitoreo y Generación de Estadísticas de Red, criterios que permitan cuantificar y justificar la necesidad de realizar aumentos de los enlaces de comunicación de las oficinas y canales del Banco.

   Del análisis realizado, determinar si es factible:
   - Estandarizar la capacidad de los enlaces por tipo de oficina (Agencia, BP Total)
   - Gestionar los ajustes que corresponda, tanto para los enlaces de comunicación de las oficinas y de canales del banco, entre ellos, el Enlace de WebBanking

Fecha cumplimiento: 31/10/2020	**Nivel de Riesgo: Medio**	**TR: CI**

Para: División de Operación de Servicios

7. Coordinar los esfuerzos requeridos para que se ejecuten las acciones que corresponda para mejorar la capacidad de monitoreo de los servicios de comunicaciones unificadas y nube de Office 365, de manera que se pueda determinar el impacto en el enlace de navegación.

Fecha cumplimiento: 30/10/2020	**Nivel de Riesgo: Medio**	**TR: CI**

4. El manejo actual de los enlaces alternos de microondas no garantiza una continuidad del servicio

Se determinó la existencia de una desigualdad significativa entre la capacidad asignada al enlace principal de fibra óptica y el alterno de microondas.

Existen 17 oficinas con enlace de microondas, de las cuales 7 cuentan con un ancho de banda con una capacidad muy inferior respecto al enlace principal, como se muestra en el siguiente cuadro:

Cuadro No. 3
Capacidad del Enlace Alterno de Microondas

Nombre Agencia	Capacidad del enlace Primario de Fibra MBPS	Capacidad del enlace secundario de Microondas MBPS	Relación Capacidad enlace Secundario/Capacidad enlace Primario
Paseo Metropolí	6	2	33%
Paquera	4	2	50%
Monteverde	4	3	75%
Cariari, Guápiles	4	2	50%
Hatillo	8	2	25%
PeriCartago	4	2	50%
Jicaral	4	2	50%

Fuente: Creación propia a partir de información facilitada por el Área de Redes y Telecomunicaciones

Ante un escenario donde se presente la caída del enlace de fibra, el enlace de microondas operando al 100% de su capacidad (lo cual no es recomendable), puede soportar solo un porcentaje del tráfico. Los casos más significativos son la Agencia de Paseo Metrópoli y la de Hatillo, los cuales podrían soportar hasta un 33% y 25% de la capacidad del enlace principal, respectivamente.

Con el fin de ilustrar con mayor detalle lo anterior, para el IV Trimestre 2019 y I Trimestre 2020, se analizó el comportamiento del enlace principal para las agencias anteriores, según se observa de seguido:

Cuadro No. 4
IV Trimestre 2019
Capacidad del Enlace Alterno de Microondas

Agencia	Comportamiento del enlace principal de Fibra (recepción y transmisión)	¿Podría soportarlo el Enlace Alterno de Microondas?	Observaciones con respecto al Enlace de Microondas
Paseo Metrópoli	Recepción: Punto máximo de 2,92 MBPS	No	Porque llega hasta 2 MBPS
	Transmisión: Punto máximo de 1,17 MBPS	Sí	Operando al 70% de su capacidad
Hatillo	Transmisión: Punto máximo fue de 4.01 MBPS	No	Microondas llega hasta 2 MBPS

Fuente: Creación propia a partir de información facilitada por el Área de Redes y Telecomunicaciones.

Cuadro No. 5
I Trimestre 2020
Capacidad del Enlace Alterno de Microondas

Agencia	Comportamiento del enlace principal de Fibra (recepción y transmisión)	¿Podría soportarlo el Enlace Alterno de Microondas?	Observaciones con respecto al Enlace de Microondas
Paseo Metrópoli	Recepción: Promedio fue de 1,70 MBPS	Sí	Operando al 85% de su capacidad
	Recepción: Punto máximo fue de 3,27 MBPS	No	Porque llega hasta 2 MBPS
Hatillo	Transmisión: Punto máximo fue de 2,84 MBPS	No	Porque llega hasta 2 MBPS

Fuente: Creación propia a partir de información facilitada por el Área de Redes y Telecomunicaciones

Adicionalmente, se determinó para el primer cuatrimestre de 2020, 15 incidentes de caídas de los enlaces de microondas, según la información registrada en el Service Manager. El detalle es el siguiente:

Cuadro No. 6
Incidentes por Oficinas con Enlaces alternos de Microondas

Nombre Oficina	Cantidad de Incidentes
Cariari, Guápiles	2
Jacó	3
San Marcos, Tarrazú	2
Centro Negocios Heredia	2
Nosara	1
Jicaral	1
Tejar del Guarco	1
San Vito	2
Limón	1
Total	**15**

Fuente: Creación propia a partir de información facilitada por el Área de Redes y Telecomunicaciones.

De los 15 casos analizados donde se da la afectación del enlace de microondas, generalmente, la solución registrada es el traslado del incidente al proveedor, no obstante, no se evidenció un análisis de causa raíz en los casos donde se presentan incidentes de manera reiterada.

El uso de enlaces de microondas obedece a una restricción geográfica del proveedor RACSA para el traslado a enlaces de fibra óptica; sin embargo, no se evidencia un accionar más proactivo de parte del Área de Redes y Telecomunicaciones, para motivar una migración o dar trazabilidad a las gestiones realizadas por RACSA para el traslado de los enlaces de microonda a fibra.

Al respecto, el **Marco de Trabajo de Referencia para el Gobierno y Administración de la Tecnología de Información Empresarial COBIT 5**, establece la siguiente práctica:

DSS01.02 Gestionar servicios externalizados de TI.
Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio.

Si bien, el enlace de microondas podría gestionar el tráfico ante la caída del enlace primario de fibra, existe un riesgo de posible saturación si no se cuenta con la misma capacidad en ambos enlaces o bien si el enlace presenta inestabilidad en su disponibilidad, afectando los servicios ofrecidos al cliente en esas oficinas comerciales.

Recomendaciones
Para: Área de Redes y Telecomunicaciones

8. Dar un seguimiento efectivo al traslado de los enlaces de microondas a fibra para oficinas, evidenciando para ello, las acciones que garanticen dicho cambio, documentando y comunicando de forma periódica lo actuado a niveles superiores, en los informes de capacidad y disponibilidad de las redes.

Fecha cumplimiento: 30/11/2020	**Nivel de Riesgo: Medio**	**TR: CI**

IV. Equipo de Auditoria

EDGAR BOLAÑOS JARA (FIRMA)
Firmado digitalmente por EDGAR BOLAÑOS JARA (FIRMA)
Fecha: 2020.07.13 15:13:23 -06'00'

Director

GERARDO ENRIQUE ZUÑIGA HERNANDEZ (FIRMA)
Firmado digitalmente por GERARDO ENRIQUE ZUÑIGA HERNANDEZ (FIRMA)
Fecha: 2020.07.13 15:03:00 -06'00'

Auditor Supervisor

CARLOS ENRIQUE ARAYA GUZMAN (FIRMA)
Firmado digitalmente por CARLOS ENRIQUE ARAYA GUZMAN (FIRMA)
Fecha: 2020.07.13 14:54:07 -06'00'

Auditor Encargado

Ebj * gzh * cag * smg

Anexos
Minuta de Discusión

CBP-A2

Formulario: 4.2
Versión: 02
Fecha: agosto 2018

ACTA DE DISCUSIÓN
Informe borrador
ATI-86-2020

Reunión iniciada a las 14 horas del día 03 de julio de 2020, por medio de videoconferencia.

Representantes de la Administración
- Geoffrey Araya Gómez, Jefe División Operación de Servicios
- Daniels Hidalgo Jiménez, Jefe Área Seguridad Operativa Informática
- Sergio Cambronero Montero, Supervisor Área Redes y Telecomunicaciones
- Jorge Alfaro Casas, Jefe Área de Monitoreo

Representantes de la Auditoría Interna
- Carlos Araya Guzmán, Auditor Encargado Auditoría de TI
- Gerardo Zúñiga Hernández, Supervisor Auditoría de TI
- Edgar Bolaños Jara, Director Auditoría de TI

El propósito de esta reunión es efectuar la discusión, análisis y aceptación de las observaciones y recomendaciones expuestas en el informe borrador ATI-86-2020 sobre la "Evaluación de la Gestión de la disponibilidad y capacidad de la red de datos", brindando un espacio de discusión que promueva aclarar los hallazgos y recomendaciones, brindar argumentos adicionales para que sean valorados por la Auditoría (cuando aplique), proponer y acordar sobre los mecanismos de mitigación de riesgos por implementar, así como realizar ajustes de redacción que permitan una mejor comprensión del informe.

Es responsabilidad de ambas partes el diseño de soluciones prácticas y viables, siendo la Administración la responsable final del diseño del sistema de control interno en procura de mitigar los riesgos comunicados en el informe.

En caso de existir desacuerdo con los hallazgos aportados en el informe podrá acogerse a lo dispuesto en la Ley General de Control Interno 8292 artículos 36°, 37° y 38°.

A continuación, se procede a detallar el contenido del informe, incluyendo los comentarios, de la Administración y del equipo de auditoría, cuando corresponda; así como el establecimiento de las fechas de cumplimiento para todas las recomendaciones:

Comentarios relativos a las conclusiones

No existen aspectos relevantes por considerar en esta sección

1. Los usuarios del Banco presentan problemas de navegación a Internet de forma recurrente	***Riesgo Alto***

Número de recomendación: *01*

Daniels Hidalgo repasa los esfuerzos coordinados y desarrollados para la instalación del Force Point y AnyConnect, así como el problema de compatibilidad del Check Point con estas herramientas, considera que es necesaria la integración de diferentes áreas de TI para atacar los problemas de actualización observados en los equipos de usuario final, siendo este un elemento de peso para solucionar los problemas experimentados por los usuarios.

Gerardo Zúñiga reitera a partir de lo indicado en el hallazgo que origina esta recomendación No.1, que a pesar que los equipos de usuario final se mantienen actualizados, los problemas de conexión remota para acceso a la Intranet del Banco e Internet son persistentes, por ello, las prácticas de actualizaciones dirigidas a los equipos de usuario final y de desinstalación de Check Point, realmente no solucionan las afectaciones originadas por Force Point y AnyConnect.

Daniels Hidalgo en función del planteamiento de la recomendación No.1, considera que el Área de Seguridad Operativa Informática tiene la potestad para valorar si será necesario elevar o no, algún caso a los respectivos proveedores del Force Point y del AnyConnect y de valorar si se requiere del acompañamiento de otras áreas de TI.

Edgar Bolaños está de acuerdo con Daniels Hidalgo, considerando la necesidad de apoyarse en otras áreas de TI para cumplir lo recomendado, a la vez, le sugiere a Daniels, elevar a su respectiva Jefatura, los problemas que enfrente en caso de presentarse falta de colaboración de algún área e incluso, comunique de esto a la Auditoría de TI.

De la solicitud de Daniels Hidalgo de modificación de la recomendación No. 1, la Auditoría de TI lo considera razonable y la recomendación se replantea así:

> *"Identificar, analizar y gestionar la solución de la causa raíz de los incidentes relacionados con ForcePoint y AnyConnect.*
>
> *Valorar la participación de los proveedores de ForcePoint y AnyConnect u otras áreas de TI para atender la causa raíz".*

Fecha y plazo de cumplimiento: 31/01/2021
Funcionario que define la fecha: Daniels Hidalgo Jiménez

Número de recomendación: *02*

Geoffrey Araya solicita la inclusión de un trabajo conjunto con el Área de Atención al Cliente Interno para la atención de la recomendación. Se acepta la solicitud y se modifica el texto de la recomendación.

Geoffrey Araya menciona que en conversaciones con la Jefatura del Área Atención al Cliente Interno y para la atención de esta recomendación 2, se brindará el acompañamiento y se buscará a nivel presupuestario, la partida para lograr la capacitación respectiva para que esta área, pueda realizar un despliegue automatizado mediante la herramienta Microsoft Configuration Manager. Mediante estos despliegues automatizados, se pretende la instalación y desinstalación de agentes conforme lo pide la recomendación.

Geoffrey Araya considera necesaria la definición de un plan para atender la recomendación, que involucre tanto al Área Atención Cliente Interno, además de contar con el acompañamiento de las áreas de TI que se consideren necesarias.

La recomendación queda de la siguiente manera:

"En conjunto con el Área de Atención al Cliente Interno, desarrollar e implementar un plan con responsables, fechas y actividades para gestionar la instalación de las herramientas ForcePoint y VPN de AnyConnect a todos los usuarios que actualmente mantienen en sus equipos de cómputo el agente de CheckPoint.

Asegurar la desinstalación del agente de CheckPoint de Symantec de todos los equipos de usuario final".

Gerardo Zúñiga menciona que es necesario por ejemplo, valorar dentro del plan de implementación, las nuevas versiones que se liberen de las aplicaciones citadas en esta recomendación 2.

Geoffrey Araya cita la fecha del 17 de agosto de 2020 bajo la condición de entregar a dicha fecha, el plan que permita cumplir lo recomendado y que sea este plan, el que se tome de base para brindar la fecha definitiva de atención.

Edgar Bolaños concuerda con lo expresado por Geoffrey Araya, por ello, en primera instancia se recibirá el plan de implementación y del análisis del mismo, se tomará la decisión de la fecha de atención definitiva.

Fecha y plazo de cumplimiento: Fecha 17/08/2020
Funcionario que define la fecha: Geoffrey Araya Gómez

Número de recomendación: *03*

Gerardo Zúñiga manifiesta la necesidad de que TI conozca la capacidad de las plataformas ForcePoint y AnyConnect, en relación con la cantidad de sesiones concurrentes, con el fin de evitar problemas observados en el pasado con el Proxy TMG.

Daniels Hidalgo menciona que solicitará a los respectivos proveedores, el análisis documentado que permita la atención de la recomendación, lo anterior también es apoyado por Geoffrey Araya.

Fecha y plazo de cumplimiento: 31/01/2021
Funcionario que define la fecha: Geoffrey Araya Gómez

Número de recomendación: *04*

Jorge Alfaro menciona con respecto a la recomendación, que esquemas de monitoreo para AnyConnect y ForcePoint están fuera del alcance definido, de las herramientas seleccionadas y del manejo del licenciamiento del proyecto del NOC, el cual, por diferentes factores, se ha visto afectado a nivel de fechas de atención.

Geoffrey Araya expresa que el Área de Monitoreo fue creada bajo un alcance específico, que es necesario ir desarrollando un nivel de madurez en dicha área, considerando una ampliación en su alcance original, pero se requiere de tiempo para lograr dicha madurez.

A partir de los comentarios anteriores, Gerardo Zúñiga indica tanto para aspectos de alcance de las diferentes áreas de TI como de esta Auditoría, que áreas cuya labor primaria no sea el monitoreo, no pueden quedar exentas actualmente y a futuro, de realizar este tipo de actividades (de monitoreo).

Jorge Alfaro, partiendo de la explicación ya citada sobre el alcance del Proyecto NOC, solicita a la Auditoría de TI, replantear la recomendación bajo el entendido, que el Área de Monitoreo realizará un análisis para determinar la factibilidad de monitorear el AnyConnect y el ForcePoint y que será ese análisis, el que permita identificar si se amplía el alcance de lo recomendado, por ello, solicita se modifique la recomendación en estos términos, lo cual es de recibo por parte de la auditoría.

Jorge Alfaro solicita el 15 de noviembre de 2020 como la fecha para entregar el análisis de factibilidad solicitado, lo cual es aceptado por la Auditoría.

La recomendación modificada queda así:

> *"Realizar un análisis para determinar la factibilidad de desarrollar esquemas de monitoreo de la capacidad y desempeño para las herramientas Cisco AnyConnect y ForcePoint, con la finalidad de mejorar la comprensión e identificación de problemas en su comportamiento y uso y para el manejo de alertas en los equipos de usuario final".*

Fecha y plazo de cumplimiento: 15/11/2020
Funcionario que define la fecha: Jorge Alfaro Casas

2. El monitoreo del tráfico de datos de red no genera un valor agregado ***Riesgo Medio***

Número de recomendación: *05*

Sergio Cambronero menciona con respecto al Contrato No. 184-2017, que este no detalla ninguna cláusula asociada específicamente al monitoreo del servicio de redes, sino que en caso de requerir del mismo, se debe realizar la solicitud del servicio bajo la figura de un "consumo por demanda", además, concuerda Sergio con la Auditoría de TI en mejorar aspectos de monitoreo del tráfico de servicios y cita las tecnologías SD-WAN y DNA, ambas están siendo gestionadas por su área, la primera para el monitoreo de tráfico y la segunda, para gestionar incidentes que se presenten en la LAN.

Sergio argumenta que las recomendaciones 5 y 6 del Informe Borrador se pueden fusionar, lo cual es de recibo por parte de la auditoría.

2. El monitoreo del tráfico de datos de red no genera un valor agregado ***Riesgo Medio***

En función de los elementos anteriores, las recomendaciones 5 y 6 se agrupan bajo la nueva recomendación 5, que queda así:

"Gestionar las acciones que corresponda para la puesta en uso de herramientas que permitan:

- El monitoreo del tráfico asociado a servicios (telefonía VOIP, Streaming) y que suministren toda la información requerida por el Banco para un seguimiento adecuado del comportamiento de los enlaces
- La generación de reportes sobre eventos dentro y fuera de los patrones habituales y que contribuyan a una mejor comprensión de las actividades recurrentes que afectan las redes".

Fecha y plazo de cumplimiento: 31/10/2020
Funcionario que define la fecha: Sergio Cambronero Montero

Número de recomendación: *06*

A solicitud del Área de Redes y Telecomunicaciones, se unen las recomendaciones 5 y 6.

Fecha y plazo de cumplimiento: No aplica
Funcionario que define la fecha: No aplica

3. Ausencia de criterios para la definición justificada de la capacidad de los enlaces ***Riesgo Medio***
Número de recomendación: *07*

Gerardo Zúñiga indica que es necesaria la definición de criterios conforme lo establece la recomendación, con el fin de asegurar un manejo estandarizado de enlaces y que ese manejo estandarizado contribuya a que no haya afectación en los servicios institucionales, de no poderse dar un manejo estandarizado de enlaces, justificar los casos que corresponda.

Sergio Cambronero solicita unir las recomendaciones 7 y 8, considerando que el análisis del comportamiento del Enlace de WebBanking, así como de los enlaces de las oficinas comerciales (Agencias y BP Totales), puede realizarse como parte de las mismas acciones, además, solicita para la recomendación 7 que se haga referencia a la Normativa de Monitoreo y Generación de Estadísticas de Red.

Edgar Bolaños analiza los argumentos anteriores y aprueba lo solicitado por Sergio Cambronero.

3. Ausencia de criterios para la definición justificada de la capacidad de los enlaces	***Riesgo Medio***

La recomendación 7 queda de la siguiente manera:

> *"Definir y aplicar, dentro de la Normativa de Monitoreo y Generación de Estadísticas de Red, criterios que permitan cuantificar y justificar la necesidad de realizar aumentos de los enlaces de comunicación de las oficinas y canales del Banco.*
>
> *Del análisis realizado, determinar si es factible:*
> - *Estandarizar la capacidad de los enlaces por tipo de oficina (Agencia, BP Total)*
> - *Gestionar los ajustes que corresponda, tanto para los enlaces de comunicación de las oficinas y de canales del banco, entre ellos, el Enlace de WebBanking"*

Fecha y plazo de cumplimiento: 31/10/2020
Funcionario que define la fecha: Sergio Cambronero Montero

Número de recomendación: 08

Gerardo Zúñiga expresa que es necesario que exista claridad al momento de justificar los aumentos de capacidades de enlaces y cuando proceda, sus disminuciones.

A solicitud del Área de Redes y Telecomunicaciones, se unen las recomendaciones 7 y 8.

Fecha y plazo de cumplimiento: No aplica
Funcionario que define la fecha: No aplica

Número de recomendación: *09*

Sergio Cambronero solicita la reasignación de la recomendación a la División de Operación de Servicios, dado que según argumenta se requiere de la colaboración del Área Seguridad Operativa Informática para su atención oportuna.

Debido que al momento de la solicitud de reasignación no se contaba con la presencia de la jefatura de la División de Operación de Servicios, se acuerda, realizar una sesión adicional con ambas jefaturas para discutir la reasignación de la recomendación.

Fecha y plazo de cumplimiento: Pendiente
Funcionario que define la fecha: Pendiente

4. El manejo actual de los enlaces alternos de microondas no garantiza una continuidad del servicio	***Riesgo Medio***

Número de recomendación: *10*

Sergio Cambronero solicita se agregue a la recomendación "para oficinas", con el fin que se tenga definido que está fuera del alcance de la recomendación el manejo de enlaces de los Cajeros Automáticos en islas, ante ello, Gerardo Zúñiga concuerda con Sergio y se modifica la recomendación de la siguiente manera:

4. El manejo actual de los enlaces alternos de microondas no garantiza una continuidad del servicio ***Riesgo Medio***

"Dar un seguimiento efectivo al traslado de los enlaces de microondas a fibra para oficinas, evidenciando para ello, las acciones que garanticen dicho cambio, documentando y comunicando de forma periódica lo actuado a niveles superiores, en los informes de capacidad y disponibilidad de las redes".

Fecha y plazo de cumplimiento: Fecha 30/11/2020
Funcionario que define la fecha: Sergio Cambronero Montero

Al ser las 17 horas, finaliza la reunión celebrada para la discusión verbal de los resultados emitidos en el informe borrador mencionado en la primera página de este documento.

Leído el documento a los presentes, se acepta la minuta.

REPRESENTANTES DE LA ADMINISTRACIÓN

Nombre: Geoffrey Araya Gómez		
Jefe División Operación de Servicios **Puesto**	Firmado digitalmente por GEOFFREY MARTIN ARAYA GOMEZ (FIRMA) Fecha: 2020.07.09 08:56:49 -06'00' **Firma** "Esta firma valida mi participación y comentarios incluidos en la presente acta de discusión"	03/07/2020 **Fecha**

Nombre: Daniels Hidalgo Jiménez		
Jefe Área Seguridad Operativa Informática **Puesto**	DANIELS HIDALGO JIMENEZ (FIRMA) Firmado digitalmente por DANIELS HIDALGO JIMENEZ (FIRMA) Fecha: 2020.07.13 09:26:36 -06'00' **Firma** "Esta firma valida mi participación y comentarios incluidos en la presente acta de discusión"	03/07/2020 **Fecha**

Nombre: Sergio Cambronero Montero		
Supervisor Área Redes y Telecomunicaciones **Puesto**	SERGIO CAMBRONERO MONTERO (FIRMA) Firmado digitalmente por SERGIO CAMBRONERO MONTERO (FIRMA) Fecha: 2020.07.09 14:09:26 -06'00' **Firma** "Esta firma valida mi participación y comentarios incluidos en la presente acta de discusión"	03/07/2020 **Fecha**

Nombre: Jorge Alfaro Casas		
Jefe Área de Monitoreo **Puesto**	JORGE ARTURO ALFARO CASAS (FIRMA) Firmado digitalmente por JORGE ARTURO ALFARO CASAS (FIRMA) Fecha: 2020.07.08 14:58:00 -06'00' **Firma** "Esta firma valida mi participación y comentarios incluidos en la presente acta de discusión"	03/07/2020 **Fecha**

REPRESENTANTES DE LA AUDITORÍA INTERNA

Nombre: Carlos Araya Guzmán		
Auditor Encargado Auditoría de TI **Puesto**	CARLOS ENRIQUE ARAYA GUZMAN (FIRMA) Firmado digitalmente por CARLOS ENRIQUE ARAYA GUZMAN (FIRMA) Fecha: 2020.07.08 12:20:42 -06'00' **Firma**	03/07/2020 **Fecha**

Nombre: Gerardo Zúñiga Hernández		
Supervisor Auditoría de TI **Puesto**	GERARDO ENRIQUE ZUÑIGA HERNANDEZ (FIRMA) Firmado digitalmente por GERARDO ENRIQUE ZUÑIGA HERNANDEZ (FIRMA) Fecha: 2020.07.10 19:10:27 -06'00' **Firma**	03/07/2020 **Fecha**

CBP-A2

CONSTRUIMOS BIENESTAR

Popular Sociedad Agencia de Seguros · Popular Valores · Popular Pensiones · Popular Fondos de Inversión

Banco Popular

Formulario: 4.2
Versión: 02
Fecha: agosto 2018

Nombre: Edgar Bolaños Jara		
Director Auditoría de TI **Puesto**	EDGAR BOLAÑOS JARA (FIRMA) Firmado digitalmente por EDGAR BOLAÑOS JARA (FIRMA) Fecha: 2020.07.10 20:14:59 -06'00' **Firma**	03/07/2020 **Fecha**

CBP-A2

CONSTRUIMOS BIENESTAR

Formulario: 4.2
Versión: 02
Fecha: agosto 2018

ACTA DE DISCUSIÓN
Informe borrador
ATI-86-2020

Reunión iniciada a las 10 horas del día 09 de julio de 2020, por medio de videoconferencia.

Representantes de la Administración
- Geoffrey Araya Gómez, Jefe División Operación de Servicios
- Sergio Cambronero Montero, Supervisor Área Redes y Telecomunicaciones

Representantes de la Auditoría Interna
- Carlos Araya Guzmán, Auditor Encargado Auditoría de TI
- Gerardo Zúñiga Hernández, Supervisor Auditoría de TI
- Edgar Bolaños Jara, Director Auditoría de TI

El propósito de esta reunión es efectuar la discusión, análisis y aceptación de las observaciones a la recomendación No.9 del informe borrador ATI-86-2020 sobre la "Evaluación de la Gestión de la disponibilidad y capacidad de la red de datos", brindando un espacio de discusión que promueva aclarar los hallazgos y dicha recomendación, brindar argumentos adicionales para que sean valorados por la Auditoría (cuando aplique), proponer y acordar sobre los mecanismos de mitigación de riesgos por implementar, así como realizar ajustes de redacción que permitan una mejor comprensión del informe.

Es responsabilidad de ambas partes el diseño de soluciones prácticas y viables, siendo la Administración la responsable final del diseño del sistema de control interno en procura de mitigar los riesgos comunicados en el informe.

En caso de existir desacuerdo con los hallazgos aportados en el informe podrá acogerse a lo dispuesto en la Ley General de Control Interno 8292 artículos 36°, 37° y 38°.

Esta minuta es de complemento a la primera minuta generada que abarcó la mayoría de las recomendaciones registradas en el Informe Borrador ATI-86-2020, quedando pendiente de análisis, la recomendación 09, por ello, se procede a detallar los comentarios, de la Administración y del equipo de auditoría, cuando corresponda; así como el establecimiento de la fecha de cumplimiento de esta recomendación:

3 Ausencia de criterios para la definición justificada de la capacidad de los enlaces	**Riesgo Medio**

Número de recomendación: *09*

Debido a la que recomendación inicialmente estaba asignada al Área de Redes y Telecomunicaciones, Sergio Cambronero solicita la reasignación de la recomendación a la División de Operación de Servicios, Geoffrey Araya acepta dicha reasignación.

SD-WAN permite el monitoreo de los servicios citados en la recomendación, incluso especificando por tipo de aplicación, el comportamiento de las aplicaciones dentro del respectivo enlace, pero aclara Sergio Cambronero, que la puesta en producción de esta tecnología requiere del involucramiento de otras áreas de TI, entre ellas, el Área Seguridad Operativa Informática, de la cual, el Área de Redes y Telecomunicaciones, requiere información asociada a especificaciones sobre la configuración del Servicio Proxy y de políticas de seguridad, entre otros puntos.

Geoffrey Araya cita la necesidad de ir aumentando el nivel de madurez y el alcance de las actividades asignadas al Área de Monitoreo, por lo que considera conveniente en función de lo requerido por la recomendación, que sea el Área de Monitoreo quien realice labores de monitoreo de los servicios de comunicaciones unificadas y de nube de Office 365 y desligar al Área de Redes y Telecomunicaciones de estas labores de monitoreo.

Gerardo Zúñiga le aclara a Geoffrey Araya que justamente el alcance del monitoreo de las comunicaciones unificadas y de nube de Office 365, es una tarea que la División Operación de Servicios debe analizar con las respectivas áreas.

Geoffrey Araya retoma lo ya mencionado con respecto a la necesidad de reasignar al Área de Monitoreo, las labores de monitoreo de los servicios observados en la recomendación.

Ante la consulta de Geoffrey Araya sobre el alcance para la atención del monitoreo de los servicios de comunicaciones unificadas y de nube de Office 365, Gerardo Zúñiga aclara que la División Operación de Servicios puede analizar y definir el respectivo alcance.

Geoffrey Araya, considerando la necesidad de coordinar con el Área Seguridad Operativa Informática, el Área de Monitoreo y el Área de Redes y Telecomunicaciones, las tareas requeridas, solicita el 30 de octubre de 2020 para la atención de la recomendación, con el fin de entregar a esa fecha, el respectivo plan de trabajo que detalle las actividades, plazos y fechas que permitan la atención definitiva de la recomendación.

Por acuerdo entre las partes, se modifica la recomendación bajo análisis, quedando la misma así:

Coordinar los esfuerzos requeridos para que se ejecuten las acciones que corresponda para mejorar la capacidad de monitoreo de los servicios de comunicaciones unificadas y nube de Office 365, de manera que se pueda determinar el impacto en el enlace de navegación.

Fecha y plazo de cumplimiento: 30/10/2020
Funcionario que define la fecha: Geoffrey Araya Gómez

Al ser las 10,45 horas, finaliza la reunión celebrada para la discusión verbal de la recomendación No.9 del informe borrador mencionado en la primera página de este documento.

Leído el documento a los presentes, se acepta la minuta.

CBP-A2

CONSTRUIMOS BIENESTAR

Popular Sociedad Agencia de Seguros | Popular Valores | Popular Pensiones | Popular Fondos de Inversión

Banco Popular

Formulario: 4.2
Versión: 02
Fecha: agosto 2018

REPRESENTANTES DE LA ADMINISTRACIÓN

Nombre: Geoffrey Araya Gómez		
Jefe División Operación de Servicios **Puesto**	Firmado digitalmente por GEOFFREY MARTIN ARAYA GOMEZ (FIRMA) Fecha: 2020.07.10 14:46:19 -06'00' **Firma** "Esta firma valida mi participación y comentarios incluidos en la presente acta de discusión"	09/07/2020 **Fecha**

Nombre: Sergio Cambronero Montero		
Supervisor Área Redes y Telecomunicaciones **Puesto**	SERGIO CAMBRONERO MONTERO (FIRMA) Firmado digitalmente por SERGIO CAMBRONERO MONTERO (FIRMA) Fecha: 2020.07.10 22:10:06 -06'00' **Firma** "Esta firma valida mi participación y comentarios incluidos en la presente acta de discusión"	09/07/2020 **Fecha**

REPRESENTANTES DE LA AUDITORÍA INTERNA

Nombre: Carlos Araya Guzmán		
Auditor Encargado Auditoría de TI **Puesto**	CARLOS ENRIQUE ARAYA GUZMAN (FIRMA) Firmado digitalmente por CARLOS ENRIQUE ARAYA GUZMAN (FIRMA) Fecha: 2020.07.09 14:18:37 -06'00' **Firma**	09/07/2020 **Fecha**

Nombre: Gerardo Zúñiga Hernández		
Supervisor Auditoría de TI **Puesto**	GERARDO ENRIQUE ZUÑIGA HERNANDEZ (FIRMA) Firmado digitalmente por GERARDO ENRIQUE ZUÑIGA HERNANDEZ (FIRMA) Fecha: 2020.07.13 08:18:08 -06'00' **Firma**	09/07/2020 **Fecha**

Nombre: Edgar Bolaños Jara		
Director Auditoría de TI **Puesto**	EDGAR BOLAÑOS JARA (FIRMA) Firmado digitalmente por EDGAR BOLAÑOS JARA (FIRMA) Fecha: 2020.07.13 09:33:59 -06'00' **Firma**	09/07/2020 **Fecha**