PAS-036/2016

Superintendencia del Sistema Financiero, en la ciudad de San Salvador, a las quince horas y treinta y seis minutos del día veinticinco de mayo de dos mil dieciocho.

El presente Procedimiento Administrativo Sancionador inició de forma oficiosa por medio de auto pronunciado el día diecinueve de julio del dos mil dieciséis, en contra de **BANCO G&T CONTINENTAL EL SALVADOR, S.A.**, en adelante el "Banco" o la "Supervisada" indistintamente, con el propósito de determinar si existe o no responsabilidad respecto de los incumplimientos relacionados en el Memorándum DR-004/2016, de fecha nueve de febrero de dos mil dieciséis y sus respectivos anexos, remitidos por la Dirección de Riesgos, en el que se evidenció que:

1) lincumplimiento al artículo 3 literal a) de las Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50), por haberse determinado que el Banco no posee procedimientos claramente definidos, que le permitan dar atención oportuna y manejar adecuadamente las notificaciones de alertas ante eventos inusuales; tal es el caso de la falta de atención y manejo de alertas generadas por Mastercard, el día veintiséis de diciembre de dos mil quince, por movimientos inusuales efectuados ese día con tarjetas de débito de clientes del Banco.

2) incumplimiento al articulo 36 literal c) de las Normas Técnicas sobre Obligaciones de las Sociedades Clasificadoras de Riesgo (NRP-07), por haberse determinado la falta de plan de sucesión del personal encargado de recibir las alertas y de medios alternativos de comunicación para la atención de las mismas, siendo que ante la ausencia del personal responsable de recibir alertas de Mastercard, no existió delegación de las responsabilidades a una persona sustituta; no suministrando el Banco de canales de comunicación alternos:

3) incumplimiento a lo dispuesto en el articulo 3 letra d) de las Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50), en relación al artículo 63 de la Ley de Bancos.

Según los hallazgos detallados a continuación, logró identificarse que los proyectos de políticas y sistemas de control a los que hacen referencia las disposiciones citadas, fueron iniciados con posterioridad al evento en cuestión:

A) Falta de monitoreo a comportamiento transaccional del cliente.

Se identifico que el Banco no posee un sistema integral de monitoreo de comportamiento transaccional del cliente que tenga mecanismos de identificación de operaciones inusuales y alertas tempranas; para el caso de fraude en referencia, se originaron transacciones en Japón por montos a partir de mil dólares ($1,000.00), sin que el mismo fuera alertado internamente sobre la inusualidad.

B) Falta de validación adicionales a nivel de marca de tarjetas o procesador.

Se identificó que el Banco no posee un sistema de monitoreo en tiempo real de transacciones y validaciones de reglas respecto a parámetros de tarjetas, tales como bines, límites de retiros y compras, vencimiento de tarjetas, entre otros, que pueda efectuarse a nivel de marca (Mastercard) ó procesador, reduciendo el flujo de transacciones que no cumplen los referidos parámetros, y que puedan ser recibidas y autorizadas por el mismo en circunstancias inusuales y ser rechazadas a ese nivel.

4) incumplimiento al articulo artículo 12 de las Normas para Gestión del Riesgo Operacional de las Entidades Financieras, NPB4-50, en relación al artículo 63 de la Ley de Bancos; por haberse determinado la falta de políticas de mantenimiento y respaldo de las bitácoras de eventos de sistemas operativos y aplicaciones en los servidores por parte del Banco, como lo advertido en el servidor FEP (Pamplona) involucrado en el evento; el cual no contaba con los registros de las bitácoras (logs) de la fecha veintiséis de diciembre de dos mil quince y fechas anteriores. Asimismo, se identificó que el nuevo servidor FEP (Rosarito) puesto en

producción desde el veinticinco de enero de dos mil dieciséis, que a la fecha de esta visita de inspección, la configuración en el registro de logs cuenta con capacidad de almacenar 20MB, por lo que de superar la capacidad de almacenamiento el sistema borra los logs más antiguos.

Falta de medidas de seguridad en las redes especializadas de prestación de servicios, debido a que el Banco mantuvo expuesto en una red de menor seguridad la Base de Datos del Sistema FEP, el cual antes de la fecha veinticinco de enero de dos mil dieciséis, el referido sistema y la base de datos se encontraban en un mismo servidor (Pamplona).

Se identificó que el supervisado no cuenta con políticas de monitoreo, mantenimiento y respaldo de logs de los equipos de seguridad, debido que los firewall no contaban con registros de logs a la fecha de la visita; además se observó que el Banco utiliza canales sin cifrado de datos, para la transferencia de información confidencial de sus clientes, tal es el caso del enlace que tiene con la empresa Promoción y Operación, S.A. de C.V., que presta al Banco el servicio de liquidación de transacciones de tarjeta de débito, por lo que existe el riesgo que esta vulnerabilidad sea aprovechada.

5) incumplimiento al artículo 3 literal c) de las Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50); por haberse determinado el uso de aplicaciones desactualizadas sin soporte del fabricante, verificando que El Banco no cuenta con políticas y planes de renovación de infraestructura tecnológica relacionada con la seguridad al mantener en producción un servidor con sistema operativo y base de datos sin soporte del fabricante, debido a que el servidor (Pamplona) contaba con el sistema operativo Microsoft Windows 2003 Server y Microsoft SQL 2000 que estaban desactualizados y fuera de soporte del fabricante.

Que la aplicación FEP instalada en el nuevo servidor (Rosarito), ha sido desarrollada Visual Basic 6.0, no cuenta con soporte del fabricante Microsoft desde el año 2008, por lo que aun podría estar expuesto a vulnerabilidades generadas por aplicaciones sin soporte.

La plataforma tecnológica del sistema Solx "core bancario" (ASTATO y MANDEVILLE), tienen instalado el sistema operativo Microsoft Windows Server 2003 R2, el cual está fuera de soporte del fabricante, lo que expone al riesgo que vulnerabilidades sean explotadas afectando la continuidad de las operaciones y la seguridad de la información.

El suscrito, en base a sus facultades establecidas en los artículos 4 literal i), 19 literal g) y 55 de la Ley de Supervisión y Regulación del Sistema Financiero, efectúa las siguientes **CONSIDERACIONES:**

A. PROCEDIMIENTO SANCIONATORIO

I. Visto el contenido del Memorándum N° DR-ROT-0224/2017, antes relacionado y la documentación probatoria anexa al mismo, por medio de auto de fecha diecinueve de julio de dos mil dieciséis, se ordenó instruir el presente Procedimiento Administrativo Sancionador y emplazar a **BANCO G&T CONTINENTAL EL SALVADOR, S.A.**, informando al mismo sobre el contenido de los incumplimientos atribuidos; lo cual se llevó a cabo en legal forma en fecha diecinueve de septiembre del mismo año; incorporado de folios uno a folio ciento trece.

II. La Supervisada hizo uso de su derecho de audiencia compareciendo en el presente Procedimiento Administrativo Sancionador a través de Apoderado General Judicial, con escrito de fecha veintiocho de septiembre de dos mil dieciséis, contestando en sentido negativo los señalamientos realizados; incorporado de folios ciento catorce a ciento veintiuno.

III. Mediante auto de fecha diecinueve de octubre de dos mil dieciséis, esta Superintendencia tuvo como parte al Apoderado General Judicial de **BANCO G&T CONTINENTAL EL SALVADOR, S.A.**, abriendo a pruebas el presente Procedimiento, así como también se requirió a la Dirección de Análisis de Entidades, remitir los últimos estados financieros

presentados por la Supervisada, determinando sobre estos la capacidad y solvencia económica del mismo; cuyo auto se notificó respectivamente el día veintiocho y veintinueve de diciembre del mismo año. Incorporado de folios ciento veintidós a ciento veinticuatro.

IV. Que mediante informe No. DAE-001-2017, de fecha tres de enero de dos mil diecisiete, la Dirección de Análisis de Entidades, remitió el análisis de la capacidad económica de **BANCO G&T CONTINENTAL EL SALVADOR, S.A.**, incorporado de folios ciento veinticinco a ciento veintinueve.

V. Que dentro del término probatorio el Licenciado Raúl Ernesto Pineda Merino, Apoderado General Judicial del Banco, presento escrito de fecha cinco de enero de dos mil diecisiete, incorporando como prueba de descargo copias simples de: 1) Procedimiento para Monitoreo Transacciones de Tarjetas de Debito, 2) Lineamientos Para entrega de Puesto, 3) Plan de Sucesión y 4) Políticas de Tecnología de Información, realizadas por **BANCO G&T CONTINENTAL EL SALVADOR, S.A.**

Así mismo, solicitó se realice inspección de ampliación los informes DR-004/2016 y DR-ROT-015/2016, aclarando: 1) Si el Banco para la fecha de la inspección contaba o no con el documento "Procedimiento para Monitoreo de Transacciones de Tarjeta de Debito", y si tiene relación o no con el art. 3 literal a) de las NPB4-50; 2) si los documentos "Lineamientos para la Entrega de Puesto", del año 2010 y el "Plan de Sucesión", de marzo 2015; vigentes al veintiséis de diciembre de dos mil quince, que en esa fecha presento el Banco fueron o no requeridos específicamente y si tienen o no que ver su contenido con el art. 3 literal b) de la NPB4-50; y 3) aclare si los proyectos en ejecución, que se les informo durante la inspección, se verificaron que se trataban de proyectos para reforzar y renovar la infraestructura que ya soportaba el modelo de monitoreo transaccional, si se verifico o no la existencia del Safety Net (MasterCard). Incorporado de folios ciento treinta a doscientos treinta y cuatro.

VI. Con auto de fecha seis de febrero de dos mil diecisiete, se requirió a la Dirección de Riesgos verificar los aspectos planteados en los numerales 1, 2 y 3 del escrito que antecede, señalando para realizar dicha inspección el día nueve de agosto del año en curso; notificada

el siete y ocho de agosto del año en curso. Incorporado a folios doscientos treinta y cinco a doscientos cuarenta y dos.

VII. Que mediante Memorándum N° DR-ROT-0224/2017, de fecha dos de octubre de dos mil diecisiete, la Dirección de Riesgos, rindió Informe por ampliación de inspección a **BANCO G&T CONTINENTAL EL SALVADOR, S.A.**, requerida en auto de fecha seis de febrero de dos mil diecisiete. Incorporado a folios doscientos cuarenta y tres a doscientos cincuenta y cuatro.

VIII. Con auto de fecha diez de noviembre de dos mil diecisiete, se ordeno remitir a **BANCO G&T CONTINENTAL EL SALVADOR, S.A.**, copia del informe N° DR-ROT-0224/2017 y sus respectivos anexos, a efecto de que pueda pronunciarse sobre el mismo en el plazo de cinco días hábiles; notificado el cuatro de enero de dos mil dieciocho. Incorporado a folios doscientos cincuenta y cinco a doscientos cincuenta y seis.

IX. Que el Licenciado Raúl Ernesto Pineda Merino, Apoderado General Judicial del Banco, presento escrito de fecha diez de enero de dos mil dieciocho, pronunciándose sobre Informe N° DR-ROT-0224/2017, solicitando se absuelva a su representado **BANCO G&T CONTINENTAL EL SALVADOR, S.A.**. Incorporado a folio doscientos cincuenta y siete.

X. Por resolución de las quince horas con treinta y cinco minutos del día quince de enero de dos mil dieciocho, se agrego el escrito referido en numeral que antecede. Incorporado al folio doscientos cincuenta y ocho.

XI. Por medio de auto emitido el día treinta de abril de dos mil dieciocho se requirió nuevo informe a la Dirección de Análisis de Entidades en el que reflejara la información actualizada sobre la capacidad económica del **BANCO G&T CONTINENTAL EL SALVADOR, S.A.** determinando con base a los estados financieros auditados al 31 de diciembre de 2017, elemento necesario para ser considerado eventualmente en la resolución final del presente procedimiento; dicho auto fue notificado a la referida Dirección el dos de mayo del año 2018 y

al Banco con fecha cuatro de mayo del corriente año. Incorporado de folio doscientos cincuenta y nueve al doscientos sesenta y uno.

XII. Por medio de informe No. DAE-167-2018 de fecha 14 de mayo de 2018, proveniente de la Dirección de Análisis de Entidades se informó sobre el análisis de la capacidad económica de **BANCO G&T CONTINENTAL EL SALVADOR, S.A.** con referencia al 31 de diciembre de 2017. Incorporado de folio doscientos sesenta y dos al doscientos sesenta y ocho.

XIII. Por medio de auto de las quince horas con cuarenta minutos del día veintidós de mayo de dos mil dieciocho, se agrego Informe referido en numeral anterior No. DAE-167-2018; y se ordeno emitir la resolución final correspondiente. Incorporado en folio doscientos sesenta y nueve.

B. ANALISIS DEL CASO Y ARGUMENTOS SOBRE CADA INFRACCIÓN

I. Sobre la presunta violación al artículo 3 literal a) de las Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50).

El Banco, manifestó contaba con procedimiento para la atención de alertas con patrón fraudulento, vigente desde el mes de mayo dos mil quince, denominado "*Procedimiento Para Monitoreo de Transacciones de Tarjeta de Debito*"; aclarando que como resultado del evento suscitado el día veintiséis de diciembre de dos mil quince, el Banco procedió a actualizar dicho procedimiento, ampliando el alcance de los eventos de fraude con una matriz de escalonamiento más amplia que permite contactar oportunamente al personal del Banco, quedando vigente a partir de febrero dos mil dieciséis. Razón por la que solicita la ampliación de informes DR-004/2016 y DR-ROT-015/2016, en el sentido de expresar si para la fecha de inspección el Banco contaba o no con el documento "*Procedimiento para Monitoreo de Transacciones de Tarjeta de Debito*", si constituye un aspecto concerniente a la gestión de factores generadores de riesgo operacional y si se solicito o no al Banco en ocasión de la inspección presentar instrumentos que permitieran concluir que se había atendido lo exigido en el art. 3 literal a) de las NPB4-50.

La Dirección de Riesgos verifico los puntos planteados por el Banco a través de inspección el día nueve de agosto del mismo año; plasmando el detalle de la misma en Informe N° DR-ROT-0224/2017 y concluyendo con base a la verificación realizada, la reconfirmación de lo planteado en Informe DR-ROT-014/2016.

El Banco a través de su apoderado, con escrito de fecha diez de enero de dos mil dieciocho, expresa que la delegada en el informe N° DR-ROT-0224/2017, concluye que el "*Procedimiento para Monitoreo de Transacciones de Tarjeta de Debito*", no aplica para atender alertas con patrón fraudulentos inusuales, pues no tiene disposiciones que indiquen en qué casos se aplica y en qué casos no; afirmación subjetiva al definir que no aplica para el caso de autos, no siendo la funcionaria delegada para la inspección facultada el determinar a qué caso le va a aplicar el instrumento y a cual caso no. Situación que demuestra la no existencia de la infracción atribuida al Banco, ya que contaba con el instrumento requerido en la Norma.

Al respecto, se aclara que el incumplimiento señalado es en razón a la falta por parte del Banco de procedimientos claramente definidos para dar atención oportuna y manejo adecuado de notificaciones de alertas ante eventos inusuales; y no la existencia o no de dicho procedimiento; puesto que el hecho que exista un documento que dicte un proceder pero que no da parámetros determinantes y precisos de cómo y cuándo será su aplicación; deficiencia que es reconocida por el apoderado del Banco al indicar que "*esto resulta por que el documento no tiene disposiciones que indiquen en qué casos se aplica y en qué casos no y menos que no aplique al que nos ocupa, de modo que el informe DR-ROT-0224/2017, es subjetivo al definir que no aplica para el caso de autos*", situación que en temas de riesgos no es tolerable, puesto que al no tener definidos de manera precisa y clara dichos parámetros es imposible garantizar un correcto proceder y adecuado manejo de las situaciones inusuales que se puedan presentar.

Situación que fue demostrada con suceso acontecido el día veintiséis de diciembre de dos mil quince, cuya falta de procedimiento pre-establecido de manera puntual y bien definida para la atención y manejo de alertas generadas por Mastercard, por 1,094 transacciones inusuales de tarjetas de debito de clientes del Banco, por un monto de $915,741.68, realizadas con 139 números de tarjetas de debito, utilizando 206 ATM´s, efectuadas en la ciudad de Tokio, Japón.

Evidenciando de forma real en la aplicación transaccional diaria realizada por el Banco, que no posee procedimientos claramente definidos, que le permitan dar atención oportuna y manejar adecuadamente las notificaciones de alertas ante eventos súbitos.

Contexto que es reconfirmado con el cruce de correos internos remitidos de forma insistente entre Centro de Monitoreo, Desarrollo de Sistemas, Canales Electrónicos, Operaciones y Administración, Administración de Sistemas, los días sábado veintiséis, domingo veintisiete y lunes veintiocho de diciembre; no pudiendo identificar los números de tarjetas en el lapso de tres días, ni realizar su bloqueo, ya que cada uno de los departamentos buscaba determinar en el otro el responsable de proceder a realizar el bloqueo correspondiente, al no tener un área definida y personal de turno responsable identificado de forma clara en un procedimiento de monitoreo.

Observaciones planteadas ante el Banco en la visita de inspección, llevando a este a adicionar el procedimiento de tarjetas de debito, al monitoreo de transacciones fraudulentas, así mismo efectuaron mejoras al proceso de recepción de alertas de MasterCard, el cual estaría finalizado al treinta y uno de marzo de dos mil dieciséis; según lo manifestado en nota de fecha veintinueve de febrero de dos mil dieciséis.

En base a lo antes expuesto el suscrito considera que ha existido incumplimiento a las disposiciones mencionadas, por lo que se puede determinar responsabilidad administrativa para el Banco.

II. Sobre la presunta violación al artículo 3 literal b) de las Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50).

El Banco Manifestó contar con manuales y procedimientos para la desvinculación de colaboradores, como son: "*Lineamientos para la Entrega de Puesto*", del 2010 y "Plan *de Sucesión*", del 2015; sin embargo, dichos documentos no fueron requeridos en la inspección generada por esta Superintendencia, debido a que el análisis fue realizado enfocándose en listado de contactos de MasterCard, administrado por el área de Canales Electrónicos y que no tiene relación con los procesos de Recursos Humanos.

Al respecto, si bien el Banco contaba con procedimientos para la entrega de puesto y de sucesión, estos son desde el enfoque del elemento humano propio del Departamento de Recursos Humanos, no de la prevención, manejo y control de Riesgos Operacionales, como el acontecido el veintiséis de diciembre de dos mil quince, en el cual la evidente falta de un plan de sucesión del personal encargado de recibir las alertas y de medios alternativos de comunicación para la atención de las mismas llevo al cruce de correos entre diferentes cargos ejecutivos del Banco, sin llegar a una solución efectiva y en tiempo real de los acontecimientos, puesto que el elemento con poder de decisión como es el Gerente de Operaciones y Administración, se encontraba de vacaciones fuera del país y no tenia cobertura telefónica en el mismo; asimismo, tenia configurado las notificaciones de alertas al correo electrónico y número telefónico fijo de oficina.

De igual manera el Jefe de Canales Electrónicos, quien sucedería en puesto al primero, tenía configurado las notificaciones de alertas al correo electrónico y número telefónico fijo de oficina. Lo que no es en ningún momento funcional, considerando que el evento origen del presente proceso sucedió fuera de horas hábiles, haciendo imposible comunicarse con ambos por cualquier medio en tiempo real; llevando a la necesidad de posponer el bloqueo, hasta el día veintiocho de diciembre del mismo año; la espera de tres días otorgo tiempo de sobra en el cual se realizaron un mil noventa y cuatro transacciones por un monto de novecientos quince mil setecientos cuarenta y un dólares de los Estados Unidos de America, con sesenta y ocho centavos ($915,741.68).

En base a lo antes expuesto el suscrito considera que ha existido incumplimiento a las disposiciones mencionadas, por lo que se puede determinar responsabilidad administrativa para el Banco.

III. Sobre la presunta violación al artículo 3 literal d) de las Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50), en relación al art 63 de la Ley de Banco.

El Banco manifiesta contar con dos sistemas de monitoreo: 1) Monitor Plus y 2) Safety Net

(MasterCard), mismos que en los informes DR-004/2016 y DR-ROT-015/2016, se expresa que en febrero de dos mil dieciséis el Banco tenía "*en ejecución proyectos para reforzar y renovar la infraestructura que soporta el modelo de monitoreo transaccional*", evidenciando que en la inspección los auditores en su oportunidad corroboraron que el Banco si contaba con sistemas de monitoreo que se le cuestionan.

Al respecto, si bien el Banco contaba con los sistemas Monitor Plus y Safety Net (MasterCard), cuyo monitoreo pese a estar diseñado para funcionar veinticuatro horas al día no son en tiempo real, motivo por el cual el Banco, posterior a los eventos suscitados el día veintiséis de diciembre, procedió a fomentar proyectos para reforzar y renovar la infraestructura que soporta el modelo de monitoreo transaccional, que incluye: el monitoreo transaccional en tiempo real, herramienta de protección desde MasterCard para operaciones internacionales, bloqueos y autorizaciones de transacciones manejado por medio de listas negras, blancas y medición de servicio mediante herramientas especializadas.

Proyectos que si bien vienen a fortalecer su sistema de monitoreo, nacieron de la evidente carencia de un sistema integral de monitoreo de comportamiento transaccional del cliente que tenga mecanismos de identificación de operaciones inusuales y alertas tempranas en tiempo real, así como de validaciones de reglas respecto a parámetros de tarjetas, tales como: bines, limites de retiros y compras, vencimiento de tarjetas, entre otros, que pueda efectuarse a nivel de marca (Mastercard) ó procesador, reduciendo con ello el flujo de transacciones que no cumplen los referidos parámetros, y que puedan ser recibidas y autorizadas por el Banco en circunstancias inusuales y ser rechazadas a ese nivel.

Situación que es confirmada por el Banco en Memorándum N° ATI-DRO-M-012-16, de fecha veintiséis de enero de dos mil dieciséis, suscrito por el Ingeniero Edgar Geovanny Fernández Rossil, Director de Monitoreo Transaccional, informando el avance del proceso de adquisición de la herramienta FRM (Fraud Rule Manager), habiendo enviando formulario requerido para su adquisición el día 14/01/2016, al personal de Mastercard; la cual sería utilizada para parametrisar reglas que apoyen a mitigar el fraude que se pueda presentar en las tarjetas de los bines que tenga asignados el Banco. Revalidando que en lo que se implementa la herramienta requerida, personal de MasterCard mantendrá activas las reglas que se

establecieron derivado del evento de fraude del veintiséis de diciembre de dos mil quince.

Siendo indispensable aclarar al Banco que la existencia de un Sistema de Monitoreo, no necesariamente efectúa los parámetros necesarios para dar cumplimiento a lo requerido por Ley; puesto que estos pueden estar alimentándose y generando reportes o avisos correspondientes, pero no en la premura necesaria, como sucedió en el evento acontecido el veintiséis de diciembre de dos mil quince, demostrando que pese a contar con los Sistemas Monitor Plus y Safety Net (MasterCard), estos no cumplieron los objetivos principales de control de riesgo y alertas en tiempo real, llevándolos a ser una herramienta insuficiente y por ende fuera de los parámetros que les permiten manejar adecuadamente sus riesgos operacionales tanto internas como las realizadas en el exterior, como es el caso que nos ocupa.

No siendo válido lo manifestado por el Apoderado del Banco, "*que no se ha configurado el incumplimiento atribuido, en razón a que hay evidencia de las alertas generadas por los sistemas y el recibo de pago del sistema Safetynet el cual comprueba que el sistema se encontraba vigente al momento de los hechos.*" Púes como se analizo anteriormente, no basta la existencia de un sistema, si este no es integral para el monitoreo de tarjetas de debito y del comportamiento transaccional del cliente, con mecanismos de identificación de operaciones inusuales y alertas tempranas para un correcto manejo de riesgos, acorde a lo que la Ley establece; evidenciado incumplimiento al artículo 3 literal d) de las Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50).

IV. Sobre la presunta violación al artículo 12 de las Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50), en relación al art 63 de la Ley de Banco.

El Banco manifiesta que la disposición legal no refleja un supuesto normativo orientado especialmente al ámbito de sistemas de información, por lo que no se les puede objetar que las deficiencias vayan en contra de lo requerido y que a la fecha del evento ya existía el documento "*Políticas de Tecnología de Información*", vigente desde mayo de dos mil catorce; definiendo el marco de gestión del riesgo de Tecnología de información asociados a los

eventos de bitácoras y mantenimiento; por lo que no procede atribuirle al Banco responsabilidad por la supuesta falta del mismo.

Al respecto, las "*Políticas de Tecnología de Información*" relacionada por el Banco, en su Introducción decanta el enfoque y objetivos buscados, como "*una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal por el uso y limitaciones de los recursos y servicios informáticos de la organización.*"; estando dirigidas a regular el correcto uso de los elementos tecnológicos como son: control de contraseñas; acceso y uso del servicio internet; antivirus; requerimientos girados al centro de soporte; responsabilidad, restricciones, prohibiciones y sanciones para encriptar información; debida diligencia para selección de proveedores de servicio; entre otras. Elementos con los que cuenta internamente el Bancaria a efecto de regular el debido proceso y manejo por parte de su personal humano, del equipo computacional disponible y puesto a su uso con el propósito de realizar los registros transaccionales bancarios diarios de sus usuarios.

En el sentido, las citadas normas no fueron elaboradas con perspectiva de prevención, identificación, control y manejo de riesgo operacional, a través de políticas de mantenimiento y respaldo de las bitácoras de eventos de sistemas operativos y aplicaciones en los servidores; medidas de seguridad en las redes especializadas de prestación de servicios; políticas de monitoreo, mantenimiento y respaldo de logs de los equipos de seguridad. Políticas, que les permitan reducir su vulnerabilidad operacional y que considerar, entre otros aspectos: 1) la categorización de eventos de pérdida, 2) las funciones y responsabilidades en la gestión del riesgo operacional, 3) criterios de identificación, 4) medición, 5) control, 6) mitigación y 7) sistemas de información para la gestión del riesgo operacional.

Deficiencia notoria en incidente del día veintiséis de diciembre de dos mil quince, al advertirse que:

1) El servidor FEP (Pamplona) involucrado en el evento; no contaba con los registros de las bitácoras (logs) de la fecha veintiséis de diciembre de dos mil quince y fechas anteriores. Asimismo, se identificó que el nuevo servidor FEP (Rosarito) puesto en producción desde el veinticinco de enero de dos mil dieciséis, a la fecha de la visita de inspección, la

configuración en el registro de logs cuenta con capacidad de almacenar 20MB, por lo que de superar la capacidad de almacenamiento el sistema borra los logs más antiguos.

2) Falta de medidas de seguridad en las redes especializadas de prestación de servicios, debido a que el Banco mantuvo expuesto en una red de menor seguridad la Base de Datos del Sistema FEP, el cual antes de la fecha veinticinco de enero de dos mil dieciséis, el referido sistema y la base de datos se encontraban en un mismo servidor (Pamplona).

3) No cuentan con políticas de monitoreo, mantenimiento y respaldo de logs de los equipos de seguridad, debido que los firewall no contaban con registros de logs a la fecha de la visita.

4) Se observó que el Banco utiliza canales sin cifrado de datos, para la transferencia de información confidencial de sus clientes, tal es el caso del enlace que tiene con la empresa Promoción y Operación, S.A. de C.V., que presta al Banco el servicio de liquidación de transacciones de tarjeta de débito, existiendo riesgo que sea aprovechada.

Por lo que el suscrito considera que ha existido incumplimiento a las disposiciones mencionadas, que nos lleva a determinar responsabilidad administrativa para el Banco.

V. Sobre la presunta violación al artículo 3 literal c) Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50).

El Banco manifiesta que a la fecha del incidente contaba con las "*Políticas de Sistemas de Información*", por lo que no puede atribuírsele la no existencia de gestiones concretas sobre el cumplimiento de la Norma.

Al respecto, tal como se analizo en el romano anterior, las "*Políticas de Tecnología de Información*", relacionada por el Banco, en su Introducción decanta el enfoque y objetivos buscados, como "*una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal por el uso y limitaciones de los recursos y servicios informáticos de la organización.*"; estando dirigidas a regular el correcto uso de los elementos tecnológicos como son: control de contraseñas; acceso y uso del servicio internet; antivirus;

requerimientos girados al centro de soporte; responsabilidad, restricciones, prohibiciones y sanciones para encriptar información; debida diligencia para selección de proveedores de servicio; entre otras. Elementos con los que cuenta internamente el Bancaria a efecto de regular el debido proceso y manejo por parte de su personal humano, del equipo computacional disponible y puesto a su uso con el propósito de realizar los registros transaccionales bancarios diarios de sus usuarios.

Pero en ningún momento están direccionadas a los factores de Riesgo tecnológico de información, como son: fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, así como la calidad de la información y una adecuada inversión en tecnología, establecidos en el articulo 3 literal c) de la NPB4-50.

Evidenciando que el Banco:

1) Mantuvo en producción un servidor con sistema operativo y base de datos sin soporte del fabricante, debido a que el servidor (Pamplona) contaba con el sistema operativo Microsoft Windows 2003 Server y Microsoft SQL 2000 que estaban desactualizados y fuera de soporte del fabricante.

2) La aplicación FEP instalada en el nuevo servidor (Rosarito), ha sido desarrollada Visual Basic 6.0, no cuenta con soporte del fabricante Microsoft desde el año 2008, por lo que aun podría estar expuesto a vulnerabilidades generadas por aplicaciones sin soporte.

3) La plataforma tecnológica del sistema Solx "core bancario" (ASTATO y MANDEVILLE), tienen instalado el sistema operativo Microsoft Windows Server 2003 R2, el cual está fuera de soporte del fabricante, lo que expone al riesgo que vulnerabilidades sean explotadas afectando la continuidad de las operaciones y la seguridad de la información.

Por lo que el suscrito considera que ha existido incumplimiento a las disposiciones mencionadas, que nos lleva a determinar responsabilidad administrativa para el Banco.

C. DETERMINACIÓN DE LA CUANTIA DE LA MULTA A IMPONER

Tanto la jurisprudencia nacional como la comparada, y la doctrina de tratadistas nacionales e internacionales en materia de derecho administrativo sancionatorio, convergen en la aplicabilidad general de los principios y garantías fundamentales del derecho penal público, en la actividad administrativa sancionatoria del Estado. En ese contexto es pertinente indicar que uno de los pilares fundamentales para la imposición de la sanción administrativa, debe ser el de proporcionalidad, en virtud del cual se constituye una frontera o límite de la actuación represiva de la Administración Pública. Como resultado de la aplicación de dicho principio, es dable afirmar que la sanción imponible debe ser la necesaria, idónea y proporcionada para obtener los objetivos perseguidos por la misma, factor que debe tomarse en consideración al momento de determinar la misma.

De conformidad con el artículo 50 de la Ley de Supervisión y Regulación del Sistema Financiero, los criterios para adecuación de la sanción que deben considerarse al momento de determinar la multa a un supervisado por la comisión de una infracción son: la gravedad del daño o del probable peligro a quienes podrían resultar afectados por la infracción cometida, el efecto disuasivo en el infractor respecto de la conducta infractora, la duración de la conducta infractora y la reincidencia de la misma, en los casos en que ésta no haya sido considerada expresamente por el legislador para el establecimiento de la sanción respectiva. Además, cuando la sanción a imponer sea una multa, deberá tomar en consideración la capacidad económica del infractor.

Con respecto a la duración de la conducta infractora y la reincidencia de la misma, el suscrito considera necesario, recalcar que en razón de los incumplimientos identificados por la Dirección de Riesgos, para efecto de realización de Memorándum 004/2016, de fecha nueve de febrero de dos mil dieciséis, la cantidad de infracciones respecto de los cuales no se dio cumplimiento a la Norma técnica respectiva, evidencian la falta de control y seguimiento de los debidos procesos y diligencias por parte del Banco.

En consecuencia, al incurrir tal entidad en las referidas infracciones, se encuentra sujeto a las sanciones de conformidad al Art. 43 Ley de Supervisión y Regulación del Sistema Financiero y

por el supuesto descrito en el Art. 44 literal b) de la Ley de Supervisión y Regulación del Sistema Financiero, que es cuando se ha infringido entre otras, normas técnicas como las del presente caso, que desarrollan las obligaciones establecidas en las leyes respectivas. Por lo que, procede declarar la responsabilidad infractora del Banco, sobre los cargos atribuidos a que este proceso se refiere, lo que así habrá que declararse.

En referencia a la determinación de la capacidad económica de la Supervisada, la Dirección de Análisis de Entidades de esta Superintendencia, mediante informe N° DAE-167-2018, realizó examen integral del patrimonio y solvencia que presenta el **BANCO G&T CONTINENTAL DE EL SALVADOR, S.A.** al 31 de diciembre de 2017 de US$60,160.8 miles, concluyendo que presentó indicadores de rentabilidad, liquidez y solvencia aceptables, permitiéndole el primero cumplir con sus obligaciones de corto plazo.

De ahí que la sanción necesaria a imponer, se considera que es la multa, la cual debe de ser en un monto tal que produzca un efecto disuasivo respecto de la conducta infractora, por el cometimiento de las infracciones a la Ley de Bancos y en las Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50), por haberse comprobado certeramente la existencia de la responsabilidad administrativa en todas las inobservancias conocidas en el presente procedimiento, en el cual se respetaron todos y cada uno de los derechos y garantías constitucionales de la Supervisada.

El suscrito, de conformidad a los anteriores disposiciones y considerandos, con fundamento en los artículos 11, 12 y 14 de la Constitución de la República; 43, 44 y 50 de la Ley de Supervisión y Regulación del Sistema Financiero; el suscrito **RESUELVE:**

a) **SANCIONAR** a **BANCO G&T CONTINENTAL DE EL SALVADOR, S.A.,** al pago de una multa que asciende a la cantidad de **SEIS MIL DIECISÉIS DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA CON OCHO CENTAVOS DE DÓLAR (US$6,016.08)** por la infracción cometida al artículo 3 literal a) de Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50), por deficiencias en la recepción y manejo de alertas, al identificarse que el Banco no posee procedimientos claramente definidos, que le permitan dar atención oportuna y manejar adecuadamente las notificaciones de alertas

ante eventos inusuales; multa que equivale al 0.01% del Patrimonio de la entidad al momento de cometerse la infracción.

b) **SANCIONAR** a **BANCO G&T CONTINENTAL DE EL SALVADOR, S.A.,** al pago de una multa que asciende a la cantidad de **SEIS MIL DIECISÉIS DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA CON OCHO CENTAVOS DE DÓLAR (US$6,016.08),** por la infracción cometida al artículo 3 literal b) de Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50), por falta de plan de sucesión del personal encargado de recibir las alertas y de medios alternativos de comunicación para la atención de las mismas; multa que equivale al 0.01 % del Patrimonio Neto de la entidad al momento de cometerse la infracción.

c) **SANCIONAR** a **BANCO G&T CONTINENTAL DE EL SALVADOR, S.A.,** al pago de una multa que asciende a la cantidad de **SEIS MIL DIECISÉIS DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA CON OCHO CENTAVOS DE DÓLAR (US$6,016.08)** por la infracción cometida al artículo 3, literal d) de las Normas Técnicas sobre Obligaciones de las Sociedades Clasificadoras de Riesgo (NRP-07), en relación al artículo 63 de la Ley de Bancos, por falta de monitoreo a comportamiento transaccional del cliente y falta de validación adicionales a nivel de marca de tarjetas o procesador; multa que equivale al 0.01% del Patrimonio Neto de la entidad al momento de cometerse la infracción.

d) **SANCIONAR** a **BANCO G&T CONTINENTAL DE EL SALVADOR, S.A.,** al pago de una multa que asciende a la cantidad de **SEIS MIL DIECISÉIS DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA CON OCHO CENTAVOS DE DÓLAR (US$6,016.08)** por la infracción cometida al artículo 12 de las Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50), en relación al artículo 63 de la Ley de Bancos, por falta de medidas de seguridad en las redes especializadas de prestación de servicios; multa que equivale al 0.01% del Patrimonio Neto de la entidad al momento de cometerse la infracción.

e) **SANCIONAR** a **BANCO G&T CONTINENTAL DE EL SALVADOR, S.A.,** al pago de una multa que asciende a la cantidad de **SEIS MIL DIECISÉIS DÓLARES DE LOS ESTADOS**

UNIDOS DE AMÉRICA CON OCHO CENTAVOS DE DÓLAR (US$6,016.08) por la infracción cometida al artículo 3, literal c) de las Normas para Gestión del Riesgo Operacional de las Entidades Financieras (NPB4-50), por uso de aplicaciones desactualizadas sin soporte del fabricante, verificando que El Banco no cuenta con políticas y planes de renovación de infraestructura tecnológica relacionada con la seguridad; multa que equivale al 0.01% del Patrimonio Neto de la entidad al momento de cometerse la infracción.

NOTIFÍQUESE.

SUPERINTENDENTE DEL SISTEMA FINANCIERO El Salvador, C.A.

José Ricardo Perdomo Aguilar
Superintendente del Sistema Financiero

6//9