SUPERINTENDENCIA
DE BANCOS
REPÚBLICA DOMINICANA

Dirección del Departamento de Seguridad de la Información

Informe técnico que justifica la excepción por exclusividad para la renovación de softwares de la plataforma tecnológica de ciberseguridad.

Fecha: 02 de febrero del 2023

Preparado por:	Revisado por:
Kendra Mazara	
Kendra Mazara **Encargado de División** **Departamento de Seguridad de la Información**	**Juan Daniel Pujols** **Subdirector** **Departamento de Seguridad de la Información**

1. Objetivo del Documento

Este documento busca establecer las razones por las cuales el Departamento de Seguridad de la Información de esta Superintendencia de Bancos busca la contratación para la Renovación de los softwares que forman parte de la plataforma tecnológica de ciberseguridad, como: Mandiant, Tenable.IO y Fortinet

2. Antecedentes

La Superintendencia de Bancos (SB) como ente supervisor de las entidades de intermediación financiera y cambiaria según lo establecido en la Ley 183-02, ha diseñado un plan estratégico 2021-2024 mediante el cual se propone: "Ser una institución referente nacional e internacionalmente, reconocida por la calidad de su supervisión y el acompañamiento que brinda a los usuarios de los servicios financieros, respaldada por un personal altamente calificado y la excelencia en su gestión". Para alcanzar esta visión se han identificado seis ejes estratégicos que engloban los objetivos estratégicos e iniciativas que durante el período 2021-2024 la SB se propone ejecutar.

Uno de estos ejes estratégicos es el de la Digitalización, Innovación y Nuevas Tecnologías, el cual le permitirá a la SB contar con procesos y herramientas tecnológicas que aumentarán la eficiencia, eficacia y el alcance de los procesos internos a través de nuevas tecnologías. La implementación de estos procesos y herramientas tecnológicas, así como la información almacenada, procesada y transmitida por estos, deben ser protegidos de manera adecuada.

Entre las soluciones de ciberseguridad implementadas para cumplir con el objetivo de proteger la infraestructura y sistemas de la Superintendencia de Bancos, así como con el Plan de Ciberseguridad, se encuentra:

1. **Mandiant**: es un servicio gestionado para identificación de amenazas y respuesta a incidentes.
2. **Tenable.io**: es una solución en la nube de gestión de vulnerabilidades de ciberseguridad, permitiendo tener una visibilidad completa de los activos y las vulnerabilidades de la SB.
3. **Firewalls Fortinet:** es una plataforma que proporciona seguridad en el perímetro de la red de la Superintendencia de Bancos.

Se hace necesario renovar los contratos de licenciamiento por UN (1) año de estos softwares para poder realizar las iniciativas que apoyan la digitalización, innovación y nuevas tecnologías a través del plan operativo anual (POA) pautado para el 2023.

3. Justificación del Uso de la excepción por exclusividad

Se busca la renovación del licenciamiento por UN (1) año de tres (3) software que forman parte de nuestra plataforma tecnológica de ciberseguridad orientado empresas que tengan las acreditaciones en el país para vender o comercializar lo siguiente:

1. Mandiant – Managed Defense for Endpoints

La Superintendencia de Bancos tiene implementado desde el 09 de abril del 2021 el servicio de MDR (Managed Detection and Response) de Mandiant, teniendo los agentes instalados en las PC y servidores de la SB, como parte de la gestión efectiva de incidentes de Ciberseguridad. Este servicio se enfoca y especializa en la identificación de eventos generados por actores maliciosos y amenazas prevalentes de alta complejidad. Mandiant es la empresa de Ciberseguridad con mayor presencia en los sectores financieros, gubernamentales y militares de Estados Unidos y el Reino Unido, así como también cuenta con la experticia en incidentes reales asociados a instituciones gubernamentales, inteligencia de amenazas, priorización de alertas, búsqueda proactiva de amenazas y un soporte al momento de asistir a sus clientes durante un ciberataque.

2. Tenable.io – Vulnerability Management

La Superintendencia de Bancos tiene implementada desde el 24 de marzo del 2020 la plataforma Tenable.io, teniendo la consola de administración en la nube y los sensores instalados en diferentes segmentos de la red de la SB, como parte de la gestión efectiva de vulnerabilidades de Ciberseguridad. Esta plataforma proporciona una visibilidad unificada y una visión continua de todos los activos de información de la SB, tanto los conocidos como los desconocidos, mediante diferentes métodos, como son, escaneo activo, agentes, supervisión pasiva, conectores en la nube, gestión de superficie de ataque externa e integraciones de CMDB, lo cual permite comprender todas las exposiciones de ciberseguridad de la SB mediante la evaluación de vulnerabilidades y la priorización de estas combinando los datos de vulnerabilidad, inteligencia de amenazas y ciencia de datos, que permiten evaluar los riesgos de los activos y saber cuáles vulnerabilidades deben corregirse primero.

3. Firewalls - Fortinet

La Superintendencia de Bancos tiene implementada desde el 13 de mayo del 2020 la plataforma Firewalls Fortigate de nueva generación, la cual proporciona seguridad en el perímetro de la red de una organización. Esto significa que actúa como una barrera entre la red interna de la organización y el mundo exterior, protegiendo la red de amenazas externas como ataques de red, así mismo, ofrece un control de acceso de red basado en políticas, lo que permite controlar quién y qué dispositivos tienen acceso a la red. También incluye una protección contra ataques de red y malware, ayudando a detectar y bloquear amenazas cibernéticas. Además, proporciona un control de aplicaciones y análisis de tráfico para ayudar a garantizar que solo las aplicaciones autorizadas se ejecuten en la red. Asimismo, se puede integrar con otras soluciones de seguridad existentes de la organización para una protección más completa.

Se solicita al comité de compras el procedimiento de excepción por exclusividad para que participen todos los proveedores que estén acreditados por Mandiant, Tenable.IO o Fortinet, para vender o comercializar la renovación de los respectivos licenciamientos solicitados. Por lo tanto, el oferente participante deberá, mediante comunicación del fabricante, acreditar que está autorizado para comercializar o vender en el país las renovaciones requeridas.

En caso de sustituir los softwares existentes, tendríamos las siguientes implicaciones: pérdida de información (históricos) de las plataformas, implementación y configuración desde cero, lo cual tomaría más tiempo, asimismo, la curva de aprendizaje sería más larga para los administradores de las plataformas, también, el costo de la adquisición sería mayor, ya que normalmente tiene un precio más elevado al de la renovación.

4. Descripción del requerimiento

Los detalles de los requerimientos para cada renovación solicitada es la siguiente:

1. Renovación **Mandiant**

Código	Descripción	Cantidad
08VV35	MANDIANT THREAT INTELLIGENCE CLDS FUSION	700
08VV52	MD FULL COVERAGE BASE CLDS	1
08VV53	MD FULL COVERAGE NODE CLDS	700
RN-EP-U-CPE-PROMO-	RNW Endpoint Security Cloud Power RENOVACION MANDIANT SUPERINTENDENCIA DE BANCOS	700

2. Renovación **Tenable.io**

Código	Descripción	Cantidad
TIOVM	LA TENABLE.IO VULNERABILITY CLDS MGMT LICS PER ASSET	512
6RV126	LA TENABLE.IO VM CONTAINER STD CLDS TENABLE.IO VM CONTAINER	1
TIO-WAS	LA TENABLE.IO WEB APP SCANNING LICS	5
TLUM	LA LUMIN CYBER EXPOSURE SLIC PLATFORM ANNUAL SUB	1

3. Renovación **Firewalls - Fortinet**

Código	Descripción	Cantidad
FC2-10-LV0VM-149 02-12	**FortiAnalyzer VM** Threat Detection service	1

FC1-10-LV0VM-248-02-12	Firmware & General Updates Enhanced Support Premium Telephone Support Premium	
FC-10-F6H0E-950-02-12	**FortiGate 600E** Advanced Malware Protection FortiGuard IPS Service AntiSpam Firmware & General Updates Enhanced Support Premium Telephone Support Premium Hardware Premium Web & Video Filtering	4
FC1-10-M3004-248-02-12	**FortiManager-VM** Firmware & General Updates Enhanced Support Premium Telephone Support Premium	1

5. Justificación legal del requerimiento.

El artículo 6, PARRAFO, numeral 3 de la Ley de Compras y Contrataciones 340-06, de fecha 20 de julio del 2006 (La Ley), establece que:

PARRAFO. Serán considerados casos de excepción y no una violación a la ley, la condición de que no se utilicen como medio para vulnerar los principios y se haga uso de los procedimientos establecidos en los reglamentos, las siguientes actividades:

*3. Las compras y contrataciones de **bienes o servicios con exclusividad** o que sólo puedan ser suplidos por una determinadas persona natural o jurídica.*

En ese mismo orden, el artículo 3, del reglamento de aplicación de la referida ley, instruido por el Decreto No. 543-12, de fecha 06 de septiembre del año 2012 establece que:

> *"Serán considerados casos de excepción y no una violación a la ley, las (situaciones) que se detalla a continuación, siempre y cuando se realicen de conformidad con los procedimientos que se establecen en el presente Reglamento."*

De igual manera el numeral 5 de este artículo define la figura de Bienes o Servicios con Exclusividad de la siguiente manera:

6. ***Bienes o Servicios con Exclusividad.*** *Aquellos que pueden ser suplidos por un número limitado de personas naturales o jurídicas.*

De acuerdo con lo anteriormente descrito, se considera las motivaciones expuestas en este documento, como válidas para enmarcarse en lo provisto en la Ley como un caso de excepción por Exclusividad y no constituye una violación de sus formalidades y plazos. Por lo que se somete a la autorización del Comité de Compras de esta superintendencia, las motivaciones y justificaciones anteriores para la recomendación del uso de la excepción, en cumplimiento con el artículo 4, numeral 3 del reglamento de aplicación de la Ley.