INFORME DE JUSTIFICACIÓN

ADQUISICIÓN DE LICENCIAS DE LA SOLUCIÓN DE CIBERSEGURIDAD
TREND MICRO

SANTO DOMINGO, R.D.
08 DE ENERO DEL 2024

TABLA DE CONTENIDO

OBJETIVO 3
ANTECEDENTES 3
JUSTIFICACIÓN TÉCNICA 4
RECOMENDACIÓN 5
Anexos: 7
Análisis de riesgos 8

OBJETIVO

Presentar la justificación técnica para la Adquisición de Licencias de la solución de ciberseguridad Trend Micro, incluyendo los servicios de soporte del fabricante.

ANTECEDENTES

En fecha 20 de octubre de 2008, la Suprema Corte de Justicia suscribió el contrato 08-327, con la empresa Consulting Resources Group, S.A. para la adquisición del antivirus corporativo "Trend Micro". El mismo se hizo a través de la Comisión de Compras y Licitaciones Públicas de la Suprema Corte de Justicia y fue aprobado por el Pleno de la misma Suprema en fecha 2 de octubre de 2008, mediante Acta Núm. 37/08.

Este contrato fue suscrito por un (1) año y valorado por la suma de Doscientos Cinco Mil Ciento Ochenta y Siete Dólares norteamericanos con 76/100 (USD$ 205,187.76) y fue renovado anualmente hasta el año 2018.

En el año 2019 fue aprobada la renovación de estas licencias mediante Acta del Consejo del Poder Judicial No. 11/2019 de fecha 20 de marzo de 2019; no obstante, luego de verificación, fue dispuesto por instrucciones de la Dirección General de Administración y Carrera Judicial, quien fue apoderada por el Consejo del Poder Judicial; la realización de un nuevo proceso de adquisición de una solución de antivirus en cumplimiento de las normativas, dejando sin efecto la renovación del anterior contrato.

El 27 de diciembre del 2019, fue adjudicado a la empresa **Figitam Technology S.R.L.** el proceso de excepción por exclusividad para la Renovación de las licencias de Trend Micro para la Solución de Protección de Puntos Finales de las distintas dependencias del Consejo del Poder Judicial, Ref. No. PEEX-CPJ-002-2019. En este proceso fueron renovadas 5,100 licencias de la suite de Trend Micro por un tiempo de un año.

El 18 de marzo 2021, fue adjudicado a la empresa **IT Global Enterprises Services,** el proceso de excepción por exclusividad para la Renovación de las licencias de Trend Micro para la Solución de Protección de Puntos Finales de las distintas dependencias del Consejo del Poder Judicial, Ref. No. PEEX-CPJ-001-2021. En este proceso fueron renovadas 5,100 licencias de la suite de Trend Micro por un tiempo de un año.

El 17 de marzo 2022, fue adjudicado a la empresa **IT Global Enterprises Services,** el proceso de excepción por exclusividad para la Renovación de las licencias de Trend Micro para la Solución de Protección de Puntos Finales de las distintas dependencias del Consejo del Poder

Judicial, Ref. No. PEEX-CPJ-001-2022. En este proceso fueron renovadas 5,100 licencias de la suite de Trend Micro por un tiempo de un año.

El 28 de marzo 2023, fue adjudicado a la empresa **IT Global Enterprises Services,** el proceso de excepción por exclusividad para la Adquisición de las licencias de Trend Micro para la Solución de Protección de Puntos Finales de las distintas dependencias del Consejo del Poder Judicial, Ref. No. PEEX-CPJ-01-2023. En este proceso fueron renovadas 5,500 licencias de la suite de Trend Micro contemplando XDR para 2,000 estaciones de trabajo por un tiempo de un año.

JUSTIFICACIÓN TÉCNICA

Actualmente el Poder Judicial cuenta con **5,500** licencias de uso de la suite de ciberseguridad de Trend Micro, contempladas para el uso de las siguientes soluciones en el Poder Judicial y sus dependencias:

- ✓ Antivirus
- ✓ Parchado virtual
- ✓ Control de aplicaciones
- ✓ Protección de correo electrónico
- ✓ Cifrado de puntos finales
- ✓ Protección ante pérdida de datos
- ✓ Protección de dispositivos móviles
- ✓ XDR

Esta solución ha sido implementada en toda la infraestructura de servicios críticos de la institución, contemplando todos los componentes de la nube híbrida. En este momento, continuamos con un proceso de despliegue a nivel nacional de la solución de antivirus, contemplando también la instalación de la herramienta de cifrado de puntos finales y MDM.

Actualmente el número de equipos con antivirus instalado asciende a 5,500 y 2,000 licencias de uso de la característica Trend Micro Vision One (XDR).

Los controles de protección ante software malicioso para el Poder Judicial son imperativos a los fines de mitigar los incidentes causados por virus, phishing y otros ciberataques que pueden detener parcial o totalmente las operaciones de la institución, dependiendo de la severidad de estos. De igual manera puede dañar la reputación institucional si es afectado el equipo de un funcionario de alto rango.

Es importante destacar que Trend Micro es utilizada como una de las fuentes de alertamiento y recopilación de información por parte de nuestro Centro de Operaciones de Seguridad (SOC).

A raíz de que la licencia de esta suite caduca el 24 de mayo del año 2024, la Gerencia de Seguridad de la Información ha iniciado el proceso de solicitud de adquisición de las licencias de esta solución, esto implica generar las especificaciones técnicas asociadas con el producto Trend Micro y ejecutar el proceso de compra dando participación a las empresas locales que representan formalmente a este fabricante en el país, derivando en un proceso de adquisición de licencias completamente transparente para los usuarios y el personal técnico especializado que soporta la solución.

Los servicios de soporte por parte del fabricante son requeridos en modalidad 24 horas, 7 días de la semana (24/7) durante un año. Este servicio es utilizado para atender directamente con el fabricante cualquier incidencia técnica con la plataforma. En adición a esto, son requeridas 40 horas al año de soporte local por parte proveedor, estas horas son utilizadas para apoyo técnico especializado en la implementación de estas soluciones, validación de configuraciones y soporte en sitio en caso de ser requerido.

RECOMENDACIÓN

La recomendación técnica es que se proceda de inmediato con la adquisición de las licencias de Trend Micro a través de un proceso de excepción por exclusividad alineado con los procesos institucionales correspondientes, dando participación a los representantes oficiales de Trend Micro en la República Dominicana. Con esto protegemos las operaciones y mitigamos el riesgo de cualquier intrusión de virus, tomando en cuenta que:

1) Poseemos un producto de ciberseguridad reconocido internacionalmente que ha dado los resultados esperados por la Institución.
2) El personal que constituye el soporte técnico ya posee el conocimiento de manejo de esta herramienta.
3) Constituye un ahorro en el costo de implementación ya que el mismo se encuentra instalado en nuestra plataforma tecnológica.

Anexos:

- ✓ *Representantes de Trend Micro en la República Dominicana.*
- ✓ *Análisis de riesgos.*

Aseguramos que los criterios utilizados en la elaboración de este documento están basados en los principios éticos, de transparencia, de imparcialidad y de procurar proteger los intereses del Poder Judicial.

Equipo de peritos:

Bernardo Barreiro
Coordinador de Seguridad y Monitoreo TIC

Adderli de la Rosa
Coordinador de Seguridad de Infraestructura

Emmanuel E. Tejada
Gerente de Seguridad y Monitoreo TIC

Revisado por:

Welvis Beltrán
Director de TIC

Anexos:

Representantes de Trend Micro en la República Dominicana. Información obtenida de: https://trendmicro.my.site.com/Gpartner/s/partner-locator/results?language=en_US

INTEGRATION & CONSULTING TECHNOLOGYINT ICT calle luisa ozema pellerano num. 7 gazcue, santo domingo, Distrito Nacional, 10205, Dominican Republic	Licencias On Line S.A.S. - Dominican Republic Puerto Plata, Dominican Republic	CONSULTORES EN SEGURIDAD TECNOLOGICA E INFORMATICA ARC, SRL Ave. Rep. de Colombia Plaza Argentina Local 6c, Santo Domingo, Distrito Nacional, 99999, Dominican Republic	IT GLOBAL ENTERPRISE SERVICES Av. Winston Churchill, no. 5 Torre Progreso, Distrito Nacional, Distrito Nacional, 10129, Dominican Republic
Redesip CALLE 1ERA NO. 6, EDIF. COHISA XXIII, SUITE 201, SANTO DOMINGO, Distrito Nacional, 10137, Dominican Republic	ASYSTEC SRL Av. Los Próceres esq. Euclides Morillo, Santo Domingo, Distrito Nacional, 999999, Dominican Republic	SAVANT CONSULTORES C/ PASEO DE BARCELONA NO. 33. PUERTA DE HIERRO ARROYO HONDO, SANTO DOMINGO, Distrito Nacional, 111095, Dominican Republic	Xirgu Investments Calle Mayor P. Valverde No.3,, Santo Domingo, Distrito Nacional, 10203, Dominican Republic
Figitam Technology, S.R.L. c/ Rafael Augusto Sanchez esq. Tiradentes, Santo Domingo, Distrito Nacional, 0, Dominican Republic	Sistema Aplicativo (Infosec) av abraham lincoln 1003 , Torre Profesional Bilmoret I, Santo Domingo, Distrito Nacional, 10103, Dominican Republic	Seti & Sidif Dominicana Edificio Ely 2A, Suite 302, Av. Ing. Roberto Pastoriza, Esq Ortega y Gasset. Ensanche Naco, Santo Domingo, D.N., Santo Domingo, Distrito Nacional, 10121, Dominican Republic	CONSULTING RESOURCES GROUP S.A. Andres Julio Aybar 49, Santo Domingo, Dominican Republic
Never off technology Calle Rafael Augusto Sánchez #33 con Av. Lope de Vega.Edif. Intercaribe Piso 3 Oficina 313. Ens. N, DF, Santo Domingo, Dominican Republic			

Análisis de riesgos

No.	Proceso	Activos de información	Riesgos	Evaluación del Riesgo				Medidas de Mitigación	
				Probab. / Impacto		Grabedad		Acciones / Actividades de Control	Responsable
1	Renovación de licencias de solución de ciberseguridad Trend Micro	Servidores, Estaciones de Trabajo (PC), Laptops, sistemas de información y cualquier documentación contenida en los mismos.	Que amenazas cibernéticas no sean detectadas.	3	3	3	Alto	Renovación de las licencias de la solución de antivirus	Dirección de Tecnología y Comunicaciones / Gerencia de Compras y Contrataciones
			Que nuestros dispositivos y los archivos contenidos sean afectados por software malicioso (virus, gusanos, troyanos, adware, spyware, etc.).	3	3	3	Alto		
			Que Ramsonware comprometa nuestros equipos. Incluso nuestros servidores pueden ser cifrados por este malware, evitando el acceso a la información contenida y pidiendo una recompensa para ser liberada.	3	3	3	Alto		
			Que se propague software malicioso a través del uso de dispositivos de almacenamiento externo (USB, CD, DVD, Discos Duros Externos).	3	3	3	Alto		
			Que los Sistemas de Información que soportan los servicios de administración de justicia sean comprometidos por algún software malicioso, afectando directamente los servicios ofrecidos al ciudadano.	3	3	3	Alto		
			Que seamos afectados por ataques dirigidos a través del correo electrónico (Phishing, Ransomware, etc.).	3	3	3	Alto		
			Que seamos objeto de una campaña de correo electrónico no deseado (SPAM).	3	3	3	Alto		

			Que se filtre información confidencial porque los controles de acceso que provee esta solución no están disponibles.	3	3	3	Alto		
			Que la reputación del Poder Judicial sea afectada luego de ser comprometidos nuestros sistemas de información.	3	3	3	Alto		

---Fin del documento---