Fecha: 06-05-2022

Descripción del Bien o Servicio Solicitado

Adquisición de Licencias de Antivirus

Ítem No.	Código UNSPSC	Bien Requerido	Cantidad	Vigencia	Presentación de Muestra	Instrucciones
1		Licenciamiento para Antivirus	100	1 Año	No	N/A

Especificaciones Técnicas

EndPoint Protection Advance Intercept X Endpoint
SUPERFICIE DE ATAQUE
Seguridad Web
Descargar reputación
Control web / Bloqueo de URL basado en categorías

Control periférico
Control de aplicaciones
ANTES DE QUE FUNCIONE EN EL DISPOSITIVO
Detección de malware de aprendizaje profundo

Escaneo de archivos anti-malware
Protección viva
Análisis de comportamiento previo a la ejecución (HIPS)

Bloqueo de aplicaciones potencialmente no deseadas (PUA)

Sistema de Prevención de Intrusión
DEJA DE EJECUTAR AMENAZA
Prevención de pérdida de datos
Análisis de comportamiento en tiempo de ejecución (HIPS)

Interfaz de exploración antimalware (AMSI)
Detección de tráfico malicioso (MTD)

Prevención de exploits
Mitigaciones activas del adversario
Protección de archivos de ransomware (CryptoGuard)

Protección de registro de arranque y disco (WipeGuard)

Protección del usuario en el navegador (navegación segura)

Bloqueo de aplicaciones mejorado
DETECTAR
Live Discover (consultas SQL entre propiedades para la búsqueda de amenazas y la higiene de las operaciones de seguridad de TI)

Biblioteca de consultas SQL (consultas preescritas y totalmente personalizables) Detección y priorización de eventos sospechosos

Detección y priorización de eventos sospechosos

Acceso rápido, almacenamiento de datos en disco (hasta 90 días)

Fuentes de datos entre productos, por ejemplo, firewall, correo electrónico (Sophos XDR)
Consulta entre productos (Sophos XDR)
Almacenamiento en la nube de Sophos Data Lake
Consultas programadas
INVESTIGAR
Casos de amenazas (análisis de causa raíz)
Análisis de malware de aprendizaje profundo

Inteligencia avanzada de amenazas de SophosLabs bajo demanda

Exportación de datos forenses
REMEDIAR
Eliminación automatizada de malware
Latido de seguridad sincronizado
Sophos limpio
Respuesta en vivo (investigue de forma remota y tome medidas)

Aislamiento de endpoints bajo demanda
Haga clic en "Limpiar y bloquear"
CAZA Y RESPUESTA A LAS AMENAZAS LIDERADAS POR LOS HUMANOS

Búsqueda de amenazas impulsada por clientes potenciales las 24 horas, los 7 días de la semana
Comprobaciones de estado de seguridad
Retención de datos
Informe de actividad
Detecciones de adversarios
Neutralización y remediación de amenazas
Búsqueda de amenazas sin plomo 24 horas al día, 7 días a la semana

Líder del equipo de respuesta a amenazas
Asistencia telefónica directa
Gestión proactiva de la postura de seguridad

Se contempla renovación de licenciamiento, ya que lo tenemos instalado.

Vigencia: 1 Año.
Tiempo de entrega: Tiempo de Entrega: 10 Días Calendario a partir de la instalación del bien o servicio posterior a la Certificación del contrato por parte de la Contraloría.

Ítem No.	Código UNSPSC	Bien Requerido	Cantidad	Vigencia	Presentación de Muestra	Instrucciones
2		Licenciamiento para Antivirus	40	1 Año	No	N/A
Especificaciones Técnicas						

REDUCCIÓN DE SUPERFICIE DE ATAQUE
Seguridad Web
Descargar reputación
Control web / Bloqueo de URL basado en categorías

Control periférico
Control de aplicaciones
Lista blanca de aplicaciones (bloqueo del servidor)

ANTES DE QUE FUNCIONE EN EL DISPOSITIVO
Detección de malware de aprendizaje profundo

Escaneo de archivos anti-malware
Protección viva
Análisis de comportamiento previo a la ejecución (HIPS)

Bloqueo de aplicaciones potencialmente no deseadas (PUA)

Sistema de Prevención de Intrusión
DEJA DE EJECUTAR AMENAZA
Prevención de pérdida de datos
Análisis de comportamiento en tiempo de ejecución (HIPS)

Interfaz de exploración antimalware (AMSI)
Detección de tráfico malicioso (MTD)
Prevención de exploits
Mitigaciones activas del adversario
Protección de archivos de ransomware (CryptoGuard)

Protección de registro de arranque y disco (WipeGuard)

Protección del usuario en el navegador (navegación segura)

Bloqueo de aplicaciones mejorado
DETECTAR
Live Discover (consultas SQL entre propiedades para la búsqueda de amenazas y la higiene de las operaciones de seguridad de TI)

Biblioteca de consultas SQL (consultas preescritas y totalmente personalizables)

Detección y priorización de eventos sospechosos

Acceso rápido, almacenamiento de datos en disco (hasta 90 días)

Fuentes de datos de productos cruzados, por ejemplo, cortafuegos, correo electrónico
Consulta entre productos
Sophos Data Lake (almacenamiento de datos en la nube)
Consultas programadas
INVESTIGAR
Casos de amenazas (análisis de causa raíz)
Análisis de malware de aprendizaje profundo

Inteligencia avanzada de amenazas de SophosLabs bajo demanda

Exportación de datos forenses
REMEDIAR
Eliminación automatizada de malware
Latido de seguridad sincronizado
Sophos limpio
Respuesta en vivo (investigue de forma remota y tome medidas)

Aislamiento de endpoints bajo demanda
Haga clic en "Limpiar y bloquear"
VISIBILIDAD
Protección de cargas de trabajo en la nube (Amazon Web Services, Microsoft Azure, Google Cloud Platform)
AWS Map, visualización multirregional
Control de aplicaciones sincronizado (visibilidad de las aplicaciones)

Gestión de la postura de seguridad en la nube (supervise y proteja los hosts en la nube, las funciones sin servidor, los depósitos S3 y más)

CONTROL
Gestión de políticas específicas del servidor
Actualizar caché y retransmisión de mensajes

Exclusiones de escaneo automático
Supervisión de la integridad de los archivos
SERVICIO GESTIONADO

Búsqueda de amenazas impulsada por clientes potenciales las 24 horas, los 7 días de la semana
Comprobaciones de estado de seguridad
Retención de datos
Informe de actividad
Detecciones de adversarios
Neutralización y remediación de amenazas
Búsqueda de amenazas sin plomo 24 horas al día, 7 días a la semana

Líder del equipo de respuesta a amenazas
Asistencia telefónica directa
Gestión proactiva de la postura de seguridad

Vigencia: 1 Año.
Tiempo de entrega: Tiempo de Entrega: 10 Días Calendario a partir de la instalación del bien o servicio posterior a la Certificación del contrato por parte de la Contraloría.

Ítem No.	Código UNSPSC	Bien Requerido	Cantidad	Vigencia	Presentación de Muestra	Instrucciones
3		Licenciamiento de Encriptación de volúmenes	10	1 Año	No	N/A

Especificaciones Técnicas

Licencia para Central Device Encryption **SOPHOS** con 5 Clientes

- Cifrado de disco
- Intuitivo
- Cumplimiento
- Portal de autoservicio
- Uso compartido seguro de archivos
- Visibilidad

Se contempla renovación de licenciamiento, ya que lo tenemos instalado.

Vigencia: 1 Año.
Tiempo de entrega: Tiempo de Entrega: 10 Días Calendario a partir de la instalación del bien o servicio posterior a la Certificación del contrato por parte de la Contraloría.

Ítem No.	Código UNSPSC	Bien Requerido	Cantidad	Vigencia	Presentación de Muestra	Instrucciones
4		Licenciamiento de Seguridad de Correo electrónico	100	1 Año	No	N/A

Especificaciones Técnicas

PROTECCIÓN DEL CORREO ELECTRÓNICO
Filtros antispam

Escaneado de malware

Espacio seguro en la nube (selección de la ubicación)

Detección de URL maliciosas

Reescritura de direcciones URL en el momento del clic

Análisis de la reputación

Detección de anomalías en encabezados

SPF (correo entrante)

DKIM (correo entrante y saliente)

DMARC (correo entrante)

PROTECCIÓN CONTRA LA SUPLANTACIÓN DE IDENTIDAD
Protección contra el phishing de suplantación de identidad con procesamiento del lenguaje natural

Análisis del nombre mostrado (VIP y marcas)

Comprobaciones de dominios de imitación

PREVENCIÓN DE FUGAS DE DATOS
Políticas DLP de múltiples reglas para grupos y usuarios individuales

Listas de control de contenido (información financiera, contenido confidencial, información médica y datos de información personal

Cifrado TLS impuesto

Cifrado S/MIME y autenticación de remitentes*

Cifrado de mensajes y archivos adjuntos basado en imposición

Cifrado integral de portal basado en extracción Complemento disponible
INTEGRACIÓN CON MICROSOFT 365
Integración con las API de reglas de flujo de correo de Microsoft 365

Integración con API para la recuperación automática de mensajes de la posentrega (URL y mensajes)

GESTIÓN DE MENSAJES
Escaneado de mensajes entrantes

Escaneado de mensajes salientes

Bandeja de entrada de emergencia (lectura)*

Políticas a nivel de dominio, grupo y usuario

Cuarentena de usuario y administrador

Listas de permitidos/bloqueados de usuario y administrador

Banners de correo electrónico entrante (remitente de confianza, externo, de no confianza)

Sincronización de AD o Sincronización de Azure AD

Integración con API de Microsoft 365
(redireccionamiento MX para otros proveedores)

Vigencia: 1 Año.
Tiempo de entrega: Tiempo de Entrega: 10 Días Calendario a partir de la instalación del bien o servicio posterior a la Certificación del contrato por parte de la Contraloría.

REQUERIMIENTO
Es importante que los oferentes demuestren mediante certificación el partnership con los fabricantes de los productos requeridos.

Firma del Enc. Del Área o Perito Designado.

Unidad de Análisis Financiero UAF República Dominicana