ESTANDARIZACIÓN DEL SOFTWARE DEL DISPOSITIVO DE SEGURIDAD PARA CORREO ELECTRÓNICO – Cisco IronPort

INFORME TÉCNICO N° 005-2018-MTC/10.06.LRBS

1. NOMBRE DE LA OFICINA

Oficina de Tecnología de Información

2. OBJETIVO

2.1. Objetivo General

Estandarizar las licencias de software del dispositivo de seguridad para correo electrónico -Cisco IronPort; que brinda protección rápida y completa del correo electrónico al bloquear el spam (correo no deseado), el malware y otras amenazas al tiempo que brinda protección antes, durante y después de un ataque a la infraestructura del servicio electrónico de mensajería del Ministerio de Transportes y Comunicaciones.

2.2 Objetivos Específicos

- Brindar una adecuada protección al servicio de correo electrónico institucional.
- Proteger la inversión realizada correspondiente a la adquisición de las licencias actuales.
- Brindar mayor seguridad, disponibilidad y eficiencia a la infraestructura existente.
- Garantizar a los usuarios seguridad y confianza en los correos electrónicos que reciben y envían diariamente como parte de sus actividades.
- Evitar que los mensajes no deseados inunden la bandeja de entrada de los usuarios y ocupen espacio innecesario tanto en el equipo como en los servidores de mensajería.
- Proteger el servicio de mensajería contra amenazas de software malicioso, virus, phishing y otras que llegan por este medio de comunicación.

OFICINA DE TECNOLOGÍA DE INFORMACIÓN - V°B° DIRECTOR

Oficina de Tecnología de Información - V°B° Seg. de la Información - OGA - MTC

Jr. Zorritos 1203 – Lima - Perú
T. (511) 615-7800
www.mtc.gob.pe

3. DESCRIPCIÓN DE LA INFRAESTRUCTURA PREEXISTENTE

El Ministerio de Transportes y Comunicaciones cuenta con un equipo preexistente denominado: "Dispositivo de seguridad para correo electrónico Cisco IronPort", instalado en el ambiente de producción del Centro de Datos.

4. DESCRIPCIÓN DEL BIEN REQUERIDO A ESTANDARIZAR

El Ministerio de Transporte y Comunicaciones requiere estandarizar lo siguiente:

4.1 Nombre del bien

Software del dispositivo de seguridad para correo electrónico Cisco IronPort.

4.2 Características principales del bien

El software del dispositivo de seguridad para correo electrónico Cisco IronPort deberá tener las siguientes características:

- Contar con funcionalidades antispam, antiphising y antivirus para protección contra propagación masiva de software malicioso como virus y otros.
- Contar con una herramienta de monitoreo incorporada, para generar reportes por: IP de origen, dominio y red de donde provenga los mensajes.
- Permitir la integración con Microsoft Active Directory, para una rápida y eficiente trazabilidad de los mensajes y la creación de reglas de seguridad aplicadas a los usuarios.
- Generar reportes programados en horarios y días de la semana, y enviarlos automáticamente por correo electrónico al administrador de la solución.
- Generar reportes automáticos de tráfico (volumen, spam, virus, etc.).
- Contar con un logging de acceso seguro.
- Permitir la gestión automatizada de correos electrónicos en el área de cuarentena y ser accesibles mediante una consola web.
- Permitir gestionar listas de seguridad blancas (dominios y/o correos de confianza) y negras (dominios y/o correos de dudosa reputación).
- Permitir la creación de reglas de seguridad orientadas a optimizar el filtro de los correos electrónicos.

Jr. Zorritos 1203 – Lima - Perú
T. (511) 615-7800
www.mtc.gob.pe

- Diagnosticar problemas y monitorear el rendimiento del equipo.
- Ser administrable mediante protocolos: GUI (HTTPS), SSH, Telnet, Console/Serial, SNMPV1-3.
- Ser actualizable automáticamente de manera segura desde internet.
- Poseer al menos 2 instancias de filtros configurables, la primera a nivel de sesión SMTP y la restante como análisis de contenido.
- Permitir aplicar políticas de correo configurables por recipiente, dominio o IP de envío/recepción, así como soportar la configuración para el límite de los archivos adjuntos (tamaño en KB o Mb).
- Poseer características de seguridad contra ataques del tipo DOS, DHA.
- Soportar el envío y recepción de correo encriptado SSL/TLS.
- Permitir la configuración de filtros con capacidad de análisis de encabezado, asunto y contenido.
- Poseer herramientas para verificación de bounces, pudiendo seleccionar entre eliminar o aceptar los bounces de acuerdo a la verificación.
- Permitir la detección preventiva de spam y consecuente bloqueo de los mensajes y conexión TCP.
- Permitir la identificación y bloqueo de spam en distintos idiomas (capacidad heurística).
- Permitir que el usuario pueda auto gestionar su propia cuarentena de mensajes.
- Permitir configurar el tiempo y espacio de almacenamiento de la cuarentena.
- Permitir la detección preventiva ante propagación de virus y consecuente gestión de la cuarentena de los mensajes.
- Permitir la capacidad de escaneo automático de los mensajes y posterior tratamiento, marcado, reparación, borrado o entrega.
- Actualizar las nuevas definiciones de virus en forma automática y sin intervención del administrador.

5. MARCO LEGAL

5.1 En el punto 8.4 del Artículo 08° del Reglamento de la Ley de Contrataciones del Estado, aprobado con el Decreto Supremo N° 056-2017-EF, que modifica al Decreto Supremo N° 350-2015-EF, segundo párrafo se establece que:

Jr. Zorritos 1203 – Lima - Perú
T. (511) 615-7800
www.mtc.gob.pe

"...no se hace referencia a fabricación o procedencia, procedimiento de fabricación, marcas, patentes o tipos, origen o producción determinados, ni descripción que oriente la contratación hacia ellos, salvo que la Entidad haya implementado el correspondiente proceso de estandarización debidamente autorizado por su Titular...".

5.2 Anexo Único del Reglamento de Contrataciones del Estado define estandarización como "*Proceso de racionalización consistente en ajustar a un determinado tipo o modelo de los bienes o servicios a contratar, en atención a los equipamientos preexistentes."*

5.3 En tal sentido, y dado que la Directiva N° 004-2016-OSCE/CD que refiere los lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular de producto, señala: "*Cuando en una contratación en particular el área usuaria -aquella de la cual proviene el requerimiento de contratar o que, dada su especialidad y funciones, canaliza los requerimientos formulados por otras dependencias- considere que resulta inevitable definir el requerimiento haciendo referencia a fabricación o procedencia, procedimiento de fabricación, marcas, patentes o tipos, origen o producción determinados o descripción que oriente la contratación hacia ellos, deberá elaborar un informe técnico de estandarización debidamente sustentado, el cual contendrá como mínimo:*

a. La descripción del equipamiento o infraestructura preexistente de la Entidad.

b. De ser el caso, la descripción del bien o servicio requerido, indicándose la marca o tipo de producto; así como las especificaciones técnicas o términos de referencia, según corresponda.

c. El uso o aplicación que se le dará al bien o servicio requerido.

d. La justificación de la estandarización, donde se describe objetivamente los aspectos técnicos, la verificación de los presupuestos para la estandarización antes señalados y la incidencia económica de la contratación.

e. Nombre, cargo y firma de la persona responsable de la evaluación que sustenta la estandarización del bien o servicio, y del jefe del área usuaria.

f. La fecha de elaboración del informe técnico."

OFICINA DE TECNOLOGÍA DE INFORMACIÓN VºBº DIRECTOR

Oficina de Tecnología de Información VºBº Seg. de la Información OGA - MTC

Jr. Zorritos 1203 – Lima - Perú
T. (511) 615-7800
www.mtc.gob.pe

5.4 Se determina que la única excepción para adquirir bienes o servicios precisando nombre de marca o tipo de producto es la existencia de un proceso de estandarización (Artículo 08° del Reglamento de Contrataciones vigente), para lo cual se procederá estrictamente con lo descrito e indicado en la Directiva N° 004-2016-OSCE/CD.

6. USO O APLICACIÓN QUE SE LE DARÁ AL BIEN REQUERIDO

El software del dispositivo de seguridad para correo electrónico Cisco IronPort, brinda protección rápida y completa del correo electrónico, bloqueando el spam, el malware y otras amenazas al tiempo que brinda protección antes, durante y después de un ataque a la infraestructura del servicio electrónico de mensajería del Ministerio de Transportes y Comunicaciones para garantizar la seguridad de la información.

La adquisición de licencias de software del dispositivo de seguridad para correo electrónico Cisco IronPort, permite mantener el funcionamiento de una solución capaz de brindar un servicio de correo electrónico seguro y controlado. Asimismo, brinda un mecanismo de soporte y protección, permitiendo lograr la eficiencia máxima en la seguridad, disponibilidad y gestión del servicio de correo electrónico.

7. JUSTIFICACIÓN DE LA ESTANDARIZACIÓN

7.1 ANÁLISIS TÉCNICO

El bien preexistente es un dispositivo (appliance) de seguridad para correo electrónico de la marca Cisco, modelo IronPort; que trabaja con un software (Cisco Email Security), el cual ofrece protección contra amenazas basadas en correo electrónico, como antispam, la solución antivirus Sophos, los filtros de brotes de virus, la agrupación en clústers y, la prevención esencial del pérdidas de datos.

Estando próximas a vencer las licencias del software, las mismas que se encuentran instaladas el bien preexistente señalado precedentemente, y que se indican en el siguiente cuadro:

Oficina de Tecnología de Información V°B° DIRECTOR

Oficina de Tecnología de Información V°B° Seg. de la Información OGA - MTC

Jr. Zorritos 1203 – Lima - Perú
T. (511) 615-7800
www.mtc.gob.pe

Feature Keys

Mode —**Machine: ironport-C380-PRI.mtc.gob.pe** Change Mode...

▷ Centralized Management Options

Feature Keys for Serial Number: 84B2611877E4-FCH1939V0ZH			
Description	Status	Time Remaining	Expiration Date
Outbreak Filters	Active	3 hours	11 Feb 2019 18:28 (GMT -05:00)
IronPort Anti-Spam	Active	3 hours	11 Feb 2019 18:28 (GMT -05:00)
Sophos Anti-Virus	Active	3 hours	11 Feb 2019 18:28 (GMT -05:00)
Bounce Verification	Active	Perpetual	N/A
Incoming Mail Handling	Active	Perpetual	N/A
IronPort Email Encryption	Dormant	30 days	13 Mar 2019 14:41 (GMT -05:00)
Data Loss Prevention	Dormant	30 days	13 Mar 2019 14:41 (GMT -05:00)
McAfee	Dormant	30 days	13 Mar 2019 14:41 (GMT -05:00)
Pending Activation			

Es necesario su renovación, toda vez que permitirá mantener activo el servicio en casos de mal funcionamiento del dispositivo de seguridad para correo electrónico – Cisco IronPort; y preparado para cualquier contingencia.

Asimismo, esto afectará la inversión realizada en la adquisición de las licencias del software y del propio hardware; ya que se tendrá que recurrir a contratar otros servicios para poder resolver las incidencias que se puedan presentar en el servicio de correo ante la falta de un equipo de seguridad adecuado, lo cual generará mayores costos significativos.

7.2 INCIDENCIAS ECONÓMICAS DE LA CONTRATACIÓN

A continuación se muestran el costo promedio referencial sobre el producto sugerido:

N°	Software	Licencias	Fabricante	Precio referencial (S/)
01	Cisco IronPort c380	Sí	Cisco	367,500.00[1]

http://www.midis.gob.pe/index.php/es/transparencia-informacion-adicional/informe-tecnico-previo-de-evaluacion-de-software-ley-28612?portal=midis&start=20

Nota: El costo aproximado es referencial del mercado internacional y fue obtenido desde ofertas publicadas en Internet. Se precisa que es potestad de la Oficina de Abastecimiento, realizar el estudio de mercado, según la normatividad vigente, en la oportunidad que corresponda.

Oficina de Tecnología de Información V°B° Director

Oficina de Tecnología de Información V°B° Seg. de la Información OGA - MTC

Jr. Zorritos 1203 – Lima - Perú
T. (511) 615-7800
www.mtc.gob.pe

El proceso de estandarización de las licencias del dispositivo de seguridad para correo electrónico Cisco IronPort, permite a la entidad proteger la inversión realizada; optimizar costos de adquisición y mantenimiento del software; obtener un ahorro en el costo del servicio de configuración, implementación de una nueva base de datos, capacitaciones, migraciones, actualizaciones, desarrollo de software, contratación de personal, tiempo de duración de las actividades indicadas, entre otras.

8. VERIFICACIÓN DE LOS PRESUPUESTOS PARA LA ESTANDARIZACIÓN

8.1 EQUIPAMIENTO O INFRAESTRUCTURA PREEXISTENTE. La entidad posee determinado equipamiento o infraestructura, pudiendo ser maquinarias, equipos, vehículos u otro tipo de bienes, así como ciertos servicios especializados.

El Ministerio de Transportes y Comunicaciones, cuenta con un bien preexistente (componente físico, hardware; de la solución) denominado "dispositivo (appliance) de seguridad para correo electrónico de la marca Cisco, modelo IronPort", que trabaja con el software "Cisco Email Security" (componente lógico, software; de la solución); instalado en el ambiente de producción del Centro de Datos del MTC.

El bien preexistente brinda una solución de seguridad de correo electrónico, que se puede implementar simple y rápidamente, con pocos requisitos de mantenimiento, baja latencia (retardo) y bajos costos operativos.

8.2 COMPLEMENTARIEDAD AL EQUIPAMIENTO PREEXISTENTE. Los bienes o servicios que se requiere contratar son accesorios o complementarios al equipamiento o infraestructura preexistente.

Se requiere la adquisición de la licencia del software que permite el funcionamiento del dispositivo de seguridad para correo electrónico marca Cisco modelo Ironport, dicho equipo es de propiedad del MTC desde el 2016, encontrándose aún vigente pero se requiere la licencia de software para que dicho equipo pueda operar.

Oficina de Tecnología de Información – V°B° – Director – OFICINA DE TECNOLOGÍA DE INFORMACIÓN – V°B° – Seg. de la Información – OGA - MTC

Jr. Zorritos 1203 – Lima - Perú
T. (511) 615-7800
www.mtc.gob.pe

Las licencias del software son complementarias al bien preexistente (dispositivo de seguridad para correo electrónico Cisco IronPort), porque permite mantener operativo todos los componentes que se integran a la solución, tales como: el motor antivirus, motor de detección de spam, firmas de seguridad, etc.

8.3 LOS BIENES A ADQUIRIR SON IMPRESCINDIBLES PARA LA OPERATIVIDAD. **Los bienes o servicios que se requiere contratar son imprescindibles para garantizar la funcionalidad, operatividad o valor económico del equipamiento o infraestructura preexistente.**

Las licencias de software son imprescindibles para garantizar la funcionalidad, operatividad o valor económico del bien preexistente porque están diseñadas y optimizadas para soportar la funcionalidad, operación y valor económico de dicho bien preexistente (dispositivo de seguridad para correo electrónico Cisco IronPort).

Garantizan la operatividad del bien preexistente (dispositivo de seguridad para correo electrónico Cisco IronPort) porque están diseñadas para operar conjuntamente con dicho bien. Esta interdependencia entre ambos garantiza su operación y nivel de servicio.

Garantizan el valor económico del bien preexistente (dispositivo de seguridad para correo electrónico Cisco IronPort) porque valoran una herramienta de comunicación institucional muy importante para prevenir vectores de ataque a través de brechas de seguridad, que pueden permitir la alteración o pérdida de datos importantes para la institución.

OFICINA DE TECNOLOGÍA DE INFORMACIÓN - V°B° DIRECTOR

9. PERIODO DE VIGENCIA DE LA ESTANDARIZACIÓN

La presente estandarización deberá tener una vigencia de cinco (5) años, contados a partir de la fecha de aprobación del acto resolutivo de estandarización. Sin embargo, de variar las condiciones que determinen su estandarización, su aprobación quedará sin efecto.

Oficina de Tecnología de Información V°B° Seg. de la Información OGA - MTC

Jr. Zorritos 1203 – Lima - Perú
T. (511) 615-7800
www.mtc.gob.pe

10. CONCLUSIONES

Por lo expuesto anteriormente, se concluye que es necesaria la estandarización de las licencia de software del dispositivo de seguridad para correo electrónico Cisco IronPort; para mantener, asegurar, desarrollar y mejorar los servicios informáticos brindados durante el proceso de intercambio de mensajería de los usuarios del MTC.

11. RESPONSABLES

11.1 DE LA EVALUACIÓN

Ing. Luis Roberto Blas Sernaqué – Especialista de normatividad y regulación de TI.

11.2 DIRECTOR DEL ÁREA USUARIA

Ing. Jaime Gutiérrez Rosas – Director de la Oficina de Tecnología de Información.

12. FIRMAS DE LOS RESPONSABLES

Ing. Luis Roberto Blas Sernaqué
Especialista en normatividad y regulación de TI

Ing. Jaime Gutiérrez Rosas
Director de Tecnología de Información

13. FECHA DE ELABORACIÓN

Lima, 20 de noviembre de 2018

Jr. Zorritos 1203 – Lima - Perú
T. (511) 615-7800
www.mtc.gob.pe