CONVOCATORIA PARA LA ELABORACIÓN DEL ESTUDIO DE MERCADO

El Servicio de Rentas Internas (SRI) a través de la Dirección Nacional de Tecnología, convoca a proveedores nacionales e internacionales a participar en el proceso de elaboración del Estudio de Mercado para la **"ADQUISICIÓN DE FIREWALL DE NUEVA GENERACIÓN".**

Este estudio de mercado será utilizado para la definición del presupuesto referencial previo a la publicación del proceso de adquisición.

El precio referencial de los bienes deberá considerar los siguientes aspectos:

- Las especificaciones técnicas detalladas adelante;
- Los precios cotizados deben estar en valor DDP Delivered Duty Paid/ Entregado con derechos pagados, incluyendo todos los derechos de aduanas e impuestos;
- La vigencia de la cotización no debe ser menor a 120 días;
- La fuente de financiamiento será realizada con recursos del Banco Interamericano de Desarrollo, por lo que los oferentes deberán pertenecer a los países miembros del BID;
- El plazo total del contrato es de hasta 1184 días calendario, contados a partir del día siguiente de la subscripción del contrato

Las cotizaciones deben ser remitidas en formato digital (firmadas), al correo institucional programaintax@sri.gob.ec hasta el día 16 de abril de 2024, con los siguientes datos:

Datos del oferente:

Razón Social:
RUC / ID:
Dirección:
Teléfono:
Correo electrónico:
Fecha de emisión de la cotización:
Vigencia de la cotización: (no debe ser menor a 120 días)
Firma de responsabilidad.

Datos del contratante:

A nombre de: Servicio de Rentas Internas
RUC: 1760013210001
Formato Presentación Cotización:

Propuesta Económica: (se solicita incluir CPC 452800041 en la cotización)

Presupuesto total del proyecto:			$	-
DESGLOSE DE COMPONENTES				
Tipo de recurso	Descripción producto / servicio	Cantidad	Costo unitario	Total

Hardware	**GATEWAYS DEL SISTEMA DE FIREWALL** Debe incluir: • Garantía y soporte de fábrica por 1 año, • Licenciamiento y/o suscripciones de seguridad por 1 año, • Accesorios para montaje e instalación, • INSTALACIÓN. Debe especificarse: • Fabricante / marca, • Modelo, • Capacidad, • Descripción del bien.	4		$ -
Hardware	**SOPORTE DE FÁBRICA PARA LOS GATEWAYS DEL SISTEMA DE FIREWALL, POR AÑO** Debe incluir: • Garantía y soporte de fábrica por 1 año de los 4 gateways en total, • Licenciamiento y/o suscripciones de seguridad por 1 año de los 4 gateways en total.	2		$ -
Hardware	**SERVIDORES DE GESTIÓN** Debe incluir: • Garantía y soporte de fábrica por 1 año, • Licenciamiento y/o suscripciones de LOM por 1 año, • Accesorios para montaje e instalación, • INSTALACIÓN. Debe especificarse: • Fabricante / marca, • Modelo, • Capacidad, • Descripción del bien.	2		$ -
Hardware	**SOPORTE DE FÁBRICA PARA LOS SERVIDORES DE GESTIÓN, POR AÑO** Debe incluir: • Garantía y soporte de fábrica por 1 año de los dos servidores en total, • Licenciamiento y/o suscripciones de firmware (ej. LOM, Cache, etc.) por 1 año de los dos servidores en total.	2		$ -
Software	**GESTORES DEL SISTEMA DE FIREWALL** Debe incluir: • Soporte de fábrica por 3 años, • Licenciamiento y suscripciones por 3 años, • INSTALACIÓN. Debe especificarse: • Fabricante / marca, • Descripción del producto.	2		$ -

Software	**COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS** Debe incluir: • Soporte de fábrica por 3 años, • Software base, • Licenciamiento y suscripciones por 3 años, • INSTALACIÓN. Debe especificarse: • Fabricante / marca, • Descripción del producto.	2		$ -
Software	**SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO, POR AÑO** Debe incluir: • Soporte de fábrica por 1 año, • Licenciamiento y suscripciones para 3384 buzones por 1 año. Debe especificarse: • Fabricante / marca, • Descripción del producto.	3		$ -
Servicios	**MIGRACIÓN**	1		$ -
Servicios	**SOPORTE LOCAL, POR 884 DÍAS** Debe incluir: • Mantenimiento preventivo, • Mantenimiento correctivo, • Asistencia técnica.	1		$ -
			Subtotal	$ -
			IVA	$ -
			TOTAL	**$ -**

Nota: Los oferentes deberán garantizar el entendimiento y el cumplimiento de todas las especificaciones técnicas y servicios conexos requeridos.

Listado de países elegibles

- Lista de países miembros cuando el financiamiento provenga del Banco Interamericano de Desarrollo: Alemania, Argentina, Austria, Bahamas, Barbados, Bélgica, Belice, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Croacia, Dinamarca, Ecuador, El Salvador, Eslovenia, España, Estados Unidos, Finlandia, Francia, Guatemala, Guyana, Haití, Honduras, Israel, Italia, Jamaica, Japón, México, Nicaragua, Noruega, Países Bajos, Panamá, Paraguay, Perú, Portugal, Reino Unido, República de Corea, República Dominicana, República Popular de China, Suecia, Suiza, Surinam, Trinidad y Tobago, Uruguay, y Venezuela.

Territorios elegibles

- Guadalupe, Guyana Francesa, Martinica, Reunión – por ser Departamentos de Francia.
- Islas Vírgenes Estadounidenses, Puerto Rico, Guam – por ser Territorios de los Estados Unidos de América.
- Aruba – por ser País Constituyente del Reino de los Países Bajos; y Bonaire, Curazao, Sint Maarten, Sint Eustatius – por ser Departamentos de Reino de los Países Bajos.
- Hong Kong – por ser Región Especial Administrativa de la República Popular de China.

SERVICIO DE RENTAS INTERNAS

ESPECIFICACIONES TÉCNICAS

1. INFRAESTRUCTURA ACTUAL

1. El sistema de Firewalls de Nueva Generación está conformado por software de propósito específico y por una infraestructura de hardware compuesta de servidores de propósito general. La infraestructura de hardware del sistema de Firewalls de Nueva Generación está compuesta por los servidores que se detallan en la tabla a continuación.

ÍTEM NRO.	EQUIPO	MARCA	MODELO	CIUDAD
1	Servidor del Clúster de Firewalls de Producción	HPE	ProLiant DL380 Gen10	Quito
2	Servidor del Clúster de Firewalls de Producción	HPE	ProLiant DL380 Gen10	Quito
3	Servidor del Clúster de Firewalls de Contingencia	HPE	ProLiant DL380 Gen10	Guayaquil
4	Servidor del Clúster de Firewalls de Contingencia	HPE	ProLiant DL380 Gen10	Guayaquil
5	Servidor del Gestor de Políticas de Producción	HPE	ProLiant DL360 Gen10	Quito
6	Servidor del Gestor de Políticas de Contingencia	HPE	ProLiant DL360 Gen10	Guayaquil
7	Servidor del Gestor de Eventos de Producción	HPE	ProLiant DL360 Gen10	Quito

Tabla 1. Detalle de los servidores que conforman el sistema de Firewalls de Nueva Generación del SRI.

2. El SRI tiene el identificador de cuenta No. 8053728 en el sistema Check Point User Center.

3. El sistema de firewalls tiene componentes ubicados en los centros de datos principal y alterno del SRI, en Quito y Guayaquil respectivamente.

4. La garantía técnica de fábrica de la infraestructura de hardware del sistema de Firewalls de Nueva Generación está vigente hasta el 3 de diciembre de 2024. El licenciamiento del sistema de Firewalls de Nueva Generación, y el soporte de fábrica del software, está vigente hasta el 16 de mayo de 2025.

5. El sistema de firewalls del SRI cuenta con alrededor de 1.200 reglas de seguridad distribuidas en 5 paquetes de políticas, uno por cada sistema (firewall) virtual.

6. El SRI cuenta con 600 licencias Microsoft Office 365 E3 que incluyen aplicaciones tales como, la suite de office, SharePoint Online, OneDrive for Business, Exchange Online, Microsoft Teams, entre otros.

7. El SRI cuenta con un sistema de directorio compuesto por:

- **7.a.** Microsoft Active Directory, desplegado en Microsoft Windows Server 2019 en la red informática del SRI;
- **7.b.** Microsoft Entra ID (Azure AD), desplegado en los servicios en línea (“cloud”) de Microsoft Office 365 E3.

8. El sistema de directorio Microsoft Active Directory del SRI está conformado por 12 controladores de

dominio, de los cuales 2 se encuentran en el centro de datos principal, 1 en el centro de datos alterno y el resto se encuentra distribuido entre las agencias a nivel nacional.

9. El sistema de correo electrónico del SRI tiene un total de 3.384 buzones y está conformado por:

9.a. Microsoft Exchange 2019, desplegado en la red informática del SRI;

9.b. Microsoft Exchange Online, como parte del servicio Office 365 E3 del SRI.

10. El sistema local de correo electrónico del SRI está conformado por 8 servidores Microsoft Exchange 2019, de los cuales 7 se encuentran en el centro de datos principal y 1 en el centro de datos alterno.

11. El SRI cuenta con una infraestructura de switch de core cuyos componentes se detallan a continuación:

COMPONENTE	SITIO	FABRICANTE	MODELO	VERSION	CANT.
APIC	CD Principal	Cisco	–	5.2 (8g)	1
Switch spine	CD Principal	Cisco	N9K-C9364C	–	2
Switch leaf	CD Principal	Cisco	N9K-C93108TC-FX	–	5
Switch leaf	CD Principal	Cisco	N9K-C9336C-FX2	–	4
Switch leaf	CD Principal	Cisco	N9K-C93180YC-FX	–	6
Switch leaf	CD Principal	Cisco	N9K- C93180YC-FX3	–	1
Switch spine	CD Alterno	Cisco	N9K-C9332D-GX2B	–	2
Switch leaf	CD Alterno	Cisco	N9K-C9336C-FX2	–	2
Switch leaf	CD Alterno	Cisco	N9K-C93108TC-FX3P	–	1
Switch leaf	CD Alterno	Cisco	N9K-C93180YC-FX3	–	3

Tabla 2. Detalle de los componentes de la infraestructura de switch de core del SRI.

12. El SRI cuenta con una plataforma de virtualización cuyos componentes se detallan a continuación.

COMPONENTE	SITIO	FABRICANTE	SOFTWARE	VERSIÓN
Servidor de gestión	CD Principal	VMware	vCenter Standard	7.0.3
Hipervisores	CD Principal	VMware	ESXi vSphere Enterprise Plus	7.0.3
Servidor de gestión	CD Alterno	VMware	vCenter Standard	6.7.0
Hipervisores	CD Alterno	VMware	ESXi vSphere Enterprise Plus	6.7.0

Tabla 3. Detalle de las versiones de software de los componentes de la plataforma de virtualización del SRI.

13. El SRI cuenta con tomas eléctricas con las siguientes especificaciones para la alimentación de los equipos:

COMPONENTE	SITIO	SOCKET	VOLTAJE
Gateways	CD Principal	Nema 5-15P	110 V-AC
Gestores	CD Principal	C14	220 V-AC
Gateways	CD Alterno	Nema 5-15P	220 V-AC

COMPONENTE	SITIO	SOCKET	VOLTAJE
Gestores	CD Alterno	Nema 5-15P	110 V-AC

Tabla 4. Detalle de los tomacorrientes donde se conectarán los competentes de hardware.

14. El SRI cuenta con bastidores ("racks") con las siguientes dimensiones para el montaje de los equipos:

COMPONENTE	SITIO	ANCHO	PROFUNDIDAD
Gateways	CD Principal	19"	22"
Gestores	CD Principal	19"	28"
Gateways	CD Alterno	19"	29"
Gestores	CD Alterno	19"	29"

Tabla 5. Dimensiones de los bastidores ("racks") donde se montarán los competentes de hardware.

NOTA: Toda la información de este apartado ha sido levantada a la fecha del presente documento. Esta puede variar en función de la operación y las necesidades institucionales y de las nuevas liberaciones de los fabricantes. Es responsabilidad del contratista hacer las validaciones correspondientes oportunamente.

2. BIENES REQUERIDOS

2.1. COMPONENTE DE HARDWARE

2.1.1. CAPACIDAD DEL HARDWARE

A. CONDICIONES GENERALES	
1.	La infraestructura del sistema de Firewalls de Nueva Generación (NGFW) debe estar constituida por hardware para centros de datos.
2.	La infraestructura deberá estar conformada por los siguientes componentes: o (2) Clúster de firewall, principal y alterno; o (2) Servidores de gestión, principal y alterno.
3.	Para garantizar la vigencia tecnológica, solamente se aceptan equipos cuyo modelo se hayan liberado desde el año 2022 en adelante.
	MONTAJE DE LOS EQUIPOS
4.	Todos los equipos deben ser servidores de bastidor ("rack-mounted servers") compatibles con las condiciones físicas de los centros de datos del SRI que constan en la **INFRAESTRUCTURA ACTUAL**.
5.	Todos los equipos deben contar con los rieles, sujetadores y demás accesorios necesarios para un montaje seguro y organizado en los centros de datos del SRI.

B. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO (4 EQUIPOS)	
1.	Los clúster de firewall, principal y alterno, deben tener capacidades, características y funcionalidades iguales.
2.	Tanto el Clúster de firewall principal como el Clúster de firewall alterno, el software del Gestor de firewall principal y el software del Gestor de firewall alterno deben ser del mismo fabricante.
3.	Cada clúster de firewall debe estar conformado por no menos de dos (2) gateways físicos (nodos) y estos deberán cumplir con las especificaciones que se detallan a continuación.
4.	Cada gateway físico (nodo) del clúster deberá consistir en un appliance de propósito específico que debe cumplir con las características que se detallan en los numerales a continuación.

5.	Capacidad de procesamiento de tráfico: • Cada gateway físico (nodo) debe tener la capacidad de procesar un volumen de tráfico ("throughput") no menor a **32.92 Gbps** con todas las funciones de seguridad habilitadas y operando a plena carga, entre las que se incluyen: o Firewall (FW), o Control de navegación, o Sistema de prevención de intrusiones (IPS), o Protección antimalware, o Protección contra amenazas no basada en firmas, o VPN de sitio a sitio ("site-to-site"), o VPN de acceso remoto ("remote access").
6.	Capacidad de procesamiento de tráfico SSL/TLS: • Cada gateway físico (nodo) debe tener la capacidad de realizar la inspección SSL/TLS de un volumen de tráfico ("throughput") no menor a **1532 Mbps**, para las funciones de seguridad que se detallan: o Protección IPS de los servidores del SRI publicados en internet y alojados en la DMZ del sistema de Firewall. • Cada gateway físico (nodo) debe tener la capacidad de realizar la inspección SSL/TLS de un volumen de tráfico ("throughput") no menor a **492 Mbps**, para las funciones de seguridad que se detallan: o Control de navegación, o Protección IPS de los clientes internos del SRI, o Protección antimalware, o Protección contra amenazas no basada en firmas. **NOTA:** Las condiciones en las que se debe cumplir con este requerimiento se establecen en el apartado **INSPECCIÓN SSL/TLS** del componente **A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO** en la sección **4.1.2. FUNCIONALIDAD DEL HARDWARE**.
7.	Almacenamiento: • Cada equipo debe tener un volumen de almacenamiento con una capacidad de no menos de 480GB de espacio; • El volumen de almacenamiento debe estar constituido por un arreglo RAID1, RAID10, RAID5 o RAID6; • El volumen de almacenamiento debe estar conformado por al menos dos (2) unidades de estado sólido (SSD).
8.	Conexión de red para tráfico de datos: • Cada equipo debe tener no menos de dos (2) interfaces físicas independientes (no compartidas) Ethernet 40 Gbps Base-SR QSFP+ LC; • Cada equipo debe tener no menos de una (1) interfaz Ethernet 10 Gbps Base-SR SFP+ LC; • Cada equipo debe contar con los transceptores ("transceivers") propios de fábrica necesarios para la operación de las interfaces de tráfico de datos.
9.	Conexión de red para sincronización: • Cada equipo debe tener no menos de una (1) interfaz para sincronización; • La interfaz de sincronización puede ser de tecnología propietaria (ej. factor de forma, protocolo, estándar, etc.), en cuyo caso el contratista deberá proveer todos los componentes físicos y lógicos para su operación; • Si la interfaz de sincronización es de tecnología abierta, cada equipo debe tener una (1) interfaz Ethernet 10 Gbps Base-SR SFP+ LC; • Cada equipo debe contar con los transceptores ("transceivers") propios de fábrica necesarios para la operación de las interfaces de sincronización.
10.	Conexión de red para administración: • Cada equipo debe tener una (1) interfaz Ethernet 1 Gbps BASE-T o BASE-SR; • Cada equipo debe contar con el transceptor ("transceiver") propio de fábrica necesario para la operación de la interfaz de administración.
11.	Alimentación: • Cada equipo debe tener instaladas dos fuentes de alimentación (PSU) redundantes tipo "hot-swap"; • Cada fuente de alimentación debe soportar un rango de entrada de 110-220 VAC o uno más amplio.

C. SERVIDORES DE GESTIÓN PRINCIPAL Y ALTERNO (2 EQUIPOS)	
1.	Los servidores de gestión principal y alterno deben tener capacidades, características y funcionalidades iguales.
2.	Cada servidor de gestión debe cumplir con las especificaciones que se detallan a continuación.
3.	Cada servidor de gestión debe contar con una protección frontal que impida la manipulación no autorizada de los componentes del servidor.

4. Procesamiento:
- Cada equipo debe tener instalados no menos de 48 núcleos (“cores”) físicos de procesamiento;
- Los núcleos (“cores”) físicos de procesamiento pueden estar distribuidos entre uno (1) o dos (2) procesadores, dependiendo de la arquitectura del fabricante;
- Cada procesador debe tener una frecuencia base de operación de no menos de 2.6 GHz.

5. Memoria RAM:
- Cada equipo debe tener instalado un total de memoria RAM de no menos de 256 GB;
- La cantidad definitiva de memoria RAM estará determinada por las condiciones de instalación que se indican en el punto a continuación;
- La instalación de memoria RAM de cada equipo debe cumplir con las condiciones de alto desempeño que se indican a continuación:
  - Se deben ocupar todos los canales de memoria de cada procesador instalado con al menos un módulo,
  - Todos los módulos de memoria deben ser de tipo DDR5, RDIMM, Single Rank,
  - Todos los módulos de memoria deben soportar una velocidad de bus de no menos de 4400 MHz,
  - Todos los módulos de memoria deben tener la misma capacidad.

6. Almacenamiento:
- Cada equipo debe tener dos grupos de unidades de almacenamiento;
- El primer grupo debe estar conformado por dos (2) unidades, cada una de no menos de 3.84 TB;
- Las unidades de almacenamiento del primer grupo deben cumplir con las siguientes características:
  - Unidad de tipo SAS,
  - Unidad de estado sólido (SSD) de uso mixto o intermedio o de escritura intensiva,
  - Unidad de 2.5” (SFF),
  - Con velocidad de transferencia de 12 Gbps,
  - Con duración DWPD (“drive writes per day”) de no menos de 3,
  - De montaje tipo “hot-swap”;
- El segundo grupo debe estar conformado por veintidós (22) unidades, cada una de no menos de 2.4 TB;
- Las unidades de almacenamiento del segundo grupo deben cumplir con las siguientes características:
  - Unidad de tipo SAS,
  - Unidad de disco duro (HDD) de 10Krpm o superior,
  - Unidad de 2.5” (SFF),
  - Con velocidad de transferencia de 12 Gbps,
  - De montaje tipo “hot-swap”.

7. Controladora del Almacenamiento:
- Cada equipo debe tener instalada no menos de una (1) controladora física de almacenamiento;
- La controladora de almacenamiento debe soportar unidades SAS;
- La controladora de almacenamiento debe soportar una velocidad de transferencia de 24 Gbps;
- La controladora de almacenamiento debe tener integrada una caché de escritura respaldada por flash (FBWC) de no menos de 8 GB;
- La controladora debe incluir una batería que permita retener la caché de escritura respaldada por flash (FBWC) en caso de interrupción de la alimentación del equipo;
- La controladora de almacenamiento debe tener activada y licenciada la funcionalidad de caching de escritura de forma que pueda utilizar las unidades de estado sólido (SSD) incluidas en el almacenamiento;
- La controladora debe soportar al menos la creación de arreglos RAID 1, RAID10, RAID 5 y RAID 6.

8. Conexión de Red:
- Cada equipo debe tener una (1) interfaz Ethernet 25Gbps Base-SR SFP+ LC;
- Cada equipo debe contar con los transceptores (“transceivers”) ópticos propios de fábrica necesarios para la operación de las interfaces Ethernet 25 Gbps.

9.	Administración Remota: • Los equipos deben contar con una función avanzada de monitoreo y administración remota (“lights-out management”) del hardware de estos. • Esta función debe estar licenciada por la duración de la garantía técnica. • Esta función debe contar al menos con las siguientes características: o Monitoreo basado en SNMP, o Actualización remota de firmware, o Consola gráfica de acceso remoto, o Consola de línea de comandos de acceso remoto SSH, o Medios virtuales (ej. CD’s, DVD’s, etc.), o Monitoreo de salud del equipo, o Autenticación mediante integración con Directorio Activo, o Una (1) interfaz Ethernet 1Gbps Base-T RJ-45. **NOTA:** Los detalles del Directorio Activo están disponibles en la **INFRAESTRUCTURA ACTUAL**.
10.	Configuración de Alto Desempeño: • El firmware de cada equipo debe tener la funcionalidad de alto desempeño (“high performance”) o equivalente; • Cada equipo debe contar con los módulos de disipación de calor, ventiladores y fuentes de alimentación (PSU) dimensionados para soportar la operación de este en modo alto desempeño (“high performance”) o equivalente.
11.	Alimentación: • Cada equipo debe tener instaladas dos fuentes de alimentación (PSU) redundantes tipo “hot-swap”; • Cada fuente de alimentación debe soportar un rango de entrada de 110-220 VAC o más amplio; • Cada fuente de alimentación debe tener una eficiencia de no menos del 90%.

2.1.2. FUNCIONALIDAD DEL HARDWARE

A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO	
1.	El sistema de Firewalls de Nueva Generación (NGFW) debe ser una solución de tipo empresa (“enterprise”) o superior. No aplican soluciones de tipo UTM (“unified threat management”) o SMB (“small business”).
2.	Todas las funciones y módulos que comprenden los **CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO** deben pertenecer a la misma solución y al mismo fabricante.
3.	Los Clúster de firewall principal y alterno deben tener capacidades, características y funcionalidades iguales.
4.	Cada Clúster de gateways debe contar con las siguientes funcionalidades: • Networking, • Alta disponibilidad, • Firewall (FW), • Control de navegación, • Sistema de prevención de intrusiones (IPS), • Protección antimalware, • Protección contra amenazas no basada en firmas, • Virtualización de sistemas, • Inspección SSL/TLS, • Identificación de usuarios, • VPN de sitio a sitio (“site-to-site”), • VPN de acceso remoto (“remote access”).
	NETWORKING
5.	El Firewall debe operar en modo capa 3 del modelo OS, esto es, como pasarela (“gateway”).
6.	El Firewall debe soportar la configuración de reglas NAT (“Network address Traslation”) y PAT (“Port address Traslation”).
7.	El Firewall debe soportar la configuración de reglas NAT66 y NAT64.
8.	El Firewall debe soportar los protocolos Virtual Extensible LAN (VXLAN) y Generic Routing Encapsulation (GRE).
9.	El Firewall debe soportar enrutamiento estático, protocolos de enrutamiento dinámico, tales como, RIP, BGP, OSPFv2, OSPFv3 y ruteo multicast.
10.	El Firewall debe soportar enrutamiento basado en políticas PBR (“policy based routing”) o reenvío basado en políticas PBF (“policy based forwarding”).

11.	El Firewall debe soportar etiquetamiento VLAN (“VLAN tagging”) mediante el protocolo IEEE 802.1Q y también debe soportar la configuración de sub-interfaces ethernet lógicas.
12.	El Firewall debe soportar agregación de interfaces de red mediante el protocolo IEEE 802.3ad LACP (Link Aggregation Control Protocol).
13.	El Firewall debe soportar jumbo frames.
	ALTA DISPONIBILIDAD
14.	Todos los nodos que conforman deben operar en un esquema de alta disponibilidad de forma que al fallar uno de los nodos el resto asume esa carga.
15.	El clúster de firewall debe soportar los siguientes esquemas de alta disponibilidad: • Activo-Pasivo, en el que solamente un nodo está activo y soporta toda la carga. • Activo-Activo, en el que todos los nodos están activos y comparten la carga.
16.	Como parte del esquema de alta disponibilidad se debe monitorear el fallo de conexiones en los nodos, ya sea ante la desconexión de al menos una de las interfaces del equipo, la desconexión de un enlace físico adyacente o la pérdida de conexión hacia una IP desde una de las interfaces.
17.	Como parte del esquema de alta disponibilidad se debe cifrar la comunicación entre todos los nodos que conforman el clúster de firewall.
	FIREWALL (FW)
18.	El Firewall debe ser soportar la configuración de políticas de seguridad mediante: • zonas, • puertos, servicios o aplicaciones, • direcciones IP, • segmentos y/o rangos de red, • país o región geográfica, • usuarios o grupos de usuarios, • direcciones URL, • tipo de archivos, • grupos de lo antes mencionado.
19.	El Firewall debe soportar la creación de reglas basadas en horarios o rangos de tiempo.
20.	El Firewall debe soportar el uso de etiquetas en los objetos para su referenciación o agrupación.
21.	El Firewall debe contar con la opción de utilizar la negación como parte de la lógica de la condición de origen o de destino de las reglas de seguridad.
22.	El Firewall debe soportar la creación de reglas temporizadas.
23.	El Firewall debe soportar la deshabilitación de reglas, sin la necesidad de eliminarlas.
24.	El Firewall debe soportar hacer grupos de reglas de seguridad utilizando etiquetas u otro método.
25.	El Firewall debe soportar que se añada un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y control de cambios.
26.	El Firewall debe mostrar la fecha de la primera y la última vez que se utilizó una regla de seguridad.
27.	El Firewall debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
28.	El Firewall debe mostrar el conteo de las veces que el tráfico ha coincidido (“hits”) con cada regla.
29.	El Firewall debe soportar la configuración de reglas y objetos para controlar tráfico VoIP.
	CONTROL DE NAVEGACIÓN
30.	El Firewall debe contar con la función de control de navegación en base a la identificación y clasificación de sitios web y de aplicaciones en línea.
31.	El Firewall debe aplicar la función de control de navegación mediante acciones tales como: permitir, bloquear, aplicar control por tiempo.

32.	El Firewall debe ser capaz de clasificar el tráfico de navegación en no menos de 70 categorías, incluyendo al menos las categorías que se muestran a continuación o sus equivalentes: • Sitios o aplicaciones maliciosos, • Sitios o aplicaciones de elusión de control, • Sitios o aplicaciones de anonimización, • Sitios o aplicaciones de redes sociales, • Sitios o aplicaciones de Microsoft Office 365, • Sitios o aplicaciones de actualización de software, • Sitios o aplicaciones de multimedia en línea, • Sitios o aplicaciones de almacenamiento virtual personal, • Sitios o aplicaciones de almacenamiento virtual organizacional, • Sitios o aplicaciones de transmisión de archivos, • Sitios o aplicaciones de mensajería instantánea, • Sitios o aplicaciones de acceso remoto, • Sitios o aplicaciones de colaboración o video conferencia, • Sitios o aplicaciones financieros, • Sitios o aplicaciones de gobierno, • Sitios o aplicaciones de correo electrónico, • Sitios o aplicaciones de inteligencia artificial, • Sitios o aplicaciones de intercambio de archivos peer-to-peer (P2P), entre otros.
33.	El Firewall debe soportar la creación de categorías personalizadas (“custom”).
34.	El Firewall debe contar con la capacidad de clasificar en línea las direcciones URL que aún no cuentan con categoría de contenido o categoría de seguridad para así aplicarle el control respectivo.
35.	El Firewall debe ser capaz de discriminar no menos de 3000 aplicaciones en línea.
36.	El Firewall debe reconocer y controlar el tráfico de aplicaciones en línea sin importar si se está utilizando el puerto estándar (TCP o UDP) o uno distinto. Por ejemplo, debe poder identificar el protocolo HTTPS ya sea que la conexión se establezca por el puerto TCP 443 o por otro puerto y debe aplicar el control respectivo.
37.	El Firewall debe contar con la capacidad de identificar las aplicaciones en base a las características del tráfico detectado.
38.	El Firewall debe controlar funciones u operaciones internas de las aplicaciones en línea, tales como, mensajería instantánea y compartición de archivos.
39.	El Firewall debe soportar la creación de aplicaciones y grupos de aplicaciones personalizados (“custom”).
40.	El Firewall debe contar con un mecanismo que permita representar servicios, aplicaciones o sistemas que por su naturaleza dinámica cambian constantemente de direcciones URL, dominios, nombres de host (“hostnames”) o direcciones IP, tales como, las aplicaciones de Microsoft Office 365, los servicios de Microsoft Azure, etc.
41.	El Firewall debe contar con la capacidad de insertar o modificar los valores en la cabecera HTTP del tráfico de aplicaciones SaaS.
42.	El Firewall debe permitir que se apliquen horarios o rangos de tiempo a los permisos de navegación.
43.	El Firewall debe permitir que se apliquen los permisos de navegación en función de usuarios y grupos de Active Directory y de direcciones IP específicas y de rangos o segmentos de red.
44.	El Firewall debe permitir la personalización de la página de bloqueo.
	PROTECCIÓN ANTIMALWARE
45.	El Firewall debe detectar y bloquear la transferencia de archivos maliciosos a través de los protocolos HTTP (versiones 1.0, 1.1, 2.0), HTTPS, FTP, SMB (versiones 1, 2, 3).
46.	El Firewall debe tener la capacidad de inspeccionar los archivos comprimidos (zip, gzip, etc.) del tráfico analizado.
47.	El Firewall debe identificar e incluir en el registro de eventos (“logs”) el nombre del país de donde provino la amenaza de seguridad detectada.
48.	El Firewall debe contar con la opción de realizar la captura de paquetes (PCAP) de las conexiones asociadas con las amenazas de seguridad detectadas para efecto de análisis forense.
49.	El Firewall debe detectar y bloquear ataques de tipo “DNS Tunneling”.
50.	El Firewall debe identificar y bloquear las consultas DNS asociadas con malware o algún otro tipo de amenazas de seguridad detectada.
51.	El Firewall debe contar con la capacidad de proporcionar una respuesta falsa a consultas DNS asociadas con malware o algún otro tipo de amenazas de seguridad detectada (“Sinkhole”).
52.	El Firewall debe detectar y bloquear conexiones hacia sitios maliciosos cuyos nombres fueron creados a través de algoritmos de generación de dominios (DGA).
53.	Los dos nodos del clúster del Firewall deben contar con el mismo paquete o grupo de firmas sincronizadamente.

54.	El Firewall debe contar con la opción de realizar la captura de paquetes (PCAP) de las conexiones asociadas con las amenazas de seguridad detectadas para efecto de análisis forense.
	SISTEMA DE PREVENCIÓN DE INTRUSIONES (IPS)
55.	El Firewall debe contar con la función de sistema de prevención de intrusos (IPS) integradamente en el mismo equipo.
56.	La función IPS debe tener la capacidad de analizar todos los protocolos identificados y detectados por la función de Firewall.
57.	Las reglas de seguridad de la función de IPS deben contar con al menos las siguientes opciones de acción o su equivalente: • Bloquear y registrar la amenaza identificada; • Detectar (y no bloquear) y registrar la amenaza identificada.
58.	Las firmas de la función IPS debe deben incluir al menos los siguientes grupo de firmas de protección o sus equivalentes: • Protecciones contra explotación de vulnerabilidades de protocolos de comunicación, • Protecciones contra explotación de vulnerabilidades de firmware, • Protecciones contra explotación de vulnerabilidades de sistemas operativos (servidores y clientes), • Protecciones contra explotación de vulnerabilidades de aplicaciones web, • Protecciones contra explotación de vulnerabilidades de servidores web, • Protecciones contra explotación de vulnerabilidades de servidores de aplicación, • Protecciones contra explotación de vulnerabilidades de bases de datos, • Protecciones contra explotación de vulnerabilidades de aplicaciones de escritorio (clientes), • Protecciones contra phishing, • Protecciones contra malware, redes autómatas (“botnets”), gusanos de red, etc.
59.	Las firmas de tipo Vulnerabilidades de aplicaciones web deben incluir protecciones contra de ataques de tipo “SQL injection”, “Cross Site Scritping”, “Directory traversal”.
60.	Las firmas deben incluir protecciones contra de ataques de tipo escaneo de puertos TCP y UDP, “Host Sweep”, entre otros.
61.	La función IPS debe tener la capacidad de inspeccionar tráfico en túneles de protocolos de aplicación, tales como: • Túneles en protocolo DNS, • Túneles en protocolo HTTP, • Túneles en protocolo GRE.
62.	La función IPS debe incluir un servicio de reputación actualizado periódicamente que incluya las direcciones IP, direcciones URL, hostnames y dominios que han sido reconocidos por ser parte de un ataque o que representan un alto riesgo de seguridad.
63.	La función IPS debe la capacidad de: • “fail open”, esto es, que en caso de sobre carga o falla de la función de IPS se deje pasar el tráfico sin analizar; • “fail close”, esto es, que en caso de sobre carga o falla de la función de IPS se bloque el tráfico.
64.	La función IPS debe mantener una actualización continua de las firmas, fuentes de mala reputación, listado de malware conocido y otros insumos que las diferentes tecnologías de protección necesiten, de manera automática, desde una red de inteligencia global propia del Fabricante de la solución ofertada.
65.	La función IPS debe permitir de la configuración de excepciones en la aplicación de los bloqueos en base a: • Origen, • Destino, • Servicio, o puerto o aplicación, • Tipo de protección, • Una combinación de las anteriores.
66.	La función IPS debe soportar la creación o importación de firmas de tipo “open source”, tales como, SNORT.
67.	La función IPS debe tener la capacidad de aplicar reglas de protección en función de la geolocalización del origen o el destino del tráfico.
68.	El Firewall debe contar con la opción de realizar la captura de paquetes (PCAP) de las conexiones asociadas con las amenazas de seguridad detectadas para efecto de análisis forense.
	PROTECCIÓN CONTRA AMENAZAS NO BASADA EN FIRMAS
69.	El Firewall debe contar con una función de protección contra amenazas no basada en firmas que debe detectar y bloquear malware y amenazas no conocidas mediante el uso de un mecanismo de análisis “inline” del tráfico.
70.	La función de protección contra amenazas no basada en firmas se podrá desarrollar en el mismo equipo o mediante el uso de un equipo complementario o mediante el uso de un servicio “cloud” del mismo fabricante.
71.	La función de protección contra amenazas no basada en firmas debe incluir el uso del análisis de caja de arena (“sandboxing”) y de aprendizaje automático (“machine learning”).
72.	La función de protección contra amenazas no basada en firmas debe detectar y bloquear la transferencia de malware y amenazas no conocidas a través de los protocolos HTTP, HTTP/2, HTTPS, FTP, SMB (versiones 1, 2, 3).

73.	La función de protección contra amenazas no basada en firmas debe ejecutar o detonar los archivos sospechosos en el ambiente de caja de arena ("sandbox") de forma automática una vez identificados en el tráfico analizado.
74.	El ambiente de caja de arena ("sandbox") debe soportar la ejecución o detonación de al menos los tipos de archivos que se indican a continuación para su análisis. • Archivos ejecutables, incluyendo: EXE, DLL, JAR, DMG, PKG; • Archivos de Microsoft Office, incluyendo: DOC, DOCX, XLS, XLSX, PPT, PPTX; • Archivos de formato portable, incluyendo: PDF; • Archivos comprimidos, incluyendo: ZIP, RAR, 7Z; • Archivos de scripts, incluyendo: VBS, PS1, JS.
75.	La función de protección contra amenazas no basada en firmas debe contar con la opción para que el administrador cargue archivos manualmente al ambiente de caja de arena ("sandbox") para su análisis.
76.	La función de protección contra amenazas no basada en firmas debe detectar y bloquear las conexiones hacia direcciones URL que corresponden a phishing, intentos de explotación, intentos de sustracción de datos (ej. de credenciales), conexiones de tipo comando y control. Esta acción debe realizarse independientemente de la categoría original a la que pertenezca la dirección URL en el módulo de control de navegación.
77.	El ambiente de caja de arena ("sandbox") debe contar con mecanismos aprueba de las técnicas de evasión utilizadas por los ataques de malware sofisticados de manera que se logre su detección bloqueo.
78.	La función de protección contra amenazas no basada en firmas debe incluir ambientes de caja de arena ("sandbox") con sistema operativo Microsoft Windows.
79.	La función de protección contra amenazas no basada en firmas debe obtener un veredicto respecto de un archivo analizado en un lapso no mayor a 5 minutos.
80.	La función de protección contra amenazas no basada en firmas debe emplear mecanismo basados en aprendizaje automático ("machine learning") para analizar imágenes en páginas web y determinar si están imitando marcas conocidas como parte de una campaña phishing.
81.	La función de protección contra amenazas no basada en firmas debe permitir al administrador la descarga de una copia o muestra de los archivos identificados como malware o como parte de un ataque.
82.	La función de protección contra amenazas no basada en firmas debe utilizar aprendizaje automático ("machine learning") para identificar las conexiones que utilizan DGA (algoritmos de generación de dominios).
83.	La función de protección contra amenazas no basada en firmas debe permitir reportar al fabricante los falsos positivos y los falsos negativos.
84.	La función de protección contra amenazas no basada en firmas debe generar automáticamente las firmas para el malware nuevo detectado y debe bloquear el acceso a las direcciones URL maliciosas asociadas a este.
	INSPECCIÓN SSL/TLS
85.	El firewall debe contar con la capacidad de realizar inspección SSL/TLS del tráfico, esto es, descifrar el tráfico ("payload" y "header") para realizar el análisis de seguridad y volver a cifrar. El mencionado análisis de seguridad debe aplicar para los módulos que se mencionan a continuación: • Protección IPS de los servidores del SRI publicados en internet y alojados en la DMZ del sistema de firewalls. • Protección IPS de los clientes internos del SRI, • Control de navegación, • Protección antimalware, • Protección contra amenazas no basada en firmas.
86.	En cuanto a la protección perimetral, la función de inspección SSL/TLS debe soportar al menos los siguientes modos de operación: • Inspección del tráfico SSL/TLS del tráfico HTTPS saliente, por ejemplo, el tráfico de navegación en Internet de los clientes y de los servidores internos del SRI. • Inspección del tráfico SSL/TLS del tráfico HTTPS entrante, por ejemplo, el tráfico de las transacciones que realizan los contribuyentes en los servidores web del SRI publicados en Internet (DMZ).
87.	La función de inspección SSL/TLS debe descifrar el tráfico HTTPS de sitios web, internos o externos, que utilizan certificados digitales firmados mediante los siguientes algoritmos de llave pública (PKI): • ECC, con módulo de 256 bits hasta 384 bits; • RSA, con módulo de 1024 bits hasta 4096 bits.
88.	La función de inspección SSL/TLS debe descifrar el tráfico que utilice el protocolo TLS versiones: 1.3, 1.2, 1.1 y 1.0.
89.	La función de inspección SSL/TLS debe descifrar el tráfico que utilice los siguientes algoritmos para intercambio de claves en los "cipher suites": • ECDHE, • RSA.

90.	La función de inspección SSL/TLS debe descifrar el tráfico que utilice los siguientes algoritmos para autenticación o firma digital en los "cipher suites": • ECDSA, • RSA.
91.	La función de inspección SSL/TLS debe descifrar el tráfico que utilice los siguientes algoritmos para cifrado de datos en los "cipher suites": • AES –al menos en modo de operación GCM–, • CHACHA20, • RC4.
92.	La función de inspección SSL/TLS debe descifrar el tráfico que utilice los siguientes algoritmos para validación de integridad en los "cipher suites": • SHA384, • SHA256, • SHA-1, • POLY1305.
93.	La función de inspección SSL/TLS debe soportar los protocolos HTTP/1.1 y HTTP/2.0.
94.	La función de inspección SSL/TLS debe incluir la revisión del SNI ("Server Name Indications"), del CN ("Common Name") y del SAN ("Subject Alternative Name") en el certificado de los sitios web externos.
95.	La función de inspección SSL/TLS debe soportar la opción de integrarse con sistemas HSM ("Hardware Security Module") para almacenar claves criptográficas y certificados SSL/TLS.
96.	La función de inspección SSL/TLS debe incluir la verificación del certificado de los sitios web externos mediante CRL ("Certificate Revocation List").
97.	La función de inspección SSL/TLS debe tener la capacidad de bloquear conexiones a sitios web externos que utilizan protocolos de cifrado obsoletos o inseguros.
98.	La función de inspección SSL/TLS de tráfico saliente debe permitir el descifrado selectivo en base a categorías de navegación, ya sea por tipo de contenido o por nivel de riesgo o por representar contenido sensible, y en base a nombres de host ("hostnames") y dominios.
	IDENTIFICACIÓN DE USUARIOS
99.	El Firewall debe contar con una función de identificación de usuarios internos.
100.	Para la identificación de usuarios internos, el Firewall debe soportar al menos dos tipos de métodos: • Identificación o autenticación transparente de usuarios; • Identificación o autenticación explícita de usuarios.
101.	La función de identificación de usuarios debe soportar ser desplegada al menos de las siguientes formas: • Sin agente ("agentless"); • Instalando un agente en los puntos finales.
102.	La función de identificación de usuarios debe soportar ser integrada al menos con las siguientes plataformas de directorio: • Microsoft Active Directory, • Microsoft Entra ID (Azure AD), • Servidores LDAP Linux, • Servidores RADIUS, • Servidores de autenticación de red (ej. AAA, NAC, etc.)
103.	La función de identificación de usuarios debe soportar al menos los siguientes protocolos: • LDAP y LDAPS, • DCE/RPC, • Kerberos v5, • RADIUS, • IEEE 802.1x.
104.	La función de identificación de usuarios debe tener la capacidad de leer las cabeceras XFF ("X-Forward-For") para obtener información de la identidad del usuario que está navegando mediante un proxy web.
105.	La función de identificación de usuarios debe tener la capacidad de eliminar en el tráfico saliente a Internet las cabeceras XFF ("X-Forward-For") introducidas por el proxy web.
106.	La función de identificación de usuarios debe permitir que se creen reglas en base a usuarios o grupos de usuarios.
107.	La función de identificación de usuarios debe soportar el uso de grupos anidados de usuarios.
108.	La función de identificación de usuarios debe tener la capacidad de que los gateways (físicos y virtuales) compartan las tablas de asociación identidad–dirección IP entre ellos, de manera que cuando el tráfico del usuario tiene que atravesar varios nodos o firewalls, si el primero ya lo identifica, no sea necesario que los demás soliciten autenticación, sino que estos ya lo reconozcan. Esto debe aplicar tanto para conexiones internas como para conexiones de acceso remoto por VPN.

	VPN DE SITIO A SITIO (“SITE-TO-SITE”)
109.	El Firewall debe incluir la función de VPN de sitio-a-sitio (“site-to-site”), esto es, conexiones de redes informáticas externas con la red informática institucional mediante un canal seguro.
110.	La función de VPN de sitio-a-sitio debe utilizar protocolo IPSEC.
111.	La función de VPN de sitio-a-sitio debe hacer intercambio seguro de llave utilizando protocolos IKE (“Internet key exchange”) versión 1 y 2.
112.	La función de VPN de sitio-a-sitio debe soportar cifrado con algoritmos de clave simétrica incluyendo 3DES, AES -128, AES-256.
113.	La función de VPN de sitio-a-sitio debe soportar validación de integridad de los datos con algoritmos de resumen (“hash”) incluyendo MD5, SHA-1, SHA-256, SHA-384, SHA-512.
114.	La función de VPN de sitio-a-sitio debe soportar cifrado con algoritmos de clave asimétrica incluyendo Diffie-Hellman grupo 1, grupo 2, grupo 5, grupo 14, grupo 19 y grupo 20.
115.	La función de VPN de sitio-a-sitio debe soportar que se utilice de NAT-Traversal en el tráfico del túnel.
116.	Las capacidades de las funciones de **FIREWALL (FW)**, **PROTECCIÓN ANTIMALWARE** y **SISTEMA DE PREVENCIÓN DE INTRUSIONES (IPS)** deben estar disponibles para dar protección al tráfico VPN de sitio-a-sitio.
	VPN DE ACCESO REMOTO (“REMOTE ACCESS”)
117.	El Firewall debe incluir la función de VPN de acceso remoto (“remote access"), esto es, conexiones de usuarios que utilizan dispositivos externos con la red informática institucional mediante un canal seguro.
118.	La función de VPN de acceso remoto debe utilizar protocolos seguros tales como IPSEC y SSL/TLS.
119.	La función de VPN de acceso remoto, tanto en el clúster de firewalls principal como en clúster de firewalls alterno, debe contar con el licenciamiento suficiente para al menos 3129 usuarios totales o 1035 usuarios concurrentes, según sea el modelo de licenciamiento del fabricante.
120.	La función de VPN de acceso remoto debe soportar ser desplegada al menos de las siguientes formas: • Sin agente (“agentless”); • Instalando un agente en los puntos finales.
121.	Para las conexiones VPN de acceso remoto realizadas sin agente el Firewall debe desplegar un portar web seguro, esto es, que utilice HTTPS (SSL/TLS).
122.	Los métodos de autenticación de la función de **IDENTIFICACIÓN DE USUARIOS** deben estar disponibles para la autenticación de los usuarios que hagan uso de VPN de acceso remoto.
123.	La función de VPN de acceso remoto debe contar con un mecanismo de generación masiva de accesos remotos por VPN para usuarios en base a una lista o mediante la integración con directorio activo.
124.	La función de VPN de acceso remoto debe soportar la autenticación de los usuarios conectados mediante VPN de acceso remoto utilizando certificados digitales.
125.	La función de VPN de acceso remoto debe soportar la autenticación de los usuarios conectados mediante VPN de acceso remoto utilizando la combinación de al menos dos factores (métodos) de autenticación (“2FA”).
126.	La función de VPN de acceso remoto debe operar de forma que a los equipos conectados remotamente por VPN se les asigne una dirección IP de tal manera que se emule que estos se encuentren en la red local.
127.	La función de VPN de acceso remoto debe tener la capacidad de discriminar si los equipos conectados remotamente por VPN pertenecen a la institución o no.
128.	La función de VPN de acceso remoto debe tener la capacidad de controlar si los equipos externos se pueden conectar o no a la red institucional en base a criterios de cumplimiento, tales como: • Versión del sistema operativo; • Versión de parche; • Condición del software antivirus.
129.	El Firewall debe hacer intercambio seguro de llave utilizando protocolos tales como IKE (“Internet key exchange”) versión 1 y 2.
130.	El Firewall debe soportar cifrado con algoritmos de clave simétrica tales como DES, 3DES, AES -128, AES-256.
131.	El Firewall debe soportar validación de integridad de los datos con algoritmos de resumen (“hash”) tales como MD5, SHA-1, SHA-256.
132.	El Firewall debe soportar cifrado con algoritmos de clave asimétrica tales como Diffie-Hellman grupo 1, grupo 2, grupo 5, grupo 14.

133. El agente de VPN de acceso remoto debe soportar al menos los siguientes sistemas operativos: • Windows 8.1, 10, 11 y posteriores; • MacOS 10.15, 11, 12, 13 y posteriores; • iOS 12 y posteriores; • Android 6 y posteriores. **NOTA:** Las versiones soportadas pueden variar a medida que los fabricantes de los sistemas operativos las vayan declarando obsoletas o en EOST ("End-of-Support") o en EOL ("End-of-Life").
134. El agente de VPN de acceso remoto debe realizar la configuración de los servidores DNS institucionales en los equipos externos.
135. El agente de VPN de acceso remoto debe contar con la opción para seleccionar el sitio con el que se establecerá la conexión.
136. Las capacidades de las funciones de **FIREWALL (FW)**, **PROTECCIÓN ANTIMALWARE** y **SISTEMA DE PREVENCIÓN DE INTRUSIONES (IPS)** deben estar disponibles para dar protección al tráfico VPN de acceso remoto.
VIRTUALIZACIÓN DE SISTEMAS
137. El sistema debe contar con la función de sistemas virtuales, esto es, la creación de dispositivos lógicos dentro de un gateway físico.
138. La función de sistemas virtuales debe ser de tecnología propietaria del fabricante del sistema de Firewalls de Nueva Generación. No se admiten tecnologías de virtualización de servidores (ej. VMware, Citrix, Microsoft, KVM y similares).
139. Los sistemas virtuales (dispositivos lógicos) deben ser de al menos los siguientes tipos: • Firewall, • Router (capa 3/OSI), • Switch (capa 2/OSI).
140. Los firewalls virtuales deben poderse activar todos en un único nodo o deben poderse distribuir entre los gateways físicos que conforman el clúster.
141. Cada gateway físico debe contar con el licenciamiento y la capacidad suficiente para crear no menos de 4 firewalls virtuales.

2.1.3. GARANTÍA TÉCNICA DEL HARDWARE

1. La garantía técnica debe cubrir todos los equipos que conforman el componente de hardware del objeto de contrato, esto es:
   - **1.a.** (2) Clúster de firewall, principal y alterno;
   - **1.b.** (2) Servidores de gestión, principal y alterno.
2. La garantía técnica del fabricante del hardware deberá incluir el servicio de reemplazo de partes, piezas e inclusive del componente afectado completo (si fuera el caso). Será responsabilidad del contratista el cumplimiento del servicio.
3. Todos los equipos que conforman el componente de hardware del objeto de contrato deberán ser nuevos y se deberá garantizar que éstos no entren en EOST ("End-of-Support") ni en EOL ("End-of-Life") durante los 5 años posteriores a la fecha de suscripción del contrato.
4. Si se evidencia que los nodos físicos del sistema de Firewalls experimenten un consumo de capacidad de cómputo (CPU o RAM) superior al 90% mientras procesan un volumen de tráfico ("throughput") inferior al 90% de lo establecido en la CAPACIDAD DE PROCESAMIENTO DE TRÁFICO o en la CAPACIDAD DE PROCESAMIENTO DE TRÁFICO SSL/TLS solicitada, se determinará que los equipos en cuestión no cumplen con este requerimiento y deberán ser fortalecidos o reemplazados por el Contratista. Esta acción se aplicará tantas veces como corresponda hasta que se evidencie que los equipos estén operando dentro de los parámetros esperados por el SRI, sin que esto represente un costo adicional para el SRI.
5. Si se evidencia que la capacidad de cómputo (CPU o RAM) de alguno de los Servidores de gestión, principal o alterno, no es suficiente para la óptima operación de las máquinas virtuales y appliance virtuales alojados, se deberá agregar la cantidad de recursos tecnológicos necesarios para este efecto, manteniendo la simetría entre principal y alterno, y cumpliendo con las condiciones de desempeño establecidas en ambos casos.
6. Los casos en los que se requiera aplicar la garantía técnica serán gestionados como incidentes del servicio de mantenimiento correctivo y deberá cumplir el contratista con el **ACUERDO DE NIVEL DE SERVICIO**.
7. El servicio de soporte del fabricante del hardware debe estar disponible 24 horas al día los 7 días de la semana durante la vigencia del contrato y debe cubrir tanto el hardware como las licencias de firmware incluidas en los equipos.
8. El servicio de soporte del fabricante del hardware debe ser del tipo directo, esto es, debe permitir al personal del SRI abrir de casos de soporte.

9. El servicio de soporte de fábrica del hardware debe incluir, pero no debe estar limitado a, las prestaciones que se indican a continuación:
   - **9.a.** Gestión de incidentes causados por el hardware;
   - **9.b.** Recomendación de versiones de firmware para los servidores del sistema;
   - **9.c.** Revisión del estado de los servidores del sistema;
   - **9.d.** Acceso a la Base de Conocimientos del fabricante;
   - **9.e.** Acceso a la Mesa de Ayuda del fabricante;
   - **9.f.** Notificaciones proactivas de nuevas versiones y parches liberados.
10. El contratista deberá dejar constancia de la entrega y vigencia de la garantía técnica mediante un **certificado de garantía técnica del hardware** que debe adjuntar la documentación que sustente el cumplimiento de todo lo solicitado en este ámbito incluyendo, pero no limitado a:
    - **10.a.** La documentación que sustente la vigencia de la garantía técnica del fabricante del hardware de todos los equipos que conforman el componente de hardware del objeto de contrato, indicando su alcance y su fecha de expiración;
    - **10.b.** La documentación que indique el tipo o el nivel de soporte de fábrica con el que cuentan todos los equipos que conforman el componente de hardware del objeto de contrato, indicando su alcance, su disponibilidad (ej. 24x7), los canales de comunicación con fábrica y su fecha de expiración.

2.1.4. INSTALACIÓN DEL HARDWARE

1. El servicio de instalación debe cubrir todos los componentes relacionados con el hardware, esto es:
   - **1.a.** (2) Clúster de firewall, principal y alterno;
   - **1.b.** (2) Servidores de gestión, principal y alterno.
2. Todos los gastos incurridos en la instalación están a cargo del contratista y el SRI no incurrirá en ningún gasto adicional.
3. Los horarios de trabajo se acordarán con el administrador del contrato, sin incluir costos adicionales por trabajar en fines de semana, feriados, o fuera del horario laboral.
4. Todas las actividades que impliquen cambios en la configuración, en la operación, o en el nivel de seguridad informática del sistema de Firewalls de Nueva Generación deberán ser informados al administrador del contrato, y deberán ser aplicados de manera controlada en coordinación con el personal del SRI.
5. El personal técnico del contratista deberá contar con todos los medios y recursos necesarios para la ejecución ágil y oportuna de todos los trabajos que son parte del objeto del presente contrato; incluyendo, pero no limitado a: equipo portátil, módem de acceso a Internet, medios removibles de almacenamiento (ej. USB Flash Drives, USB External Hard Drives, etc.), cables de conexión a puertos de consola, “patch cords”, etc.
6. El clúster de firewall principal operará en el centro de datos de Quito y el clúster de firewall alterno operará en el centro de datos de Guayaquil.
7. El servidor de gestión principal operará en el centro de datos de Quito y el servidor de gestión alterno operará en el centro de datos de Guayaquil.
8. Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como appliance virtual o como máquina virtual en su respectivo servidor de gestión tal como se indica en la tabla a continuación.

COMPONENTE DE SOFTWARE	SERVIDOR FÍSICO	SITIO
Gestor de firewall principal	Servidor de gestión principal	CD Principal
Componente de análisis de configuración y eventos principal	Servidor de gestión principal	CD Principal
Gestor de firewall alterno	Servidor de gestión alterno	CD Alterno
Componente de análisis de configuración y eventos alterno	Servidor de gestión alterno	CD Alterno

Tabla 6. Correspondencia entre instancias virtuales y servidores físicos.

9. El contratista deberá entregar un oficio en el que deje constancia de los equipos trasladados a las instalaciones del SRI y debe adjuntar al menos la siguiente documentación:
   - **9.a.** Fecha de entrega de los equipos;
   - **9.b.** Detalle de los equipos entregados, incluyendo fabricante, modelo, y número de serie;
   - **9.c.** Detalle de la capacidad y las características técnicas de cada servidor;
   - **9.d.** Identificación de cada servidor de acuerdo con su rol en el nuevo sistema.
10. El contratista deberá instalar el hardware siguiendo las mejores prácticas de ensamblaje, montaje, configuración de parámetros y de conexión recomendadas por el fabricante de este.
11. El contratista debe proveer e instalar los rieles, bandejas, sujetadores y demás accesorios necesarios para que el montaje y la interconexión de los equipos se realice de forma segura y organizada en los centros de datos del SRI.
12. El contratista debe proveer, como parte de la instalación de cada equipo entregado, los transceptores ("transceivers") que sean necesarios para su conexión con la infraestructura de red del SRI, en los centros de datos principal y alterno, utilizando los modelos que se indican en la tabla a continuación.

MEDIO	TIPO DE CONEXIÓN	FABRICANTE	MODELO
Óptico	40Gbps BASE-SR QSFP+ LC	Cisco	QSFP-40/100-SRBD
Óptico	25Gbps BASE-SR SFP+ LC	Cisco	SFP-25G-SR-S
Óptico	10Gbps BASE-SR SFP+ LC	Cisco	SFP-10G-SR
Óptico	1Gbps BASE-SX SFP LC	Cisco	GLC-SX-MMD

Tabla 7. Modelos de transceptores ("transceivers") soportados por el switch de core institucional.

13. El contratista debe proveer, como parte de la instalación de cada equipo entregado, los cables ("patch cords") de par trenzado y de fibra óptica que sean necesarios para su conexión con la infraestructura de red del SRI, tanto en el centro de datos principal como en el alterno. Los cables ("patch cords") deben ser certificados.
14. El contratista deberá proveer cables ("patch cords") de fibra óptica de tipo multimodo OM4 LC-LC para las conexiones de 10 Gbps, 25 Gbps y 40 Gbps.
15. El contratista deberá proveer cables ("patch cords") de fibra óptica de tipo multimodo OM3 LC-LC para las conexiones de 1 Gbps.
16. El contratista deberá instalar la última versión estable liberada y con el último paquete de parches y actualizaciones del software del sistema de Firewalls de Nueva Generación, según corresponda a cada componente.
17. El contratista deberá instalar la última versión estable liberada y con el último paquete de parches y actualizaciones del firmware del sistema de Firewalls de Nueva Generación, según corresponda a cada componente.
18. El contratista deberá dejar constancia de la culminación de la instalación del hardware mediante un **oficio de culminación de la instalación del hardware** al que debe adjuntar la documentación que sustente el cumplimiento de todo lo solicitado en este ámbito, incluyendo:
    - **18.a.** La evidencia documental del ingreso, montaje y cumplimiento de las ESPECIFICACIONES TÉCNICAS del componente de hardware;
    - **18.b.** La evidencia documental de la instalación, activación y vigencia del licenciamiento y soporte de fábrica del componente de software correspondiente a la INSTALACIÓN DEL SOFTWARE;
    - **18.c.** La evidencia documental de la operación del componente de hardware en la red tecnológica del SRI con su correspondiente componente de software.

2.2. COMPONENTE DE SOFTWARE

2.2.1. ALCANCE

El componente de software deberá estar conformado por los siguientes elementos:

A. (2) Gestores de firewall, principal y alterno;
B. (2) Componentes de análisis de configuración y eventos, principal y alterno;
C. (1) Servicio SaaS de protección de correo electrónico.

2.2.2. PRODUCTOS ESPERADOS

	A. GESTORES PRINCIPAL Y ALTERNO
1.	Los gestores principal y alterno deben tener capacidades, características y funcionalidades equivalentes y deben desplegarse como appliance o máquinas virtuales.
2.	Todas las funciones y módulos que comprenden los **GESTORES PRINCIPAL Y ALTERNO** deben pertenecer a la misma solución y al mismo fabricante.
3.	Los gestores principal y alterno deben contar con la capacidad y el licenciamiento suficiente para gestionar todos los clúster de firewalls, nodos físicos y sistemas virtuales que confirman el sistema de firewalls ofertado.
4.	El gestor de principal y el gestor de alterno deben operar en un esquema de alta disponibilidad de tipo activo-pasivo multi-sitio.
5.	El gestor alterno debe mantenerse en constante sincronización con el gestor principal, esto es, debe mantener una réplica de las políticas y eventos de seguridad que tiene el principal.
6.	Tanto el gestor principal como el gestor alterno deben cumplir con las especificaciones que se indican a continuación.
7.	Las funciones de gestión pueden distribuirse en más de una instancia si la arquitectura del fabricante así lo requiere.
8.	La instancia (máquina virtual) de gestión donde se almacenen los registros de eventos (“logs”) debe tener la capacidad de que su almacenamiento pueda crecer al menos hasta 24TB.
9.	La gestión debe soportar la designación de roles a los administradores, de forma que se les puedan dar privilegios diferenciados en base a sus funciones.
10.	La gestión debe incluir una CA (entidad certificadora) interna que sirva para emitir certificados digitales para los gateways y para los usuarios en los casos que las funciones de seguridad del sistema así lo requieran para su operación, por ejemplo, para la autenticación mediante certificados digitales de usuarios de VPN de acceso remoto, y para la autenticación de los gateways con los gestores.
11.	La gestión debe contar con un mecanismo automático o manual de renovación o cambio de llaves criptográficas de la CA (entidad certificadora) interna.
12.	La gestión debe tener la capacidad de funcionar como entidad certificadora subalterna de una entidad certificadora externa al sistema de Firewalls.
13.	La comunicación entre los gateways y los gestores debe estar protegida por mecanismos de cifrado.
14.	La gestión debe permitir que sistemas externos realicen tareas de administración mediante integración por API.
	GESTIÓN DE POLÍTICAS
15.	Los gestores deben centralizar la gestión de políticas de todas las funciones de seguridad de los clúster, nodos físicos y sistemas virtuales que conforman el sistema de firewalls ofertado.
16.	La gestión de políticas debe soportar el acceso concurrente de más de un administrador, de forma que varios administradores puedan modificar diferentes grupos de reglas o distintas partes de un mismo grupo de reglas simultáneamente.
17.	La gestión de políticas debe soportar que cada administrador concurrente aplique los cambios que ha realizado independientemente sin afectar o sobrescribir los cambios realizados por los demás administradores.
18.	La gestión de políticas debe tener la capacidad de aplicar solamente los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
19.	La gestión de políticas debe permitir que sistemas externos realicen tareas de administración mediante integración por API.
20.	La gestión de políticas debe incluir una función de búsqueda para encontrar objetos que conforman las políticas de seguridad, tales como, hosts, puertos, segmentos de red, usuarios, gateways, etc.
21.	La gestión de políticas debe incluir una función de búsqueda para encontrar de las reglas que utilizan un objeto específico.
22.	La gestión de políticas debe realizar validaciones de consistencia de las reglas antes de ser aplicadas o instaladas.
23.	La gestión de políticas debe permitir que todos los tipos de reglas, esto es, de todas las funciones de seguridad, sean gestionados en un único panel de política de seguridad.
24.	La gestión de políticas debe soportar que se creen grupos, conjuntos o paquetes de reglas de seguridad independientes por cada nodo físico y sistema virtual.
25.	La gestión de políticas debe tener la capacidad de integrarse con el sistema vCenter del SRI (véase **INFRAESTRUCTURA ACTUAL**) para importar objetos de manera que se puedan utilizar como origen o destino para crear reglas de seguridad.

26.	La gestión de políticas debe tener la capacidad de integrarse con el sistema Active Directory del SRI (véase **INFRAESTRUCTURA ACTUAL**) para importar objetos de manera que se puedan utilizar como origen o destino para crear reglas de seguridad.
27.	La gestión de políticas debe tener la capacidad de integrarse con el sistema Cisco ACI del SRI (véase **INFRAESTRUCTURA ACTUAL**) para importar objetos de manera que se puedan utilizar como origen o destino para crear reglas de seguridad.
28.	La gestión de políticas debe tener la capacidad de que los objetos importados reflejen automáticamente los cambios que se realicen en las plataformas origen.
29.	La gestión de políticas debe contar con la capacidad de exportar las reglas de seguridad en formato CSV.
30.	La gestión de políticas debe contar con un apartado donde conste el historial de versiones de la política de seguridad de forma que se permita, por ejemplo, regresar a un estado anterior y comparar la versión actual de la política con una versión anterior.
31.	La gestión de políticas debe contar con la función de generación y exportación periódica de respaldos de configuraciones.
32.	La gestión de políticas debe soportar el uso de etiquetas en los objetos de la política para facilitar su búsqueda o para establecer asociaciones entre estos.
33.	La gestión de políticas debe tener la capacidad de crear paquetes de políticas que se puedan compartir para su uso simultáneo en varios gateways.
	GESTIÓN DE EVENTOS
34.	Los gestores deben centralizar la gestión de los eventos de los clúster, nodos físicos y sistemas virtuales que conforman el sistema de firewalls ofertado.
35.	La gestión de los eventos debe concentrar e indizar los registros de eventos (“logs”) de tráfico y debe proveer información como, por ejemplo: • Throughput (bytes o bits por segundo), • Tasa de paquetes por segundo, • Conexiones o sesiones concurrentes, • Tasa de conexiones o de sesiones por segundo, • Tráfico identificado de acuerdo con su origen, destino y puerto, • Cantidad de tráfico (bytes) transferida, • Fecha y hora.
36.	La gestión de los eventos debe concentrar e indizar los registros de eventos (“logs”) de seguridad y debe proveer información como, por ejemplo: • Regla(s) o política(s) con la(s) que el tráfico ha hecho coincidencia (“match”), • Función(es) de seguridad que ha(n) procesado el tráfico, • Acción tomada sobre el tráfico (ej. permitir, bloquear, rechazar, desviar, etc.), • Criterio de coincidencia (ej. origen, destino, protocolo, firma, tipo de archivo, etc.), • Fecha y hora.
37.	La gestión de los eventos debe concentrar e indizar los registros de eventos (“logs”) de auditoría y debe proveer información como, por ejemplo: • Regla(s) o configuración(es) en la(s) que se realizó alguna modificación, • Administrador que realizó la modificación, • Rol o perfil o privilegios con los que cuenta dicho administrador, • Dirección IP del host desde donde el administrador hizo la modificación, • Fecha y hora.
38.	La gestión de los eventos debe contar con una interfaz de visualización de registros de eventos (“logs”) que permita ver el flujo de evento en tiempo real, esto es, a medida que los gateways detectan el tráfico y actúan sobre este.
39.	La gestión de los eventos debe contar con una interfaz de visualización de registros de eventos (“logs”) que permita realizar una revisión histórica de eventos.
40.	La gestión de los eventos debe contar con una interfaz de generación de reportes estadísticos sobre los eventos generados en el sistema de firewalls. Estos reportes deberán ser de tipo: • Reportes Top, • Reportes detallados, • Reportes basados en rango de tiempo, • Reportes basados en usuarios, • Reportes basados en protocolo o puerto o servicio, • Reportes basados en origen o destino, • Reportes basados en aplicación o grupo de aplicación.
41.	El sistema de Firewall debe soportar el envío de registros de eventos (“logs”) a sistemas externos, tales como sistemas SIEM o de correlación de eventos.

42.	El envío de registros de eventos (“logs”) a sistemas externos debe soportar el uso de mecanismos de cifrado tales como TLS.
43.	La interfaz de gestión de los eventos debe contar con un apartado de búsqueda para aplicar filtros sobre los eventos que se muestran basándose en origen, destino, protocolo o puerto o servicio, usuario(s), fecha, hora, función de seguridad, severidad, etc.
44.	La interfaz de gestión de los eventos debe permitir al administrador seleccionar qué campos o columnas se muestran en la lista de eventos.
45.	La gestión de los eventos debe generar los reportes en formatos PDF y CSV.
46.	La gestión de los eventos debe permitir la exportación de un conjunto seleccionado de registros de eventos (“logs”) en formato texto o CSV.
47.	La gestión de los eventos debe permitir crear nuevos tipos de reportes personalizados, así como modificar los reportes predefinidos.
48.	La gestión de los eventos debe permitir al administrador configurar el tamaño del archivo para rotación de los archivos de registros de eventos (“logs”).
49.	La gestión de los eventos debe ofrecer al administrador un mecanismo de navegación de tipo "drill-down" para investigación de los registros de eventos (“logs”).
50.	La gestión de los eventos debe generar reportes forenses sobre las acciones realizadas por los ataques de malware detectados en la red institucional, incluyendo la siguiente información: • Tipo o familia de malware; • Acciones realizadas durante la emulación en el entorno de caja de arena (“sandbox”).

B. COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS	
1.	Las funciones y módulos que comprenden el COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS pueden pertenecer a diferentes fabricantes.
2.	Las funciones y módulos que comprenden el COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS deben desplegarse como máquinas virtuales o appliance virtuales.
3.	El COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS debe contar con las siguientes funciones: • Análisis automático de configuración; • Respaldo automático de configuración; • Respaldo automático de eventos; • Recolección y correlación de eventos; • Análisis de eventos; • Supervisión.
4.	El COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS debe ser desplegado de forma simétrica en los centros de datos principal y alterno.
5.	El COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS del centro de datos principal y el del centro de datos alterno deben mantener la misma información, esto es, como medida de contingencia. Para el efecto se pueden utilizar mecanismos sincrónicos o asincrónicos.
	ANÁLISIS AUTOMÁTICO DE CONFIGURACIÓN
6.	La función de análisis automático de configuración debe contar con la capacidad y el licenciamiento suficiente para obtener y/o leer la configuración del sistema de Firewalls ofertado.
7.	La función de análisis automático de configuración debe ser capaz de proveer al menos las siguientes estadísticas generales de reglas: • Número total de reglas; • Número de reglas permitidas; • Número de reglas denegadas; • Número de reglas de tráfico de entrada; • Número de reglas de tráfico de salida; • Número de reglas inactivas; • Número de reglas deshabilitadas; • Número de reglas permitidas con origen y destino “ANY”; • Número de reglas permitidas con servicio “ANY”.

8.	La función de análisis automático de configuración debe realizar al menos los siguientes tipos de análisis: • Análisis de optimización de reglas; • Análisis de depuración o limpieza de reglas; • Análisis de reglas temporizadas; • Análisis de seguridad de reglas; • Análisis de cambios en reglas.
9.	La función de análisis automático de configuración debe ser capaz de proveer la siguiente información en los reportes de análisis de reglas: • Irregularidades en reglas; • Reglas sugeridas; • Reglas no utilizadas; • Afinamiento de política; • Utilización de objetos; • Objetos duplicados; • Detalles de irregularidades; • Sugerencias de reordenación de reglas; • Detalles de reglas excesivamente permisivas; • Amenazas de seguridad en servicios o aplicaciones; • Análisis de direcciones IP en listas negras; • Análisis de puertos riesgosos.
10.	La función de análisis automático de configuración debe ser capaz de proveer la siguiente información en los reportes de reglas temporizadas: • Detalles de todas las reglas temporizadas; • Las reglas temporizadas activas; • Las reglas temporizadas próximas a activarse; • Las reglas temporizadas expiradas; • Las reglas temporizadas recurrentes.
11.	La función de análisis automático de configuración debe ser capaz de realizar un análisis de los cambios realizados en el firewall.
12.	La función de análisis automático de configuración debe ser capaz de proveer la siguiente información en los reportes de análisis de cambio de reglas: • Fecha y hora del cambio de regla; • Usuario que realizó el cambio; • Dirección IP del usuario que realizó el cambio; • Versión del cambio de configuración; • Número de nuevas adiciones de reglas; • Número de nuevas modificaciones de reglas; • Número de nuevas eliminaciones de reglas; • Estadística histórica de cambios.
13.	Si para establecer la integración de la función de análisis automático de configuración con los componentes cubiertos se necesita realizar conectores, scripts, mecanismos o configuraciones personalizadas, se deberán incluir los trabajos, componentes de software con su licenciamiento y servicios de fábrica necesarios para este fin.
	RESPALDO AUTOMÁTICO DE CONFIGURACIÓN
14.	La función de respaldo automático de configuración debe contar con la capacidad y el licenciamiento suficiente para respaldar la configuración de: • El sistema de Firewalls ofertado; • El sistema de Proxy Web del SRI (Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG).
15.	La función de respaldo automático de configuración debe incluir los mecanismos necesarios para respaldar y restaurar la configuración de los componentes cubiertos, incluyendo: • Obtención automática de respaldo en base a calendario; • Almacenamiento histórico de respaldos en base a periodo de retención, • Verificación de integridad o errores del archivo de respaldo; • Identificación de respaldos fallidos o vacíos; • Rotación automática de archivos de respaldo; • Restauración de respaldo bajo demanda.

16.	Si para establecer la integración de la función de respaldo automático de configuración con los componentes cubiertos se necesita realizar conectores, scripts, mecanismos o configuraciones personalizadas, se deberán incluir los trabajos, componentes de software con su licenciamiento y servicios de fábrica necesarios para este fin.
	RESPALDO AUTOMÁTICO DE EVENTOS
17.	La función de respaldo automático de logs debe contar con la capacidad y el licenciamiento suficiente para respaldar los registros de eventos ("logs") de: • El sistema de Firewalls ofertado; • El servicio SaaS de protección de correo electrónico ofertado; • El sistema de Proxy Web del SRI (Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG).
18.	La función de respaldo automático de logs debe incluir los mecanismos necesarios para respaldar y recuperar los registros de eventos ("logs") de los componentes cubiertos, incluyendo: • Obtención automática de respaldo en base a calendario; • Discriminación de los eventos a respaldar en base a la fuente o a su tipo; • Respaldo de eventos de red, de seguridad y de auditoría; • Almacenamiento histórico de respaldos en base a periodo de retención, • Verificación de integridad o errores del archivo de respaldo; • Identificación de respaldos fallidos o vacíos; • Rotación automática de archivos de respaldo; • Exportación de respaldo bajo demanda.
19.	Si para establecer la integración de la función de respaldo automático de logs con los componentes cubiertos se necesita realizar conectores, scripts, mecanismos o configuraciones personalizadas, se deberán incluir los trabajos, componentes de software con su licenciamiento y servicios de fábrica necesarios para este fin.
	RECOLECCIÓN Y CORRELACIÓN DE EVENTOS
20.	La función de recolección y correlación de logs debe contar con la capacidad y el licenciamiento suficiente para recolectar y correlacionar los registros de eventos ("logs") de: • El sistema de Firewalls ofertado; • El servicio SaaS de protección de correo electrónico ofertado; • El sistema de Proxy Web del SRI (Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG).
21.	La función de recolección y correlación de logs debe soportar los mecanismos, protocolos y conexiones disponibles en los componentes cubiertos para la recolección de los registros de eventos ("logs").
22.	La función de recolección y correlación de logs debe incluir los mecanismos necesarios para recolectar y correlacionar los registros de eventos ("logs") de los componentes cubiertos, incluyendo: • Discriminación de los eventos a recolectar o almacenar en base a la fuente o a su tipo; • Recolección de eventos de red, de seguridad y de auditoría; • Correlación de los eventos obtenidos de los componentes cubiertos; • Almacenamiento de información de eventos en base a periodo de retención; • Rotación automática de archivos de información de eventos; • Exportación de respaldo bajo demanda.
23.	La función de recolección y correlación de logs debe permitir a los administradores realizar búsquedas rápidas de eventos en función de: • Direcciones IP, • Puertos o servicios, • Usuarios, • Periodo de tiempo, • Fuente.
24.	La función de recolección y correlación de logs debe permitir a los administradores generar reportes de eventos en función de: • Direcciones IP, • Puertos o servicios, • Usuarios, • Periodo de tiempo, • Fuente.
25.	Si para establecer la integración de la función de recolección y correlación de logs con los componentes cubiertos se necesita realizar conectores, scripts, mecanismos o configuraciones personalizadas, se deberán incluir los trabajos, componentes de software con su licenciamiento y servicios de fábrica necesarios para este fin.
	ANÁLISIS DE EVENTOS

26. En cuanto al análisis de eventos de Proxy, la solución debe ayudar a determinar: • Los sitios web más visitados; • Las páginas web o URL más visitadas; • Las principales páginas web denegadas; • El uso de caché, basado en el código de caché; • El uso de proxy, basado en el código de estado HTTP; • El uso del proxy, basado en el estado del par; • Los principales usuarios o hosts que acceden al proxy.
27. En cuanto al análisis de eventos de Proxy, la solución debe generar los siguientes reportes: • Reporte(s) de direcciones URL; • Reporte(s) de uso de Proxy; • Reporte(s) de detalles de sitios Web; • Reporte(s) de los principales hosts y protocolos que generan tráfico a través del servidor proxy.
28. En cuanto al análisis de eventos de Firewall, la solución debe ser capaz de generar los siguientes reportes de tráfico: • Reporte(s) consolidado(s) de eventos; • Reporte(s) de tráfico; • Reporte(s) de uso de protocolos; • Reporte(s) de uso Web; • Reporte(s) de uso de correo electrónico; • Reporte(s) de reglas de Firewall; • Reporte(s) de tráfico entrante (“inbound”) y saliente (“outbound”); • Reporte(s) de seguridad; • Reporte(s) de malware (ej. Virtus); • Reporte(s) de ataques.
29. Entre las métricas de conexiones VPN de acceso remoto que debe analizar la solución se deben incluir: • Quién inició sesión VPN; • Cuántos intentos fallidos de inicio de sesión en la VPN; • Cuántos inicios de sesión VPN se producen cada día; • Cuántas sesiones de usuario de VPN están activas actualmente; • Cuáles son las sesiones VPN y los usuarios con mayor duración; • Cuánto ancho de banda consume cada usuario a través de la VPN; • Qué protocolos se utilizaron para acceder a la VPN; • Cuáles son las tendencias de uso de la VPN; • Si el uso de la conexión VPN aumenta durante un día o una hora concretos.
30. En cuanto al análisis de eventos de Firewall, la solución debe ser capaz de generar los siguientes reportes respecto del servicio de VPN de acceso remoto: • Reporte(s) de usuarios activos en VPN; • Reporte(s) de sesiones VPN; • Reporte(s) de usuarios principales; • Reporte(s) de uso de VPN; • Reporte(s) de estado de VPN.
31. Entre las métricas de actividad de los usuarios que debe analizar la solución se deben incluir: • Ancho de banda total consumido por los usuarios; • Las aplicaciones más utilizadas por los usuarios; • Los servicios en la nube más utilizados por los usuarios; • Los sitios web permitidos para los usuarios; • Los sitios web bloqueados para los usuarios; • Comunicaciones en las que han participado los usuarios; • Detalles de protocolo y URL de los usuarios; • Detalles de VPN de cualquier usuario específico.
SUPERVISIÓN
32. La función de supervisión debe contar con la capacidad y el licenciamiento suficiente para supervisar el estado de: • El sistema de Firewalls ofertado; • Los servidores de gestión.
33. La función de supervisión debe tener disponible un tablero (“dashboard”) personalizable donde se presenten los datos de monitoreo mediante gráficos históricos de varios tipos, indicadores cuantitativos o cualitativos, y un apartado específico para las alertas que se encuentran activas por severidad.

34.	En cuanto a la supervisión del sistema de Firewalls, la función de supervisión debe tener la capacidad de monitorear los parámetros disponibles en los MIB de este sistema, entre los que se debe incluir: • Firewalls físicos y virtuales monitoreados; • Tráfico (ancho de banda o "throughput") de los nodos físicos y sistemas virtuales; • Conexiones concurrentes de los nodos físicos y sistemas virtuales; • Procesamiento ocupado de los nodos físicos; • Memoria RAM ocupada de los nodos físicos; • Almacenamiento libre y ocupado de los nodos físicos; • Estado de las conexiones VPN de sitio a sitio ("site-to-site"); • La cantidad de conexiones VPN activas.
35.	En cuanto a la supervisión del sistema de los servidores de gestión, entre las métricas de estado que debe analizar la solución se deben incluir: • Procesamiento ocupado del equipo físico; • Memoria RAM ocupada del equipo físico; • Procesamiento ocupado de las máquinas virtuales; • Memoria RAM ocupada de las máquinas virtuales; • Almacenamiento libre y ocupado del equipo físico; • Almacenamiento libre y ocupado de las máquinas virtuales; • Ocupación de interfaces de red (ancho de banda o "throughput"); • Máquinas virtuales activas.
36.	La función de supervisión debe emitir alertas al menos por correo electrónico y por mensajería instantánea Telegram.
37.	La función de supervisión debe proveer reportes de la operación de los componentes cubiertos, incluyendo: • Históricos de los parámetros monitoreados; • Histórico de las alertas emitidas.
38.	Si para establecer la integración de la función de supervisión con los componentes cubiertos se necesita realizar conectores, scripts, mecanismos o configuraciones personalizadas, se deberán incluir los trabajos, componentes de software con su licenciamiento y servicios de fábrica necesarios para este fin.

C. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO	
1.	Todas las funciones y módulos que comprenden el servicio SaaS de protección de correo electrónico deben pertenecer a la misma solución y al mismo fabricante.
2.	La solución debe contar con el licenciamiento suficiente para proteger el total de buzones del SRI que se detalla en la **INFRAESTRUCTURA ACTUAL**.
3.	El servicio debe proporcionar una interfaz gráfica de gestión que permita a los administradores: • Configurar políticas y reglas de seguridad; • Administrar las carpetas de cuarentena de la organización; • Generar registros de eventos ("logs") y generar reportes.
4.	La interfaz de gestión de la solución debe contar con la función de control de acceso basado en roles (RBAC) para diferenciar los permisos y privilegios de los administradores en base a perfiles administrativos.
5.	La solución debe tener la capacidad de integrarse con los sistemas de directorio del SRI (véase **INFRAESTRUCTURA ACTUAL**), esto es: • Microsoft Active Directory, • Microsoft Entra ID (Azure AD).
6.	La solución debe integrarse con los componentes del sistema de directorio institucional utilizando protocolos seguros basados en TLS versiones 1.2 o 1.3.
7.	La solución, para integrarse con los componentes del sistema de directorio institucional, debe soportar SAML 2.0 para la autenticación y el control de acceso.
8.	Los componentes del servicio SaaS deben actualizarse permanente y continuamente para garantizar un nivel adecuado de seguridad.
9.	La disponibilidad del servicio SaaS debe ser de no menos del 99.9%.
10.	El servicio SaaS debe alojar los servicios contratados del SRI en una instancia dedicada y separada de los servicios de otros clientes del fabricante.
11.	El servicio SaaS debe contar con al menos alguna de estas certificaciones: • SOC 2, • ISO 27001.

	PROTECCIÓN DE CORREO ELECTRÓNICO
12.	La solución debe contar con una función de protección de correo electrónico.
13.	La solución debe tener la capacidad de integrarse con el servicio Microsoft Exchange Online institucional al menos en los siguientes modos de operación: • Como gateway de seguridad de correo electrónico (“Email Security Gateway” – ESG); • Mediante integración API con Exchange Online.
14.	La solución, cuando opere en modo ESG, debe tener la capacidad de ser desplegada de las siguientes formas, en función de los requerimientos de seguridad de la arquitectura de correo electrónico institucional: • Como servicio SaaS que reciba primero el tráfico de correo electrónico y que lo reenvíe depurado al servicio de Exchange Online institucional.
15.	La solución debe tener la capacidad de analizar los mensajes de correo electrónico entrantes, salientes e internos de Exchange Online.
16.	La solución debe tener la capacidad de analizar los mensajes de correo electrónico entrantes y salientes de la infraestructura de correo electrónico local.
17.	La solución debe tener una consola de gestión tanto para la definición de políticas como para la recolección de eventos y generación de informes.
18.	La solución debe permitir proteger múltiples dominios sin necesidad de incurrir en licenciamiento adicional por dicha funcionalidad.
19.	La solución debe incluir al menos las siguientes funciones de seguridad de correo electrónico: • Protección del protocolo SMTP –en modo de operación ESG–, • Control antispam, • Control de phishing, • Control antimalware, • Remediación.
20.	La solución debe tener la capacidad de realizar al menos las siguientes acciones de control sobre las amenazas de correo electrónico identificadas: • Descartar o eliminar el mensaje, • Modificación del asunto o del cuerpo del mensaje, • Reescritura de hipervínculos, • Colocar en cuarentena el mensaje, • Redirigir el mensaje, • Eliminar el archivo adjunto, • Enviar copia a otro destinatario.
21.	La solución debe contar con la opción de configuración de listas blancas y listas negras. Esto debe poderse configurar para una función de protección específica o con alcance general.
22.	La solución debe tener soporte multilingüe para el análisis del contenido de los mensajes de correo electrónico, incluyendo al menos el Inglés, el Español y el Francés.
23.	La solución debe detectar la manipulación sospechosa de buzones de usuarios y reglas de correo en Exchange Online, por parte de un perfil administrador, y debe tomar acciones de respuesta, tales como, la eliminación de la regla identificada como riesgosa.
24.	La solución debe permitir la adición de etiquetas en el correo electrónico entrante que permitan, al menos, informar al destinatario: • Cuando un correo electrónico es enviado desde un dominio externo, • Si se trata de un remitente desconocido, • Si es un dominio recientemente registrado.
	PROTECCIÓN DE PROTOCOLO SMTP
25.	La solución debe contar con la función de protección de protocolo SMTP cuando opera en modo de gateway de seguridad de correo electrónico (ESG).
26.	La solución debe soportar el uso de TLS, al menos con SSL v3.0 o TLS v1.2, para proteger la confidencialidad del tráfico de correo electrónico entrante y saliente.
27.	La solución debe permitir al administrador definir políticas de cifrado de canal (SSL v3.0 o TLS v1.2) de correo electrónico entre dominios específicos y debe permitir tomar acciones en caso el cifrado falle, incluyendo: • Rechazar mensaje, • Solicitar reintento.

28.	La solución debe ser totalmente compatible con los siguientes mecanismos de autenticación de correo electrónico: • Sender Policy Framework (SPF), • DomainKeys Identified Mail (DKIM), • Domain-based Message Authentication, Reporting & Conformance (DMARC).
29.	La solución debe permitir al administrador implementar directivas de autenticación basadas en SPF, DKIM y DMARC de manera se pueda tomar acciones específicas tales como, permitir, bloquear, poner en cuarentena, en los casos de fallas de autenticación.
30.	La solución debe permitir realizar el firmado DKIM de los correos salientes de la organización utilizando una llave privada que puede ser generada directamente en la solución o importada.
31.	La solución debe verificar el destinatario de los mensajes entrantes, aprovechando la integración con el sistema de directorio institucional, para proteger el servicio de correo electrónico contra ataques de recolección de directorio (DHA).
32.	La solución debe bloquear automáticamente las conexiones de correo electrónico que provengan de los hosts, las direcciones IP y los dominios que se encuentren las listas de remitentes de mala reputación reduciendo así el riesgo de seguridad y el riego de sobrecarga al evitar la necesidad de analizar sus mensajes.
33.	La solución debe monitorear los hosts, las direcciones IP y los dominios que se encuentren las listas de remitentes de mala reputación de manera que, entre más ataques generen, mayor sea el nivel de bloqueos que se les aplique, entre menos ataques generen, menor sea el nivel de bloqueos que se les aplique, e inclusive, si dejan de generar ataques, se los remueva de la lista.
34.	La solución debe ser capaz de limitar el sondeo SMTP y comprobar la validez de la información del sobre antes de aceptar un mensaje para su entrega.
35.	La solución debe aplicar automáticamente restricciones de conexión a los hosts, direcciones IP o dominios externos proporcionalmente a los ataques de correo electrónico que estos han realizado. Esto es, a los remitentes con peor comportamiento se les debe aplicar mayores restricciones de conexión y viceversa.
36.	La solución debe contar con una fuente propia de inteligencia de seguridad, esto es, una red de inteligencia, que mantenga una lista de remitentes (ej. hosts, direcciones IP, dominios) de mala reputación que se actualice continuamente para que se aplique automáticamente su bloqueo.
37.	La solución debe contar con la capacidad de establecer un límite en el tamaño permitido para los archivos adjuntos de los mensajes entrantes o salientes.
38.	La solución debe permitir al administrador configurar las reglas de protección de correo electrónico en base de al menos los siguientes parámetros: • Tamaño de archivo adjunto, • Cantidad de archivo adjunto, • Cantidad de archivos contenidos en un solo archivo comprimido, • Metadatos de archivo adjuntos, • Campo MFROM del remitente y receptor, • Campo desde el subtítulo y el receptor, • Extensión de archivo adjunta, • Nombre de archivo adjunto, • Tamaño de archivo comprimido, • Contenido HTML contenido en el cuerpo del correo electrónico, • Cualquier etiqueta HTML contenida en el cuerpo del correo electrónico, • Número de restantes, • Lenguaje utilizado en el cuerpo del correo electrónico, • Código de país Origen enviando correo electrónico, • Tiempo de registro de dominio utilizado en los campos de o MFROM, • Detectar si el correo electrónico está encriptado, • Campo Helo, • Número de conexiones SMTP de una sola IP, • Antigüedad del dominio utilizado en el campo desde y/o MFROM.
	CONTROL ANTISPAM
39.	La solución debe tener un alto índice de eficacia para la detección de spam, esto es, no menos del 99%.
40.	La solución debe tener un sistema de reputación propietario para la detección de spam/phishing, no serán aceptados sistemas abiertos.
41.	La función de control antispam debe ser al menos de tercera generación, incluyendo análisis por medio de aprendizaje automático (“machine learning”).
42.	La solución debe ser capaz de detectar los ataques de spam basados en texto, imágenes, multimedia y archivos adjuntos.

43.	La solución debe ser capaz de detectar y bloquear distintos tipos de correos electrónicos no deseados, incluyendo: • Correo impostor, • Spam, • Correo gris (“graymail”), • Correo masivo (“bulk”), • Correo ofensivo, • Correo de mercadeo (“marketing”).
44.	La solución debe bloquear las amenazas detectadas en el tráfico de correo electrónico entrante, en el tráfico saliente y en el tráfico intercambiado entre los usuarios de Exchange Online.
45.	La solución debe permitir a los administradores realizar al menos las siguientes acciones sobre los mensajes retenidos en cuarentena: • Mantenerlo en cuarentena; • Reportar que no es spam (o sea, declararlo como falso positivo); • Liberarlo de la cuarentena.
46.	La solución debe contar un mecanismo que permita a los usuarios administrar su propia cuarentena realizando al menos las siguientes acciones sobre los mensajes retenidos: • Mantenerlo en cuarentena; • Reportar que no es spam (o sea, declararlo falso positivo); • Liberarlo de la cuarentena.
47.	La solución debe contar con un mecanismo para que los usuarios reporten mensajes maliciosos o no deseados (o sea, declararlos falsos negativos) que han recibido en su bandeja de entrada.
48.	Las acciones disponibles para que los usuarios administren de su propia cuarentena deben ser configurables por el administrador y no deben tener la posibilidad de liberar mensajes que han sido calificados como maliciosos con un alto nivel de certeza.
49.	La cuarentena debe almacenar los mensajes en carpetas diferenciadas de acuerdo con el tipo motor de detección.
50.	La solución debe permitir al administrador establecer el tiempo máximo que los mensajes pueden permanecer en cada una de las cuarentenas. Los mensajes que superen este periodo deberán ser eliminados definitivamente.
51.	La solución debe proporcionar una función de "vista previa segura" para que los administradores puedan ver información detallada de los mensajes en cuarentena y decidir las acciones necesarias.
39.	La solución debe permitir al administrador realizar personalizaciones o configurar excepciones en las reglas de seguridad basándose en al menos las siguientes opciones: • Hosts, • direcciones IP, • Usuarios, • Grupos de usuarios, • Dominios, • Sentido del tráfico (entrada o salida).
	CONTROL ANTIMALWARE
52.	La solución debe detectar y bloquear malware conocido, así como malware de día cero, esto es, para las que aún no existen firmas.
53.	La solución debe tener la capacidad de detectar y bloquear: • Virus, • Riskware, • Spyware, • Archivos cifrados, • Archivos con contraseña.
54.	La solución debe soportar el análisis y la aplicación de acciones específicas para archivos cifrados o protegidos por contraseña o con compresión múltiple.
55.	La solución debe contar con inteligencia que permita intentar acceder a un archivo protegido con contraseña utilizando información contextual del mensaje utilizado para su envío.
56.	La solución debe contar con descarga automática de actualizaciones de firmas, así como del motor.
57.	La solución debe tener la capacidad de reprocesar un correo sospechoso después de recibir actualizaciones de las firmas antimalware de día cero.
58.	La solución debe incluir el uso del análisis de sandboxing para revisar los archivos adjuntos y los recursos web asociados a los hipervínculos incluidos en los mensajes.
59.	El análisis de sandboxing debe obtener un veredicto respecto de un archivo adjunto o del recurso web asociado a un hipervínculo en un lapso no mayor a 5 minutos.

60.	Si al momento de realizar análisis de sandboxing de un hipervínculo el recurso web asociado no se encuentra disponible, la solución debe contar con la opción de que el mensaje sea entregado no sin antes reescribir la dirección URL del hipervínculo de manera que, si el usuario hace clic, este se despliegue en un entorno controlado y aislado.
61.	La solución debe ser capaz de identificar malware inclusive si el archivo ha sido cambiado de extensión.
62.	La solución debe ser capaz de analizar al menos los siguientes tipos de archivos: EXE, DLL, DOC, DOCX, XLS, XLSX, PPT, PPTX, JPG, PNG, PDF, SWF, MP3, MP4, JAVA, VBS, scripts y archivos PowerShell.
63.	La solución debe ser capaz de analizar al menos los siguientes tipos de archivos comprimidos: ZIP, TGZ, 7Z, CAB, LZH, RAR, TNEF.
	CONTROL DE PHISHING
64.	La solución debe contar con las siguientes capacidades para control de phishing: • Puntuación compuesta de mensajes de correo electrónico en base a atributos; • Inteligencia artificial (IA); • Aprendizaje automático (“machine learning”); • Análisis de reputación.
65.	La solución debe tener la capacidad de identificar los patrones de comunicación de la organización para así detectar anomalías que representen un riesgo de phishing.
66.	La solución debe tener la capacidad de detectar impostores e intentos de suplantación de identidad.
67.	La solución debe contar con protecciones especializadas para amenazas de tipo: • “Email Account Compromise” (EAC), • “Business Email Compromise” (BEC), • “spear phishing”, • “whaling”, • “delayed exploits”.
68.	La solución debe ser capaz de analizar tanto el encabezado como el contenido del mensaje para detectar e identificar ataques de suplantación de dominio, suplantación de nombre para mostrar y estrategias de “typosquatting”.
69.	La solución debe realizar una inspección en tiempo real de las direcciones URL contenidas en los mensajes de correo electrónico y los archivos adjuntos de ofimática (ej. documentos de MS Office, PDF, etc.).
70.	La solución debe detectar y bloquear los ataques de phishing que suplantan las páginas de inicio de sesión.
71.	La solución debe tener la capacidad de reescribir las direcciones URL en los mensajes de correo electrónico entrantes y salientes a fin de proveer un ambiente seguro de inspección.
72.	El análisis de las direcciones URL debe incluir el uso de aprendizaje automático (“machine learning”), de entorno de caja de arena (“sandbox”) y de revisión de reputación.
73.	La solución debe contar con una página de bloqueo personalizable para impedir el acceso de los usuarios a los sitios web maliciosos asociados a los hipervínculos contenidos en los mensajes de correo analizados.
74.	La solución debe tener la capacidad de reescribir la dirección URL del hipervínculo de manera que, si el usuario hace clic, este se despliegue en un entorno controlado y aislado.
75.	La solución debe ser capaz de retener la entrega de los mensajes de correo electrónico mientras se analizan todas las direcciones URL que contienen.
76.	La solución debe discriminar a los usuarios que estadísticamente han recibido más mensajes de phishing o con direcciones URL maliciosas para aplicarle protecciones de seguridad más rigurosas.
77.	La solución debe permitir a los administradores configurar excepciones para los bloqueos de direcciones URL.
78.	La solución debe incluir técnicas antievasión en el análisis de los mensajes para incrementar la precisión de su detección.
79.	La solución debe detectar y tomar acciones de control sobre los mensajes maliciosos que los usuarios intercambian internamente en Exchange Online.
80.	La solución debe proporcionar una consola de gestión y configuración basada en web que centralice la configuración, el registro, la cuarentena y la generación de informes del sistema, y que sea compatible con los navegadores actuales para la configuración y la gestión.
81.	La solución debe detectar y detener ataques de fraude a través de códigos QR (“QRshing”), esto es, debe realizar la interpretación de la imagen de los códigos QR incluidos en los mensajes de correo electrónico, debe detectar las direcciones URL ocultas en estos y debe bloquear los enlaces maliciosos.
	ACCIONES DE REMEDIACIÓN
82.	La solución debe contar con un mecanismo para analizar continuamente los mensajes ya entregados a la bandeja del usuario, conforme las funciones de seguridad vayan descargando nuevas actualizaciones, para identificar si estos representan una amenaza de seguridad que previamente no era conocida.
83.	En la revisión posterior de los mensajes, la solución debe incluir el análisis de las direcciones URL incluidas en estos con la finalidad de prevenir ataques de tipo detonación retardada (“delayed exploits”).

84.	Si se detecta que un mensaje ya entregado es malicioso o no deseado, la solución debe contar con un mecanismo para recuperarlo automáticamente, esto es, retirarlo de la bandeja del usuario, para prevenir el acceso a este.
85.	Una vez recuperado el mensaje desde la bandeja del usuario, la solución debe permitir a los administradores analizarlo y eliminarlo o retenerlo en cuarentena.
	GESTIÓN DE EVENTOS, REPORTES Y AUDITORÍA
86.	La solución debe ser capaz de generar registros de eventos (“logs”) con una sincronización cercana al tiempo real de los mensajes de correo electrónico de entrada y de salida y debe ofrecer una función de búsqueda de registros de eventos (“logs”) con filtros que permitan a los administradores a encontrar la información solicitada en base a los criterios de búsqueda ingresados.
87.	La solución debe generar registros de eventos (“logs”) de auditoría de las actividades realizadas por los administradores.
88.	La solución debe contar con paneles (“dashboards”) o reportes que provean al administrador información sobre estadísticas y tendencias de las amenazas de seguridad detectadas, incluyendo: • Cuentas comprometidas, • Archivos confidenciales potencialmente expuestos, • Correos electrónicos filtrados, • Credenciales de usuarios expuestas, • Accesos OAuth no seguros, • Usuarios o cuentas que han sido más atacados, • Usuarios con comportamientos de alto riesgo, • Acciones del análisis de caja de arena (“sandbox”), • Accesos (clics) a direcciones URL, • Malware detectado, • Mensajes spam, • Cómo se atacan esas cuentas, • Compartición riesgosa de archivos en las aplicaciones de Microsoft Office 365, • Demás amenazas detectadas por la solución.
89.	La solución debe tener la capacidad de asignar niveles de gravedad o de riesgo a las amenazas de seguridad detectadas.
90.	La solución debe proporcionar visibilidad en tiempo real de los ataques basados en el correo electrónico dirigidos a la institución.
91.	La solución debe contar con paneles (“dashboards”) o reportes que provean al administrador información forense de los ataques detectados, incluyendo: • Posible secuencia del ataque; • Desarrollo del ataque; • Indicadores de Compromiso (IoC); • Vector del ataque; • Cuentas o usuarios involucrados en el ataque.
92.	La solución debe contar con paneles (“dashboards”) o reportes que provean al administrador información sobre la operación del sistema, incluyendo: • Volumen de tráfico de correo electrónico, • Mensajes procesados, • Mensajes rechazados o retenidos en cuarentena, • Flujos de comunicación.
93.	La solución debe generar reportes al menos en formato PDF y/o CSV y debe tener la capacidad de enviarlos mediante correo electrónico de forma periódica y programada.
94.	La solución debe brindar el detalle del análisis de un archivo identificado como malicioso incluyendo los comportamientos riesgosos que fueron identificados y las técnicas identificadas
95.	La solución debe emitir alertas en base a condiciones asociadas a las políticas, las carpetas de cuarentena y los umbrales de cola.
96.	La solución debe contar con la capacidad de reenviar los registros de eventos ("logs”) mediante API (entorno SaaS) o mediante el uso de Syslog o Remote Syslog (entorno local) con el objetivo de integrarse con sistemas de terceros, por ejemplo, para realizar la correlación de eventos.
97.	La retención de los registros de eventos (“logs”) debe ser de no menos de 14 días.
	PROTECCIÓN DE DATOS
98.	El fabricante deberá garantizar la eliminación segura de la información y los registros de eventos (“logs”) que hayan sido cargados o recibidos durante el servicio SaaS, al final de la vigencia del licenciamiento.
99.	El servicio SaaS deberá proveer las facilidades necesarias para descargar o reenviar la información generada, incluyendo los registros de eventos (“logs”).

2.2.3. INSTALACIÓN DEL SOFTWARE

1. La instalación del software debe cubrir los siguientes componentes:
   - **1.a.** (2) Gestores de firewall, principal y alterno;
   - **1.b.** (2) Componentes de análisis de configuración y eventos, principal y alterno.
2. La instalación del software debe realizarse como parte de la **INSTALACIÓN DEL HARDWARE**, cumpliendo los mismos plazos e incluyéndose como parte de las condiciones para la solicitud de suscripción del acta de entrega recepción correspondiente.
3. Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como instancias virtuales (máquina o appliance) en los servidores de gestión de acuerdo con el detalle de la **tabla 6**.
4. Para efecto de lo mencionado en el punto anterior, como parte de la entrega de esta fase, el contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la instalación, activación y funcionamiento del software de virtualización necesario para el despliegue de las instancias virtuales (máquina o appliance) de los componentes de software, de acuerdo con el estándar del SRI (véase **INFRAESTRUCTURA ACTUAL**).
5. El contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la integración del software de virtualización instalado con la infraestructura virtual del SRI.
6. Si para la instalación de los componentes de software se requiere software base como, por ejemplo, sistemas operativos, bases de datos, etcétera, el contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la instalación, activación y funcionamiento de dichos prerrequisitos siguiendo las mejores prácticas de fábrica, aplicando los estándares tecnológicos institucionales y cumpliendo con los requerimientos técnicos del SRI.
7. La vigencia del licenciamiento y soporte de fábrica del software de virtualización y del software base incluido debe cubrir el mismo periodo de vigencia de los componentes software.
8. Los gestores de firewall pueden desplegarse en tantas instancias virtuales (máquina o appliance) como lo requiera la arquitectura del fabricante; siendo obligatorio que la instancia virtual que almacene los registros de eventos (“logs”) sea independiente de aquella que administre las políticas de seguridad.
9. Los componentes de análisis de configuración y eventos pueden desplegarse en tantas instancias virtuales (máquina o appliance) como lo requiera la arquitectura del fabricante.
10. El sistema de Firewalls debe ser instalado, activado y debe ponerse en funcionamiento de forma integral garantizándose la correcta operación de cada uno de sus componentes.
11. El sistema del componente de análisis de configuración y eventos debe ser instalado, activado y debe ponerse en funcionamiento de forma integral garantizándose la correcta operación de cada uno de sus componentes.
12. El software de virtualización debe ser instalado, activado y debe ponerse en funcionamiento siguiendo las mejores prácticas de fábrica, aplicando los estándares tecnológicos institucionales y cumpliendo con los requerimientos técnicos del SRI.
13. Cada instancia virtual deberá ser configurada de acuerdo con las mejores prácticas de fábrica, aplicando los estándares tecnológicos institucionales y cumpliendo con los requerimientos técnicos del SRI.
14. La distribución de los recursos de los servidores físicos, esto es, de la capacidad de procesamiento, de memoria y de espacio de almacenamiento, entre todas las instancias virtuales deberá ser aprobada por el personal técnico del SRI en función de los requerimientos operativos de los componentes de software, los estándares tecnológicos institucionales y los requerimientos técnicos del SRI.

3. SERVICIOS CONEXOS REQUERIDOS

3.1. MIGRACIÓN

1. El servicio de migración comprenderá todos los componentes incluidos en el objeto de contrato, así como sus dependencias, esto es:
   - **1.a.** Sistema de Firewalls que incluye:
     - (2) Clúster de firewall, principal y alterno;

- (2) Servidores de gestión, principal y alterno;
- (2) Gestores de firewall, principal y alterno;

1.b. (2) Componentes de análisis de configuración y eventos, principal y alterno;

1.c. (1) Servicio SaaS de protección de correo electrónico.

2. El servicio de migración comprenderá las **etapas** consecutivas que se indican a continuación, según corresponda a cada componente:

2.a. Preparación,

2.b. Transición,

2.c. Puesta en producción,

2.d. Estabilización,

2.e. Documentación.

3. Es responsabilidad del Contratista en conjunto con el personal especializado del Fabricante velar por que se incluyan en cada etapa todas las actividades y recursos necesarios para conseguir una migración exitosa con un impacto reducido y controlado.

4. Todas las actividades de la migración asociadas con la intervención de equipos tecnológicos deberán realizarse presencialmente por el personal técnico del Contratista.

5. Todas las actividades de las etapas de Transición, Puesta en producción y Estabilización asociadas con la intervención de equipos tecnológicos deberán realizarse presencialmente por el personal especializado del Fabricante en conjunto con el personal técnico del Contratista.

6. Si el SRI considera necesaria la intervención del personal especializado del Fabricante en cualquiera de las etapas de migración, este podrá solicitarla formalmente, aplicándose el ACUERDO DE NIVEL DE SERVICIO para Asistencia Técnica con prioridad 3.

7. Es responsabilidad del Contratista y del personal técnico especializado del Fabricante generar las evidencias de toda actividad realizada de manera que se pueda demostrar el cumplimiento de lo establecido en este apartado.

8. La etapa de **preparación** consistirá en la realización de las configuraciones necesarias para la operación básica de cada componente de manera que cada uno quede listo para recibir las políticas de seguridad, incluyendo, pero no limitándose a:

8.a. Elaborar la **arquitectura de seguridad**, conformada por la arquitectura de seguridad informática propuesta para el SRI en base a los componentes del objeto de contrato, a los marcos de seguridad vigentes de cada fabricante y de las mejores prácticas de la industria, incluyendo:

8.a.i. Diseños HLD (“high level desing”) de cada componente,

8.a.ii. Diseños LLD (“low level desing”) de cada componente,

8.a.iii. Diagramas lógicos de despliegue de cada componente,

8.a.iv. Diagramas de seguridad de cada componente,

8.a.v. Descripción del rol de seguridad de cada componente,

8.a.vi. Descripción de las integraciones de cada componente con los servicios tecnológicos del SRI;

8.b. Elaborar el **plan de migración**, conformado por las etapas indicadas en el numeral **2** incluyendo la respectiva evaluación de riegos de las actividades de migración y la mitigación correspondiente.

8.c. Aplicar las recomendaciones y mejores prácticas de fábrica para la configuración del hardware, del firmware y del software de cada componente;

8.d. Realizar la interconexión de cada componente con la infraestructura y servicios tecnológicos del SRI según corresponda a cada componente;

8.e. Realizar todas las configuraciones de integración con los sistemas centralizados (ej. Active Directory, vCenter, etc.) necesarias para la operación de cada componente;

8.f. Realizar la configuración de los usuarios, grupos de usuarios y perfiles de administración de cada componente;

8.g. Configurar y validar los mecanismos de descarga de actualización, de descarga de firmas y demás componentes que se requieran descargar desde los sistemas del fabricante o cargar en estos;

8.h. Configurar y validar los canales de envío de alertas, de reportes y notificaciones (ej. Correo electrónico);

8.i. Realizar pruebas de la función de alta disponibilidad de todos los componentes en los que sea factible;

8.j. Ajustar los parámetros de configuración de cada componente para un desempeño óptimo y seguro de acuerdo con las recomendaciones y mejores prácticas de fábrica;

8.k. Otras actividades que el SRI requiera que se incluyan en esta etapa.

9. La etapa de **transición** consistirá en la elaboración y aplicación de las nuevas políticas, reglas y configuraciones de seguridad y de operación en los nuevos componentes y la preparación para la puesta en producción, incluyendo, pero no limitándose a:

9.a. Configurar y aplicar las nuevas políticas, reglas y configuraciones de seguridad y de operación, en cada componente de acuerdo con el **diseño del nuevo sistema** y la **arquitectura de seguridad** entregados;

9.b. Realizar el afinamiento de las políticas, reglas y configuraciones de seguridad y de operación en cada componente de acuerdo con las recomendaciones y mejores prácticas de fábrica y los requerimientos del SRI;

9.c. Realizar las pruebas de seguridad y de operación de cada componente y aplicar las correcciones correspondientes de forma que se procure que el paso a producción tenga un impacto controlado y reducido en la operación del SRI;

9.d. Elaborar la documentación correspondiente al paso a producción, incluyendo: las actividades técnicas para la ejecución del cambio, las actividades de contingencia y las de reverso, por cada componente involucrado, ciñéndose a la normativa de cambios tecnológicos del SRI;

9.e. Elaborar la documentación que describa el procedimiento técnico detallado de: El paso a producción, El mecanismo de contingencia, y El mecanismo de reverso, cada uno por separado;

9.f. Otras actividades que el SRI requiera que se incluyan en esta etapa.

10. La etapa de **puesta en producción** consistirá en el reemplazo de los componentes actuales por los nuevos componentes en la operación de la red informática del SRI, incluyendo, pero no limitándose a:

10.a. Elaborar el cronograma de ventanas de mantenimiento en función de la planificación y normativa vigente del SRI, la complejidad, del impacto de cada componente y los plazos que corresponden a cada uno;

10.b. Realizar el paso a producción de cada componente de acuerdo con el cronograma;

10.c. Repetir la puesta en producción de los componentes cuyo paso a producción no haya sido exitoso.

11. La etapa de **estabilización** debe incluir, pero no limitarse a:

11.a. Mantener monitoreados los nuevos componentes hasta certificar un nivel de estabilidad razonable;

11.b. Atender los incidentes generados por la **puesta en producción** de los nuevos componentes;

11.c. Realizar las actividades de corrección y afinamiento de los nuevos componentes;

11.d. Configurar los reportes de seguridad y de operación que solicite el SRI en los nuevos componentes;

11.e. Contar con acompañamiento del personal técnico especializado del fabricante para resolver en el menor tiempo posible y con el mínimo impacto los problemas que se presenten después de la puesta en producción.

12. La etapa de **documentación** debe incluir, pero no limitarse a:

12.a. Realizar las pruebas de aceptación y elaborar la documentación con los resultados de estas;

12.b. Elaborar la documentación de la **memoria técnica**;

12.c. Elaborar la **arquitectura de seguridad** final, incluyendo:

12.c.i. Diseños HLD (“high level desing”) de cada componente,

12.c.ii. Diseños LLD (“low level desing”) de cada componente,

12.c.iii. Diagramas lógicos y esquemáticos de despliegue de cada componente,

12.c.iv. Diagramas lógicos de las integraciones de cada componente con los servicios tecnológicos del SRI,

12.c.v. Diagramas de seguridad de cada componente,

12.c.vi. Descripción del rol de seguridad de cada componente,

12.c.vii. Descripción de las integraciones de cada componente con los servicios tecnológicos del SRI;

12.d. Actualizar la **arquitectura de seguridad**, conformada por la arquitectura de seguridad informática propuesta para el SRI en base a los componentes del objeto de contrato, a los marcos de

seguridad vigentes de cada fabricante y de las mejores prácticas de la industria;

12.e. Elaborar el **estándar de configuración**, esto es, la guía que debe seguir cualquier administrador en función de la convención establecida, de cada componente en base a los requerimientos del SRI, incluyendo al menos:

12.e.i. Descripción del esquema de políticas de seguridad implementadas en cada componente,

12.e.ii. Descripción de la convención de nombres, de colores, de distribución o agrupación de reglas y de otros aspectos relevantes de las políticas de seguridad implementadas en cada componente;

12.f. Elaborar el documento y el video ilustrativo de **guía de instalación y de configuración de clientes VPN de acceso remoto para usuarios**, de forma que estos puedan realizar esta actividad autónomamente;

12.g. Realizar una presentación de la nueva arquitectura de seguridad al personal técnico del SRI que determine el administrador del contrato, la que deberá incluir al menos el diseño, la arquitectura y el detalle de componentes del nuevo sistema, así como, sus diferencias y ventajas con respecto al sistema anterior.

13. Las condiciones particulares de migración de cada componente se encuentran en las secciones **5.1.1**, **5.1.2** y **5.1.3**.

14. Los horarios de trabajo se acordarán con el administrador del contrato, sin incluir costos adicionales por trabajar en fines de semana, feriados, o fuera del horario laboral.

15. Todas las actividades que impliquen cambios en la configuración, en la operación, o en el nivel de seguridad informática de los componentes de seguridad informática involucrados deberán ser informados al administrador del contrato y deberán ser aplicados de manera controlada en coordinación con el personal del SRI.

16. El personal técnico del contratista deberá contar con todos los medios y recursos necesarios para la ejecución ágil y oportuna de todos los trabajos que son parte del objeto del presente contrato; incluyendo, pero no limitado a: equipo portátil, módem de acceso a Internet, medios removibles de almacenamiento (ej. USB Flash Drives, USB External Hard Drives, etc.), cables de conexión a puertos de consola, “patch cords”, etc.

17. Toda actividad de este ámbito deberá ser realizada siguiendo las mejores prácticas de fábrica, aplicando los estándares tecnológicos institucionales y cumpliendo con los requerimientos técnicos del SRI.

3.1.1. SISTEMAS DE FIREWALLS

La migración del sistema de firewalls debe incluir los siguientes aspectos particulares:

1. Las políticas del sistema de firewalls deberán ser transcritas desde el sistema actual al nuevo sistema.

2. La transcripción de las políticas debe incluir el análisis operativo y de seguridad de cada regla en función de las necesidades de seguridad informática del SRI, de las mejores prácticas del fabricante y de la industria.

3. Se deben realizar las siguientes depuraciones y optimizaciones durante la transcripción de políticas:

3.a. Eliminar o unificar los objetos de red duplicados;

3.b. Eliminar o unificar los objetos de puertos, protocolos o servicios duplicados;

3.c. Unificar o consolidar las reglas que así corresponda;

3.d. Eliminar las reglas no utilizadas o sin “hits”;

3.e. Eliminar las comunidades VPN no utilizadas o sin “hits”;

3.f. Eliminar las reglas temporales expiradas;

3.g. Agrupar o asociar las reglas comunes entre gateways en paquetes de políticas compartidos;

3.h. Organizar las reglas en función de la optimización operativa (ej. Aceleración), la optimización de seguridad y de la efectividad de la administración operativa.

4. Se deben utilizar las integraciones establecidas en la etapa de preparación, por ejemplo, con Active Directory, con vCenter, con ACI, para reemplazar objetos de red de las reglas existentes con los obtenidos en estas integraciones.

5. Las nuevas políticas de seguridad deben ser elaboradas utilizando los objetos, las funciones, las capacidades, la lógica y la tecnología del nuevo sistema de Firewalls, cumpliendo con los requerimientos técnicos del SRI.

6. Se deben depurar las reglas en las que se esté otorgando un permiso más amplio que: el que la institución requiere, o el que correspondiente al tráfico efectivo. Para el efecto se debe considerar al menos:
   - **6.a.** Revisar los registros de eventos ("logs") del tráfico efectivo;
   - **6.b.** Validar que los objetos de red realmente existan;
   - **6.c.** Validar que el tráfico realmente esté coincidiendo con los objetos de puertos, servicios o protocolos;
   - **6.d.** Discriminar los distintos flujos de tráfico que pueden ser separados en reglas de seguridad independientes;
   - **6.e.** Otros métodos que sirvan para el efecto.
7. Se deben depurar las reglas de traducción NAT manuales y automáticas.
8. Los gestores de políticas, de eventos y los repositorios de logs de los centros de datos principal y alterno deben sincronizarse.
9. Se deben crear las políticas y reglas de control de navegación en base a la política de navegación institucional y los requerimientos técnicos del SRI.
10. Se deben crear las reglas de la función integrada de IPS en base a la infraestructura tecnológica institucional, las capacidades técnicas del nuevo sistema de Firewalls y los requerimientos técnicos del SRI.
11. En las nuevas políticas se debe hacer una optimización del uso de los registros de eventos ("logs") en función de la ocupación de espacio de disco, del impacto en la operación de los gateways, de los requerimientos de reportes de actividad de usuarios, de los requerimientos de detección y resolución de problemas ("troubleshooting") y de los requerimientos de auditoría del SRI.
12. En el nuevo sistema de Firewalls se deben crear los usuarios VPN de acceso remoto existentes en la configuración actual, previa depuración, con sus respectivas reglas de acceso, utilizando doble factor de autenticación.
13. En el nuevo sistema de Firewalls se deben crear las comunidades VPN de sitio a sitio ("site-to-site") existentes en la configuración actual, previa depuración.
14. Se debe validar que los problemas o errores de configuración, de desempeño o de seguridad, del sistema actual no se hereden al nuevo sistema.
15. Se debe desplegar el software del nuevo agente VPN en los equipos institucionales donde ya se encuentra instalado el agente VPN actual.

3.1.2. COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS

La implementación del Componente de análisis de configuración y eventos debe incluir los siguientes aspectos particulares:

1. Se deben configurar todas las integraciones (conectores, scripts, mecanismos o configuraciones personalizadas) necesarias para la implementación de las funciones y módulos del Componente de análisis de configuración y eventos descritas en las especificaciones.
2. Se deben configurar todas las funciones y módulos del Componente de análisis de configuración y eventos descritas en las especificaciones.
3. Se deben configurar los procesos o tareas de respaldo de:
   - **3.a.** La configuración y los registros de eventos ("logs") del sistema de Firewalls;
   - **3.b.** Los registros de eventos ("logs") de la Protección de correo electrónico.
4. Si para establecer la integración de cualquier función del Componente de análisis de configuración y eventos se necesitan realizar conectores, scripts, mecanismos o configuraciones personalizadas, se deberán incluir los trabajos, componentes de software con su licenciamiento y servicios de fábrica necesarios para este fin.

3.1.3. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO

La migración del servicio SaaS de protección de correo electrónico debe incluir los siguientes aspectos particulares:

1. El servicio SaaS de protección de correo electrónico debe ser desplegado, activado y debe ponerse en funcionamiento siguiendo las mejores prácticas de fábrica, aplicando los estándares tecnológicos institucionales y cumpliendo con los requerimientos técnicos del SRI.
2. El servicio SaaS de protección de correo electrónico debe desplegarse de manera que proteja los buzones de correo electrónico institucionales adaptándose a la arquitectura de correo electrónico del SRI.

3. En lo que respecta a los dominios de correo electrónico institucionales, se debe dar protección al dominio **sri.gob.ec** y a los demás dominios institucionales que el personal técnico del SRI establezca necesarios.

3.1.4. TRANSFERENCIA DE CONOCIMIENTO

1. La transferencia de conocimiento se debe organizar considerando una asistencia de hasta nueve (9) funcionarios del SRI y una duración de no menos de cincuenta y seis (56) horas.
2. Toda logística asociada con la transferencia de conocimiento correrá por cuenta del Contratista.
3. La transferencia de conocimiento se debe organizar considerando que un (1) funcionario labora en las oficinas del SRI en Guayaquil y que los ocho (8) restantes laboran en las oficinas del SRI en Quito.
4. El calendario y horario de entrega de la transferencia de conocimiento se acordará con el administrador del contrato en función de la disponibilidad operativa del personal del SRI.
5. La transferencia de conocimiento se deberá realizar de forma presencial en instalaciones provistas por el contratista y deberá incluir los temas, materiales, laboratorios, facilidades (ej. aulas, ordenadores, acceso a internet, etc.) y talleres necesarios para la correcta asimilación del contenido y la generación de las destrezas necesarias en los asistentes.
6. Todos los asistentes deberán recibir el número total de horas y todos los temas de transferencia de conocimiento establecido cumpliendo con las mismas condiciones.
7. La transferencia de conocimiento deberá impartirse en al menos dos grupos en función de la disponibilidad del personal institucional y la distribución que el SRI establezca.
8. Los temas, materiales, laboratorios, facilidades, talleres y demás aspectos de la organización de la transferencia de conocimiento deben prepararse e impartirse de forma que cubran todos los componentes implementados y se garantice la consecución de los objetivos que se indican a continuación, sin costo adicional para el SRI.
    - **8.a.** Desarrollar la compresión adecuada de la arquitectura tecnológica, operativa y de seguridad, de todos los componentes del objeto de contrato;
    - **8.b.** Desarrollar el conocimiento y las destrezas de administración y gestión tecnológica de todos los componentes del objeto de contrato;
    - **8.c.** Desarrollar las destrezas para implementar estrategias y tácticas de seguridad para proteger los servicios tecnológicos institucionales;
    - **8.d.** Desarrollar las destrezas para implementar estrategias y tácticas de seguridad para responder ante ataques contra los servicios tecnológicos institucionales.
9. los Para constancia de la entrega de la transferencia de conocimiento se suscribirá el **acta de asistencia** en la que constará la lista de asistentes, el temario, las fechas de las sesiones y su duración.

El contratista deberá dejar constancia de la culminación de la migración mediante un **oficio de culminación de la migración** al que debe adjuntar la documentación que sustente el cumplimiento de todo lo solicitado en este ámbito, incluyendo:

- La **arquitectura de seguridad**;
- El **plan de migración**;
- El **acta de asistencia**;
- Demás documentación que evidencie la transferencia de conocimiento.
- Toda la documentación generada en la última etapa de la migración.

3.2. SOPORTE LOCAL

El servicio conexo de soporte local deberá estar conformado por los siguientes elementos:

- Servicio de mantenimiento preventivo;
- Servicio de mantenimiento correctivo;
- Servicio de asistencia técnica.

3.2.1. MANTENIMIENTO PREVENTIVO

1. El servicio de mantenimiento preventivo debe cubrir todos los equipos que conforman el componente de hardware del objeto de contrato, esto es:
   - **1.a.** (2) Clúster de firewall, principal y alterno;
   - **1.b.** (2) Servidores de gestión, principal y alterno.
2. El servicio de mantenimiento preventivo consistirá en la revisión física de los equipos que conforman el componente de hardware instalado.
3. En cada periodo, el contratista deberá realizar una (1) visita de mantenimiento preventivo por cada centro de datos, en la que se debe realizar las siguientes actividades:
   - **3.a.** Revisar alarmas visibles de cada equipo;
   - **3.b.** Revisar físicamente cada equipo;
   - **3.c.** Limpiar cada equipo siguiendo las mejores prácticas recomendadas por el fabricante del hardware haciendo uso de utensilios especializados para este fin;
   - **3.d.** Instalar los últimos parches o actualizaciones de firmware recomendados por el fabricante del hardware (ej. BIOS, lights–out management, controladoras, etc.)
4. Una vez completada la vista de mantenimiento preventivo se debe entregar un **informe de visita de mantenimiento preventivo** que tiene que incluir al menos lo siguiente:
   - **4.a.** El diagnóstico basado en las alarmas visibles de cada equipo;
   - **4.b.** El diagnóstico basado en la revisión física de cada equipo;
   - **4.c.** El reporte de la actualización de firmware realizada, especificando versión anterior, versión actual y correcciones significativas que incluyó;
   - **4.d.** Las conclusiones sobre el estado de los equipos;
   - **4.e.** Las acciones correctivas o preventivas recomendadas, en los casos que ameriten.
5. En caso de que la actualización de firmware o la modificación de algún parámetro de configuración de firmware, llevada a cabo por el contratista, genere la falla, o error, o degradación, o comportamiento no esperado de algún servidor del sistema de Firewalls de Nueva Generación o de alguno de sus componentes, el contratista deberá aplicar la remediación correspondiente; sin costo adicional para el SRI, cumpliendo con el **ACUERDO DE NIVEL DE SERVICIO**.
6. Si de acuerdo con los procedimientos institucionales alguna actividad del mantenimiento preventivo (por su impacto) requiere ser gestionada mediante cambio tecnológico, el contratista deberá entregar un documento que detalle las actividades técnicas de su parte o del fabricante para la ejecución del cambio, las actividades de contingencia y las de reverso, por cada componente involucrado.
7. Al final de cada periodo, el contratista deberá dejar constancia de la entrega del mantenimiento preventivo mediante el **oficio de culminación de periodo de soporte local** al que debe adjuntar la documentación que sustente el cumplimiento de todo lo solicitado en este ámbito, incluyendo:
   - **7.a.** Los **informes de visita de mantenimiento preventivo**.

3.2.2. MANTENIMIENTO CORRECTIVO

1. El servicio de mantenimiento correctivo debe cubrir todos los componentes del objeto de contrato, esto es:
   - **1.a.** (2) Clúster de firewall, principal y alterno;
   - **1.b.** (2) Servidores de gestión, principal y alterno;
   - **1.c.** (2) Gestores de firewall, principal y alterno;
   - **1.d.** (2) Componentes de análisis de configuración y eventos, principal y alterno;
   - **1.e.** (1) Servicio SaaS de protección de correo electrónico.
2. El servicio de mantenimiento correctivo debe estar disponible las 24 horas del día, los 7 días de la semana, durante la vigencia del contrato.
3. El servicio de mantenimiento correctivo se manejará en base a incidentes, los cuales serán registrados mediante los canales de comunicación provistos por el contratista en la fase de **INSTALACIÓN**.
4. Las actividades necesarias para atender un incidente podrán ser realizadas remota o presencialmente según lo requiera el personal técnico del SRI.
5. Las actividades necesarias para atender un incidente podrán llevarse a cabo tanto en horario laboral como fuera de horario laboral, sin costo adicional para a el SRI.

6. Si de acuerdo con los procedimientos institucionales las actividades necesarias para atender un incidente (por su impacto) requieren ser gestionadas mediante cambios tecnológicos, el contratista deberá entregar la documentación que detalle las actividades técnicas de su parte o del fabricante para la ejecución del cambio, las actividades de contingencia y las de reverso, por cada componente involucrado.
7. Si la atención de un incidente requiere el levantamiento de información, la ejecución de algún comando, la captura u obtención de datos o la obtención de registros de eventos ("logs"), es responsabilidad del contratista hacer todas las solicitudes y gestiones necesarias de forma oportuna y previsiva para obtener estos(as), sin perjuicio del cumplimiento del **ACUERDO DE NIVEL DE SERVICIO**.
8. Si la atención de un incidente requiere que se abra un caso de soporte con el fabricante, es responsabilidad del contratista hacer todas las solicitudes y gestiones necesarias de forma oportuna y previsiva para cubrir los requerimientos de información o de acción solicitados por el fabricante dentro de los tiempos que este último requiera.
9. Si durante la atención de un incidente se identifica que se requiere instrumentos, herramientas, materiales o datos con los que no se cuenta en el sitio de atención, se pueden suspender las actividades temporalmente hasta que estos(as) se consigan.
10. Una vez iniciados los trabajos de mantenimiento correctivo en sitio, el contratista deberá garantizar la permanencia del personal técnico necesario durante el tiempo que sea requerido para que se solucione el incidente y el sistema regrese a un estado de operación normal o aceptable para el SRI, o hasta que se haya logrado un progreso aceptable para el SRI, autorizado por el administrador del contrato.
11. Si la atención de un incidente requiere el reemplazo de hardware, este se cerrará cuando se haya instalado el repuesto definitivo habiendo validado el correcto funcionamiento del componente afectado del sistema.
12. Al final de cada periodo anual del servicio de soporte local, se deberá entregar un **reporte de mantenimiento correctivo** en el que se consolide la información de todos los incidentes atendidos durante este. El detalle de atención de cada incidente deberá incluir al menos la siguiente información:
    - **12.a.** La fecha y hora de apertura del caso;
    - **12.b.** Vía de apertura del caso (ej. Por teléfono, email, portal de servicios, etc.);
    - **12.c.** La condición de prioridad a la que corresponde el caso según el **ACUERDO DE NIVEL DE SERVICIO**;
    - **12.d.** El nivel de prioridad del caso según el **ACUERDO DE NIVEL DE SERVICIO**;
    - **12.e.** El tiempo de respuesta máximo establecido en el **ACUERDO DE NIVEL DE SERVICIO**;
    - **12.f.** El tiempo de respuesta real del caso;
    - **12.g.** Breve descripción del incidente reportado por el SRI;
    - **12.h.** Las acciones de remediación aplicadas;
    - **12.i.** Las acciones preventivas recomendadas, cuando corresponda.
13. Al final de cada periodo, el contratista deberá dejar constancia de la entrega del mantenimiento correctivo mediante el **oficio de culminación de periodo de soporte local** al que debe adjuntar la documentación que sustente el cumplimiento de todo lo solicitado en este ámbito, incluyendo:
    - **13.a.** Los **reportes de mantenimiento correctivo**.

3.2.3. ASISTENCIA TÉCNICA

1. El servicio de asistencia técnica debe cubrir todos los componentes del objeto de contrato, esto es:
    - **1.a.** (2) Clúster de firewall, principal y alterno;
    - **1.b.** (2) Servidores de gestión, principal y alterno;
    - **1.c.** (2) Gestores de firewall, principal y alterno;
    - **1.d.** (2) Componentes de análisis de configuración y eventos, principal y alterno;
    - **1.e.** (1) Servicio SaaS de protección de correo electrónico.
2. El servicio de asistencia técnica debe estar disponible las 24 horas del día, los 7 días de la semana, durante la vigencia del contrato.
3. El servicio de asistencia técnica se manejará en base a requerimientos, los cuales serán registrados mediante los canales de comunicación provistos por el contratista en la fase de **INSTALACIÓN**.
4. Las actividades necesarias para atender un requerimiento de asistencia técnica podrán ser realizadas remota o presencialmente según lo requiera el personal técnico del SRI.
5. Las actividades necesarias para atender un requerimiento de asistencia técnica podrán llevarse a cabo tanto en horario laboral como fuera de horario laboral, sin costo adicional para a el SRI.

6. A partir del segundo periodo, el contratista deberá realizar hasta una (1) revisión técnica por cada periodo, bajo demanda, si ahí lo solicita el SRI, en la que se deben realizar las siguientes actividades:
    - **6.a.** Realizar un análisis del estado de salud, de desempeño o de seguridad, de cada componente del objeto de contrato, según corresponda en cada caso, utilizando herramientas y metodologías del fabricante y de acuerdo con el alcance que solicite el SRI;
    - **6.b.** Realizar depuraciones de configuración, afinamientos de desempeño o de seguridad, según corresponda en cada caso, utilizando herramientas y metodologías del fabricante;
    - **6.c.** Realizar la actualización ("upgrade") o instalación de parches de software, según corresponda en cada caso, siguiendo las metodologías del fabricante.
7. El administrador del contrato informará por medio de correo electrónico al Contratista la fecha de inicio de la revisión técnica con al menos 5 días calendario de anticipación.
8. Una vez completada la revisión técnica se debe entregar un **informe de revisión técnica** que tiene que incluir al menos lo siguiente:
    - **8.a.** La fecha y hora de las actividades realizadas;
    - **8.b.** Los resultados o hallazgos del análisis del estado de salud, de desempeño y de seguridad, de acuerdo con el alcance solicitado por el SRI;
    - **8.c.** Las depuraciones de configuración, afinamientos de desempeño o de seguridad que eran necesarios realizar, de acuerdo con el alcance solicitado por el SRI;
    - **8.d.** Las depuraciones de configuración, afinamientos de desempeño o de seguridad realizados;
    - **8.e.** Las actualizaciones ("upgrade") o instalación de parches de software que eran necesarias realizar, de acuerdo con el alcance solicitado por el SRI;
    - **8.f.** Las actualizaciones ("upgrade") o instalación de parches de software realizadas;
    - **8.g.** Las conclusiones sobre el estado de cada componente del objeto de contrato;
    - **8.h.** Las acciones correctivas o de mejora recomendadas, en los casos que ameriten.
9. Si, como resultado de la revisión técnica, se requiere realizar alguna acción correctiva o de mejora sobre alguno de los componentes del objeto de contrato, se deberá acordar la fecha y hora de ejecución con el personal técnico del SRI, siguiendo lo establecido en los procedimientos institucionales.
10. Entre las actividades bajo demanda que cubrirá la asistencia técnica, sin costo adicional para el SRI, se incluyen:
    - **10.a.** Modificar la arquitectura de los componentes implementados;
    - **10.b.** Modificar la topología de los componentes implementados;
    - **10.c.** Modificar el esquema de operación o de integración de los componentes implementados;
    - **10.d.** Realizar la reconfiguración o la reinstalación de los componentes implementados;
    - **10.e.** Realizar el afinamiento de operación o de seguridad de los componentes implementados;
    - **10.f.** Realizar la revisión de salud de los componentes implementados y la respectiva remediación;
    - **10.g.** Configurar nuevos conectores, monitores, "scripts", "jobs" o "tasks" en el Componente de análisis de configuración y eventos;
    - **10.h.** Configurar la protección de correo electrónico para nuevos dominios;
    - **10.i.** Realizar el análisis de seguridad de registros de eventos ("logs") o reportes específicos de los componentes implementados;
    - **10.j.** La documentación que sustente las actividades realizadas.
11. Periódicamente, o cuando el personal del SRI lo solicite, se deberá generar un paquete de información de diagnóstico del sistema de Firewalls de Nueva Generación. El periodo se definirá en conjunto con el personal del SRI. Se procurará que esta actividad se realice automáticamente mediante el uso "scripts", "jobs" o "tasks", en función de las capacidades del sistema.
12. Si de acuerdo con los procedimientos institucionales las actividades necesarias para atender un requerimiento (por su impacto) requieren ser gestionadas mediante cambios tecnológicos, el contratista deberá entregar la documentación que detalle las actividades técnicas de su parte o del fabricante para la ejecución del cambio, las actividades de contingencia y las de reverso, por cada componente involucrado.
13. Al final de cada periodo del periodo del servicio de soporte local se deberá entregar un **reporte de asistencia técnica** en el que se consolide la información de las actividades realizadas durante este. El detalle de cada actividad realizada deberá incluir al menos la siguiente información:
    - **13.a.** La fecha y hora de la solicitud, o la fecha y hora programada, según sea el caso;
    - **13.b.** Vía de solicitud (ej. Por teléfono, email, portal de servicios, oficio, etc.);

13.c. La condición de prioridad a la que corresponde la actividad según el **ACUERDO DE NIVEL DE SERVICIO**;
13.d. El nivel de prioridad de la actividad según el **ACUERDO DE NIVEL DE SERVICIO**;
13.e. El tiempo de respuesta máximo establecido en el **ACUERDO DE NIVEL DE SERVICIO**;
13.f. El tiempo de respuesta real de la actividad;
13.g. Breve descripción solicitud realizada por el SRI;
13.h. Resumen de las actividades realizadas.

14. Al final de cada periodo, el contratista deberá dejar constancia de la entrega de la asistencia técnica mediante el **oficio de culminación de periodo de soporte local** al que debe adjuntar la documentación que sustente el cumplimiento de todo lo solicitado en este ámbito, incluyendo:
14.a. El **reporte de asistencia técnica**;
14.b. El **informe de revisión técnica**.

Una vez culminado cada periodo de soporte local y habiéndose cumplido lo establecido en este ámbito a satisfacción del SRI se suscribirá el **acta de entrega recepción de soporte local**.

3.3. ACUERDOS DE NIVEL DE SERVICIO

1. El tiempo de respuesta se define como el lapso entre el momento en que el SRI hace la solicitud de servicio y el momento en que inicia el análisis técnico por parte del ingeniero especialista designado a dicho requerimiento. Aplica a los servicios de mantenimiento correctivo y de asistencia técnica.
2. La notificación de recepción del requerimiento no es aceptada como el inicio del análisis técnico.
3. El tiempo de reemplazo se define como el lapso desde que se diagnostica la falla de hardware hasta el momento en el que se instala el repuesto y se recupera la operación normal del equipo. Aplica exclusivamente a los incidentes de mantenimiento correctivo que requieren que se aplique garantía técnica.

PRIORIDAD	MANTENIMIENTO CORRECTIVO	ASISTENCIA TÉCNICA	REEMPLAZO DE PARTES Y PIEZAS
1	**a.** Alarma, avería, fallo, o error de alguno de los componentes implementados en el centro de datos principal; **b.** Inhibición completa o parcial de alguno de los componentes implementados en el centro de datos principal; **c.** Indisponibilidad o degradación o alguna afectación de los servicios tecnológicos de producción del SRI que dependen de los componentes implementados; **d.** Corrupción o pérdida de datos del sistema (ej. registros de eventos, registros de auditoría, archivos de políticas, archivos de configuración, etc.); **e.** Atención de alarmas que indiquen una condición grave de los componentes implementados en el centro de datos principal.	**a.** Solicitudes de asistencia o de información asociadas a los componentes implementados en el centro de datos principal; **b.** Solicitudes de asistencia asociadas a servicios tecnológicos de producción del SRI protegidos por los componentes implementados.	**a.** Aplicación de garantía técnica que requiere el reemplazo de alguna parte o pieza, o de equipo completo de los componentes implementados en el centro de datos principal.
2	**f.** Alarma, avería, fallo, o error de alguno de los componentes implementados en el centro de datos alterno; **g.** Inhibición completa o parcial de alguno de los componentes implementados en el centro de datos alterno; **h.** Indisponibilidad o degradación de los servicios tecnológicos del SRI que no son de producción y que dependen de los componentes implementados; **i.** Si los componentes implementados están operando con funcionalidad reducida o limitada, sin afectar a los servicios tecnológicos de producción del SRI.	**c.** Solicitudes de asistencia o de información asociadas a los componentes implementados en el centro de datos alterno; **d.** Solicitudes de asistencia asociadas a servicios tecnológicos del SRI que no son de producción y que están protegidos por los componentes implementados.	**b.** Aplicación de garantía técnica que requiere el reemplazo de alguna parte o pieza, o de equipo completo de los componentes implementados en el centro de datos alterno.
3	**j.** Advertencias ("warnings") de operación de los componentes implementados que no estén causando ninguna indisponibilidad o degradación del mismo sistema ni de los servicios tecnológicos del SRI que dependen de estos.	**e.** Solicitudes de información acerca de nuevas versiones disponibles; **f.** Planificación de trabajados relacionados con los componentes implementados; **g.** Reportes e informes bajo demanda de diagnóstico de los componentes implementados; **h.** Asistencia técnica para afinamiento de los componentes implementados; **i.** Solicitudes de información de diagnóstico obtenida previamente; **j.** Requerimientos de asistencia o intervención presencial del personal especializado del fabricante; **k.** Demás requerimientos de asistencia técnica.	**c.** No aplica.

Tabla 8. Descripción de los niveles de prioridad del ACUERDO DE NIVEL DE SERVICIO.

4. La **tabla 8** describe los niveles de prioridad del **ACUERDO DE NIVEL DE SERVICIO**.
5. En los niveles de prioridad del ACUERDO DE NIVEL DE SERVICIO (**tabla 8**) se considera a el servicio SaaS de protección de correo electrónico como parte de los componentes implementados en el centro de datos principal.
6. La **tabla 9**, de tiempos de respuesta por prioridad, establece los umbrales máximos aceptables de tiempo de espera para cada prioridad. El tiempo de respuesta está medido en horas consecutivas salvo que se indique lo contrario.

Prioridad	Mantenimiento Correctivo	Asistencia Técnica	Reemplazo de Partes y Piezas
1	1 hora	3 horas	8 horas
2	3 horas	6 horas	16 horas laborables
3	24 horas	16 horas laborables	N/A

Tabla 9. Tiempos de respuesta por prioridad.

4. PLAZO DE EJECUCIÓN

El plazo de ejecución de este contrato será de **1.184 días calendario**.

4.1. BIENES REQUERIDOS

1. El plazo de la entrega de los bienes instalados será de hasta **90 días calendario** contados a partir de la notificación del administrador del contrato. Para el efecto, el contratista deberé entregar el **oficio de culminación de la instalación del hardware**.
2. El plazo de la vigencia de la garantía técnica y del soporte de fábrica será de **1.095 días calendario** contados a partir de la fecha de la culminación de la instalación del hardware.

4.2. SOFTWARE Y SERVICIOS CONEXOS REQUERIDOS

1. El plazo de la vigencia del licenciamiento de todos los elementos del componente de software será de **1.095 días calendario** contados a partir de la fecha de la culminación de la instalación del hardware.
2. El plazo de la entrega del servicio de migración, mediante el **oficio de culminación de migración**, será de hasta **240 días calendario**, contados a partir del día siguiente de la culminación de la instalación del hardware.
3. El plazo de la vigencia del servicio de soporte local será de hasta **884 días calendario**, contados a partir del día siguiente de la culminación de la migración, divididos en tres periodos:
   3.a. Primer periodo: 295 días,
   3.b. Segundo periodo: 295 días,
   3.c. Tercer periodo: 294 días.

4.3. DOCUMENTOS Y ACTIVIDADES

1. Cualquier recurso o acceso que necesite el contratista para cumplir de manera exitosa con las actividades objeto del presente contrato deberá ser solicitado al SRI con al menos **2 días hábiles** de antelación.
2. Cualquier información, dato o registro que necesite el contratista para cumplir de manera exitosa con las actividades objeto del presente contrato deberá ser solicitado al SRI con al menos **2 días hábiles** de antelación.
3. El administrador del contrato informará mediante correo electrónico al Contratista las fechas de las visitas para realizar las actividades de mantenimiento con al menos **5 días calendario** de anticipación.
4. El plazo de la entrega de los **informes de visita de mantenimiento preventivo** será de hasta **10 días hábiles** contados a partir del día siguiente de la culminación de la visita.

5. El plazo de la entrega de los **reportes de mantenimiento correctivo** será de hasta **5 días hábiles** contados a partir del día siguiente de la fecha de finalización del periodo correspondiente.
6. El plazo de la entrega de los **reportes de asistencia técnica** será de **5 días hábiles** contados a partir del día siguiente de la fecha de finalización del periodo correspondiente.

5. FORMA Y CONDICIONES DE PAGO

1. **Componente de hardware, instalación y garantía técnica de hardware, licenciamiento del componente del software:** El 100% de este rubro se pagará contra entrega, previa presentación de la planilla de pago y la suscripción del acta de entrega recepción correspondiente.
   Como condición para la suscripción del **acta de entrega recepción de la instalación del hardware** el contratista deberá entregar, mediante oficio dirigido al administrador del contrato, la siguiente documentación:
   - **1.a.** El **oficio de entrega de hardware**, con sus adjuntos;
   - **1.b.** El **certificado de garantía técnica del hardware**, con sus adjuntos;
   - **1.c.** El **oficio de culminación de la instalación del hardware**, con sus adjuntos;
   - **1.d.** El detalle de los canales de comunicación disponibles para la apertura de incidentes de mantenimiento correctivo y requerimientos de asistencia técnica, siendo obligatorios el medio telefónico, el correo electrónico y un portal de gestión de requerimientos tecnológicos (ITSM);
   - **1.e.** El procedimiento de ingreso y escalamiento de incidentes de mantenimiento correctivo y requerimientos de asistencia técnica.
2. **Migración:** El 100% de este rubro se pagará contra entrega previa presentación de la planilla de pago y la suscripción del acta de entrega recepción correspondiente.
   Como condición para la suscripción del **acta de entrega recepción de la migración** el contratista deberá entregar el **oficio de culminación de la migración**, con sus adjuntos.
3. **Soporte local:** Se pagará en partes iguales, al final de cada periodo, previa presentación de la planilla de pago y la suscripción del acta de entrega recepción correspondiente.
   Como condición para la suscripción del **acta de entrega recepción periódica del soporte local** el contratista deberá entregar el **oficio de culminación de periodo de soporte local**, con sus adjuntos.

6. LUGAR DE ENTREGA

1. Los equipos que correspondan a los componentes de hardware principales y las actividades que requieran una intervención directa sobre estos deben entregarse en el Centro de Datos Principal del SRI, ubicado en la ciudad de Quito.
2. Los equipos que correspondan a los componentes de hardware de contingencia y las actividades que requieran una intervención directa sobre estos deben entregarse en el Centro de Datos Alterno del SRI, ubicado en la ciudad de Guayaquil.
3. Las actividades que no requieran una intervención directa de los equipos deben entregarse en la ciudad de Quito, Av. Río Amazonas entre Unión Nacional de Periodistas y Alfonso Pereira, Plataforma Gubernamental de Gestión Financiera, Bloque 5 (Azul), piso 1.
4. Toda documentación deberá ser entregada principalmente en formato digital, suscrita electrónicamente y dirigida la dirección de correo electrónico del administrador del contrato o a la que este defina. En los casos en que el administrador del contrato admita que la documentación sea diligenciada en formato físico, esta deberá entregarse en la ciudad de Quito, Av. Río Amazonas entre Unión Nacional de Periodistas y Alfonso Pereira, Plataforma Gubernamental de Gestión Financiera, Bloque 5 (Azul), piso 1, o donde señale el administrador del contrato.
5. En todos los casos el administrador del contrato podrá actualizar la dirección de entrega durante el período de ejecución del contrato, si bien esta modificación no producirá un cambio de ciudad.