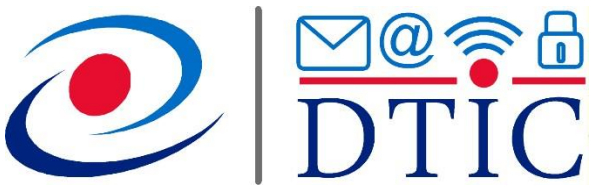

Términos de Referencias para la Renovación del Mantenimiento utilizado en los Firewalls

Dirección de Tecnología de la información y Comunicaciones

Introducción

De acuerdo a la ley 10-04 del 20 de enero de 2004 y su reglamento No. 06-04 de fecha 20 de septiembre del mismo año 2004 , la Cámara de Cuentas es el órgano superior del Sistema Nacional de Control, Fiscalización y Auditoria de los bienes Públicos y tomando en cuenta los dos primeros considerando de la referida ley que establecen que actualmente en la Republica Dominicana está en marcha un importante proceso de reforma y modernización de las instituciones que conforman el Estado en procura de hacerlas más dinámicas y eficientes.

Justificación

Tomando en cuentas que las informaciones almacenadas en nuestras redes de datos y que las amenazas de red pueden provenir de cualquier parte, presentarse en cualquier momento y generar problemas incluso antes de que sepa de su existencia. Para afrontarlas necesitamos continuar con la solución de seguridad actualizada y licenciada para mantener unas actualizaciones constantes de cara a todas las amenazas que surgen diariamente.

Los servicios utilizados por suscripción son los siguiente: **APT Blocker**, **Application Control**, **Instrusion Prevention Services**, **Web Blocker**, **Spam Blocker**, **Data Loss Prevention**, **Reputation Enabled Defense**.

Los potentes servicios de seguridad basados en estas suscripciones aumentan la protección en áreas de ataque críticas para brindar múltiples niveles de defensa. WatchGuard es capaz de integrar componentes de seguridad de primer nivel en una sola plataforma para brindar seguridad más potente.

Objetivo General

Renovar el servicio de mantenimiento correspondiente a los firewalls watchguard.

Definiciones

APT Blocker: es un servicio basado en la nube que usa una combinación de espacio aislado y todo un sistema de emulación para detectar y bloquear amenazas avanzadas persistentes (Advanced Persistent Threats, APT) altamente sofisticadas.

Application Control: permite proteger y monitorear el uso de aplicaciones improductivas, inadecuadas y peligrosas para nuestra infraestructura.

Intrusion Prevention Service, IPS: ofrece protección integrada de las vulnerabilidades maliciosas, incluyendo los desbordamientos del búfer, inyecciones de código SQL y ataques de scripts entre sitios.

Web Blocker: controla el acceso a los sitios que alojan materiales cuestionables o representan riesgos de seguridad para nuestra institución.

Gateway Antivirus (GAV): analiza el tráfico en todos los protocolos principales para detener amenazas.

Spam Blocker: ofrece una protección continua contra correos electrónicos peligrosos y no deseados.

Reputation Enabled Defense: garantiza una exploración web rápida y segura con la aplicación de seguridad a sitios web basada en su reputación en la nube.

Data Loss Prevention: inspecciona automáticamente los datos en movimiento para detectar infracciones de la política corporativa al detectar y prevenir la exfiltración de carácter sensible para la institución.

Threat Detection and Response: recopila, correlaciona y analiza datos de red y equipos finales para detectar, priorizar y permitir acciones inmediatas para detener amenazas.

DNS Watch: reduce las infecciones de malware al detectar y bloquear solicitudes DNS maliciosas, redirigiendo a los usuarios a una página segura con información para reforzar las mejores prácticas de seguridad.

Access Portal: Proporciona una ubicación central para acceder a aplicaciones alojadas en la nube y acceso seguro y sin cliente a recursos internos y RDP y SSH.

Comando Dimension: Tome medidas inmediatas para bloquear las amenazas de red potenciales y activas identificadas por Dimension.

IntelligentAV: utiliza IA para proporcionar protección predictiva contra malware de día cero.

Especificaciones

ESPECIFICACIONES TECNICAS	
Nombre del Equipo	Watchguard
Modelo	M470
Cantidad de Firewalls	2
Firecluster	**Activo/Pasivo**
Seriales	80100483DDCCE 801004835F80E
Licencias para renovar	1) Application Control 2) Reputation Enabled Defense 3) SpamBlocker 4) LiveSecurity Service 5) WebBlocker 6) APT Blocker 7) Data Loss Prevention 8) Gateway Antivirus (AV)

	9) Intrusion Prevention 10) Threat Detection and Response 11) DNS Watch 12) Access Portal 13) Comando Dimension 15) IntelligentAV
Tipo de licencia	TOTAL SECURITY

Condiciones del Oferente:

- Deberá demostrar mediante carta escrita que su compañía tiene más de 5 años en el Mercado y demostrar evidencia de ser Partner Autorizado.
- Apoyo disponible del proveedor, soporte de producto y soporte técnico.
- Deberá cumplir con los aspectos técnicos contenidos en este documento.
- Deberá incluir entrenamiento actualizado para hasta 3 personas.
- Todos los procesos y actividades serán evaluados según la normativa vigente de Compra y contrataciones.