**Anexo tecnico**

**Objeto: Servicio de Soporte para los sistemas de seguridad de la entidad designada por la CCD**

**Junio 2025**

**Objeto: Servicio de Soporte para los sistema de seguridad de la entidad designada por la CCD.**

1. Descripción del Servicio

El servicio comprende la gestión, actualización, soporte y mantenimiento de la red de seguridad de la entidad designada por la CCD, asegurando la correcta operación y protección de los entornos en la nube AWS, la nube Oracle y la red interna de la entidad. Esto incluye la administración de dispositivos Fortinet, como FortiGate y FortiAnalyzer, así como la implementación de medidas de seguridad para prevenir y mitigar ciberataques.

2. Alcance del Servicio

El alcance del servicio comprende la gestión integral de la red de seguridad perimetral de la entidad designada por la CCD, incluyendo la administración de dispositivos Fortinet (FortiGate y FortiAnalyzer), el soporte técnico especializado, el mantenimiento preventivo y correctivo, el monitoreo de amenazas, el escaneo de vulnerabilidades y la aplicación de mejores prácticas de seguridad, con cobertura sobre los entornos tecnológicos del Instituto:

- Nube pública AWS
- Nube Oracle
- Red interna de la entidad designada por la CCD

El contratista deberá prestar un servicio que incluya las siguientes actividades:

Actualmente la entidad designada por la Corporación cuenta con la siguiente infraestructura de seguridad:

- FortiGate 600E - FG6H0ETB20907695
- FortiGate 600E - FG6H0ETB20907720
- FortiAnalyzer 200F - FL-2HFTB20001011

Para las plataformas tipo NGFW, el oferente deberá suministrar el soporte:

1. Servicios de prevención de instrucciones – IPS
2. Servicios de protección de malware (AMP), antivirus, malware en dispositivos móviles, botnets, CDR (content disarm and reconstruction), protección contra propagación de virus, servicios de Sandbox Cloud

3. URL, DNS y servicio de filtrado de video
4. Anti-Spam
5. Servicio de prevención de malware basado en inteligencia Artificial
6. Servicio de prevención de perdida de datos
7. Control de aplicaciones, a través de la suscripción con el fabricante.
8. Control de aplicaciones tipo SaaS - CASB, a través de la suscripción con el fabricante.
9. Gestionar el soporte y garantía de fabricante en modalidad 7x24 por 12 meses a partir del 10 de junio de 2025.
10. El servicio de soporte y garantía del fabricante debe incluir el recambio de las unidades afectadas en caso de una falla critica.

Para la plataforma FortiAnalyzer 200F el oferente deberá suministrar el soporte para:

1. Gestionar el soporte y garantía de fabricante en modalidad 7x24 por 12 meses a partir de la fecha 27 de junio de 2025.
2. El servicio de soporte y garantía del fabricante debe incluir el recambio de la unidad afectada en caso de una falla critica.

- Administración y optimización del firewall, asegurando configuraciones seguras y alineadas con las políticas de seguridad de la entidad en los entornos de AWS, Oracle y la red interna.
- Gestión de reglas de seguridad y accesos, incluyendo configuración de políticas de filtrado de tráfico, segmentación de red y cierre de puertos TCP innecesarios.
- Monitoreo y detección de amenazas, mediante herramientas de seguridad avanzadas como FortiAnalyzer, asegurando la identificación proactiva de ataques y accesos no autorizados.
- Soporte técnico especializado para la resolución de incidentes, ajustes de configuración y actualizaciones de firmware y software de los dispositivos Fortinet.
- Mantenimiento preventivo y correctivo, asegurando la operatividad del firewall y su alineación con las mejores prácticas de seguridad.
- Escaneo de seguridad y análisis de vulnerabilidades, identificando brechas en la configuración del firewall y recomendando medidas correctivas.
- Gestión integral del firewall en todas las plataformas involucradas (nube AWS, nube Oracle y red interna de la entidad designada por la CCD), asegurando una administración centralizada y efectiva.

3. Modelo de Trabajo

El modelo de trabajo estará basado en un enfoque estructurado que garantice la correcta gestión, actualización, soporte y mantenimiento de la red de seguridad de la entidad designada por la CCD en los entornos mencionados hasta el 31 de diciembre de 2025, asegurando la continuidad operativa y el cumplimiento de las políticas de seguridad de la entidad.

3.1 Diagnóstico y documentación inicial

- Levantamiento del estado actual de la configuración del firewall en la nube AWS, la nube Oracle y la red interna de la entidad designada por la CCD.
- Revisión y documentación de reglas de seguridad existentes en los dispositivos Fortinet (FortiGate y FortiAnalyzer).
- Identificación de brechas de seguridad y análisis de vulnerabilidades en la infraestructura de red.
- Elaboración de un informe con el estado de la configuración del firewall y recomendaciones iniciales.

3.2 Gestión Soporte y actualización de la configuración del firewall

- Implementación de ajustes en las reglas de seguridad para optimizar el control de tráfico y accesos.
- Aplicación de actualizaciones de firmware y software en los dispositivos Fortinet para fortalecer la seguridad.
- Configuración y ajuste de políticas de seguridad en los entornos de AWS, Oracle y la red interna de la entidad designada por la CCD.
- Cierre de puertos no autorizados y segmentación de la red según las mejores prácticas.
- Atención de incidentes relacionados con la seguridad perimetral y el funcionamiento del firewall.
- Monitoreo proactivo de los dispositivos Fortinet mediante FortiAnalyzer, identificando amenazas y accesos no autorizados.
- Aplicación de parches y correcciones de seguridad en caso de vulnerabilidades detectadas.
- Respaldo y gestión de configuraciones del firewall para garantizar la recuperación ante incidentes.

3. 3 Cierre del servicio y entrega de informe final

- Elaboración de un informe consolidado con los ajustes implementados, hallazgos detectados y mejoras realizadas en la seguridad de la red.
- Evaluación del cumplimiento de los objetivos del servicio y recomendaciones finales para la optimización de la red de seguridad del de la entidad designada por la CCD.

3. 4 Renovación del licenciamiento de Fortinet

- Renovación de licencia anual de dispositivos Fortinet FortiGate 600E - FG6H0ETB20907695, FortiGate 600E - FG6H0ETB20907720 y FortiAnalyzer 200F - FL-2HFTB20001011.
- Evaluación del cumplimiento de los objetivos del servicio y recomendaciones finales para la optimización de la red de seguridad de la entidad designada por la CCD.

4. Beneficios del Servicio

La implementación del servicio de gestión, soporte, mantenimiento y actualización de la red de seguridad de la entidad designada por la CCD ofrece beneficios estratégicos, operativos y técnicos que contribuyen al fortalecimiento de la postura de seguridad de la Entidad. Entre los principales beneficios se destacan:

✅ 1. Fortalecimiento de la seguridad perimetral

Se garantiza una protección más robusta de los entornos tecnológicos de la entidad designada por la CCD (nube AWS, nube Oracle y red interna), mediante una administración centralizada de firewalls Fortinet y la aplicación constante de mejores prácticas en ciberseguridad.

✅ 2. Prevención de ciberataques y accesos no autorizados

El monitoreo proactivo, la detección de amenazas y la respuesta oportuna ante incidentes minimizan el riesgo de brechas de seguridad, protegiendo la integridad, confidencialidad y disponibilidad de la información institucional.

✅ 3. Reducción de vulnerabilidades

La aplicación de actualizaciones de firmware, escaneos periódicos de seguridad y ajustes en la configuración permiten identificar y corregir vulnerabilidades técnicas antes de que puedan ser explotadas.

✅ 4. Continuidad operativa asegurada

✅ mantenimiento preventivo y correctivo de los dispositivos Fortinet evita interrupciones del servicio de red y garantiza el funcionamiento continuo de las plataformas que soportan los procesos misionales y administrativos de la entidad designada por la CCD Administración técnica especializada

La intervención de un equipo técnico certificado y con experiencia comprobada en dispositivos Fortinet y gestión de seguridad permite tomar decisiones informadas, implementar configuraciones seguras y asegurar el cumplimiento de normativas como ISO 27001, NIST y lineamientos de Gobierno Digital.

✅ 5. Visibilidad y trazabilidad de los eventos de seguridad

El uso de FortiAnalyzer y herramientas de monitoreo brinda a la entidad designada por la CCD reportes detallados sobre el comportamiento de la red, eventos anómalos y tendencias de ataque, facilitando una gestión proactiva de la seguridad.

✅ 6. Cumplimiento normativo y auditoría

El servicio fortalece el cumplimiento de las políticas internas de seguridad de la información y las exigencias normativas del sector público, permitiendo evidenciar la gestión ante auditorías internas y externas.

✅ 7. Optimización de la administración de reglas de firewall

La revisión, documentación y depuración continua de las reglas de firewall asegura que las políticas de acceso estén alineadas con los requerimientos operativos y de seguridad, mejorando el rendimiento y control de la red.

✅ 8. Transferencia de conocimiento y sostenibilidad

El modelo de trabajo propuesto incluye la entrega de documentación técnica, informes periódicos y recomendaciones, lo que fortalece las capacidades internas de la entidad designada por la CCD y facilita la sostenibilidad de la operación.

5. Fases de Ejecución del Servicio

La ejecución del servicio de gestión, mantenimiento y soporte de la red de seguridad de la entidad designada por la CCD se desarrollará en cinco fases hasta el 31 de Diciembre de 2025, de acuerdo con el modelo de trabajo planteado. Cada fase incluye actividades específicas orientadas a garantizar la operación segura, actualizada y monitoreada de los dispositivos de seguridad en los entornos AWS, Oracle y red interna del Instituto.

Fase 1. Diagnóstico y documentación inicial

**Objetivo:** Establecer la línea base del estado actual de la red de seguridad y la configuración de los dispositivos Fortinet.

**Actividades:**

- Levantamiento del estado de configuración en AWS, Oracle y red interna.
- Revisión de reglas, políticas de seguridad y segmentación de red.
- Identificación de brechas de seguridad y vulnerabilidades.
- Elaboración de informe diagnóstico con hallazgos y recomendaciones.

Fase 2. Gestión Soporte y actualización de la configuración del firewall

**Objetivo:** Optimizar la configuración de seguridad perimetral de acuerdo con las mejores prácticas y necesidades institucionales.

**Actividades:**

- Ajustes en reglas de acceso y políticas de tráfico.
- Cierre de puertos abiertos innecesarios.
- Segmentación de red por niveles de seguridad.
- Aplicación de actualizaciones de firmware/software en FortiGate y FortiAnalyzer.
- Registro y control de los cambios aplicados.

- Soporte ante incidentes relacionados con los firewalls.
- Aplicación de parches y correcciones de seguridad.
- Monitoreo continuo mediante FortiAnalyzer.
- Respaldos de configuraciones y gestión de cambios.
- Mantenimientos preventivos y correctivos.

Fase 3. Cierre del servicio

**Objetivo:** Consolidar los resultados del servicio prestado, entregar la documentación final y presentar recomendaciones para la continuidad de la operación segura.

**Actividades:**

- Elaboración de informe final del servicio, incluyendo:
  - Ajustes implementados.
  - Incidentes atendidos.
  - Vulnerabilidades mitigadas.
  - Recomendaciones técnicas.
- Validación del cumplimiento de objetivos.
- Entrega formal de documentación y configuraciones finales.
- Acta de cierre del servicio con la entidad designada por la CCD

Fase 4. Gestión de Licencias Fortinet Firewall y Fortianalyzer

**Objetivo:** Gestionar el licenciamiento de los dispositivos Fortinet Fortigate y Fortyanalizer de la entidad designada por la CCD por 12 meses.

**Actividades:**

- Gestionar el Licenciamiento previo a las fechas de vencimiento.
- Instalación de Licencias.
- Generación de certificado de Licenciamiento.

**Objetivo:** Evaluar y mejorar continuamente la postura de seguridad de la entidad designada por la CCD con base en análisis técnicos e indicadores de riesgo.

**Actividades:**

- Ejecución periódica de escaneos de vulnerabilidades.
- Análisis de eventos de seguridad, tendencias de ataque y comportamientos anómalos.
- Generación de reportes técnicos con hallazgos y recomendaciones de mejora.
- Documentación de mejoras implementadas y ajustes proactivos.

6. Entregables por Fase del Servicio Firewall para la entidad designada por la CCD

Fase 1: Documentación inicial del estado de la red de seguridad

Objetivo: Realizar un diagnóstico detallado del estado actual de la red de seguridad de la entidad designada por la CCD, incluyendo la nube AWS, la nube Oracle y la red interna, con énfasis en la configuración y operación de los dispositivos Fortinet.

Entregables:

Fase 1 – Diagnóstico y documentación inicial

Objetivo: Establecer el estado actual de la red de seguridad en AWS, Oracle y la red interna.

Entregables:

- Informe de diagnóstico técnico del estado actual del firewall en cada entorno.
- Inventario de dispositivos Fortinet con su configuración actual.
- Documentación de reglas y políticas de seguridad existentes.
- Identificación de brechas de seguridad, puertos abiertos y vulnerabilidades.
- Recomendaciones iniciales para mejorar la seguridad perimetral.

Fase 2 – Gestión, Soporte y actualización de la configuración del firewall

Objetivo: Optimizar la configuración de los dispositivos Fortinet con base en las recomendaciones y políticas institucionales.

Entregables:

- Registro de ajustes aplicados en reglas de seguridad y políticas de acceso.
- Bitácora de cambios en la configuración de los dispositivos Fortinet.
- Evidencia de actualizaciones de firmware y software implementadas.
- Validación técnica de cierre de puertos innecesarios y segmentación aplicada.
- Informe de adecuaciones realizadas conforme a buenas prácticas de seguridad.
- Reportes mensuales de atención a incidentes de seguridad.
- Registro de parches aplicados y respaldos de configuración.
- Informe de mantenimientos preventivos y correctivos realizados.
- Bitácora de soporte técnico con tiempos de respuesta y resolución.
- Documentación de configuraciones actualizadas posterior a cada intervención.

Fase 3 – Cierre del servicio

Objetivo: Consolidar los resultados del servicio prestado y entregar formalmente la documentación final.

Entregables:

- Informe final consolidado del servicio, incluyendo:
    - Estado de la red al cierre del contrato.
    - Ajustes realizados.
    - Incidentes gestionados.
    - Vulnerabilidades mitigadas.
    - Recomendaciones finales.
- Repositorio digital con la documentación técnica y respaldos.
- Acta de cierre del servicio firmada por ambas partes.

Fase 4. Gestión de Licencias Fortinet Firewall y Fortianalyzer

Alcance: Gestionar el licenciamiento de los dispositivos Fortinet Fortigate y Fortyanalizer de la entidad designada por la CCD por 12 meses. Entregables:

- Licenciamiento Instalado en dispositivos Fortinet.
- Certificación de licenciamiento por 12 meses emitido por el fabricante.

**INFORMES**

**1. Informe de diagnóstico inicial**
📅 **Plazo de entrega:** Dentro de los primeros 10 días hábiles desde el acta de inicio.
📄 **Contenido mínimo:**
Estado actual de configuración de los firewalls en AWS, Oracle y red interna.
Políticas y reglas activas en FortiGate y FortiAnalyzer.
Puertos abiertos, servicios activos y riesgos potenciales.
Brechas de seguridad detectadas.
Recomendaciones iniciales para ajustes técnicos.

**2. Informes mensuales de ejecución**
📅 **Periodicidad:** Cada mes, dentro de los primeros cinco (5) días hábiles del mes siguiente.
📄 **Contenido mínimo:**
Actividades ejecutadas (mantenimientos, soporte, actualizaciones).
Cambios realizados en las reglas o configuración del firewall.
Incidentes atendidos, con tiempo de respuesta y resolución.
Eventos detectados (accesos no autorizados, ataques, anomalías).
Escaneos de vulnerabilidades realizados y acciones tomadas.
Parches o actualizaciones aplicadas.
Estado de los dispositivos Fortinet.
Recomendaciones técnicas o preventivas.

**3. Reportes de escaneo de seguridad**

📅 **Periodicidad:** Bimensual o según la frecuencia definida por la entidad designada por la CCD.

📄 **Contenido mínimo:**

Resultados del escaneo (vulnerabilidades, configuraciones débiles).
Análisis de criticidad y priorización de hallazgos.
Acciones de mitigación sugeridas o ejecutadas.
Evolución frente a escaneos anteriores.

**4. Reportes de eventos de seguridad**

📅 **Periodicidad:** Trimestral o por cada evento crítico.

📄 **Contenido mínimo:**

Descripción de incidentes relevantes detectados en FortiAnalyzer.
Análisis técnico del evento (fuente, técnica, comportamiento).
Medidas de contención o respuesta aplicadas.
Evaluación del impacto.
Recomendaciones de mejora.

**5. Informe de mejoras y endurecimiento**

📅 **Periodicidad:** Trimestral (o según cronograma pactado con la entidad designada por la CCD).

📄 **Contenido mínimo:**

Cambios realizados para fortalecer la seguridad perimetral.
Optimización de reglas, zonas seguras y segmentación de red.
Nuevas configuraciones aplicadas.
Justificación técnica y respaldo normativo.

**6. Informe final del servicio**

📅 **Plazo de entrega:** Últimos 10 días del contrato.

📄 **Contenido mínimo:**

Consolidado de todas las actividades realizadas.
Estado final de la red de seguridad y dispositivos.
Historial de incidentes y acciones tomadas.
Vulnerabilidades mitigadas.
Documentación técnica generada (configuraciones, reportes, respaldos).
Recomendaciones para continuidad y mejora.
Lecciones aprendidas.

**TIEMPOS DE RESPUESTA A INCIDENTES Y REQUERIMIENTOS**

Se definen tiempos de atención de incidentes y requerimientos, durante la vigencia del contrato.

| PRIORIDAD | DESCRIPCIÓN |
|---|---|

| | | |
|---|---|---|
| 1 | Crítica | La producción está parada o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la entidad y/o está en situación de emergencia. |
| 2 | Alta | Experimenta perdida del servicio, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida. |
| 3 | Media | Experimenta una pérdida de servicio menor, el impacto es un inconveniente. |
| 4 | Baja | No impacta la operación del programa, no se experimenta perdida del servicio y no se impide la operación de los sistemas. |

| PRIORIDAD | | DESCRIPCIÓN |
|---|---|---|
| 1 | Crítica | De manera remota (2) horas de atención y (3) horas de traslado a sitio. |
| 2 | Alta | De manera remota (3) horas de atención y (4) horas de traslado a sitio. |
| 3 | Media | De manera remota (8) horas y de ser necesario traslado a sitio |
| 4 | Baja | De manera remota (24) horas y de ser necesario traslado a sitio |

7. PERFILES MÍNIMOS PARA LA EJECUCIÓN DEL CONTRATO

El contratista deberá ser PARTNER certificado por FORTINET y deberá presentar un certificado emitido por el fabricante dirigido a la entidad.

| PERFILES | | |
|---|---|---|
| EQUIPO | TITULO / CERTIFICACIONES / CURSOS | EXPERIENCIA PROFESIONAL ESPECIFICA |
| Gerente de Proyecto<br>Un (01) Ingeniero | Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.<br>Posgrado en Gerencia de Proyectos y/o Certificación PMP.<br>Certificación Itil Foundation v3 o superior | Experiencia general de cinco (5) años en gerencia de proyectos de TI. |
| Líder Técnico<br>Un (01) Ingeniero | Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. | Experiencia general de con cinco (5) años en proyectos de TI.<br>Certificaciones de Experiencia especifica de mínimo de cinco (5) |

| | | |
|---|---|---|
| | Certificación en Scrum y/o Foundation Professional y/o similares | años, implementación en plataformas de seguridad, soporte y en gestión de incidentes o eventos de seguridad. |
| Implementador Un (01) Ingeniero | Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.<br><br>Certificación vigente como profesional, analista de seguridad en redes y/o Certificación vigente en Arquitecto de seguridad | Experiencia general de tres (3) años en proyectos de TI. |