# INFORME DE JUSTIFICACIÓN

## ADQUISICIÓN DE EQUIPOS DE SEGURIDAD PERIMETRAL FORTINET

SANTO DOMINGO, R.D.
18 DE ENERO DEL 2024

TABLA DE CONTENIDO

# 1. Objetivo

Presentar la justificación técnica para adquisición de equipos de ciberseguridad de la marca Fortinet a ser utilizados para la seguridad perimetral, la interconexión entre localidades, administración centralizada, protección de dispositivos finales y el fortalecimiento de la ciberseguridad de la infraestructura tecnológica del Poder Judicial Dominicano.

# 2. Antecedentes

El Poder Judicial ha estado trabajando en la implementación de su Plan Estratégico Institucional, Visión Justicia 20/24. Este Plan Estratégico Institucional inició en el año 2020 un proceso de transformación digital y evolución de todo el sistema de administración de justicia que ha tomado impulso con la ley 339-22 sobre el uso de medios digitales en el Poder Judicial.
El pasado 4 de agosto del 2020 fue adjudicado el proceso de Excepción Por Exclusividad para la Adquisición De Equipos De Gestión Unificada De Amenazas (UTM) Para El Poder Judicial Dominicano, Ref. PEEX-CPJ-007-2020. En este proceso se adquirieron equipos de seguridad de la marca Fortinet y están siendo utilizados para integrar las sedes judiciales a través de la implementación de canales seguros y otros controles de seguridad.

Actualmente el Poder Judicial cuenta con 21 sedes protegidas mediante equipos de seguridad perimetral de gestión de amenazas unificadas (UTM). Cada una de estas localidades posee enlaces seguros (VPN) para la interconexión hacia nuestro Datacenter principal, facilitando el acceso a los recursos internos que no se encuentran publicados en internet y aplicando medidas de protección ante ciberataques:

| No. | Modelo | Localidad | Región |
|---|---|---|---|
| 1 | FortiGate 300E | Edif. De las Cortes | Distrito Nacional |
| 2 | FortiGate 500E | Edif. Suprema Corte de Justicia | Distrito Nacional |
| 3 | FortiGate 1100E | NAP del Caribe | Santo Domingo |
| 4 | FortiGate 80E | San Juan de la Maguana | Sur |
| 5 | FortiGate 100E | San Francisco de Macorís | Norte |
| 6 | FortiGate 100E | Puerto Plata | Norte |
| 8 | FortiGate 200E | KM22 | Santo Domingo |
| 9 | FortiGate 300E | Santiago | Norte |
| 10 | FortiGate 100E | Sto. Dgo. Este | Santo Domingo Este |
| 11 | FortiGate 300E | Ciudad Nueva | Santo Domingo Este |
| 12 | FortiGate 100E | San Pedro de Macorís | Este |

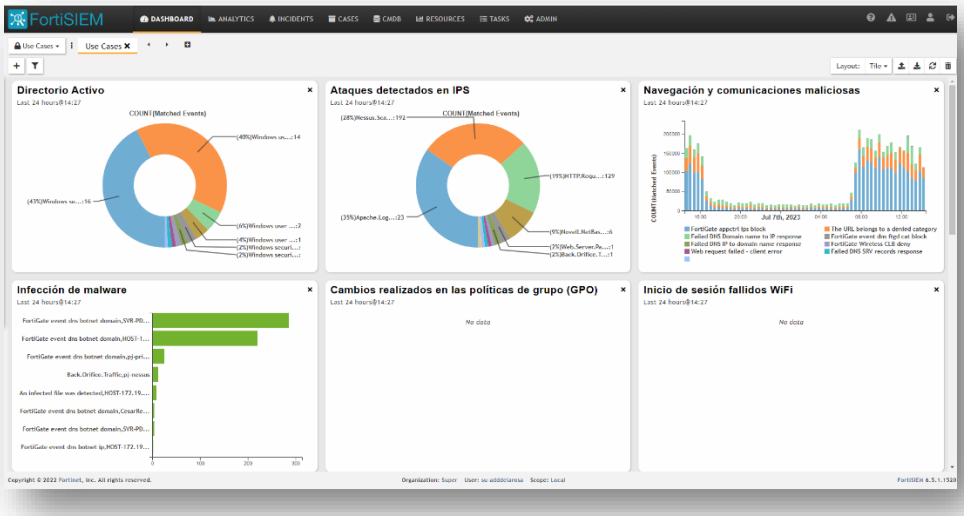
| | | | |
|---|---|---|---|
| 13 | FortiGate 80E | La Romana | Este |
| 14 | FortiGate 60E | KM22 | Santo Domingo |
| 15 | FortiGate 100E | Bonao | Norte |
| 16 | FortiGate 100E | Monte Cristi | Norte |
| 17 | FortiGate 80E | Jdo. Paz. 1ra. | Santo Domingo Este |
| 18 | FortiGate 60E | Juzgado de Trabajo D.N. | Distrito Nacional |
| 19 | FortiGate 80E | Barahona | Sur |
| 20 | FortiGate 80E | La Vega | Norte |
| 21 | FortiGate 100E | San Cristóbal | Sur |

El 13 de abril del 2021 fue adjudicada la empresa IT Global Enterprise Services, INC. el proceso de referencia número: LPN-CPJ-14-2021 a fin de adquirir soluciones para la gestión de controles de acceso y el análisis y correlación de eventos de seguridad para la infraestructura tecnológica del Poder Judicial.

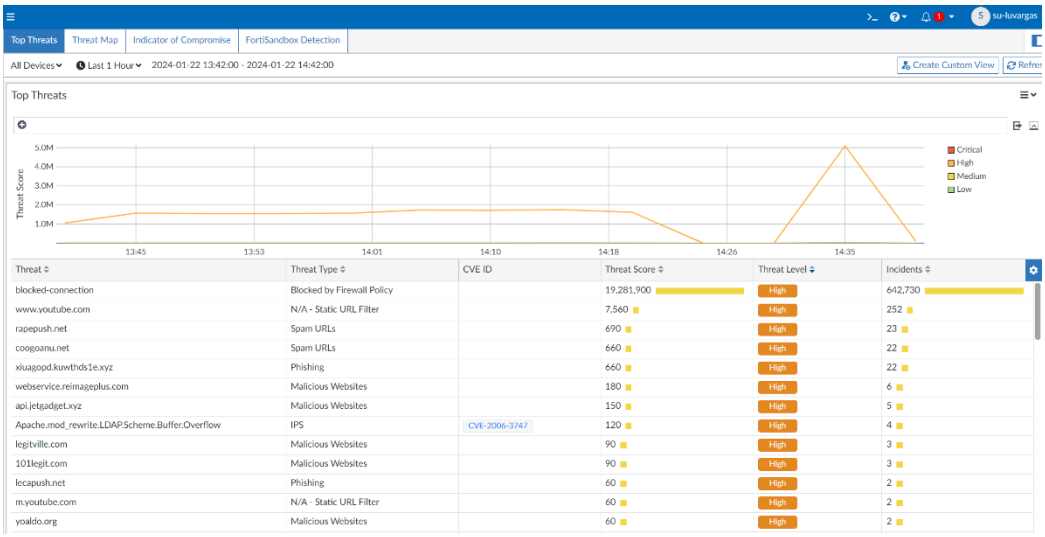
El 9 de mayo del 2023 fue adjudicada a la empresa Multicomputos S.R.L. el proceso de referencia número: PEEX-CPJ-06-2023 a fin de renovar los servicios de suscripción de las soluciones de ciberseguridad de Fortinet.

En ese sentido, hemos incorporado los siguientes componentes de ciberseguridad de Fortinet a nuestra infraestructura de protección:

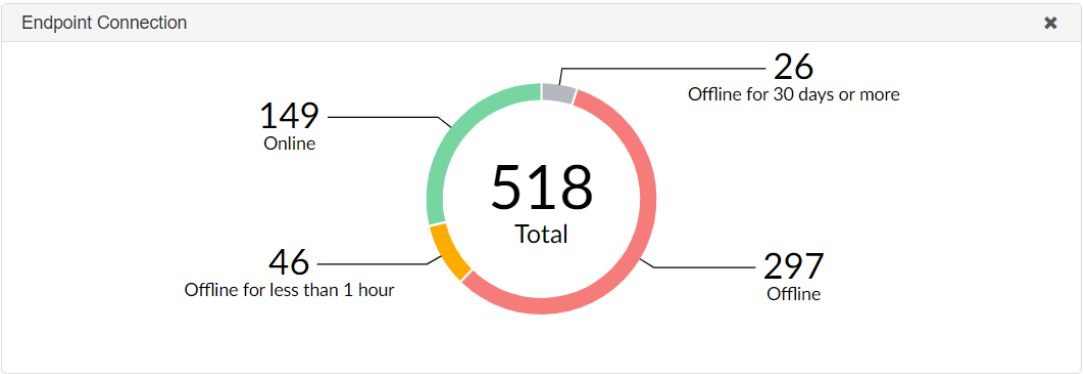
Sistema de gestión y correlación de eventos de seguridad FortiSIEM. Una solución que nos permite centralizar los eventos de seguridad de las diferentes plataformas tecnológicas, brindando visibilidad del ciberespacio y facilitando la detección y respuesta a incidentes cibernéticos.



Sistema de analíticas y capacidades y automatización FortiAnalyzer. Nos permite generar reportes a sobre la situación de la ciberseguridad a partir de las analíticas con las que cuenta la solución.




Solución de protección para los equipos laptops Forticlient. Una herramienta que nos permite administrar, monitorear, aprovisionar, aplicar parches de seguridad, poner en cuarentena, categorizar dinámicamente y proporcionar una visibilidad profunda de las laptops en tiempo real.

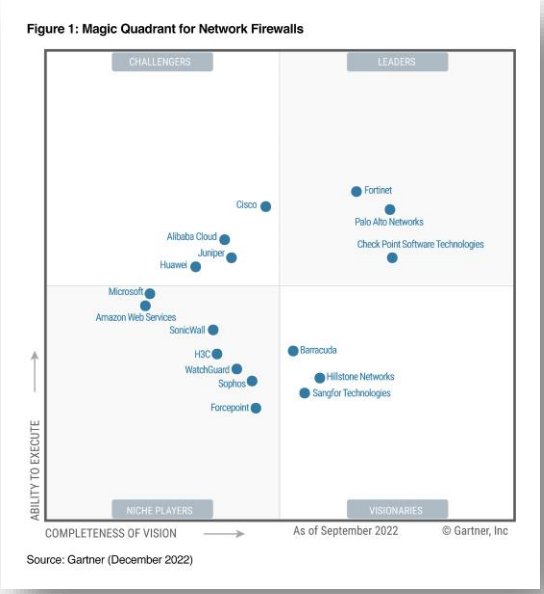



Redes inalámbricas seguras. El uso de redes inalámbricas seguras es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información. Durante el año 2021 fueron implementados 50 FortiAP modelo FAP-421E en el Edificio Suprema Corte de Justicia, el Palacio de Justica de Santiago de los Caballeros y en el Palacio de Justica de la Vega.

## 3. Justificación técnica

Actualmente contamos con soluciones de ciberseguridad de Fortinet que nos ayudan a mitigar los riesgos asociados con la seguridad de la información y las redes de comunicación en general, y a su vez, se encuentran aplicando controles de seguridad que nos brindan la visibilidad necesaria para actuar de manera proactiva ante situaciones que pudieran comprometer a la institución.

El Cuadrante Mágico de Gartner para cortafuegos de red reconoció como líder por treceava vez a la empresa Fortinet, destacada por sus soluciones de ciberseguridad.




Fortinet también ha sido seleccionado por cuarta vez consecutiva como líder por su solución de SD-WAN, una arquitectura de red que utiliza software para controlar el tráfico de red a través de una variedad de enlaces de transporte, como Internet, esto permite a las empresas aprovechar las ventajas de cada enlace, como el rendimiento y la seguridad, para crear una WAN más eficiente y rentable.

Figure 1: Magic Quadrant for SD-WAN


Source: Gartner (September 2023)

Es importante destacar, que en este momento el Poder Judicial en su centro de datos principal, así como en sus sedes, tiene estos equipos soportando los siguientes servicios:

a) Acceso directo a través de enlaces seguros a la plataforma Servicio Judicial que esta alojada en la nube de Microsoft.
b) Publicación de correo electrónico.
c) Publicación de aplicaciones institucionales.
d) Red desmilitarizada.
e) Acceso a internet protegido a través del uso de antivirus, sistema de prevención de intrusos, filtrado web basado.
f) Acceso remoto a las facilidades de la institución a través de redes privadas virtuales (VPN), facilitando el teletrabajo y la asistencia técnica de los especialistas.

Así mismo, como parte del plan de implementación del Sistema de Gestión de Casos, durante este año 2024, en las siguientes localidades se estarán realizando adecuaciones en las redes de comunicaciones, los servicios de acceso a internet e incorporando controles de seguridad:

| No. | Modelo | Localidad | Región |
|---|---|---|---|
| 1 | FortiGate 40F | Palacio de Justica de Jarabacoa | Norte |
| 2 | FortiGate 40F | Edif. Palacio de Justicia de Constanza | Norte |
| 3 | FortiGate 40F | Edif. Tribunal niños, niñas y adolescentes de Cotuí | Norte |
| 4 | FortiGate 40F | Edif. Tribunal niños, niñas y adolescentes de SFM | Norte |
| 5 | FortiGate 40F | Palacio de Justica de Bahoruco | Norte |

| | | | |
|---|---|---|---|
| 6 | FortiGate 40F | Palacio de Justica de Independencia (Jimani) | Sur |
| 8 | FortiGate 40F | Palacio de Justica Dajabón | Sur |
| 9 | FortiGate 40F | Edif. Juzgado de Primera Instancia de Hato Mayor | Este |
| 10 | FortiGate 40F | Palacio de Justica de Azua | Sur |
| 11 | FortiGate 40F | Palacio de Justica de María Trinidad Sánchez (Nagua) | Norte |
| 12 | FortiGate 40F | San Pedro de Macorís | Este |
| 13 | FortiGate 40F | Palacio de Justica de Peravia | Sur |
| 14 | FortiGate 40F | Palacio de Justica de Samaná | Este |
| 15 | FortiGate 40F | Palacio de Justica de Santiago Rodriguez | Norte |
| 16 | FortiGate 40F | Palacio de Justica del Seibo | Este |
| 17 | FortiGate 40F | Palacio de Justica de Valverde | Norte |
| 18 | FortiGate 40F | Palacio de Justicia para Asuntos de Familia | Distrito Nacional |
| 19 | FortiGate 40F | Edificio de la Corte de trabajo del Distrito Nacional | Distrito Nacional |
| 20 | FortiGate 40F | Juzgado especial de Transito del Distrito Nacional | Distrito Nacional |

En este sentido, nuestros especialistas han sido entrenados y certificados como expertos en la gestión de estas soluciones y han estado desarrollando las destrezas necesarias para la gestión de estas, apoyando el resguardo de toda la infraestructura tecnológica.

Por las razones antes descritas solicitamos la adquisición de los equipos de seguridad perimetral y los servicios de suscripción para los puntos de acceso a redes inalámbricas seguras descritos en las especificaciones técnicas. Emitimos este informe para sus consideraciones.

## 4. Recomendaciones

La recomendación técnica es que se proceda de inmediato con la adquisición de las licencias y equipos Fortinet a través de un proceso de excepción por exclusividad alineado con los procesos institucionales correspondientes, dando participación a los representantes oficiales de Fortinet en la República Dominicana. Con esto protegemos las operaciones y mitigamos el riesgo de cualquier intrusión de Ciber atacantes, tomando en cuenta que:

1) Poseemos un producto de ciberseguridad reconocido internacionalmente que ha dado los resultados esperados por la Institución.
2) El personal que constituye el soporte técnico ya posee el conocimiento de manejo de esta herramienta.
3) Constituye un ahorro en el costo de implementación ya que el mismo se encuentra instalado en nuestra plataforma tecnológica.

Este documento sustituye, deroga y deja sin efecto cualquier otro relativo al informe de justificación para la adquisición de equipos de ciberseguridad.

Equipo de peritos:

**Luis Vargas**
Analista de Seguridad y Monitoreo TIC

**Adderli de la Rosa**
Coordinador de Seguridad de Infraestructura

**Emmanuel E. Tejada**
Gerente de Seguridad y Monitoreo TIC

Revisado por:

**Welvis Beltrán**
Director de TIC