INFORME TÉCNICO N° JCTIC-013-2025

ESTANDARIZACION DE LA PROTECCIÓN PERIMETRAL TI (NGFW) Y DE LA PROTECCION DE USUARIO FINAL ENDPOINT (XDR) EN LA INFRAESTRUCTURA CRÍTICA DEL GRUPO DISTRILUZ

01 de abril de 2025

1. OBJETIVO

Estandarizar la Protección Perimetral TI (NGFW) y de la Protección de Usuario Final (Endpoint XDR) en la infraestructura crítica del Grupo Distriluz (Electronoroeste S.A., Electronorte S.A., Hidrandina S.A., Electrocentro S.A.).

2. ANTECEDENTES

En 2021, las empresas del Grupo Distriluz adquirieron e implementaron 10 Firewalls de Nueva Generación (NGFW) con sus respectivas funcionalidades (Software), y 2112 licencias Cortex XDR (Software) para las estaciones de trabajo y consolas de gestión, de la marca Palo Alto Networks.

De acuerdo con el ISO 27001, las redes deben ser gestionadas y controladas para proteger los sistemas de información (A.13.1.1). En Distriluz, este control se cumple mediante la implementación de los Firewalls de Nueva Generación (NGFW) de la marca Palo Alto, los cuales permiten segmentar las redes y filtrar el tráfico (IPS/IDS) para evitar intrusiones a los sistemas de información.

Otro control relevante (A.13.2.1) Políticas de transferencia de información, el cual requiere establecer controles para la protección de la información transferida a través de las redes. El NGFW brinda funcionalidades de inspección profunda (DPI) para bloquear exfiltración de datos.

Así mismo el ISO 27001, establece un control clave para la protección contra malware (A.8.1.3). el cual requiere implementar controles para detectar y prevenir malware en los Endpoint. En el marco de la ISO27001, un Endpoint (Dispositivo) se refiere a cualquier dispositivo terminal que interactúa con la red corporativa y almacena, procesa o transmite información. Estos dispositivos son críticos para la seguridad de la información, ya que son blancos frecuentes de ataques. La aplicación en Distriluz se realiza mediante el Cortex XDR para la detección y prevención ante Malware, Cortex XDR cumple con la detección de Ransomware en las laptops y servidores y respuesta automatizada aislando los equipos comprometidos.

Por otro lado, el control clave A.12.6.1, Gestión de Vulnerabilidades, requiere identificar y corregir vulnerabilidades en Endpoint. El Cortex XDR correlaciona vulnerabilidades con ataques activos.

La integración NGFW + XDR según ISO27001 promueve un enfoque holístico (Cláusula 6.1.2), de esta forma, si el NGFW detecta un ataque a la red (A.13.1.1), el

XDR investiga si los Endpoint están comprometidos (A.8.1.3). Esto cumple con el principio de defensa en profundidad (Múltiples capas de seguridad).

3. DESCRIPCIÓN DEL EQUIPAMIENTO PREEXISTENTE EN LAS EMPRESAS DEL GRUPO DISTRILUZ

Las empresas del Grupo Distriluz tienen implementados una solución integrada de Protección Perimetral TI con Firewalls de Nueva Generación (NGFW) y Protección de Usuario Final (Endpoint XDR) y consolas, todas de la marca Palo Alto Networks. El detalle de esta solución es el siguiente:

Hardware: Firewall de Nueva Generación (NGFW):

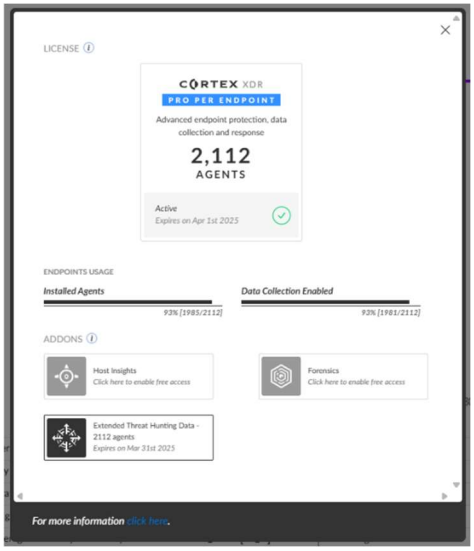
Empresas del Grupo DISTRILUZ	Cantidad NGFW	Total
Electronoroeste S.A.	02	2
Electronorte S.A.	02	2
Hidrandina S.A.	04	4
Electrocentro S.A.	02	2
TOTAL	**10**	**10**

Software: Licencias instaladas en el NGFW:

FUNCIONALIDAD	DEFINICION
Prevención de Amenazas	Conjunto de tecnologías integradas en los firewalls Palo Alto NGFW para **detectar y bloquear amenazas** en tiempo real, como malware, exploits, ataques de red y comandos C2 (Command & Control).
URL	Dirección web que los usuarios ingresan para acceder a sitios de Internet. Palo Alto NGFW incluye capacidades para **filtrar y categorizar URLs** basadas en riesgos (ej.: phishing, malware, sitios no productivos).
Asistencia Técnica	Servicio ofrecido por Palo Alto Networks para resolver problemas técnicos, actualizar configuraciones y optimizar la operación de sus firewalls NGFW y soluciones Cortex.
WildFire	Plataforma de **análisis de malware basada en sandboxing** (entorno controlado) que detecta amenazas desconocidas (*zero-day*) en archivos y URLs.
Cortex Data Lake	Repositorio centralizado en la nube donde Palo Alto almacena **logs y datos de seguridad** de firewalls NGFW, Cortex XDR y otras soluciones.
Seguridad de DNS	Protección contra amenazas que usan el protocolo DNS (ej.: dominios maliciosos para robo de datos o conexiones C2).
SD-WAN	Tecnología que optimiza la conectividad entre sucursales usando múltiples enlaces (ej.: Internet, MPLS) con base en políticas de seguridad y rendimiento.
Filtrado de URL Avanzado	Va más allá del bloqueo básico de URLs, usando **machine learning** para categorizar sitios en tiempo real y detectar dominios maliciosos nuevos.
Advanced Threat Prevention	Conjunto de tecnologías para detener amenazas avanzadas, como: • **Evasión de sandboxing** (malware que detecta entornos de análisis). • **Ataques sin archivos** (*fileless attacks*).
Consola Panorama	Es la plataforma de **gestión unificada** de Palo Alto Networks que permite administrar, monitorear y configurar múltiples firewalls NGFW (Physical, VM-Series) y servicios de seguridad (Cortex XDR, Cloud, SD-WAN) **desde una única consola**.

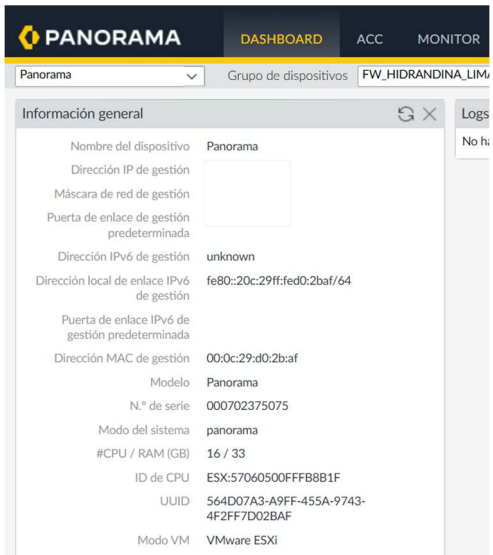
Las características de la aplicación Cortex XDR se describen a continuación:

Especificación	Detalle
Modelo	Cortex XDR pro per Endpoint
Licencias (Agentes)	2,112 licencias
Fabricante	Palo Alto Networks
Plataforma	Windows
Idioma	Inglés/español



Las licencias del Cortex XDR están instalados en las laptops, notebooks y computadores personales y los servidores de Distriluz.

Características técnicas de la consola de gestión de los NGFW:



4. DESCRIPCIÓN DE LA SOLUCION - MARCA PALO ALTO NETWORKS

Las empresas del Grupo Distriluz están comprometidas con la innovación tecnológica y la mejora continua de sus servicios, alineándose con el Objetivo Estratégico Institucional 8: "Implementar proyectos de modernización y transformación digital".

En cumplimiento de la norma ISO27001, las empresas requieren proteger sus activos de información, brindando protección perimetral y de Endpoint.

Considerando este contexto, se hace necesario estandarizar la solución compuesta por la Protección Perimetral TI (NGFW) y de la Protección de Usuario Final (Endpoint XDR) de la marca Palo Alto Networks, a fin de garantizar la continuidad operativa durante el tiempo de vida útil de los equipos (Hardware) prevista en siete (07) años, y continuar con el mantenimiento, capacitación, soporte técnico preventivo y correctivo y adquisición (Hardware y Software), fortaleciendo así, la capacidad de las empresas del Grupo Distriluz para ofrecer servicios eléctricos de calidad y cumplir con los estándares regulatorios vigentes.

5. USO O APLICACIÓN QUE SE LE DARÁ PROTECCIÓN PERIMETRAL TI (NGFW) Y DE LA PROTECCIÓN DE USUARIO FINAL (ENDPOINT XDR)

La solución compuesta por la Protección Perimetral TI (NGFW) y de la Protección de Usuario Final (Endpoint XDR) de la marca Palo Alto Networks, permitirá a las empresas del Grupo Distriluz proteger los activos de información de manera oportuna basadas en datos confiables y actualizados, optimizando así la eficiencia operativa y cumpliendo los controles de la norma ISO 27001. La estandarización permitirá además la actualización, servicios de soporte técnico, mantenimiento y capacitación asociados, garantizando su funcionalidad continua y su óptimo desempeño en el tiempo.

6. JUSTIFICACIÓN DE LA PROTECCION

La Protección Perimetral TI (NGFW) y de la Protección de Usuario Final (Endpoint XDR) se justifica por su capacidad integrada para proteger los activos de información del Grupo Distriluz. Sus módulos permiten proteger el perímetro de la red corporativa de Distriluz separando Internet y la Extranet de la red Interna.

A continuación, se acredita el cumplimiento de los presupuestos que deben verificarse, a efecto que la estandarización sea procedente, de acuerdo con lo que establece en la Directiva Nº004-2016-0SCE/CD, aprobada por la Resolución N° 011-2016-OSCE-PRE:

a. La entidad posee determinado equipamiento o infraestructura pudiendo ser maquinarias, equipos, vehículos, u otros tipos de bienes, así como ciertos servicios especializados.

Al respecto, se debe tener presente que las empresas del Grupo Distriluz han adquirido 10 Firewalls de Nueva Generación (NGFW) con sus respectivas funcionalidades (Software), 2112 licencias Cortex XDR (Software) y consolas de gestión, del fabricante Palo Alto Networks, lo que confirma la existencia previa del bien, según lo establecido en el numeral 3 del presente documento. El Cortex XDR está instalado en cada uno de los Endpoint tales como Laptops, Computadoras Personales y Servidores de Distriluz.

b. Los bienes o servicios que se requiere contratar son accesorios o complementarios al equipamiento o infraestructura preexistente, e imprescindibles para garantizar la funcionalidad, operatividad o valor económico de dicho equipamiento o infraestructura.

Sobre este presupuesto, se debe señalar:

i. Estos bienes y servicios son esenciales para asegurar la protección en el perímetro de la red corporativa y los Endpoint. Actualmente, el grupo Distriluz

ha adquirido 10 equipos Firewall (NGFW) y 2112 licencias de protección de usuario final con sus respectivas consolas, todas ellas completamente instaladas y funcionando óptimamente. Además, el personal técnico de soporte de Distriluz ha recibido la capacitación correspondiente para brindar el soporte técnico preventivo y correctivo.

ii. Los servicios asociados a la Protección Perimetral TI (NGFW) y de la Protección de Usuario Final (Endpoint XDR), son los siguientes: servicio de soporte técnico postventa (Preventivo y correctivo) con reemplazo de partes, Servicio de monitoreo y gestión del Firewall y XDR, Servicios de mantenimiento y capacitación.

iii. La actualización del software de Protección Perimetral TI (NGFW) y de la Protección de Usuario Final (Endpoint XDR) garantiza que las licencias existentes mantengan su valor y funcionalidad, asegurando que el sistema esté siempre operativo, optimizado y seguro.

iv. Los beneficios económicos de la Protección Perimetral TI (NGFW) y la protección de usuario final (XDR), han sido identificados dentro de un horizonte de siete años de vida útil. Por esa razón, no sería posible el reemplazo por otra marca. Por otro lado, la preexistencia ha reducido la curva de aprendizaje, se han establecido procesos y procedimientos para la respuesta de incidentes y alertas de seguridad. Cambiar a otra marca, implicaría mayor inversión y costos adicionales a la empresa.

7. VIGENCIA

El periodo de vigencia del proceso de estandarización deberá ser por el plazo de cinco (05) años, contados a partir de la fecha de firma de la Resolución de Gerencia General que apruebe esta propuesta. El tiempo de vigencia se justifica en la importancia de mantener la estabilidad de la infraestructura que respalda los procesos de lectura de medidores y otras operaciones complementarias.

8. EXCEPCIÓN DE VIGENCIA

Sin perjuicio de lo indicado en el punto anterior, el plazo de vigencia será menor en caso varíen las condiciones que hoy justifican la estandarización (por ejemplo, cambios en el entorno tecnológico y costos).

9. CONCLUSIONES.

- Se requiere estandarizar a la marca Palo Alto Networks, para la Protección Perimetral TI (NGFW) y la Protección de Usuario Final (Endpoint XDR) en la infraestructura crítica del Grupo Distriluz (Electronoroeste S.A., Electronorte S.A., Hidrandina S.A., Electrocentro S.A.).
- La estandarización de la Protección Perimetral TI (NGFW) y la Protección de Usuario Final (Endpoint XDR) es fundamental para contratar servicios de soporte técnico postventa (Preventivo y correctivo) con reemplazo de partes, Servicio de monitoreo y gestión del Firewall y XDR, Servicios de mantenimiento y capacitación.

- La preexistencia de 10 licencias de Firewall NGFW y 2,112 licencias de software de Cortex XDR garantiza una transición fluida hacia la estandarización y optimiza la seguridad y accesibilidad de los datos gestionados.

- Se está cumpliendo con los presupuestos para la estandarización que se mencionan en la Directiva Nº004-2016-0SCE/CD, aprobada por la Resolución N° 011-2016-OSCE-PRE.

- El Anexo A.17.1.1 de la NTP ISO/IEC 27001 resalta la importancia de la planificación para garantizar la continuidad de la seguridad de la información en situaciones adversas. Establecer requisitos claros y anticipar posibles crisis permite minimizar el impacto de interrupciones y proteger los activos de información. En el caso del Grupo Distriluz, una planificación efectiva fortalece su resiliencia y le permite responder adecuadamente ante desastres o incidentes de seguridad.

10. RESPONSABLES DE LA EVALUACIÓN

Carlos Cueva Vivas - Jefe TIC - ENOSA
Miguel Fuentes Díaz - Jefe TIC - ENSA
Henry Arreategui Cruz - Jefe TIC (e) - HIDRANDINA
Karina Laura León - Jefe TIC – ELECTROCENTRO

JEFE DEL AREA USUARIA

Roberto Díaz Leiva - Jefe Corporativo TIC (e) - DISTRILUZ

Firmado digitalmente por CUEVA VIVAS Carlos Alberto FAU 20102708394 soft
Fecha: 2025.04.10 17:50:51 -05'00'

Carlos Cueva Vivas
Jefe TIC - ENOSA

Firmado digitalmente por LAURA LEON Karina Sandy FAU 20129646099 soft
Fecha: 2025.04.10 16:45:15 -05'00'

Karina Laura León
Jefe TIC - ELECTROCENTRO

Firmado digitalmente por FUENTES DIAZ Miguel Angel FAU 20103117560 hard
Fecha: 2025.04.10 16:50:42 -05'00'

Miguel Fuentes Díaz
Jefe TIC - ENOSA

ARREATEGUI CRUZ Henry Wilberto FAU 20132023540 soft
Firmado digitalmente por ARREATEGUI CRUZ Henry Wilberto FAU 20132023540 soft
Fecha: 2025.04.10 17:01:24 -05'00'

Henry Arreátegui Cruz
Jefe TIC (e) - HIDRANDINA

DIAZ LEIVA Roberto Carlos FAU 20132023540 soft
x JCTIC (e)
2025.04.10 17:54:53 -05'00'

Roberto Diaz Leiva
Jefe Corporativo TIC (e)