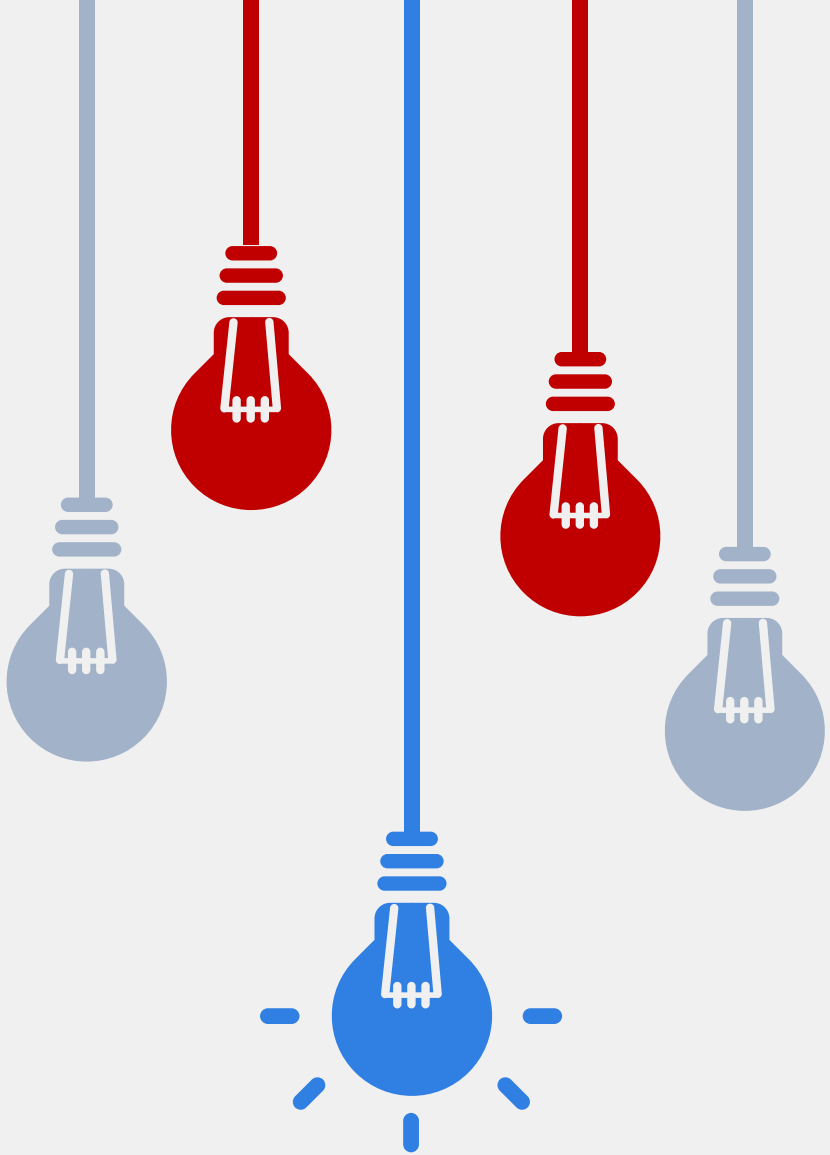
Tendencias de Ciberseguridad
Resultados de Assessment

John Cardona – System Engineer
johnc@fortinet.com







Objetivo del Análisis

Estar cada vez más cerca de nuestros clientes y mejorar la experiencia con nuestra línea de soluciones basadas en AI

Brindar al cliente las recomendaciones y buenas prácticas que permitan un uso óptimo de la tecnología para su proceso de transformación digital.

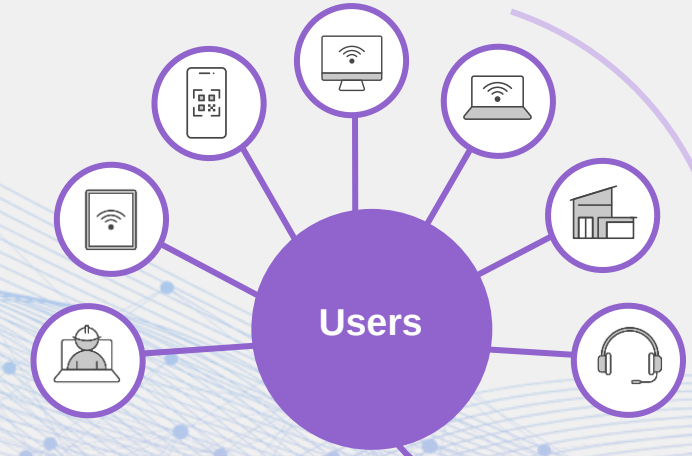
Este análisis está basado en las recomendaciones del Instituto Nacional de Normas y Tecnología (**NIST**).

Identificar las condiciones, controles y proyectos necesarios para minimizar los impactos al negocio, generados por ataques de la ciberdelincuencia a la infraestructura de TI

© Fortinet Inc. All Rights Reserved.

Tendencias

Las redes tradicionales se basan en confiar en todos y conectarlo todo!



84%

Companies are hybrid

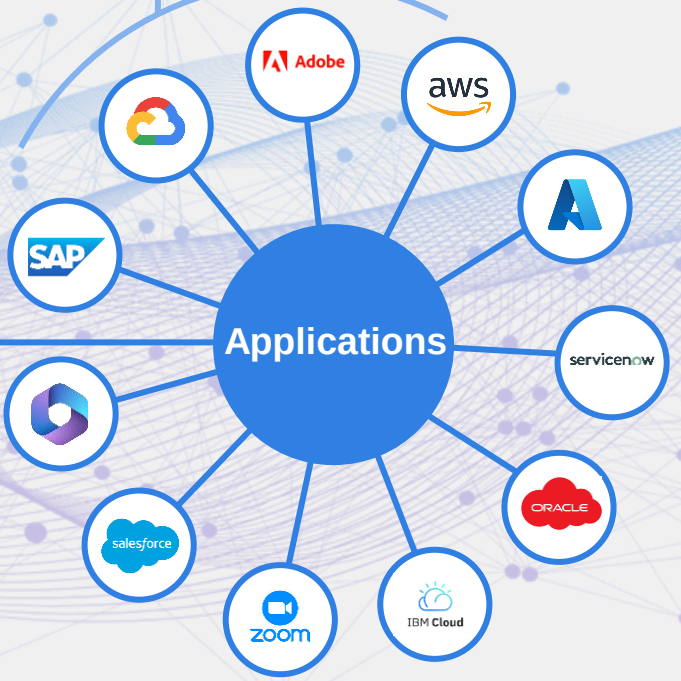
Forbes: Remote Work Statistics and Trends

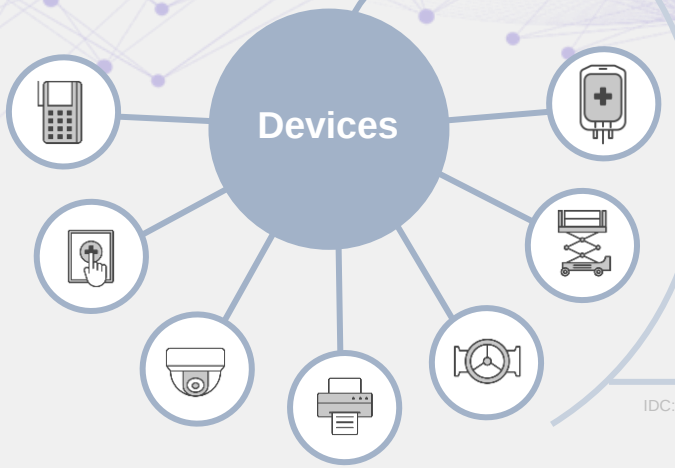
125+

Distributed applications used by enterprise

2022 Gartner: Market Guide for SaaS Management Platforms







42B

IoT devices

IDC: World-Wide IDC Forecast

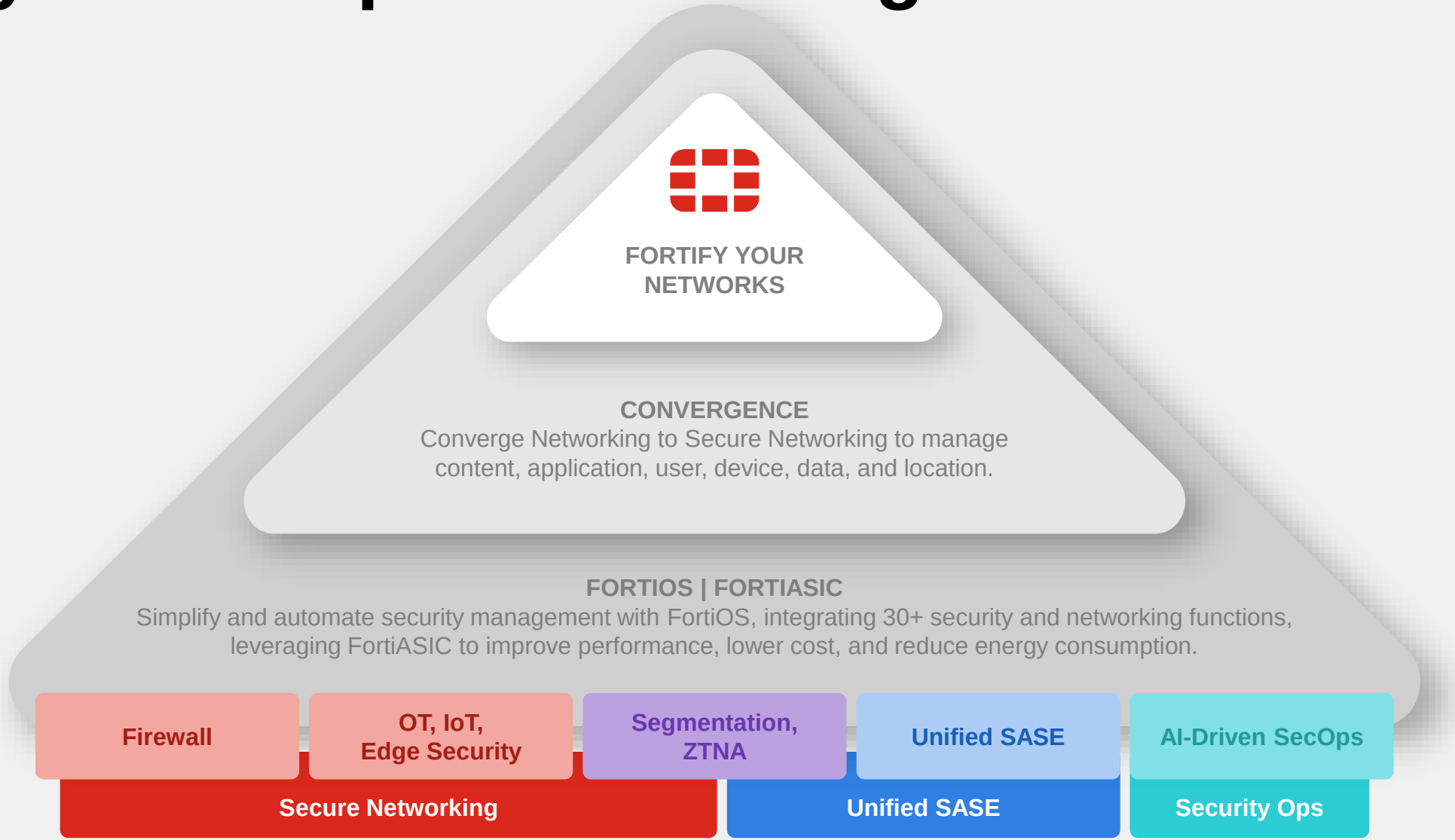
90%

Of enterprises will have experienced a security incident related to the edge network by 2026

2022 Gartner: 2022 Strategic Roadmap for Edge (IoT) Networking

© Fortinet Inc. All Rights Reserved.

Converger redes para redes seguras!



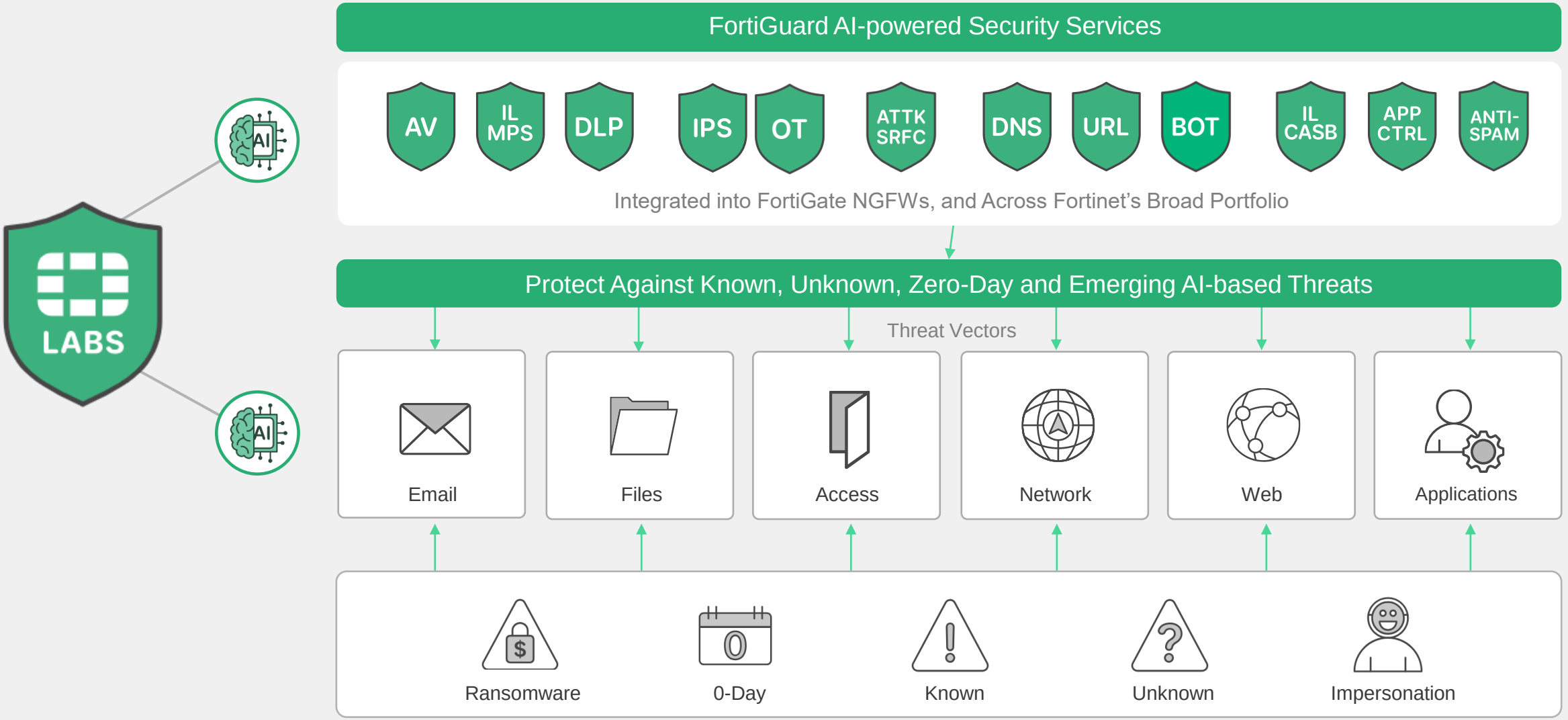
© Fortinet Inc. All Rights Reserved.

El sistema operativo de seguridad de redes más potente del mundo!



© Fortinet Inc. All Rights Reserved.

FortiGuard AI-Powered Security Services



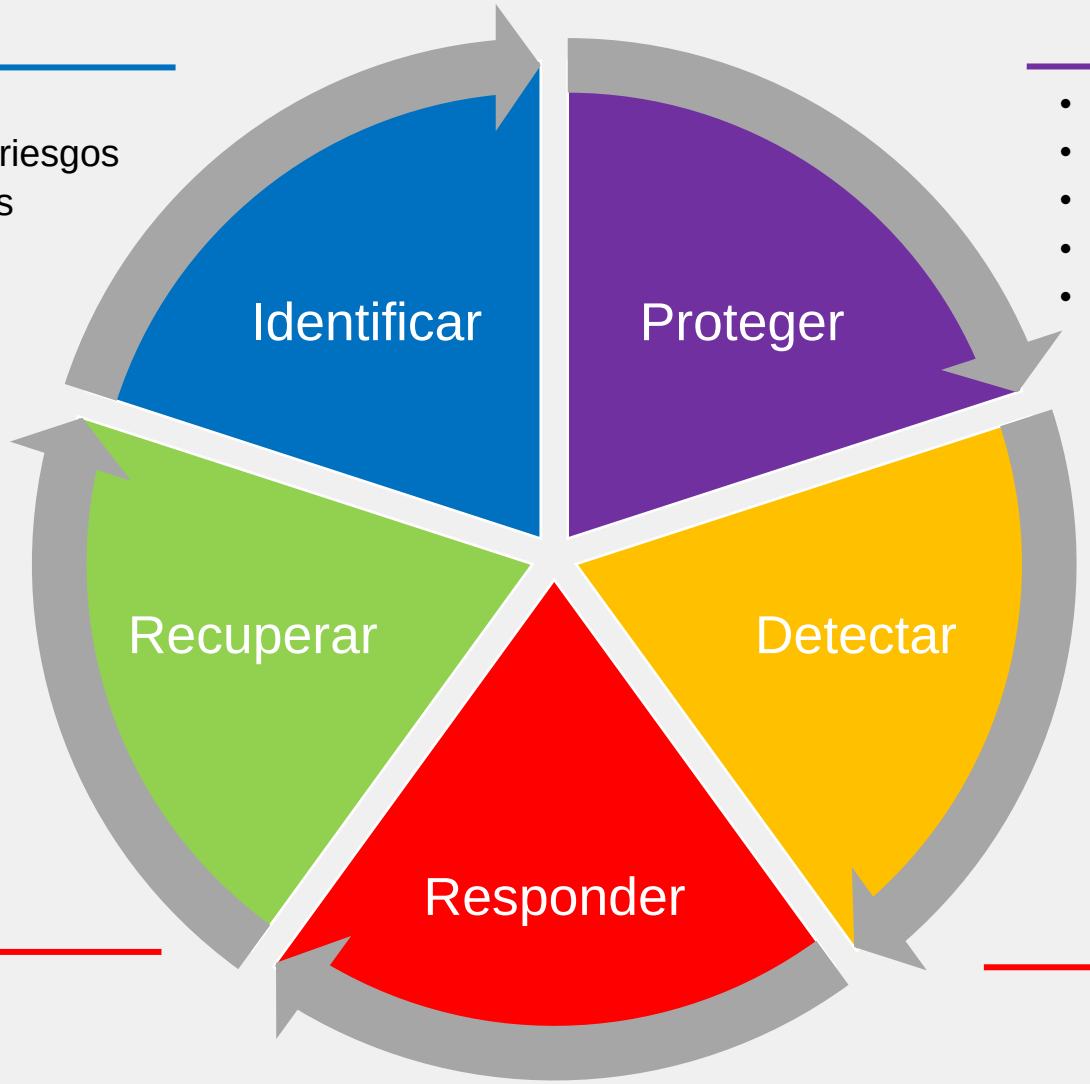
© Fortinet Inc. All Rights Reserved.

Marco de referencia

Marco de ciberseguridad NIST

- Gestión de activos
- Análisis y gestión de riesgos
- Políticas y estándares

- Control de accesos
- Entrenamiento
- Gestión de servicios
- Seguridad de datos
- Tecnologías de seguridad



- Plan de recuperación
- Backups
- Alta disponibilidad

- Gestión de eventos / Anomalías
- Monitoreo seguridad y procesos

- Plan de respuesta
- Comunicaciones
- Análisis

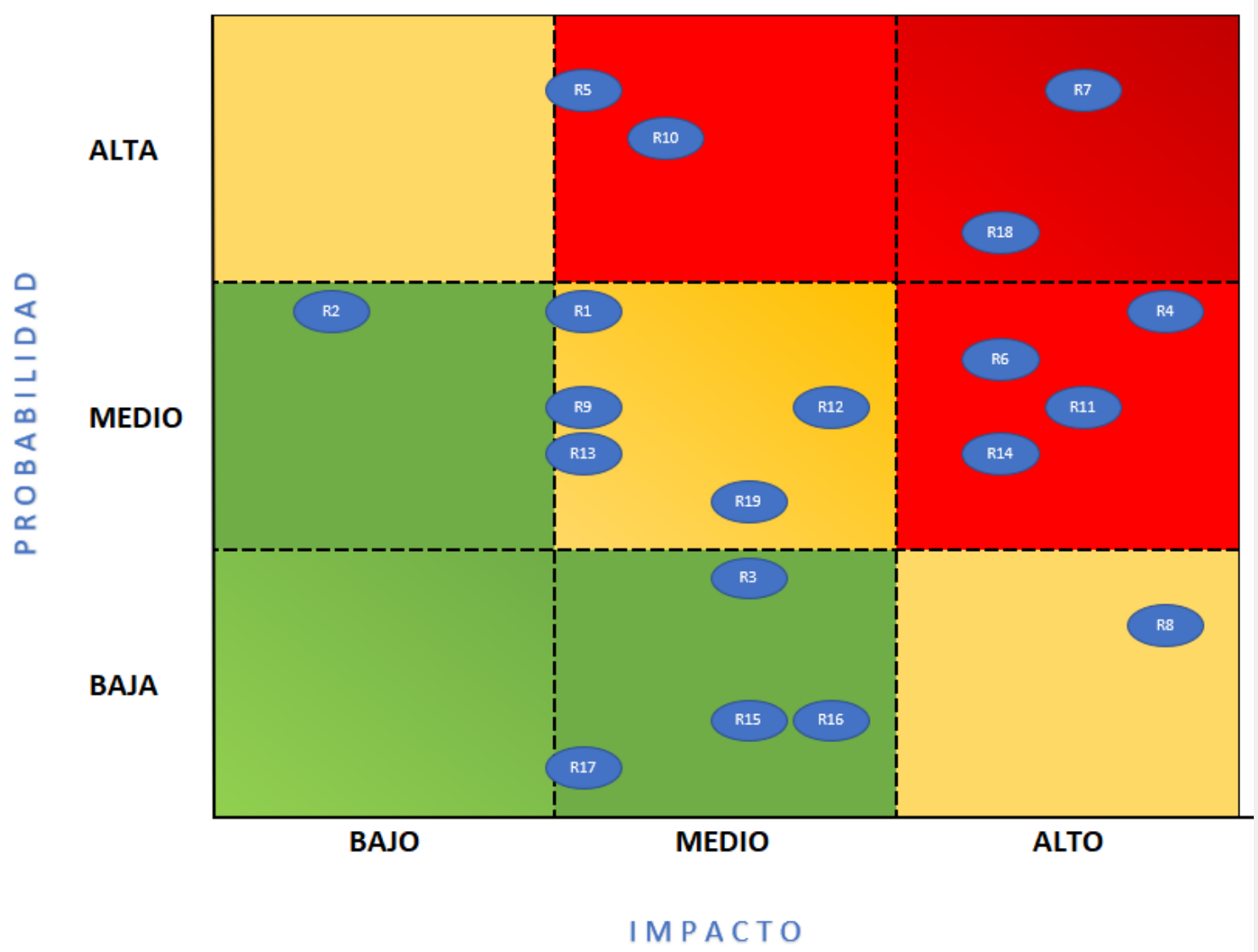
- Mitigación
- Mejoras

© Fortinet Inc. All Rights Reserved.

Marco de referencia – NIST - https://www.nist.gov/cyberframework

Gestión de Riesgos

Mapa de Riesgo Actual



ID	Tipo de Riesgos Identificados
R1	*Acceso de dispositivos No autorizados*
R2	*Instalación de Software No autorizado*
R3	*Dispositivos de Usuario Final inseguros*
R4	*Vulnerabilidades en sistemas*
R5	*Usuarios con Exceso de privilegios*
R6	*Utilización indebida de recursos tecnológicos*
R7	*Malware - Phishing en correo Electrónico*
R8	*Malware - Ataques en Aplicaciones web Internas o externas*
R9	*Malware - Secuestro de Información*
R10	*Acceso a la red de personal no autorizado*
R11	*Perdida de Información por Fallas críticas de sistemas*
R12	*Errores de Configuración en dispositivos de red*
R13	*Acceso a información crítica por canales alternos sin protección*
R14	*Fuga de Información*
R15	*Acceso a red Inalámbrica sin control*
R16	*Desconocimiento de usuarios en el manejo de ciberseguridad*
R17	*Errores de programación segura en aplicaciones*
R18	*Incidentes de Seguridad sin gestión*
R19	*Desconocimiento del estado actual de la ciberseguridad de la plataforma IT*

© Fortinet Inc. All Rights Reserved.

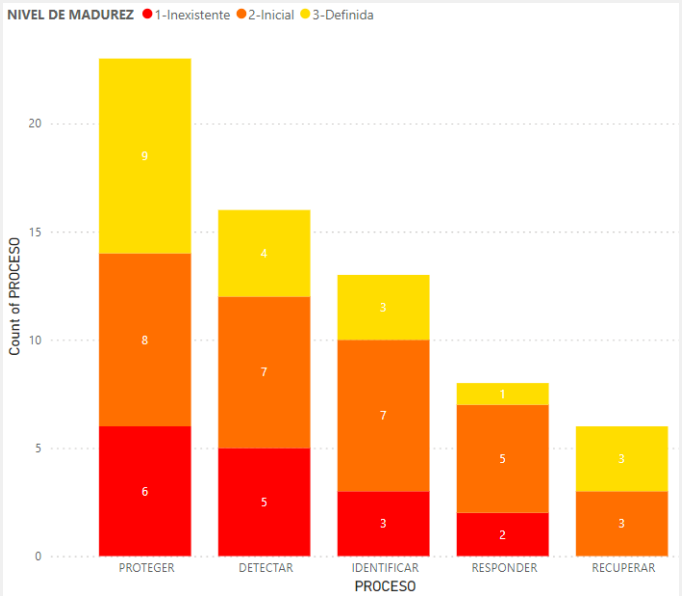
Estado General Actual

Evaluación de seguridad – Estado General



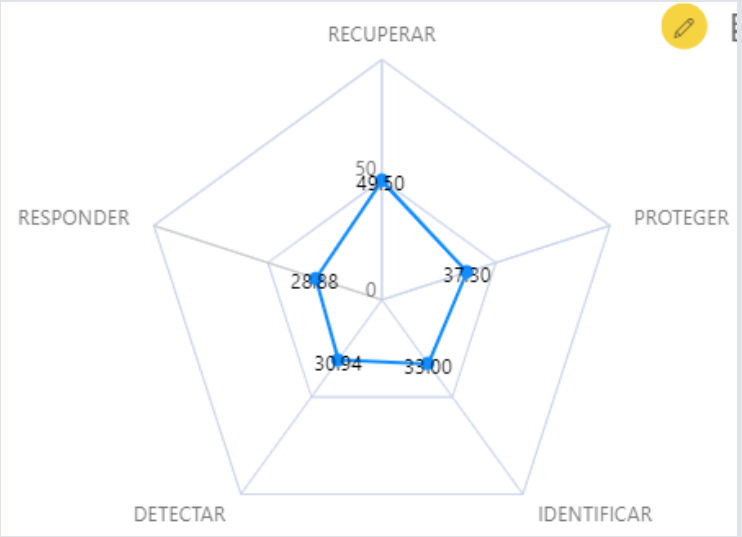
Procesos Generales NIST

Los procesos de **Proteger y Recuperar** son los más maduro, lo que significa que el cliente cuenta con múltiples controles técnicos y se encuentra implementando estrategias de **DRP**.



Nivel de madurez general

35.00% - **Medio - Bajo** basado en el análisis completo de los procesos evaluados.



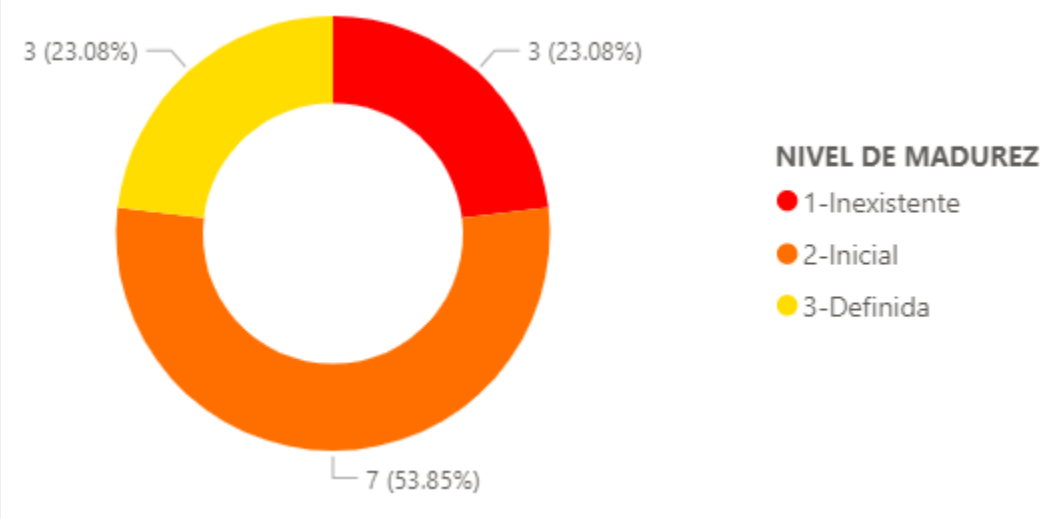
Madurez por Proceso General

Todos los procesos se encuentran cercanos a la media.

© Fortinet Inc. All Rights Reserved.

Análisis por Procesos

Proceso Identificar



Subproceso Definidos

- Gestión de activos.
- Gobierno de Aplicaciones y activos.
- Evaluación de Riesgos de Terceros.

Subproceso Inicial

- Gobierno de Roles y Responsabilidades.
- Gestión de Activos.
- Evaluación de Riesgos.

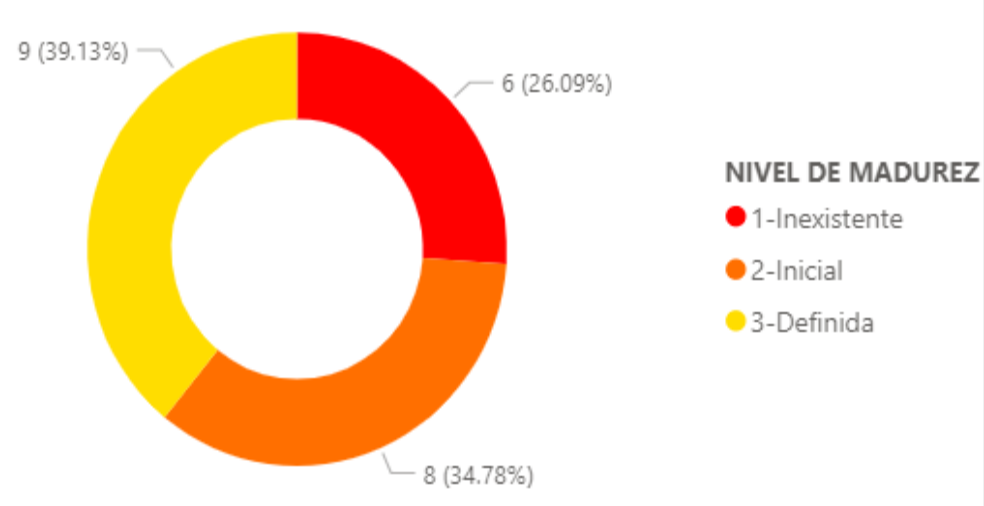
- Actualmente NO se cuenta con una estrategia de gestión y custodia de cuentas privilegiadas (PAM). Lo que permitiría a un atacante hacer uso de estas cuentas privilegiadas SIN quedar registros de responsables directos.

- Se sugiere culminar la Matriz de Roles y Responsabilidades (Incluyendo área de Seguridad), esto facilitaría la implementación de una estrategia basada en Roles.

- Buscar llevar todos los sub-procesos a un estado “Definido”, mediante el uso de herramientas que permitan automatizar las labores requeridas.

© Fortinet Inc. All Rights Reserved.

Proceso Proteger



Subprocesos Iniciales

- Capacitación.
- Tecnologías de Protección – Correo, EDR,

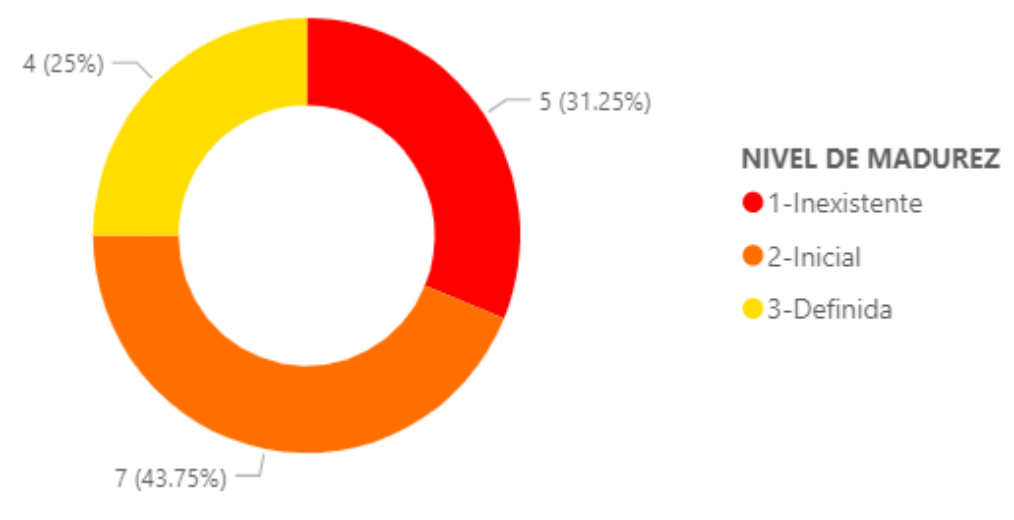
Subprocesos Inexistentes

- Control de Acceso.
- Protección de datos – Cifrado/DLP.

- No se tiene una cobertura completa de autenticación de doble factor de manera centralizada.
- Se sugiere implementar una solución de protección avanzada de correo que complemente la protección actual.
- No se realiza validación de postura de usuarios terceros (ZTNA), lo que podría permitir la propagación de ataques a través de la VPN.
- Implementación de cifrado de datos en reposo y tránsito.
- Implementación de estrategias de Segmentación de Red (SDBRANCH) complementado con estrategias de control de acceso a la red (NAC).

© Fortinet Inc. All Rights Reserved.

Proceso Detectar



Subprocesos Iniciales

- Monitoreo continuo – Salubridad y Disponibilidad.
- Procesos de Detección – Definición de política respaldada por soluciones de seguridad.

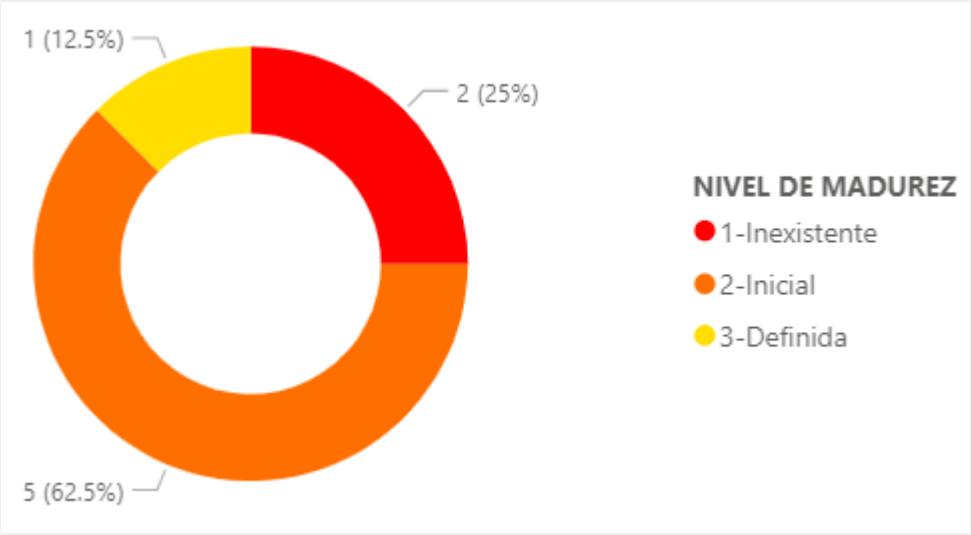
Subprocesos Inexistentes

- Monitoreo continuo – Implementación de SOC.
- Anomalías y eventos – NDR/EDR, SandBox, Deceptor.

- No se cuenta con un sistema de correlación de eventos centralizado lo que dificulta la identificación proactiva/correlacionada de eventos en un esquema 7x24.
- Hay soluciones como Firewalls de Red, WAF y servidores de archivos, los cuales se encuentran por fuera de estrategia Sandbox.
- Se recomienda utilizar soluciones que hagan uso de IA/ML (NDR) que permita realizar detección de amenazas avanzadas y permita ser integrado con la infraestructura de red actual.
- Implementar controles de tipo “Engaño/Señuelo”, que permita identificar comportamientos anómalos al interior de la red (Honeypots/Deceptor).

© Fortinet Inc. All Rights Reserved.

Proceso Responder



Subprocesos Iniciales

- Comunicaciones – En construcción.
- Análisis – SOAR, SIEM,
- Mitigación – NGSOC y BCP.

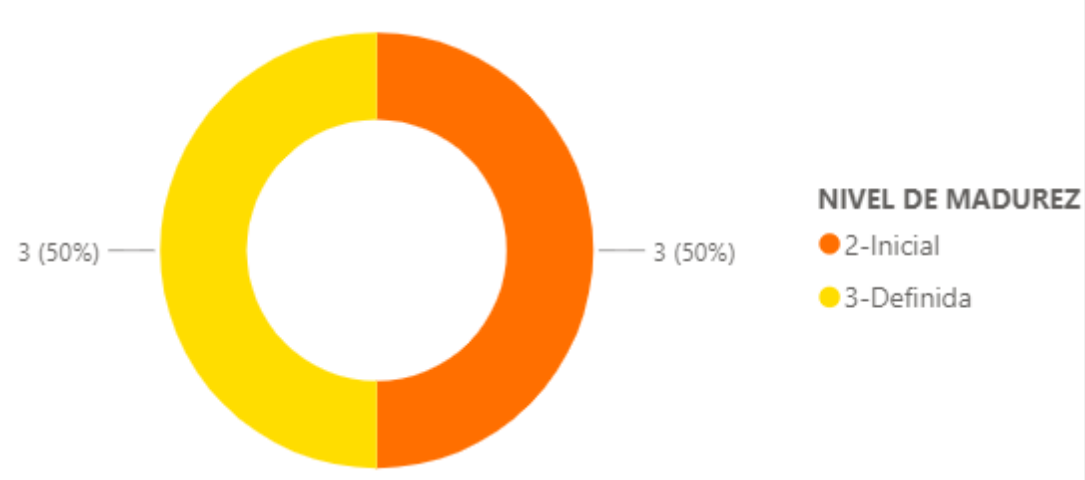
Subprocesos Inexistentes

- Análisis – EDR.
- Mitigación – CyberSecurity Mesh.

- Llevar todos los procesos a un nivel “Optimizado” mediante la implementación de soluciones tipo “Orquestación, automatización y respuesta a incidentes” (SOAR).
- Implementar una estrategia de monitoreo y correlación respaldada por un SOC/SOAR. Esto permitirá correlacionar y generar respuestas automatizadas ante eventos de seguridad.
- Definición de planes de continuidad de negocio soportados por soluciones como SDWAN, Balanceo de Carga Global o balanceo de carga entre servidores.
- Implementación de estrategias CyberSecurity Mesh (Security Fabric en Fortinet) integrando las soluciones de seguridad actual con el fin de identificar situaciones y respuestas automatizadas.

© Fortinet Inc. All Rights Reserved.

Proceso Recuperar



Subprocesos Definidos

- Comunicaciones – Plan de comunicación claro y definido.
- Mejoras – DRP Implementado.

Subprocesos Iniciales

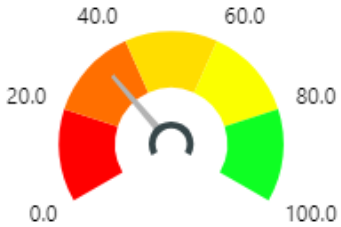
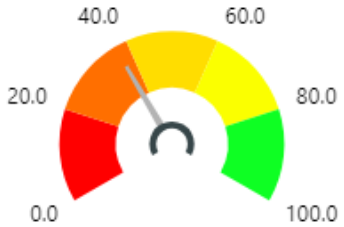
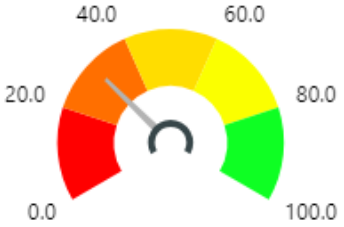
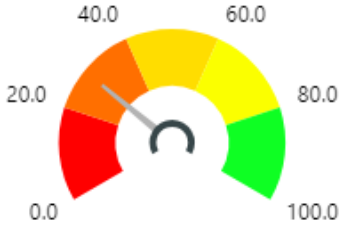
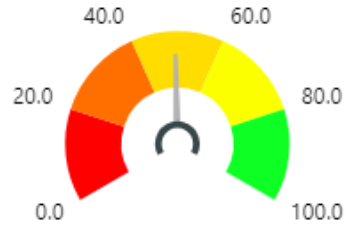
- Planificación – BD de lecciones aprendidas.
- Mejoras – Estrategias de SDWAN y aseguramiento de servicios en nube.

- Definición de una estrategia de continuidad (BCP/SDWAN) de negocio para todas las aplicaciones y servicios críticos de la Universidad.
- Documentación de estrategias de recuperación, apoyadas de validación de estas estrategias (Mínimo 1 vez al año) con sus respectivas base de datos de lecciones aprendidas y debidas actualizaciones.

© Fortinet Inc. All Rights Reserved.

Controles de Apoyo

Madurez actual de los procesos

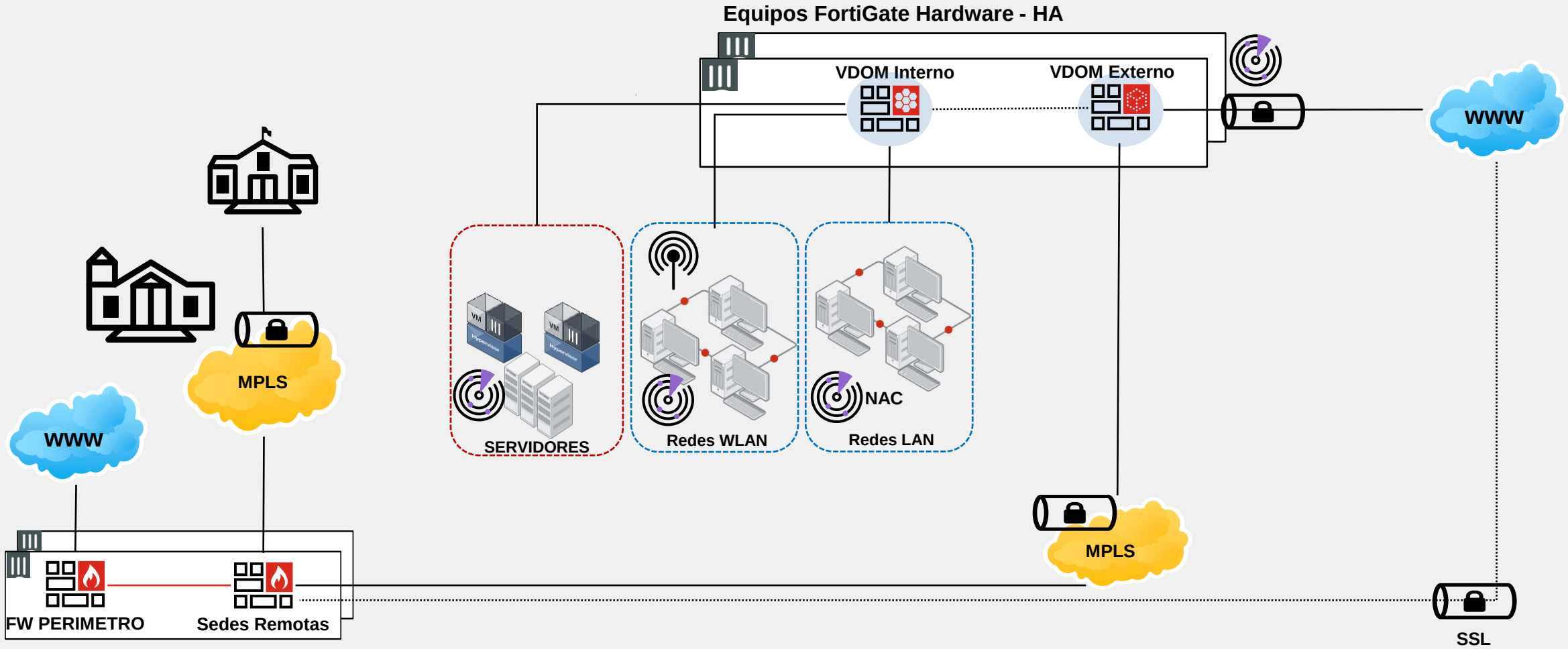
CALIFICACION IDENTIFICAR	CALIFICACION PROTEGER	CALIFICACION DETECTAR	CALIFICACION RESPONDER	CALIFICACION RECUPERAR
				
Identificar	**Proteger**	**Detectar**	**Responder**	**Recuperar**
FortiEDR NAC FortiAuthenticator FortiToken FortiSIEM Playbooks	2FA NAC FortiEDR LAN-Edge CRED Gestión de Identidades IAM MAIL	Sandbox FortiEDR Correlación y Analítica FortiSIEM Playbooks	LAN-Edge FortiSOAR Micro segmentación Correlación y Analítica	Plan de Comunicaciones Automatización Contención

© Fortinet Inc. All Rights Reserved.

¡Arquitecturas de Seguridad Propuestas!

Plan de Mejora Identificación y Protección

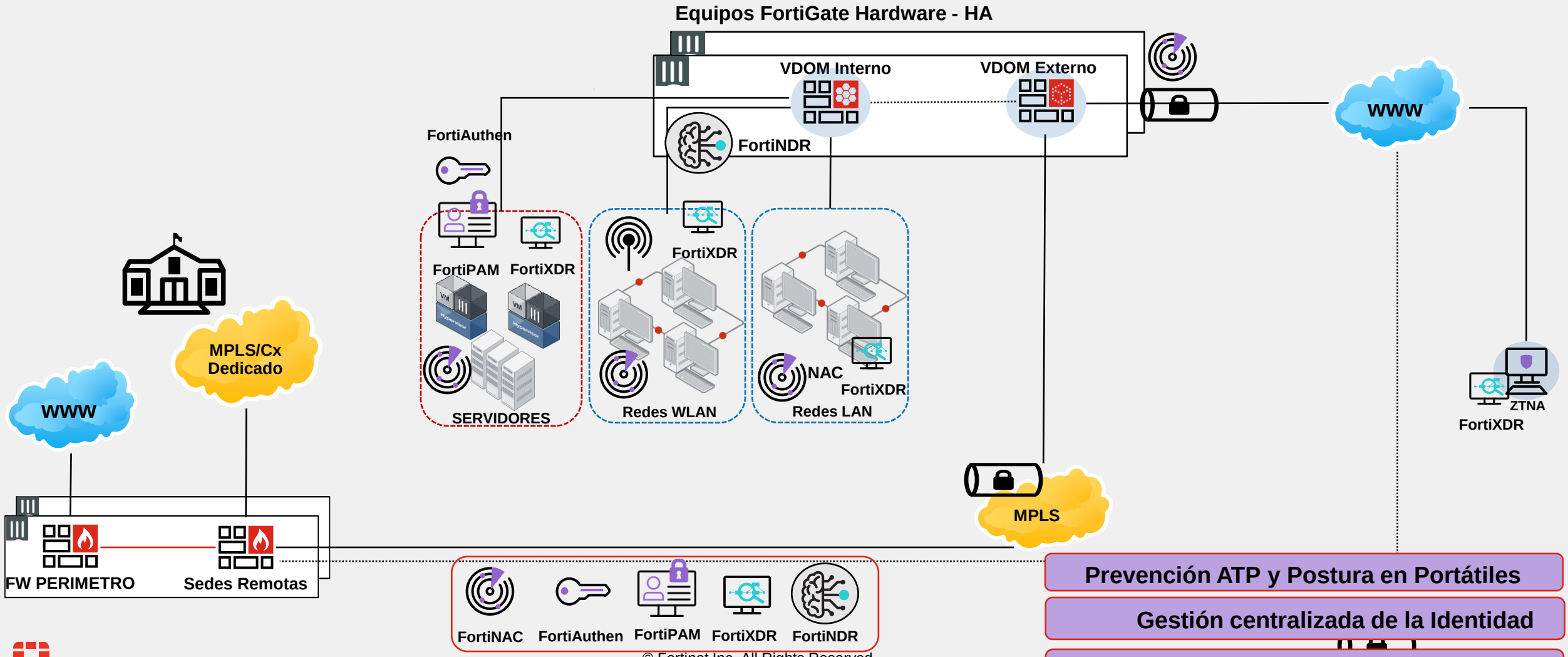
Segmentación de red con Control de Acceso



© Fortinet Inc. All Rights Reserved.

Plan de Mejora Identificación, Protección, Detección y Respuesta

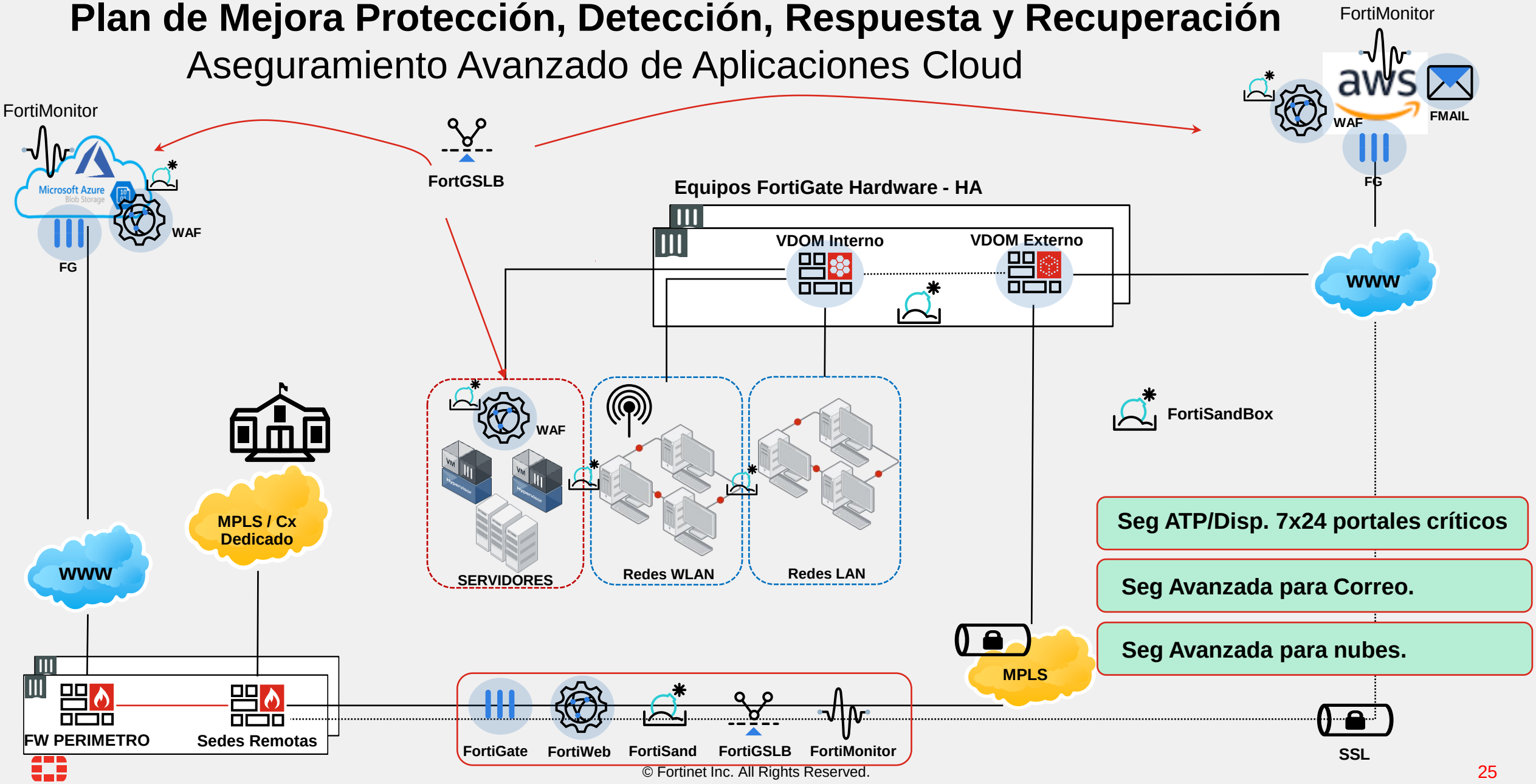
Aseguramiento Avanzado de Punto Final y control de acceso.



© Fortinet Inc. All Rights Reserved.

Plan de Mejora Protección, Detección, Respuesta y Recuperación

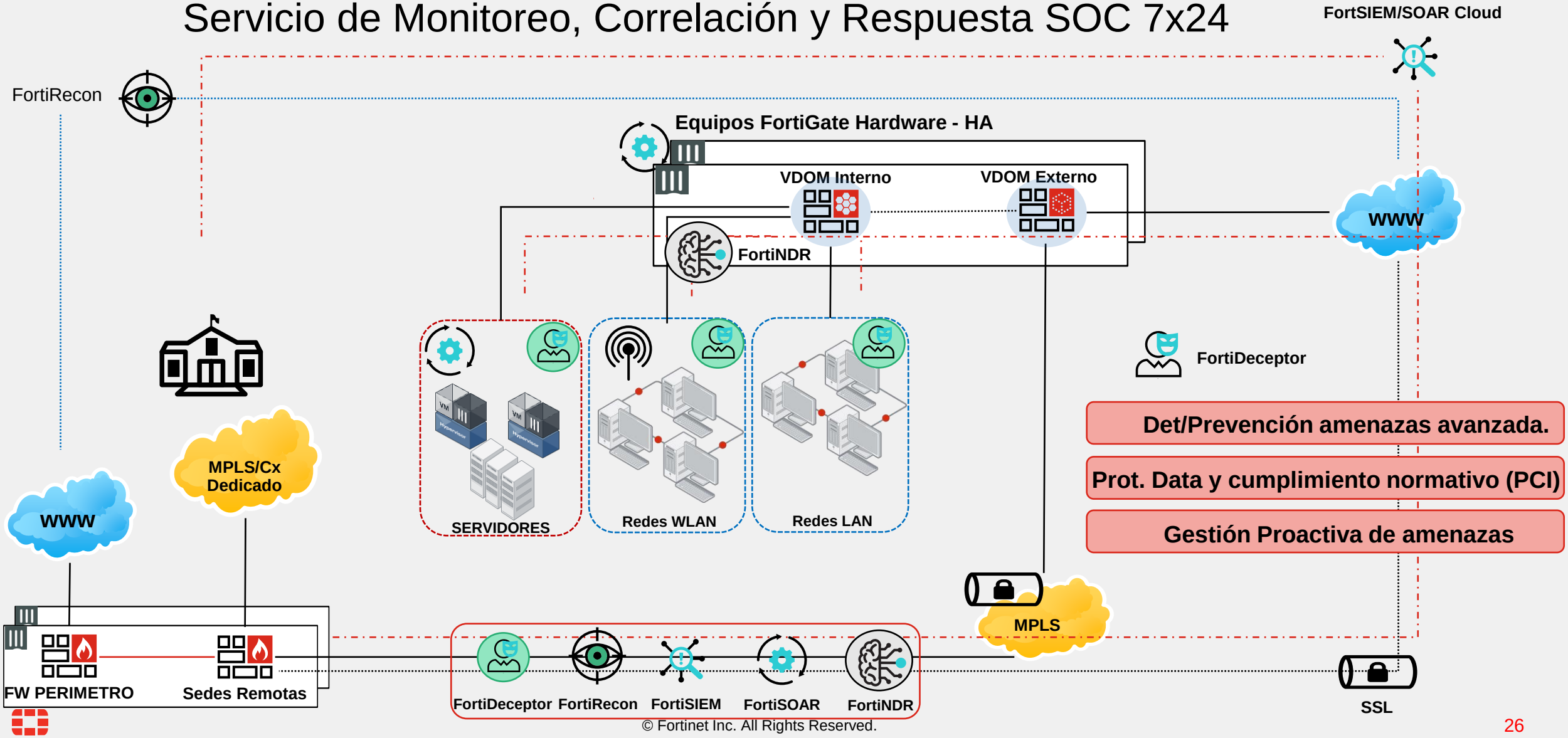
Aseguramiento Avanzado de Aplicaciones Cloud



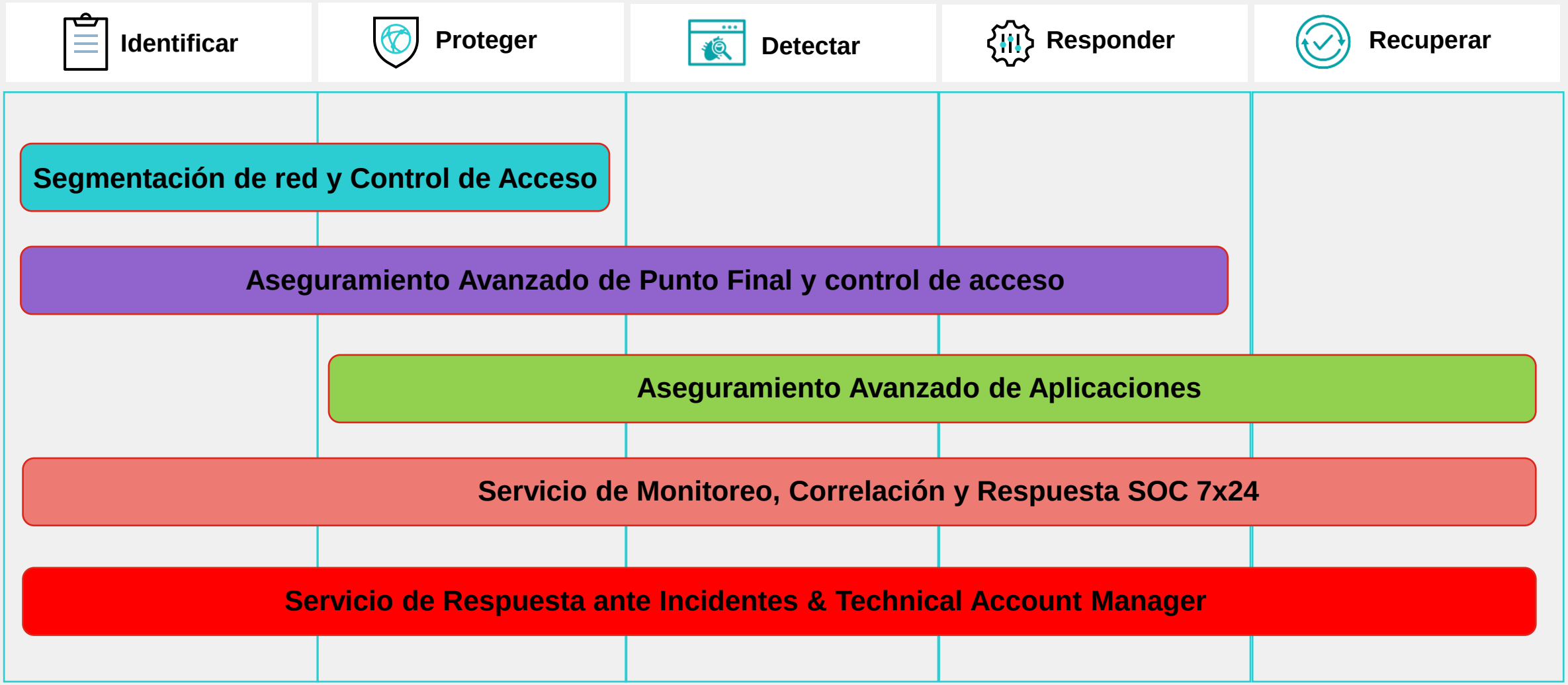
© Fortinet Inc. All Rights Reserved.

Plan de Mejora Identificación, Protección, Detección, Respuesta y Recuperación

Servicio de Monitoreo, Correlación y Respuesta SOC 7x24

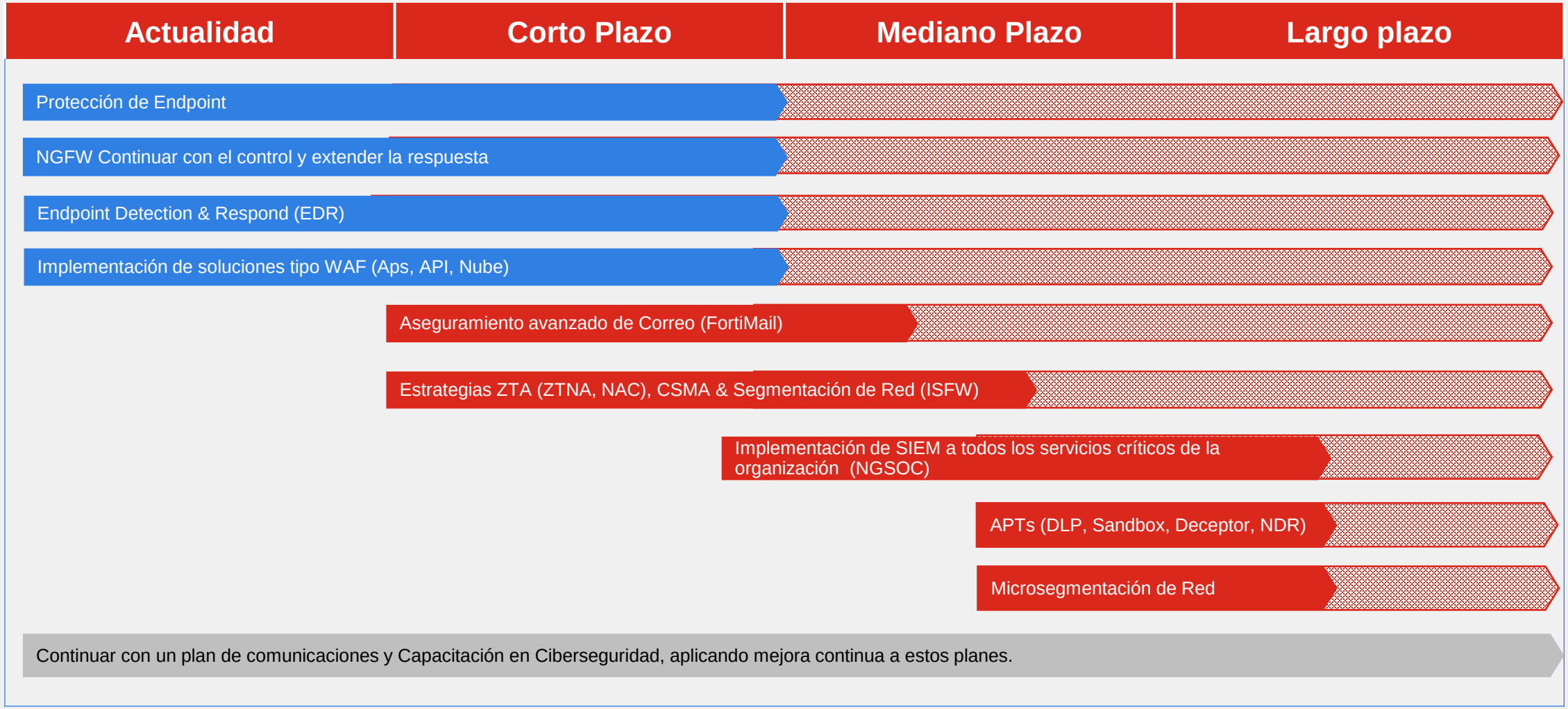


© Fortinet Inc. All Rights Reserved.



© Fortinet Inc. All Rights Reserved.

Roadmap de mejoramiento de ciberseguridad



Tecnologías Fortinet Tecnologías / Actividades de la organización o de terceros Tecnologías mixtas integradas (Fortinet - Cliente - Terceros) Continuidad en el Tiempo Proyectos de Optimización

© Fortinet Inc. All Rights Reserved.


FORTINET