Construyendo su Fortaleza Digital

Una Arquitectura Integral de Ciberseguridad y Resiliencia por securIT

securIT
IT & CYBERSECURITY

Nuestra Misión: Una Infraestructura Unificada, Segura y Preparada para el Futuro

Seguridad Perimetral y de Red: Blindaje contra amenazas externas y control interno granular.

Protección de Endpoints: Defensa proactiva en cada servidor y estación de trabajo.

Continuidad de Negocio: Sistema robusto de copias de seguridad para garantizar la resiliencia de los datos.

Gestión y Visibilidad Centralizada: Herramientas para el control total y la monitorización del estado de la infraestructura.

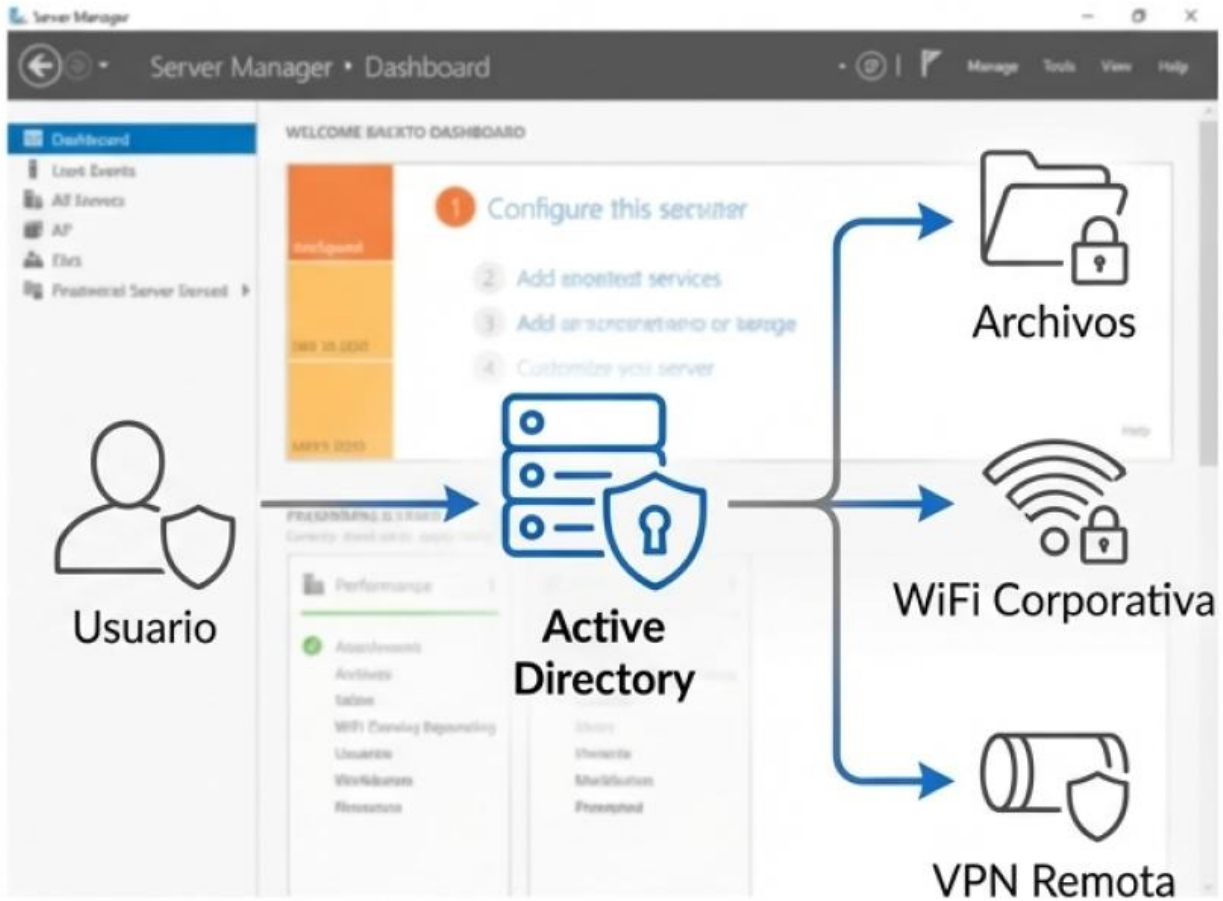
Acceso Remoto Seguro: Habilitación del teletrabajo sin comprometer la seguridad.

Capa 1: Los Cimientos - Windows Server y Active Directory

Toda fortaleza necesita una autoridad central.
La seguridad comienza con la identidad.
Implementamos y configuramos Windows Server con Active Directory (AD) para servir como el único punto de verdad para la identidad de los usuarios y equipos, garantizando que solo el personal autorizado tenga acceso a los recursos críticos.

- **Gestión Centralizada de Usuarios:**
- Creación y gestión de cuentas desde una única consola.
- **Control de Acceso Granular**: Asignación de permisos precisos para garantizar el acceso solo a los datos necesarios.
- **Fuente de Autenticación Unificada**: AD se integra con componentes clave de la fortaleza, sirviendo como fuente de autenticación para:

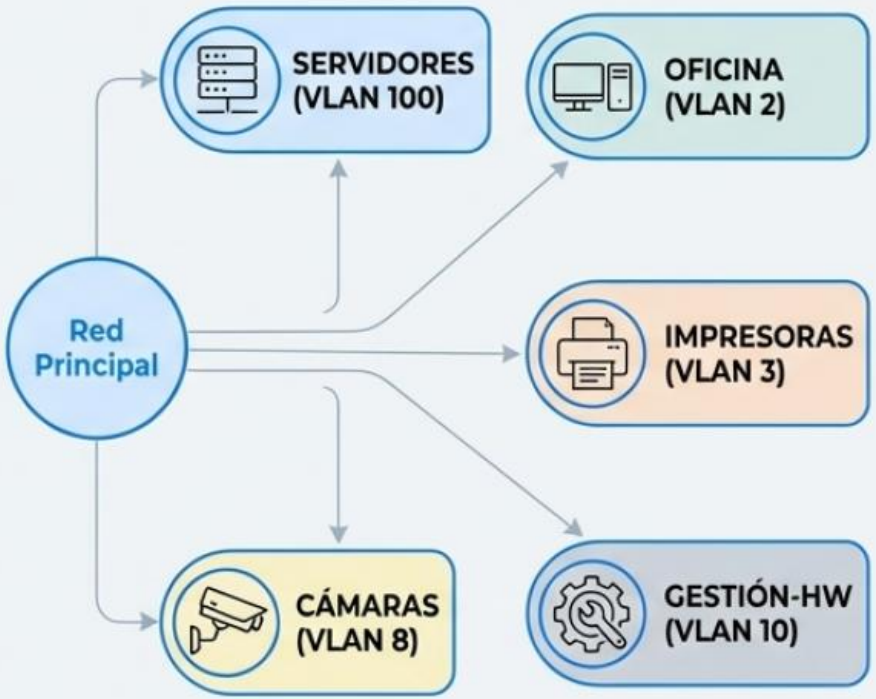
– Acceso a la red corporativa (WiFi WPA2-Enterprise).
– Conexiones remotas seguras (VPN SSL).



El Plano: Segmentación Estratégica de la Red

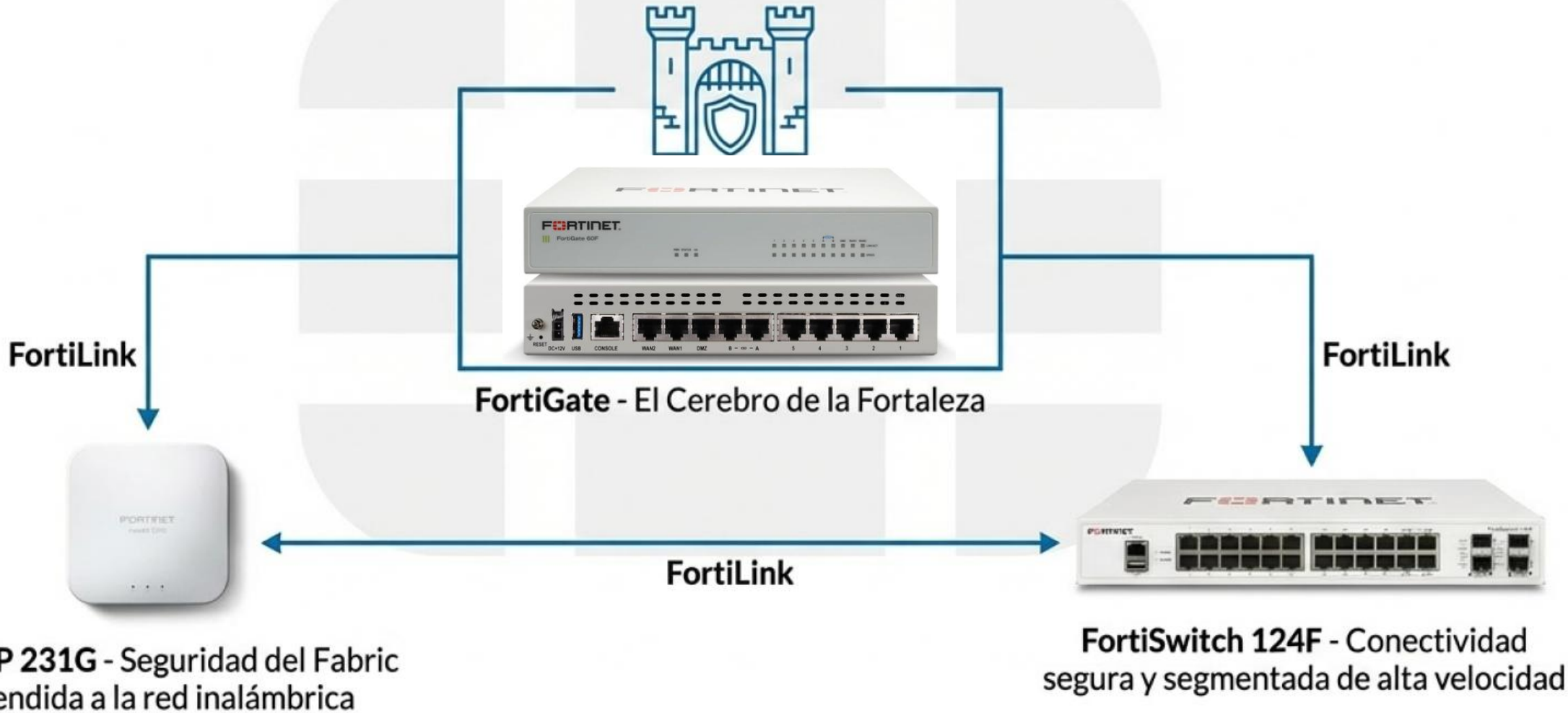
Concepto Clave: Antes de construir las murallas, definimos los distritos. Hemos reestructurado la red creando VLANs (Redes de Área Local Virtuales) para aislar y proteger los diferentes tipos de tráfico. Esto limita la capacidad de cualquier amenaza para propagarse lateralmente.

VLAN ID	Nombre	Red	Descripción
100	SERVIDORES	192.168.100.1/24	Aísla la infraestructura crítica del servidor.
2	OFICINA	192.168.2.1/24	Para equipos de sobremesa de uso diario.
3	IMPRESORAS	192.168.3.1/24	Segmento dedicado para dispositivos de impresión.
8	CÁMARAS	192.168.8.1/24	Red segura para el sistema de videovigilancia.
10	GESTIÓN-HW	192.168.10.1/24	Red restringida para la administración de dispositivos.



Capa 2: Las Murallas - El Ecosistema Fortinet Security Fabric

Sustituimos componentes de red dispares por una plataforma de seguridad unificada. El Fortinet Security Fabric permite que el firewall, los switches y los puntos de acceso operen como un único sistema, gestionado de forma centralizada y coherente.



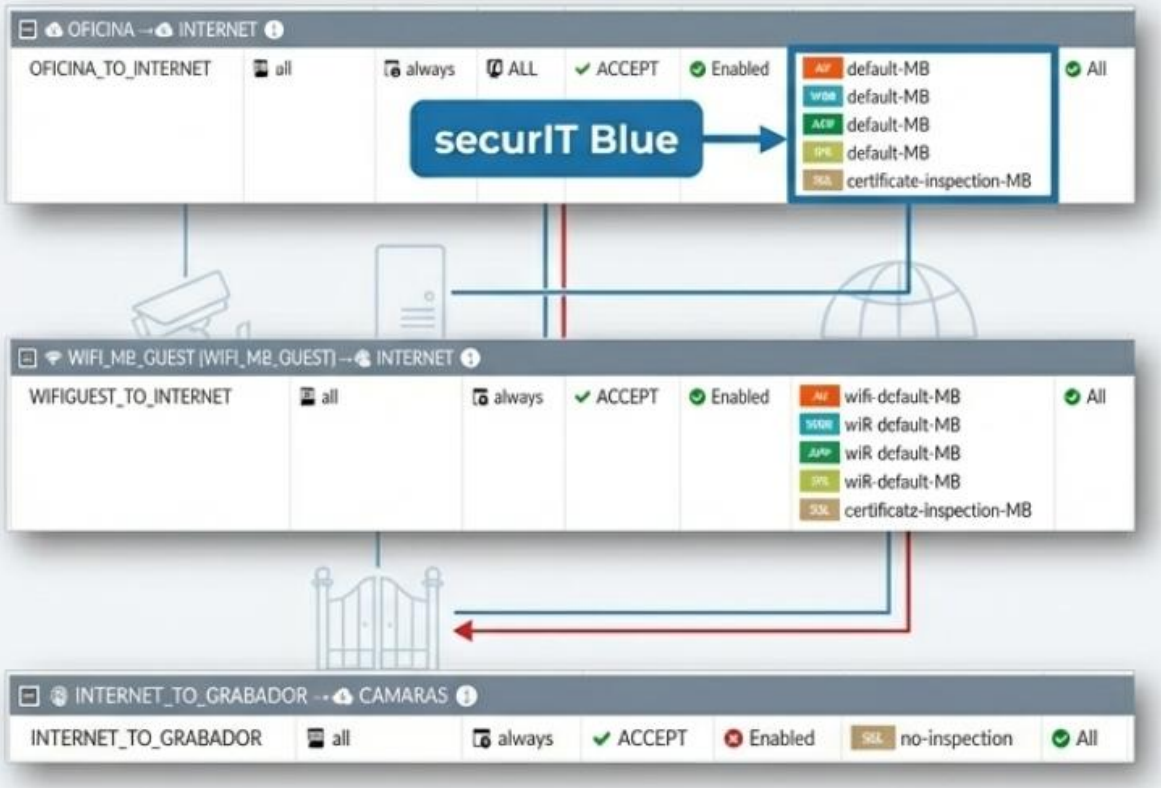
FortiGate - El Cerebro de la Fortaleza

FortiAP 231G - Seguridad del Fabric extendida a la red inalámbrica

FortiSwitch 124F - Conectividad segura y segmentada de alta velocidad

Concepto Clave : Las murallas tienen puertas vigiladas. Hemos definido políticas de firewall específicas que controlan con precisión el flujo de comunicación entre las distintas VLANs y hacia Internet.

- **Oficina → Internet:** Los equipos de oficina pueden navegar por Internet, pero todo el tráfico es inspeccionado por los perfiles de seguridad.
- **Servidores → Oficina:** El servidor puede comunicarse con los equipos de la oficina para tareas de gestión y servicio.
- **Wi-Fi Invitados → Internet:** Los dispositivos en la red de invitados tienen acceso exclusivo a Internet y están completamente aislados de la red corporativa interna.
- **Acceso Externo a Cámaras:** Se permite el acceso seguro al grabador de cámaras desde Internet a través de una regla de port forwarding (VIP).



Defensa Activa: Inspección y Filtrado de Amenazas (UTM)

Todo el tráfico que entra y sale de la red de Martinez Barba es inspeccionado por múltiples motores de seguridad para bloquear amenazas antes de que puedan causar daño.

Antivirus

Bloquea virus, spyware y otro malware en el gateway.

Web Filter

Impide el acceso a sitios maliciosos, de phishing y categorías no deseadas (Adulto/Maduro, Riesgo de Seguridad).

Application Control

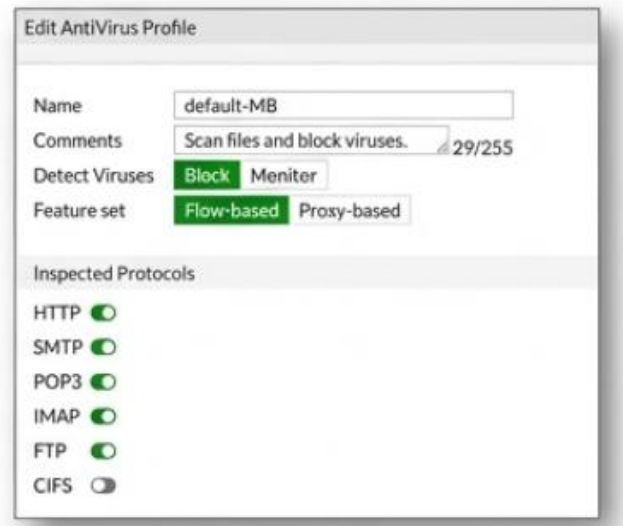
Identifica y controla el uso de aplicaciones para prevenir la exfiltración de datos y el uso de software de riesgo.

Intrusion Prevention (IPS)

Protege contra intentos de explotación de vulnerabilidades de red.

SSL Inspection

Descifra e inspecciona el tráfico HTTPS para encontrar amenazas ocultas, una capacidad crítica en el panorama actual.

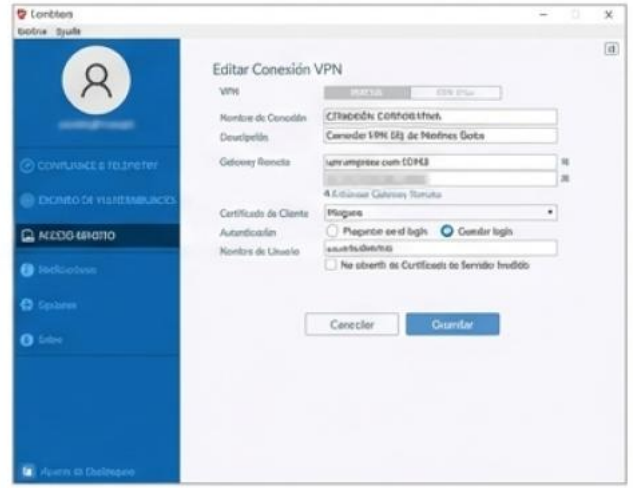


Conectividad Segura y Resiliente para el Negocio

Habilitamos el trabajo remoto de forma segura y garantizamos la continuidad del negocio con una infraestructura de alta disponibilidad.

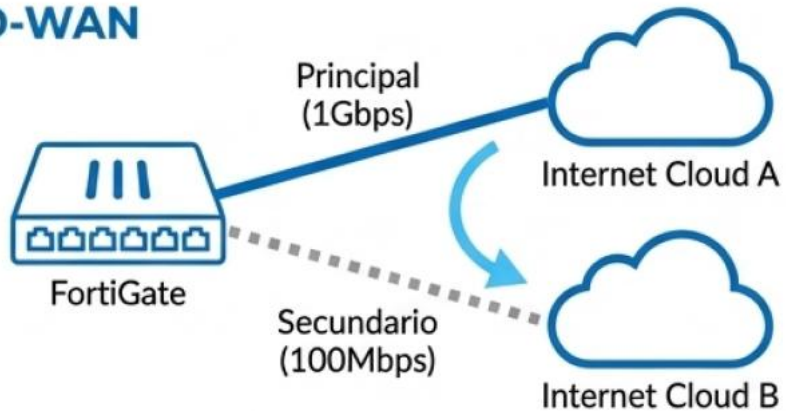
Acceso Remoto Seguro con FortiClient VPN

- **Túnel Cifrado:** Todo el tráfico está protegido con cifrado SSL de extremo a extremo.
- **Autenticación con Dominio:** Los usuarios validan sus credenciales de Active Directory, simplificando la gestión.
- **Acceso Granular:** Políticas de firewall garantizan que los usuarios remotos solo accedan a los recursos estrictamente necesarios.



Continuidad de Negocio con SD-WAN

Doble Conexión a Internet:
Configuramos dos enlaces (principal de 1Gbps y secundario de 100Mbps). Si la línea principal falla, el tráfico se redirige automáticamente a la secundaria sin interrupción.



Capa 3: La Guardia Interna - Protección Avanzada de Endpoints con CrowdStrike

La protección del perímetro es esencial, pero una defensa en profundidad requiere seguridad avanzada en cada endpoint. CrowdStrike protege servidores y estaciones de trabajo contra amenazas como el ransomware y los ataques sin fichero.

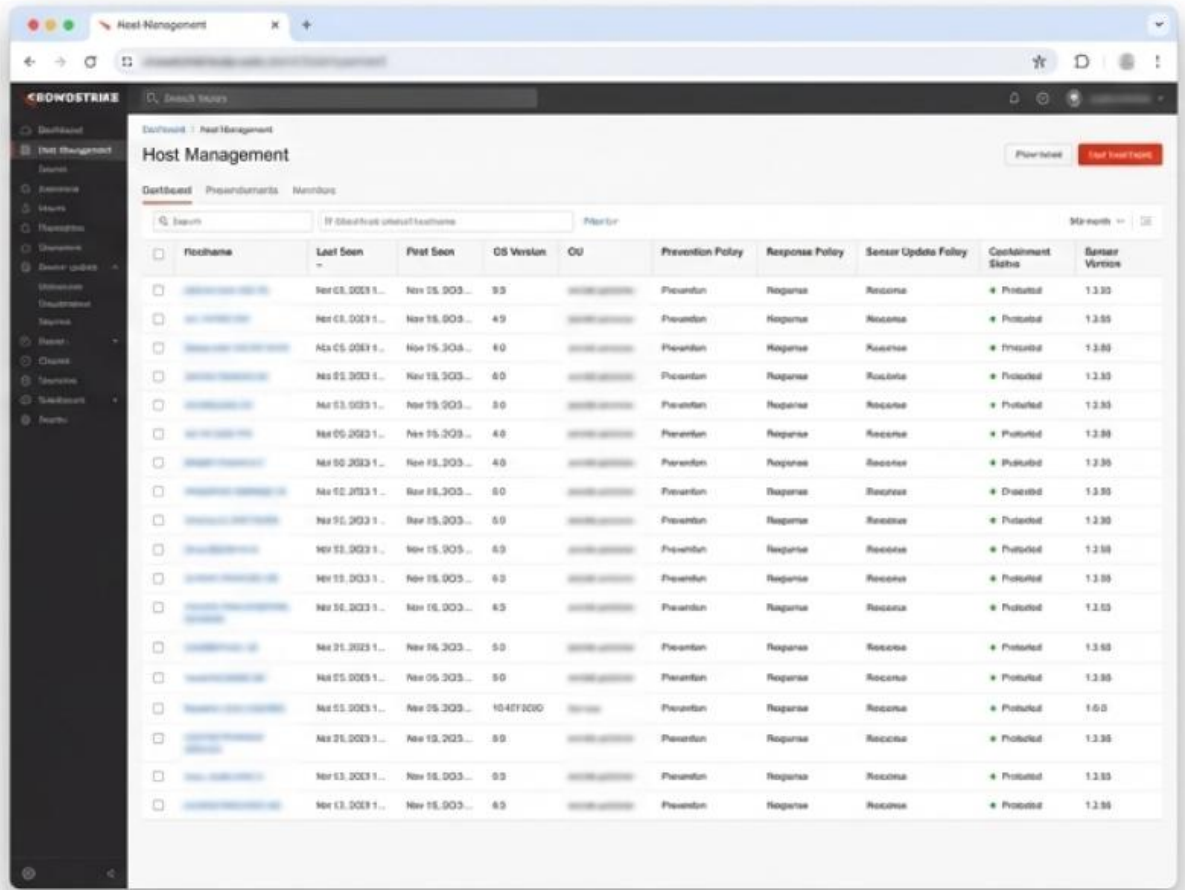
¿Por qué CrowdStrike?

Inteligencia Artificial y Machine Learning: Detecta amenazas conocidas y desconocidas basándose en el comportamiento, no solo en firmas.

Detección y Respuesta (EDR): Ofrece visibilidad completa para investigar y responder a incidentes rápidamente.

Plataforma en la Nube: Siempre actualizada y gestionada centralmente sin sobrecargar los equipos.

Despliegue: El agente de CrowdStrike está instalado y activo en todos los equipos de la oficina y en el servidor principal.



Los Centinelas: Protección Avanzada de Endpoints con CrowdStrike

Hemos desplegado CrowdStrike Falcon, una solución de ciberseguridad de nueva generación, en todos los servidores y estaciones de trabajo. Protege contra malware, ransomware y ataques sin fichero utilizando inteligencia artificial.

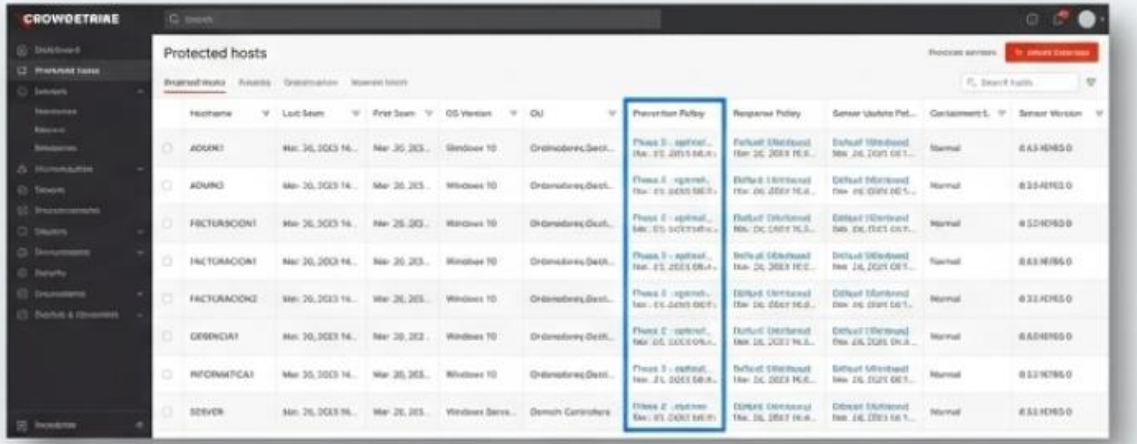
Características de la Política de Prevención "Phase 3 – optimal protection":

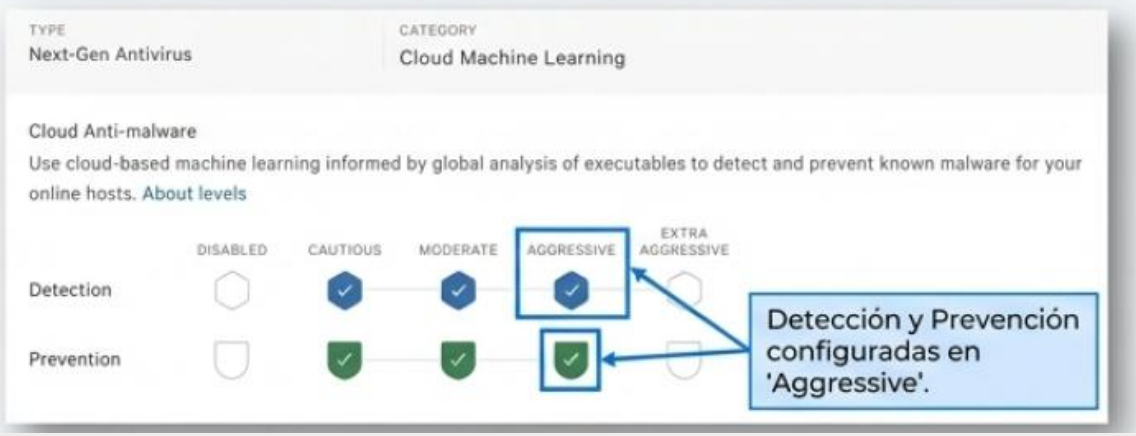
Niveles Agresivos: Detección y prevención de malware y adware configuradas en el nivel "Aggressive" para una máxima protección.

Protección Proactiva: Bloqueo de procesos, scripts y operaciones de registro sospechosas en tiempo real.

Escaneo Inteligente: Análisis automático de cualquier dispositivo USB que se conecte a un equipo.

Anti-Tampering: El sensor de CrowdStrike está protegido contra intentos de desactivación o desinstalación no autorizada.





Capa 4: La Bóveda Acorazada - Resiliencia con Veeam y Synology

La continuidad del negocio es primordial. Implementamos una solución de backup robusta para garantizar que los datos y sistemas críticos puedan recuperarse rápidamente ante cualquier eventualidad.

Componente 1: Repositorio Seguro (Synology DS418)

Un dispositivo NAS dedicado, configurado con 4 discos de 4TB en RAID-5 para un total de 10.5TB de capacidad segura y redundante.

Componente 2: Motor de Backup (Veeam B&R 12)

El software líder en la industria que automatiza y gestiona las copias de seguridad, garantizando su consistencia y fiabilidad.

Nuestra Estrategia de Backup: Frecuencia, Retención y Fiabilidad

Definimos múltiples tareas y políticas para minimizar la pérdida de datos (RPO) y garantizar múltiples puntos de restauración (RTO).

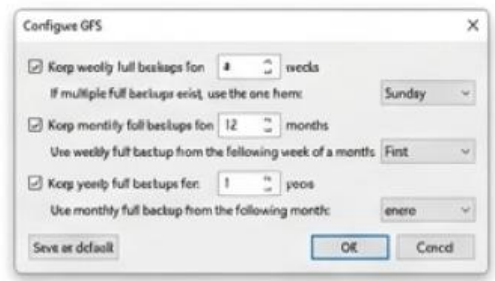
Detalle de las Tareas

- **BCK_Server_2300**: Copia de seguridad completa del servidor (imagen) cada día a las 23:00.
- **BCK_CarpetaDatos_1600 y _2200**: Copia de seguridad de la carpeta de datos críticos dos veces al día para una protección granular.

Panel de control de Veeam: Estado de las tareas de backup y última ejecución exitosa.

Política de Retención Inteligente (GFS)

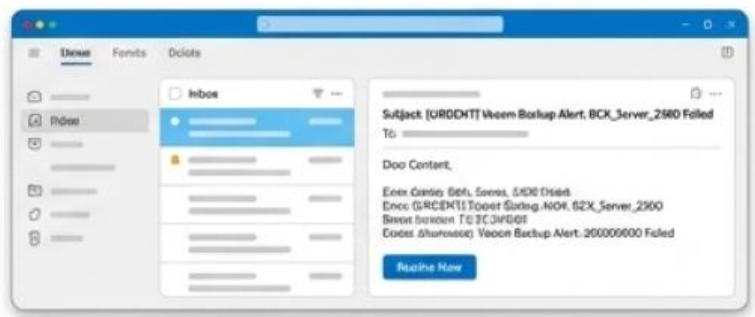
- **Corto Plazo**: 30 días de retención para recuperaciones operativas.
- **Largo Plazo**: Se conservan copias completas adicionales: 4 semanales, 12 mensuales y 1 anual para archivo.



Configuración de Retención GFS: Políticas a largo plazo para cumplimiento y archivo histórico.

Alertas Proactivas

El sistema está configurado para enviar notificaciones por correo electrónico ante cualquier fallo o advertencia, asegurando una supervisión constante.



Ejemplo de notificación por correo electrónico ante fallo.

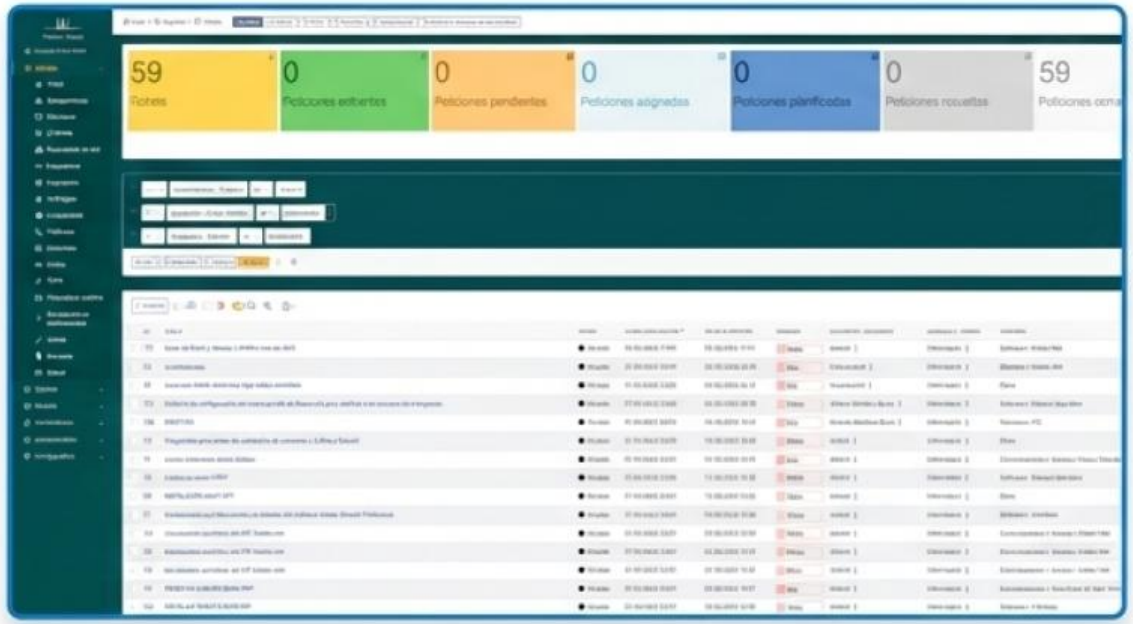
Capa 5: La Torre de Mando - Visibilidad y Gestión Proactiva

Una infraestructura segura es una infraestructura bien gestionada. Implementamos herramientas líderes para tener una visibilidad completa y un control total sobre las operaciones de TI.

Gestión de Servicios con GLPI

Función: Un sistema centralizado para la gestión de tickets de soporte, seguimiento de incidencias e inventario automatizado de todo el hardware y software de la red.

Beneficio: Centraliza la comunicación, proporciona un historial de intervenciones y ayuda a gestionar el ciclo de vida de los activos tecnológicos.



Monitorización de Sistemas con Pandora FMS

Función: Supervisión en tiempo real del estado de salud de todos los servidores y equipos críticos. Control de métricas clave: Carga de CPU, uso de disco, memoria y tráfico de red.

Beneficio: Alertas tempranas para prevenir problemas antes de que afecten a los usuarios, permitiendo una resolución rápida.

Capa 6: Protocolo de Acceso - Fortaleciendo al Usuario con KeePass

La seguridad más fuerte puede ser **vulnerada** por una contraseña débil. Implementamos una solución de gestión de contraseñas para fortalecer las credenciales de los usuarios y proteger las cuentas de la empresa.

Bóveda Cifrada
Almacena todas las contraseñas en una base de datos única y altamente cifrada.

Elimina Malos Hábitos
Fomenta el uso de contraseñas largas, complejas y únicas para cada servicio.

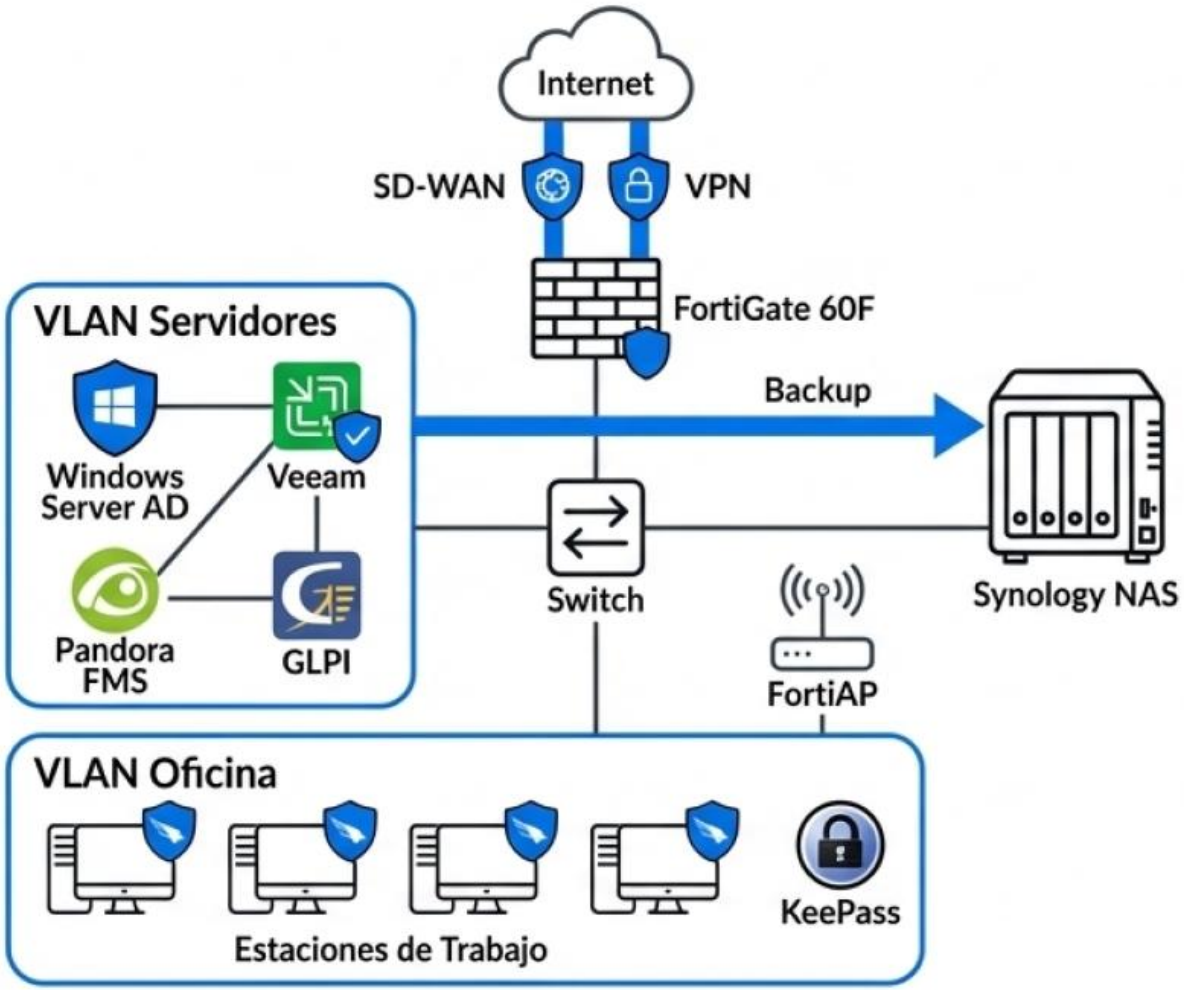
Protección contra Phishing
Autocompletar solo en sitios web legítimos reduce el riesgo.

Acceso Seguro
Permite compartir credenciales de forma segura, eliminando el envío por correo o chat.

securIT

La Arquitectura Completa: Su Fortaleza Digital Integrada

Cada tecnología ha sido cuidadosamente seleccionada e integrada para cumplir una función específica dentro de una estrategia de seguridad unificada, protegiéndole desde el núcleo hasta el usuario final.



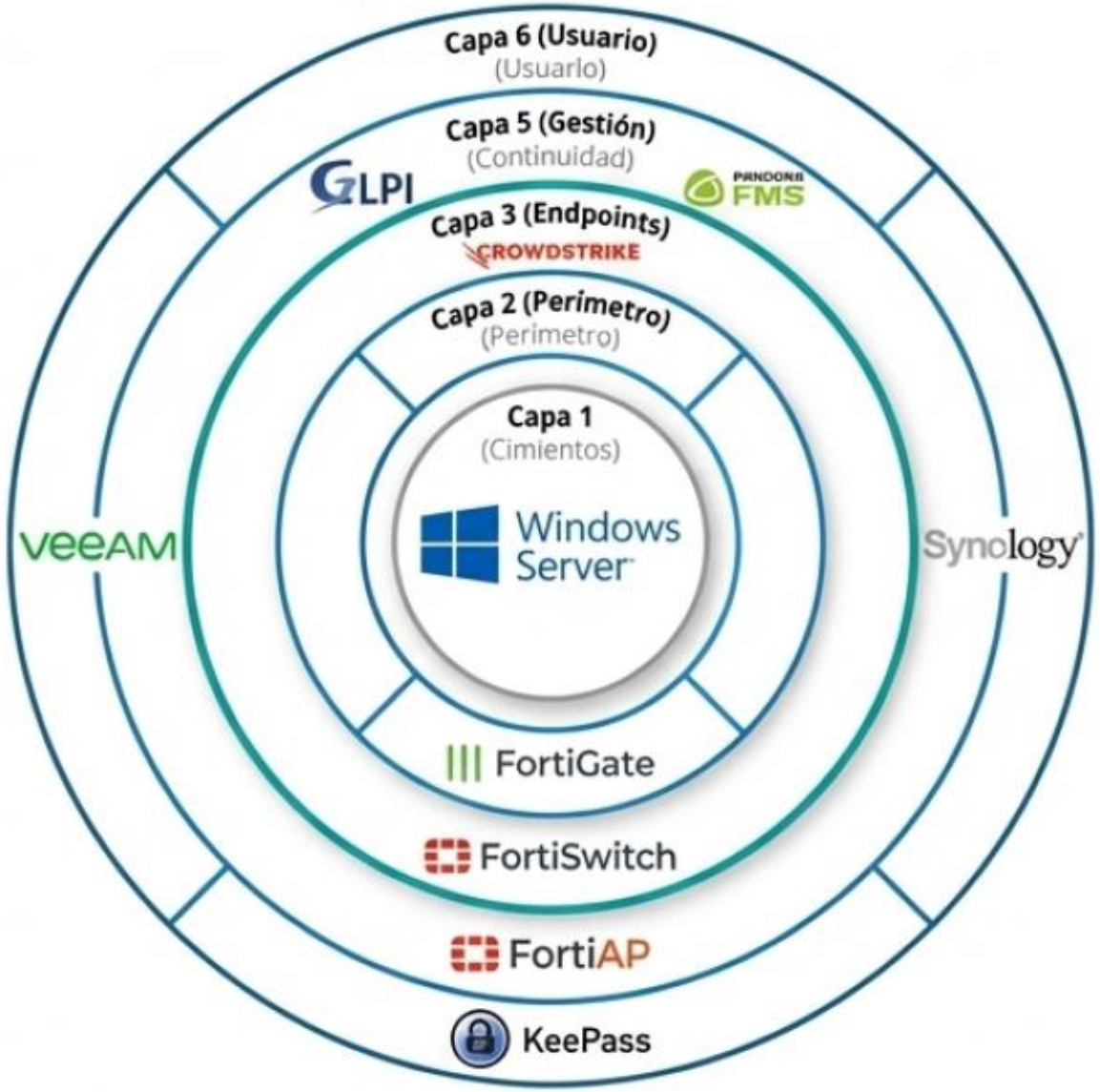
Protección 360°: Defensa en capas desde el perímetro hasta el endpoint.

Alta Disponibilidad y Resiliencia: Redundancia en la conectividad y en el almacenamiento de datos.

Control Centralizado: Gestión unificada de seguridad, usuarios y backups.

Visibilidad Total: Monitorización proactiva y gestión de incidencias.

La Arquitectura Completa: Su Fortaleza Digital



securIT: Su Socio Estratégico en Ciberseguridad

Estamos comprometidos a ser los arquitectos y guardianes de su seguridad digital, ahora y en el futuro. Hablemos de cómo podemos construir su fortaleza.

securIT
IT & CYBERSECURITY

Dpto. Comercial: Alejandro Abellán Merelo de Barberá
Teléfono: +34 677 809 561
Email: info@securit.es
Web: https://www.securit.es