Guía de Adecuación al ENS con WatchGuard

CUMPLIMIENTO DEL REAL DECRETO 311/2022 (ESQUEMA NACIONAL DE SEGURIDAD)

Resumen Ejecutivo: Esta guía técnica orienta a Administraciones Públicas y sus proveedores tecnológicos en la alineación con las medidas de seguridad del Esquema Nacional de Seguridad (ENS), utilizando el ecosistema de seguridad de WatchGuard (Firebox UTM/NGFW, AuthPoint MFA, WatchGuard EPDR/EDR y WatchGuard Cloud).

1. Introducción y Marco Normativo

El Real Decreto 311/2022 actualiza el **Esquema Nacional de Seguridad (ENS)** para responder a los nuevos desafíos cibernéticos. Las entidades del sector público y las empresas privadas que prestan servicios a la Administración deben implantar medidas organizativas, operativas y técnicas clasificadas en niveles **Básico, Medio y Alto**.

La arquitectura unificada de **WatchGuard Unified Security Platform** permite dar respuesta directa a múltiples controles del Anexo II del ENS, garantizando la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad del sistema.

2. Mapeo de Soluciones WatchGuard con Medidas ENS

MEDIDA ENS (RD 311/2022)	SOLUCIÓN WATCHGUARD APLICABLE	MECANISMO DE CUMPLIMIENTO
[op.acc.1] Control de acceso global	AuthPoint (MFA) / Firebox VPN	Autenticación multifactor obligatoria (MFA) con análisis contextual (IP, ubicación, hora) y Single Sign-On (SSO).
[op.acc.2] Identificación y autenticación	AuthPoint MFA / Firebox SSO	Validación de identidad robusta mediante empuje móvil (Push), tokens QR y compatibilidad con Active Directory/LDAP.
[op.net.1] Protección de la red local	Firebox UTM/NGFW	Segmentación por VLANs, inspección profunda de paquetes (HTTPS/TLS 1.3), prevención de intrusiones (IPS).
[op.net.2] Interconexión de redes	Firebox Branch Office VPN / SD-WAN	Túneles VPN seguros con cifrado robusto (AES-256) e inspección de tráfico entre sedes y entornos cloud.
[op.exp.8] Protección contra malware	WatchGuard EPDR / EDR	Servicio Zero-Trust Application (clasificación del 100% de procesos antes de su ejecución) y Threat Hunting.
[op.mon.1] Monitorización del sistema	WatchGuard Cloud / Log Server	Registro centralizado de eventos, correlación de amenazas, generación de alertas en tiempo real e informes auditables.

MEDIDA ENS (RD 311/2022)	SOLUCIÓN WATCHGUARD APLICABLE	MECANISMO DE CUMPLIMIENTO
[op.exp.10] Protección del correo electrónico	Firebox SpamBlocker / Cloud Mail Security	Filtrado de antispam, antiphishing, reputación de dominios y análisis en espacio aislado (Sandbox).
[mp.eq.1] Protección de puestos de trabajo	WatchGuard EPDR / Full Encryption	Protección del endpoint, firewall local, control de dispositivos USB y cifrado de disco centralizado (BitLocker).

3. Requisitos de Configuración por Dimensión de Seguridad

A. Confidencialidad e Integridad (op.net.1, op.net.2, mp.info.3)

- **Decodificación SSL/TLS:** Activar la inspección profunda HTTPS en el Firebox para evitar que malware evade los controles de red mediante tráfico cifrado.
- **Políticas Cero Confianza en Red:** Configurar reglas estricta de Firewall permitiendo únicamente los puertos y protocolos autorizados entre zonas de confianza y DMZ.
- **Cifrado de Datos en Transito:** Utilizar IKEv2 / IPsec con algoritmos de cifrado aprobados (AES-GCM-256) para enlaces VPN intersitio y acceso remoto.

B. Disponibilidad y Resiliencia (op.cont.1, op.exp.1)

- **Alta Disponibilidad (HA):** Configurar clústeres Firebox en modo Active/Passive o Active/Active para garantizar la continuidad operativa.
- **Multi-WAN y SD-WAN:** Configurar enlaces redundantes de Internet con failover automático y medición de calidad de enlace (jitter, pérdida de paquetes).

C. Trazabilidad y Monitorización (op.mon.1, op.mon.2)

- **Retención de Registros (Logs):** Configurar el envío continuo de logs cifrados a WatchGuard Cloud o a un servidor SIEM externo.
- **Informes para Auditoría ENS:** Utilizar los informes predefinidos de WatchGuard Dimension o Cloud para documentar incidentes, bloqueos de malware y autenticaciones fallidas.