Controles del ENS y cómo cumplirlos con edorteam DLP

Si tu organización está en proceso de certificación en el **Esquema Nacional de Seguridad** (ENS), sabrás que exige un riguroso nivel de protección y auditoría de la información.

Te mostramos cómo **Edorteam DLP cubre muchas de las medidas técnicas exigidas por el ENS**, automatizando las políticas de seguridad, previniendo fugas y simplificando enormemente la gestión diaria. Además, su integración nativa con la herramienta oficial del CCN allana el terreno con los auditores.

MARCO OPERACIONAL

Control de acceso [op.acc]

Control del ENS	Implementación con Edorteam DLP
[op.acc.4] Proceso de gestión de derechos de acceso Se limitarán los derechos de acceso bajo los principios de prohibición por defecto, mínimo privilegio, necesidad de conocer y control de acceso remoto.	» Aplica el principio de mínimo privilegio restringiendo y supervisando el acceso de los usuarios a carpetas con información confidencial. » Permite bloquear aplicaciones críticas, incluso exigiendo una contraseña secundaria como autorización expresa antes de permitir su ejecución. » Facilita la gestión remota y centralizada de estas directrices, asegurando el cumplimiento de la política de accesos fuera de la oficina.

Explotación [op.exp]

Control del ENS	Implementación con Edorteam DLP
[op.exp.1] Inventario de activos Se mantendrá un inventario actualizado de los elementos del sistema y se dispondrá de herramientas para visualizar de forma continua el estado de los equipos.	» Integra la auditoría CLARA (herramienta oficial del CCN) para extraer informes automáticos sobre el estado de los componentes con el formato exigido por el ENS. » Permite visualizar de forma continua y centralizada el estado de todos los endpoints desplegados a través de su panel de administración en la nube.
[op.exp.6] Protección frente a código dañino Se establecerán mecanismos de prevención y reacción en tiempo real frente a malware con herramientas orientadas a detectar, investigar y resolver actividades sospechosas.	» Detecta y frena en tiempo real ataques de ransomware o cryptolocker mediante reglas de comportamiento anómalo. » Actúa con capacidades de respuesta inmediata bloqueando la acción sospechosa, enviando alertas (e-mail/SMS) o apagando el equipo de inmediato.
[op.exp.7] Gestión de incidentes Los incidentes deben documentarse, investigarse y aplicarse medidas correctivas de forma inmediata.	» Recoge evidencias y trazabilidad inalterable (usuario, hora, equipo) esenciales para investigar incidentes de seguridad y brechas de datos personales (RGPD). » Identifica y alerta por e-mail o SMS sobre intentos de fuga de información o accesos no autorizados. » Aplica medidas de contención inmediata bloqueando de forma automática la acción sospechosa o apagando el equipo de inmediato.
[op.exp.8] Registro de la actividad Se registrarán las actividades en los sistemas de información y servidores, que incluirá, al menos, el usuario, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento.	» Registra la apertura, creación, modificación, copia y supresión de ficheros, dejando constancia inalterable de fecha, hora, usuario y equipo en cada interacción. » Protege los registros impidiendo de forma local que los usuarios desactiven o alteren el agente en el endpoint. » Ofrece un visor de informes con filtros y gráficas analíticas para revisar la actividad y detectar comportamientos anómalos.

Monitorización del sistema [op.mon]

Control del ENS	Implementación con Edorteam DLP
[op.mon.1] Detección de intrusión Se dispondrá de herramientas de detección o prevención de intrusiones basadas en reglas, con procedimientos y acciones automáticas de respuesta ante alertas.	» Aplica políticas de seguridad basadas en reglas de comportamiento para detectar anomalías en los endpoints. » Detecta y frena en tiempo real ataques de ransomware o cryptolocker mediante reglas de comportamiento anómalo. » Actúa con capacidades de respuesta inmediata bloqueando la acción sospechosa, enviando alertas (e-mail/SMS) o apagando el equipo de inmediato.
[op.mon.2] Sistema de métricas Se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad, evaluar la efectividad de la gestión de incidentes y medir la eficiencia de los recursos consumidos en términos de horas.	» El visor de informes aportan las métricas requeridas para evaluar el comportamiento del sistema ante incidentes. » Integra herramientas de cálculo de productividad y control de presencia que registran las horas reales de actividad y uso de aplicaciones, ofreciendo datos objetivos sobre la eficiencia de los recursos de la organización.
[op.mon.3] Vigilancia Se dispondrá de un sistema automático de recolección de eventos, que detecte amenazas avanzadas y prevenga la minería de datos alertando en tiempo real.	» Recolecta eventos de seguridad registrando de forma continua la actividad de ficheros, aplicaciones, portapapeles y tráfico web. » Identifica y bloquea en tiempo real ciberamenazas avanzadas y conductas anómalas como el ransomware. » Frena la minería de datos monitorizando el tráfico web de salida con alertas por e-mail o SMS o el apagado del equipo.

MEDIDAS DE PROTECCIÓN

Gestión del personal [mp.per]

Control del ENS	Implementación con Edorteam DLP
[mp.per.3] Concienciación del personal El personal debe estar concienciado sobre su responsabilidad, la normativa de buen uso de los sistemas y la identificación de comportamientos sospechosos.	» Lanza notificaciones en pantalla cuando el usuario realiza operaciones de riesgo o interactúa con información sensible, ayudándole a identificar conductas sospechosas o fallos de seguridad.

Protección de los equipos [mp.eq]

Control del ENS	Implementación con Edorteam DLP
[mp.eq.3] Protección de equipos portátiles Se protegerán los equipos que salen de las instalaciones, regulando su conexión remota y aplicando cifrado frente a pérdidas o robos.	» Monitoriza la actividad incluso en entornos de teletrabajo fuera de la red informática empresarial, controlando de forma estricta la salida de información de la empresa.
[mp.eq.4] Otros dispositivos conectados a la red Se debe garantizar el control del flujo de entrada y salida de la información regulando los dispositivos periféricos o personales (BYOD) conectados.	» Detecta, audita y bloquea la conexión de periféricos, soportes o equipos personales (BYOD) no autorizados. » Asegura una configuración estricta en el endpoint para controlar el flujo de entrada y salida de los datos corporativos.

Protección de las comunicaciones [mp.com]

Control del ENS	Implementación con Edorteam DLP
[mp.com.2] Protección de la confidencialidad Se protegerá la confidencialidad de la información en tránsito por las redes de comunicaciones.	» Usa la herramienta de cifrado integrada en Edorteam DLP, equipada con el algoritmo de encriptado de máximo nivel AES 256. » Protege los datos tanto en tránsito como en reposo.

Protección de los soportes de información [mp.si]

Control del ENS	Implementación con Edorteam DLP
[mp.si.2] Criptografía Se garantizará la confidencialidad e integridad de la información aplicando mecanismos criptográficos, especialmente en dispositivos USB que salgan de áreas controladas.	» Permite forzar el cifrado de la información transferida a dispositivos USB mediante el algoritmo AES 256. » Protege la confidencialidad de los datos tanto en tránsito como en reposo local.

Control del ENS	Implementación con Edorteam DLP
[mp.si.3] Custodia Se protegerán los soportes de información frente a pérdidas, robos o accesos no autorizados durante su transporte o fuera de las instalaciones.	» Aplica medidas lógicas mediante el cifrado preventivo de soportes extraíbles (USB) antes de salir de las instalaciones. » Impide accesos no autorizados a la información custodiada en caso de pérdida o robo del dispositivo periférico.
[mp.si.4] Transporte Los dispositivos deben permanecer bajo control durante su transporte fuera de las zonas controladas, empleando obligatoriamente protección criptográfica	» Satisface la protección criptográfica exigida forzando el cifrado automático de la información volcada en soportes extraíbles. » Registra la trazabilidad de los ficheros transferidos a USB antes de su desplazamiento, identificando al usuario y equipo responsable de la salida.
[mp.si.5] Borrado y destrucción Asegurar el borrado seguro de los soportes que se vayan a reutilizar o desechar para impedir la recuperación de su contenido.	» La función “Eliminación segura” borra datos de forma definitiva e irrecuperable incluso para herramientas forenses.

Protección de las aplicaciones informáticas [mp.sw]

Control del ENS	Implementación con Edorteam DLP
[mp.sw] Protección de las aplicaciones informáticas Se debe proteger el entorno de las aplicaciones garantizando el principio de mínimo privilegio y estableciendo mecanismos de protección de la información tratada.	» Permite establecer contraseñas adicionales específicas para abrir ciertos programas o archivos en el equipo, añadiendo una capa extra de autorización.

Protección de la información [mp.info]

Control del ENS	Implementación con Edorteam DLP
[mp.info.1] Datos personales Los sistemas contarán con las medidas técnicas necesarias para la protección de datos personales de acuerdo con los riesgos del RGPD.	» Monitoriza, audita y protege de forma continua los ficheros que contienen datos de carácter personal (RGPD) en los endpoints. » Aplica reglas automatizadas de bloqueo, alertas o cifrado en función del riesgo y la sensibilidad del dato personal detectado.

Control del ENS	Implementación con Edorteam DLP
[mp.info.2] Calificación de la información Se clasificará la información según su sensibilidad y aplicarán niveles de seguridad adecuados a su confidencialidad.	» Identifica automáticamente qué ficheros que contienen datos personales (DNI, IBAN, teléfono, etc.), clasificándolos por nivel de criticidad. » Automatiza las políticas de protección y restricción en base a esta clasificación, evitando la carga de revisar documentos manualmente. » La monitorización ayuda a evaluar qué datos son los más consultados, modificados o transferidos, facilitando su calificación y priorización defensiva.

Auditorías de seguridad

Control del ENS	Implementación con Edorteam DLP
Auditoría de seguridad El sistema debe someterse a auditorías regulares para verificar la eficacia de las medidas adoptadas.	» Edorteam DLP realiza la auditoría CLARA, la herramienta oficial del Centro Criptológico Nacional (CCN). » Extrae informes con el formato exacto exigido en la certificación del ENS.

Toma el control de tu información sensible

CYBERSECURITY MADE IN EUROPE

We care about your data

edorteam

edorteam.com

Con más de 30 años de trayectoria como consultora tecnológica de referencia, en Edorteam somos especialistas en protección de datos, ciberseguridad y cumplimiento normativo para empresas. Equipamos a las organizaciones para enfrentar desafíos digitales, comprometidos con el control y la seguridad de la información. Porque tus datos son lo que más nos importa.