					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P20					Título del documento: **Política de Protección de Endpoints / Protección contra Código Malicioso**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	La protección de endpoints y los controles antimalware son necesarios para cumplir los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI)
ISO/IEC 27002:2022	Controles 8.7, 8	Proporciona controles técnicos y directrices para la protección contra código malicioso, la defensa de endpoints y la gestión de incidentes
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Define requisitos de protección contra código malicioso, monitorización centralizada y configuración de referencia
RGPD de la UE	Artículo 32	Exige medidas técnicas adecuadas para proteger los datos personales, incluida la protección contra código malicioso
Directiva NIS2 de la UE	Artículo 21(2)(d)	Requiere el despliegue de medidas preventivas y de detección de amenazas a nivel de endpoint
DORA de la UE	Artículo 9	Exige la gestión del riesgo de las TIC en relación con malware y amenazas que afectan a los endpoints
COBIT 2019	DSS05.01, DSS01.04, MEA	Exige la protección, monitorización y evaluación de los controles de endpoint

1. Propósito

1.1 Esta política define los controles obligatorios y los requisitos operativos para proteger los endpoints de la organización, incluidos equipos de sobremesa, portátiles, dispositivos móviles y servidores, frente al malware y amenazas relacionadas.

1.2 Establece los estándares mínimos para la protección de endpoints, la detección de malware, la respuesta de contención y el análisis de comportamiento, garantizando que los sistemas mantengan su resiliencia frente a variantes de malware tanto comunes como avanzadas.

1.3 La política respalda directamente el cumplimiento de la cláusula 8.1 y del control 8.7 del Anexo A de ISO/IEC 27001:2022, y se alinea con las obligaciones regionales de ciberseguridad en virtud del RGPD de la UE, la Directiva NIS2 de la UE y DORA de la UE.

2. Alcance

2.1 Esta política se aplica a todos los endpoints, incluidos:

2.1.1 Equipos de sobremesa, portátiles, dispositivos móviles e instancias virtuales propiedad de la organización o gestionados por esta.

2.1.2 Dispositivos de propiedad personal autorizados conforme a la Política de BYOD, sujetos a la instalación de MDM o de un agente de endpoint.

2.1.3 Servidores y activos de infraestructura, incluidas máquinas virtuales alojadas en la nube y dispositivos perimetrales.

2.1.4 Sistemas operativos, controladores, servicios locales, agentes de endpoint y controles de seguridad instalados en cada nodo.

2.2 Esta política cubre a todo el personal con responsabilidad administrativa, técnica u operativa sobre cualquier endpoint, incluidos:

2.2.1 Empleados internos y contratistas.

2.2.2 Proveedores de servicios gestionados, servicios externalizados de soporte de puesto de trabajo y administradores de TI externos.

2.2.3 Usuarios autorizados para operar sistemas portátiles, portátiles con VPN habilitada o acceso móvil a las redes de la organización.

2.3 La cobertura de amenazas en virtud de esta política incluye, entre otras:

2.3.1 Virus, gusanos, troyanos, ransomware, spyware, rootkits, adware, registradores de teclas y botnets.

2.3.2 Malware sin archivos, cargas útiles de día cero, malware de elevación de privilegios y kits de explotación del navegador.

2.3.3 Código malicioso distribuido mediante soportes extraíbles, vectores de phishing, descargas involuntarias o ataques basados en USB.

3. Objetivos

3.1 Proteger la integridad, disponibilidad y confidencialidad de los sistemas endpoint y de los datos que tratan mediante mecanismos fiables de prevención, detección y respuesta frente al malware.

3.2 Evitar la ejecución o propagación de código malicioso en las redes de la organización mediante la aplicación de salvaguardas técnicas, configuraciones de referencia seguras y telemetría en tiempo real.

3.3 Integrar la protección de endpoints con otros controles del SGSI, incluida la gestión de vulnerabilidades, el control de acceso, el registro y monitorización de eventos, y la respuesta a incidentes.

3.4 Garantizar la visibilidad continua de los endpoints mediante plataformas de protección gestionadas centralmente, incluidos agentes antivirus/antimalware, detección y respuesta en endpoints (EDR) y telemetría hacia el SIEM.

3.5 Cumplir los requisitos legales, reglamentarios y normativos que exigen seguridad de endpoints (por ejemplo, artículo 32 del RGPD de la UE, artículo 21 de la Directiva NIS2 de la UE y artículo 9 de DORA de la UE).

3.6 Definir funciones con responsabilidades claras, aplicar acuerdos de nivel de servicio para la respuesta a parches y alertas, y facilitar la preparación para auditorías mediante documentación e informes.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es el responsable de esta política y garantiza su alineación con el SGSI y la estrategia global de seguridad.

4.1.2 Revisa trimestralmente las métricas de protección de endpoints, las tendencias de incidentes y la eficacia de las herramientas.

4.1.3 Aprueba las excepciones y las aceptaciones de riesgo residual relacionadas con la cobertura de endpoints.

4.2 Responsable de Seguridad de Endpoints / Responsable del SOC

4.2.1 Gestiona los sistemas de protección de endpoints (por ejemplo, AV, EDR, MDM).

4.2.2 Supervisa la aplicación de la política, el ajuste de la detección de amenazas y los procedimientos operativos de respuesta.

4.2.3 Mantiene estadísticas de cobertura, registros de incidentes de malware y configuraciones de referencia de alertas.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1 Esta política debe revisarse anualmente o cuando:

9.1.1 Se produzcan campañas importantes de malware o incidentes de seguridad en endpoints.

9.1.2 Nuevos tipos de amenazas (por ejemplo, malware sin archivos o variantes de ransomware) exijan estrategias actualizadas de detección o respuesta.

9.1.3 Las plataformas de protección de endpoints o las arquitecturas de agentes cambien de forma significativa.

9.1.4 Se actualicen los requisitos legales o reglamentarios que afecten a los controles de endpoint.

9.2 La revisión será iniciada por el Responsable de Seguridad de Endpoints y coordinada con las funciones de CISO, Jurídico, Riesgos y Auditoría.

9.3 Las revisiones aprobadas deben documentarse en el Registro de Control Documental del SGSI, asignarse a un nuevo identificador de versión y comunicarse a todas las partes afectadas.

9.4 Las versiones sustituidas deben archivarse, restringirse en cuanto al acceso y conservarse para mantener la integridad de la pista de auditoría conforme a los calendarios de conservación del SGSI.

10. Políticas relacionadas y vinculaciones

10.1 P1 - Política de Seguridad de la Información. Establece principios fundamentales para la protección de sistemas, datos y redes. Esta política aplica dichos principios en el nivel de endpoint mediante controles técnicos y procedimentales de protección contra código malicioso.

10.2 P4 - Política de Control de Acceso. Define restricciones de acceso de usuarios que se aplican en la capa de endpoint, incluidas protecciones frente a elevaciones de privilegios e instalaciones no autorizadas de software no validado.

10.3 P5 - Política de Gestión de Cambios. Garantiza que las actualizaciones del software de protección de endpoints, las reglas de política o las configuraciones de agentes estén sujetas a aprobación y a procesos de despliegue controlado.

10.4 P12 - Política de Gestión de Activos. Proporciona la clasificación de activos y el inventario de activos de referencia necesarios para la visibilidad de endpoints, la cobertura de parches y la definición del alcance de la protección contra malware.

10.5 P22 - Política de Registro de Eventos y Monitorización. Permite la integración de alertas de endpoints, el estado de salud de los agentes y la inteligencia de amenazas en sistemas SIEM centralizados para detección en tiempo real y trazabilidad forense.

10.6 P30 - Política de Respuesta a Incidentes. Vincula los incidentes de malware en endpoints con flujos de trabajo estandarizados de contención, erradicación, investigación y recuperación, con funciones asignadas y umbrales de escalado.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001:

11.1.1 Cláusula 8.1 - Planificación y control operacional: exige la implantación de controles técnicos, incluidas salvaguardas de endpoint, para mantener los objetivos del SGSI.

11.2 ISO/IEC 27002:2022 - Controles 8.7, 8:

11.2.1 Proporciona orientación técnica detallada sobre medidas antimalware, despliegue seguro de software, monitorización y preparación ante incidentes para entornos de endpoint.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Protección contra código malicioso: exige el uso de herramientas antimalware con análisis en tiempo real, análisis en acceso y análisis de comportamiento.

11.3.2 SI-4 - Monitorización del sistema: respalda la integración de telemetría con plataformas centralizadas de detección.

11.3.3 CM-6 - Ajustes de configuración: refuerza los ajustes de control de la configuración de referencia en endpoints, incluida la aplicación de agentes de protección.

11.4 RGPD de la UE (2016/679):

11.4.1 Artículo 32 - Seguridad del tratamiento: exige que las organizaciones implanten medidas técnicas adecuadas para proteger los datos personales, incluida la protección frente a amenazas de malware.

11.5 Directiva NIS2 de la UE (2022/2555):

11.5.1 Artículo 21(2)(d): obliga a las entidades a desplegar medidas de detección y prevención de amenazas, incluidos mecanismos de defensa contra malware a nivel de endpoint.

11.6 DORA de la UE (2022/2554):

11.6.1 Artículo 9 - Requisitos de gestión del riesgo de las TIC: exige que las entidades financieras adopten medidas de protección para prevenir, detectar y responder al malware y a las amenazas que afectan a los endpoints.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Protección contra malware: exige la detección y mitigación del malware en todos los endpoints de la organización.

11.7.2 DSS01.04 - Gestionar la disponibilidad y la capacidad: garantiza que la protección contra malware se equilibre con el rendimiento del sistema y la continuidad del negocio.

11.7.3 MEA03 - Supervisar, evaluar y valorar el cumplimiento: exige la auditoría periódica de los controles de endpoint y de la eficacia de la protección.