					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P20S					Título del documento: **Política de Protección de Endpoints frente al Malware**							
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**

Aviso legal (derechos de autor y restricciones de uso)

(C) 2025 Clarysec LLC. All rights reserved.

Este documento es propiedad intelectual de Clarysec LLC. Ninguna parte de este documento podrá copiarse, reutilizarse, distribuirse ni modificarse con fines comerciales o de implantación sin autorización previa y expresa por escrito.

El uso no autorizado está estrictamente prohibido y puede dar lugar a acciones legales.

Para cuestiones de licenciamiento, contacte con: info@clarysec.com

Alineación con normas y reglamentos, cuando corresponda

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	Controles operativos para la protección frente al código malicioso
ISO/IEC 27002:2022	Control 8	Medidas de control para la protección de endpoints
NIST SP 800-53 Rev.5	SI-3, SI-4	Protección frente al código malicioso y respuesta a incidentes
Directiva NIS2 de la UE	Artículos 21(2)(d), (e)	Malware y gestión de riesgos para entidades esenciales e importantes
DORA de la UE	Artículos 10(1), 15	Resiliencia operativa y verificación de terceros
COBIT 2019	DSS05.02, DSS05.04	Protección de endpoints y redes, y monitorización
RGPD de la UE	Artículos 32(1)(b), 33	Medidas técnicas y organizativas y notificación de violaciones de seguridad de los datos personales

1. Propósito

1.1 Esta política establece los requisitos mínimos técnicos, procedimentales y de comportamiento para proteger todos los endpoints, incluidos portátiles, equipos de sobremesa, dispositivos móviles y soportes extraíbles, frente al código malicioso, incluidos virus, ransomware, spyware, rootkits y otras amenazas de malware.

1.2 Su propósito es garantizar que los endpoints estén equipados, mantenidos y utilizados de forma que se reduzca el riesgo de infección por malware, su propagación y el compromiso de los sistemas.

1.3 La organización reconoce que los endpoints son puntos habituales de entrada de malware y, por tanto, deben someterse a bastionado, supervisarse y protegerse mediante un modelo de defensa en capas.

1.4 Esta política respalda los objetivos de certificación ISO/IEC 27001:2022 de la organización y se alinea con el Reglamento General de Protección de Datos de la UE (RGPD), la Directiva NIS2, DORA y otros marcos aplicables.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los endpoints de la organización, incluidos equipos de sobremesa, portátiles, tabletas, teléfonos móviles y terminales de punto de venta.

2.1.2 Dispositivos de propiedad personal utilizados para acceder a aplicaciones o datos de la organización.

2.1.3 Dispositivos de almacenamiento extraíbles, como unidades USB y discos duros externos.

2.1.4 Cualesquiera sistemas operativos, software de endpoint o herramientas de comunicación que se ejecuten en estas plataformas.

2.2 Se aplica por igual a:

2.2.1 Personal interno, contratistas, becarios y proveedores de servicios gestionados.

2.2.2 Dispositivos utilizados en las instalaciones, de forma remota o en modalidades de trabajo híbrido.

2.2.3 Endpoints conectados a la nube o desconectados que almacenen datos de la organización o datos personales.

3. Objetivos

3.1 Prevenir la infección por malware y su propagación a través de sistemas internos, dispositivos de usuario y conexiones externas.

3.2 Detectar y contener con rapidez las amenazas relacionadas con malware mediante tecnologías automatizadas de seguridad de endpoints y procedimientos de escalado definidos.

3.3 Garantizar que solo se utilicen dispositivos autorizados, protegidos y supervisados para acceder a la información de la organización.

3.4 Establecer responsabilidades claras para el personal y normas de comportamiento para los usuarios con el fin de reducir el riesgo de incidentes relacionados con malware.

3.5 Mantener registros trazables y auditables de las detecciones de malware, las respuestas aplicadas y el cumplimiento de la política.

3.6 Proteger los datos personales y los datos de la organización frente a su compromiso por malware mediante estrategias de defensa en profundidad.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Es responsable de esta política y garantiza que existan recursos suficientes para la protección de endpoints.

4.1.2 Aprueba el software antivirus, las herramientas de gestión de dispositivos móviles (MDM) y las reglas de acceso de terceros.

4.1.3 Revisa los informes de incidentes de malware, los resúmenes de impacto y las notificaciones de violaciones de seguridad que involucren endpoints.

4.2 Proveedor de soporte de TI / Administrador interno de TI

4.2.1 Selecciona y despliega software antivirus, antimalware y de detección y respuesta en endpoints (EDR).

4.2.2 Garantiza que las actualizaciones se apliquen de forma coherente y que los registros se conserven.

4.2.3 Responde a las alertas de malware, aísla los sistemas infectados y lleva a cabo la remediación.

4.2.4 Aplica controles sobre el uso de dispositivos USB y otros dispositivos externos.

[... 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 Requisito de revisión anual

9.1.1 Esta política debe revisarse formalmente al menos una vez al año por el Director General, en coordinación con el proveedor de soporte de TI y el Coordinador de Privacidad.

9.2 Actualizaciones motivadas por eventos desencadenantes

9.2.1 La política también debe actualizarse cuando:

9.2.1.1 Una nueva amenaza de malware importante o un brote significativo tenga como objetivo endpoints utilizados por la organización.

9.2.1.2 Las herramientas antivirus o EDR se modifiquen, actualicen o sustituyan.

9.2.1.3 Un incidente de malware revele debilidades en el alcance o la aplicación de esta política.

9.2.1.4 Se actualicen los requisitos legales o reglamentarios, por ejemplo, RGPD, DORA o la Directiva NIS2.

9.3 Control de versiones y comunicación

9.3.1 Todos los cambios en la política deben documentarse con número de versión, fecha y resumen de cambios.

9.3.2 Se debe notificar al personal las actualizaciones, especialmente si modifican requisitos operativos o de comportamiento.

9.3.3 Las versiones anteriores deben conservarse en el archivo de políticas durante al menos 3 años para respaldar las auditorías.

10. Políticas relacionadas y vinculaciones

10.1 Esta política debe implantarse conjuntamente con las siguientes políticas para pymes:

10.1.1 P9S – Política de Trabajo Remoto: garantiza que los requisitos de protección de endpoints se apliquen en los dispositivos utilizados fuera de las instalaciones o en entornos híbridos.

10.1.2 P12S – Política de Gestión de Activos: respalda el seguimiento y control de todos los endpoints y garantiza que solo se utilicen dispositivos autorizados y protegidos.

10.1.3 P17S – Política de Protección de Datos y Privacidad: refuerza la prevención del malware como control esencial de privacidad para proteger los datos personales y sensibles frente a su compromiso.

10.1.4 P22S – Política de Registro de Eventos y Supervisión: establece los requisitos para el registro de eventos de malware y el mantenimiento de la visibilidad de las alertas para una respuesta temprana.

10.1.5 P30S – Política de Respuesta a Incidentes: define el escalado, la contención y los pasos de notificación externa si el malware provoca un compromiso de datos o una interrupción operativa.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Requiere la implantación de controles operativos para reducir riesgos como los ataques de malware.

11.2 ISO/IEC 27002

11.2.1 Control 8.7 – Detalla prácticas de control del malware, incluidos antivirus, análisis en tiempo real, actualizaciones y formación de usuarios.

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Requiere el despliegue de mecanismos de protección frente al código malicioso en los endpoints.

11.3.2 SI-4 – Exige acciones de supervisión, detección, análisis y respuesta para amenazas y alertas a nivel de endpoint.

11.4 RGPD de la UE

11.4.1 Artículo 32(1)(b) – Requiere controles técnicos y organizativos, como antivirus, para proteger los datos personales.

11.4.2 Artículo 33 – Obliga a notificar violaciones de seguridad cuando el malware comprometa la integridad, confidencialidad o disponibilidad de los datos.

11.5 Directiva NIS2 de la UE

11.5.1 Artículo 21(2)(d) – Requiere medidas para prevenir y responder a amenazas de malware dentro de entidades esenciales e importantes.

11.5.2 Artículo 21(2)(e) – Exige estrategias de gestión del riesgo de ciberseguridad por capas, incluida la protección de endpoints frente al malware.

11.6 DORA de la UE

11.6.1 Artículo 10(1) – Requiere que los sistemas TIC estén protegidos frente al malware y otras amenazas como parte de la resiliencia operativa.

11.6.2 Artículo 15 – Obliga a las organizaciones financieras a verificar la protección frente al malware en proveedores de servicios externos.

11.7 COBIT 2019

11.7.1 DSS05.02 – Hace hincapié en medidas de protección para defender endpoints y redes frente a amenazas de malware.

11.7.2 DSS05.04 – Refuerza la supervisión y el alertado sobre eventos de seguridad relacionados con malware como parte de las operaciones continuas.