HORNETSECURITY
BY proofpoint.

INFOSHEET
AI POWERED

365 4 TOTAL PROTECTION Y NIS2



¿Cómo ayuda 365 Total Protection a cumplir con la NIS2?

A medida que evolucionan las ciberamenazas, la NIS2 eleva el nivel exigido para la gestión de riesgos de ciberseguridad en toda la Unión Europea, con un mayor énfasis en la gobernanza, la resiliencia, la respuesta ante incidentes, la continuidad de negocio y la concienciación de las personas. Cumplir estos requisitos exige un enfoque integral que combine gobernanza, tecnología, resiliencia y concienciación. **365 Total Protection puede ayudar a las organizaciones en este proceso mediante medidas de seguridad y capacidades relacionadas con el cumplimiento que se alinean con varios requisitos de NIS2.**

HORNETSECURITY BY proofpoint.

INFOSHEET AI POWERED

DISPOSICIÓN	QUÉ EXIGE AL CLIENTE	CÓMO PUEDEN AYUDAR LOS PRODUCTOS	CÓMO AYUDA 365 TOTAL PROTECTION	CORRESPONDENCIA CON LOS PILARES DE NIST	ÁMBITO DE NIS2
ARTÍCULO 20(1)	Los órganos de dirección deben aprobar las medidas de gestión de riesgos de ciberseguridad adoptadas por las entidades para cumplir el artículo 21 y supervisar su aplicación.	Paneles de gobernanza, flujos de trabajo para aprobar controles, informes para la dirección y paquetes de evidencias.	Consola del Control Panel Paneles y vistas de auditoría de 365 Permission Manager Historial de copias de seguridad/ restauración y aprobación 4-eyes de 365 Total Backup Estado de Security Awareness Service y certificado de empresa Email Live Tracking Registros de auditoría	Gobernar	Gestión de riesgos de ciberseguridad
ARTÍCULO 20(2)	Los órganos de dirección deben completar la formación en ciberseguridad y las entidades deben ofrecer formación similar al personal.	Plataformas de formación y concienciación, seguimiento de finalización, acreditaciones y formación basada en roles.	Módulos de e-learning de Security Awareness Service, simulaciones de spear phishing, vídeos breves y cuestionarios Certificado anual de empresa de SAS	Gobernar	Gestión de riesgos de ciberseguridad
ARTÍCULO 21(1)	Las entidades incluidas en el ámbito de aplicación deben adoptar medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos de ciberseguridad.	Plataformas de controles básicos, herramientas de gestión de riesgos, aplicación de políticas y recopilación de evidencias.	Conjunto combinado de controles para seguridad del correo electrónico, cifrado, continuidad, copias de seguridad, gobernanza de permisos y concienciación: Spam and Malware Protection, Content Control, Compliance Filter, Global S/MIME/PGP encryption, Websafe, Email Continuity Service, 365 Total Backup, 365 Permission Manager, Security Awareness Service, AI Recipient Validation, Teams Protection	Gobernar	Gestión de riesgos de ciberseguridad
ARTÍCULO 21(2)(A)	Políticas de análisis de riesgos y de seguridad de los sistemas de información. Herramientas para registros de riesgos, gestión del ciclo de vida de las políticas y correspondencia de controles de seguridad.	Herramientas para registros de riesgos, gestión del ciclo de vida de las políticas y correspondencia de controles de seguridad.	Reglas personalizadas de Compliance Filte Políticas de cumplimiento de 365 Permission Manager, nueva auditoría automática y periódica de accesos aprobados previamente y, próximamente, clasificación de la gravedad de los riesgos; Email Live Tracking Registros de auditoría Vistas de panel sobre el estado de cumplimiento y de las copias de seguridad	Gobernar	Gestión de riesgos de ciberseguridad

HORNETSECURITY
BY proofpoint.

INFOSHEET
AI POWERED

DISPOSICIÓN	QUÉ EXIGE AL CLIENTE	CÓMO PUEDEN AYUDAR LOS PRODUCTOS	CÓMO AYUDA 365 TOTAL PROTECTION	CORRESPONDENCIA CON LOS PILARES DE NIST	ÁMBITO DE NIS2
ARTÍCULO 21(2)(B)	Gestión de incidentes.	SIEM/SOAR, gestión de casos de incidentes, playbooks y sistemas de tickets.	Integración con SIEM y SOAR, de forma nativa o mediante API Función nativa de alertas y Monitoring en CP	Detectar / Responder	Gestión de riesgos de ciberseguridad
ARTÍCULO 21(2)(C)	Continuidad de negocio, incluida la gestión de copias de seguridad, la recuperación ante desastres y la gestión de crisis.	Orquestación de copias de seguridad, pruebas de recuperación ante desastres, planificación de continuidad y flujos de trabajo para crisis.	Email Continuity Service 365 Total Backup	Recuperar	Gestión de riesgos de ciberseguridad
ARTÍCULO 21(2)(D)	Seguridad de la cadena de suministro, incluidos los aspectos de seguridad de las relaciones con proveedores directos y proveedores de servicios.	Gestión de riesgos de terceros, cuestionarios para proveedores y supervisión continua de proveedores.	Controles de uso compartido externo de 365 Permission Manager, detección y corrección de enlaces compartidos y detección de permisos anómalos AI Recipient Validation para evitar la pérdida accidental de datos al enviarlos a un proveedor o proveedor de servicios Email encryption para proteger las comunicaciones externas con proveedores y proveedores de servicios	Gobernar	Gestión de riesgos de ciberseguridad
ARTÍCULO 21(2)(F)	Políticas y procedimientos para evaluar la eficacia de las medidas de gestión de riesgos de ciberseguridad.	Pruebas de controles, cumplimiento continuo, evidencias de auditoría y paneles de KPI/KRI.	Paneles de cumplimiento y registro de actividad de 365 Permission Manager; Estado de las copias de seguridad, registro de actividad e historial de restauraciones de 365 Total Backup ESI, estadísticas y certificado anual de Security Awareness Service Email Live Tracking y otras estadísticas del correo electrónico Registros de auditoría	Gobernar	Gestión de riesgos de ciberseguridad
ARTÍCULO 21(2)(G)	Prácticas básicas de ciberhigiene y formación en ciberseguridad.	Concienciación en seguridad, simulaciones de phishing, niveles básicos de ciberhigiene y comprobaciones del estado de los endpoints.	Módulos de e-learning de Security Awareness Service, simulaciones de spear phishing, vídeos breves y cuestionarios; Certificado anual de empresa de SAS	Proteger	Gestión de riesgos de ciberseguridad
ARTÍCULO 21(2)(H)	Políticas y procedimientos sobre criptografía y, cuando proceda, cifrado.	Gestión de claves, aplicación de políticas de cifrado y herramientas para gestionar el ciclo de vida de los certificados.	Email encryption	Proteger	Gestión de riesgos de ciberseguridad

HORNETSECURITY
BY proofpoint.

INFOSHEET
AI POWERED

DISPOSICIÓN	QUÉ EXIGE AL CLIENTE	CÓMO PUEDEN AYUDAR LOS PRODUCTOS	CÓMO AYUDA 365 TOTAL PROTECTION	CORRESPONDENCIA CON LOS PILARES DE NIST	ÁMBITO DE NIS2
ARTÍCULO 21(2)(I)	Seguridad de los recursos humanos, políticas de control de acceso y gestión de activos.	IAM, flujos de trabajo de altas, cambios y bajas, inventario de activos y control de accesos privilegiados.	Informes de permisos de 365 Permission Manager, delegación en propietarios de sitios, niveles de uso compartido externo, auto-remediation y registro de actividad; controles de acceso privado/de prueba al archivo de correo electrónico	Proteger	Gestión de riesgos de ciberseguridad
			Gestión masiva de usuarios de 365 Total Backup		
ARTÍCULO 21(2)(J)	MFA o autenticación continua, comunicaciones de voz, vídeo y texto protegidas, y comunicaciones de emergencia seguras, cuando proceda.	MFA/SSO, acceso condicional, comunicaciones seguras y comunicaciones de emergencia.	Email encryption	Proteger	Gestión de riesgos de ciberseguridad
			Websafe		
ARTÍCULO 23(2)	Notificación sin demoras indebidas, en un plazo de 24 o 72 horas, según el tipo de incidente.	Alertas en 24 horas, automatización del triaje, clasificación inicial y soporte para turnos de guardia.	Alertas en tiempo real y AutoRemediate de Advanced Threat Protection	Responder	Intercambio de información
			Email Live Tracking		
			AI Email Security Analyst ayuda a caracterizar incidentes relacionados con el correo electrónico		
			Correcciones automatizadas de 365 Permission Manager		

Refuerza tu estrategia de ciberseguridad para NIS2

El cumplimiento de NIS2 requiere un enfoque que abarque a toda la organización y combine gobernanza, procesos, personas y tecnología. Ningún producto de seguridad puede garantizar el cumplimiento por sí solo.

365 Total Protection puede contribuir a esta estrategia más amplia aportando funcionalidades de seguridad, resiliencia, gobernanza y concienciación que ayudan a las organizaciones a abordar medidas asociadas a requisitos clave de NIS2, desde la seguridad y el cifrado del correo electrónico hasta las copias de seguridad, la gestión de permisos, la visibilidad de los incidentes y la concienciación en seguridad.

En conjunto, estas funcionalidades pueden ayudar a las organizaciones a reforzar su postura de ciberseguridad y respaldar de forma continua su camino hacia el cumplimiento de NIS2.

SOLICITA TU DEMO

Fuentes: Página de políticas de la Comisión Europea · Preguntas frecuentes de la Comisión Europea sobre NIS2 · Texto oficial de NIS2 en EUR-Lex