					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P40					Título del documento: **Política de pruebas de seguridad y ejercicios de red team**							
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**

Alineada con las normas y reglamentos aplicables

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	9.1, 9.2, 9.3	
ISO/IEC 27002:2022	5.7, 5.36, 8.8, 8.29, 8.30, 8.1	
NIST SP 800-53 Rev.5	CA-2, CA-7, CA-8, RA-5	
RGPD de la UE	Art. 32(1)(d)	
Directiva NIS2 de la UE	Art. 21(2)(f)	
DORA de la UE	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Propósito

1 Establecer un programa estructurado de pruebas periódicas de seguridad sobre las redes, los sistemas y las aplicaciones de la organización, incluidas evaluaciones de vulnerabilidades, pruebas de penetración y ejercicios de red team, para dar cumplimiento a los requisitos del artículo 21(2)(f) de la Directiva NIS2 de la UE relativos a la evaluación de la eficacia de las medidas de ciberseguridad.

1.1 Garantizar que las debilidades en las medidas técnicas y organizativas se identifiquen y corrijan de forma proactiva mediante pruebas controladas, mejorando de manera continua la postura de seguridad de la organización.

2. Alcance

2 Esta política cubre todos los sistemas de información críticos, las aplicaciones y la infraestructura de soporte propiedad de la organización o gestionados por esta. También incluye las pruebas de seguridad física de las instalaciones cuando sean relevantes para la ciberseguridad (por ejemplo, ingeniería social o pruebas de intrusión física, si están dentro del alcance del red team).

2.1 La política se aplica a los equipos internos de seguridad, a cualquier empresa externa contratada para realizar pruebas de seguridad y a los propietarios de sistemas o aplicaciones correspondientes. Todas las actividades de prueba deben estar autorizadas y seguir los procedimientos aquí establecidos para evitar interrupciones no intencionadas.

3. Objetivos

3 Verificar la eficacia de los controles de ciberseguridad implantados —técnicos, operativos y organizativos— mediante pruebas periódicas y simulaciones, en consonancia con el mandato de la Directiva NIS2 de la UE de medir dicha eficacia.

3.1 Detectar vulnerabilidades o deficiencias que los procesos operativos habituales puedan no identificar, incluidos problemas de configuración o vulnerabilidades de día cero, en escenarios de ataque realistas (red teaming), antes de que sean explotadas por actores maliciosos.

3.2 Proporcionar a la dirección aseguramiento y recomendaciones prácticas mediante la comunicación de los resultados de las pruebas, permitiendo decisiones informadas sobre el tratamiento de riesgos y la mejora continua del programa de seguridad.

4. Funciones y responsabilidades

4 Coordinador de Pruebas de Seguridad (STC): designado por el Director de Seguridad de la Información (CISO), es responsable de planificar y supervisar todas las actividades de pruebas de seguridad. Garantiza que las pruebas estén claramente definidas en cuanto a alcance, cuenten con la debida autorización y que sus resultados se comuniquen y gestionen adecuadamente.

4.1 Equipo Interno de Seguridad (Blue Team): colabora en las pruebas, por ejemplo, proporcionando información para la definición del alcance y supervisando los sistemas durante su ejecución. En los ejercicios de red team, el Blue Team responde a los ataques simulados y se evalúa su capacidad de detección y respuesta.

4.2 Red Team / probadores de penetración: puede tratarse de un equipo interno de seguridad ofensiva o de consultores externos. Ejecutan las pruebas conforme a las reglas de actuación acordadas, documentan todas las vulnerabilidades detectadas y las rutas de explotación, y mantienen la confidencialidad.

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

9. Seguimiento y auditoría

9 El STC mantendrá un calendario y un registro de todas las actividades de pruebas de seguridad realizadas. Este registro deberá incluir la fecha, el alcance, quién realizó la prueba y un resumen de los resultados. Se revisará para garantizar el cumplimiento del calendario exigido, por ejemplo, que ningún sistema crítico quede sin probar más allá del ciclo anual.

9.1 El progreso de la remediación de los hallazgos de las pruebas será objeto de seguimiento y se informará mensualmente. Los problemas pendientes de alta severidad se revisarán en reuniones de dirección hasta su cierre.

9.2 Auditoría Interna o un auditor independiente revisará anualmente el programa de pruebas de seguridad para verificar que las pruebas están debidamente autorizadas, ejecutadas y documentadas; que los hallazgos críticos han sido tratados; y que el programa cumple las expectativas regulatorias, por ejemplo, que se realizó una prueba de penetración antes del lanzamiento de un nuevo servicio en línea cuando así se exija. Cualquier desviación dará lugar a planes de acción correctiva.

10. Revisión y mantenimiento

10 Esta política y el plan general de pruebas se revisarán al menos una vez al año. La revisión tendrá en cuenta los cambios en el panorama de amenazas, por ejemplo, la aparición de nuevas técnicas de ataque que nuestras pruebas actuales podrían no cubrir, y adaptará en consecuencia los alcances o las frecuencias.

10.1 Tras cualquier incidente grave de ciberseguridad o brecha de seguridad, esta política deberá revisarse para determinar si pruebas adicionales o más frecuentes podrían haber prevenido o detectado el problema. La política se actualizará posteriormente para incorporar dichos ajustes, por ejemplo, añadiendo un nuevo escenario a los ejercicios de red team basado en patrones de ataque observados.

10.2 Las actualizaciones de esta política deberán ser aprobadas por el Director de Seguridad de la Información y puestas en conocimiento del Consejo de Administración. Todo el personal pertinente será informado de los cambios, y los socios externos que participen en las pruebas serán notificados si algún cambio afecta a sus términos de contratación.

11. Políticas relacionadas y vinculaciones

11.1 P06 – Política de gestión de riesgos. Los resultados de las pruebas impulsan la evaluación y el tratamiento de riesgos.

11.2 P22 – Política de registro y monitorización. Valida la cobertura de detección durante los ejercicios.

11.3 P24 – Política de desarrollo seguro. Integra los hallazgos de las pruebas en los controles del ciclo de vida de desarrollo seguro (SDLC).

11.4 P25 – Política de requisitos de seguridad de las aplicaciones. Garantiza que los requisitos reflejen los aprendizajes obtenidos en las pruebas.

11.5 P30 – Política de respuesta a incidentes. Los escenarios de red team perfeccionan los playbooks y la respuesta.

11.6 P31 – Política de recopilación de evidencias y análisis forense. Recopila artefactos durante las pruebas de forma segura.

11.7 P32 – Política de continuidad de negocio y recuperación ante desastres. Los ejercicios verifican la resiliencia frente a ataques.

11.8 P33 – Política de auditoría y supervisión del cumplimiento. Proporciona supervisión independiente de la eficacia del programa de pruebas.

12. Referencias

12.1 Directiva NIS2 (UE 2022/2555), artículo 21(2), letra (f) (políticas y procedimientos para evaluar la eficacia de las medidas de gestión de riesgos de ciberseguridad)

12.2 Reglamento de Ejecución (UE) 2024/2690 de la Comisión, anexo, sección 7 (requisitos para supervisar, probar y evaluar la eficacia de las medidas de ciberseguridad)

12.3 Guía técnica de ENISA (2025) – anexo sobre pruebas de seguridad y auditoría (directrices para la realización de ejercicios de ciberseguridad y pruebas técnicas)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:

12.5 Buenas prácticas del sector: OWASP Testing Guide, NIST SP 800-115 (guía técnica de pruebas de seguridad), CBEST/GREEN Team (marcos de red teaming del sector financiero como referencia)