CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de auditoría de sistemas

Versión 1.0

APROBACIONES

Elaborado por:	Revisado por:	Aprobado por:
<Nombre>	<Nombre>	<Nombre>
<Cargo>	<Cargo>	<Cargo>
<Firma>	<Firma>	<Firma>

HISTORIAL DE REVISIONES

Versión	Fecha	Revisión
1.0	Diciembre 2021	Versión Inicial

Contenido

1. Introducción

1.1 Autoridad

El Centro Nacional de Seguridad Digital fue creado el 9 de enero del 2020, mediante Decreto de Urgencia N° 007-2020, es el encargado de gestionar, dirigir, articular y supervisar la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. También es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

El Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital.

1.2 Propósito

El propósito de esta política es obtener evidencias de cómo los sistemas de información cumplen con los requisitos de seguridad deseados.

1.3 Alcance

Esta política se aplica a todos los empleados y afiliados de la organización.

2. Política

2.1 Se debe tener identificado los activos más relevantes que deben ser auditados, estos activos pueden ser desde archivos, bases de datos, páginas web, equipos o programas hasta servicios completos.

2.2 Se debe enfocar el proceso de auditoría desde un punto de vista de mejora continua o de consecución de niveles de madurez.

2.3 Se debe realizar auditorías específicas para verificar el cumplimiento de los requerimientos legales.

2.4 Se debe realizar auditorías forenses para determinar lo ocurrido tras un incidente de seguridad.

2.5 Se debe definir y/o revisar los procedimientos detallados para auditar la seguridad de cada activo clave de los sistemas de información.

2.6 Se debe seleccionar el tipo de auditoría más conveniente, como, por ejemplo: test de penetración, auditoría de red, auditoría de seguridad perimetral, auditoría web, auditoría forense, auditoría legal, etc.

2.7 Se debe definir con detalle los procedimientos y logs necesarios para realizar cada tipo de auditoría.

2.8 Se debe concretar cómo registrar los resultados de las revisiones.

2.9 Se debe realizar auditorías de los sistemas de información al menos dos veces por año.

2.10 Se debe evaluar si se repite las auditorías tras la implantación de algún cambio significativo en los sistemas.

2.11 Se debe analizar los resultados de la auditoría en busca de debilidades a corregir.

3. Cumplimiento de políticas

3.1.1 Medición de cumplimiento

Se verificará el cumplimiento de esta política a través de varios métodos, incluidos, entre otros, recorridos periódicos, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas y comentarios al propietario de la póliza.

3.1.2 Excepciones

Cualquier excepción a la política debe ser aprobada con anticipación.

3.1.3 Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, hasta e incluyendo la terminación del empleo.