CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de respuesta a incidentes

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 asegurar que todos los miembros de la organización conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información.

1.3 Alcance

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

2. Política

2.1 Se debe notificar los incidentes de seguridad de la información que afecten a la integridad o la disponibilidad.

2.2 Los empleados y contratistas que utilizan los sistemas y servicios de información de la organización deben informar de las debilidades a la mesa de servicio, al equipo de seguridad de TI a través de la prestación de servicios o la gestión de relaciones.

2.3 Los eventos clasificados como eventos de seguridad de la información deben ser evaluados para confirmar si deben clasificarse como incidentes de seguridad de la información.

2.4 Los eventos de seguridad de la información deben se respondidos de acuerdo con el impacto comercial del evento y su gravedad.

2.5 Se deben revisar los incidentes para determinar la causa raíz, el impacto, para reducir la probabilidad y mejorar el impacto de incidentes futuros.

2.6 Los sistemas deben conservarse para permitir la recolección de evidencia siempre que el proceso de preservación no ponga en peligro la integridad de ningún sistema.

2.7 Las funciones, responsabilidades y procedimientos de gestión deben establecerse, comunicarse y documentarse en un plan de respuesta a incidentes para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

2.8 El plan debe incorporar la cadena de suministro y acciones de respuesta de servicios de terceros.

2.9 Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados lo más rápido posible y se alienta a los miembros del personal a informar los incidentes.

2.10 Los empleados y contratistas que utilicen los sistemas y servicios de información de la organización deben anotar y notificar cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

2.11 Todo incidente que se presente en la organización a efectos de cumplir con la legislación vigente, deberá ser reportado al Centro Nacional de Seguridad Digital, mediante el correo incidentes@cnsd.gob.pe.

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.