CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de buenas prácticas en redes sociales

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 explicar cómo se deben usar las redes sociales y establecer las normas de comportamiento que se esperan de los usuarios.

1.3 Alcance

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

2. Política

2.1 Como administrador de las redes sociales, se debe utilizar una contraseña fuerte y habilitar siempre que sea posible el doble factor de autenticación en todos los perfiles de la organización.

2.2 Se debe establecer la configuración de la privacidad de manera que permita utilizar las distintas redes sociales de forma efectiva.

2.3 Se debe permitir interactuar con el público sin descuidar la seguridad y privacidad del perfil de la organización.

2.4 Se debe elegir un responsable de publicación.

2.5 Se debe definir normas de publicación.

2.6 Se debe elegir la imagen que desea reflejar, qué publica y qué no, el tono o lenguaje, cómo se responde a las consultas y quejas de los usuarios.

2.7 Antes de conceder acceso u otro permiso a ciertas aplicaciones (de gestión, estadísticas, publicitarias, etc.), se debe analizar detalladamente los riesgos que pueden suponer para el perfil de la organización (acceso a información confidencial, publicaciones sin supervisión, etc.)

2.8 Se debe estar informado de las distintas campañas utilizadas por los ciberdelincuentes para conseguir acceso a los perfiles de las organizaciones en las distintas redes sociales.

2.9 Se debe formar a los empleados en ciberseguridad y seguridad de la información para minimizar los riesgos relativos al uso de las tecnologías, en particular las redes sociales.

2.10 Se debe tratar los enlaces de las redes sociales y los documentos adjuntos con las mismas precauciones que el correo electrónico.

2.11 En caso de que un enlace lo dirija a cualquier web que solicite cualquier tipo de información confidencial o bancaria, se debe comprobar el certificado de seguridad y que corresponda con el sitio al que se está accediendo.

2.12 Se debe usar el sentido común al momento de publicar, ya que puede afectar la imagen de la organización.

2.13 Se debe evitar acciones como dar información confidencial, participar en discusiones, propagar noticias falsas, entre otros.

2.14 No se debe publicar mensajes, actualizaciones de estado o enlaces a material o contenido que sea inapropiado: pornografía, insultos raciales o religiosos, comentarios específicos de género, información que fomente las habilidades delictivas o terrorismo, o materiales relacionados con cultos, juegos de azar o drogas ilegales.

2.15 Solo se debe publicar actualizaciones, mensajes o utilizarlos de otro modo como: responder a las consultas, solicitudes, compartir publicaciones de blog, artículos y otros contenidos creados relevante para la entidad.

2.16 Se debe usar un lenguaje de una manera respetuosa, buena ortografía y gramática a la hora de crear contenidos en las redes sociales.

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.