CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de contraseñas

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 proporcionar lineamientos que los usuarios deben tener en consideración al momento de generar sus contraseñas de acceso.

1.3 Alcance

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

2. Política

Debe tener en cuenta seguir estos pasos para generar y/o cambiar sus contraseñas:

2.1 Utilice una frase de contraseña larga. De acuerdo con la guía de NIST, debe considerar usar la contraseña o frase de contraseña más larga permisible. Por ejemplo, puede usar una frase de contraseña como un titular de noticias o incluso el título del último libro que leyó. Luego agregue algo de puntuación y mayúsculas.

2.2 No haga que las contraseñas sean fáciles de adivinar. No incluya información personal en su contraseña, como su nombre o nombres de mascotas. Esta información suele ser fácil de encontrar en las redes sociales, lo que facilita que los ciberdelincuentes hackeen sus cuentas.

2.3 Evite usar palabras comunes en sus contraseñas. Sustituir letras por números y signos de puntuación o símbolos, por ejemplo, @ puede reemplazar la letra "A" y un signo de exclamación (!) puede reemplazar las letras "I" o "L".

2.4 Sea creativo. Use reemplazos fonéticos, como "PH" en lugar de "F". O cometer errores ortográficos deliberados, pero obvios, como "enjin" en lugar de "motor".

2.5 Mantenga sus contraseñas en secreto. No le diga a nadie sus contraseñas y esté atento a los atacantes que intentan engañar para que revele sus contraseñas a través de correo electrónico o llamadas. Cada vez que comparte o reutiliza una contraseña, se elimina su seguridad al abrir más vías en las que podría ser mal utilizada o robada.

2.6 **Cuenta única, contraseña única.** Tener diferentes contraseñas para varias cuentas ayuda a prevenir que ciberdelincuentes puedan obtener acceso a estas cuentas y protegerlo en caso de incumplimiento. Es importante mezclar las cosas—encuentre formas fáciles de recordar de personalizar su contraseña estándar para diferentes sitios.

2.7 Duplique su protección de inicio de sesión. Habilite la autenticación multifactor (MFA) para asegurarse de que la única persona que tiene el acceso a su cuenta es usted. Úselo para correo electrónico, banca, redes sociales y cualquier otro servicio que requiera iniciar sesión.

2.8 Si MFA es una opción, habilítela usando un dispositivo móvil confiable, como su teléfono inteligente, una aplicación de autenticación o un token seguro: un pequeño dispositivo físico que puede engancharse en su llavero.

2.9 Utilice un administrador de contraseñas para recordar todas sus contraseñas largas. La forma más segura de almacenar todas sus contraseñas es mediante el uso de un administrador de contraseñas. Con solo una contraseña maestra, una computadora puede generar y recuperar contraseñas para cada cuenta que tenga, protegiendo su información en línea, incluidos los números de tarjetas de crédito y sus códigos de valor de verificación de tarjeta (CVV) de tres dígitos, respuestas a preguntas de seguridad y más.

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.