CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de uso del correo electrónico

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 de correo electrónico es garantizar el uso adecuado del sistema de correo electrónico y hacer que los usuarios sean conscientes de lo que se considera como uso aceptable e inaceptable de su sistema de correo electrónico. Esta política describe los requisitos mínimos para el uso del correo electrónico dentro de la Red de la organización.

1.3 Alcance

Esta política cubre el uso apropiado de cualquier correo electrónico enviado desde una dirección de correo electrónico de <Nombre organización> y se aplica a todos los empleados, proveedores y agentes que operan en nombre de <Nombre organización>.

2. Política

2.1 Todo uso del correo electrónico debe ser consistente con las políticas y procedimientos de conducta ética, seguridad, cumplimiento de las leyes aplicables y prácticas comerciales adecuadas.
2.2 No comparta la contraseña de su cuenta de correo electrónico con nadie.
2.3 Utilice la delegación, cuando corresponda, si otro usuario necesita acceso a su correo electrónico.
2.4 No utilice el correo electrónico para acosar a otros.
2.5 No falsifique cuentas de correo electrónico para enviar correos electrónicos como otra persona.
2.6 No inunde / envíe spam a las personas con correo electrónico en un intento de interrumpir su servicio.
2.7 No acepte números de tarjetas de crédito enviados por correo electrónico para fines de pago.
2.8 No cree reglas que permitan el reenvío automatizado a cuentas de correo electrónico que no sean de la institución.
2.9 No envíe datos confidenciales a ninguna parte por correo electrónico sin usar cifrado.
2.10 No utilices direcciones de correo electrónico personales, como Gmail o Yahoo!, para comunicaciones relacionadas con el trabajo.
2.11 La cuenta de correo electrónico debe usarse principalmente para fines institucionales; la comunicación personal está permitida de forma limitada, pero no para usos institucionales relacionados, en este caso están prohibidos.
2.12 Todos los datos contenidos en un mensaje de correo electrónico o un archivo adjunto deben protegerse de acuerdo con el Estándar de Protección de Datos.
2.13 El correo electrónico debe conservarse solo si califica como un registro comercial. El correo electrónico es un registro comercial si existe una razón comercial legítima y continua para preservar la información contenida en el correo electrónico.
2.14 El correo electrónico que se identifica como un registro comercial, se conservará de acuerdo con la Programación de retención de registros.
2.15 El sistema de correo electrónico no se utilizará para la creación o distribución de mensajes perturbadores u ofensivos, incluidos comentarios ofensivos sobre raza, género, color de cabello, discapacidades, edad, orientación sexual, pornografía, creencias y prácticas religiosas, creencias políticas u origen nacional. Los empleados que reciban correos electrónicos con este contenido de cualquier empleado de deberá informar el asunto a su supervisor de inmediato.
2.16 Los usuarios tienen prohibido reenviar automáticamente un correo electrónico a un sistema de correo electrónico de terceros. Los mensajes individuales que son reenviados por el usuario no deben contener información confidencial o superior.

2.17 Los usuarios tienen prohibido utilizar sistemas de correo electrónico y servidores de almacenamiento de terceros como Google, Yahoo y MSN Hotmail, etc. para llevar a cabo un negocio, para crear o conmemorar cualquier transacción vinculante, o para almacenar o retener correo electrónico en nombre de la organización. Dichas comunicaciones y transacciones deben llevarse a cabo a través de los canales adecuados utilizando documentación aprobada.

2.18 El uso de una cantidad razonable de recursos para correos electrónicos personales es aceptable, pero el correo electrónico no relacionado con el trabajo se guardará en una carpeta separada del correo electrónico relacionado con el trabajo. Está prohibido enviar cartas en cadena o correos electrónicos de broma desde una cuenta de correo electrónico de la organización.

2.19 El tamaño de todos los mensajes de correo electrónico salientes y entrantes, incluidos los archivos adjuntos, a **XX** megabytes (MB)

2.20 Cualquier dato considerado como de naturaleza confidencial que deba transmitirse por correo electrónico utilizará cifrado cuando se envíe a través de una red insegura y solo se enviará a destinatarios que tengan una necesidad legítima de la información.

2.21 El correo electrónico enviado dentro de la red interna se considera contenido dentro de un entorno seguro de confianza.

2.22 Aviso de confidencialidad que deberá ir al final de todo correo: *"Aviso de confidencialidad: Esta transmisión de correo electrónico, y cualquier documento, archivo o mensaje de correo electrónico anterior adjunto a ella, pueden contener información confidencial y / o privilegiada y pueden estar legalmente protegidos contra la divulgación. Cualquier revisión, uso, divulgación o distribución no autorizada está estrictamente prohibida. Si usted no es el destinatario previsto, o una persona responsable de entregarlo al destinatario previsto, comuníquese con el remitente por correo electrónico de respuesta y destruya todas las copias del mensaje original, incluidos los archivos adjuntos."*

2.23 La delegación se produce cuando el propietario de una cuenta de correo electrónico (el "delegado") concede permisos a otro usuario ("el delegado") para acceder al correo electrónico, el calendario y/o los contactos del propietario. La delegación no está permitida compartiendo contraseñas o iniciando sesión en la cuenta para que la use el delegado: el delegado debe usar su propia cuenta.

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.