SENCICO
SERVICIO NACIONAL DE CAPACITACIÓN PARA LA INDUSTRIA DE LA CONSTRUCCIÓN

USO DEL CORREO ELECTRÓNICO INSTITUCIONAL Y PLATAFORMA COLABORATIVA

RESOLUCIÓN Nº 167-2024-02.00/SENCICO

Departamento de Informática

AGOSTO 2024

FIRMA DIGITAL
Firmado digitalmente por:
VARAS GRAUS Roger Hector
FAU 20131377810 soft
Motivo: Firmado
Digitalmente
Fecha: 28/08/2024 17:41:42-0500

Firmado digitalmente por
GUERRERO SILVA SOLIS Luis
Martin FAU 20131377810 soft
Motivo: Doy V° B°
Fecha: 28.08.2024 17:59:16 -05:00

<table>
<tr><td rowspan="4">SENCICO</td><td colspan="2">DIRECTIVA</td><td colspan="2">DI/PE/OAF-INF/001-2024</td></tr>
<tr><td colspan="4">USO DEL CORREO ELECTRÓNICO INSTITUCIONAL Y PLATAFORMA COLABORATIVA</td></tr>
<tr><td>Aprobado por:</td><td>Presidencia Ejecutiva</td><td rowspan="2">Fecha de Aprobación:</td><td rowspan="2"></td></tr>
<tr><td>Propuesto por:</td><td>Departamento de Informática</td></tr>
<tr><td>Dejar sin Efecto:</td><td>DI/PE/OPP/007-2015</td><td>Fecha de Publicación:</td><td></td></tr>
</table>

1. OBJETIVO

Establecer los lineamientos para la asignación, administración y uso adecuado del correo electrónico y plataforma colaborativa institucional como instrumentos de comunicación y colaboración interna y externa por parte de todas las dependencias y usuarios que tienen asignada una cuenta por el Servicio Nacional de Capacitación para la Industria de la Construcción – SENCICO.

2. ALCANCE

La presente directiva es de aplicación obligatoria para todas las dependencias y usuarios del servicio de correo electrónico y plataforma colaborativa asignados por el Servicio Nacional de Capacitación para la Industria de la Construcción – SENCICO en los dominios sencico.gob.pe y sencico.edu.pe.

3. VIGENCIA

Esta directiva entra en vigencia a partir de la emisión de la Resolución que la aprueba y su actualización se realiza en función a los cambios o necesidades que surjan en adelante.

4. BASE LEGAL

- Decreto Ley N° 21673, Ley Orgánica de SENCICO.
- Ley N° 27269, Ley de Firmas y Certificados Digitales y Ley N° 27310 que la modifica.
- Ley N° 27291, Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la manifestación de voluntad y la utilización de firma electrónica.
- Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal.
- Ley N° 27444, Ley del Procedimiento Administrativo General y sus modificatorias
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y su modificatoria.
- Ley N° 27815, Ley del Código de Ética de la Función Pública y su reglamento aprobado mediante Decreto Supremo N° 033-2005-PCM.
- Ley N° 28493, Ley que regula el Uso del Correo Electrónico Comercial no Solicitado (SPAM).
- Ley N° 28716, Ley de Control Interno de las Entidades del Estado.
- Ley N° 29733, “Ley de protección de datos personales”.
- Ley 30057, Ley del Servicio Civil.
- Ley N° 30096, Ley de Delitos Informáticos y su modificatoria Ley N° 30171.
- Decreto Legislativo N° 147, Ley de Organización y Funciones del SENCICO.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N° 031-2005-MTC que aprueba el Reglamento de la Ley N° 28493.
- Decreto Supremo N° 052-2008-PCM, reglamento de la Ley de Firmas y Certificados Digitales y sus modificaciones contenidas en el Decreto Supremo N° 070-2011-PCM y en el Decreto Supremo N° 105-2012-PCM.

- Decreto Supremo N° 003-2013-JUS, que aprueba el reglamento de la Ley N° 29733 Ley de Protección de Datos Personales.
- Decreto Supremo N° 033-2018-PCM, que crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital.
- Decreto Supremo N° 029-2021-PCM, Reglamento de la Ley de Gobierno Digital.
- Resolución Jefatural N° 207-2002-INEI, que aprueba la Directiva N° 010-2002-INEI/DTNP, Normas Técnicas para la asignación de nombres de dominio de las entidades en la Administración Pública.
- Resolución Jefatural N° 088-2003-INEI, que aprueba la Directiva N° 005-2003-INEl/DTNP sobre: Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014. Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de seguridad de la información. Requisitos 2da Edición" en todas las entidades integrantes del Sistema Nacional de Informática y su modificatoria.
- Resolución Ministerial N° 119-2018-PCM que dispone la creación de un comité de Gobierno Digital en cada entidad de la Administración Pública.
- Resolución de Secretaría de Gobierno Digital N° 001-2018-PCM/SEGDI, que aprueba los lineamientos para uso de servicios en la nube para entidades de la Administración Pública del Estado Peruano.
- Resolución de Contraloría General N° 320-2006-CG, aprueba Normas de Control Interno.
- Resolución de Presidencia Ejecutiva N° 31-2014-02.00, aprueba la Política del Sistema de Gestión de la Seguridad de la Información del SENCICO.
- Resolución de Presidencia Ejecutiva N° 51-2017-02.00 que aprueba el "Reglamento Interno de Servidores Civiles del SENCICO".
- Resolución de Presidencia Ejecutiva N° 43 - 2021-02.00, que aprueba el Plan de Gobierno Digital del Servicio Nacional de Capacitación para la Industria de la Construcción – SENCICO para el período 2021 – 2023.
- Resolución de Presidencia Ejecutiva N° 52-2021-02.00, que aprueba la Directiva DI/PE/OPP-AL/001-2021, Elaboración, aprobación y difusión de documentos normativos.

5. DEFINICIONES

a) Administrador de correo electrónico y plataforma colaborativa: Es el responsable de crear nuevos usuarios, asignar licencias, distribuir credenciales a nuevos usuarios y administrar y configurar el servicio de correo electrónico y plataforma colaborativa.

b) Antimalware: Software diseñado para detectar, prevenir y eliminar software malicioso o malware de un sistema informático.

c) Antispam: Servicio, aplicación o herramienta informática que ayuda a los usuarios de correo electrónico a restringir la entrada de emails no deseados, previene el ingreso en su bandeja de entrada de "correo basura".

d) Cliente de correo electrónico: Es un programa (software) usado para leer y enviar mensajes de correo electrónico.

e) Contraseña: Combinación de letras, números y signos que deben digitarse para tener acceso al correo electrónico.

f) Cuentas Genéricas: Es una casilla electrónica genérica asignada a cada unidad orgánica, con un responsable asignado, cuya identificación está asociada con su sigla o acrónimo;

debe ser usado solamente para el envío/recepción de documentos relacionados con la actividad que se realiza en la Institución.

g) **CSIRT:** Es el equipo de respuesta a incidentes de seguridad digital del SENCICO.
h) **Doble factor de autenticación:** El doble factor de autenticación se basa en algo que el usuario sabe, como su nombre de usuario y contraseña, y algo que tiene el usuario, como una llave de seguridad, un teléfono inteligente o una aplicación que se ejecuta en su dispositivo móvil.
i) **EDR (Endpoint Detection and Response):** Es una herramienta que proporciona monitorización y análisis continuo del dispositivo final (computadora, smartphone, laptop, entre otros) para mitigar amenazas cibernéticas maliciosas complejas.
j) **Envió Masivo:** Remisión de mensaje de correo electrónico dirigido a más de 20 destinatarios de dominios externos.
k) **Hotspot:** o "punto caliente» es un lugar que ofrece acceso a Internet a través de una red inalámbrica y un enrutador conectado a un proveedor de servicios de Internet. Los hotspots se encuentran en lugares públicos, como aeropuertos, bibliotecas, centros de convenciones, cafeterías, hoteles, etc.
l) **Machine Learning**: El machine learning es un subconjunto de la inteligencia artificial (IA) donde las computadoras aprenden a partir de los datos y mejoran con la experiencia sin ser programadas explícitamente.
m) **Malware**: Un término genérico que se refiere a cualquier software que tiene una intención maliciosa, ya sea obvia u oculta; tales como: los virus, gusanos, caballos de troya, rootkits, ransomware, etc. capaz de causar daños o alteraciones al sistema operativo, archivos u otros componentes de computadoras y redes informáticas.
n) **Mesa de Servicios de TI**: Servicio de soporte informático que brinda el Departamento de Informática a los usuarios de la institución. Cuenta con hardware y software que facilita la resolución de problemas.
o) **Phishing:** Es una técnica de ciberdelincuencia que utiliza el fraude, el engaño y el timo a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio para manipularla con la finalidad que realice acciones indebidas y/o revele información confidencial.
p) **Plataforma colaborativa:** Es una herramienta compuesta por procedimientos y componentes tecnológicos en la que se habilita a los usuarios la capacidad de relacionarse y colaborar en entornos digitales utilizando videoconferencias, mensajería instantánea, llamadas por internet, edición en línea de documentos, compartir archivos, almacenamiento, entre otros.
q) **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información, por medio de un conjunto de medidas técnicas, organizativas y legales.
r) **Servicio de Correo Electrónico:** Es un servicio que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante sistemas de comunicación electrónica. Permite enviar también archivos adjuntos al mensaje. Es una herramienta de comunicación e intercambio de información oficial entre personas, no es una herramienta de difusión indiscriminada de información, excepto las listas de grupos de distribución de mensajes de correo establecidos por la institución para sus propios fines.
s) **Software:** Componentes lógicos de programas y rutinas que permiten a un computador realizar determinadas tareas.
t) **Spam**: Se llama spam o correo basura a los mensajes no solicitados, no deseados o de remitente desconocido y que son sumamente molestos. Por lo general, las direcciones remitentes son: robadas, compradas, recolectadas en la web o tomadas de cadenas de mail. Muchos de estos mensajes vienen infectados de virus, gusanos y caballos de Troya.
u) **Usuario:** Persona que utiliza el correo electrónico y la plataforma colaborativa del SENCICO para fines laborales.

6. ABREVIATURAS

a) **EDR:** Endpoint Detection and Response.
b) **SEGDI:** Secretaría de Gobierno y transformación Digital.

7. RESPONSABILIDAD

7.1. DEPARTAMENTO DE INFORMÁTICA

7.1.1. El Departamento de Informática es responsable de la administración del servicio de correo electrónico y plataforma colaborativa institucional, está facultado para adoptar las medidas necesarias para garantizar la seguridad y privacidad del mismo.

7.1.2. Por recomendación de la SEGDI, el Departamento de Informática utilizará sistemas o programas de bloqueo y/o filtro para la recepción o transmisión de mensajes de correo no deseado o malware que se efectúe a través del servicio. Estas medidas son complementarias a las tomadas por el proveedor de servicio de correo Office 365.

7.1.3. Es el responsable de informar a la Oficina de Administración y Finanzas el incumplimiento de la presente directiva en caso sea detectado.

7.2. DEPARTAMENTO DE RECURSOS HUMANOS

7.2.1. Es el responsable de comunicar al Departamento de Informática dentro de las 72 horas de aceptados sean los ceses, renovaciones y traslados del personal que trabaja en el SENCICO.

7.2.2. Es el responsable de mantener actualizado el sistema interno de personal, para fines relacionados a la presente directiva.

7.2.3. Es el responsable de fomentar programas de capacitación y entrenamiento permanente en el uso del correo electrónico institucional y plataforma colaborativa.

7.3. OFICINA DE SECRETARIA GENERAL

7.3.1. Es el responsable de definir el uso del logo institucional para todo tipo de comunicación interna y/o externa.

7.4. USUARIO

7.4.1. Cumplir con las disposiciones señaladas en la presente directiva. En caso de incumplimiento se le suspenderá el servicio de correo electrónico y plataforma colaborativa, además de aplicársele las sanciones administrativas, conforme a los dispositivos legales vigentes sin perjuicio de las responsabilidades civiles y/o penales a que hubiera lugar.

7.4.2. El usuario es responsable de preservar la confidencialidad de la cuenta de acceso al correo electrónico y plataforma colaborativa.

7.4.3. El usuario se hará responsable de todas las actividades que se realicen con la cuenta asignada por la institución.

7.4.4. El usuario del servicio de correo electrónico y plataforma colaborativa institucional que accede al mismo fuera de las instalaciones del SENCICO y dentro del territorio nacional, debe hacerlo desde un equipo que cumpla con los niveles de seguridad adecuados (antimalware y sistema operativo actualizados y vigentes) así como evitar el acceso desde cabinas públicas y hotspots gratuitos.

7.4.5. El usuario que se va a conectar al servicio de correo electrónico y plataforma colaborativa fuera del Perú deberá notificarlo por medio del correo electrónico a csirt@sencico.gob.pe indicando el país desde el cual accederá a estos servicios con un día de anticipación, de lunes a viernes entre las 8:30 am y 5:15 pm. En caso contrario, se procederá con el bloqueo de la cuenta una vez producida la detección del acceso anómalo, para minimizar el riesgo de compromiso de la misma.

7.4.6. El usuario es responsable de salvaguardar su información (copia de respaldo) del servicio de correo electrónico y plataforma colaborativa. En el Anexo N° 04, se encuentran las instrucciones para realizar la copia de respaldo del correo electrónico.

7.4.7. En relación a las cuentas genéricas y las asignadas a los locadores de servicio, la responsabilidad de salvaguardar la información de correo electrónico y plataforma colaborativa recae en el responsable del área.

7.5. RESPONSABLE DEL ÁREA USUARIA

7.5.1. Es el responsable de tomar las previsiones necesarias en el caso de que el personal a su cargo salga de vacaciones, tome licencias, en caso de ceses/bajas, teniendo en cuenta que la solicitud de acceso, interceptación o intervención de la información de correo electrónico de cualquier usuario está supeditada al inciso 10 del artículo 2 de la Constitución Política del Perú, así como a lo dispuesto a la normativa vigente sobre la materia.

7.5.2. Es el responsable de comunicar la reasignación y/o finalización de uso de las cuentas genéricas asignadas a su dependencia que están bajo su responsabilidad.

8. DISPOSICIONES GENERALES:

8.1. DEL SERVICIO DE CORREO ELECTRÓNICO Y PLATAFORMA COLABORATIVA

8.1.1. El sistema de correo electrónico y plataforma colaborativa institucional proporciona al usuario los siguientes servicios:

- Envío y recepción de correo electrónico.
- Herramientas de plataforma colaborativa integradas como: plataforma unificada de comunicación y colaboración (Teams), servicio de alojamiento de archivos (OneDrive), Herramienta para la gestión documental y trabajo en equipo (SharePoint), herramienta para la creación de encuestas y cuestionarios con marcado automático (forms), etc.

8.1.2. El SENCICO no es responsable de lo que se haga o escriba a través de una cuenta de correo electrónico institucional.

8.1.3. El servicio de correo electrónico y plataforma colaborativa son de uso oficial y para fines estrictamente laborales en la institución.

8.1.4. La gestión y administración del servicio de correo electrónico y plataforma colaborativa institucional, está a cargo del Departamento de Informática del SENCICO.

8.1.5. El buzón de correo electrónico del SENCICO no es un repositorio de almacenamiento de archivos. Es responsabilidad del usuario eliminar los archivos y/o mensajes periódicamente de acuerdo a su criterio de utilidad considerando el límite máximo con el cual cuenta su buzón.

8.2. DE LAS POLITICAS DE PRIVACIDAD Y USO ACEPTABLE DEL PROVEEDOR DEL SERVICIO

8.2.1. El proveedor de servicio garantiza la privacidad de las cuentas de correo electrónico y plataforma colaborativa institucional de todos los usuarios sin excepción. La política de privacidad del servicio se encuentra en https://privacy.microsoft.com/es-es/privacystatement.

8.2.2. También se tiene una política de uso aceptable del correo electrónico publicadas en http://www.microsoft.com/online/legal/v2/?langid=es-es&docid=12, las cuales deben ser cumplidas por los usuarios del servicio, así como las contenidas en la presente directiva.

8.2.3. Los detalles de la protección de los datos alineada a los de la privacidad del servicio de correo electrónico y plataforma corporativa se pueden leer en https://www.microsoft.com/es-ww/trust-center/privacy?langid=es-es&docid=12.

8.3. DEL ACCESO Y SEGURIDAD DEL SERVICIO DE CORREO ELECTRÓNICO Y PLATAFORMA COLABORATIVA

8.3.1. La cuenta de correo electrónico y plataforma colaborativa asignada a los usuarios, es suministrada con el fin de servir como medio de comunicaciones, colaboración interna con proveedores, clientes y terceros para actividades exclusivamente de uso oficial y para fines estrictamente laborales de la institución.

8.3.2. El usuario del servicio de la cuenta de correo electrónico y plataforma colaborativa podrá acceder al mismo mientras esté vinculado con la institución. Se accede a la cuenta de correo electrónico y plataforma colaborativa a través del software cliente y/o a través de su portal de acceso web.

8.3.3. En el caso de que se requiera brindar acceso a terceros (locadores de servicios), se otorgará el acceso contemplando las limitaciones y permisos que las áreas contratantes les permitan, en razón a la naturaleza de las actividades para las cuales han sido contratados, lo cual deberá estar taxativamente previsto en los términos de referencia de su contratación. Los accesos se solicitarán obligatoriamente mediante el sistema “Solicitud de accesos de servicios de red y aplicaciones” en https://formatof4.sencico.gob.pe.

8.3.4. El servicio de correo electrónico y plataforma colaborativa cuenta con capacidades de filtrado de malware, phishing y spam. Complementariamente, se cuenta con una solución de seguridad del correo electrónico y plataforma colaborativa basada en machine learning como una capa adicional de protección contra estas amenazas.

8.3.5. El EDR se integra al software cliente, correo electrónico y plataforma colaborativa, realizando una inspección a cada uno de los mensajes y archivos recibidos o enviados para minimizar el riesgo de envío/recepción de malware que ponga en riesgo la integridad de la información o imagen del SENCICO.

8.3.6. La plataforma colaborativa cuenta con protección antimalware, por lo que los archivos compartidos en ella son inspeccionados y en el caso de detectarse malware son eliminados y/o puestos en cuarentena.

8.3.7. Los servicios proporcionados por la plataforma colaborativa se activan cuando se crea la cuenta de correo electrónico principal del usuario.

9. DISPOSICIONES ESPECÍFICAS

9.1. Altas, bajas y bloqueos de cuentas de correo electrónico y plataforma colaborativa

9.1.1. El responsable del órgano o unidad orgánica al que pertenece el usuario, debe solicitar la creación de una cuenta de correo electrónico y plataforma colaborativa, mediante el sistema "Solicitud de accesos de servicios de red y aplicaciones" en https://formatof4.sencico.gob.pe.

9.1.2. Para el caso de cuentas de correo electrónico genéricas y plataforma colaborativa asignadas a los contratistas, a las oficinas y servicios, siempre se asignará un responsable de la cuenta. En caso no se indique el responsable, se asignará al solicitante.

9.1.3. Para dar de baja a la cuenta de correo electrónico y plataforma colaborativa de un usuario, se seguirá los siguientes lineamientos:

a) En el caso del personal DL 728, DL 276, DL 1057 (CAS) y practicantes, la baja se realizará después de la comunicación del cese por parte del Departamento de Recursos Humanos.

b) En el caso del personal contratado por órdenes de servicio, al término de la prestación del servicio registrado en el sistema "Solicitud de accesos de servicios de red y aplicaciones".

c) En el caso de cuentas genéricas y de servicios, mediante la comunicación del responsable de la dependencia que la solicitó.

d) En todos los casos anteriores, luego de 30 días de efectuada la baja, el Departamento de Informática eliminará de forma automática la cuenta de usuario de Correo y Plataforma colaborativa, sin posibilidad de recuperar la información eliminada; por lo tanto, el responsable del área al cual pertenecía el usuario cesado deberá haber tomado las previsiones del caso.

9.1.4. Cuando un jefe o gerente sea reemplazado, el funcionario saliente entregará, como parte de su entrega de cargo, la lista de cuentas genéricas y de servicios de su dependencia al funcionario entrante y éste a su vez, para mantener la confidencialidad de la misma, solicitará el cambio de clave a la Mesa de Servicios del Departamento de Informática (anexo 2222).

9.1.5. El Departamento de Informática, a través del CSIRT, bloquea las cuentas de correo electrónico y plataforma colaborativa de manera excepcional y con la evidencia técnica de la vulneración/compromiso de dichas cuentas. A los usuarios cuyas cuentas de Microsoft 365 (Correo, OneDrive, SharePoint, Teams) hayan sido comprometidas ("hackeadas"), se les activará el doble factor de autenticación. El primer factor es la contraseña y el segundo factor puede ser un mensaje SMS a su número de celular o la aprobación con el aplicativo Microsoft Authenticator el cual puede ser descargado de Play Store de Android o app store de Apple.

9.2. Contraseñas de correo electrónico y plataforma colaborativa

9.2.1. Los usuarios que tienen asignada una cuenta de correo electrónico y plataforma colaborativa institucional, deberán mantener en secreto su contraseña para que no pueda ser utilizada por otra persona.

9.2.2. Como parte de la política de seguridad del SENCICO, el cambio de contraseña se debe realizar cada 90 días. También se recomienda cambiar las contraseñas siempre que el usuario sospeche que la confidencialidad de su contraseña pueda estar comprometida o vulnerada y debe informar al Departamento de Informática para efectuar el análisis correspondiente.

9.2.3. El formato y sintaxis de cada contraseña queda establecido bajo los siguientes lineamientos de formato, tamaño, número de caracteres y tiempo de vida:

a) Longitud mínima de 10 caracteres.

b) Combinación mínima obligatoria de letras mayúsculas, letras minúsculas, números y mínimo un carácter especial.

c) Vigencia de 90 días, al término de los cuales se forzará el cambio de contraseña.

Las contraseñas no deben ser palabras comunes o simples variaciones del nombre del trabajador, usuario, nombre de la computadora, servidor o empresa. Por ejemplo, una contraseña fuerte puede ser: 23Libre$Alfin. En el Anexo N° 03, se muestran las buenas prácticas para generación de contraseñas robustas

9.2.4. Al crearse cada cuenta de correo electrónico y plataforma colaborativa, se establece una contraseña temporal, la cual es forzada a cambiarse por el sistema luego del primer inicio de sesión. El usuario elige la contraseña con el formato y sintaxis indicados en esta directiva y asume la responsabilidad sobre la confidencialidad de su contraseña desde ese momento y cada vez que la renueve.

9.2.5. Para casos donde se requiera cambiar una contraseña por pérdida u olvido de la misma, el usuario podrá solicitarlo directamente a la Mesa de Servicios de TI (anexo 2222) del Departamento de Informática, quienes deberán reconfirmar la identidad del usuario solicitante, con el apoyo del personal que conozca directamente la identidad del usuario solicitante.

9.3. Nombre de la cuenta de correo electrónico y plataforma colaborativa

9.3.1. Para la creación del nombre de una cuenta de correo electrónico y plataforma colaborativa para la parte administrativa se utilizará el siguiente estándar: Primera letra del nombre de pila del usuario seguido inmediatamente del apellido paterno ligado por el símbolo "@" al nombre del dominio sencico.gob.pe. En caso de existir dos construcciones de cuenta de usuario similares, se añadirán progresivamente las letras del apellido materno hasta establecer la diferencia. Por ejemplo:

Nombre del usuario: Nombres Apellidos

Nombre de cuenta de correo electrónico: napellido@sencico.gob.pe

9.3.2. Para la creación del nombre de una cuenta de correo electrónico y plataforma colaborativa para la parte educativa (alumnos y profesores), se utilizará el siguiente estándar: Un número autogenerado no repetitivo de 8 dígitos ligado por el símbolo "@" al nombre del dominio sencico.edu.pe. Por ejemplo:

Nombre del alumno: Nombres Apellidos

Nombre de cuenta de correo electrónico: 12345678@sencico.edu.pe

9.3.3. Para la creación de cuentas de correo electrónico genéricas, se deberá consignar mediante el sistema "Solicitud de accesos de servicios de red y aplicaciones", aparte del responsable, la fecha de vencimiento de la misma. Solo se habilitarán las licencias para el funcionamiento del correo electrónico.

9.3.4. Para la creación de cuentas de correo electrónico de los locadores de servicio, el nombre estándar se designará según la información proporcionada por el sistema "Solicitud de accesos de servicios de red y aplicaciones".

Se crea de la siguiente manera:

1. Las 4 primeras letras (como máximo) que identifica al departamento y/o Gerencia Zonal y/o unidad operativa y/o Centro de formación. Para el caso de la Sede Central se obviará el nombre del departamento de Lima.
2. Seguido por un número de dos dígitos

Ejemplos:
abasXX@sencico.gob.pe
tesoXX@sencico.gob.pe
trujXX@sencico.gob.pe
aqpXX@sencico.gob.pe
tiXX@sencico.gob.pe

9.4. Nombre de los grupos, repositorios o equipos de trabajo de la plataforma colaborativa

9.4.1. Para la creación de los nombres de grupos, repositorios o equipos de trabajo en la plataforma colaborativa, se sigue el siguiente estándar:

- Las 3 o 4 primeras letras identifican a la dependencia: Ejemplos: ABAS, TESO, OPP, etc.
- Los siguientes caracteres identifican la finalidad de las actividades, funciones u objetivos del grupo.

9.5. Lectura de Correo

9.5.1. Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben mantener en línea el software de correo electrónico y activada la opción de avisar cuando llegue un nuevo mensaje, o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes, ya que es un medio de comunicación oficial.

9.5.2. En el caso que el usuario reciba un mensaje de correo electrónico, de un remitente que no pertenezca a la entidad y que lo considere inapropiado, debe solicitar a administrador@sencico.gob.pe, la inclusión de la cuenta de correo electrónico del remitente en la lista negra.

9.5.3. Corresponde al usuario la liberación de sus mensajes de correo electrónico puestos en cuarentena por la plataforma de seguridad del correo electrónico y plataforma colaborativa, teniendo en cuenta que dichos mensajes se eliminarán de manera automática en 30 días a partir de la recepción de la notificación de la cuarentena y no se podrán recuperar. Una guía para la liberación de los mensajes se muestra en el Anexo N° 01.

9.6. Envío del correo

9.6.1. En la redacción de mensajes nuevos es de carácter obligatorio utilizar el campo “asunto”. Se sugiere consignar el tema del mensaje a fin de que el receptor pueda identificar rápidamente de qué trata el mensaje. Si se envía en blanco no se garantiza la transmisión del mensaje.

9.6.2. Evitar el uso generalizado de letras mayúsculas porque se puede interpretar que el remitente está alzando la voz.

9.6.3. Evite usar las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, ya que esto afecta la capacidad de almacenamiento del buzón de correo electrónico del remitente.

9.6.4. Evite enviar mensajes a listas globales, a menos que sea un asunto oficial que involucre a todos los miembros de la lista global.

9.6.5. Los correos electrónicos a los cuales se adjunten documentos que no han sido creados por el remitente, deberán citar siempre la fuente de origen y/o los autores, con la finalidad de respetar los derechos de propiedad intelectual.

9.6.6. Evitar el envío de correos electrónicos que contengan la contraseña de sus cuentas de usuario, de producirse el caso, el usuario podrá solicitar el cambio de contraseña a serviciosti@sencico.gob.pe.

9.6.7. El tamaño de los archivos, adjuntos a los mensajes de correo electrónico, es de 5 MB para las listas de distribución de correos y 35 MB para las cuentas de correo asignadas a un usuario. Se sugiere, para archivos más grandes de 5 MB, copiarlos en el OneDrive y enviar el enlace por correo electrónico.

9.6.8. Existen restricciones para el envío de archivos adjuntos a los mensajes de correo electrónico. En el Anexo N° 02 se listan las extensiones de archivos no permitidas.

9.6.9. Los mensajes de correo electrónico enviados después del horario de trabajo, se considerarán enviados al siguiente día útil.

9.7. Autofirmas

9.7.1. La firma debe ser breve e informativa a fin de que el receptor del mensaje permita identificar al autor del mismo.

9.7.2. No incluir la dirección de correo en la firma, porque ésta ya fue incluida de manera automática en la parte superior del mensaje.

9.7.3. La firma de correo electrónico debe considerar el Logo de SENCICO, nombre el usuario, área al que corresponde, teléfono-anexo, número de celular asignado, de la siguiente manera:

9.8. Vigencia de los mensajes y características de los buzones

9.8.1. Los mensajes tendrán una vigencia no mayor de 180 días desde la fecha de entrega o recepción de los mismos, o de acuerdo a la política establecida por el Departamento de Informática. Superada la fecha de vigencia, los mensajes deberán ser eliminados del servidor de correo. En caso se requieran conservar los mensajes, se debe guardar en carpetas personales externas al gestor de correo electrónico.

9.8.2. Los buzones de correo electrónico tienen un tamaño máximo de 50 GB, lo cual también es afectado por la capacidad de gestión del cliente de correo electrónico que al tener un tamaño de buzón de 2 GB empieza a presentar problemas de lentitud en la carga de mensajes. Es recomendable mantener el tamaño del buzón a menos de 2 GB (tamaño del archivo *.pst).

9.9. Mal uso del correo electrónico

9.9.1. El usuario debe conocer la diferencia de utilizar cuentas de correo electrónico institucionales y cuentas privadas ofrecidas por otros proveedores de correo electrónico.

9.9.2. Se considera como mal uso del correo electrónico institucional las siguientes actividades:

a) Utilizar el correo electrónico institucional para propósitos fraudulentos, comerciales, políticos, publicitarios, difamatorios, racistas, obscenos y/o distintos a los fines laborales.
b) Participar en la propagación de mensajes encadenados o en esquemas piramidales o similares.
c) Distribuir mensajes con contenidos impropios y/o lesivos a la moral.
d) Utilizar mecanismos y/o sistemas que intenten ocultar o suplantar la identidad del emisor de correo.
e) Utilizar el correo electrónico institucional para recoger los mensajes de correos de otro proveedor de correo.
f) Todo lo que constituya complicidad con hechos delictivos, por ejemplo: apología del terrorismo, uso y/o distribución de software que no haya sido adquirido por SENCICO o cuya distribución no esté autorizada o información protegida por derechos de autor, todo tipo de pornografía, amenazas, estafas, malware o código hostil en general, entre otros.
g) Hacer uso del servicio del correo electrónico para realizar envío masivo hacia cuentas de correo externas, teniendo en cuenta que el servicio de correo electrónico no es un servicio dedicado de mailing. En caso de incumplimiento por primera vez será suspendido por 15 días, por segunda vez por 30 días y por tercera vez se suspenderá definitivamente la cuenta de correo electrónico.
h) Enviar información o documentos clasificados y contraseñas o datos que puedan afectar la seguridad de los activos institucionales o violen las leyes del Estado Peruano.
i) Utilizar el correo electrónico para enviar información tipificada como datos personales y/o datos sensibles por la Ley N.º 29733, "Ley de protección de datos personales".
j) Facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas.
k) Enviar mensajes comprometiendo la seguridad de la información o la imagen de la institución.
l) Remitir mediante el correo electrónico, material protegido por leyes de derechos de autor o poner dicho material a disposición de otros para ser copiado.
m) Acceder a enlaces desconocidos o de fuentes no confiables recibidos por correo electrónico.
n) Difundir por correo electrónico y plataforma colaborativa documentos que contengan información confidencial sin contar con la autorización correspondiente.

9.9.3. El Departamento de Informática, suspenderá el servicio de correo electrónico al usuario que realice mal uso del mismo, además se le aplicará las sanciones administrativas, conforme a los dispositivos legales vigentes sin perjuicio de las responsabilidades civiles y/o penales a que hubiera lugar.

9.10. Uso de la plataforma colaborativa

9.10.1. Los usuarios, en coordinación con su dependencia, agendan sus reuniones de trabajo, crean sus grupos de trabajo y gestionan toda la información almacenada y generada en sus repositorios de la plataforma colaborativa.
9.10.2. Las reuniones pueden ser grabadas directamente por el usuario que la ha agendado. Antes de iniciar la grabación, se deberá informar a los asistentes que la reunión será grabada. Estas grabaciones se almacenan en la plataforma colaborativa y pueden ser accedidas o descargadas de acuerdo a los permisos que les otorgue el usuario autorizado. El usuario y su dependencia son los únicos responsables del acceso o difusión de la grabación de sus reuniones. La grabación será almacenada en la plataforma por 30 días, luego serán eliminadas.

9.10.3. El uso de los servicios proporcionados por la plataforma colaborativa es única y exclusivamente para fines institucionales y no debe ser utilizada para fines personales.

9.10.4. No está permitida la copia de instaladores de software y/o ejecutables en los repositorios de la plataforma colaborativa.

10. ANEXOS

Anexo N° 01: "Guía de liberación de mensajes de correo electrónico puestos en cuarentena por la solución de seguridad del correo electrónico y plataforma colaborativa"

Anexo N° 02: Extensiones de archivos no permitidas

Anexo N° 03: Buenas prácticas para crear contraseñas robustas

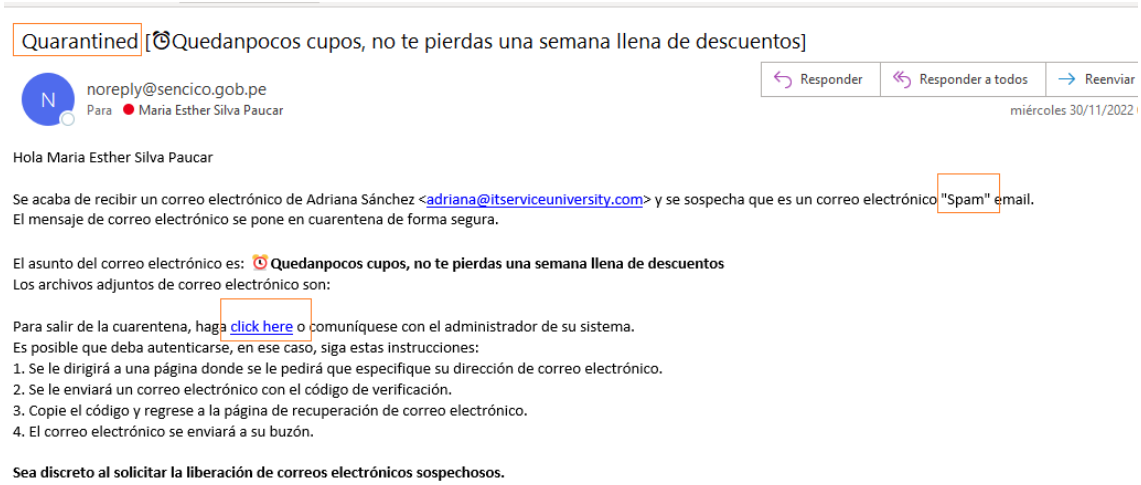
Anexo N° 04: Instructivo para hacer copia de seguridad del correo electrónico

Anexo N° 01: “Guía de liberación de mensajes de correo electrónico puestos en cuarentena por la solución de seguridad del correo electrónico y plataforma colaborativa”

A: **Cuarentena CASO SPAM**

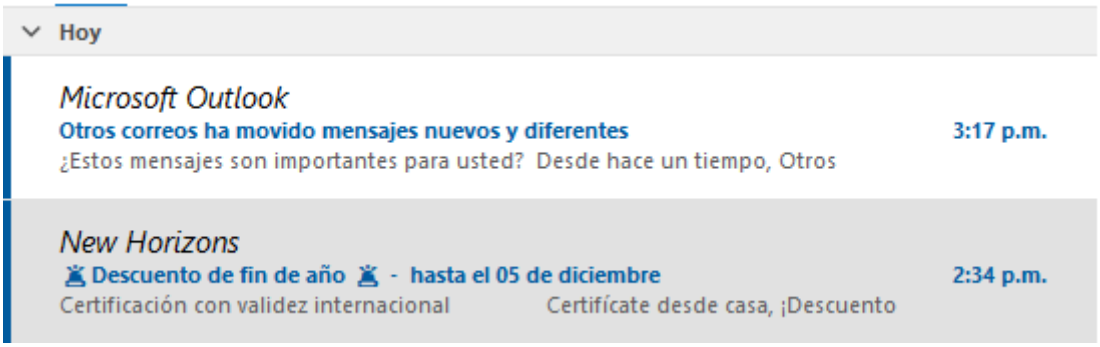
1. Recibirá el mensaje de correo electrónico indicando que el mensaje ha sido puesto en cuarentena por sospecha de ser un mensaje del tipo **Spam**:

2. Revise cuidadosamente el cuerpo del mensaje en el cual se identifican al remitente, el asunto del mensaje y los adjuntos (de existir). Si considera que el mensaje es de su contacto y es esperado, haga click en el enlace “**Click here**” para restaurarlo de la cuarentena.



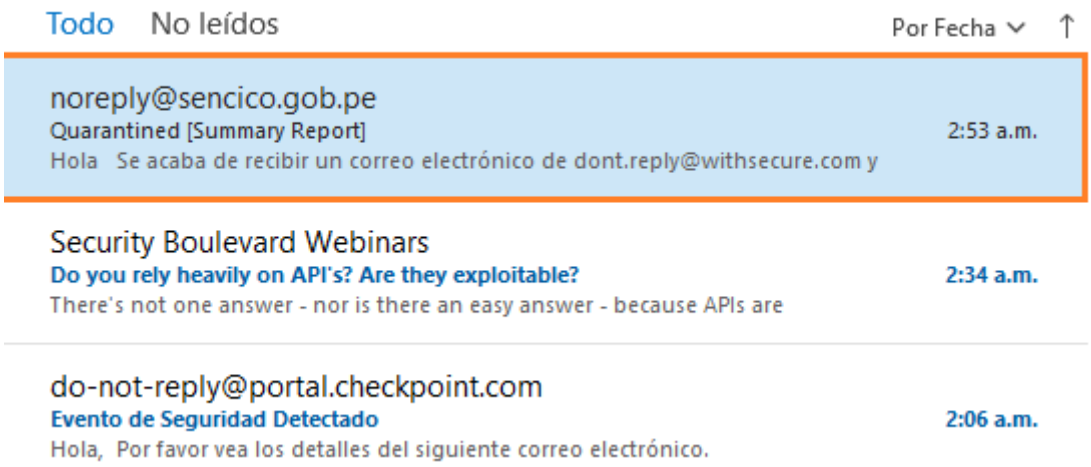
3. Al hacer clic en el enlace, se abrirá una página web en el browser en la cual se le comunica que se su mensaje ha sido restaurado exitosamente.

4. El mensaje de aviso de cuarentena desaparecerá de su buzón de correo y el mensaje original se visualizará en la bandeja en la que habitualmente lo recibe.

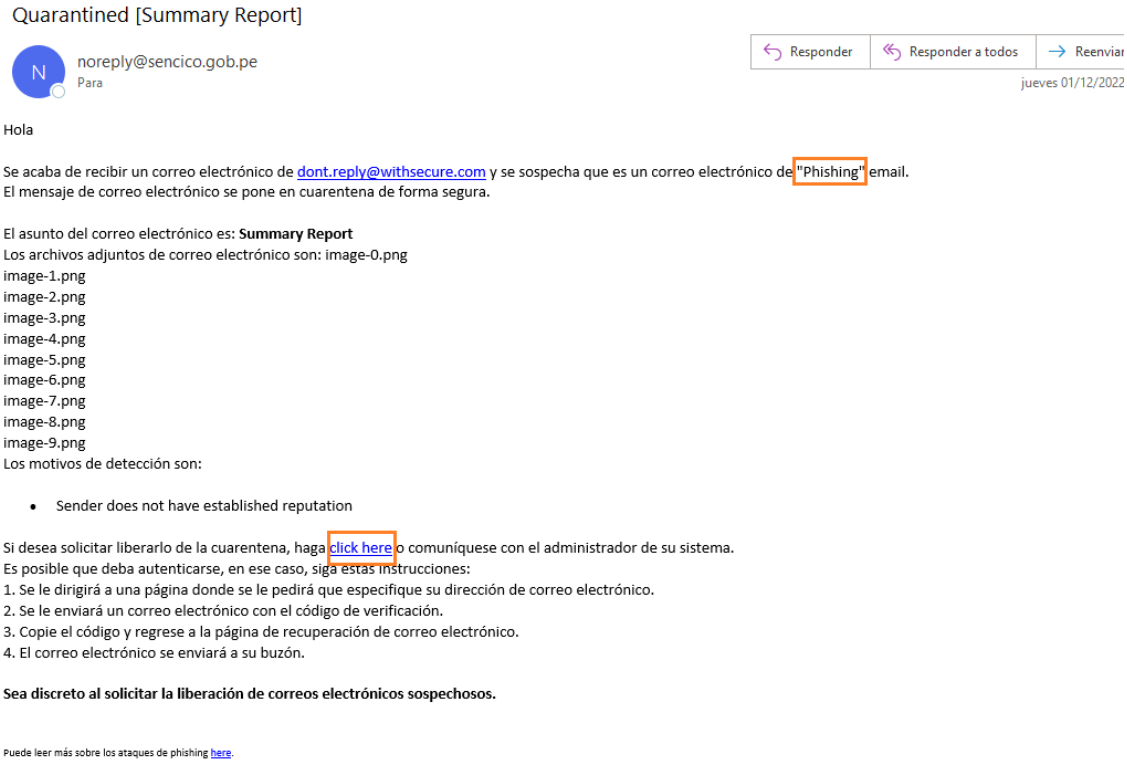


B: **Cuarentena CASO PHISHING**

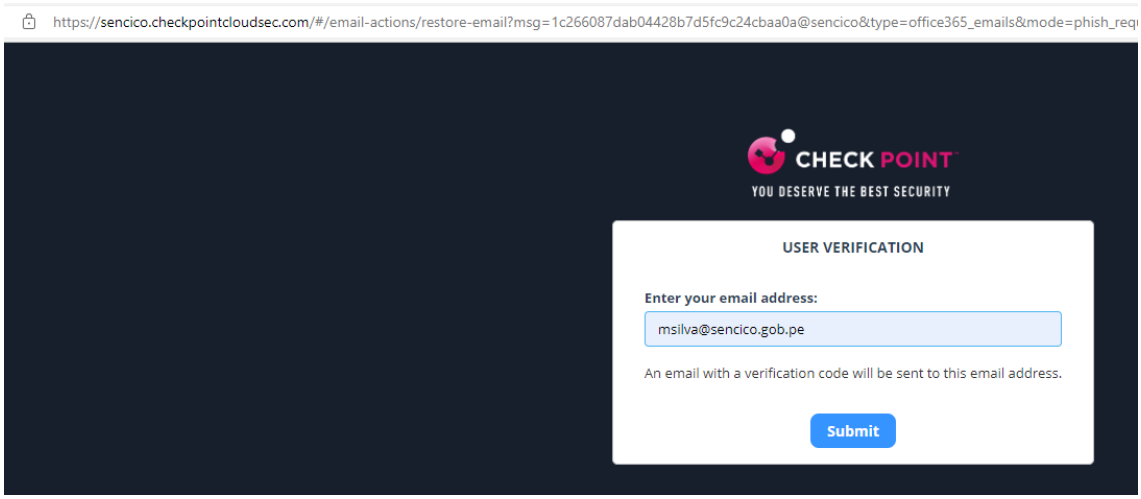
1. Recibirá el mensaje de correo electrónico indicando que el mensaje ha sido puesto en cuarentena por sospecha de ser un mensaje del tipo **Phishing**:



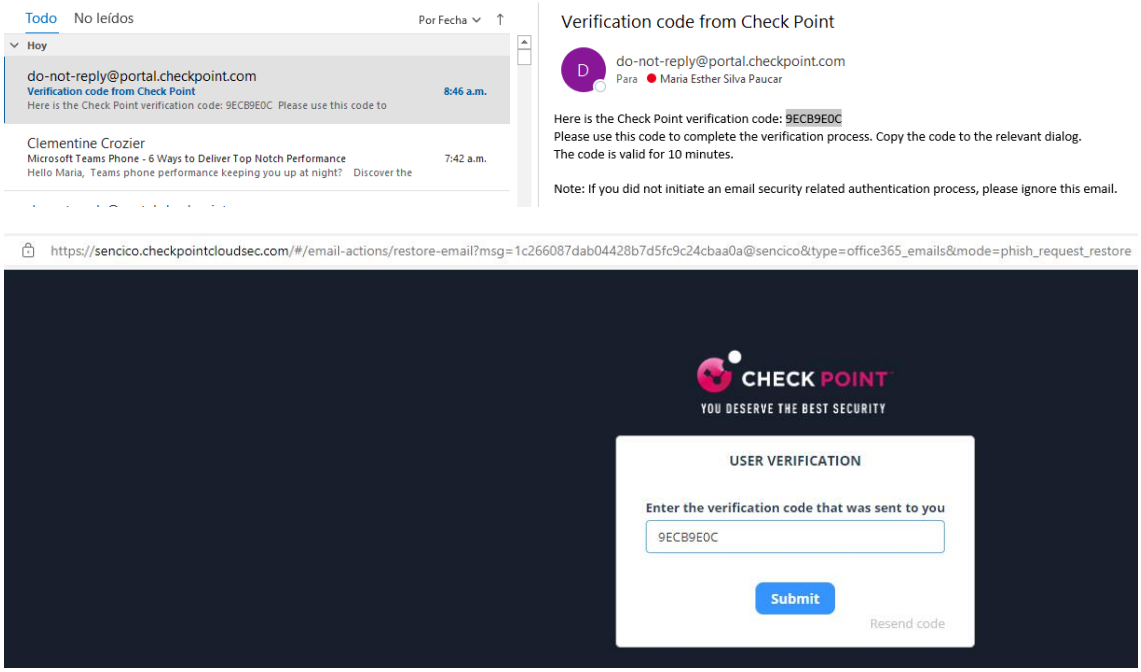
2. Revise cuidadosamente el cuerpo del mensaje en el cual se identifican al remitente, el asunto del mensaje y los adjuntos (de existir). Si considera que el mensaje es de su contacto y es esperado, haga click en el enlace "**Click here**" para solicitar la restauración desde la cuarentena.



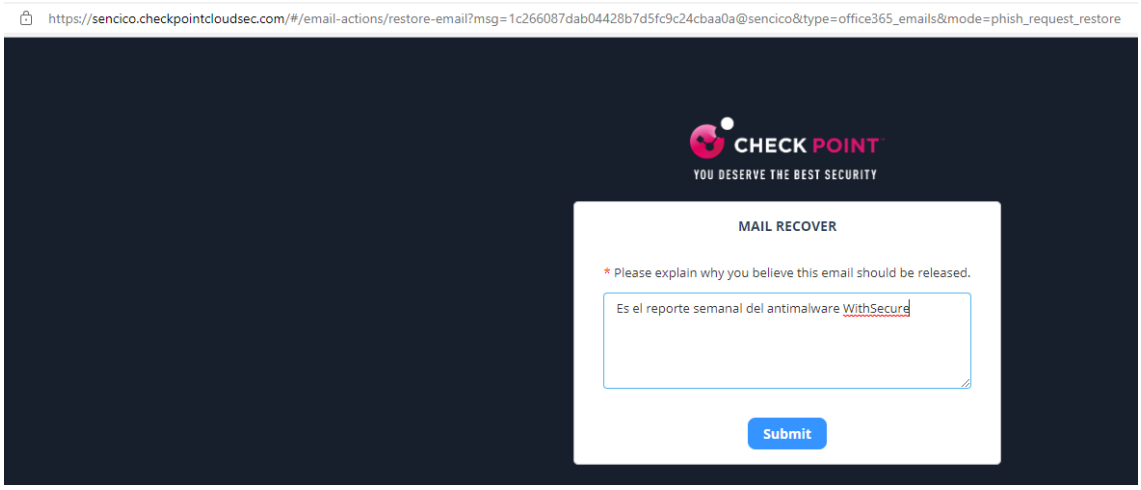
3. Al hacer clic en el enlace, se abrirá una página web en el browser en la cual se le solicitará su dirección de correo electrónico SENCICO y se le comunica que se enviará un código de verificación, digítela y haga clic en el botón "**Submit**".



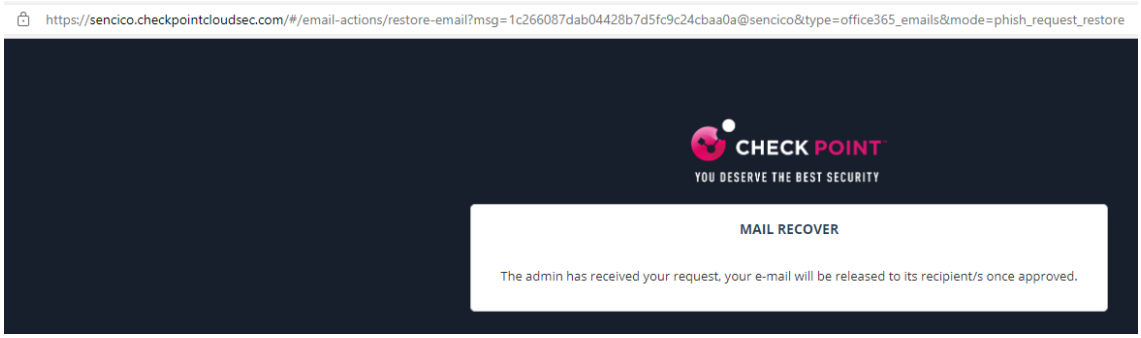
4. Revise su buzón de correo electrónico y verifique la recepción del código de verificación, cópielo y péguelo en la ventana de "**USER VERIFICATION**"



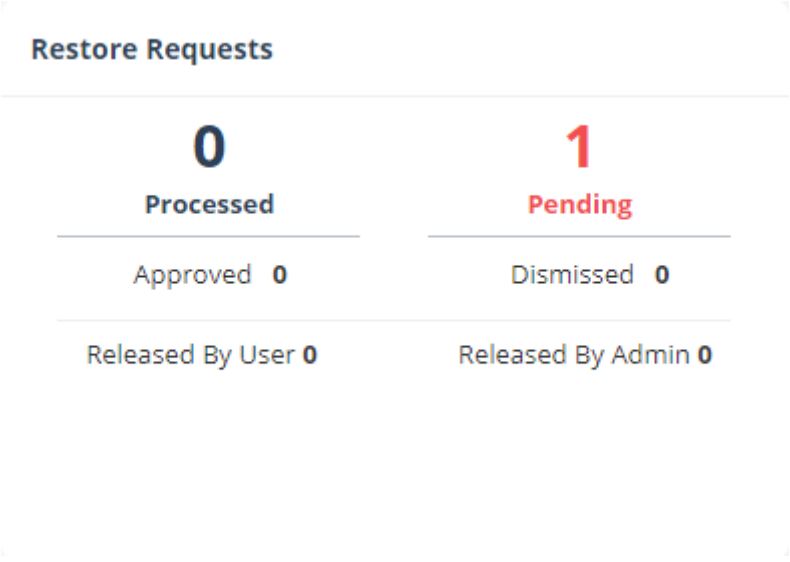
5. Ingrese el motivo por el cual está solicitando la liberación del mensaje del estado de cuarentena y haga clic en el botón “**SUBMIT**”.

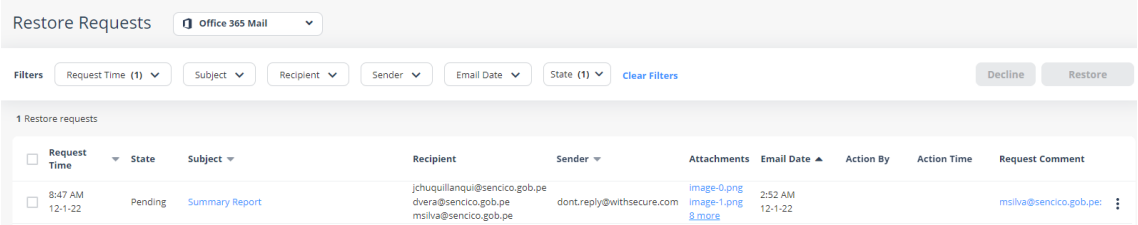


6. Recibirá la notificación de que el requerimiento ha sido enviado al administrador de la plataforma de seguridad del correo electrónico.

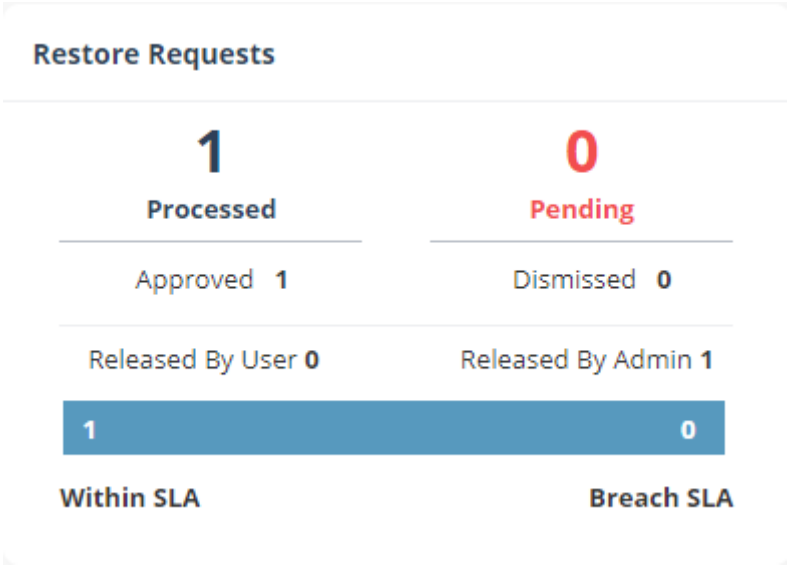


7. El administrador de la plataforma de seguridad del correo electrónico verificará su pedido en la lista de requerimientos de restauración.





8. Luego del análisis del motivo por el cual el mensaje fue puesto en cuarentena y de los riesgos e indicadores de compromiso que califiquen al mensaje como confiable y sin riesgo de comprometer la cuenta de correo y/o la información institucional, el administrador de la plataforma de seguridad del correo electrónico procederá con la restauración del mismo.



9. El mensaje de aviso de cuarentena desaparecerá de su buzón de correo y el mensaje original se visualizará en la bandeja en la que habitualmente lo recibe.

Anexo N° 02: Extensiones de archivos no permitidas

*.ace	*.ani	*.apk	*.app	*.appx	*.arj	*.bat
*.cmd	*.com	*.cpl	*.crt	*.deb	*.dex	*.dll
*.docm	*.dos	*.elt	*.exe	*.hta	*.img	*.jar
*.js	*.kext	*.lha	*.lib	*.library	*.lnk	*.lzh
*.macho	*.msc	*.msi	*.msix	*.msp	*.mst	*.pif
*.ppa	*.ppam	*.ps1	*.reg	*.rev	*.scf	*.scr
*.sct	*.sys	*.uif	*.vb	*vbe	*.vbs	*.vxd
*.wsc	*.wsf	*.wsl	*.xll	*.xz	*.z	

Anexo N° 03: Buenas prácticas para crear contraseñas robustas

Usar al menos 15 caracteres: Crear **contraseñas largas, de al menos 15 caracteres** (siempre que sea posible), minimiza el riesgo de que un ciberdelincuente consiga acceder a tus dispositivos y cuentas. Las contraseñas cortas son más fáciles de descifrar. La longitud de una contraseña es uno de los factores más críticos para proteger contraseñas frente a ataques de fuerza bruta.

Nunca usar información personal: También es importante evitar que las contraseñas sean fáciles de adivinar. N**o utilizar información personal** —como la ciudad de nacimiento, el cumpleaños, números de teléfono o direcciones, nombres de familiares o mascotas. E**vitar el uso de palabras reales** —como nombres propios o palabras del diccionario— para impedir que los ciberdelincuentes puedan descifrar tus contraseñas usando software malicioso.

Combinar letras, números y símbolos: Combina de forma aleatoria letras en mayúscula, letras en minúscula, números y símbolos para crear contraseñas más seguras. Además, también es recomendable:

- Evitar el uso de secuencias de números o letras, como «123456», «abcdef» o «qwerty».
- Evitar el uso de sustituciones habituales, como podría ser reemplazar «CONTRASEÑA» por «C0NT8A53ÑA».
- Elige símbolos que no se suelen usar como las llaves {}, los corchetes [] o los paréntesis ().

Elegir las primeras iniciales en una frase: Crear contraseñas largas y complejas suena bien, pero acordarnos de todas ellas puede resultar todo un reto. Así que, un truco para crear contraseñas seguras, y fáciles de recordar, es coger las letras iniciales de una frase que tenga algún significado personal.

Por ejemplo: «Mi primer viaje a Japón con Marta en mayo de 1990 fue inolvidable».

De modo que la contraseña sería: «MpvaJcMemd1990fi».

Este método se conoce como «**el método de la frase**» o «**el método Bruce Schneier**».

Usar un gestor de contraseñas: Teniendo en cuenta la gran cantidad de cuentas y dispositivos que usamos, crear y gestionar contraseñas complejas y largas puede resultar verdaderamente abrumador. Así que, **usar un gestor de contraseñas para generar contraseñas más fuertes y guardarlas de forma segura** puede ser de gran ayuda. Asimismo, los gestores de contraseñas suelen sugerir contraseñas robustas al crear nuevos inicios de sesión. Para generar contraseñas fuertes, **también puedes usar un generador de contraseñas aleatorias**. Además, algunos de los navegadores más populares actualmente incluyen herramientas de gestión de contraseñas y generación de contraseñas seguras.

Nunca reutilizar o duplicar contraseñas: Nunca reutilices la misma contraseña para diferentes inicios de sesión. Esto es sumamente importante cuando se trata de proteger cuentas o dispositivos que guardan información sensible.

Usar la autenticación de dos factores: Siempre que sea posible, **usa la autenticación de dos factores**, también conocida como autenticación de múltiples factores, para proteger aún más tus cuentas. La autenticación de múltiples factores añade una capa de protección adicional.

Conocer las técnicas para hackear contraseñas: Estar informado sobre los métodos que usan los ciberatacantes para acceder a una cuenta o dispositivo también es útil. Al entender cómo se hackean las contraseñas, es más fácil comprender las buenas prácticas a seguir para crear contraseñas seguras. Los ciberdelincuentes usan diversas técnicas para hackear contraseñas:

- **Ataques de fuerza bruta**. Consiste en un método de «ensayo y error». Los ciberatacantes introducen todas las contraseñas posibles hasta encontrar una que funcione.
- **Ataques de diccionario**. Consiste en probar todas las palabras del diccionario para descifrar una contraseña.
- **Ataques de tablas *Rainbow* o tablas arcoíris**. Consiste en usar listas de consulta con combinaciones de contraseña junto con sus valores *hash* correspondientes.
- **Estafas de *phishing***. Consiste en engañar, intimidar o presionar a un usuario para que haga algo mediante ingeniería social.

Cambiar contraseñas de forma periódica: No es necesario cambiar las contraseñas todos los meses, pero modificarlas con cierta regularidad es una buena técnica para **estar siempre un paso por delante de los ciberatacantes**.

Buenas prácticas adicionales para proteger contraseñas

Usar una VPN al conectarse a redes Wi-Fi públicas: Es recomendable usar una VPN para asegurarse de que nadie pueda interceptar las credenciales al conectarse a una red pública.

Elegir preguntas de seguridad difíciles de adivinar: También es recomendable elegir preguntas de seguridad que sean difíciles de adivinar al registrarse en una nueva web o aplicación. Además, es importante asegurarse de que la respuesta a la pregunta de seguridad no se pueda encontrar en medios sociales.

No compartir contraseñas con nadie: Por último, pero no menos importante —y aunque pueda parecer obvio—, **no hay que compartir contraseñas con nadie**, ni siquiera con familiares.

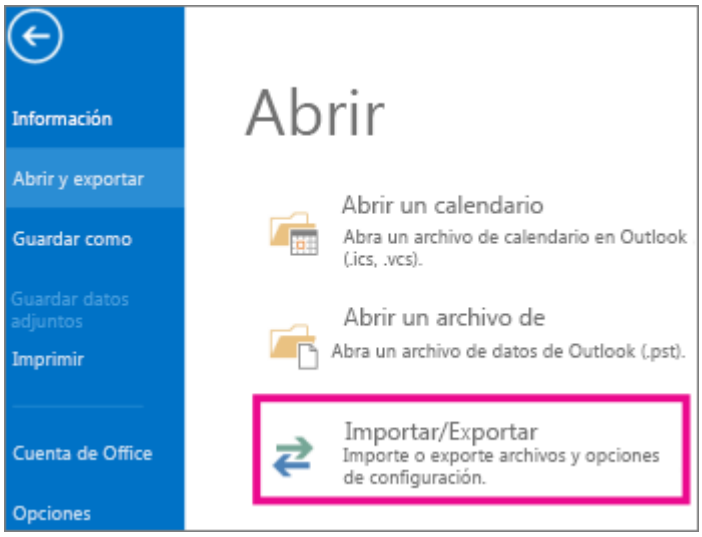
No permitir que el navegador almacene las contraseñas: Si estás visitando una página web por vez primera y creando una contraseña, el navegador pedirá autorización para almacenar su contraseña.

Si bien esto suena bien en teoría, no lo es realmente. Para las empresas que desarrollan navegadores, el enfoque principal no es la seguridad de sus clientes, sino la usabilidad y el obtener más clientes. Es por eso que sus contraseñas no estarán seguras con ellos.

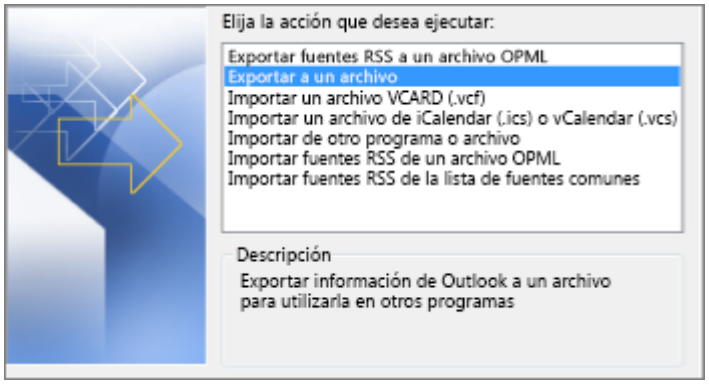
FUENTE: https://www.stackscale.com/es/blog/buenas-practicas-contrasenas-seguras/

Anexo N° 04: Instructivo para hacer copia de seguridad del correo electrónico

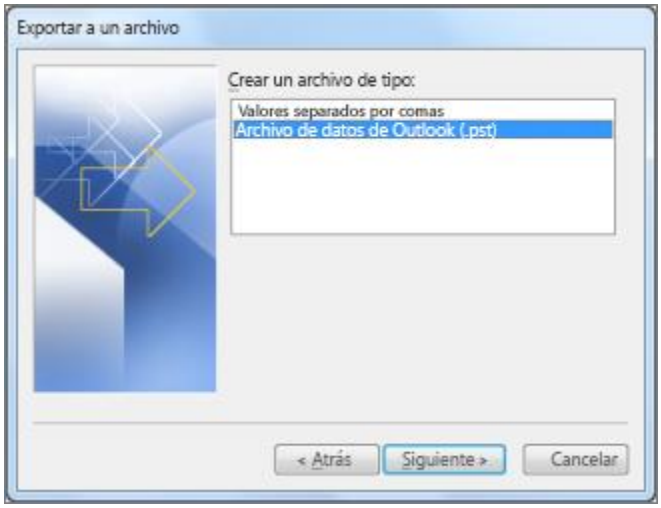
1. Si desea hacer copia de seguridad local de las carpetas de mensajes (además de mantenerlos en el servidor), puede mover o eliminar automáticamente los elementos más antiguos con Archivar automáticamente o exportar los elementos a un archivo .pst que puede restaurar y usar más tarde, si es necesario, con una importación.
2. Seleccione Archivo > Abrir y exportar > Importar o exportar, como se muestra a continuación:



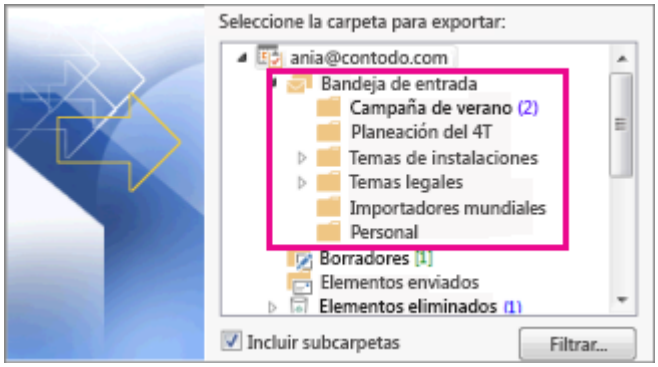
3. Seleccione Exportar a un archivo y luego Siguiente.



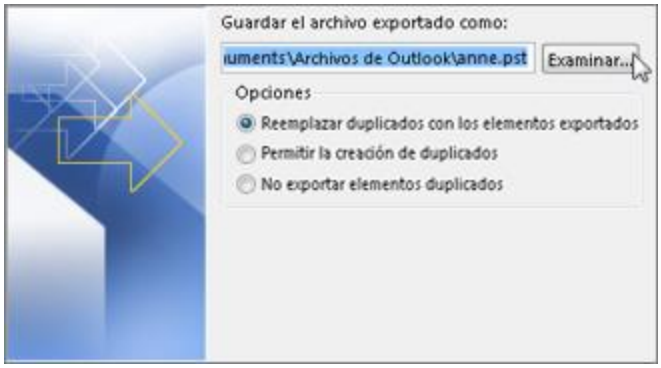
4. Seleccione Archivo de datos de Outlook (.pst) y Siguiente.



5. Seleccione todas las carpetas de correo de las que quiere hacer una copia de seguridad y haga clic en Siguiente.



6. Elija una ubicación y un nombre para el archivo de copia de seguridad y luego seleccione Finalizar.



7. Si quiere asegurarse de que nadie tenga acceso a sus archivos, introduzca y confirme una contraseña y luego seleccione Aceptar.
8. La copia de seguridad lo puede resguardar en una memoria USB, disco duro u otro medio de almacenamiento.
9. Realizar la copia de seguridad periódicamente; por lo menos, una vez al año.

FUENTE:

https://support.microsoft.com/es-es/office/hacer-copia-de-seguridad-del-correo-electr%C3%B3nico-e5845b0b-1aeb-424f-924c-aa1c33b18833#:~:text=Seleccione%20Archivo%20%3E%20Abrir%20y%20exportar,y%20haga%20clic%20en%20Siguiente

https://support.microsoft.com/es-es/topic/importar-el-correo-electr%C3%B3nico-los-contactos-y-el-calendario-desde-un-archivo-pst-de-outlook-431a8e9a-f99f-4d5f-ae48-ded54b3440ac