LINEAMIENTOS DE SEGURIDAD PARA

CUENTAS GUBERNAMENTALES

INTRODUCCIÓN

En el presente documento, encontrarás lineamientos y recomendaciones para cuidar la seguridad, datos e información de las cuentas gubernamentales de redes sociales. Además, conocerás los **riesgos más comunes** de estas plataformas.

Si bien solemos enfocar los esfuerzos de nuestras estrategias en el contenido y alcance de este, la seguridad digital es fundamental, pues **su vulneración podría provocar el uso de parte de externos para compartir información falsa o engañosa, o atribuirse la vulneración de sistemas institucionales,** generando un tremendo impacto comunicacional y de imagen.

Les recordamos que las redes sociales son un bien institucional y su resguardo es responsabilidad de quienes tengan asignado su manejo en las diferentes instituciones. Así, atendido lo dispuesto en dictamen E545210N24, de CGR, tanto la pérdida de acceso a sus redes sociales o su uso indebido puede dar lugar a un procedimiento disciplinario.

RIESGOS DE SEGURIDAD MÁS COMUNES

Existen distintos tipos de riesgos que pueden ser internos y externos:

INTERNOS

- **Cuentas y dispositivos con riesgo de que puedan ser vulneradas**: filtración de claves, falta de autenticación multifactor y mecanismos de alerta en caso de acceso no convencional, entre otros.

EXTERNOS

- Enlaces engañosos y estafas.
- Cuentas impostoras.
- Ataques cibernéticos e incidentes de ciberseguridad.

RIESGOS DE SEGURIDAD MÁS COMUNES

Internos - Cuentas con baja seguridad

Este riesgo se puede originar por contraseñas poco seguras, por compartirlas y por la ausencia de dos pasos de seguridad. Es por esto que:

Crea contraseñas seguras:

- Usa palabras o frases aleatorias.
- Agrega símbolos y letras.
- Utiliza letras en mayúsculas y minúsculas.
- No uses información personal (dirección, cumpleaños, nombres de mascotas, RUT, etc).
- No repitas tus claves.

***Cambia tus claves si:** fueron filtradas, perdiste tu dispositivo, las compartiste con un tercero o las ingresaste en un sitio web sospechoso.

MANEJO DE CONTRASEÑAS

No escribas las contraseñas en documentos compartidos ni archivos personales. Tampoco en agendas, papeles u otro medio analógico.

Recomendamos en lugar de lo anterior usar un gestor de contraseñas como Bitwarden (que es gratis para uso personal) o 1password (pagado y fácil de usar) para **generar contraseñas aleatorias**.

La contraseña maestra de estos gestores de contraseña puede ser una “passphrase” (frase creada juntando 4 o 5 palabras aleatorias, por ejemplo. El sitio www.palabrasaleatorias.com entrega sugerencias para ello).

RIESGOS DE SEGURIDAD MÁS COMUNES

Internos - Dispositivos con baja seguridad

Las cuentas institucionales deben ser manejadas en dispositivos que sean destinados exclusivamente para este uso. Por lo tanto, estos equipos deben tener seguridad propia mediante contraseñas que cumplan con las siguientes características:

- **Para dispositivos móviles: PIN** de 6 dígitos o más mediante desbloqueo manual; se recomienda tecnología de desbloqueo biométrico (facial o dactilar). No inicies sesión de cuentas personales en el mismo dispositivo en que usas redes sociales laborales, pues corres el riesgo de confundir contenido entre ambas.

- **Para dispositivos de escritorio:** Contraseñas memorizables (puede ser con “passphrase”) de 8 caracteres mínimo. No accedas a cuentas laborales (institucionales o de autoridad) en equipos que puedan ser utilizados por terceros.

Cualquier duda relacionada con la seguridad de tus dispositivos, comunícate con el encargado de seguridad de la información de tu ministerio.

VERIFICACIÓN EN DOS PASOS Y AUTENTICACIÓN DE GOOGLE

Habilita la verificación en dos pasos, registrando el mail y teléfono de la institución, así como mail y teléfono de recuperación.

La autenticación en dos pasos puede centralizarse en el Google Authenticator, además de tener activados los otros métodos.

El Autenticador de Google agrega una capa adicional de seguridad a tus cuentas en línea mediante un segundo paso de verificación cuando accedes a tu cuenta. Esto significa que, además de la contraseña, también deberás **ingresar un código generado por la app del Autenticador de Google en el teléfono.**

El código de verificación puede ser generado **aunque no tengas conexión de red o móvil.**

- Instala la aplicación en **un sólo dispositivo móvil. Procura que sea de la institución,** no personal de algún funcionario.

- En configuración, habilita la **pantalla de privacidad** para mayor seguridad. Así, requerirás el PIN del dispositivo o el acceso biométrico para acceder a la app con los códigos.

VERIFICACIÓN EN DOS PASOS Y AUTENTICACIÓN DE GOOGLE

Si pierdes tu teléfono, te recomendamos lo siguiente:

- **Sal de tu cuenta**

Tu cuenta de Google > Seguridad > Tus dispositivos > Gestionar todos los dispositivos >
Selecciona el dispositivo > Cerrar sesión.
*También puedes cerrar todas las sesiones asociadas al nombre de ese dispositivo.

Cambia la contraseña de tu Cuenta de Google

Seguridad > Contraseña > Cambiar Contraseña.

Existen diferentes formas de volver a acceder a la cuenta según las circunstancias. Conócelas aquí.

Si necesitas el código de verificación para entrar a tu cuenta, **utiliza otro método de autenticación en dos pasos,** como correo electrónico.

A través de cada plataforma, vincula un nuevo dispositivo al Google Authenticator.

RIESGOS DE SEGURIDAD MÁS COMUNES

Externos - Enlaces engañosos, fraudulentos y estafas

Desconfía de cualquier mensaje que recibas de remitentes desconocidos.

Ten cuidado con los links en redes sociales, aunque parezcan de fuentes confiables. Muchas veces son publicidad que se hace pasar por instituciones conocidas para robar datos bancarios o credenciales.

Cuidado al instalar extensiones en el navegador. Ojalá instalar solamente 2: la del gestor de claves y un bloqueador de anuncios como uBlock para evitar campañas de publicidad maliciosa.

Comunícate con el encargado de seguridad de la información de tu institución en caso de dudas o posibles alertas.

RIESGOS DE SEGURIDAD MÁS COMUNES

Externos - Cuentas impostoras

Por otra parte, es posible que encuentres cuentas que suplanten a tu autoridad, a tu cartera o busquen usar recursos comunicacionales del gobierno para parecer auténticos. Ante este escenario, **debes informar al encargado de seguridad de la información de tu ministerio y al sectorialista de Secom Digital.**

Cabe destacar que si bien desde Secom Digital se pueden reportar estos casos, el ministerio a cargo también puede hacerlo a través de plataforma de Meta. La eliminación de estas cuentas no está garantizada y puede tomar varios días una vez ingresada la solicitud. Secom puede **dar urgencia y prioridad** a estas solicitudes de manera interna entendiendo el escenario político que prime en dicho momento.

CHILE
AVANZA
CONTIGO