RECOMENDACIONES 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.

Es posible que muchas veces enfoquemos los esfuerzos de nuestras estrategias en el contenido y alcance de éste, sin embargo, el cuidado de las cuentas es fundamental ya que sirven como una herramienta de primera línea en la comunicación con las personas. El arriesgar la seguridad de una cuenta **podría frenar temporal o indefinidamente** la publicación de los contenidos y por consecuencia, obstaculizar la comunicación.

RIESGOS DE SEGURIDAD MÁS COMUNES

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

INTERNOS

- Cuentas institucionales con baja seguridad
- Dispositivos con baja seguridad

EXTERNOS

- Enlaces engañosos, fraudulentos y estafas
- Cuentas impostoras
- Ataques cibernéticos y hacks

RIESGOS DE SEGURIDAD MÁS COMUNES

Internos - Cuentas institucionales con baja seguridad

Este riesgo se origina por dos motivos principales: contraseñas poco seguras y ausencia de dos pasos de seguridad. Es por esto que:

1. **Las contraseñas deben ser cambiadas todos los meses** y ser respaldadas en un documento que bajo ningún motivo, puede estar disponible en la red (Drive, Dropbox, sitios web, etc). Una buena extensión de caracteres para una contraseña es de 12 a 14 y pueden ser generador en esta web: LastPass.

2. Además, es importante sumar una segunda capa de seguridad al ingresar a una cuenta, conocido comúnmente como **autenticación de dos pasos**. Recomendamos el autenticado de Google, aquí encontrarás un paso a paso.

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 tantos estos equipos deben tener seguridad propia mediante contraseñas que cumplan con las siguientes características:

- **Para dispositivos móviles:** 4 a 6 dígitos mediante desbloqueo manual, se recomienda tecnología de desbloqueo facial. En dichos dispositivos, si se guarda el ingreso automático a cuentas institucionales, el dispositivo no debe registrar acceso a cuentas personales.

- **Para dispositivos de escritorio:** Contraseñas de 8 caracteres mínimo en equipos no compartidos. Si se guardan los accesos en el llavero del equipo o del navegador, el equipo debe contar con software de detección de virus, malware, entre otros.

Cualquier duda relacionada con la seguridad de tus dispositivos, comunícate con el equipo de TI de tu cartera.

RIESGOS DE SEGURIDAD MÁS COMUNES

Externos - Enlaces engañosos, fraudulentos y estafas

Cualquier mensaje vía WhatsApp o correo electrónico que recibas de remitentes desconocidos, con asuntos que apelen a la **seguridad de tus cuentas o información confidencial** tanto de cuentas institucionales como de asuntos políticos, es una alerta que debes considerar.

Todo hipervínculo que no provenga desde una fuente confiable (información oficial de plataformas como Meta, Google o X o directamente de tu sectorialista) puede considerarse como **potencialmente engañoso o fraudulento**.

Te recomendamos no abrir enlaces de mensajes que contengan faltas de ortografía, redacción poco clara y enlaces con estructuras confusas. Comunícate con tu sectorialista 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 comunicarte con tu sectorialista** ya que éste es el puente entre plataformas como Meta y X, entre otros.

Es importante entender que la eliminación de estas cuentas no está garantizada y puede tomar varios días una vez ingresada la solicitud. Desde Secom podemos **dar urgencia y prioridades** a estas solicitudes de manera interna entendiendo el escenario político que prima en dicho momento.

RIESGOS DE SEGURIDAD MÁS COMUNES

Externos - Ataques cibernéticos y hacks

Si tus cuentas son vulneradas, te recomendamos reportar inmediatamente al Departamento Digital de Secom, para dar urgencia a la recuperación de éstas y reestablecer su configuración de seguridad con ayuda de los equipos internos de cada plataforma.

Con los pasos explicados anteriormente, el **riesgo de amenazas** se reduce de forma importante.

Gobierno de Chile

gob.cl