



¿Por qué es importante?

En la Universidad de Aysén trabajamos a diario con información crítica: datos personales de estudiantes y funcionarios, notas, proyectos, correos, sistemas de gestión y documentos administrativos. Muchos de estos datos son sensibles y están protegidos por ley.

Una filtración, pérdida o acceso no autorizado puede afectar el desarrollo normal de nuestras funciones, dañar la confianza institucional e incluso generar sanciones legales. Por eso, proteger la información no es solo una buena práctica: es una responsabilidad de toda la comunidad universitaria.

La seguridad de la información es un pilar estratégico para asegurar la continuidad, reputación y sostenibilidad de la Universidad. Implementar buenas prácticas y participar activamente en este esfuerzo colectivo nos permite prevenir incidentes, cumplir la normativa y construir una cultura de protección y mejora continua.

Objetivo

Queremos asegurar que la información:

- Solo sea vista por las personas autorizadas.
- Se mantenga correcta y sin cambios no permitidos.
- Esté disponible cuando se necesite.



● Lo que debes saber y aplicar

Tu rol como personal administrativo, de apoyo o académico:

- Cumple con las políticas y buenas prácticas que entrega la universidad.
- Participa en las capacitaciones o charlas sobre seguridad digital.
- Informa de inmediato si ves algo sospechoso al correo: osi@uaysen.cl

Uso correcto de los recursos digitales (TIC)

Los computadores, redes, correos y sistemas que entrega la universidad son para uso institucional, es decir, para trabajar, hacer clases o tareas propias de la universidad.

¿Qué incluye?

- Computadores, notebooks, impresoras, proyectores, cámaras.
- Sistemas como correo institucional, Drive institucional, software que usamos.
- Internet y redes dentro de la universidad.

Reglas básicas:

- No compartas tus claves ni prestes tu computador con sesión abierta.
- No uses los recursos de la universidad para negocios personales o cosas ajenas al trabajo.
- Guarda tus archivos importantes en Google Drive institucional o en los espacios autorizados.
- Cierra sesión y cuida tus equipos al terminar tu jornada.

Reglas para proteger la información

Contraseñas

- Elige claves difíciles (usa letras, números y símbolos).
- Cámbialas regularmente.
- No se las digas a nadie.

Programas y virus

- Instala solo lo que necesitas para trabajar o hacer clases.
- Descarga solo desde sitios oficiales (nunca uses software pirata).
- No uses programas raros o que no entiendas sin consultar al equipo TI.
- No actives servidores o páginas web sin permiso del área técnica.

Si ves algo extraño

Si recibes un correo sospechoso, si tu computador anda mal o detectas que hay archivos perdidos, avisa de inmediato al OSI: ✉ osi@uaysen.cl

- También puedes informar a la **Dirección de Administración y Finanzas**.

Correo institucional

- Úsalo solo para temas de la universidad.
- Si tienes que enviar información sensible (ej. con RUTs, notas o datos personales), pide apoyo si no sabes cómo protegerla.
- No hagas clic en enlaces raros o de personas desconocidas.

Navegación segura

- No entres a páginas con contenido inadecuado o ilegal desde el trabajo.
- Usa Internet solo para cosas propias de tu función.

Lo que está prohibido

- Tratar de “entrar” a sistemas sin permiso.
- Instalar programas que no estén autorizados.
- Levantar páginas, correos o servidores sin pedir ayuda al área TI.

Mantente informado

- Participa en las capacitaciones que se te inviten.
- Mantente atento/a a las orientaciones que comparta la Universidad sobre seguridad de la información.

Reglas para proteger la información

Escritorio limpio y cuidado de papeles

- Guarda bajo llave si es posible, cualquier documento con datos confidenciales (como listas de estudiantes, datos personales, notas, contratos, etc.).
- No dejes papeles con datos personales a la vista si no estás en tu escritorio.
- Destruye o tritura los documentos que ya no necesites y que tengan información sensible.

¿Qué hacer ante un incidente?

Si ves algo que no te parece normal, como:

- Un correo raro que pide tu clave,
- Archivos borrados o movidos sin explicación,
- Acceso a tu computador sin permiso,

Comunícalo de inmediato al **Oficial de Seguridad de la Información**, al correo: osi@uaysen.cl

La seguridad es tarea de todos

Cuidar la información no es solo trabajo del área de informática. Todas y todos debemos ayudar a proteger los datos y sistemas que usamos en la universidad.

¿Dónde está la política completa?

Puedes leer la versión oficial publicada en el sitio web de la universidad, en la sección “**Actos y Resoluciones**”, bajo Resolución Exenta N°368 de 2024.

Resolución Exenta N°368

(Aprueba política general de seguridad de la información de la Universidad de Aysén)

