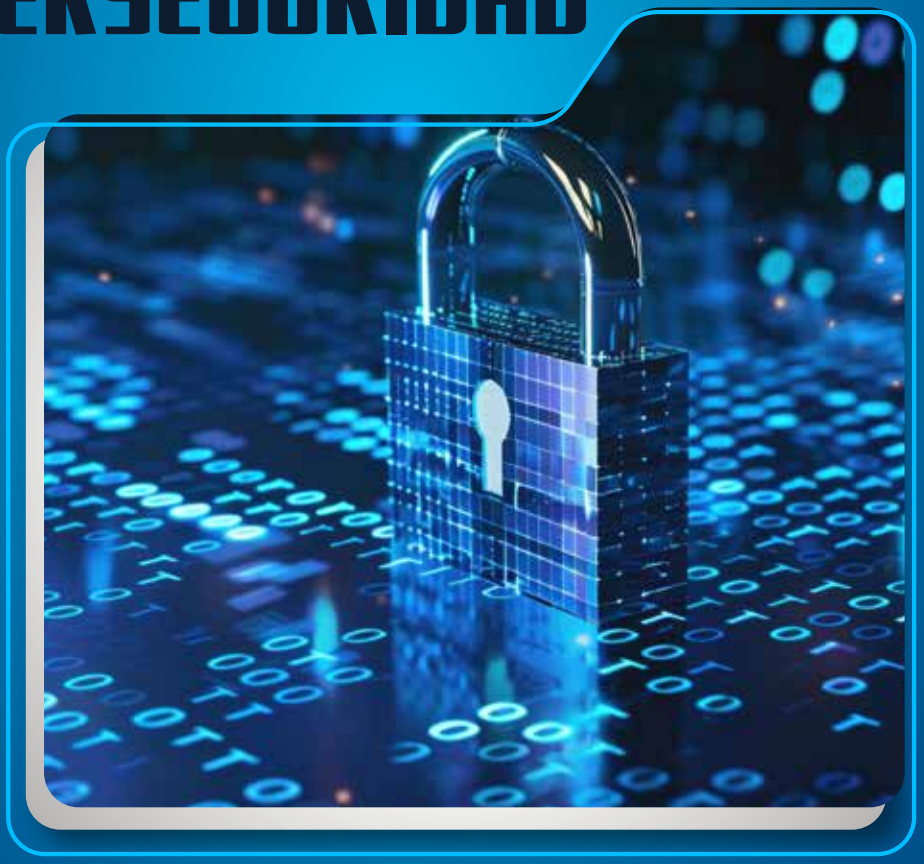
UNIVERSIDAD DE LA FRONTERA
DIRECCIÓN DE INFORMÁTICA

DESARROLLO Y
TRANSFORMACIÓN
VRAF - UFRO DIGITAL

BUENAS PRÁCTICAS EN CIBERSEGURIDAD

RTSIC



RTSIC: *Reglamento Técnico de Seguridad de la Información y Ciberseguridad*

Dirección de Informática / Universidad de La Frontera

dinfo.ufro.cl/ Dinfo UFRO Dirección de Informática UFRO

CIBERSEGURIDAD

¿Qué son ?

Son técnicas o herramientas que velan por la seguridad de los usuarios que comparten información de la Universidad en internet o entre sistemas que transitan por dicha red. Con ellas se busca proteger los sistemas, redes y datos digitales.

GLOSARIO TECNOLÓGICO

Sistemas y aplicaciones:
programas informáticos diseñados para tareas específicas, como Intranet, campus virtual, Gmail, entre otros. Las aplicaciones también se conocen como APP.

¿Por qué son importantes?

Para proteger la información confidencial:
Evitar el robo o la exposición de datos sensibles de estudiantes, académicas, académicos y del personal.

Para mantener la integridad de los sistemas:
Prevenir la manipulación no autorizada de sistemas y aplicaciones.

Para garantizar la disponibilidad de recursos:
Asegurar que los servicios digitales estén disponibles cuando se necesiten, sin interrupciones por ataques o incidentes de seguridad informática.

BUENAS PRÁCTICAS EN CIBERSEGURIDAD

Contraseñas seguras

Elige contraseñas variadas y robustas.

- Combina el uso de letras mayúsculas, minúsculas, números y símbolos.
- Utiliza una contraseña con mínimo 7 caracteres.
- No guardes contraseñas en equipos que no sean personales.
- Cambia tus contraseñas regularmente. Internacionalmente se recomienda cada seis meses.
- Utiliza contraseñas diferentes en webs, correos y redes sociales.
- Evita contraseñas comunes o fáciles de adivinar, como fechas de nacimiento, nombres de mascotas, o “123456”.

- **No compartas tus contraseñas con nadie, estas son personales e intransferibles.** Imagina que tu contraseña es como la llave de tu casa, si la compartes, es como si le dieras la llave de tu casa a cualquier persona.

GLOSARIO TECNOLÓGICO

El equipamiento de la Universidad de La Frontera, “incluye equipos computacionales, periféricos computacionales y todo otro equipamiento tecnológico conectado a la red corporativa. Entre otros se incluyen: computadores, impresoras, proyectores, cámaras, etc.” (Reglamento Técnico de Seguridad de la Información y Ciberseguridad).

PROTECCIÓN DE DISPOSITIVOS

- **Bloquea los dispositivos cuando no estén en uso.** Por ejemplo, configura el bloqueo automático de la pantalla después de cierto período de inactividad, y desbloqueo con clave.
- Descarga **aplicaciones de confianza.**
- Usa opciones de **autentificación de múltiples factores**, especialmente en el correo electrónico o redes sociales. Esta medida añade una capa adicional en la protección de tus cuentas.
- Utiliza **sólo licencias autorizadas**, recuerda que todo software debe estar debidamente licenciado.
- En dispositivos públicos: **Cierra siempre las sesiones iniciadas**, borra archivos temporales de internet y el historial de navegación.
- Instala **antivirus** en tus dispositivos.
- Mantén tus equipos actualizados, **actualiza el software de tus dispositivos**, como sistema operativo, programas, aplicaciones y navegadores.

GLOSARIO TECNOLÓGICO

Dispositivo: cualquier equipo electrónico o informático, como computadoras, celulares, tablets u otro dispositivo que pueda recibir, procesar y enviar información.

Autentificación de múltiples factores: *es un método de seguridad que requiere más de una forma de verificar la identidad, como por ejemplo antes de permitir el acceso al correo se solicita una contraseña enviada al teléfono móvil de la persona.*

Software: *programas informáticos, como sistemas y aplicaciones.*

Hardware: *componente físico y tangible de un equipo tecnológico, es decir, todo lo que puedes tocar y ver, por ejemplo, un teclado, pantalla, disco duro, entre otros.*

Sistema operativo: *es un conjunto de programas que controla el hardware y software en un sistema informático, por ejemplo, Windows, macOS, Linux, iOS y Android.*

ACCESO SEGURO A LA RED

- Utiliza conexiones seguras, como VPN, al acceder a sistemas informáticos UFRO desde fuera de la universidad.
- Evita redes Wi-Fi públicas que no sean seguras, como las ofrecidas en aeropuertos, para proteger tus datos de posibles ataques de intermediarios. Los ciberdelincuentes pueden configurar redes Wi-Fi falsas que parecen legítimas (por ejemplo, con nombres como "Free Airport Wi-Fi") para engañar a las personas y robar sus datos.

GLOSARIO TECNOLÓGICO

VPN: *Servicio de Red Privada Virtual, es una tecnología que crea una conexión segura y encriptada.*

HTTPS: *"Hyper Text Transfer Protocol Secure" o "Protocolo Seguro de Transferencia de Hipertexto" quiere decir que todas las comunicaciones entre el navegador y el sitio web están encriptadas.*

URL: *Dirección web.*

- Accede a webs donde la dirección URL comience por HTTPS.
- Descarga programas y aplicaciones sólo desde sitios oficiales. Evita páginas web con un gran número de anuncios.
- No hagas clic sobre cualquier enlace. Cada vez los delincuentes son más cuidadosos en lo que hacen, y si un correo o mensaje tiene el logo de una marca, lenguaje o dirección de correo aparentemente bueno, no necesariamente significa que sea legítimo.

Siempre verifica y ten cuidado en las siguientes situaciones:

- Si el mensaje o correo no tiene una firma válida o datos de contacto.
- Si solicitan información personal, ignora el mensaje.
- Al abrir correos electrónicos de remitentes desconocidos.
- Cuando existan errores gramaticales y/o de ortografía.
- Si existe lenguaje amenazante o urgente, por ejemplo, "tu cuenta ha sido bloqueada", "intento de inicio de sesión no autorizado".
- Por ejemplo, la Universidad o un banco jamás le pedirá sus claves por correo, mensajes de texto o WhatsApp.

PROTEGE TU INFORMACIÓN

- Realiza copias de seguridad periódicas y almacénalas en lugares seguros.
- No compartas demasiada información en tus redes sociales. Existen atacantes que utilizan la información para manipular, solicitando datos de manera amable, amigable y respetuosa.
- Sé consciente de la información que compartes en línea.
- No dejes dispositivos como pendrives, en cualquier lugar como por ejemplo en impresoras.
- No uses ni conectes dispositivos encontrados del que no sepas su origen, tales como pendrives.
- Recuerda cerrar tus sesiones de aplicaciones, por ejemplo, de Campus Virtual o Intranet en equipos de las salas de clases.

GLOSARIO TECNOLÓGICO

¿Cómo efectuar una copia de seguridad?

1. *Identifica los datos o información importante (archivos y datos críticos).*
2. *Selecciona un método de respaldo, puede ser en un dispositivo externo, en la nube o una mezcla de estos.*
3. *Efectúa copias periódicamente.*

ES NUESTRO DEBER:

Recuerda que es deber de todas y todos:

- Informar cualquier evento o actividad que atente contra los principios de Seguridad de la Información de la Universidad de La Frontera.
- Participar en capacitaciones o talleres en relación a materias de Seguridad de la Información y Ciberseguridad.

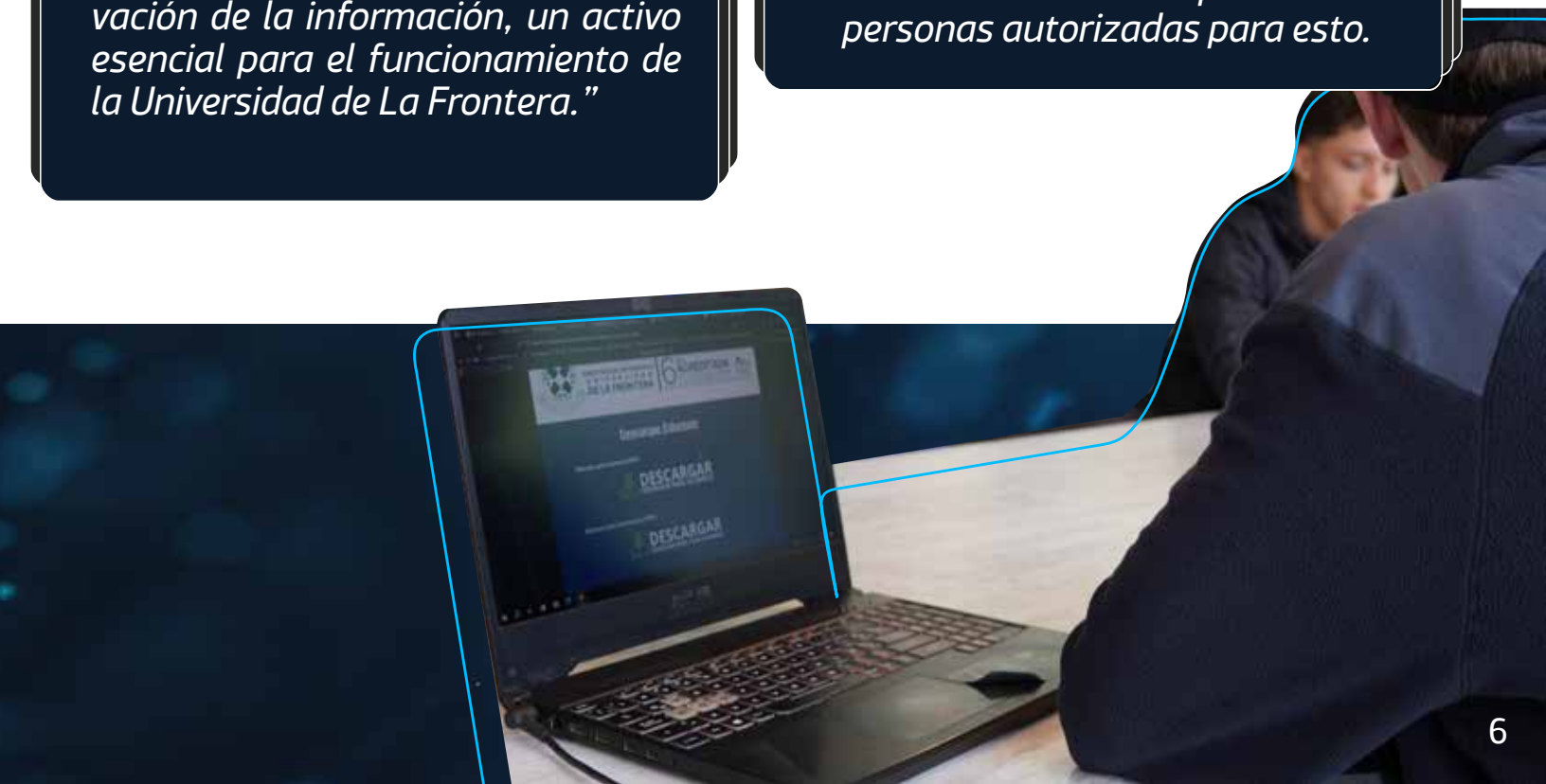
GLOSARIO TECNOLÓGICO

El Reglamento Técnico de Seguridad de la Información y Ciberseguridad de la Universidad de La Frontera, define seguridad de la información (SI) como *"Conjunto de principios: confidencialidad, integridad y disponibilidad, que aseguran la preservación de la información, un activo esencial para el funcionamiento de la Universidad de La Frontera."*

GLOSARIO TECNOLÓGICO

Principios SI:

1. *Confidencialidad: hace referencia a la privacidad de la información.*
2. *Integridad: se refiere a la confiabilidad y certeza de la información.*
3. *Disponibilidad: indica que la información debe estar disponible a las personas autorizadas para esto.*



UNIVERSIDAD DE LA FRONTERA
DIRECCIÓN DE INFORMÁTICA

DESARROLLO Y TRANSFORMACIÓN DIGITAL
VRAF - UFRO

BUENAS PRÁCTICAS EN CIBERSEGURIDAD

Siguiendo estas buenas prácticas, aseguramos la protección de nuestra información y promovemos un entorno digital seguro. ***¡Protege tus datos y contribuye a mantener la seguridad digital en la Universidad de la Frontera!***

Acción derivada del **Reglamento Técnico de Seguridad de la Información y Ciberseguridad**, que tiene por objetivo *"Establecer medidas para resguardar la seguridad de la información abordando riesgos y oportunidades, enfocadas en la mejora continua y asegurando la confidencialidad, integridad y disponibilidad de la información".* A partir del plan de implementación de la **Política de Desarrollo y Transformación Digital de la Universidad de La Frontera.**