UNIVERSIDAD ADOLFO IBÁÑEZ

TRANSFORMA
¿Sabías que?

AGOSTO

La ciberseguridad es un pilar fundamental para proteger la información en un entorno digital cada vez más expuesto a amenazas. En este documento te entregamos conceptos clave, buenas prácticas y pasos para actuar ante incidentes de ciberataque.

1 ¿QUÉ ES LA CIBERSEGURIDAD?

La ciberseguridad es el conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas informáticos, redes y datos frente a accesos no autorizados, ataques, daños o robos que pueden ocurrir de forma virtual. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información en entornos digitales.

2 ¿CUÁL ES LA DIFERENCIA ENTRE CIBERSEGURIDAD Y SEGURIDAD INFORMÁTICA?

Seguridad informática se refiere a la protección de los sistemas informáticos en general, incluyendo hardware, software, redes y datos, sin importar si están o no conectados a internet.

Ciberseguridad, en cambio, se enfoca específicamente en proteger los sistemas, redes y datos frente a amenazas que provienen del entorno digital o cibernético, es decir, desde internet.

3 ¿CÓMO SABER QUE ESTÁS ANTE UN INCIDENTE DE CIBERSEGURIDAD? ¿QUÉ DEBES HACER?

Si notas un correo extraño o sospechoso, un archivo que no abriste, incluso un comportamiento inusual en tu equipo; podrías estar frente a un incidente de ciberseguridad.

Errores frecuentes:

- Remitente **desconocido**.
- **Faltas de ortografía** o gramática.
- **Mensajes de urgencia** o amenaza.
- Enlaces **falsos de promociones o beneficios**.
- Archivos **adjuntos sospechosos**, como: .ZIP, .EXE, .DOCX o incluso PDFs infectados. Si no esperabas recibir algo, no abras el archivo.

En esos momentos, saber cómo actuar puede marcar la diferencia entre un susto menor y una crisis mayor. Y lo más importante: no te quedes callado. Alerta al equipo de ciberseguridad que está capacitado para afrontar la situación y para ayudarte.

Qué hacer:

- **No ignores** la situación.
- No intentes **resolverlo solo**.
- Reporta el correo a **mesadeservicio@uai.cl** o directamente en el portal web **mesadeservicio.uai.cl**

- **Mientras más rápido actúes**, menor será el impacto.

Consecuencias institucionales

- Pérdida de datos personales
- Interrupción de servicios críticos
- Daño reputacional
- Riesgo legal

4 ¿QUÉ ES EL PHISHING Y CÓMO DETECTARLO?

El phishing es una forma de ciberataque diseñada para engañarte y obtener información personal o confidencial. Actualmente, se estima que cerca del 90 % de los ataques informáticos a nivel mundial se inician a través de correos electrónicos fraudulentos.

Los atacantes se hacen pasar por instituciones confiables, como bancos, plataformas conocidas o incluso compañeros de trabajo, para que hagas clic en un enlace, descargues un archivo o entregues tus datos personales.

¿Cómo reconocerlo?

- Correos con **mensajes urgentes** como "¡Tu cuenta será bloqueada!".
- **Hipervínculos sospechosos** o con errores ortográficos.
- **Remitentes desconocidos** o con direcciones extrañas.

5 ¿CÓMO PROTEGER LA INFORMACIÓN PERSONAL Y DE LA UNIVERSIDAD?

Un descuido, como enviar un archivo sensible por el canal equivocado o dejar documentos visibles en tu escritorio, puede tener consecuencias graves. La seguridad de la información empieza con hábitos simples, pero conscientes. Por eso te recomendamos:

- **No compartir información sensible** por correo o chat.
- **Guardar archivos importantes** en carpetas seguras.
- **Evitar dejar documentos visibles** en tu escritorio.
- Si no estás seguro de si un dato es sensible **trátalo como si lo fuera**.

6 ¿CÓMO CREAR Y GESTIONAR CONTRASEÑAS SEGURAS?

Si tu contraseña es débil o fácil de adivinar, estás dejando la puerta abierta y facilitando la entrada de un posible atacante. Muchas personas aún usan contraseñas como "123456" o "contraseña", sin saber que son las primeras que prueban los atacantes.

Para crear una contraseña segura, usa:

- Al menos 12 caracteres.
- Letras, números y símbolos.
- Nada personal ni fácil de adivinar.

Por ejemplo:

- "**uai2024**" ✗
- "**U@l_COntr@s3n@_25**" ✓
- Además, te recomendamos **usar contraseñas distintas** para cada cuenta.

7 ¿CÓMO HACER USO CORRECTO DE LOS EQUIPOS?

Hay acciones que a veces, sin darnos cuenta pueden poner en riesgo tus datos y los de la Universidad como, por ejemplo, dejar los dispositivos desbloqueados, conectarse a redes Wi-Fi públicas o instalar programas sin verificar su origen.

Por eso, adoptar buenas prácticas digitales es una responsabilidad compartida.

Te recomendamos algunas buenas prácticas:

- Bloquea tu equipo al alejarte.
- Evita redes Wi-Fi públicas.
- No instales software no autorizado.

8 ¿QUÉ ROL CUMPLIMOS LOS COLABORADORES EN LA PROTECCIÓN DE DATOS?

Los colaboradores somos la primera línea de defensa en ciberseguridad.

Nuestro rol incluye:

- **Reconocer y evitar** correos sospechosos o fraudulentos (phishing).
- **Usar contraseñas seguras** y no compartirlas.
- **No instalar** software no autorizado.
- **Seguir buenas prácticas digitales** que minimicen los riesgos de fuga o robo de información, como las que te hemos dejado en este documento.

La UAI tendría diversas consecuencias tras una brecha de seguridad, tales como:

- **Pérdida de información confidencial:** datos personales de estudiantes, académicos y administrativos.
- **Interrupción de servicios:** afectación a plataformas educativas, sistemas de matrícula, bibliotecas digitales, etc.
- **Daño reputacional:** pérdida de confianza por parte de la comunidad universitaria.

¿Dudas o incidentes?

No los ignores.
Actúa rápido no dudes
En comunicarte.

Reporta a:
mesadeservicio@uai.cl

¿Quieres saber más sobre la ciberseguridad en la UAI. permanece atento a toda la información que transforma está preparando para ti.

LA CIBERSEGURIDAD COMIENZA CONTIGO
¡ESTEMOS ATENTOS Y PREPARADOS!