CIBERSEGURIDAD

1. Ciberseguridad y Ciberresiliencia

La ciberseguridad y la ciberresiliencia son dos conceptos relacionados pero distintos en el ámbito de la tecnología y la seguridad de la información.
Ambos conceptos son fundamentales para proteger los sistemas y datos de la institución y permiten afrontar vulneraciones en los sistemas con acciones concretas para asegurar la operatividad perpetua del ecosistema UTEM ante ataques cibernéticos.

Ciberseguridad

Es un conjunto de prácticas, tecnologías y medidas diseñadas para proteger los sistemas informáticos, las redes, los dispositivos y los datos de ataques cibernéticos. Su objetivo principal es prevenir el acceso no autorizado, el robo de información, la interrupción de servicios y otros tipos de amenazas cibernéticas. La ciberseguridad abarca una variedad de áreas, incluyendo la protección de redes, la identificación y autenticación de usuarios, la encriptación de datos, la detección de intrusiones y el mantenimiento de parches de seguridad. Algunas medidas comunes de ciberseguridad incluyen el uso de firewalls, sistemas de detección de intrusiones, antivirus, autenticación multifactor, capacitación en concienciación sobre seguridad para usuarios y la implementación de políticas de seguridad robustas.

Ciberresiliencia

Por otra parte la ciberresiliencia se refiere a la capacidad de nuestra organización (sistemas y funcionarios) para resistir, adaptarse y recuperarse rápidamente de ataques cibernéticos o incidentes de seguridad, minimizando los efectos negativos y manteniendo la continuidad de las operaciones críticas. La ciberresiliencia ayuda a la planificación y preparación de reaccionar a la posibilidad de que ocurran estos ataques. Las estrategias de ciberresiliencia implican la planificación de respuesta a incidentes, la segmentación de redes para limitar la propagación de ataques, la realización de copias de seguridad regulares y la creación de planes de recuperación ante desastres.

2. Políticas de Ciberseguridad UTEM

Consejos básicos para fortalecer la ciberseguridad

A continuación te presentamos algunos consejos básicos sugeridos por SISEI para fortalecer tu dispositivo y te informamos sobre los procedimientos que deben efectuarse para evitar pérdida o secuestro de datos en caso de ataques cibernéticos.

A. Desplegar antivirus Cylance

Antivirus con inteligencia artificial el cual no trabaja bajo firmas, es decir, la protección parte desde el primer día.

B. Uso de la VPN Institucional Forticlient

Este servicio se utiliza para ingresar de forma segura a recursos y servicios que provee la universidad. *No todos los funcionarios cuentan con VPN.

Las VPN se encuentra sólo con perfil de usuario asignado, no toda la comunidad.

C. Concientizar para prevenir el Phishing

Tener cuidado con abrir correos perjudiciales. "No todo lo que brilla es oro". Nunca des clic en esos enlaces.

D. Proyecto Respaldo Avanzado

En SISEI se pretende mantener respaldado todos los sitios de la universidad y todos los datos en caso de cualquier vulneración virtual y de ése modo ser capaces de reestablecer los sistemas con celeridad.

E. Despligue de Active Directory

Es un servicio para seguritizar los terminales, los equipos de los usuarios y permite crear perfiles para cada funcionario con permisos restringidos según el cargo.

F. Cuida tus datos y los de la institución

Toda la información con la que se trabaja es confidencial. Evita usar tu correo institucional para fines personales. Recuerda que el almacenamiento y respaldo, si no es asegurado, da pie a conflictos con fraudes.

3. Protección de Datos

Pilares de la Ciberseguridad

Integridad

Necesario para velar en la protección de los datos tanto física como lógica.

- Actualización de equipamiento lógico y físico.
- Hacking ético.
- Respaldo híbrido centralizado.
- Site contingencia.

= Protección

Disponibilidad

Trabaja para darle acceso seguro a los servicios y datos.

- Red centralizada.
- Conectividad de calidad.
- Mejora continua de enlaces.

= Acceso

Confidencialidad

Apoya la seguridad desde la perspectiva de la privacidad y confidencialidad, es decir, ver sólo lo que corresponde al perfil.

- Directorio Activo centralizado.
- Permisos y perfiles.
- Equipamiento controlado y actualizado.

= Privacidad