Seguridad Informática

¿Qué es un incidente de seguridad informática?
Un incidente de seguridad informática está indicado por un o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones de los procesos de negocio y amenazar la seguridad de los activos de información.

Ej. Alerta de virus en tu computador, correo sospechoso, alerta de página web con contenido sospechoso, descarga de archivos con contenido ilegible o confuso, alerta de falla en respaldo de información, sospecha de acceso no autorizado a tu equipo, sospecha de robo de credenciales, eliminación de archivos sin autorización. Etc.

¿Cómo reportar un incidente de seguridad informática?
Para reportar un incidente de seguridad informática los colaboradores deben ingresar a la aplicación de mesa de ayuda (https://helpdesk.udes.edu.co/indexglpi.php) y crear un ticket de soporte indicando tipo "incidente" y categoría "seguridad informática", datos del solicitante, puesto de trabajo, extensión y demás datos que solicita el formato.

¿Cómo se realiza el respaldo de la información en mi estación de trabajo?
Si la estación de trabajo está incluida en el programa de respaldo de información institucional, el subproceso de Seguridad informática coordinará la instalación de aplicación de respaldo y ejecutará las actividades respectivas.

¿Cómo se realiza una solitud de restauración de la información?
Para solicitar restauración de información los colaboradores deben ingresar a la aplicación de mesa de ayuda (https://helpdesk.udes.edu.co/indexglpi.php) y crear un ticket de soporte indicando tipo "requerimiento" y categoría "seguridad informática", datos del solicitante, puesto de trabajo, extensión, información a restaurar y demás datos que solicita el formato de solicitud.

¿Cada cuánto se realizan las copias de respaldo de mi estación de trabajo?
Una vez se ingresa una estación de trabajo al programa de respaldo de la información, las copias se realizan de forma diaria mediante un proceso automatizado que se ejecuta desde los servidores institucionales de respaldo de la información.

¿El subproceso de Seguridad Informática tiene coordinadores líderes en los campus de Cúcuta y Valledupar?

El subproceso de seguridad informática de la UDES solo cuenta con un jefe de seguridad informática a nivel nacional y se apoya en los jefes de TI y subproceso de servicio al usuario de los campus de Cúcuta y Valledupar para las actividades relacionadas son seguridad informática

¿Qué tipo de información se incluye en el respaldo de la información institucional?

El subproceso de seguridad informática realiza respaldo de la información institucional, la información a respaldar son solo documentos relacionados con la labor institucional y académica, no se incluye información personal almacenada en los equipos de cómputo, se excluyen imágenes y videos si estos no están relacionados con las funciones del puesto de trabajo.

¿Qué se requiere de parte del usuario para lograr una eficaz copia de respaldo de información?

Para facilitar las actividades de respaldo y restauración de la información institucional los colaboradores deben mantener sus archivos agrupados y clasificados en carpetas relacionadas con los procesos y funciones actividades que manejan en su puesto de trabajo.

¿Qué debo hacer cuando me retiro de mi puesto de trabajo para garantizar la privacidad de la información?

Con el fin de salvaguardar la información y como un control preventivo se recomienda que los usuarios realicen el bloque de la pantalla de sus equipos de cómputo cuando se retiran de sus puestos de trabajo a descanso u otras actividades durante la jornada laboral. Este bloqueo se realiza en el sistema operativo Microsoft Windows presionando la combinación de teclas **ctrl alt supr + enter**

¿Cuáles son los beneficios destacables que brinda el subproceso de seguridad informática?

- ✓ Tratamiento oportuno y especializado de incidentes relacionados con la seguridad de la información.
- ✓ Respaldo y Restauración de la información institucional crítica para la continuidad de los procesos.
- ✓ Tener procedimientos definidos para la operación y monitoreo de la infraestructura tecnológica de la institución.
- ✓ Seguimiento y trazabilidad de incidentes a través de proceso de gestión de servicios la mesa de ayuda.

- ✓ Asesorar la unidades académico-administrativas sobre buenas prácticas y mejoras de procedimientos para asegurar los activos de información.

¿Cuáles son las recomendaciones para construir contraseñas seguras o robustas?

La construcción de contraseña debe cumplir con unos parámetros mínimos para garantizar

- ✓ Debe ser alfanumérico
- ✓ Debe contener mínimo 7 caracteres
- ✓ Debe contener una mayúscula
- ✓ ¡Debe contener un caracter especial (! * # $ % &), Etc
- ✓ No repita contraseñas
- ✓ No use datos relacionados con el nombre de la institución, proceso o subproceso.
- ✓ No use información personal como nombre, edad, fecha de nacimiento, nombres de hijos o mascotas, colores o canciones favoritas, etc
- ✓ Cambie la contraseña de forma periódica (el sistema lo exigirá cada 120 días)

¿Qué es un ataque informático?

Un ataque informático se puede describir como una actividad malintencionada contra un sistema informática que puede ser un equipo, un dispositivo móvil o cualquier elemento de la plataforma tecnológica, se realiza de manera organizada en una serie de pasos que buscan hacer daño, extraer información o interrumpir la operación de los sistemas de información.

¿Qué es una copia de respaldo?

Una copia de respaldo o copia de seguridad (Backup) es la actividad consistente en mantener una copia de archivos físicos o virtuales o bases de datos y llevarlos a una ubicación secundaria para su preservación en caso de falla de equipos u otro incidente que atente contra la disponibilidad, integridad y confidencialidad de la información

¿Qué es ingeniería social?

La ingeniería social es una actividad malintencionada que suelen realizar los atacantes informáticos en las etapas previas a un ataque informático y consiste en engañar a las personas con suplantación de identidad para extraer información.

¿Qué es un phishing?

El término phishing es utilizado en informática para referirse a una

técnica o actividad de ingeniería social consistente en engañar a las personas a través del correo electrónico, es uno de los más utilizados para estafar a los usuario de internet obteniendo los datos de sus cuentas bancarias y tarjetas de crédito, lo más común es que la víctima reciba un correo con información falsa de la página de su banco solicitando la clave de acceso a la cuenta o el código de seguridad de su tarjeta de crédito.

¿Cuánto tiempo tarda una restauración?

El proceso de restauración de información es ejecutado por personal de Servicio al usuario previa validación del subproceso de seguridad informática, el tiempo de restauración de la información no tiene un estimado aproximado y depende del volumen de archivos que contenga la copia solicitada.

¿Cuáles son las recomendaciones para proteger la información en mi puesto de trabajo?

- Si recibe un correo electrónico con información de la cual desconfía, por favor no lo abra e informe de inmediato a seguridad informática.
- Evite guardar o escribir las contraseñas en sitios o documentos visibles.
- No comparta con nadie las contraseñas o credenciales de acceso a los sistemas de información.
- Al retirarse de su estación de trabajo mantenga bloqueada su pantalla.
- Evite descargar software o contenido diferente al autorizado en su proceso.
- Informe al Seguridad informática si nota algo fuera de lo normal con equipo de cómputo, archivos o dispositivos electrónicos.