Departamento de Seguridad Informática
Dirección General de Sistemas

Seguridad de la Información: Recomendaciones

La información es un activo de mucho valor para la Universidad y como tal debe ser protegido. Es por ello que en la implementación de la seguridad de la información se debe procurar:

> Salvaguardar la exactitud y totalidad de la información almacenada o transmitida, cuyo contenido debe permanecer inalterado a menos que sea modificado por personal autorizado **=> Integridad de la información** .
>
> Evitar que personas no autorizadas puedan acceder a la información almacenada en un determinado sistema **=> Confidencialidad de la información**.
>
> Que la información y los recursos relacionados estén disponibles toda vez que el personal autorizado los requiera **=> Disponibilidad de la información**.

Las siguientes recomendaciones son pautas básicas para preservar estas 3 características principales de la información.

Claves de acceso

Una clave de acceso o contraseña es una serie de caracteres que el usuario debe utilizar para autenticarse ante el sistema de información.

Características de una contraseña segura

- Personal
- Secreta
- Intransferible
- Fácil de recordar
- Difícil de averiguar
- De renovación periódica

Cómo crear claves de acceso robustas

- No utilice palabras comunes, de diccionario,ni nombres de fácil deducción por terceros.
- No las vincule a un dato personal.
- No utilice como contraseña su nombre de usuario ni derivados del mismo.
- Constrúyalas utilizando al menos 12 caracteres.
- Combine letras mayúsculas y minúsculas, números y signos.
- Use claves distintas para máquinas y/o sistemas diferentes.
- Elija una palabra sin sentido, aunque pronunciable.
- Elija una clave que no pueda olvidar, para evitar escribirla en alguna parte.

Normas de uso de claves

- Cuide que nadie observe cuando escribe su clave.
- No observe a otros mientras lo hacen.
- No escriba la clave en papeles, post-it, ni en archivos sin cifrar.
- No comparta su clave con otra persona.
- No pida la clave de otra persona.
- No habilite la opción de “recordar claves” en los programas que utilice.
- Si por algún motivo debe anotar la clave, no la deje al alcance de terceros, ni debajo del teclado, y nunca pegada al monitor.
- No envíe su clave por correo electrónico ni la mencione en una conversación.
- No entregue la clave a nadie, ni siquiera al administrador del sistema. El personal de Servicio

Técnico de la Dirección General de Sistemas está autorizado a solicitarle su clave de acceso en caso de requerirla para realizar reparaciones del equipo o software. Luego de la tarea de reparación la clave de acceso deberá ser modificada.
- No mantenga una contraseña indefinidamente. Cámbiela regularmente.

Política de escritorios y pantallas limpios

- Guarde bajo llave la información crítica, preferentemente en una caja fuerte o gabinete ignífugo.
- Si utiliza una notebook, manténgala en un lugar seguro para evitar hurtos o robos.
- No deje pendrives, CD's, diskettes, u otro elemento removible con información en lugares visibles y accesibles.
- No deje accesibles documentos impresos que contengan datos confidenciales.
- Deje su lugar de trabajo en orden, apague los equipos y guarde los documentos al finalizar la jornada laboral.
- Cierre la sesión al ausentarse o dejar de utilizar un sistema informático.
- Si debe abandonar, aunque sea momentáneamente, su puesto de trabajo, bloquee su terminal con un protector de pantalla que solicite el ingreso de una clave.

Carpetas compartidas

- Establezca contraseñas robustas en las carpetas compartidas a través de la red y cámbielas periódicamente.
- No comparta todo el disco de la computadora.
- Distribuya la información a compartir en distintas carpetas.

Traslado de información crítica

Todo traslado de información crítica debe realizarse de manera de preservar la seguridad de la información:

- Uso de sobres cerrados y firmados.
- Entrega en mano al personal autorizado.
- En caso de ser medios digitales, proteger los archivos con contraseña.

Eliminación segura

La eliminación de la información crítica, ya sea que resida en un medio digital o en papel, deberá realizarse mediante un proceso que asegure su confidencialidad hasta su destrucción. La eliminación segura impide obtener información mediante trashing, que es la práctica de recuperar información técnica o confidencial a partir de material descartado, y suele ser la manera de obtener datos para posteriormente cometer otros delitos (robo, intrusión en los sistemas de información u otros incidentes).

- Trashing físico: papeles o impresos descartados, diskettes, discos compactos, etc.
- Trashing lógico: contenido de la papelera de reciclaje, historial de sitios visitados, contraseñas almacenadas, etc.

Ingeniería social

- No responda preguntas sobre características de los sistemas. De ser necesario, derive la consulta a los responsables que tengan competencia para dar dicha información.
- Cerciórese de la identidad del interlocutor antes de brindar información sobre un sistema.
- Utilice el servicio técnico de confianza.
- Para evitar ser víctima del fraude informático lea el documento Cómo protegerse del phishing.

Resguardo de la información

El resguardo permite tener disponible e íntegra la información ante una contingencia.

- Realice copias periódicas de la información crítica y de trabajo diario.
- Guarde las copias en lugar seguro.
- Verifique la integridad física y lógica de los respaldos.
- Garantice la confidencialidad de los datos respaldados.
- Practique la reutilización segura de los medios.

Utilización apropiada del correo electrónico

El documento *Recomendaciones para el uso del correo electrónico* contiene consejos para realizar una utilización apropiada del correo electrónico de la Universidad. También encontrará consejos importantes en el documento *Como actuar frente al spam y a hoaxes*.

Navegación en Internet

- Utilice un navegador seguro y con la configuración recomendada por la UNLu.
- Evite acceder a sitios desconocidos o no confiables.
- No acepte la instalación automática de software.
- No descargue archivos de sitios web no confiables.
- Siempre descargue los archivos en una carpeta y analícelos con un antivirus actualizado antes de abrirlos.
- No ingrese información crítica o personal en formularios, páginas o foros.
- Si un sitio requiere que ingrese información crítica o personal sólo hágalo en sitios seguros (la dirección debe comenzar por https).

Código malicioso

El código malicioso o malware es software diseñado para infiltrarse en una computadora sin el conocimiento de su dueño con el fin de robar, dañar o eliminar el software y la información almacenada, o aprovechar los recursos de la misma para efectuar otras acciones maliciosas. El término código malicioso es una expresión general que engloba una variedad de formas de software o código hostil e intrusivo: virus informáticos, gusanos, troyanos, la mayoría de los rootkits y programas espía

- Utilice un antivirus reconocido, con la configuración recomendada por la Universidad.
- Verifique que siempre esté activo y actualizado a la fecha.
- Analice siempre los medios removibles (discos, disquettes, pen-drives, mp3, celulares, cámaras digitales) que se conecten a la computadora.
- Ejecute un análisis completo (análisis en profundidad) del equipo al menos una vez por semana.

Si tiene alguna duda o desea realizar una consulta puede comunicarse con el Departamento de Seguridad Informática de la UNLu a la dirección seguridadinformatica@unlu.edu.ar, o bien por teléfono al 02323 42-3171 / 42-3979, interno 1312.