# CONSEJOS SOBRE
# SEGURIDAD INFORMATICA

## La seguridad de la Universidad empieza por nosotros

### LOS TRES PILARES DE LA SEGURIDAD

La seguridad de la información consiste en conservar y proteger las tres propiedades de la información:

#### Disponibilidad

La información debe estar disponible cuando la necesitemos. La falta de la misma se puede dar por problemas de configuración o por ataque cibernético.

#### Integridad

La información debe estar libre de modificaciones y o errores que impliquen cambios en su contenido. Esta falla se puede dar por modificación, borrado (parcial o total) y puede ocurrir accidentalmente o por ataque cibernético.

#### Confidencialidad

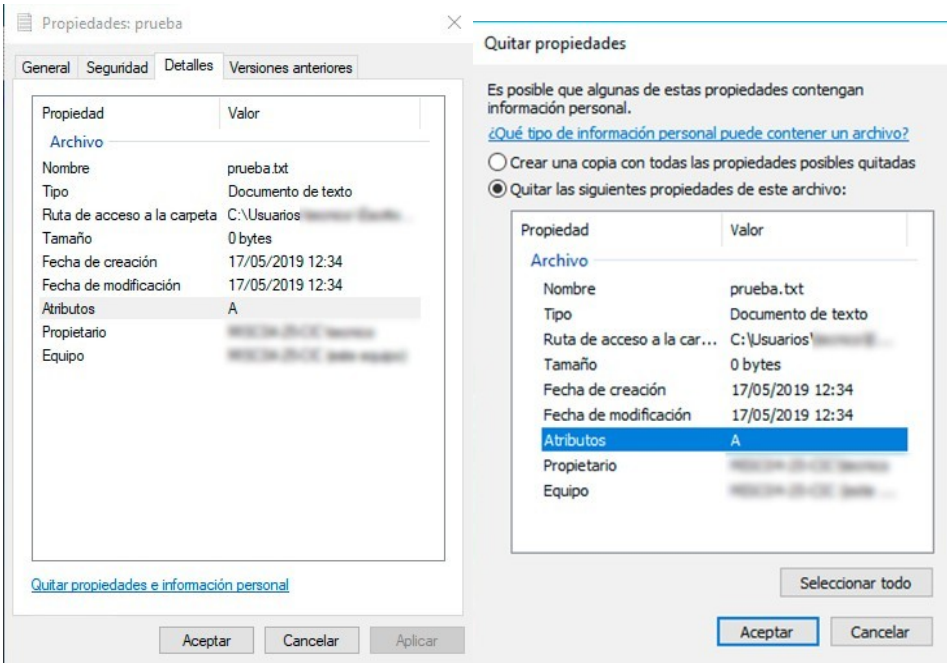
La información no se debe poner a disposición o ser revelada a individuos, entidades o procesos no autorizados. La información debe ser **confidencial.**

### METADATOS, RIESGOS Y CÓMO ELIMINARLOS

Un «metadato» es aquella información que se incluye en archivos, pero que no forma parte del contenido. Algunos ejemplos de metadatos son la fecha de creación, la fecha de modificación o el autor del archivo. Pueden proporcionar información valiosa sobre nosotros a los ciberdelincuentes, como nombres de usuario, fechas de creación o modificación de los documentos, ubicación de las fotografías, aplicación utilizada, etc.

Por ello, debemos eliminar los metadatos antes de enviar el archivo a otra persona, o subirlos a la página web de la universidad o a un servicio de almacenamiento en la nube.

La mayoría de programas de ofimática más utilizados incorporan funcionalidades para eliminar esta información. También se puede hacer desde el propio sistema operativo como es el caso de Windows mediante la opción de botón derecho => Propiedades => Detalles. A continuación, se selecciona «Quitar propiedades e información personal» y se abrirá una nueva ventana. Se selecciona la opción «Quitar las siguientes propiedades de este archivo» y posteriormente «Seleccionar todo”. Por último, clic en «Aceptar» y el proceso de borrado de metadatos ha terminado.




## COPIAS DE SEGURIDAD O BACKUPS

Almacenamiento local: copia para trabajar en forma cotidiana. No tiene copia de seguridad, por lo tanto, la información puede perderse.

Nube, Carpeta compartida ó disco z, y, x etc.: tiene copia de seguridad, mensuales, semanales y diarios. La información siempre está disponible.

## CORREO ELECTRÓNICO

Como toda herramienta de comunicación es necesario definir su uso correcto y seguro, ya que, además de abusos y errores no intencionados el correo electrónico se ha convertido en uno de los medios más utilizados por los ciberdelincuentes para llevar a cabo sus ataques.

Es habitual que a los buzones de usuarios llegue spam, correos de tipo Phishing o correos que suplantan entidades o personas. En estos casos utilizan técnicas de ingeniería social para conseguir sus fines maliciosos, por ejemplo, infectar el equipo o

incluso toda la red de la universidad, robar credenciales, datos bancarios o información confidencial.

En un correo malicioso, tanto el remitente, como el asunto, el cuerpo, los adjuntos o los enlaces que contiene, pueden estar diseñados para engañar al receptor del mensaje.

**Phishing**

Se trata de un engaño basado, generalmente, en la suplantación de una empresa o entidad fiable como un banco, una red social o entidades públicas. La finalidad es hacerse con claves de acceso o información sensible como pueden ser datos fiscales o bancarios. El canal mediante el cual se intenta perpetuar el fraude suele ser el correo electrónico, pero también pueden usarse otros como los SMS o aplicaciones de mensajería instantánea como WhatsApp.

**Malware**

Es un código malicioso que podría infectar los dispositivos. Los correos podrían contener algún tipo de archivo adjunto o enlaces a webs donde una vez descargado y ejecutado el fichero infectará el dispositivo. La infección también puede producirse al hacer clic en anuncios fraudulentos (malvertising) o aprovechando alguna vulnerabilidad en los navegadores (drive-by-download). Una vez en nuestro equipo, podría distribuirse a través de la red institucional, infectando todo tipo de dispositivos conectados a la misma, como discos duros, pero también otros sistemas de la red e incluso servicios en la nube.

**Detección de correos fraudulentos**


**Verificar remitente y firma:** Los ciberdelincuentes suelen utilizar cuentas de correo de otros usuarios a los que han hacheado para enviar los correos electrónicos fraudulentos. También pueden falsificar la dirección del remitente haciendo que, a simple vista, no se identifique el correo como fraudulento. Esta técnica se conoce

como e-mail spoofing. Con respecto a la firma, un cambio de esta o su ausencia, debe ponernos en alerta.

**Ingeniería social en el cuerpo y asunto:** La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios para que les envíen datos confidenciales, infectar sus computadoras con malware o abran enlaces a sitios infectados. Habitualmente, indican en los correos que el servicio al que representan se cancelará en varias horas o directamente que ya ha sido cancelado. Otro método utilizado es llamar la atención con dinero como un supuesto reembolso que espera a que sea reclamado.

**Comunicaciones impersonales:** Los ciberdelincuentes cuando envían correos fraudulentos realizan comunicaciones impersonales refiriéndose al destinatario como usuario, cliente, etc. Las entidades legítimas en las comunicaciones suelen utilizar el nombre y apellidos del destinatario, haciendo que la comunicación sea más personal.

**Documentos adjuntos maliciosos:** Cualquier documento adjunto en un correo electrónico debe ser una señal de alerta. Por norma, ninguna entidad ya sea bancaria, pública, energética, etc., envía a sus destinatarios documentos adjuntos en el correo. Si es necesario que se descargue algún archivo se hará desde su portal web o aplicación oficial. Se utilizan para infectar computadoras.

- .exe - El tradicional archivo ejecutable de Windows.
- .vbs - Archivo Visual Basic Script que también puede ser ejecutado.
- .docm - Archivo Microsoft Word con macros.
- .xlsm - Archivo Microsoft Excel con macros.
- .pptm - Archivo Microsoft PowerPoint con macros

También hay que tener cuidado con ficheros comprimidos como los .zip o .rar, ya que pueden contener archivos maliciosos, como los anteriores, en su interior. Jamás ejecutes archivos adjuntos, solo descárgalos y analízalos con el antivirus. Si es posible, hay que contactar al remitente por otro canal, como una llamada de teléfono para que confirme el mensaje y el adjunto.

**Mala redacción:** Cuando un correo presenta graves faltas de ortografía es una señal bastante certera de que ese mensaje es fraudulento. Los correos fraudulentos, en ocasiones, utilizan expresiones que no son las habituales. Ante un correo cuya forma de expresarse no es la común también habrá que comprobar su procedencia.

**Enlaces falsos:** Los correos electrónicos de tipo Phishing o sencillamente los que pretenden redirigir al usuario a un sitio web fraudulento, suelen contar con enlaces falseados. Las entidades legítimas por norma no envían enlaces en sus comunicaciones oficiales y solicitan al usuario que acceda al sitio web, utilizando su navegador web o la aplicación específica.

**CCO ó BCC (copia carbónico oculta):** Cuando envíes correo a varios destinatarios siempre utiliza estas opciones, ya que es una de las formas de fuga de información. Al utilizar CCO el receptor del correo no verá las direcciones del resto de destinatarios, ya que el correo electrónico es considerado un dato personal y estaríamos divulgándolo sin consentimiento del propietario.

## CONTRASEÑAS

En el control de accesos, el nombre de usuario nos identifica y la contraseña nos autentica, con ella se comprueba que somos quienes decimos ser. El uso de la contraseña es el método más utilizado, esto significa que su gestión es uno de los aspectos más importantes para asegurar los sistemas de la universidad. Las contraseñas deficientes o mal custodiadas pueden favorecer el acceso y el uso no autorizado de los datos y servicios. No permitas que tu navegador recuerde tus contraseñas.

**Robustez:** la complejidad de la contraseña es una de las principales medidas de seguridad. En muchas ocasiones, se eligen contraseñas débiles fáciles de recordar para acceder a los servicios que provee la universidad. Esto supone un riesgo.

► longitud mínima de 8 caracteres, ya que cuanto más larga sea esta, más tiempo se tardará en descubrirla;

► utilizar combinaciones de letras mayúsculas, minúsculas, números y símbolos.

Una forma de conseguir contraseñas robustas es utilizar reglas nemotécnicas aplicadas a una frase:

► seleccionamos una frase: «en un lugar de Quilmes»;

► hacemos uso de mayúsculas: «En un lugar de Quilmes»;

► incluimos el servicio: «En un lugar de Quilmes Correo»;

► añadimos números: «En un lugar de Quilmes Correo de 2023»;

► añadimos caracteres especiales: «En un lugar de Quilmes Correo de 2023!»;

► podemos comprimirla para hacerla más fácil de recordar, utilizando, por ejemplo, la primera letra de cada palabra, de tal forma quedará: «EuldQCd2023!».

NOTA: La forma más segura de obtener una contraseña robusta es utilizar un generador de contraseñas que nos permita elegir longitud, tipo de caracteres, etc. No obstante, cuanto más complejas sean, mayor será la dificultad para recordarlas. Por

ello, lo más recomendable es utilizar un gestor de contraseñas y así solo tener que recordar y conservar la clave maestra, la que abre el gestor.

**No compartida:** La contraseña debe ser intransferible y nadie bajo ningún concepto debe saber cuál es. Si otra persona conocedora de tu contraseña hiciera algo con tus credenciales de acceso, podrías ser responsable pues aparecerá registrado como si lo hubieses hecho vos.

**No usar la misma:** Utilizar la misma clave para acceder al correo electrónico, redes sociales, aplicaciones y servicios ofrecidos por la universidad, etc., no es una práctica segura. La reutilización de las contraseñas es uno de los errores más comunes que se cometen. Cada servicio debe tener su propia contraseña de acceso.

**Gestores de contraseñas:** Para evitar tener que recordar todas esas contraseñas existen herramientas específicas que simplifican el trabajo, conocidas como gestores de contraseñas. Utilizando este tipo de herramientas, únicamente será necesario, acordarse de una contraseña, la que permite el acceso al gestor.

## PUESTO DE TRABAJO

El puesto de trabajo es clave desde un punto de vista de la seguridad de la información

Son varios los riesgos a los que se expone el puesto de trabajo:

► información en papel al alcance de cualquiera

► la falta de confidencialidad de los medios de comunicación tradicionales como el teléfono

► accesos no autorizados a los dispositivos;

► infecciones por malware;

► robo de información;

► etc.

### Mesas limpias

Al acabar la jornada se debe guardar la documentación que se encuentre a la vista (información de la universidad, estudiantes, profesores, etc.). De esta manera, se evitarán miradas indiscretas que puedan derivar en una fuga de información, además del robo de documentos que pueden contener información confidencial.

► el puesto de trabajo debe estar limpio y ordenado

► la documentación que no se utilice en un momento determinado debe estar guardada correctamente, especialmente cuando se abandona el puesto de trabajo o se finaliza la jornada;

► no debe haber ni usuarios ni contraseñas puestas en pegatinas o similares.

**Bloqueo de sesión**

**l**os dispositivos, como ordenadores, tablets o móviles, con los que se esté trabajando siempre deben estar bloqueados, a no ser que se esté en presencia de ellos. Los dispositivos de escritorio se bloquean de la siguiente manera.

► Windows: Win + L

► Sistema operativo Mac: Control + Opción + Q

► Linux: Control + Alt + L

Al terminar la jornada, dejaremos siempre los equipos apagados y si fueran portátiles o móviles, bajo llave.

## Software actualizado

Todos los sistemas de la universidad deben estar actualizados a la última versión disponible, de esta manera estarán protegidos ante nuevas vulnerabilidades descubiertas y contarán con las últimas funcionalidades que haya liberado el fabricante. Se recomienda que las actualizaciones se realicen de manera automática. Un dispositivo desactualizado es un riesgo de seguridad para la Universidad.

## Antivirus y firewall

Tanto el antivirus como el firewall o cortafuegos son las herramientas de seguridad que protegen al equipo de trabajo del software malicioso. Ambas herramientas siempre deben estar activadas, ya que son complementarias,

El antivirus es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso, también conocido como malware. Actualmente, incorporan otras herramientas de seguridad como detección de webs fraudulentas o protección contra ransomware.

El firewall o cortafuegos tienen el objetivo de permitir y limitar, el flujo de tráfico que va desde y hacia Internet evitando así que el malware pueda comunicarse con el exterior y que ataques procedentes de Internet sean bloqueados