# PROTECCIÓN DE SUS DATOS

# PROTEGE TUS DISPOSITIVOS DE RED

## 💻 PROTEGE TUS DISPOSITIVOS INFORMÁTICOS

- Mantener el firewall encendido: Esto es para evitar infiltraciones o paso de malware no deseado
- Utilice un antivirus y Antispyware: Todo tipo de Malware que pueda tener acceso a sus datos, o al computador. Estos pueden ralentizar al pc, borrar sus datos o apoderarse del ella. Una excelente elección es solo descargar software de sitio oficiales para evitar descargar un Malware. Es recomendable que el antivirus bloqueé mails maliciosos, o Spyware que recopilen información o Adwares que envié anuncios emergentes de forma constante.
- Administrar su SO y navegador: Hackers están siempre intentando aprovechar vulnerabilidades del SO o el navegador, peor eso es recomendable siempre actualizarlos y descargar parches y actualizaciones de seguridad
- Proteger todos los dispositivos: Todos los dispositivos deben de estar protegidos con contraseña para evitar el acceso de personas no autorizadas, y evite guardar en los mismos información que se vea comprometido a un delincuente, y siempre mantén tu información cifrada para evitar cualquier inconveniente, si tus datos se ve comprometido y los delincuentes tienen acceso a todos tus datos en la nube, contrata con so SP de nube(Google Drive, OneDrive, etc.)

Se ha hablado del problema de los dispositivos del IoT, ya que estos al tener un firmware bajo en seguridad y sus parámetros en la mayoría quedan por default, esto afecta a que hackers aprovechen estos dispositivos y realizar un ataque o tengan acceso a tu información personal, la solución que se plantea ante esta situación es contar con dispositivos de IoT con una red aislada compartida únicamente con otros dispositivos de IoT.

Puede visitar https://www.shodan.io/, para ejecutar un escáner en dispositivos de IoT basado en la web.

## 🌐 USE LAS REDES INALÁMBRICAS EN FORMA SEGURA

Muchas de las redes inalámbricas permite que se conecten dispositivos a través de un SSID. Un gran problema es cuando un ISP a no actuar las prácticas de seguridad adecuadas deja por default estas configuraciones, los hackers son consientes de estas vulnerabilidades y por eso as llegan a aprovechar. Además, hay peligro en la encriptación de WPA2 en el router inalámbrico,

- Ejemplos
    - Visite **https://www.krackattacks.com/** para saber más acerca de KRACK.

Cuando está lejos de casa, los puntos públicos de acceso inalámbrico permiten tener acceso a su información en línea y navegar por Internet. Sin embargo, es mejor no acceder ni enviar información personal confidencial a través de una red pública inalámbrica. Verifique si su computadora está configurada para compartir archivos y medios digitales y si requiere la autenticación de usuario con encriptación. Para evitar que una persona intercepte su información (lo que se conoce como “eavesdropping”) mientras utiliza una red pública inalámbrica, utilice túneles VPN y servicios encriptados. El servicio VPN proporciona acceso seguro a Internet con una conexión cifrada entre la computadora y el servidor VPN del proveedor de servicios VPN. Con un túnel VPN encriptado, aunque se intercepte una transmisión de datos, no podrá descifrarse

Puedes visitar **https://www.fcc.gov/consumers/guides/how-protect-yourself-online** para obtener más información acerca de la protección al usar redes inalámbricas.

No habilite el Bluetooth den lugares publicaos, ya que estos dan oportunidades a hackers para encontrar fallos y aprovecharlos, por ejemplo, control de forma remota del dispositivo o espiar al dispositivo, distribución del malware y consumir batería. Para evitar esto, desactiva el bluetooth cuando no lo utilices

## 🔠 UTILIZA CONTRASEÑAS ÚNICAS PARA CADA CUENTA EN LÍNEA

**Consejos para elegir una buena contraseña**:

- No use palabras del diccionario o nombres en ningún idioma.
- No emplee errores ortográficos comunes de palabras del diccionario.
- No emplee nombres de equipos o cuentas.
- De ser posible, utilice caracteres especiales como " ! @ # $ % ^ & * ( )".
- Use una contraseña con diez o más caracteres.

| Aceptable | Buena | Mejor |
|---|---|---|
| allwhitecat | a11whitecat | A11whi7ec@t |
| Fblogin | 1FBLogin | 1.FB.L0gin$ |
| ilikeGoLearning | 1LikeG0Learning | 1L1k3G0L34rnin6 |

## 📑 USA UNA FRASE EN LUGAR DE UNA PALABRA COMO CONTRASEÑA

**Sugerencias para elegir una buena frase:**

- Elija una oración que signifique algo para usted.
- Agregue caracteres especiales, Ej: ! @ # $ % ^ & * ( ).
- Mientras más larga, mejor.
- Evite oraciones populares o famosas, por ejemplo, letras de una canción popular.

**Resumen de las nuevas pautas:**

- Esta debe tener una longitud mínima de 8 caracteres, pero no más de 64 caracteres.
- No emplee contraseñas frecuentes ni que se puedan adivinar con facilidad; por ejemplo, contraseña, abc123.
- No hay reglas de composición, como el tener que incluir números y letras mayúsculas y minúsculas.
- Mejore la precisión de escritura permitiendo que el usuario vea la contraseña mientras la escribe.
- Se permiten todos los caracteres de impresión y espacios.
- Sin pistas de contraseña.
- Sin fecha de caducidad periódica o arbitraria de la contraseña.
- Sin autenticación basada en conocimientos, tales como información de preguntas secretas compartidas, datos de marketing, historial de transacciones.

Puedes visitar **https://pages.nist.gov/800-63-3/** para obtener más información sobre el requisito de contraseña mejorado del NIST.

# 🔗 MANTENIMIENTO DE DATOS

## 🔐 LA ENCRIPTE SUS DATOS

a encriptación es el proceso de conversión de la información a un formato que una parte no autorizada no puede leer. Solo una persona de confianza autorizada con la contraseña o clave secreta puede descifrar los datos y acceder a ellos en su formato original. La encriptación en sí misma no evita que una persona intercepte los datos. La encriptación únicamente puede evitar que una persona no autorizada vea o acceda al contenido.

El sistema de encriptación de archivos (EFS, Encrypting File System) es una característica de Windows que permite encriptar datos. El EFS está directamente vinculado a una cuenta de usuario determinada. Solamente el usuario que cifró los datos puede acceder a estos una vez encriptados con el EFS. Para encriptar datos con EFS en todas las versiones de Windows, siga estos pasos:

**Paso 1**: Seleccione uno o más archivos o carpetas.

**Paso 2**: Haga clic derecho en los datos seleccionados y en **>Propiedades**.

**Paso 3**: Haga clic en **Opciones avanzadas...**

**Paso 4**: Seleccione la casilla de verificación **Encriptar contenido para proteger datos**.

**Paso 5**: Las carpetas y los archivos encriptados con el EFS se muestran en verde, como se muestra en la ilustración.

## 💾 REALICE UN RESPALDO DE SUS DATOS

Su disco duro puede fallar. Su computadora portátil puede perderse. Pueden robar su teléfono. Quizá borró la versión original de un documento importante. Tener un respaldo puede evitar la pérdida de datos irreemplazables, como fotos familiares. Para hacer un respaldo correcto de los datos, necesitará una ubicación de almacenamiento adicional para los datos y deberá copiar los datos en dicha ubicación periódica y automáticamente.

La ubicación adicional para los archivos de copia de seguridad puede estar en su red doméstica, una ubicación secundaria o la nube. Si almacena los respaldos de los datos de manera local, tendrá el control total de los datos. Puede decidir copiar todos sus datos en un dispositivo de almacenamiento

conectado a la red (NAS), un disco duro externo simple o puede seleccionar solo algunas carpetas fundamentales para hacer un respaldo en unidades de memoria USB, CD/DVD o incluso cintas. En dicho escenario, es usted el propietario y es totalmente responsable del costo y el mantenimiento de los equipos del dispositivo de almacenamiento. Si contrata un servicio de almacenamiento en la nube, el costo depende de la cantidad de espacio de almacenamiento que necesita. Con un servicio de almacenamiento en la nube, como Amazon Web Services (AWS), tendrá acceso a sus datos de respaldo siempre que tenga acceso a su cuenta. Cuando contrata servicios de almacenamiento en línea, es posible que deba ser más selectivo respecto de los datos que respalda debido al costo del almacenamiento y las constantes transferencias de datos en línea. Uno de los beneficios de guardar un respaldo en una ubicación alternativa es que es seguro en caso de incendio, robo u otro desastre, excepto que falle el dispositivo de almacenamiento.

## ❌ ELIMINACIÓN DE SUS DATOS EN FORMA PERMANENTE

- Los datos no se eliminan de forma permanente de los discos duros cuando los eliminas de la papelera de reciclaje, debido a los rastros magnéticos, si quieren borrarse de forma definitiva, deben sobreescribirse 1 y 0 para que los datos no se puedan encontrar, aunque algunos forenses informáticos pueden recuperarlos o en laboratorios especiales,
- Unos programas para elimitar datos son
    - Windows SDelete
    - Linux Shred
    - MacOSX Secure Empty Trash

La única forma de destruir los datos es deshacerse del dispositivo de almacenamiento, ya sea destruyéndolo o ejecutando otro proceso