

LA INFORMACIÓN

Proteja la información en su centro de Trabajo

- Establezca acuerdos de confidencialidad con personas que manejen información institucional sensible.
- Use lineamientos de resguardo y protección de la información. Permita el acceso a los usuarios únicamente a la información necesaria para realizar su trabajo.
- Aplique medidas para evitar accesos no autorizados y detectar intentos de acceso a la información.
- Clasifique y cifre la información confidencial.
- Haga copias de seguridad de la información importante, confidencial y sensible.
- Compruebe que sus copias de seguridad funcionen correctamente.
- Elimine los atributos de los archivos (metadatos), antes de enviar o compartir los archivos. Para mayor información, visite el siguiente enlace:



<https://docs.google.com/document/d/1avw6h5euiZgqzkWakkl8ZCUOYHE7XCYwLV239ygwSGs/edit>

Información confidencial información que requiera de medidas de seguridad para evitar su difusión. No importa el medio de almacenamiento, el tipo de información o si se ha comunicado verbalmente.

- LA LEGISLACIÓN Y NORMATIVA en materia de protección de información puede ser consultada en algunas leyes como:



LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES Ley n.o 8968, **LEY DE PROCEDIMIENTOS DE OBSERVANCIA DE LOS DERECHOS DE PROPIEDAD INTELECTUAL** ley el N° 8039, **LEY DE MARCAS Y OTROS SIGNOS DISTINTIVOS** ley N° 7978 y R-102-2015 “Directrices de Seguridad de Información de la Universidad de Costa Rica”.

- EL CIFRADO de la información es una de las medidas más eficaces a la hora de proteger la información. Debemos cifrar la información vital de la Institución, los datos personales y cualquier información sensible que vayamos a enviar a terceros. Para mayor información, visite el siguiente enlace:

<https://docs.google.com/document/d/12WZUJKI37CKINru9Uf8W03B0qwKw6qaps0GHnm9qtXY/edit>

LA INFORMACIÓN

Proteja la información en su centro de Trabajo

- Establezca acuerdos de confidencialidad con personas que manejen información institucional sensible.
- Use lineamientos de resguardo y protección de la información. Permita el acceso a los usuarios únicamente a la información necesaria para realizar su trabajo.
- Aplique medidas para evitar accesos no autorizados y detectar intentos de acceso a la información.
- Clasifique y cifre la información confidencial.
- Haga copias de seguridad de la información importante, confidencial y sensible.
- Compruebe que sus copias de seguridad funcionen correctamente.
- Elimine los atributos de los archivos (metadatos), antes de enviar o compartir los archivos. Para mayor información, visite el siguiente enlace:



<https://docs.google.com/document/d/1avw6h5euiZgqzkWakkl8ZCUOYHE7XCYwLV239ygwSGs/edit>

Información confidencial información que requiera de medidas de seguridad para evitar su difusión. No importa el medio de almacenamiento, el tipo de información o si se ha comunicado verbalmente.

- LA LEGISLACIÓN Y NORMATIVA en materia de protección de información puede ser consultada en algunas leyes como:



LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES Ley n.o 8968, **LEY DE PROCEDIMIENTOS DE OBSERVANCIA DE LOS DERECHOS DE PROPIEDAD INTELECTUAL** ley el N° 8039, **LEY DE MARCAS Y OTROS SIGNOS DISTINTIVOS** ley N° 7978 y R-102-2015 “Directrices de Seguridad de Información de la Universidad de Costa Rica”.

- EL CIFRADO de la información es una de las medidas más eficaces a la hora de proteger la información. Debemos cifrar la información vital de la Institución, los datos personales y cualquier información sensible que vayamos a enviar a terceros. Para mayor información, visite el siguiente enlace:

<https://docs.google.com/document/d/12WZUJKI37CKINru9Uf8W03B0qwKw6qaps0GHnm9qtXY/edit>

- Las copias de seguridad garantizan la continuidad de las operaciones y servicios de TIC en nuestra Institución, ya que permite recuperar datos en caso de pérdida o fallo. Es fundamental establecer aspectos como la frecuencia, el tipo de copia y el medio donde se realizan y comprobar cada cierto tiempo que funcionen correctamente.
- Es necesario clasificar y definir niveles de información así como las medidas de seguridad oportunas para su correcto tratamiento.

- Las copias de seguridad garantizan la continuidad de las operaciones y servicios de TIC en nuestra Institución, ya que permite recuperar datos en caso de pérdida o fallo. Es fundamental establecer aspectos como la frecuencia, el tipo de copia y el medio donde se realizan y comprobar cada cierto tiempo que funcionen correctamente.
- Es necesario clasificar y definir niveles de información así como las medidas de seguridad oportunas para su correcto tratamiento.