Uruguay Presidencia | agesic

Kit de concientización
Guía de implementación

Seguridad de la Información. Gestión y Auditoría

Versión 1.0

Año 2021

Tabla de Contenido

1 Objetivo

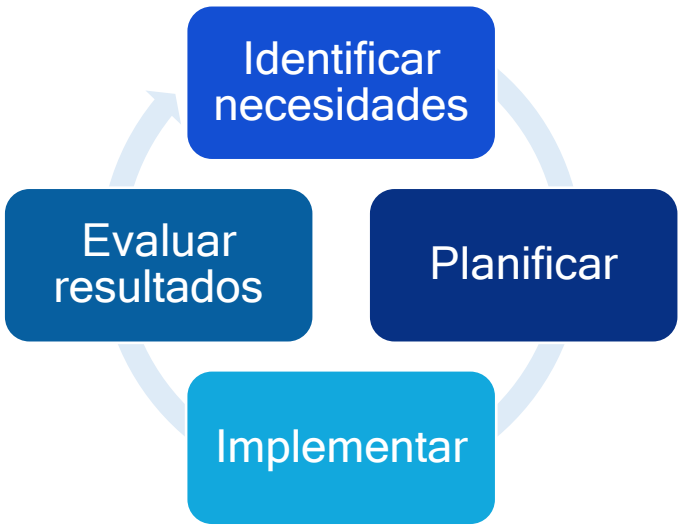
Esta guía tiene por objetivo facilitar a las organizaciones la planificación y realización de instancias periódicas de concientización en seguridad de la información dirigidas a todas las personas que trabajen en ella y a otros involucrados, como clientes y proveedores.

Para realizar estas instancias serán útiles los materiales gráficos y audiovisuales disponibles en *Seguro te Conectás en* el portal de Agesic.

2 Fases de implementación

Cada organización es diferente, con misiones y objetivos definidos, por lo que se recomienda adaptar las fases o materiales propuestos, a las particularidades de cada una.

Las actividades que se realizan para la concientización en aspectos de seguridad de la información pueden agruparse en 4 grandes fases: identificar necesidades, planificar, implementar y evaluar resultados.



2.1 Identificar necesidades

Esta etapa podrá realizarse a través de una encuesta donde se pregunta a quienes trabajan en la organización sobre sus hábitos y conocimientos de los aspectos claves de seguridad de la información. También se podrían tomar como insumos los incidentes ocurridos en un periodo dado; u otros elementos que denoten la necesidad de reforzar la concientización.

Estas iniciativas podrán dirigirse a toda la organización o un grupo particular sobre los que se hayan previamente identificado necesidades específicas de sensibilización.

En términos generales, el resultado de esta etapa mostrará la necesidad de comunicar aspectos que pueden referirse a:

- políticas y procedimientos vigentes, teniendo en cuenta al público objetivo de cada una de ellas
- hábitos y capacidades para tener contraseñas seguras
- prevención de ataques de ingeniería social, como el *phishing*
- prevención de infección de *malware* en los dispositivos
- gestión de la información de la organización sea esta física o digital

Se puede disponer de este tipo de encuestas en la sección *Anexo II: Cuestionario para evaluar hábitos y conocimientos referentes a Seguridad de la Información.*

Esta fase es importante porque:

- permite tener una representación actualizada del conocimiento de quienes trabajan en la organización respecto a los aspectos claves de seguridad de la información.
- es un insumo fundamental para la etapa de planificación de las instancias ya que permite saber sobre qué aspectos claves de la seguridad de la información debemos reforzar y a quiénes deberá ir dirigida.

2.2 Planificar

Teniendo en cuenta el resultado de la fase anterior, en esta etapa se realizará el plan de concientización que incluirá todas las actividades a realizar durante el año.

Para el desarrollo de este plan se deberá tener presente:

- **Qué** objetivos están planteados, lo que permitirá seleccionar los temas a tratar.
- Quiénes serán los responsables de esas comunicaciones.
- A **quiénes** van a dirigirse las acciones: alta dirección, mandos medios, administrativos, tecnología, proveedores, o cualquier otra segmentación que se entienda pertinente.
- Qué **materiales** hay disponibles y cuáles requieren adaptación según el tipo de organización. *Anexo I: Materiales gráficos y audiovisuales disponibles*.
- Qué **canales** serán utilizados para la comunicación, por ejemplo, correo electrónico, publicación en la intranet de la organización, algún directorio compartido, webinar, charlas o talleres presenciales, etc.
- Dónde se dejarán disponibles los materiales brindados, de forma de facilitar su consulta posterior.
- Cómo se evaluará cada instancia de concientización.

Además, se recomienda definir y/o establecer:

- un **cronograma** para las instancias de concientización planificadas el cual dirigirá la ejecución del proceso formativo. Cada organización debe tener en cuenta las particularidades de su negocio para establecer un cronograma propio.
- Los **recursos** económicos, materiales y humanos requeridos para cada instancia.
- **Actividades** de evaluación, seguimiento y mejora

A continuación, se muestra un ejemplo de cronograma que utiliza semanas como unidad de tiempo, para la definición de los aspectos mencionados.

2.2.1 Cronograma general

Cronograma por Semana																			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	A																		
		B	B																
				C	C	C													
							D	D	D	D	D	D	D	D	D				
																E	E		
																		F	F
G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G

A	Definir y armar la encuesta inicial
B	Lanzamiento de encuesta y análisis de resultados
C	Planificación de concientización, preparación de mensajes y materiales a utilizar en la comunicación
D	Ejecución de las instancias planificadas
G	Recursos educativos a utilizar a lo largo de todo el proceso
E	Definir y armar la evaluación
F	Lanzamiento de encuesta y análisis de resultados

2.3 Implementar

En esta etapa se ejecutan las actividades definidas en el plan de concientización elaborado en la etapa anterior, utilizando los recursos formativos elegidos, de forma organizada y espaciada de acuerdo al cronograma estipulado. Las distintas acciones que se lleven a cabo deberán cumplir con los objetivos de concientización planteados, como: transmitir información útil sobre seguridad de la información o bien compartir consejos o buenas prácticas a la hora de manejar la información de la organización.

2.4 Evaluar resultados

De manera similar a la fase de *Identificar necesidades* se volverá a preguntar sobre el conocimiento de aspectos claves trabajados durante la implementación del plan de concientización.

Se puede disponer de este tipo de encuestas en la sección *Anexo II: Cuestionario para evaluar hábitos y conocimientos referentes a Seguridad de la Información.*

Esta fase es importante porque permite tener una representación de las mejoras de hábitos y conocimiento de quienes trabajan en la organización respecto aspectos claves de seguridad de la información. Además, es un insumo fundamental para la planificación de nuevas instancias de concientización, ya que brinda información sobre qué aspectos claves aún no quedan claros o necesitan continuar abordándose, si los medios utilizados fueron los adecuados, y cualquier otro aspecto que se pueda mejorar.

3 Proceso educativo

El proceso educativo de las personas que trabajan en la organización respecto a seguridad de la información debe ser continuo. El primer hito que marca esta necesidad es el ingreso de una persona a trabajar en la organización. Tener disponibles cursos de inducción que permita a quien ingrese a adoptar habilidades, conocimientos, y hábitos básicos, sobre seguridad de la información.

Se puede utilizar el curso disponible en la sección

Cursos *del portal de Agesic.*

Anualmente se deberá generar un nuevo plan de concientización que atienda las necesidades de la organización alineado a las nuevas amenazas que surjan.

4 Anexo I: Materiales gráficos y audiovisuales disponibles

4.1 Guías

- Guía de ciberseguridad para pequeñas empresas y emprendimientos
- Guía para la gestión de vulnerabilidades
- Guía didáctica de Seguridad de la Información

4.2 Infografías con recomendaciones de seguridad

- 5 claves para mejorar la ciberseguridad de una empresa o emprendimiento
- Usá contraseñas para proteger tus datos
- Realizá copias de seguridad
- Mantené seguros tus dispositivos móviles
- Protegé tu empresa de malware
- Prevení ataques de phishing
- Uso de Redes sociales en mi empresa o emprendimiento
- Medios de pago

4.3 Otras Imágenes

- Calendario de consejos diarios
- Afiches Seguro te conectás
- Trípticos

4.4 Didácticos

- Juegos Seguro te Conectás

4.5 Videos

- Contraseña segura
- Tarjeta de crédito
- Compras online
- Phishing

4.6 Cursos

- Seguridad de la Información

4.7 Más información en:

- Glosario de términos de ciberseguridad
- Contraseñas: recomendaciones y buenas prácticas
- ¿Qué es un ataque de phishing?
- ¿Qué es el Ransomware?
- Seguridad en los dispositivos móviles
- Doble factor de autenticación
- Software para proteger sistemas
- Uso de redes sociales en empresas o emprendimientos
- Medios de pago

5 Anexo II: Cuestionario para evaluar hábitos y conocimientos referentes a Seguridad de la Información

#	Pregunta	Opciones de respuesta	Valor
1	La seguridad de la información es	El conjunto de medidas preventivas y reactivas, tomadas por personas, sistemas y organizaciones que permitan resguardar y proteger la información buscando mantener su confidencialidad, disponibilidad e integridad.	Correcto
		Mantener actualizado el antivirus de cada equipo.	
		No lo tengo claro	
2	La política de seguridad de mi empresa se encuentra en	Una carpeta en un directorio compartido	
		La nube	
		No sé dónde está	
3	¿Qué debería incluir una contraseña segura?	Mi nombre o algún dato personal que pueda recordar	
		Hasta 8 caracteres	
		Una combinación de caracteres alfanuméricos, símbolos especiales y un largo de más de 8 caracteres	Correcto
4	¿Cuál de los siguientes ejemplos de contraseñas consideras la más segura?	..L0p3Z*.*	
		%CE184l%	
		Par4lel3pip3dO_9102.	Correcto
5	El *Phishing* es	Acción que busca obtener datos de acceso a un dispositivo	
		Acción que busca obtener información personal	
		Técnica que simula servicios web conocidos	
		Las definiciones anteriores son correctas	Correcto
		No lo tengo claro	
6	Indica cuál/es de las siguientes alternativas son prácticas seguras en el uso de computadoras compartidas. (Marcá todas las que te parezcan correctas)	Utilizarla para ingresar a mi cuenta de banco	
		Asegurarme de cerrar sesión en las redes sociales, navegadores, correo electrónico o la máquina antes de retirarme	Correcto
		Evitar seleccionar “Guardar contraseña”	Correcto
		Compartir mi contraseña con personas de mi mayor confianza para facilitar el uso	
		Guardar los documentos en el escritorio de la computadora así puedo seguirlos trabajando otro día	
7	El *Ransomware* se caracteriza por	Robar información bancaria y enviarla a bandas delictivas	
		Secuestrar información local del equipo y pide rescate	Correcto
		Espiar por la cámara web	
8	¿En qué situaciones reportarías un	Correo que parece phishing	Correcto
		Desaparecen documentos de la NAS	Correcto

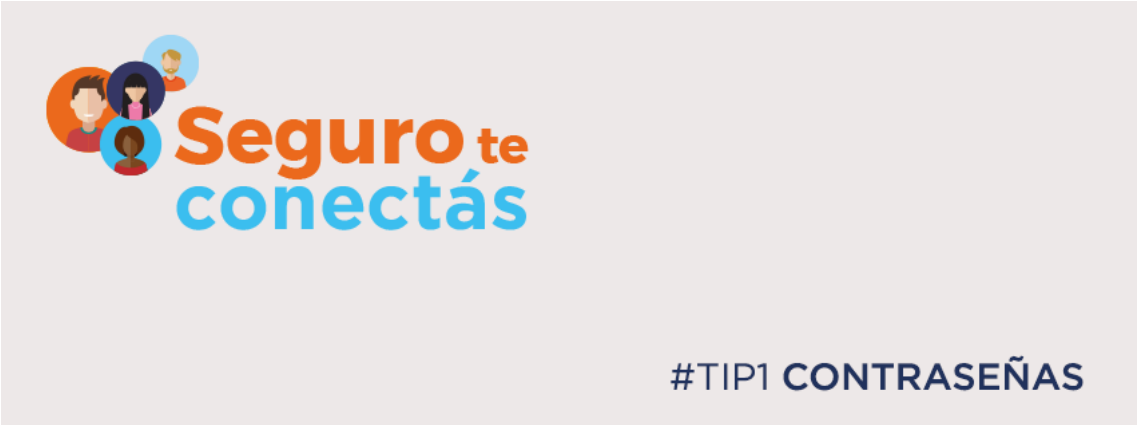
	posible incidente de seguridad?	Perdí o me robaron mi celular donde tengo información y contactos de la empresa.	Define la empresa según su Política.
		Se rompió la impresora	
9	¿Qué riesgos implica utilizar una memoria USB?	No pueden guardar fotos	
		Pueden tener virus	Correcto
		Son caras	
10	Indica la respuesta correcta	La documentación en formato físico puede contener información confidencial, que debe estar siempre bajo custodia del empleado y ser guardada en un lugar seguro al terminar la jornada laboral	Correcto
		Las contraseñas de acceso a los servicios corporativos pueden apuntarse en un post- it para que sean más fáciles de recordar	
		No es necesario que el puesto de trabajo esté limpio y ordenado	
		Las memorias USB y discos duros externos pueden estar siempre conectados al dispositivo incluso cuando termina la jornada laboral	
11	¿Cuáles son las buenas prácticas para protección del puesto de trabajo?	Contar con una política de escritorios limpios, difundirla y hacerla cumplir	
		Mantener todo el software actualizado	
		Instalar, activar y mantener actualizados los antivirus y cortafuegos	
		Bloquear la sesión cuando dejamos el puesto desatendido	
		Todas las anteriores	Correcto
12	¿Qué hay que hacer cuando un dispositivo deja de ser útil para la empresa?	Desecharlo en el contenedor o ubicación específica para tal fin sin necesidad de llevar a cabo ninguna acción sobre el mismo.	
		Solamente si se va a volver a dar uso al dispositivo debe realizarse un borrado seguro de la información	
		Aplicar un borrado seguro al dispositivo independientemente si este va a ser reutilizado o no	Correcto
13	En los perfiles de las redes sociales de la empresa, las opciones de privacidad:	Deben ser lo más débiles posibles a fin de poder llegar a la mayor cantidad de personas	
		Deben revisarse y estar configuradas adecuadamente manteniendo un equilibrio entre privacidad e interacción con las personas	Correcto
		Deben estar configuradas lo más restrictivamente posible	
		No son importantes ya que los perfiles empresariales no presentan ningún riesgo	
14	¿Las redes sociales pueden ser utilizadas	No, ese tipo de acciones se realizan siempre fuera de las redes sociales.	

	por ciberdelincuentes para cometer fraudes?	No, ya que las redes sociales cuentan con mecanismos de protección lo suficientemente robustos como para evitar cualquier acción maliciosa.	
		Sí, pueden realizar distintos tipos de fraude como suplantaciones, campañas de *malware* o *phishing*	Correcto
15	En caso de recibir un documento adjunto por medio de una red social	Se debe abrir inmediatamente ya que la agilidad de respuesta en este tipo de herramientas es clave para generar confianza en el usuario.	
		Se puede abrir sin ningún riesgo ya que la red social eliminaría todo rastro de malware en caso de existir	
		Se debe abrir sin ningún tipo de riesgo a no ser que la extensión del archivo sea .exe	
		Se deben seguir las mismas recomendaciones de seguridad que en el caso de archivos adjuntos en el correo electrónico.	Correcto
16	¿Los dispositivos móviles, como smartphones y tablets, pueden infectarse con malware?	No, están diseñados para no infectarse	
		Sí, todos los dispositivos pueden infectarse	Correcto
		Sí, pero solamente si se descargan aplicaciones de tiendas no oficiales	
17	Utilizar redes wifi de lugares públicos es	Una práctica recomendable, ya que así se reduce el consumo de datos de la tarifa móvil.	
		Una práctica desaconsejable, ya que la red puede estar bajo el control de un atacante y toda la información que se envía y recibe puede ser espiada.	Correcto
18	Ante una comunicación por correo electrónico cuyo remitente parece legítimo pero existen sospechas sobre su legitimidad, la mejor forma de proceder es:	Acceder a lo que solicita el correo, pero esto solamente si es abrir un archivo adjunto ya que los enlaces son más peligrosos.	
		Comprobar la casilla de correo, que contenga el dominio adecuado, y ante la menor duda no interactuar con el correo de ninguna manera. Además es recomendable borrarlo directamente para evitar futuras situaciones peligrosas.	Correcto
		Acceder a lo que solicita el correo, pero esto solamente si solicita abrir un enlace o responder a la propia comunicación ya que los archivos adjuntos son más peligrosos.	
		Ninguna de las anteriores.	

6 Anexo III: Modelos de mensajes a comunicar

6.1 #Tip1- Contraseñas: recomendaciones y buenas prácticas

Cada vez es más fácil comprar y acceder a distintos servicios en línea, lo que representa un gran avance, pero también supone retos en cuanto a la seguridad y la privacidad de nuestros datos en la red.



Compartimos algunos consejos para crear contraseñas seguras:

¡Fácil de recordar, difícil de adivinar!

- Creá contraseñas que tengan letras mayúsculas y minúsculas, espacios, símbolos y números. Además, es importante que tenga ocho o más caracteres; esto disminuye la posibilidad de adivinarla.
- Si el sitio donde estás creando una cuenta te ofrece utilizar una “pregunta de seguridad”, para recuperar tu clave en caso de olvidarla, no utilices una pregunta trivial.
- Cambiá la contraseña varias veces al año.

¡La contraseña es tuya!

No las compartas con otras personas ni las dejes escrita en lugares visibles.

Recordá cerrar la sesión al terminar de utilizar el servicio.

Nunca compartas datos como tu usuario o tu contraseña por correo electrónico. Si recibís un correo que te solicita estos u otros datos, no lo contestes y notificá a la empresa u organización que dice ser la que envió el correo.

¡Utilizá la creatividad!

No uses la misma contraseña para más de un sitio aplicación y evitá repetir contraseñas anteriores.

Evitá asociarlas a datos personales que permitan su deducción, como nombres, fechas, números de documento, dirección, teléfono, etc.

- No utilices palabras relacionadas con el sitio. Por ejemplo, si lo que se está creando es una cuenta de Facebook no uses claves como “face” o “facebook”.

Estrategias para crear contraseñas seguras

1. Podés generarla a partir de una frase larga

Creá una frase que te resulte familiar.

Ejemplo: "La pizza fría me encanta"
Contraseña: **LaPizzaFríaMeEnc@nt@**

Acá se utiliza un mecanismo de generación de contraseñas en el que cada palabra comienza con mayúscula; la última palabra sustituye las vocales por números o símbolos.

2. Podés generarla a partir de una frase

- Identificá una frase larga que te resulte fácil de recordar.

Ejemplo: "Todas las mañanas me levanto a la misma hora y como tres galletas".
Contraseña: **TlmmlalmhyC3G**

Acá se utiliza un mecanismo en el cual la contraseña toma la primera letra de cada palabra y comienza y termina siempre con mayúsculas. Recuerda incluir algún número y/o símbolo.

3. Utilizá gestores de contraseñas

Los gestores de contraseñas, además de guardarlas, te permiten crear contraseñas fuertes.

Ejemplos de gestores: KeePass, Password Safe y los provistos por soluciones antivirus, entre otros.

Divertite probando contraseñas en la plataforma de juegos de Agesic

MAS INFORMACIÓN

bit.ly/STC_Contraseñas

CONTACTO

Para reportar un incidente escribir a: ejemplo@ejemplo.uy

Por dudas o consultas escribir a: ejemplo@ejemplo.uy

6.2 #Tip2- Phishing

El Phishing es una técnica de ingeniería social que consiste en un correo electrónico, en el que el remitente simula ser una entidad legítima (red social, banco, institución pública, etc.)

Prevení ataques de *Phishing*

Estos correos, pueden tener adjuntos, archivos infectados o enlaces a páginas fraudulentas, con el objetivo de obtener información privada, un cargo económico o infectar el dispositivo.

A través de estos mensajes, alegando problemas técnicos, cambios en las políticas de seguridad, entre otros, suelen solicitar la confirmación de sus datos de usuario, contraseñas u otros datos personales.

Conocé algunas variantes:

- ***Spear***

El *Spear Phishing* es similar al *Phishing*, pero está dirigido a personas, empresas u organizaciones específicas.

- ***Whaling***

Un *Whaling* utiliza un método similar al *Phishing* pero se caracteriza porque el remitente del mensaje simula ocupar cargos de nivel superior en una organización y así, mediante suplantación de identidad, engañar a gerentes y directivos dentro de una misma organización, con el objetivo de recibir una transferencia, conseguir información confidencial u obtener acceso a sus sistemas informáticos con fines delictivos.

- ***Smishing***

El *Smishing* es aquel que utiliza los mensajes de texto para realizar el engaño, ya sea por SMS, *WhatsApp* o cualquier red de mensajería. Generalmente quieren que nos dirijamos al link enviado, o que respondamos al número de teléfono sugerido.

- Vishing

El medio utilizado para el engaño, en este caso, puede ser una llamada telefónica. La persona que se comunica, a través de una suplantación de identidad, intenta generar confianza para conseguir información personal o de la empresa.

¿Cómo podemos prevenir estos ataques?

Evitá brindar información personal o confidencial por correo electrónico o por teléfono. En caso de recibir una notificación de este tipo, comunícate con la organización para verificar su validez.

- **Verifica que la cuenta es original**

Comprobá que el email coincide con la empresa que envía el correo. Generalmente utilizan dominios públicos o que se parecen al correo oficial.

- **Sentido de urgencia**

Habitualmente los correos de *Phishing* piden el envío de información o respuesta con urgencia, por ejemplo "¡*si no responde a este correo en la próxima hora dejará de acceder al correo institucional!*"

- **Comprobá la ortografía y redacción**

Muchos de los correos de *Phishing* contienen errores ortográficos o de redacción, debido al uso de traductores automatizados. La estética también se asemeja mucho a la original, pero algún detalle siempre se escapa.

- **Revisá la URL**

Cuando recibas un correo con un acceso a un sitio en línea, (e-banca, compras, redes sociales, etc,) evitá hacerlo a través de enlaces e ingresá manualmente la dirección en el navegador o revisa la URL del enlace antes de hacer clic en él.

Antes de iniciar sesión en el sitio, confirmá que la dirección web sea la correcta y corroborá que en la barra del navegador aparezca el candado que indica la autenticidad del sitio.

- **¿Recibiste archivos adjuntos?**

Cuando recibas un archivo adjunto en un correo, corroborá que sea de un remitente conocido y si esperabas recibirlo. Si no podés confirmar que se trata de un mensaje legítimo, desestima el archivo, no lo abras ni descargues.

MAS INFORMACIÓN

bit.ly/STC_Phishing

Mirá el video de phishing

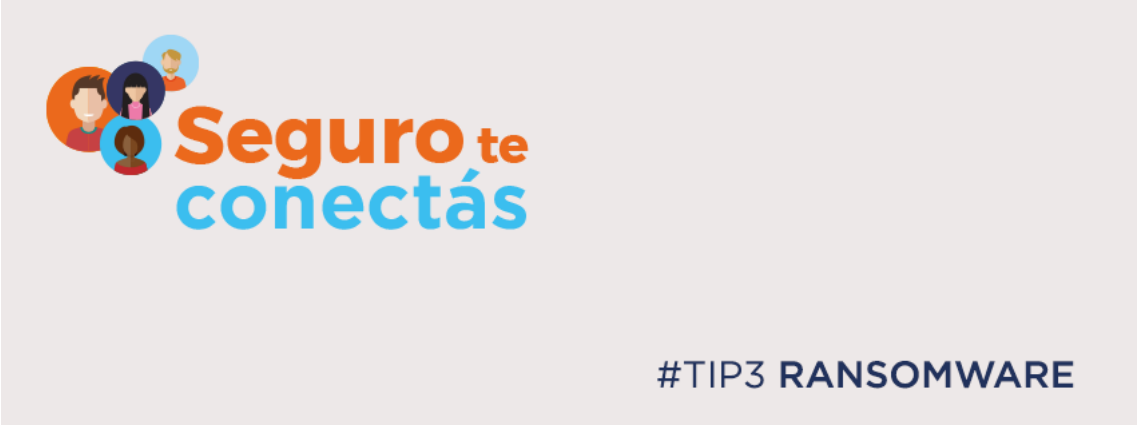
CONTACTO

Para reportar un incidente escribir a: ejemplo@ejemplo.uy

Por dudas o consultas escribir a: ejemplo@ejemplo.uy

6.3 #Tip3- Ransomware

El *Ransomware* es un tipo de *Malware*, equivalente a un secuestro informático de la información.



Secuestro de datos: ¿tenés tu información respaldada?

El *Ransomware* (de “ransom” en inglés que significa “rescate”) es un tipo de *Malware* que restringe el acceso a la información y que, para desbloquearla, generalmente, quien ataca pide dinero a cambio.

Este tipo de *Malware* puede causar graves daños, impidiendo acceder a los datos o incluso a las aplicaciones que se utilizan en el día a día tanto por personas como organizaciones.

Objetivos:

- Los ataques de *Ransomware* se caracterizan por exigir a la víctima un rescate a cambio de la liberación de los datos. Si se logra robar información, además de infectar los sistemas y bloquearlos, existe el riesgo de exposición de esa información para:
    - Amenzar a la víctima con hacer públicos los datos robados.
    - Vender los datos robados en una subasta, en cuyo caso, los datos confidenciales de la persona u organización atacada, irán al mejor postor, ya sea la misma víctima, como cualquier otra organización legal o criminal.

Ejemplos de casos recientes:

Colonial Pipeline en EEUU

Un ciberataque a Colonial Papeline, la mayor empresa de oleoductos de Estados Unidos responsable del 45% de los suministros de combustible para el este de Estados Unidos, obligó al país a declarar estado de emergencia.

El oleoducto, cuyos propietarios incluyen Royal Dutch Shell (RDSA) y Koch Industries, declaró que "desconectó proactivamente ciertos sistemas para contener la amenaza" e

inmediatamente contrató a terceros expertos cibernéticos para iniciar una investigación.

Tener medidas de seguridad establecidas en los marcos regulatorios son la base de prevención de este tipo de ataques.

Servicio Público de Empleo Estatal en España

En marzo de este año, el *Ransomware Ryuk*, paralizó sistemas internos del Servicio Público de Empleo Estatal (SEPE) de España, durante dos semanas.

El alcance fue bastante grande en cuanto a número de equipos y sistemas afectados. Según expresó la Central Sindical Independiente y de Funcionarios (CSIF), este *Malware*, paralizó la actividad tanto en las 710 oficinas que prestan servicio presencial, como en las 52 telemáticas.

Este mismo ransomware afectó posteriormente al Ministerio de Trabajo del mismo país, entre otros, paralizando nuevamente las operaciones de los organismos.

En Uruguay

En nuestro país se dieron algunos casos en los que quienes realizaron los ataques, se justificaron afirmando que realizaban esta actividad maliciosa a personas usuarias que navegaban en sitios de pornografía infantil. Sin embargo, no es necesariamente real, debido a que se utilizaron estos mensajes para chantajear a la víctima evitando que pida ayuda públicamente y hacerse así del dinero más fácilmente.

Algunas víctimas, debido a la necesidad de acceder a la información, no han tenido otra alternativa que pagar el rescate; pese a que esta medida es totalmente desaconsejada.

Tomando las medidas básicas de protección de la información, este tipo de ataques no sería tan efectivo.

¿Qué medidas de protección podemos tomar?

Algunas de las claves de prevención son:

- Mantener actualizado el Software de la PC.
- De ser posible utilizar un firewall.
- Evitar abrir correos de procedencia desconocida.
- No hacer clic en vínculos sospechosos.
- Realizar respaldos de la información frecuentemente siguiendo los procedimientos vigentes.

Sin embargo, a pesar de tomar todas las medidas antes nombradas, nadie está exento de ser víctima de un ataque informático. Es por esto que **es imprescindible contar con un respaldo de la información**. De esta manera, en caso de ser víctima de un ataque de *Ransomware*, se podrá levantar el respaldo minimizando así la pérdida de información.

MAS INFORMACIÓN

bit.ly/STC_Malware

CONTACTO

Para reportar un incidente escribir a: ejemplo@ejemplo.uy

Por dudas o consultas escribir a: ejemplo@ejemplo.uy

6.4 #Tip4 - Respaldos

Para que podamos dar continuidad a nuestro trabajo, es fundamental que usemos XXXXXXXXXXXXXXXX como repositorio único de información.

Este espacio de almacenamiento se controla y respalda periódicamente, por lo que podemos utilizarlo para guardar documentación de nuestro trabajo de forma segura.

Recordá:

- Utilizá los repositorios provistos por la organización para este fin.
- Evitá almacenar información como música, videos, imágenes y otros documentos personales en estos medios.
- Es responsabilidad personal mantener los respaldos de la información en los equipos y de los correos descargados de forma local.

Es importante que no almacenes información de la empresa en sitios o dispositivos no recomendados. Utilizar sistemas externos puede determinar brechas de seguridad.

MAS INFORMACIÓN

bit.ly/STC_Respaldos

CONTACTO

Para reportar un incidente escribir a: ejemplo@ejemplo.uy

Por dudas o consultas escribir a: ejemplo@ejemplo.uy

6.5 #Tip5- Antivirus

Es un tipo de software cuyo objetivo es detectar y eliminar Malware, término que refiere a un software malicioso, del inglés malicious software.

Con el transcurso del tiempo, los antivirus han evolucionado hacia programas más avanzados que, además de buscar y detectar *Malware*, consiguen bloquearlos, limpiar archivos y prevenir su infección.

Ejemplos de *Malware* que un antivirus nos ayuda a prevenir:

- **Virus informático.** Busca modificar el funcionamiento normal del dispositivo. Requiere la interacción de una persona para propagarse a otros archivos y sistemas
- **Gusano informático.** Puede replicarse desde un dispositivo infectado a otros a través de la red, con el objetivo de lograr acceso a ordenadores de forma no autorizada.
- **Troyano.** Accede al sistema de la persona como un archivo o aplicación inofensiva y realiza acciones no deseadas en segundo plano.
- **Spyware.** Espía el dispositivo afectado. Sus funciones son recoger datos e información del dispositivo y observar la actividad de la persona sin su consentimiento.
- **Adware**. Rastrea el navegador y el historial de descargas de la persona con la intención de mostrar anuncios emergentes o banners no deseados para atraer al usuario a realizar una compra o hacer clic.

¿Cómo pueden acceder a nuestro dispositivo?

En unidades USB infectadas, SPAM, *Phishing*, algunos sitios web, por vulnerabilidades de aplicaciones o software no oficiales o no actualizados.

Recordá:

- Evitá instalar un software no autorizado o no oficial.
- Navegá por sitios seguros.
- Realizá escaneos completos frecuentemente.
- Aprovechá a escanear tu equipo cuando no vayas a utilizarlo.
- Escaneá previamente cualquier dispositivo externo que conectes a tu equipo.

Mantené siempre instalado y actualizado un antivirus en tu equipo. En caso de que la organización suministre equipos de trabajo, mencionar que antivirus tienen incorporado para ser utilizado y que políticas de actualización se recomiendan.

Reportá a ejemplo@ejemplo.uy cuando:

• Recibas un correo no deseado (SPAM, *Phishing*) enviando el texto que surge al hacer clic con el botón derecho sobre el correo sospechoso, y seleccionando dentro del menú desplegado "Mostrar original".

• Todas las alertas del antivirus o si creés que el equipo en el que estás trabajando, está infectado.

MAS INFORMACIÓN

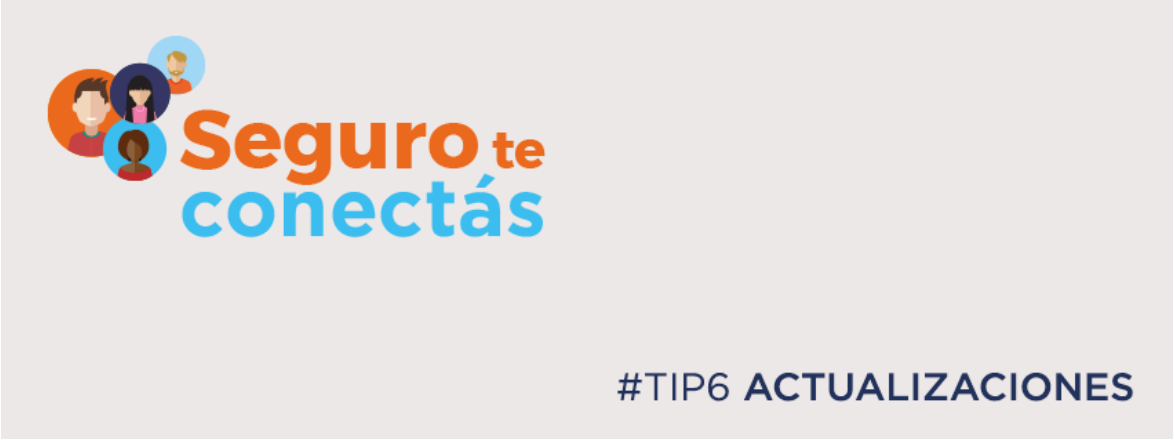
bit.ly/STC_Malware

CONTACTO

Para reportar un incidente escribir a: ejemplo@ejemplo.uy
Por dudas o consultas escribir a: ejemplo@ejemplo.uy

6.6 #Tip6- Actualizaciones

Las actualizaciones son modificaciones o complementos que se realizan sobre los sistemas operativos o aplicaciones que tenemos instalados en nuestros equipos, con el objetivo de mejorar tanto aspectos de funcionalidad como de seguridad.



Para mantener tu equipo actualizado:

• Implementá una rutina semanal para chequear las actualizaciones de todos los sistemas o programas: sistema operativo, antivirus, lectores de texto, navegadores, y cualquier otro que utilices frecuentemente.

• Aceptá la actualización del sistema operativo o de antivirus sugeridos, así como el reinicio recomendado para completar la instalación. Si no apagas tu equipo, las actualizaciones podrían no finalizar su instalación.

Recordá

En los equipos que utilices, tenés que incluir las siguientes herramientas en tu rutina de actualizaciones:

- Sistema operativo: Aclarar utilizado por la empresa
- Antivirus: Aclarar utilizado por la empresa
- Aplicaciones más utilizadas: Aclarar utilizado por la empresa
- Navegadores: Google Chrome, Microsoft Edge, Mozilla Firefox
- Aplicaciones con las que compartimos archivos: Aclarar utilizado por la empresa
- Pluggins y extenciones: PDF, Adobe Flash Player, Java, Sconnect

Agregá a la lista otros sistemas y aplicaciones que utilices frecuentemente y que refieran específicamente a tus tareas. Si necesitás ayuda para implementarla, comunicate con ejemplo@ejemplo.uy

MAS INFORMACIÓN

bit.ly/STC_Dispositivos

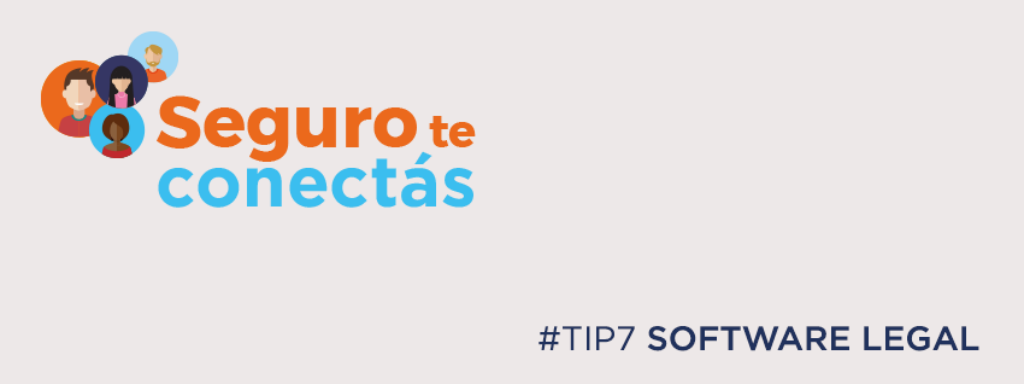
CONTACTO

Para reportar un incidente escribir a: ejemplo@ejemplo.uy

Por dudas o consultas escribir a: ejemplo@ejemplo.uy

6.7 #Tip7- Software legal

Cada una de las estaciones de trabajo que XXX pone a disposición, cuenta con un sistema operativo y software legal ya instalado para que puedas utilizar.



Cuando usamos un software ilegal o pirata, estamos accediendo a una copia no autorizada de un programa informático con derechos de autor registrados y por lo tanto no cuenta con licencia para su uso de manera legal.

Es importante que sepas que utilizar un software ilegal en tu equipo tiene riesgos:

- Utilizarlo puede provocar bajo rendimiento o pérdida y fuga de datos.
- Dejás de tener la posibilidad de actualizar programas o aplicaciones pudiendo quedar obsoletas o inseguras.
- Se pierde la garantía del fabricante del software o de nuestro dispositivo.
- Se pueden tener inconvenientes legales.

Recordá:

- Utilizá siempre software legal, en particular el sistema operativo.
- Actualizá semanalmente el sistema operativo y software de tus dispositivos.
- Descargá software solo de sitios webs del fabricante.
- Analizá el programa descargado con el antivirus antes de instalarlo.

Consultá siempre a ejemplo@ejemplo.uy si necesitás nuevas herramientas y/o tenés dudas sobre la legalidad de algún software que necesitás para desarrollar tus tareas.

MAS INFORMACIÓN

bit.ly/STC_Dispositivos

CONTACTO

Para reportar un incidente escribir a: ejemplo@ejemplo.uy

Por dudas o consultas escribir a: ejemplo@ejemplo.uy