



## Capacitación de concientización sobre la seguridad de la información y las reglas de comportamiento para el año fiscal 2010

Esta versión alternativa de la capacitación está destinada a empleados, contratistas y socios del Departamento de Agricultura de los Estados Unidos (*U.S. Department of Agriculture, USDA*) que no puedan completar su capacitación en el sitio de aprendizaje en línea, AgLearn. **Se debe hacer todo lo posible para usar AgLearn.**

Después de leer el material del curso, **debe hacer y aprobar una evaluación**, que debe estar en poder de su supervisor. Los supervisores son los encargados de tomar la prueba. Para aprobarla, es necesario obtener una calificación de 70%.

A fin de obtener **créditos por completar** esta versión de la capacitación, se debe informar y registrar que usted la completó. Su agencia le brindará información sobre cómo hacerlo.

## Concientización sobre la seguridad de los sistemas de información

### Lección 1: Introducción al curso

---

Bienvenido.

Al completar este curso, usted cumple con el requisito legal que establece que todos los usuarios de los sistemas de información federales deben realizar la capacitación anual sobre seguridad informática. Este curso está diseñado para ayudarlo a comprender la importancia de la seguridad de los sistemas de información (*Information Systems Security, ISS*), sus principios fundamentales y lo que representa para su agencia.

Le permitirá identificar posibles riesgos y vulnerabilidades asociados a los sistemas de información federales, revisará lo que usted debe hacer para proteger estos sistemas y le proporcionará pautas que debe seguir en el trabajo y en el hogar para evitar ataques a los sistemas de información.



Este curso consta de seis lecciones:

1. En la **Introducción**, se proporcionará información general sobre el curso.
2. En la lección llamada **Importancia de la seguridad de los sistemas de información**, se presentarán los principios de la ISS, su evolución y las leyes y políticas relacionadas con ella. También se introducirá el programa para la protección de infraestructuras fundamentales.
3. En la lección titulada **Amenazas para la seguridad de los sistemas de información** se explicará la diferencia entre amenazas y vulnerabilidades. Además, se proporcionará información sobre distintos tipos de amenazas.
4. En la lección llamada **Código malicioso**, se presentará el concepto de código malicioso, su impacto y los métodos que utiliza para infectar a los sistemas de información.
5. En la lección **Roles y responsabilidades del usuario**, se identificarán las pautas importantes para garantizar un sistema seguro, se definirán los niveles de clasificación para la información federal y se dará una explicación breve de su rol como usuario en la protección de esta información.
6. Por último, en la lección llamada **Seguridad del equipo personal y del hogar**, se presentarán las amenazas relacionadas con el robo de identidad y las vulnerabilidades del comercio electrónico. Además, se proporcionarán consejos de seguridad que usted debe implementar en su rutina diaria para aumentar la seguridad del equipo de su hogar.

**Una vez finalizado este curso, usted debería ser capaz de hacer lo siguiente:**

- Identificar qué es la seguridad de los sistemas de información y por qué es importante.
- Explicar la diferencia entre amenaza y vulnerabilidad e identificar los riesgos asociados a ellas.
- Comprender la amenaza que representa un código malicioso e identificar la manera de proteger los sistemas de información federales de estos códigos.
- Explicar los niveles de clasificación de la información federal e identificar lo que debe hacer para proteger dicha información.
- Identificar las pautas que debe seguir para garantizar la seguridad del equipo de su hogar.

**Concientización sobre la seguridad de los sistemas de información**  
**Lección 2: Importancia de la seguridad de los sistemas de información (ISS)**

---



Internet ha permitido que sea extremadamente fácil obtener y transferir información. Si bien la conectividad global es muy conveniente, también aumenta nuestra vulnerabilidad a ataques externos. El objetivo de la ISS es proteger nuestra información y nuestros sistemas de información.

La ISS protege la información contra el acceso o la modificación por parte de fuentes no autorizadas, y garantiza que los sistemas de información estén disponibles para sus usuarios.

Esto significa que un sistema de información seguro mantiene la **confidencialidad, integridad y disponibilidad** de la información.

**Historia de la ISS**

Hace cincuenta años, los sistemas informáticos presentaban desafíos a la seguridad relativamente simples. Eran costosos, sólo unos pocos los entendían y se encontraban en centros remotos y controlados.

Protegerlos implicaba controlar el acceso a la sala de informática y limitar la pequeña cantidad de especialistas que necesitaban tener acceso a ella.



A medida que los sistemas informáticos evolucionaron, la conectividad se expandió. Primero lo hizo a través de terminales remotas y finalmente a través de redes de área local (LAN) y de área amplia (WAN).

Cuando el tamaño y el precio de las computadoras se redujeron, comenzaron a aparecer microprocesadores en el lugar de trabajo y el hogar en todo el mundo



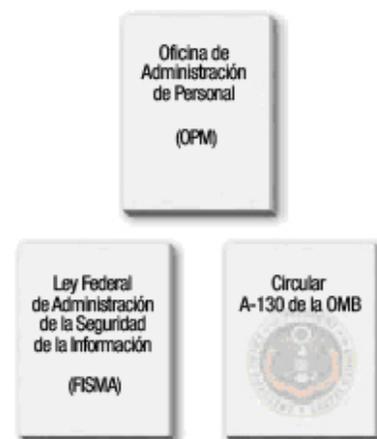
Lo que en un momento era un conjunto de sistemas individuales hoy es una única red conectada a nivel global. En la actualidad, la ISS incluye infraestructuras que no pertenecen al gobierno federal ni están controladas por éste. Debido a esta conectividad global, un riesgo para uno representa un riesgo para todos.

### **Requisitos legales de la ISS**

Es importante que sepa que existe la posibilidad de que se produzcan ataques contra los sistemas federales y que conozca los métodos a los que pueden recurrir estos ataques.

Comprender cuáles son sus responsabilidades para proteger los recursos de información y cómo puede ayudar a prevenir un ataque contribuirá a la seguridad de los sistemas de información federales.

La Ley Federal de Administración de la Seguridad de la Información (*Federal Information Security Management Act*, FISMA) y la Circular A-130 de la Oficina de Administración y Presupuesto (*Office of Management and Budget*, OMB) exigen que todos los usuarios de sistemas informáticos federales reciban capacitación sobre cuestiones relacionadas con la seguridad de los sistemas de información. Además, las normas de la Oficina de Administración de Personal de los Estados Unidos (*Office of Personnel Management*, OPM) también exigen que cada agencia realice una capacitación de concientización sobre la seguridad de la información.

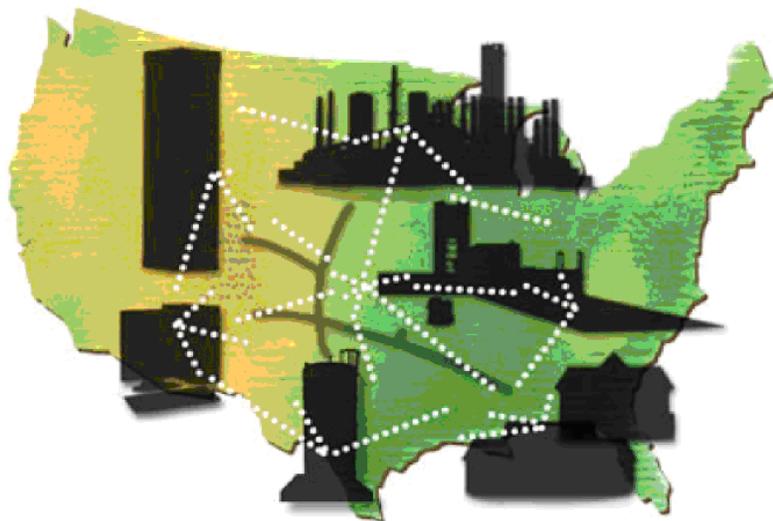


## **Infraestructuras fundamentales**

El programa para la Protección de Infraestructuras Fundamentales (*Critical Infrastructure Protection, CIP*) es un programa nacional que se estableció para proteger las infraestructuras fundamentales de nuestro país. Cuando hablamos de infraestructura fundamental nos referimos a los sistemas físicos y cibernéticos que son esenciales para el funcionamiento básico de la economía y el gobierno.



Los sectores que se consideran parte de la infraestructura fundamental de nuestra nación incluyen, entre otros, la tecnología de la información y las telecomunicaciones, la energía, las operaciones bancarias y finanzas, el transporte y la seguridad fronteriza, el agua y los servicios de emergencia. Muchas de estas infraestructuras han estado desde siempre física y lógicamente separados y han tenido escasa interdependencia. Sin embargo, se han convertido en sistemas cada vez más automatizados e interconectados. Esta mayor conectividad crea nueva vulnerabilidades.



De esta manera, las fallas en los equipos, los errores humanos y el clima, así como también los ataques cibernéticos y físicos que afectan a un sector, podrían tener un posible impacto en toda la infraestructura fundamental de nuestra nación. Por ejemplo, si un virus informático alterase el suministro de gas natural y si se cortara la energía eléctrica, se apagarían los equipos y se interrumpirían las comunicaciones. También se verían afectados las carreteras, el tráfico aéreo

y el transporte ferroviario. Además, se complicaría el trabajo de los servicios de emergencia. Toda una región podría debilitarse porque se atacó un elemento fundamental de nuestra infraestructura.

El programa CIP se estableció para definir e implementar medidas proactivas que protejan nuestra infraestructura fundamental y para actuar ante los ataques que efectivamente ocurran.

## **Concientización sobre la seguridad de los sistemas de información** **Lección 3: Amenazas para la seguridad de los sistemas de información**

### **Amenazas y vulnerabilidades**

Es importante comprender la diferencia que existe entre una amenaza y una vulnerabilidad, y el modo en que éstas pueden afectar a su sistema.



Una amenaza es toda circunstancia o evento que posiblemente dañe un sistema de información, ya sea destruyéndolo, divulgando información almacenada en él, modificando datos negativamente o haciendo que el sistema no esté disponible.

Una vulnerabilidad es una debilidad en un sistema de información o en sus componentes que puede llegar a aprovecharse. Las vulnerabilidades se presentan cuando hay una falla o una debilidad en el hardware o el software de un equipo, de la cual los hackers podrían llegar a sacar provecho. A menudo, las vulnerabilidades son el resultado de una falla en la codificación del software. Para solucionar una vulnerabilidad, los proveedores lanzan una reparación en forma de parche para el software.

## Categorías de amenazas

Existen dos categorías de amenazas: ambientales y humanas.



Existen eventos naturales del medioambiente, como relámpagos, incendios, huracanes, tornados o inundaciones, que representan amenazas para su sistema e información. El propio entorno del sistema, por ejemplo, el cableado de mala calidad en el establecimiento o una ventilación insuficiente para los sistemas, también pueden dañar los sistemas de información.

Las amenazas humanas pueden ser internas o externas. Una amenaza interna puede referirse a un usuario malicioso o descontento, a un usuario que esté al servicio de grupos terroristas o países extranjeros, o a un daño involuntario autoinfligido, por ejemplo, un accidente o un mal hábito.

Una amenaza externa puede estar constituida por hackers, grupos terroristas, países extranjeros o manifestantes.

### Las amenazas humanas internas en comparación con las externas

#### Amenaza interna/ insider



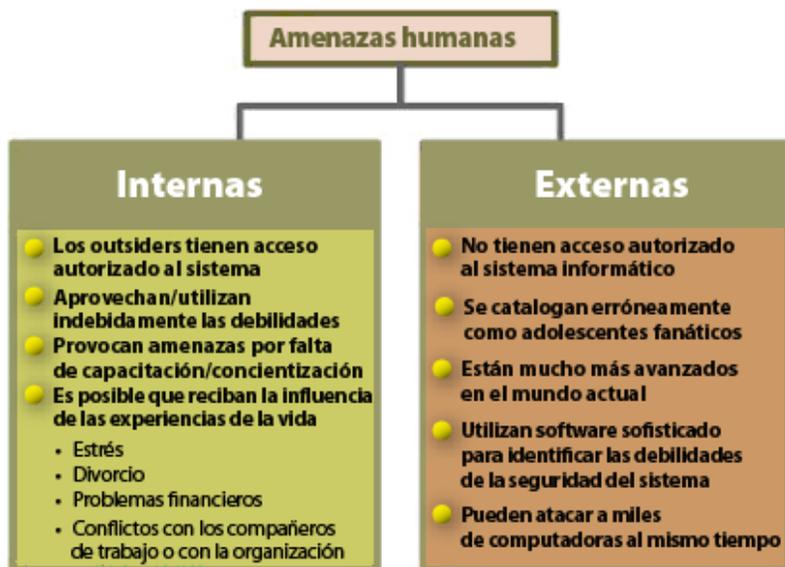
Analicemos más detalladamente las amenazas humanas para los sistemas de información federales. Las mayores amenazas para los sistemas de información federales son internas, es decir, de personas que tienen conocimiento práctico de los recursos informáticos de su organización y acceso a dichos recursos.

Una amenaza interna o *insider* es toda persona que tiene acceso administrativo o físico legítimo al sistema informático. Algunos *insiders* pueden hacer un uso indebido de las debilidades del sistema o aprovecharlas. Otros, por falta de

#### Amenaza externa/ outsider



capacitación y conocimiento, pueden causar daños graves. Aunque existen programas de seguridad para evitar el acceso no autorizado a los sistemas de información y se investigan los antecedentes de los empleados, determinadas experiencias de vida pueden alterar el comportamiento habitual de una persona e impulsarla a actuar de manera ilegal. Algunas situaciones que pueden transformar a un usuario confiable en una amenaza del tipo *insider* son el estrés, el divorcio, los problemas financieros o los conflictos con los compañeros de trabajo o con la organización.



Las amenazas externas o también llamadas *outsiders* son, en su mayoría, los hackers. Un *outsider* es un individuo que no tiene acceso autorizado al sistema informático de una organización. En el pasado, se catalogó a los hackers como adolescentes inadaptados a nivel social, que intentaban atacar a una computadora por vez.

En la actualidad, los hackers pueden incluir representantes de países extranjeros, de grupos terroristas o del crimen organizado. Además, los hackers de hoy tienen muchas más habilidades informáticas y acceso a software de piratería que les permite identificar las debilidades de seguridad de un sistema de manera rápida y sencilla. Mediante el uso de herramientas disponibles en Internet, un hacker puede ejecutar aplicaciones de ataque automáticas contra miles de equipos host a la vez. Por este motivo, representan una amenaza grave para la seguridad de los sistemas de información federales.

### **Información general sobre ingeniería social**



La ingeniería social es una técnica de piratería informática que se basa en la naturaleza humana. Muchos hackers utilizan este enfoque con el fin de obtener información valiosa para acceder a un sistema seguro.

En vez de usar software para identificar las debilidades | de seguridad, los hackers intentan engañar a las personas para que revelen sus contraseñas y demás información que pueda comprometer la seguridad de sus sistemas.

Utilizan tácticas de ingeniería social para conocer contraseñas, identificación de inicio de sesión de usuario, nombres de servidores, sistemas operativos u otra información confidencial.

Por ejemplo, para intentar obtener información del sistema, un hacker puede engañar a un empleado al actuar como si fuera un técnico del servicio o un administrador del sistema ante un problema de acceso urgente.

Nadie debe solicitarle sus contraseñas jamás. Esto incluye a los administradores del sistema y al personal de la mesa de ayuda.

### **Su rol frente a la ingeniería social**

Cómo evitar la ingeniería social:

- Verifique la identidad.
- No revele contraseñas.
- No revele información del empleado.
- No siga instrucciones de fuentes no verificadas.
- No distribuya números de acceso telefónico de ningún sistema informático, excepto los usuarios autorizados.
- No participe en encuestas telefónicas.



Cómo reaccionar frente a la ingeniería social:

- Use un identificador de llamadas para registrar números de teléfono.
- Tome notas detalladas.
- Solicite el nombre/puesto de la persona.
- Informe los incidentes.

**Conocer los comportamientos de la ingeniería social le permitirá reconocerlos, y así evitará divulgar información de seguridad importante a fuentes no autorizadas.**

### **Suplantación de identidad**

La suplantación de identidad es una estafa de la ingeniería social sobre la que usted debe saber. Es una estafa de alta tecnología que utiliza el correo electrónico o los sitios web con el fin de engañar a las personas para que divulguen sus números de tarjeta de crédito, información de cuentas bancarias, número de seguro social, contraseñas u otra información confidencial.

Quienes utilizan la suplantación de identidad envían mensajes de correo electrónico o mensajes emergentes que afirman proceder de una empresa u organización con la que usted trabaja. Por ejemplo, estas personas a menudo se hacen pasar por su proveedor de servicio de Internet, un banco, un servicio de pago en línea e incluso una agencia gubernamental.



El mensaje generalmente indica que debe actualizar o validar su información de cuenta. Además, podría implicar consecuencias graves si usted no responde. Este mensaje lo dirige a un sitio web que parece el sitio de una organización legítima pero que de ninguna manera pertenece a dicha organización.

El propósito de este sitio falso es engañarlo para que divulgue información personal y para que los operadores puedan robar su identidad y emitir facturas o cometer delitos en nombre de usted. Además, ese sitio puede instalar un código malicioso en su sistema.

**Si recibe un mensaje emergente o un mensaje de correo electrónico que le solicita información personal o financiera, no lo responda ni haga clic en el vínculo del mensaje.**

Las empresas legítimas no solicitan este tipo de información por correo electrónico. Si le preocupa su cuenta, comuníquese con la organización que figura en el mensaje de correo electrónico y llame a un número de teléfono que sepa que es real.



Un ejemplo real y reciente de ingeniería social, ocurrió cuando un empleado del gobierno de los Estados Unidos que visitaba otro país entregó su tarjeta de presentación a varias personas.

Unos meses después, un funcionario muy conocido del gobierno de los EE. UU. recibió un mensaje de correo electrónico “de apariencia oficial” que contenía un archivo adjunto que provenía de una dirección “.gov” válida.

Afortunadamente, este funcionario no abrió el archivo adjunto en cuestión, sino que lo reenvió a la persona que él creía que lo había enviado, para verificar.

Finalmente, se comprobó que el correo electrónico que originó el mensaje había interceptado la dirección de correo electrónico del empleado del gobierno que había viajado al país extranjero. El archivo adjunto contenía un código malicioso.

## Cookies

Existen varios riesgos de seguridad asociados con la navegación en Internet. Un riesgo común es lo que se conoce como cookies.

Una cookie es un archivo de texto que un servidor web almacena en su disco duro cuando usted visita un sitio web. Este servidor recupera la cookie cada vez que usted visita nuevamente ese sitio. En cada visita, la cookie lo reconoce y le ahorra el problema de tener que registrarse de nuevo.

El problema de seguridad más serio ocurre cuando las cookies ‘almacenan’ información personal no cifrada, por ejemplo, números de tarjeta de crédito o de seguro social, para facilitar operaciones comerciales futuras con ese sitio.

Otro problema con las cookies es que el sitio posiblemente rastrea sus actividades en la web.

A fin de reducir el riesgo asociado a las cookies y proteger más su sistema, debe configurar su explorador de tal modo que no acepte cookies.



### Código móvil



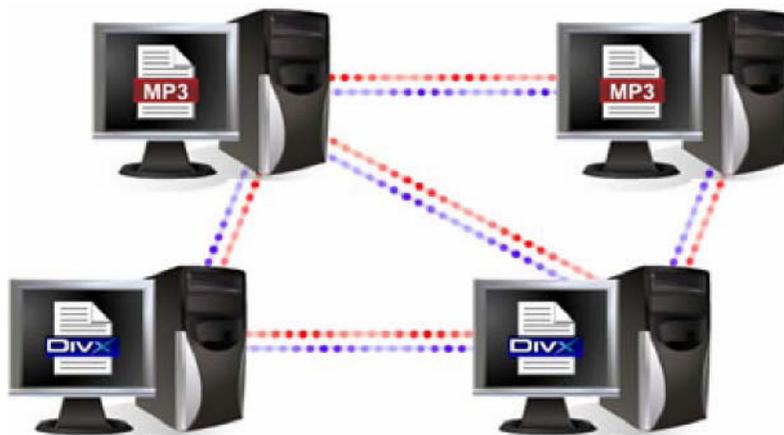
El código móvil, como ActiveX y Java, es un lenguaje de secuencias de comandos que se usa en las aplicaciones de Internet.

El código móvil insertado en una página web puede reconocer los eventos del usuario y responder a ellos. Estos eventos pueden incluir clics del ratón, datos en formularios y navegación en una página. También puede reproducir fragmentos de audio.

Sin embargo, presenta algunos riesgos de seguridad. El código móvil puede ejecutar programas hostiles en su equipo de manera automática sin que usted lo sepa, simplemente porque visitó un sitio web. El programa descargado podría tratar de acceder a la información almacenada en su máquina o dañarla, o bien insertar un virus.

Es posible que su agencia haya desarrollado pautas para el uso del código móvil. Si esto es así, puede restringir la aplicación de este código a los sistemas de información de su agencia. Si tiene alguna pregunta sobre el uso del código móvil, comuníquese con la mesa de ayuda o con el punto de contacto de seguridad.

### Punto a punto (P2P)



La frase “punto a punto” (*peer-to-peer*, P2P) se refiere a las aplicaciones que se utilizan para compartir archivos, como Morpheus y BitTorrent, que permiten que los equipos conectados a Internet se transfieran archivos entre sí.

El software de punto a punto permite acceder y transferir los archivos con facilidad.

Sin embargo, existen cuestiones legales, éticas y de seguridad relacionadas con el uso de aplicaciones de punto a punto no autorizadas.

Los archivos que más comúnmente se transfieren usando este tipo de software no autorizado son archivos de música, pornografía y archivos de video. Obtener estos archivos sin costo alguno no sólo plantea cuestiones éticas, sino que también podría generar una responsabilidad penal o civil por duplicación y transferencia ilegal de material protegido por derechos de autor. Además, participar en la transferencia de este tipo de archivos aumenta su vulnerabilidad. Abrir su equipo por Internet le brinda a extraños un vínculo a su sistema, genera riesgos y crea la posibilidad de una brecha de seguridad.

El punto a punto es una vía común para transferir virus informáticos y spyware.



Además, la instalación y el uso de aplicaciones de punto a punto no autorizadas pueden causar vulnerabilidades importantes para las redes de su agencia, entre las que se incluyen la exposición al acceso no autorizado de información y la pérdida en la integridad de las configuraciones de la red.

La siguiente lista ofrece ejemplos de software P2P dividido por categorías.

Mensajería/telefonía instantánea:

- Yahoo Messenger
- Windows Messenger
- Skype
- MSN Messenger
- AOL Instant Messenger

Transferencia de archivos:

- Bit Torrent
- Gnutelle
- Kazaa
- WinMX
- Napster
- PC Anywhere
- Edonkey
- Morpheus
- EMule
- Limewire
- BearShare
- Timbuktu

La Oficina de Administración y Presupuesto (OMB) exige que todas las agencias desarrollen pautas para el uso de aplicaciones de punto a punto.

Para obtener más información sobre su política específica para el uso de este tipo de aplicaciones, comuníquese con su punto de contacto de seguridad.

## **Incidentes**

### ***¿A qué se considera un incidente de seguridad?***

Un incidente de seguridad es todo evento que va en contra de la ley, los reglamentos o las políticas de seguridad. (Consulte el documento DM3505-000 titulado *USDA Computer Incident Response Procedures* [Procedimientos de respuesta ante incidentes de seguridad en los sistemas informáticos del USDA] en <http://www.ocio.usda.gov/directives/index.html>.)

Entre las instancias de abuso o de uso indebido del equipo se incluyen los siguientes:

- Uso de pornografía, uso de software para transferir archivos de punto a punto (por ejemplo, LimeWire, Gnutella), instalación de software no autorizado y otras acciones que vayan en contra de la política de uso aceptable. Intentos de obtener acceso (físico o electrónico) o información confidencial por teléfono, correo electrónico o en persona, por parte de individuos no autorizados (ingeniería social).
- Intentos de obtener información personal o empresarial que sea confidencial a través de engaños, como mensajes de correo electrónico fraudulentos de apariencia oficial (proceso que se conoce como suplantación de identidad) por parte de personas no autorizadas o no identificadas.
- Intentos de enviar el equivalente electrónico del correo no deseado, a menudo en forma de anuncios comerciales, por parte de personas no autorizadas o no identificadas. Provocar la caída de un programa al saturar un búfer fijo con cantidades excesivas de información, a fin de que una persona o grupo de noticias reciba grandes cantidades de mensajes irrelevantes o inapropiados. (Correo electrónico SPAM)

Otras referencias:

*USDA Cyber Security Standard Operations Procedures for Reporting Security and Personally Identifiable Information Incidents* (Procedimientos estándar de seguridad informática para comunicar incidentes de seguridad y de información personal identificable del USDA) ([http://www.ocionet.usda.gov/ocio/security/docs/SOP-SCD-001\\_USDA\\_CIRT\\_SOP.pdf](http://www.ocionet.usda.gov/ocio/security/docs/SOP-SCD-001_USDA_CIRT_SOP.pdf)).

### ***¿Qué se entiende por información personal identificable (PII)?***

Por lo general, se define a la información personal identificable (*Personally Identifiable Information*, PII) como información sobre un individuo o relacionada con éste. Parte de esta información personal es confidencial mientras que la otra no lo es, si se la considera como un atributo único. Sin embargo, las combinaciones de la información pueden crear una situación en la que la confidencialidad del conjunto de información garantice restricciones de uso y divulgación.

Puede ser difícil definir el nivel de confidencialidad de cada combinación de PII. Por ello, se debe recurrir al sentido común cuando se maneja la PII, a fin de evitar su divulgación. La PII confidencial, como el nombre y el número de seguro social (*social security number*, SSN), debe protegerse en todo momento. Además, se debe proteger cada uno de los siguientes elementos de PII cuando se combina con el nombre o SNN de una persona:

- Lugar de nacimiento
- Fecha de nacimiento
- Nombres de los padres o apellidos de soltero(a)
- Registro biométrico
- Información de la historia clínica
- Antecedentes penales
- Información laboral que incluye calificaciones, acciones disciplinarias, y elementos y estándares de desempeño
- Información financiera
- Números de tarjetas de crédito
- Números de cuentas bancarias
- Historial de autorizaciones de seguridad o información relacionada (sin incluir autorizaciones actuales)

**Nota importante:** Es responsabilidad del individuo cuando ingresa información en cualquier sitio web o SharePoint (un espacio de trabajo cooperativo, una herramienta para la administración y automatización de los procesos comerciales y una plataforma de redes sociales) asegurarse de que no haya PII disponible o de que si lo está, su acceso esté limitado sobre la base del principio “debo saber sólo lo necesario”.

## **Contactos en caso de incidentes**

Todos los incidentes relacionados con la PII deben informarse a la línea directa del Equipo de Respuesta ante Incidentes Informáticos (*Computer Incident Readiness Team*, CIRT) del USDA en el plazo de una hora a partir del momento en que se descubrió o detectó el incidente.

El robo o extravío de equipos debe informarse inmediatamente a la misma línea directa.

Equipos extraviados o robados	(888) 926-2373
Incidentes relacionados con la información personal identificable (PII)	(888) 926-2373 or (877) PII2YOU (744-2968)

## Concientización sobre la seguridad de los sistemas de información

### Lección 4: Código malicioso

#### ¿Qué es un código malicioso?

Código malicioso es un término que hace referencia a software o firmware destinado a realizar un proceso no autorizado que tendrá un impacto negativo en la confidencialidad, integridad o disponibilidad de un sistema de información.



El código malicioso se crea con el objetivo de rechazar, destruir, modificar o dificultar la configuración de archivos de datos, programas o sistemas.

Puede adoptar diferentes formas que incluyen virus, troyanos y gusanos.

Los métodos más comunes para transmitir un código malicioso son los archivos adjuntos en mensajes de correo electrónico y la descarga de archivos de Internet, aunque también se pueden transmitir sólo con visitar sitios web.

#### Correo electrónico y archivos adjuntos

	<b>.exe</b>	Los mensajes de correo electrónico y los archivos adjuntos son una vía común para transmitir un código malicioso.
	<b>.com</b>	Siempre tenga precaución cuando abra un archivo adjunto, ya que es posible que contenga un código malicioso que podría dañar archivos, borrar su disco duro o permitir que un hacker obtenga acceso a su equipo. En particular, debe tener cuidado con los archivos adjuntos con extensión .exe, .com, .vbs, .bat y .shs ya que pueden contener un código malicioso.
	<b>.vbs</b>	
	<b>.bat</b>	No asuma que un archivo adjunto es seguro porque se lo envió un amigo o compañero de trabajo. Guárdelo en su disco duro y analícelo con un software antivirus actualizado antes de abrirlo. Algunos códigos maliciosos se activan con sólo abrir el mensaje.
	<b>.shs</b>	

### **Proteja su sistema informático**

- Analice los archivos adjuntos de los mensajes de correo electrónico y los archivos externos con un software antivirus actualizado.
- Asegúrese de analizar su sistema diariamente.
- Elimine mensajes de correo electrónico de fuentes desconocidas o imprevistas.
- Desactive la opción de descarga automática de archivos adjuntos.

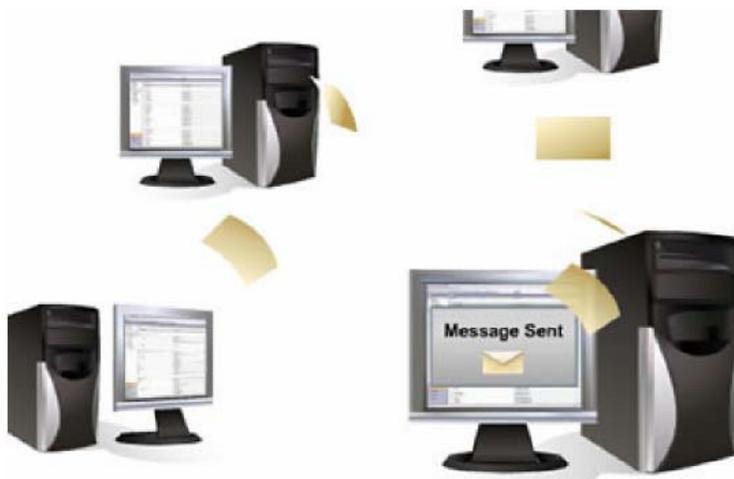
### **Responda ante un ataque de virus**

- No envíe por correo electrónico el archivo infectado.
- Comuníquese con la mesa de ayuda o con el contacto de seguridad.

### **Mensajes engañosos**

Los mensajes engañosos de Internet son mensajes de correo electrónico destinados a impulsarlo a reenviar dichos mensajes a todos sus contactos.

A fin de que usted lo haga, estos mensajes engañosos advierten sobre nuevos virus, promueven sistemas para obtener dinero o citan causas ficticias. Debido a que fomentan la distribución masiva, estos mensajes engañosos obstruyen redes y hacen que el servicio de Internet y de correo electrónico funcione lentamente para los usuarios.



Si recibe un mensaje de correo electrónico en el que se le solicita reenviar a todos sus amigos y compañeros de trabajo, no lo haga.

## **Concientización sobre la seguridad de los sistemas de información**

### **Lección 5: Roles y responsabilidades del usuario**

---

#### **Pautas básicas para el usuario**

Como usuario autorizado de sistemas de información federales, debe cumplir con determinadas responsabilidades cuando utiliza una máquina del gobierno.

Recuerde que sus derechos de privacidad están limitados cuando utiliza recursos informáticos del gobierno.

Toda actividad realizada en un sistema gubernamental puede monitorearse. Cada vez que usted inicia sesión en un sistema del gobierno, da su consentimiento para este monitoreo. Recuerde que debe utilizar su equipo sólo para asuntos gubernamentales.



Evite el uso indebido de estos equipos. Algunos ejemplos de uso indebido son: ver o descargar pornografía, apostar por Internet o jugar juegos de azar, realizar actividades comerciales u operaciones personales con fines de lucro, cargar software personal o realizar cambios no autorizados en la configuración.

Existen ocho pautas éticas básicas generales que deben regir sus acciones cuando utiliza un sistema informático del gobierno.

#### **Pautas éticas**

- No use el equipo para causar daño.
- No interfiera en el trabajo de los demás.
- No se entrometa con los archivos de otra persona.
- No use el equipo para cometer delitos.
- No use ni grabe software sin licencia.
- No robe propiedad intelectual.
- No use el equipo para hacerse pasar por otra persona.
- No use recursos informáticos sin autorización.

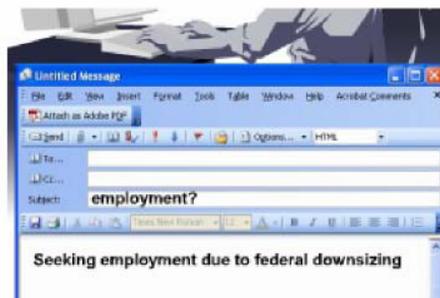
### Uso adecuado del correo electrónico

El correo electrónico también debe utilizarse para asuntos oficiales. Es posible que su organización permita algún uso incidental y casual del correo electrónico.

Las pautas respecto del uso de correo electrónico personal que puede estar autorizado o no son las siguientes:



- El uso del correo electrónico no debe afectar negativamente el desarrollo de las tareas oficiales.
- El uso del correo electrónico no debe representar al gobierno de manera negativa.
- No se puede utilizar el correo electrónico del gobierno para enviar mensajes con contenido pornográfico, racista, sexista u ofensivo de algún otro modo, ni tampoco para enviar cadenas de mensajes o vender.
- El uso del correo electrónico no debe sobrecargar el sistema, tal como ocurre cuando se envían correos electrónicos masivos.
- Para mantener las redes abiertas y en correcto funcionamiento, no se deben reenviar bromas, imágenes ni cuentos inspiradores.
- Del mismo modo, debe evitarse el uso de la opción “Responder a todos”, a menos que sea absolutamente necesario.
- Es posible que se autorice el uso del correo electrónico personal si se utiliza con una duración y frecuencia razonables, y preferentemente durante los períodos de descansos individuales de los empleados, por ejemplo, el horario de almuerzo.



- También está permitido usar el servicio de correo electrónico con fines de interés público legítimo, por ejemplo, cuando permite a los empleados buscar un puesto de trabajo en respuesta a una reducción de personal por parte del gobierno federal.

### **Infraestructura de clave pública**

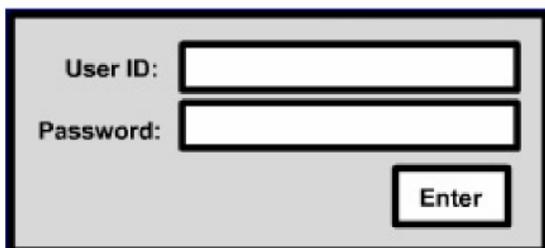
Los sistemas de información federales identifican y autentican a cada usuario, ya sea a través de una tarjeta inteligente de inicio de sesión o de la identificación y contraseña de usuario.

El método preferido para acceder a los sistemas de información es el uso de la infraestructura de clave pública (*Public Key Infrastructure*, PKI) que le permite a su agencia emitir claves electrónicas, llamadas certificados digitales, para los usuarios autorizados.

La PKI les permite a los usuarios cifrar y firmar digitalmente documentos y mensajes de correo electrónico.



### **Consejos para crear una contraseña segura**



The image shows a simple login interface. It consists of a rectangular box with a light gray background. On the left side, there are two labels: 'User ID:' and 'Password:'. To the right of each label is a white rectangular input field. Below the 'Password:' field, there is a small rectangular button with the word 'Enter' written on it.

Numerosos sistemas de información federales todavía identifican y autentican a sus usuarios a través de su identificación de usuario y contraseña. Esta identificación de usuario y contraseña determinan su derecho a acceder al sistema.

Recuerde que es su responsabilidad garantizar que toda actividad que se realice con su identificación de usuario constituya un uso adecuado de los recursos de los sistemas de información federales.

Es importante crear una contraseña compleja a fin de evitar que los sistemas de información gubernamentales corran riesgos.

- Combine letras, números y caracteres especiales.
- Use combinaciones alfanuméricas o asociaciones de frases.
- Evite las palabras o frases que figuran en el diccionario.
- Evite utilizar información personal.
- Memorice su contraseña y no la registre por escrito.
- Cambie su contraseña regularmente.

## **Seguridad física**

La protección de los sistemas de información federales y de la información que contienen comienza con la seguridad física, comúnmente relacionada con armas, puertas y guardias.

La seguridad física incluye la protección de todo el edificio, desde el perímetro externo hasta las oficinas dentro del edificio, incluidos los sistemas de información y la infraestructura.

Es su responsabilidad conocer las políticas de seguridad física de su organización y cumplirlas. Su organización debe contar con procedimientos para ingresar, asegurar su área de trabajo al anochecer y procedimientos en caso de emergencia. Entre ellos se pueden incluir los siguientes:

- Usar una credencial o código para ingresar.
- Cerrar su cabina.
- Desconectar su computadora portátil y guardarla en un lugar separado.
- Bloquear los dispositivos de almacenamiento de datos, como discos duros y unidades de almacenamiento en miniatura, antes de que se retire cuando finaliza la jornada laboral y durante procedimientos de emergencia, por ejemplo, en caso de que se accione una alarma de incendio.



Usted también debe asegurarse de que los demás cumplan con las políticas de seguridad física de la organización y cuestionar a quienes no lo hagan. No permita que individuos que no usan su propia credencial o código ingresen a los edificios o las oficinas al entrar detrás de una persona que sí los usa.

Cuestione a quienes no utilizan credenciales o pases. Si usted es la última persona en salir cuando finaliza la jornada laboral, asegúrese de que los demás hayan asegurado sus equipos adecuadamente.

Por último, usted es responsable de informar toda actividad sospechosa que observe.

## **Control del inventario**

La seguridad física también incluye controlar el inventario de los equipos en los que se almacena la información federal. Cuando se extravían o se roban computadoras portátiles del gobierno, lo mismo ocurre con la información almacenada en ellas. En los últimos años, los procedimientos de control del inventario federal se han intensificado en respuesta a la pérdida de miles de computadoras portátiles pertenecientes al gobierno.



Las agencias federales son responsables de controlar su inventario de equipo informático y de oficina, lo que incluye teléfonos, computadoras, impresoras, máquinas de fax, monitores y unidades de almacenamiento en miniatura.

Cuando recibe propiedad del gobierno, debe firmar un recibo para certificarlo. Una vez que haya firmado, usted es responsable de ese equipo y de tomar las medidas necesarias para asegurarse de que no se extravíe ni lo roben.

Para retirar equipos del edificio o ingresarlos, es posible que su organización requiera un pase de bienes firmado por el administrador de bienes.



Si el bien en cuestión se extravía o lo roban, siga los procedimientos de su organización para informar el hecho. Además de informar la pérdida del equipo, debe informar la pérdida de la información que estaba almacenada en él y la importancia de esa información.

### **Procedimientos de teletrabajo**



El teletrabajo, también conocido como trabajo a distancia, está emergiendo como una opción viable para muchos empleados gubernamentales. Los avances informáticos y de las telecomunicaciones hacen que el teletrabajo sea cada vez más práctico.

Sin embargo, existen riesgos relacionados con el acceso remoto a la red informática del gobierno.

Si usted recibió aprobación para trabajar a distancia, debe cumplir con los requisitos establecidos en las pautas y políticas de su agencia.

### **Información clasificada y no clasificada**

Toda información federal, dadas las circunstancias y condiciones adecuadas, podría proporcionar una visión interna hostil de nuestras capacidades e intenciones. Además, el conjunto de información no clasificada puede elevar el nivel de confidencialidad de la información.

Por ello, hasta la información no clasificada, si es comprometida, podría tener un impacto en la seguridad de nuestro personal y nuestros sistemas.

Toda información federal no clasificada que no se especifica como información de difusión pública requiere cierto grado de protección de seguridad. Como mínimo, se debe revisar antes de su difusión, de cualquier forma, fuera del ámbito del gobierno de los Estados Unidos. Cada agencia tiene su propia política de información no clasificada. Comuníquese con su punto de contacto de seguridad para recibir información adicional sobre las políticas de su agencia.

#### **Información no clasificada:**

- Información sólo para uso oficial (*For Official Use Only*, FOUO), información controlada no clasificada (*Controlled Unclassified Information*, CUI) e información confidencial pero no clasificada (*Sensitive but unclassified*, SBU).
- Por ejemplo: información del personal, financiera, de nómina de pago, médica, operativa y sobre la Ley de Privacidad.
- La CUI debe almacenarse en una gaveta con llave o en un compartimento seguro. Cuando ya no se la necesite, se debe destruir.

#### **Información clasificada:**

- Confidencial, secreta o sumamente secreta.
- El nivel específico de clasificación está determinado por la autoridad de clasificación original.
- Debe utilizarse en una zona que haya sido aprobada y autorizada para el nivel de clasificación correspondiente.
- Cuando no se la utiliza, debe almacenarse en un contenedor o una cámara aprobada de la Administración de Servicios Generales (*General Services Administration*, GSA).

## **Copias de seguridad, almacenamiento y etiquetado**

Una gran cantidad de información federal se almacena en dispositivos móviles tales como CD, unidades de almacenamiento en miniatura, pen drives o discos duros extraíbles. Debido a que estos dispositivos pueden almacenar grandes cantidades de información, usted debe ser sumamente cuidadoso e impedir que se extravíen o los roben.



Es muy importante hacer copias de seguridad de los archivos clave en forma regular y almacenarlos en un lugar seguro. Esto minimizará la pérdida de información si su disco duro falla o se infecta con un virus.

Conserve todos los dispositivos móviles como CD, unidades de almacenamiento en miniatura y discos duros extraíbles en contenedores de almacenamiento duraderos (por ejemplo, gabinetes metálicos) para protegerlos de los daños causados por el fuego y el agua.

Es muy importante etiquetar todos los dispositivos móviles, lo que incluye las copias de seguridad y su contenido, a fin de reflejar la clasificación o el grado de confidencialidad de la información que contiene cada dispositivo.

Estos dispositivos deben estar claramente etiquetados y almacenados de acuerdo con la clasificación de seguridad correspondiente de la información que contienen.

Cuando ya no necesite la información del dispositivo móvil, no la borre ni la “desinfecte”. Los dispositivos móviles deben desmagnetizarse o destruirse si no se los volverá a utilizar en el mismo nivel de clasificación del sistema en que se usaron o en uno superior.



Siga las políticas de su agencia respecto del manejo, el almacenamiento, el etiquetado y la destrucción de los dispositivos móviles.

## **Dispositivos multimedia**

Sea extremadamente cuidadoso cuando utilice máquinas de fax, teléfonos celulares, computadoras portátiles, asistentes personales digitales (*personal digital assistants*, PDA) y redes inalámbricas. Debe ser tan cuidadoso respecto de la seguridad en estos dispositivos como lo es con su equipo en el trabajo.



### **Máquinas de fax**

Si envía información confidencial a través de una máquina de fax, asegúrese de que el destinatario esté presente para recoger el fax de inmediato. Comuníquese directamente con el destinatario para confirmar su recepción. Nunca envíe información confidencial a través de una máquina de fax que no sea segura.

Use siempre una hoja de portada para que el contenido del fax no sea visible inmediatamente.



### **Teléfonos celulares**

Si usa un teléfono celular, cualquier persona que cuente con el equipo adecuado posiblemente pueda escuchar su conversación. Los teléfonos celulares son sólo transmisores.

Use una línea fija para mayor privacidad y nunca comente información confidencial en un teléfono que no sea seguro.



### **PDA**

Los asistentes personales digitales (PDA), como Blackberry o Palm Pilot, representan una amenaza para la seguridad por varios motivos.

Su pequeño tamaño y bajo costo los hacen fáciles de obtener pero difíciles de controlar.

Tienen una gran capacidad de conectividad y de almacenamiento y son sumamente populares. Puede ser muy fácil para una persona conectar un PDA para descargar información desde su equipo.

Todos los PDA que se utilizan para conectarse con los sistemas gubernamentales deben cumplir con las políticas de su agencia y con las pautas de la OMB.



### **Computadoras portátiles**

La practicidad de las computadoras portátiles y de otros dispositivos informáticos extraíbles también los hace sumamente vulnerables frente al robo o las infracciones de la seguridad.

La información de inicio de sesión de usuario siempre debe estar protegida con contraseñas.

Tenga cuidado con la información que se muestra en su pantalla cuando está visible para otros, especialmente en espacios reducidos, por ejemplo, un avión.

Mantenga su computadora portátil consigo en todo momento cuando viaje para evitar que se la roben. Cuando llegue a su destino de viaje temporal, asegúrese de que su computadora esté adecuadamente asegurada cuando no la esté controlando.

Si su computadora portátil tiene capacidad de conexión inalámbrica, asegúrese de que las características de seguridad inalámbrica estén correctamente configuradas, de acuerdo con las políticas de seguridad inalámbrica de su agencia. Cuando no la use, la conectividad inalámbrica de su computadora portátil debe estar en modo “off”, es decir, apagada. Si esto no es posible, debe estar configurada para conectarse en puntos de acceso a Internet reconocidos y no en redes ad hoc.

La Oficina de Administración y Presupuesto (OMB) emitió un documento en el que indica que toda información confidencial almacenada en computadoras portátiles y en otros dispositivos informáticos extraíbles debe estar cifrada. Asegúrese de cumplir con las pautas de su agencia y las de la OMB respecto del cifrado de información confidencial en computadoras portátiles.



### **Red inalámbrica**

Las redes inalámbricas transmiten y reciben información usando señales de radio en vez de usar los tradicionales cables del equipo.

Los usuarios no autorizados pueden interceptar sus comunicaciones con un receptor y acceder a su red.

Esto es peligroso porque estas personas no autorizadas pueden capturar no sólo la información que usted está transmitiendo, sino también todos los datos que estén almacenados en su red.

Asegúrese de cumplir con las políticas de su agencia respecto del uso de las tecnologías inalámbricas.

### **Spillage**

Cuando información que pertenece a un nivel de clasificación superior se introduce en una red de un nivel de clasificación inferior ocurre un *spillage*, también llamado contaminación. Es el almacenamiento, la transmisión o el procesamiento inadecuados de información clasificada en un sistema no clasificado.

Un ejemplo puede ser cuando la información clasificada como “secreta” se introduce en una red no clasificada. Cualquier usuario que identifique un *spillage* o sospeche que ha ocurrido debe informarlo inmediatamente a su punto de contacto de seguridad.

Hacer una limpieza después de producirse un *spillage* es un proceso que utiliza recursos intensivos. Puede llevar aproximadamente tres semanas contener y limpiar un sistema de información que se vio afectado. Recuerde que un *spillage* puede afectar significativamente la seguridad de la información federal.



### **Consejos útiles:**

- Revise todos los mensajes de correo electrónico en busca de posible información clasificada.
- Identifique y almacene adecuadamente todos los dispositivos móviles.
- Asegúrese de que todos los nombres de los archivos y asuntos identifiquen el grado de confidencialidad de la información.

### **Información personal**



La Ley de Privacidad (*Privacy Act*), promulgada en 1975, exige que el gobierno proteja la información sobre los individuos que se procesa en los sistemas informáticos de las agencias federales o de contratistas. Esta misma ley dispone que el gobierno debe permitir que los individuos accedan a dicha información y la modifiquen, en caso de que no sea precisa, oportuna, completa o relevante.

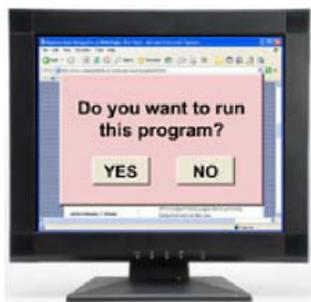
En varios documentos de la OMB figuran pautas nuevas más importantes referidas a las medidas de protección de la información personal identificable (PII).

Por ejemplo, la OMB establece que la PII extraviada o robada se debe informar en el plazo de una hora de ocurrido el hecho al Equipo de Respuesta ante Emergencias Informáticas de los (*Computer Emergency Response Team, CERT*) de los Estados Unidos.

Cada agencia tiene sus propias políticas para implementar las pautas de la OMB. Comuníquese con su punto de contacto de seguridad para conocer los requisitos adicionales de PII.

Como usuario autorizado, usted debe garantizar que la información personal identificable esté protegida en los sistemas informáticos federales.

## Su responsabilidad



La información es un recurso sumamente importante para el gobierno de los Estados Unidos. Es su responsabilidad proteger la información gubernamental confidencial y clasificada que se le haya confiado.

Comuníquese con su punto de contacto de seguridad para obtener más información sobre la clasificación o el manejo de la información.

## Concientización sobre la seguridad de los sistemas de información **Lección 6: Seguridad del equipo personal y del hogar**

### Robo de identidad

Según las estadísticas del FBI, el robo de identidad sigue siendo el delito que crece más rápidamente en el país.

El robo de identidad ocurre cuando otra persona utiliza el nombre, dirección, número de seguro social, número de cuenta bancaria o de tarjeta de crédito, u otra información personal que lo identifique a usted sin su conocimiento y con el fin de cometer fraude u otros delitos.



Los ladrones de identidad pueden utilizar la información que obtuvieron para abrir cuentas de tarjetas de crédito, solicitar préstamos o vaciar una cuenta bancaria sin que usted lo sepa.



El robo de identidad es un grave problema que tiene consecuencias extremas para sus víctimas. Usted es la primera línea de defensa contra este delito. Es importante que haga lo que esté a su alcance para minimizar su riesgo.

### **Proteja su identidad:**

- Pregunte cómo se usará la información antes de proporcionarla.
- Preste atención a su resumen de tarjeta de crédito y estado de cuenta bancaria.
- Evite usar nombres o fechas comunes, como contraseñas y números de identificación personal (*Personal Identification Number*, PIN).
- Retire su correspondencia a la brevedad.

- Destruya los documentos personales.
- Cancele las tarjetas de crédito que no utilice.
- Evite llevar consigo la tarjeta del SSN y el pasaporte.
- Solicite anualmente un informe de crédito.

#### **Cómo actuar frente al robo de identidad:**

- Comuníquese con las agencias de información de crédito: Equifax, TransUnion y Experian.
- Comuníquese con las instituciones financieras o crediticias para cerrar cuentas:
  - Tarjetas de crédito
  - Cuentas bancarias
- Controle los resúmenes de tarjeta de crédito en busca de compras no autorizadas.
- Informe el delito a la policía local.

### **Spyware**

Spyware es un término general que se utiliza para hacer referencia a las aplicaciones de software que muestran anuncios no deseados, recopilan información personal o cambian la configuración del equipo, sin su consentimiento.

Su equipo puede estar infectado con spyware si recibe anuncios emergentes aun cuando no esté conectado a Internet, la página principal de su explorador de Internet ha cambiado o aparece una nueva barra de herramientas en su explorador que usted no deseaba.

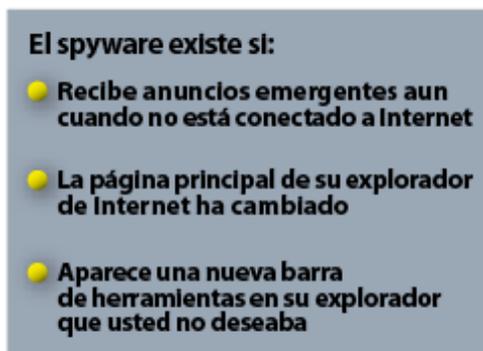
Existen varias maneras en que el spyware u otro software no deseado tengan acceso a su sistema. Un truco común es instalar el software de manera encubierta durante la instalación de otro software que usted deseaba instalar. Cada vez que instale algo en su equipo, asegúrese de leer detenidamente todos los avisos, incluido el acuerdo sobre licencia y la declaración de privacidad.

Para detectar y eliminar programas de spyware de su equipo, utilice un programa actualizado de detección y eliminación de spyware que analice su equipo en busca de este tipo de software y lo elimine.

#### **Usted está ante la presencia de Spyware si ocurre lo siguiente:**

- Recibe anuncios emergentes aun cuando no está conectado a Internet.
- La página principal de su navegador de Internet ha cambiado.
- Aparece una nueva barra de herramientas en su explorador que usted no deseaba.

**Utilice un programa de detección y eliminación de spyware** si su agencia lo autoriza.



## **E-Commerce**



El comercio electrónico o e-commerce se refiere a las transacciones comerciales que se efectúan utilizando documentos electrónicos en vez de papel.

El e-commerce ofrece mayor flexibilidad para los consumidores y las empresas respecto de cuándo y cómo se realizan las transacciones.

Por ejemplo, el hecho de que su empleador deposite directamente su salario en una cuenta bancaria elimina la necesidad de usar los tradicionales cheques de papel.

El E-commerce es una forma común en que los individuos pueden resultar víctimas del robo de identidad. Realizar transacciones comerciales en línea aumenta la vulnerabilidad del usuario frente al robo de identidad debido a que se transmite información personal a través de Internet.



A fin de reducir el riesgo de robo de identidad, verifique que el sitio de e-commerce que está utilizando efectúe sus transacciones a través de un enlace cifrado antes de ingresar información personal.

El acrónimo “https” incluido en la URL indica que el vínculo está cifrado. Tenga en cuenta que no todos los sitios https son legítimos y sigue expuesto al riesgo cuando ingresa su información en línea.

## **Principios básicos de seguridad**

### **Consejos de seguridad:**

- Analice su sistema regularmente con software actualizado:
  - Antivirus.
  - Detección y eliminación de Spyware.
- Analice todos los archivos adjuntos de los mensajes de correo electrónico y los archivos que descargue de Internet.
- Elimine los archivos infectados.
- Descargue regularmente actualizaciones de software y parches.
- Instale y utilice un firewall cuando esté conectado a Internet.
- Haga copias de seguridad de todos los archivos importantes.
- Use contraseñas complejas.



- Desconecte su equipo de Internet cuando no esté en línea.
- Proteja su red inalámbrica con una contraseña.
- Conozca los riesgos de los programas de P2P.

### **Denegación de servicio distribuido (DDoS)**

Los ataques de denegación de servicio distribuido (*Distributed denial of service*, DDoS) son una amenaza para la seguridad de Internet.

Por medio de estos ataques se bombardea un servidor web con grandes cantidades de datos provenientes de numerosos equipos y ubicaciones diferentes, con el fin de provocar una caída del servidor y denegar su disponibilidad.

Los ataques pueden lanzarse desde sistemas dispersos en Internet pero con el mismo objetivo, o bien, desde sistemas vulnerables controlados por servidores que pueden camuflar el verdadero origen del ataque.

Usted puede ayudar a disminuir los ataques de DDoS si implementa hábitos informáticos seguros a fin de evitar que el equipo de su hogar se utilice para lanzar estos ataques.



### **Tecnología**



Las necesidades de seguridad deben mantenerse constantemente a la par de las tecnologías y aplicaciones en constante cambio. El ritmo acelerado de los avances tecnológicos genera nuevos desafíos para la seguridad de los sistemas de información.

Es importante que usted se mantenga informado sobre estos cambios para poder así protegerse mejor usted mismo, proteger el equipo de su hogar y los sistemas de información federales.

**AQUÍ FINALIZA EL MATERIAL DE CAPACITACIÓN.  
AHORA DEBE HACER Y APROBAR LA EVALUACIÓN.  
COMUNÍQUESE CON SU SUPERVISOR.**

## GLOSARIO

---

### **Amenaza**

Hace referencia a toda circunstancia o evento que posiblemente dañe un sistema de información, ya sea destruyéndolo, divulgando información almacenada en él, modificando datos negativamente o haciendo que el sistema no esté disponible.

### **Circular A-130, Apéndice III, de la Oficina de Administración y Presupuesto (OMB)**

Exige que todos los sistemas de información federales hagan lo siguiente:

- Posean planes de seguridad de la información.
- Traten el tema de la seguridad informática en informes que se presentarán ante el Congreso por medio de la OMB.
- Ofrezcan capacitación de concientización sobre la seguridad de la información para los usuarios, operadores y administradores del sistema.
- Lleven a cabo planes de contingencia mejorados.
- Mantengan las capacidades formales de respuesta ante emergencias.
- Asignen la responsabilidad operacional de seguridad a una única persona.

### **Código malicioso**

Hace referencia al software o firmware destinado a realizar un proceso no autorizado que tendrá un impacto negativo en la confidencialidad, integridad o disponibilidad de un sistema de información.

### **Comercio electrónico (e-commerce)**

Hace referencia a las transacciones comerciales que se realizan utilizando documentos electrónicos en vez de papel.

### **Confidencialidad**

Es la garantía de que la información no se divulga a individuos, procesos o dispositivos no autorizados.

### **Cookie**

Es un archivo de texto que un servidor web almacena en su disco duro cuando usted visita un sitio web.

### **Denegación de servicio distribuido (DDoS)**

Son ataques que representan una amenaza para la seguridad de Internet. Por medio de estos ataques se bombardea un servidor web con grandes cantidades de datos provenientes de numerosos equipos y ubicaciones diferentes, con el fin de provocar una caída del servidor y denegar su disponibilidad.

### **Disponibilidad**

Es el acceso confiable y oportuno a la información y los servicios de información para usuarios autorizados.

### **Información personal identificable (PII)**

Se refiere a toda la información que una agencia tiene sobre una persona que incluye, entre otros, información sobre educación, transacciones financieras, historias clínicas, antecedentes penales o laborales y aquella que pueda utilizarse para identificar o rastrear la identidad de una persona, por ejemplo, el nombre, el número de seguro social, la fecha y el lugar de nacimiento, el apellido de soltera de la madre, los registros biométricos y cualquier otra información que pueda asociarse a un individuo.

### **Integridad**

Hace referencia a la cualidad de un sistema de información que refleja la exactitud lógica y la confiabilidad del sistema operativo, la integridad lógica del hardware y software para implementar mecanismos de protección, y la coherencia de las estructuras de información y de los casos de información almacenada. Tenga en cuenta que, en modo de seguridad formal, la integridad se interpreta más estrictamente como protección contra la modificación o la destrucción no autorizada de la información.

### **Ley Federal de Administración de la Seguridad de la Información (FISMA)**

- Establece que debe haber un programa de seguridad informática en todas las agencias federales.
- Contiene disposiciones para el desarrollo y mantenimiento de los controles mínimos necesarios para proteger los sistemas de información federales.
- Ofrece un marco global para garantizar la eficacia de los controles de seguridad de la información.
- Requiere que las agencias identifiquen los niveles de riesgo e implementen la protección adecuada.
- Requiere que cada agencia desarrolle y mantenga un inventario de los sistemas de información más importantes.
- Requiere que los empleados y contratistas gubernamentales que utilizan estos sistemas realicen periódicamente una capacitación sobre seguridad informática.
- Requiere que las agencias informen al Congreso respecto del cumplimiento de la FISMA.
- Define los sistemas de seguridad nacional.

### **Mensajes engañosos de Internet**

Mensajes de correo electrónico destinados a impulsar a los usuarios a reenviar dichos mensajes a todos sus contactos.

### **Protección de Infraestructuras Fundamentales (CIP)**

Es un programa nacional que se estableció para proteger la infraestructura fundamental de nuestro país. Cuando hablamos de infraestructura fundamental nos referimos a los sistemas físicos y cibernéticos que son esenciales para el funcionamiento básico de la economía y el gobierno.

### **Punto a punto (P2P)**

Hace referencia a las aplicaciones que se utilizan para compartir archivos, como Morpheus y BitTorrent, que permiten que los equipos conectados a Internet se transfieran archivos entre sí.

### **Seguridad de los sistemas de información (ISS)**

Es la protección de los sistemas de información contra el acceso a información o su modificación no autorizados, ya sea que esté en almacenamiento, procesamiento o tránsito, y contra la denegación del servicio a usuarios autorizados, lo que incluye medidas para detectar, documentar y contraatacar tales amenazas.

### **Spillage**

Ocurre cuando la información de un nivel de clasificación superior se introduce en una red de un nivel de clasificación inferior. Es el almacenamiento, la transmisión o el procesamiento inadecuados de información clasificada en un sistema no clasificado.

### **Spyware**

Software malicioso que muestra anuncios no deseados, recopila información personal o cambia la configuración de un equipo, sin el consentimiento del usuario.

### **Suplantación de identidad**

Hace referencia a una estafa de alta tecnología que utiliza el correo electrónico o los sitios web con el fin de engañar a las personas para que divulguen sus números de tarjeta de crédito, información de cuentas bancarias, número de seguro social, contraseñas u otra información confidencial.

### **Vulnerabilidad**

Hace referencia a una debilidad en un sistema de información o en sus componentes que puede llegar a aprovecharse. Las vulnerabilidades se presentan cuando hay una falla o una debilidad en el hardware o el software de un equipo, de la cual los hackers podrían llegar a sacar provecho. A menudo, las vulnerabilidades son el resultado de una falla en la codificación del software. Para solucionar una vulnerabilidad, los proveedores lanzan una reparación en forma de parche para el software.

**AQUÍ FINALIZA EL MATERIAL DE CAPACITACIÓN.  
AHORA DEBE HACER Y APROBAR LA EVALUACIÓN.**