



Año Fiscal 2017: Conciencia en la Seguridad Informática

1 de octubre de 2016

CONTENIDO

Visión del Curso	6
Destino 1: Importancia en la Seguridad de los Sistemas de Información (ISS)	6
Historia de ISS	7
ISS y los Requisitos de las Reglas de Comportamiento	7
Revisión de Conocimiento #1	7
Reglas de Comportamiento- Comportamiento Aceptable y Penalidades	8
Infraestructura Crítica	8
Infraestructura Crítica- Amenazas	9
Revisión de Conocimiento #2	9
Destino 2: Amenazas a la Seguridad de los Sistemas de la Información	10
Categorías de Amenazas	10
Amenazas Ambientales	10
Amenazas Humanas Internas vs Externas	11
Amenazas Externas.....	12
Destino 3: Amenaza de la Ingeniería Social	13
Resumen de Ingeniería Social.....	13
Su Rol con la Ingeniería Social.....	13
Reglas de Comportamiento- Ingeniería Social	14
Reglas de Comportamiento- Acceso.....	14
Revisión de Conocimiento #3.....	15
Reportar un Incidente.....	15
Fraude Electrónico (Phishing)	16
Destino 4: Internet y Amenazas a la Red.....	18
Cookies	18
Código Móvil.....	18
Revisión de Conocimiento #4.....	19
Peer-to-Peer (P2P)	19
Vulnerabilidades P2P.....	19
Reglas de Comportamiento - Compartir Archivos P2P.....	20

Uso General de un Software	21
Reglas de Comportamiento- Software General	21
Revisión de Conocimiento #5	21
Código Malicioso/Malware	22
Correos Electrónicos y Archivos Adjuntos.....	22
Revisión de Conocimiento #6	22
Revisión de Conocimiento #7	23
Hoaxes (Broma o Fraude).....	23
Revisión de Conocimiento #8.....	24
Destino 5: Dispositivos de Medios y Seguridad Móvil	25
Dispositivos de Medios.....	25
Dispositivos Celulares (no inteligentes) & Asistentes Personales Digitales (PDAs).....	25
Seguridad Básica de los Dispositivos Móviles	26
Los Teléfonos Inteligentes y Tabletas son Computadoras, NO Teléfonos Celulares.....	26
No Jailbreak (Destrahe o Desbloquee) su Dispositivo Móvil	26
Tenga Precaución Al Descargar las Aplicaciones	27
Mantenga Físicamente Seguro su Dispositivo Móvil.....	27
Inmediatamente Reporte el Dispositivo Móvil Perdido o Robado.....	27
Regularmente realice una Copia de Respaldo (Backup) en su Dispositivo Móvil.....	27
¡Aprenda Más!.....	28
Computadoras Portátiles & Máquinas de Fax	28
Redes Inalámbricas	28
Destino 6: Seguridad Física e Información Clasificada.....	30
Seguridad Física.....	30
Seguridad Física- Enfoque Proactivo.....	31
Control de Inventario	31
Procedimientos de Teletrabajo.....	31
Información Clasificada y No Clasificada.....	32
Dispersión de Información (Spillage).....	32
Información Personal de Identificación (PII)	33

Revisión de Conocimiento #9.....	33
Revisión de Conocimiento #10.....	34
Destino 7: Roles y Responsabilidades del Usuario.....	35
Guías Básicas para Usuarios.....	35
Guía de Privilegios de los Usuarios.....	36
Reglas de Comportamiento- Responsabilidad/ Rendición de Cuentas.....	37
Reglas de Comportamiento- Integridad.....	38
Revisión de Conocimiento # 11.....	38
Reglas de Comportamiento: Uso Apropiado de Correo Electrónico.....	38
Infraestructura Pública Clave.....	39
Consejos para Crear una Contraseña Segura.....	40
Copias de Respaldo, Almacenaje y Rotulación.....	40
Reglas de Comportamiento- Copias de Respaldo, Almacenaje y Rotulación.....	41
Revisión de Conocimiento #12.....	41
Revisión de Conocimiento #13.....	42
Destino: Recta Final.....	43
Su Responsabilidad.....	43
Reconocimiento de las Reglas de Comportamiento de USDA y Próximos Pasos.....	43
Apéndice- Respuestas de la Evaluación.....	45

AÑO FISCAL (AF) 2017: ADIESTRAMIENTO SOBRE CONCIENCIA EN LA SEGURIDAD INFORMÁTICA Y REGLAS DE COMPORTAMIENTO

¡Bienvenidos a “Destino ISA” Adiestramiento sobre Conciencia en la Seguridad Informática y Reglas de Comportamiento AF 2017!

El adiestramiento sobre *Conciencia en la Seguridad Informática (ISA por sus siglas en inglés)* y *Reglas de Comportamiento* es obligatorio para todos los empleados, contratistas, socios y voluntarios del Departamento de Agricultura de los Estados Unidos (o USDA por sus siglas en inglés). Para los nuevos empleados, socios y voluntarios es requerido completar el adiestramiento antes de que estos obtengan acceso al sistema. Todos los usuarios deben estar al tanto de las políticas, requisitos y problemas de seguridad. También deben hacer un esfuerzo consciente para evitar brechas de seguridad permaneciendo alerta a las vulnerabilidades de la red.

Al tomar este curso anualmente, usted está cumpliendo con un requisito legal para todos los usuarios de los sistemas de información federales. Este adiestramiento está diseñado para ayudarle a entender la importancia de la Seguridad en los Sistemas de Información (o ISS por sus siglas en inglés), sus principios guías y lo que esto significa para su agencia. También este curso incluye las “Reglas de Comportamiento” que gobiernan el uso de la información tecnológica (IT) de los recursos de USDA.

Este adiestramiento identificará los riesgos potenciales y las vulnerabilidades asociadas a los sistemas de información federal, le ayudará a revisar su rol protegiendo estos sistemas y proveerá las directrices a seguir en el trabajo para la protección en contra los ataques a los sistemas informativos.

VISIÓN DEL CURSO

La Conciencia en la Seguridad Informática (ISA por sus siglas en inglés) es un proceso continuo- es como un viaje en el que todos navegamos e interactuamos con una variedad de tecnologías en el transcurso de realizar nuestro trabajo. Para reflejar este “viaje”, este curso ha sido diseñado en lo que llamamos siete (7) Direcciones o Destinos de la Conciencia en la Seguridad Informática.

Su rol al tomar este curso es navegar por cada uno de estos Destinos y aprobar exitosamente la evaluación relacionada a los mismos.

Este curso consiste en siete (7) direcciones o destinos.

- Destino 1: Importancia en la Seguridad de Sistemas Informativos
- Destino 2: Amenazas a la Seguridad de Sistemas Informativos
- Destino 3: Amenazas de la Ingeniería Social
- Destino 4: Amenazas del Internet
- Destino 5: Seguridad en los Dispositivos de Medios y Móviles
- Destino 6: Seguridad Física e Información Clasificada
- Destino 7: Roles y Responsabilidades del Usuario

DESTINO 1: IMPORTANCIA EN LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN (ISS)

El internet ha permitido que el obtener y transferir la información sea rápido y extremadamente fácil. Mientras que la conectividad global es muy conveniente, también incrementa la vulnerabilidad a los ataques externos. Los objetivos de la Seguridad de los Sistemas De Información ISS (por sus siglas en inglés) y las Reglas de Comportamiento son el proteger nuestra información y sistemas de información.

ISS y las Reglas de Comportamiento protegen a la información de la modificación y del acceso no autorizado y aseguran que los sistemas de información estén disponibles para otros usuarios. Esto significa que un sistema seguro mantiene su confidencialidad, integridad y disponibilidad.

Objetivo de Aprendizaje

Luego de completar esta lección, usted podrá:

- Identificar qué es la seguridad en los sistemas de información y por qué esto es importante.

Esta lección incluye los siguientes tópicos:

- Historia de ISS
- ISS y los Requerimientos Legales de las Reglas de Comportamiento
- Reglas de Comportamiento- Comportamiento Aceptable y Penalidades
- Infraestructura Crítica

HISTORIA DE ISS

Cincuenta años atrás, los sistemas de computadoras presentaban retos de seguridad relativamente simples. Eran costosos, entendidos sólo por unos pocos y se encontraban aislados en facilidades controladas.

La protección de estos sistemas de computadoras consistía en controlar el acceso al salón de computadoras y en la autorización de un pequeño grupo de especialistas que necesitaban permiso para entrar en el área.

Como los sistemas de computadoras evolucionaron, la conectividad se expandió, primero por los terminales remotos y eventualmente por áreas locales y amplias en las redes (o LANs o WANs respectivamente por sus siglas en inglés).

Por otro lado, mientras el tamaño y el precio de las computadoras disminuían, los microprocesadores comenzaron aparecer en el área de trabajo y en hogares alrededor del mundo.

Lo que una vez fue una colección de sistemas separados, ahora es mejor entendido como un sólo sistema global conectado a la red. ISS ahora incluye infraestructuras que no son propiedades o controladas por el gobierno federal. Debido a esto, la conectividad global es un riesgo para uno y es un riesgo para todos.

ISS Y LOS REQUISITOS DE LAS REGLAS DE COMPORTAMIENTO

Es muy importante que esté alerta ante la posibilidad de ataques a los sistemas federales y a los métodos en el cuales los mismos puedan ocurrir.

Entendiendo sus responsabilidades en la protección de los recursos informativos y cómo usted puede contribuir a prevenir de los ataques y ayudará a la seguridad de los sistemas informativos federales.

Es requerido por ley que USDA asegure que cualquiera que utilice los recursos de IT de la agencia, esté consciente de sus responsabilidades y que cumpla con las Reglas de Comportamiento establecidas.

¿Qué usted necesita saber?

El Acta del Manejo de Seguridad de la Información Federal (o FISMA por sus siglas en inglés) (parte del Acta E-Gobierno 2002, Ley Pública 107-347 con fecha del 17 de diciembre de 2002) y la Oficina de Manejo y Presupuesto (OMB por sus siglas en inglés) Circular A-130 requieren que todos los usuarios de las computadoras en sistemas federales estén adiestrados en el cuidado y el cumplimiento de lo establecido en las Reglas de Comportamiento. Las regulaciones de la Oficina del Manejo de Personal de los Estados Unidos (OPM por sus siglas en inglés) requieren que cada agencia tenga adiestramientos que creen conciencia sobre la seguridad de las computadoras.

REVISIÓN DE CONOCIMIENTO #1

Llene el espacio en blanco.

Todos los siguientes son aspectos importantes para la Seguridad de los Sistemas Informativos excepto_____.

1. Protección de la información en las redes de las computadoras del gobierno.
2. Bloqueo al acceso no autorizado en las redes de las computadoras del gobierno.
3. Prevención de la modificación digital no autorizada en las redes de las computadoras del gobierno.
4. Restricciones específicas escritas para el uso de las redes en las computadoras del gobierno.

La respuesta correcta puede ser encontrada en el Apéndice.

REGLAS DE COMPORTAMIENTO- COMPORTAMIENTO ACEPTABLE Y PENALIDADES

Las Reglas de Comportamiento establecen los comportamientos esperados y aceptados en computación. Debido a que estas guías escritas no pueden cubrir cada incidente, es requerido que los usuarios utilicen su juicio y altos estándares de ética en el momento de tomar una decisión.

USDA tomará acciones correctivas y/o reforzará el uso de penalidades en contra de cualquier usuario que viole cualquier política del sistema de seguridad de USDA o Federal utilizando cualquiera o todas las siguientes:

- Acciones correctivas (tomadas de acuerdo a las reglas de regulaciones y leyes existentes) incluyen: reprimendas escritas, suspensión temporera de los deberes, reasignación o descenso de categoría y terminación del empleo Federal.
- Suspensión del sistema de privilegios.
- Posible acusación criminal

¿Qué usted debe saber?

Las siguientes son actividades no oficiales que están prohibidas en cualquier computadora que sea propiedad o rentada por el gobierno:

- Apostar.
- Intencionalmente visitar o descargar material de páginas web pornográficas.
- Hacer presión (lobby) en el Congreso o cualquier agencia gubernamental.
- Hacer campaña- actividad política.
- Cualquier tipo de transferencia de audio o video de organizaciones comerciales, privadas, noticias o financieras, excepto aquellas que estén expresamente autorizadas por la administración.
- Actividades que están conectadas con cualquier tipo de empleo exterior.
- Endoso de cualquier productos, servicios y organizaciones no gubernamentales.

INFRAESTRUCTURA CRÍTICA

La Protección Crítica a la Infraestructura (o CIP por sus siglas en inglés) es un programa nacional establecido para proteger a la infraestructura crítica de nuestra nación. La Infraestructura Crítica se refiere a los sistemas físicos y cibernéticos esenciales para las operaciones mínimas de la economía y el gobierno.

Los sectores que son considerados parte de la infraestructura crítica de nuestra nación incluyen, pero no están limitados a: información tecnológica y telecomunicaciones, energía, banca y finanzas, transportación y seguridad fronteriza, agua y servicios de emergencia. Muchas de las infraestructuras críticas de la nación han sido históricamente física y lógicamente sistemas separados que tenían poco interdependencia. Sin embargo, estas infraestructuras se han convertido cada vez más automatizadas e interconectadas. El aumento en la conectividad crea nuevas vulnerabilidades.

INFRAESTRUCTURA CRÍTICA- AMENAZAS

Fallas en el equipo, un error humano, el clima, al igual que los ataques físicos y cibernéticos impactan a un sector, también pueden potencialmente impactar la infraestructura crítica de nuestra nación. Por ejemplo: si el suministro de gas natural es interrumpido por un virus en las computadoras y la luz eléctrica se ha ido, las computadoras y las comunicaciones estarían fuera de servicio. Las calles, el tráfico aéreo y la transportación en los trenes también se podrían ver impactados. Los servicios de emergencias pudieran estar obstaculizados. Una región completa puede ser debilitada porque un elemento crítico de nuestra infraestructura ha sido atacado.

CIP fue establecido para definir e implementar medidas proactivas para la protección de nuestra infraestructura y responder ante cualquier ataque que ocurra.

REVISIÓN DE CONOCIMIENTO #2

Seleccione la respuesta correcta.

¿Cuál de los siguientes sistemas no debería ser incluido en el programa de Protección de Infraestructura Crítica nacional?

1. Seguro Social
2. Planta Eléctrica
3. Escuela Elemental
4. La Reserva Federal

La respuesta correcta puede ser encontrada en el Apéndice.

DESTINO 2: AMENAZAS A LA SEGURIDAD DE LOS SISTEMAS DE LA INFORMACIÓN

Es muy importante entender las diferencias entre las vulnerabilidades y las amenazas y cómo estas pueden afectar un sistema.

Una amenaza es cualquier circunstancia o evento que potencialmente puede afectar a un sistema de información, ya sea destruyéndolo, divulgando la información almacenada en el sistema, modificando la data adversamente o haciendo que el sistema no esté disponible.

Una vulnerabilidad es una debilidad en los sistemas de información o en sus componentes y que la misma pueda ser aprovechada. Las vulnerabilidades existen cuando hay una falla o debilidad en un software o hardware y puede ser aprovechada por los hackers (piratas cibernéticos). También estas son frecuentemente el resultado de una falla en la codificación del software. Para corregir una vulnerabilidad, el proveedor emitiría una solución en forma de un parcho para el software.

Objetivo de Aprendizaje

Luego de completar esta lección, usted podrá:

- Diferenciar entre una amenaza y vulnerabilidad e identificar los riesgos asociados a cada una de ellas.

Esta lección incluye los siguientes tópicos:

- Categorías de Amenazas
- Amenazas Ambientales
- Amenazas Humanas Internas vs Externas

CATEGORÍAS DE AMENAZAS

Hay dos tipos de categorías de amenazas: las ambientales y las humanas.

AMENAZAS AMBIENTALES

Los eventos naturales ambientales, incluyendo los rayos, incendios, huracanes, tornados o inundaciones, representan amenazas a los sistemas de información. El ambiente de un sistema, incluyendo el pobre alambrado del edificio o la insuficiencia en la refrigeración de los sistemas, también puede causar daño a los sistemas de información.

¿Cómo puede protegerse contra de las amenazas ambientales?

Reglas de Comportamiento- Hardware/ Amenazas Ambientales

Los usuarios deberán hacer lo mejor posible para proteger a su equipo de computadora de daños, abuso, robo y uso sin autorización. Los usuarios deberán proteger sus equipos de amenazas tales como:

- Temperaturas Extremas;

- Tormentas Eléctricas;
- Agua y Fuego;
- Electricidad estática;
- Derrames de Comida y Bebida;
- Objetos Caídos;
- Ambientes con Exceso de Polvo, y
- Materiales Combustible

AMENAZAS HUMANAS INTERNAS VS EXTERNAS

Las amenazas humanas pueden ser internas o externas. Una amenaza interna puede ser un usuario malicioso o disgustado, un usuario al empleo de grupos terroristas o países extranjeros o un daño auto-infligido no intencional, tal como un accidente o un mal hábito.

Una amenaza externa puede ser: hackers, grupos terroristas, países extranjeros o manifestantes.

Si miramos de cerca a las amenazas humanas al sistema de información federal. Las grandes amenazas a este sistema son internas, de personas que tienen el conocimiento y el acceso a los recursos computadorizados de su organización.

Una amenaza interna o una persona dentro una organización, es cualquiera con acceso legítimamente físico o administrativo a una computadora y puede hacer un mal uso o aprovecharse de la debilidad del sistema. Otros, debido a la falta de entrenamiento o conocimiento pueden hacer daño. Aunque hay programas de seguridad para prevenir el acceso no autorizado a los sistemas de información y empleados que son sujetos a una investigación de trasfondo, ciertas experiencias en la vida pueden alterar el comportamiento normal de las personas y esto ocasiona que ellos actúen ilegalmente. El estrés, divorcio, problemas financieros o frustraciones con los compañeros de trabajos o alguna organización son algunos ejemplos que pueden transformar a un usuario de confianza en una amenaza interna.

¿Cómo puede protegerse en contra las amenazas internas humanas?

Reglas de Comportamiento- Amenazas Internas

Los usuarios deberán:

- Mantener un inventario de todos los equipos que le han sido asignados.
- Utilizar solamente equipos para los cuales se les ha concedido autorización.
- No dejar su computadora en un vehículo estacionado o en una localización que no sea segura y su equipo pueda ser robado.
- Seguir los procedimientos establecidos cuando se remueva equipo de las facilidades de USDA. Esto usualmente requiere un pase de la propiedad.

- No instalar o utilizar un software o hardware no autorizado en la red, incluyendo computadoras portátiles, computadoras de bolsillo, asistentes personales digitales y teléfonos celulares habilitados en la red; excepto los que han sido expresamente autorizados.
- No alterar la configuración, incluyendo la instalación de software y periféricos en equipos del gobierno a menos de que esté autorizado.
- Notificar a la administración antes de relocalizar los recursos informáticos.
- Cuando sea posible, utilice dispositivos de bloqueo físico para computadoras portátiles y tenga cuidado adicional para otros equipos portátiles.

AMENAZAS EXTERNAS

Las amenazas externas o intrusos son principalmente los hackers. Un intruso es un individuo que no tiene acceso autorizado a un sistema informático de una organización.

¿Qué usted debe saber?

Hoy día los hackers pueden incluir representantes de países extranjeros, grupos terroristas u organizaciones criminales. Los hackers están muy avanzados en las destrezas de computadoras y tienen acceso a piratear (hacking) el software que provee la capacidad de rápida y fácilmente identificar una debilidad en el sistema de seguridad. Utilizando herramientas disponibles en el internet, un hacker es capaz de poner a funcionar aplicaciones automatizadas en contra de miles de computadoras al mismo tiempo. Debido a esto, los piratas cibernéticos o hackers representan un riesgo muy serio para la seguridad del sistema de información federal.

DESTINO 3: AMENAZA DE LA INGENIERÍA SOCIAL

La ingeniería social es una técnica de piratería (hacking) que se basa en la naturaleza humana. Este acercamiento puede ser utilizado por muchos hackers para obtener información valiosa y tener acceso un sistema seguro.

Objetivos de Aprendizaje

Luego de completar esta lección, usted debe:

- Entender la definición de Ingeniería Social
- Reconocer ejemplos de Ingeniería Social
- Entender sus responsabilidades para reportar incidentes de Ingeniería Social
- Verificar seis (6) formas en las que usted puede prevenir las amenazas de la Ingeniería Social

Esta lección incluye los siguientes temas:

- Ingeniería Social
- Reglas de Comportamiento- Acceso
- Reporte de Incidente
- Fraude Electrónico (Phishing)

RESUMEN DE INGENIERÍA SOCIAL

Cuando Kate contestó una llamada, el hombre en la línea sonaba muy autoritario. Él le dijo que está investigando posible incidente de seguridad en la página USDA Web TA (Tiempo y Asistencia) y necesita que ella verifique su contraseña.

En vez de utilizar un software que identifica las debilidades en el sistema, los hackers intentan burlar a los individuos a que revelen las contraseñas y otro tipo de información que pueda comprometer la seguridad del sistema.

Ellos utilizan la naturaleza innata de las personas en aprender las contraseñas, la identificación (ID) de inicio de sección, los nombres de los servidores, sistemas operativos y otros de información sensible o confidencial.

Por ejemplo: Un hacker puede intentar ganar acceso al sistema de información haciéndose pasar por un técnico de servicios o un administrador del sistema con una situación de acceso urgente a un problema.

Nadie debe preguntarle su contraseña. Esto incluye a los administradores del sistema o el personal de ayuda al cliente (help desk).

SU ROL CON LA INGENIERÍA SOCIAL

El entender la ingeniería social le permitirá reconocerla y evitará que usted provea a fuentes no autorizadas información de seguridad importante.

Previniendo la Ingeniería Social:

- Verifique la identidad.
- No dé a conocer su contraseña.
- No dé a conocer su información de empleado.
- No siga comandos de fuentes que no han sido verificadas.
- No distribuya su número telefónico en ningún sistema de computadoras; excepto a usuarios válidos.
- No participe de encuestas telefónicas.

Reaccionando a la Ingeniería Social:

- Utilice llamada identificada para documentar el número de teléfono.
- Tome notas detalladas.
- Pregunte el nombre y la posición de la persona.
- Reporte incidentes.

REGLAS DE COMPORTAMIENTO- INGENIERÍA SOCIAL

Los usuarios serán responsables y rendirán cuentas por cualquier acción tomada bajo su identificación de usuario.

¿Qué usted debe saber?

Usted debe:

- Proteger su contraseña del acceso de otros individuos.
- Nunca dar su contraseña a personas, incluyendo a su supervisor o alguna persona que este proveyendo servicio al cliente.
- No preguntar a nadie por sus contraseñas.
- Crear contraseñas efectivas siguiendo la política de contraseñas complejas de USDA

REGLAS DE COMPORTAMIENTO- ACCESO

Los usuarios deberán tener acceso y sólo utilizarán la información para la cual tienen autorización oficial.

¿Qué usted debe saber?

Usted debe:

- Seguir los procedimientos establecidos para tener acceso a la información, incluyendo el uso de la identificación y autenticación del usuario, contraseñas y otras precauciones físicas y lógicas.
- Seguir los canales establecidos para solicitar y diseminar la información.
- Tener acceso sólo a los archivos, directorios y aplicaciones para las cuales la autorización del acceso ha sido concedidas por el administrador del sistema.
- Utilizar el equipo del gobierno sólo para los propósitos aprobados.

En adición los usuarios NO deben:

- Dar información a otros empleados o individuos externos que no tienen autoridad de acceso.
- Guardar información sensible o confidencial en un sistema, a menos de que los controles de acceso estén protegidos (Ejemplos: contraseñas, salones cerrados y LAN) al utilizarse.
- Usar la posición de confianza y derechos de acceso para tomar ventaja de los sistemas de control o tener acceso a la data por alguna otra razón que no se sea la de ejecutar las tareas oficiales.
- Explorar otros archivos de usuarios (por ejemplo: ¿a qué pueden tener acceso?).

REVISIÓN DE CONOCIMIENTO #3

Selecciona la respuesta correcta.

Kate recibe una llamada telefónica de un hombre que dice está investigando un posible incidente de seguridad en el USDA Web TA o sistema de información de tiempo y asistencia y necesita que ella confirme su contraseña. ¿Qué puede hacer Kate para prevenir o desalentar esta llamada y no ser víctima de un hacker que está utilizando ingeniería social?

1. Verificar la identidad de la persona que llame y obtener su nombre y posición.
2. No dar a conocer su contraseña.
3. Tomar notas detalladas y reportar la llamada a su supervisor.
4. Todas las anteriores. Todas las repuestas son métodos para prevenir el ataque a las computadoras de parte de hackers que usan ingeniería social

La respuesta correcta puede ser encontrada en el Apéndice.

REPORTAR UN INCIDENTE

Cada usuario es responsable de reportar cualquier forma de violación a la seguridad, ya sea una pérdida, fraude o abuso a través del mecanismo de reportar incidentes de USDA.

¿Qué usted debe saber?

Usted debe:

- Reportar los incidentes de seguridad o cualquier incidente sospechoso de fraude, pérdida o mal uso de los recursos de USDA o la divulgación de información de identificación personal (PII por sus siglas en inglés) llamando al USDA Help Desk (1-888-926-2373) o PII Hotline (1-877-PII-2-YOU), o llamando al Administrador designado de IT Información de Seguridad de la agencia.
- Reportar las vulnerabilidades y violaciones a la seguridad tan pronto como sea posible llamando al USDA PII Hotline (1-877-PII-2-YOU), o llamando al Administrador designado de IT Información de Seguridad de la agencia para que acciones correctivas sean tomadas.
- Tomar acciones razonables inmediatamente después de haber descubierto una violación para prevenir daños adicionales tales como: desconectarse de un terminal o cerrar la propiedad.
- Cooperar libremente con los planes oficiales de acción para lidiar con las violaciones de seguridad.

FRAUDE ELECTRÓNICO (PHISHING)

Linda recibe un email de su banco indicándole que la cuenta de su tarjeta de débito puede estar en riesgo y que ella necesita verificar su número cuenta y PIN. ¿A caso alguien está tratando de hacer un fraude electrónico (phishing) con la información privada de Linda?

El “phishing” es un caso de ingeniería social del cual usted tiene que estar alerta. El fraude electrónico es una estafa de alta tecnología que utiliza correos electrónicos con apariencia oficial para confundir al destinatario y que estos abran los archivos “oficiales” adjuntos o haciendo clic en los enlaces falsos. Cuando estas páginas de la web son abiertas, puede entrar un software malicioso y se instala en la computadora personal o en la de los individuos que están motivados a difundir la información personal susceptible como los números de tarjetas de crédito, números de identificación personal (o PINs por sus siglas en inglés) o cualquier contraseña.

Los estafadores (phishers) envían un email o un mensaje emergente (pop-up) de un negocio u organización con la que el usuario tiene transacciones. Por ejemplo: un estafador se presenta frecuentemente al usuario con servicio de pago en línea por internet o aún más, de una agencia de gobierno. El mensaje usualmente dice que el usuario tiene que actualizar o validar la información en su cuenta y también lo puede amenazar con algunas consecuencias si el usuario no responde. El mensaje dirige al usuario a un sitio web que se parece al sitio legítimo pero no está afiliado a la organización de ninguna manera. El propósito del sitio web falso es confundir al usuario y que este divulgue información personal, así los operadores pueden robar la identidad, crear facturas y cometer delitos a nombre del usuario. También este sitio falso puede instalar códigos maliciosos en el sistema del usuario.

Si usted recibe un correo electrónico o un mensaje emergente (pop-up) que pregunte por información personal o financiera, NO responda o haga clic al link en el mensaje.

Las compañías legítimas no le piden este tipo de información vía correo electrónico. Si usted está preocupado sobre su cuenta, contacte a la organización identificada en el correo electrónico llamando a un número de teléfono que usted sepa es el genuino. Tenga mucha precaución si recibe un correo electrónico acerca de alguna transacción financiera que tenga enlaces para obtener más información o discutir algún cargo, aunque sea de los proveedores que usted recibe correspondencia. Siempre filtre estos enlaces para asegurarse de que estos vayan a un dominio válido asociado con este negocio. No haga clic si piensa que es un enlace sospechoso. Pregunte por una forma de verificación de este negocio, ya sea por un correo electrónico legítimo o a través de su portal web.

Ejemplos de estos dominios:

Válido <https://www.amazon.com/gp/pdp/profile/...>

Sospechoso <http://www.amazon.com.suspicious.me/wp-...>

Sospechoso <http://suspicious.me/www.amazon.com/e4f6d23...>

Recientemente, los destinatarios de los correos electrónicos del gobierno de los Estados Unidos han recibido mensajes de individuos externos en el mismo campo de negocios. Estos mensajes fueron enviados a través de los servicios de entrega de archivos conocidos como Dropbox.com, Box.com o Yousendit.com. Estos archivos estuvieron disponibles para ser descargados y contenían códigos maliciosos con extensiones tales como: .scr, .exe y .doc. Si se hubiesen abierto los archivos con estos softwares de acceso remoto, los mismos habrían sido instalados, permitiéndole a las organizaciones externas tener acceso a los archivos y sistemas de gobierno de Estados Unidos.

La precaución principal por parte de los compañeros de trabajo es la de someter estos incidentes a las operaciones de Seguridad en la Información en su agencia antes de tener acceso o hacer clic en los enlaces. Si usted necesita instrucciones sobre cómo someter un suceso como este, verifique con su servicio al cliente de IT.

DESTINO 4: INTERNET Y AMENAZAS A LA RED

Cualquier red facilita la comunicación entre individuos. Una red puede todo desde una colección pequeña de aparatos en una localización dada para el internet global. En cualquier caso, una red es frecuentemente el blanco de un intento malicioso. Por su tamaño increíble, el internet es una fuente de innumerables amenazas en contra de la Agencia.

Objetivo de Aprendizaje

Después de completar esta lección, usted debe ser capaz de:

- Entender las ocho (8) amenazas de ISA asociadas con el internet y las redes.
- Identificar tres (3) o más amenazas Peer-to-Peer.
- Identificar sus responsabilidades y las “Reglas de Comportamiento” relacionadas al internet y a la red basada en las amenazas.

Esta lección incluye los siguientes temas:

- Cookies
- Código Móvil
- Peer-To-Peer (P2P)
- Reglas De Comportamiento - Compartir Archivos P2P
- Software Generales
- Códigos Maliciosos
- Correos Electrónicos y Documentos Adjuntos
- Hoaxes (broma o fraude)

COOKIES

Hay diferentes riesgos asociados con la navegación en el internet. Unos de estos es conocidos como cookies.

Un cookie es un archivo de texto que ha sido almacenado por el servidor de la web en el disco duro de su computadora cuando usted visita un sitio web. El servidor recupera el cookie cada vez que usted vuelve a visitar el sitio web. El cookie reconoce que es usted y le ahorra el dilema de tener que volver registrarse.

La parte más seria del problema de seguridad con los cookies ha ocurrido cuando los mismos han sido “guardados” con información personal sin cifrar o no codificada (unencrypted), tales como: las tarjetas de crédito o números de seguro social, con el fin de facilitar futuros negocios con ese portal. Otro problema con los cookies, es que los mismos pueden potencialmente rastrear sus actividades en la web.

Para reducir los riesgos asociados con los cookies y proteger mejor a su sistema, su navegador debe ser programado para no aceptar los mismos.

CÓDIGO MÓVIL

Mike quiere ver un sitio web gracioso del que su amigo le habló, pero primero tiene que descargar y hacer funcionar una aplicación para tener acceso y ver el mismo. Si Mike ejecuta la aplicación, él puede ser vulnerable a un Código Móvil malicioso.

Los códigos móviles como el ActiveX y Java son lenguajes de secuencias de comando utilizados por las aplicaciones en el internet.

Un código móvil introducido en una página web puede reconocer y responder a eventos de usuario, como los clics del ratón, formulario de entrada y la página de navegación. También puede reproducir clips de audio.

Sin embargo, esto implica algunos riesgos de seguridad. Los códigos maliciosos pueden hacer funcionar programas hostiles automáticamente en su computadora sin su conocimiento, simplemente porque usted visitó un sitio en la red. El programa descargado puede tratar de tener acceso o dañar la data en su computadora e insertar un virus.

Revise las políticas de su agencia para objetivos específicos o restricciones en el uso de código móvil.

REVISIÓN DE CONOCIMIENTO #4

Llene el espacio en blanco.

Linda recibió un correo electrónico de su banco donde le pedían verificar los números de su cuenta y PIN para prevenir un robo de identidad. Esto podría ser una forma de un riesgo en la seguridad de la información conocido como_____.

1. Hoax (Broma o Fraude)
2. Phishing
3. Correo de Ingeniería
4. Robar cookies

La respuesta correcta puede ser encontrada en el Apéndice.

PEER-TO-PEER (P2P)

Peer-to-peer o P2P se refiere a las aplicaciones para compartir archivos tales como: Morpheus y BitTorrent. Los cuales permiten que las computadoras se conecten al internet para la transferencia de archivos entre sí.

VULNERABILIDADES P2P

Peer-to-peer es un software que permite tener acceso a los archivos y que sean transferidos con facilidad.

La música, la pornografía y las películas son los archivos de mayores transferencias sin autorización por los softwares peer-to-peer. Al obtener estos archivos sin costo, esto presenta no sólo una preocupación

ética, más bien puede ser el resultado de un cargo criminal o civil por la duplicación ilegal y divulgación de material con derechos reservados. En adición, participar y compartir archivos peer to peer aumenta la vulnerabilidad. Al conectarse al internet en su computadora, le provee a los intrusos un enlace a su sistema, crea riesgos y les permite a estos la posibilidad de encontrar una brecha en la seguridad.

La siguiente lista incluye ejemplos de algunos casos del software P2P dividido por categorías:

Mensajes Instantáneos/ Telefonía:

- Yahoo! Messenger
- Windows Live Messenger
- Skype
- AOL Instant Messenger

Compartir Archivos:

- BitTorrent
- Gnutella
- Kazaa
- WinMX
- Napster
- PC Anywhere
- eDonkey
- Morpheus
- eMule
- LimeWire
- BearShare
- Timbuktu

REGLAS DE COMPORTAMIENTO - COMPARTIR ARCHIVOS P2P

Las conexiones peer-to-peer son avenidas comunes para la dispersión de virus y programas espías (spyware).

La instalación y uso de aplicaciones peer-to-peer sin autorización puede representar vulnerabilidades significativas para las redes en su agencia, incluyendo la exposición al acceso no autorizado de la información y comprometer la configuración de la red.

La Oficina de Manejo y Presupuesto (OMB por sus siglas en inglés) requiere que todas las agencias desarrollen una guía para uso de las aplicaciones peer-to-peer.

Para más información relacionada a la política específica del uso de aplicaciones peer-to-peer, comuníquese con el punto de contacto de seguridad.

¿Qué usted necesita saber?

Está prohibido que los usuarios usen peer-to-peer (P2P) para compartir archivos. Esto representa una amenaza a la seguridad de la información tecnológica (IT). También permite a los empleados transferir archivos entre computadoras sin los controles apropiados de seguridad. Estos programas pueden ser utilizados para la distribución de materiales inapropiados, violación de la ley de derechos reservados y poner la información del gobierno en riesgo. Los usuarios deben de estar familiarizados con la política para compartir archivos USDA P2P localizada en los directivos del sitio intranet de USDA.

USO GENERAL DE UN SOFTWARE

Los usuarios no deben instalar softwares no autorizados, estándares, de dominio público o programa compartido (shareware) en sus computadoras sin la aprobación del oficial de manejo adecuado. Los usuarios de computadoras deben proteger los softwares y el equipo de USDA adquiridos de los software maliciosos.

REGLAS DE COMPORTAMIENTO- SOFTWARE GENERAL

Usted no debe:

- Utilizar software comprado por el USDA en su computadora personal o en computadoras que no sean de USDA a menos de que sea autorizado.
- Alterar la configuración, incluyendo la instalación del software y periféricos en la computadora del gobierno, a menos de que esté autorizado.
- Descargar, instalar, o ejecutar programas de seguridad o utilidades que puedan revelar las debilidades en las medidas de seguridad o acceso privilegiado a cualquier sistema a menos de que sea expresamente autorizado.

En adición los usuarios deben:

- Cumplir con todas las licencias y acuerdos de los softwares y las leyes de derechos reservados federales.

REVISIÓN DE CONOCIMIENTO #5

Llene el espacio en blanco.

Mike quiere ver un enlace de un sitio web gracioso del cual le habló su amigo, pero él necesita instalar y ejecutar primero una aplicación de ActiveX. ActiveX es una forma de Código Móvil. Todas las siguientes son formas de Código Móvil excepto _____.

1. Ver audio clips.

2. Insertar un virus en la computadora.
3. Permitir la comunicación en un teléfono celular cifrado o codificado (encrypted).
4. Controlar la navegación en un sitio web.

La respuesta correcta puede ser encontrada en el Apéndice.

CÓDIGO MALICIOSO/MALWARE

Malware es un nombre corto para “código malicioso” y se refiere a los programas de software designados a dañar o a cualquier otra acción no deseada en un Sistema de computadora. Los ejemplos más comunes incluyen virus, gusanos, caballos de Troya y los programas espías (spyware).

Los códigos maliciosos son definidos como un software o firmware que tienen la intención de llevar a cabo procesos sin autorización que puedan impactar adversamente la confidencialidad, integridad y disponibilidad de los sistemas de información.

Está diseñado para denegar, modificar o impedir la configuración de los sistemas, programas o archivos de datos.

Los métodos más comunes de dispersar los códigos maliciosos son a través de archivos en correos electrónicos y por la descarga de archivos en el internet, pero también se pueden recibir códigos maliciosos con la visita a un sitio web infectado.

CORREOS ELECTRÓNICOS Y ARCHIVOS ADJUNTOS

Los mensajes en los correos electrónicos y los archivos adjuntos proveen una ruta en común para transferir los códigos maliciosos.

Siempre sea precavido al abrir un email con archivos adjuntos. Estos pueden contener un código malicioso que puede corromper archivos, borrar la data del disco duro o permitir que un hacker gane acceso a su computadora.

Los archivos con estas u otras extensiones pasan a cuarentena. Los archivos con los que debe de tener precaución incluyen: .html, .lnk, .pdf, .url, .doc(x), .xls(x), o .rtf y cualquier extensión de archivo que el remitente le pide que cambie a una extensión diferente (por ejemplo: .xxx to .exe).

No asuma que es un archivo adjunto es seguro porque lo envió un amigo o un compañero de trabajo. Algunos de estos códigos maliciosos se activan solamente cuando usted abre el mensaje. Guarde el archivo en su disco duro y proceda a escanearlo antes de abrirlo con un software de anti virus que este actualizado.

Nunca haga clic en un enlace o mensaje de correo electrónico sospechoso aunque aparente ser de alguien con quien usted este familiarizado.

REVISIÓN DE CONOCIMIENTO #6

Seleccione la respuesta correcta.

¿Cuál de los siguientes es un tipo de Malware?

1. Adware (programa de publicidad)
2. Spyware (programa espía)
3. Rootkit (juego de herramientas o programas)
4. Caballo de Troya (Trojan horse)
5. Keyloggers (registrador de teclas)
6. Todas las anteriores

La respuesta correcta puede ser encontrada en el Apéndice.

¿Qué usted debe saber?

Proteja a su Sistema de Computadora

- Escanear los archivos adjuntos de sus correos electrónicos y archivos externos utilizando un software anti-virus que este actualizado.
- Asegurar que el sistema sea escaneado diariamente.
- Borrar cualquier correo electrónico de fuentes inesperadas o desconocidas.
- Apagar el software con la opción de descargar automáticamente los archivos adjuntos.

Responda a un Ataque de un Virus

- No envíe por correo electrónico una copia del archivo infectado.
- Contacte al servicio de ayuda (help desk) o contacto de seguridad.

REVISIÓN DE CONOCIMIENTO #7

Seleccione la respuesta correcta.

¿Cuál de los siguientes es una señal(es) de un malware en su computadora?

1. Lentitud
2. Reducción del espacio en el disco duro
3. Errores
4. Mensajes pop-ups
5. Todas las anteriores

La respuesta correcta puede ser encontrada en el Apéndice.

HOAXES (BROMA O FRAUDE)

Phyllis recibe un correo electrónico de una amiga que incluye un aviso serio sobre un virus de computadoras. Su amiga les dice a todos los que ella conoce. Si Phyllis reenvía el correo electrónico a su grupo oficial de contactos, ¿estará ella ayudando a promover un “hoax en el internet”?

Los hoaxes (broma o fraude) en el internet son mensajes de correo electrónicos con el fin de influenciar al recipiente a que envíe los mismos a cada uno de sus contactos.

Los hoaxes invitan que usted reenvíe el correo electrónico advirtiéndole sobre un nuevo virus, promoviendo los esquemas para hacer dinero o citando una causa ficticia. Promoviendo una distribución masiva, los hoaxes bloquean las redes y reducen la velocidad del sistema de internet y el servicio de correos electrónicos en la computadora del usuario.

Si usted recibe un correo electrónico con un mensaje que le pide que envíe hacia adelante el mismo a sus amigos y compañeros de trabajo, no lo haga.

REVISIÓN DE CONOCIMIENTO #8

Seleccione la respuesta correcta.

Phyllis recibe un correo electrónico del proveedor de su teléfono celular indicando que la cantidad que ella debe es diferente a la que debería ser. ¿Qué pasos no debería Phyllis seguir antes de abrir enlace en el correo electrónico?

1. Es apropiado que haga clic a cualquier enlace, ya que el correo electrónico proviene de su compañía de teléfonos.
2. Verificar si hay alguna referencia a su número de cuenta o número de teléfono móvil.
3. Filtrar todos los enlaces en el mensaje para asegurarse que todos vayan a un dominio válido.
4. Llamar al servicio al cliente de su proveedor o entrar en su sitio web escribiendo su dominio para verificar el mensaje de correo electrónico.

La respuesta correcta puede ser encontrada en el Apéndice.

DESTINO 5: DISPOSITIVOS DE MEDIOS Y SEGURIDAD MÓVIL

Las amenazas a la seguridad de la información provienen de diferentes recursos. Este destino discute las amenazas de los dispositivos tales como: la unidad de almacenaje de USB (thumb drive), teléfonos celulares y redes inalámbricas.

En adición a las amenazas discutidas, este destino provee consejos sobre cómo mantener su dispositivo móvil este seguro y que usted debe de hacer si pierde su teléfono.

Objetivos de Aprendizaje

Luego de completar esta lección, usted debe ser capaz de:

- Entender las amenazas de ISA de áreas tales como: los dispositivos de medios (ejemplo- unidad de almacenaje de USB), dispositivos móviles y redes inalámbricas.
- Conocer qué hacer si usted pierde su celular en respecto con ISA.
- Entender las reglas de comportamiento para el acceso de la red inalámbrico.

Esta lección incluyen los siguientes temas:

- Dispositivos de Medios
- Celular (no inteligente) y Asistentes Personales Digitales (PDA por sus siglas en ingles)
- Seguridad en los Dispositivos Móviles
- Computadoras Portátiles y Maquinas de Fax
- Redes Inalámbricas
- Información de Identificación

DISPOSITIVOS DE MEDIOS

Sea extremadamente cuidadoso cuando use teléfonos celulares, teléfonos inteligentes, computadoras portátiles, tabletas, máquinas de fax y redes inalámbricas. Usted necesita estar vigilante sobre la seguridad de estos aparatos de igual manera que si ustedes estuvieran en su computadora de trabajo.

DISPOSITIVOS CELULARES (NO INTELIGENTES) & ASISTENTES PERSONALES DIGITALES (PDAs)

Si usted utiliza su teléfono celular, cualquier persona que tenga el equipo apropiado puede potencialmente escuchar su conversación. Los teléfonos celulares son sólo transmisores.

Utilice un teléfono fijo para más privacidad y nunca discuta información sensitiva en un teléfono que no sea seguro.

Los PDAs tienen seguridad adicional para las amenazas de seguridad por varias razones.

Su tamaño es pequeño y relativamente tienen un bajo costo, lo que los hace fáciles de obtener y dificulta su control.

Todos los PDAs conectados al sistema de gobierno tienen que estar en cumplimiento con las políticas de su agencia y con las directrices de OMB.

SEGURIDAD BÁSICA DE LOS DISPOSITIVOS MÓVILES

Las mismas características que hacen populares a los teléfonos inteligentes y las tabletas, también los convierte en un blanco ideal para los ladrones. Siga las seguridades básicas detalladas abajo para la protección para sus dispositivos móviles y la información contenida en los mismos.

LOS TELÉFONOS INTELIGENTES Y TABLETAS SON COMPUTADORAS, NO TELÉFONOS CELULARES

Hoy día los dispositivos móviles tienen las mismas funciones que las computadoras tradicionales; también pueden enfrentar las mismas amenazas. Para mantener la seguridad de su dispositivo móvil, usted debe de seguir las siguientes prácticas de seguridad para las computadoras.

Por ejemplo:

- Para prevenir el acceso no autorizado de su teléfono o tableta, programe un número de identificación personal (PIN).
- No abra mensajes de correos electrónicos no solicitados.
- No siga los enlaces de correos electrónicos no solicitados o archivos adjuntos.
- No abra los enlaces que vienen de mensajes de texto no solicitados.
- No almacene correos electrónicos, fotos o documentos sensitivos en su dispositivo móvil.
- Mantenga su dispositivo móvil actualizado y reforzado con las últimas versiones.
- Asegure su data frecuentemente y tenga copia de respaldo.

NO JAILBREAK (DESTRABE O DESBLOQUEE) SU DISPOSITIVO MÓVIL

Los dispositivos móviles deben ser tratados como computadoras. Sin embargo, hay una manera principal en que los mismos difieren de las computadoras y requieren una atención principal. Los teléfonos inteligentes y las tabletas pueden ser desbloqueados (jail-broken).

Al desbloquear un teléfono inteligente se remueven las protecciones de seguridad que vienen instaladas en el dispositivo móvil que lo protege de aplicaciones maliciosas.

¿Qué usted debe saber?

Es muy importante que usted no modifique la programación de seguridad en su teléfono inteligente por conveniencia. Manipular la programación de fábrica de los teléfonos inteligentes (jail-breaking o rooting),

desestabilizan la estructura de seguridad que ya haya sido instaladas y ofrecidas por la compañía de servicio inalámbrico y de su teléfono inteligente y hace que los mismos más susceptibles a un ataque.

TENGA PRECAUCIÓN AL DESCARGAR LAS APLICACIONES

Los dispositivos móviles pueden ser rápidamente modificados con un alto rango de aplicaciones. Desafortunadamente, el descargar aplicaciones nuevas puede ser algunas veces demasiado fácil. Las aplicaciones maliciosas pueden causar problemas de ejecución y acceso a la información que usted no tiene intención de obtener, o aún más, tomar el control de su dispositivo.

Utilice las siguientes recomendaciones al seleccionar e instalar aplicaciones:

- Sólo descargue aplicaciones de un vendedor aprobado en la tienda de aplicaciones.
- Investigue las aplicaciones antes de descargarlas. Lea las evaluaciones, compare las aplicaciones que provean funciones similares y compare la consistencia de la aplicación del auspiciador oficial del sitio web con la del enlace de la tienda de aplicaciones.
- No sienta temor de seleccionar “No Permitir” cuando instale nuevas aplicaciones. Si una aplicación es está preguntando información o capacidades tales como: el rastreo de GPS en su aparato móvil y no está relacionado con su uso, elija “No permitir” cuando aparezca en su pantalla.

MANTENGA FÍSICAMENTE SEGURO SU DISPOSITIVO MÓVIL

Debido a que su dispositivo móvil puede perderse o ser robado, es importante asegurarlo y mantenerlo siempre su rastro. Si alguien encuentra su aparato móvil, pueden intentar usarlo o tener acceso sus cuentas y a su información.

Para mantener su dispositivo móvil físicamente seguro utilice los siguientes consejos disponibles en el sitio web [US-CERTs](https://www.us-cert.gov/ncas/tips/ST04-017) (<https://www.us-cert.gov/ncas/tips/ST04-017>)

INMEDIATAMENTE REPORTE EL DISPOSITIVO MÓVIL PERDIDO O ROBADO

Si su aparato móvil ha sido robado o está perdido, usted debe reportarlo inmediatamente. Los aparatos de USDA perdidos o robados deben ser reportados a:

- La línea caliente 24 horas de equipos robados (888-926-2373)
- Las autoridades locales (si es robado)
- Cualquier personal que este requerido en la cadena de comandos de su agencia

Después de que dispositivo móvil sea reportado como perdido, USDA se asegurará de que el aparato esté apagado y electrónicamente sea borrado. Esto previene que las personas no autorizadas a utilizar aparatos perdidos o encontrados tengan acceso a los recursos de USDA.

Mientras que el costo de reemplazar el aparato móvil es mínimo, la pérdida o exposición de las data de USDA no tiene precio.

REGULARMENTE REALICE UNA COPIA DE RESPALDO (BACKUP) EN SU DISPOSITIVO MÓVIL

La información almacenada localmente en su dispositivo móvil no puede ser recuperada si usted no crea manualmente una copia de respaldo.

Las copias de respaldo (backup) son fáciles y rápidas; diseñe una rutina que sea fácil de recordar y seguir.

¡APRENDA MÁS!

Haga funcionar el [Verificador de Seguridad del Teléfono Inteligente](#), es una herramienta en línea que le ayuda a los consumidores asegurar sus dispositivos móviles al visitar al sitio y seleccionar el sistema operativo de su móvil.

Esta herramienta le proveerá 10 pasos modificados y consejos para proteger a su aparato celular.

COMPUTADORAS PORTÁTILES & MÁQUINAS DE FAX

La conveniencia de las computadoras portátiles o laptops las hace extremadamente vulnerables a los ladrones o a las brechas de seguridad.

Utilizar la información para iniciar la sesión siempre debe estar protegido por una contraseña.

Tenga mucho cuidado cuando este mostrando algo en su pantalla y sea visible a otros, especialmente aquellos que están cerca de las estaciones tales como: los aviones.

Mantenga en su posesión su computadora portátil en todo momento mientras esté viajando. Cuando llegue a sus destino, verifique que su computadora portátil este propiamente asegurada cuando sea dejada sin atención. Si su laptop tiene capacidad de conexión inalámbrica (wi-fi), asegúrese que tenga configurado propiamente la política de su agencia para IAW. Cuando no esté en uso su computadora portátil o laptop, debe apagar la conexión inalámbrica o si no es posible, debe configurarlo para que al conectarlo reconozca los puntos de accesos de internet y no las redes que están ad-hoc.

Un memorando de OMB establece: Toda data susceptible que esté almacenada en una laptop debe estar cifrada o codificada (encrypted). Asegure que usted está siguiendo tanto las guías y directrices de su agencia, como las de OMB relacionadas a este asunto.

Cuando se transmite información susceptible vía una máquina de fax, asegúrese que el destinatario esté presente para recoger la misma inmediatamente. Contacte al destinatario directamente para confirmar que recibió el fax. Nunca transmita información clasificada vía una máquina de fax que no sea segura.

Siempre utilice una página de cobertura, así su contenido en el fax no estará inmediatamente visible.

REDES INALÁMBRICAS

Las redes inalámbricas operan utilizando señales de radio en vez los cables tradicionales de las computadoras para transmitir y recibir data.

Los usuarios no autorizados con un receptor, pueden interceptar sus comunicaciones y acceso a la red.

Esto es muy peligroso porque usuarios no autorizados pueden ser capaces de no sólo capturar la data que usted está transmitiendo, también la data almacenada en su red.

Reglas de Comportamiento- Redes Inalámbricas

Para todo empleado y contratista de USDA está prohibido el uso sin autorización aparatos 802.11x entre edificios de USDA. Los usuarios deben de asegurarse que cualquier aparato con capacidad inalámbrica incluyendo: computadoras portátiles, PDAs, y teléfonos con Bluetooth, tengan la misma desactivada. La única forma aceptable de comunicación inalámbrica es a través del servicio de mensajes de USDA.

La red inalámbrica es vulnerable porque los usuarios no autorizados pueden capturar no sólo la data que usted está transmitiendo, sino cualquier data que esté almacenada en su red.

Asegúrese de que usted está en cumplimiento con las políticas de su agencia relacionadas al uso de tecnologías inalámbricas.

DESTINO 6: SEGURIDAD FÍSICA E INFORMACIÓN CLASIFICADA

Este destino se enfoca en la seguridad física relacionada a la Seguridad de la Información, el trato de los Datos Clasificados y la Información Personal de Identificación. La seguridad física es la primera línea de defensa de la seguridad de la información y consiste de todo, desde como usted tiene acceso a su ambiente de trabajo, proteger sus contraseñas, hasta mantener rastro del equipo que le ha sido asignado.

Objetivos de Aprendizajes

Luego de completar su lección, usted debe:

- Reconocer que hace la seguridad física de los sistemas de información
- Entender la efectividad en la creación y manejo de una contraseña
- Entender la diferencia entre la Información Clasificada y No Clasificada
- Definir la Dispersión De Información o “Spillage” con respecto a Conciencia sobre la Seguridad Informática (ISA)
- Recordar los requerimientos para reportar una brecha en la Información Personal de Identificación (PII por sus siglas en inglés)

Esta lección incluye los siguientes temas:

- Esenciales de la Seguridad Física
- Control de Inventario
- Información Clasificada y No Clasificada
- Dispersión de Información (Spillage)
- Manejo de la Información Personal de Identificación (PII)

SEGURIDAD FÍSICA

Proteger los sistemas de información federal y la información contenida en los mismos comienza con la seguridad física.

La seguridad física incluye la protección completa de la facilidad, desde los perímetros exteriores hasta las oficinas dentro del edificio, incluyendo todos los sistemas de información e infraestructura.

Usted es responsable por conocer las políticas de seguridad física de su organización y de seguir las mismas. Su organización debe tener procedimientos para tener acceso de entrada, para asegurar su área de trabajo en las noches y para situaciones de emergencia.

Estas deben incluir:

- El uso de una tarjeta de identificación o un código clave para la entrada.
- Bloquear su cubículo.

- Remover su computadora portátil de la estación de acoplamiento (docking station) y colocarla en una localización separada.
- Asegurar su data en dispositivos de almacenamiento, tales como: el disco duro y memoria USB durante procedimiento de emergencias.

SEGURIDAD FÍSICA- ENFOQUE PROACTIVO

Usted debe asegurarse que otros miembros en su organización sigan las políticas de seguridad física y convencer a las personas que no hacen lo mismo. No permita que las personas entren a su edificio u oficina simplemente porque está siguiendo a alguien en vez de utilizar su propio código o tarjeta de identificación.

Exhorten a las personas que no tengan pases o tarjetas de identificación. Si usted es la última persona en salir en la tarde, asegúrese de que otros hayan asegurado sus equipos propiamente.

Finalmente, usted es responsable de reportar cualquier actividad sospechosa.

CONTROL DE INVENTARIO

Parte de la seguridad física incluye el control del inventario del equipo que almacena la información federal. Cuando una computadora portátil del gobierno está perdida o es robada, la información que contiene también lo está. En años recientes, el procedimiento del inventario de control federal ha sido restringido en respuesta de la pérdida de miles de computadoras portátiles del gobierno.

Las agencias federales son responsables de controlar sus inventarios de los equipos de oficinas y computadoras, incluyendo los teléfonos, computadoras, impresoras, máquinas de fax y USB portátiles.

Cuando usted recibe una propiedad del gobierno, debe de firmar por ella. Una vez haya sido firmada, usted es responsable del equipo y debe de tomar las precauciones necesarias para asegurar que el mismo no se pierda o sea robado.

Para remover el equipo o traer el mismo dentro del edificio, su organización puede requerir que usted tenga un pase de propiedad firmado por el administrador de propiedad.

Si la propiedad se pierde o es robada, siga los procedimientos de su organización para reportar la pérdida. En adición al reporte, usted también debe reportar la pérdida de información que está en el equipo y la importancia de la misma.

PROCEDIMIENTOS DE TELETRABAJO

El teletrabajo también conocido como trabajo a distancia y está surgiendo como una opción viable para muchos empleados gubernamentales. Los avances y las capacidades en las telecomunicaciones y computadoras hacen del teletrabajo cada vez más práctico.

Hay riesgos asociados con el acceso remoto en la red de la computadora del gobierno.

Si usted ha recibido la aprobación para hacer teletrabajo, se requiere que cumpla con los requisitos de las políticas y directrices de su agencia.

INFORMACIÓN CLASIFICADA Y NO CLASIFICADA

Toda la información federal, junto con las condiciones y circunstancias adecuadas, podría proporcionar al adversario una visión de nuestras capacidades e intenciones. Además, la agregación de información no clasificada puede elevar el nivel de sensibilidad de la información.

Por lo tanto, incluso información no clasificada, si ve comprometida, podría afectar la seguridad de nuestro personal y sistemas.

Toda la información federal no clasificada que no ha sido específicamente aprobada para el público, requiere cierto nivel de protección de seguridad. Como mínimo, la misma debe ser revisada antes de ser publicada en cualquier forma fuera del gobierno de los Estados Unidos.

¿Qué usted debe saber?

Información No Clasificada

- La información no clasificada incluye: “Para Uso Oficial Solamente” (o FOUO por sus siglas en inglés), “Información No Clasificada Controlada” (o CUI por sus siglas en inglés) y “No Clasificada pero Sensitiva” (o SBU por sus siglas en inglés).
- Ejemplos: información del personal, financiera, de nómina, médica, operacional y del Acta de Privacidad.
- CUI debe ser guardada en una gaveta cerrada o en un contenedor seguro. Cuando ya no sea necesaria, debe ser destruida.

Información Clasificada

- La información clasificada incluye la “Confidencial”, “Secreta” y “Altamente Confidencial” (Top Secret).
- Los niveles específicos de clasificación son determinados por la clasificación original de autoridad.
- La información clasificada debe ser utilizada en un área que haya sido aprobada y determinada para el nivel apropiado de clasificación.
- Cuando no se esté usando la información clasificada debe ser guardada en una bóveda o contenedor aprobado por la Administración de Servicios Generales (o GSA por sus siglas en inglés).

DISPERSIÓN DE INFORMACIÓN (SPILLAGE)

Spillage, también se refiere a contaminación, es cuando la información de alta clasificación es introducida a una de menor nivel de clasificación, Esto es debido al almacenaje inadecuado, la transmisión o el procesamiento de información clasificada a un sistema no clasificado.

Un ejemplo puede ser cuando la información clasificada como Secreta es introducida a una red no clasificada. Cualquier usuario que identifique o sospeche que ha ocurrido una dispersión de la información, inmediatamente tiene que notificarlo a su punto de contacto de seguridad.

Luego de remediar la contaminación es un proceso de recursos intensivos. Puede tomar aproximadamente hasta tres semanas para contener y limpiar la información afectada en el sistema. Está consiente que la dispersión de información puede crear un gran impacto en la seguridad de la información federal.

Recomendaciones de gran ayuda:

- Verifique los correos electrónicos con posible información clasificada.
- Marque y almacene propiamente todos los medios removibles.
- Asegure que todos los nombres de los encabezados de los archivos revelen la sensibilidad de la información.

INFORMACIÓN PERSONAL DE IDENTIFICACIÓN (PII)

El Acta de Privacidad firmada como ley en 1975, requiere que el gobierno proteja la información de individuos que es procesada por agencias federales o contratistas de sistemas de computadoras. El Acta también requiere que el gobierno facilite el acceso a la información por parte del individuo y para corregir si la misma no es precisa, adecuada, completa, o relevante.

¿Qué usted debe de saber?

Las nuevas directrices relacionadas a las grandes medidas de protección de PII son delineadas en diferentes memorandos de OPM.

Por ejemplo: OMB requiere que todo PII que haya sido robado o perdido sea reportado dentro de una hora al Equipo de Respuestas de Emergencias de Computadoras de Estados Unidos (o CERT por sus siglas en inglés).

Cada agencia tiene sus propias políticas para implementar las directrices de OMB. Verifique con su punto de contacto de seguridad para información adicional sobre los requisitos de PII.

Como un usuario autorizado, usted debe de asegurar que PII esté protegido en los sistemas de computadoras federales.

REVISIÓN DE CONOCIMIENTO #9

Llena los espacios en blanco.

Kyle, un empleado de USDA, está trabajando en su escritorio cuando se da cuenta que su billetera con su identificación del gobierno está perdida. La directriz de OMB para la protección de la Información Personal de Identificación requiere que Kyle reporte su billetera perdida al CERT_____.

1. Lo más pronto posible.
2. Dentro de una hora.
3. Cerca del finalizar su día de trabajo
4. Dentro 24 horas.

La respuesta correcta puede ser encontrada en el Apéndice.

REVISIÓN DE CONOCIMIENTO #10

Selección Múltiple (Escoja todas las respuestas que apliquen)

¿Cuál no es PII?

1. Nombre y otros nombres usados
2. Número de Seguro Social completo y acortado
3. Número de teléfono del celular y el de la casa
4. La localización de la oficina
5. Información de Aplicación de la Ley

La respuesta correcta puede ser encontrada en el Apéndice.

DESTINO 7: ROLES Y RESPONSABILIDADES DEL USUARIO

Como usuario autorizado a los sistemas de información federal, usted tiene ciertas responsabilidades y la necesidad de recordar que su derecho a la privacidad está limitado cuando está usando una computadora del gobierno.

Cualquier actividad conducida en el sistema de gobierno puede ser monitoreada. Cada vez que usted se conecta al sistema de gobierno, usted está consintiendo ser monitoreado. Usted debe usar la computadora solo para uso oficial del gobierno.

Evite el mal uso de la computadora. Ejemplos: ver o descargar pornografía, apostar en el internet, llevar a cabo actividades de negocios comerciales privado o empresas con fines de lucros, descargar un software personal o hacer cambios en la configuración no autorizados.

Objetivos de Aprendizaje

Luego de completar esta lección, usted podrá:

- Reconocer la clasificación de los niveles de información federal e identificar lo que debe de hacer para ayudar a proteger la información federal.
- Identificar sus responsabilidades y las “Reglas de Comportamiento” que el gobierno utiliza para los recursos de IT en USDA.

Esta lección incluye los siguientes tópicos:

- Guías Básicas para Usuarios
- Guías de Privilegio de los Usuarios
- Reglas de Comportamiento – Responsabilidad o Rendición de Cuentas
- Reglas de Comportamiento- Uso Apropiado del Correo Electrónico
- Infraestructura Pública Clave
- Consejos para Crear una Contraseña Segura
- Copias de Respaldo, Almacenamiento y Rotulación

GUÍAS BÁSICAS PARA USUARIOS

Existen ocho generalidades básicas aceptadas en las guías de ética que deben ser ejecutadas con sus acciones cuando esté utilizando un sistema de computadoras del gobierno.

Directrices Éticas

- No utilice computadoras para hacer daño.
- No interfiera con el trabajo de otros.
- No espíe los archivos de otros.

- No utilice su computadora para cometer crímenes.
- No utilice o copie software que no esté autorizado.
- No robe propiedad intelectual.
- No utilice una computadora para fingir que es otra persona.
- No utilice los recursos para computadoras sin aprobación.

GUÍA DE PRIVILEGIOS DE LOS USUARIOS

- Seguir las disposiciones de USDA Información Tecnológica / Seguridad de la Información (IT/IS por sus siglas en inglés) Reglas de Comportamiento Generales para usuarios, excepto aquellos con variaciones requeridas para realizar actividades privilegiadas del usuario que han sido autorizadas.
- Limitar la ejecución de actividades privilegiadas del usuario a cuenta(s) privilegiada(s).
- Consentir el monitoreo y la búsqueda de cualquier equipo IT/IS usado mientras el mismo haya estado, haya sido traído o removido de las facilidades de USDA que son propiedades, controladas o rentadas.
- Completar el adiestramiento sobre Conciencia en la Seguridad Informática.
- Completar exitosamente cualquier adiestramiento requerido por USDA que esté relacionado a competentes y operaciones de seguras de IT e IS para las cuales tiene un estatus de usuario privilegiado.
- Someter para investigación y monitoreo adicional las actividades privilegiadas de usuario que son necesarias para garantizar la integridad de las mismas.
- Reportar inmediatamente cualquier incidencia anormal, incluyendo errores y omisiones relacionadas a las actividades de “mi usuario privilegiado” a la Oficial de Seguridad de Sistema de Información (ISSO por sus siglas en inglés), Administrador de Seguridad de Sistema de Información (ISSM por sus siglas en inglés) o al Director de Seguridad (CSO por sus siglas en inglés) de acuerdo al Plan de Respuesta a Incidentes de USDA.
- Utilizar *mi rol privilegiado del usuario* para llevar a cabo sólo actividades de usuario privilegiado aprobadas para el beneficio de USDA.
- Proteger *mi cuenta de “origen”* o *“súper usuario”* incluyendo contraseñas y privilegios al nivel más alto de seguridad de data.
- Cambiar la contraseña de la cuenta de *mi usuario privilegiado* cada 90 días según sea requerido por razones de seguridad.
- Proteger todo lo que este en formato impreso, electrónico u óptico de acuerdo con la política de USDA.
- Llevar a cabo escaneo de virus e integridad a cualquier medio que sea utilizado para la transferencia de información en un sistema de USDA.
- Notificar al ISSO cuando *mi acceso privilegiado del usuario* al sistema ya no sea necesario (por ejemplo: transferencia, terminación, permiso para ausentarse o cualquier periodo de uso no

extendido). *Si soy un ISSO, entonces notificaré al CSO cuando mi cuenta de acceso privilegiado de usuario ya no sea necesaria.*

Comportamiento Expresamente Prohibido

A menos de que sea parte de sus tareas oficiales como Usuario Privilegiado de USDA IT/IS, **Yo No:**

- Compartiré *mi acceso privilegiado de usuario* o privilegios con una persona no autorizada.
- Utilizaré *mi acceso de usuario o privilegio* para “hack” o piratear cualquier IT/IS (en o fuera de la red).
- Intentaré ganar acceso a la data para la cual usted no está específicamente autorizado, para incluir correos electrónicos o archivos de usuarios en los directorios de sus hogares.
- Utilizaré *mi acceso privilegiado de usuario* para negocios no gubernamentales.
- Introduciré ningún software o hardware que no haya sido aprobado a través de los Procesos de Cambio en Administración en los sistemas o redes de USDA IT/IS.
- Utilizaré ninguna comunicación, transmisión, procesamiento o componentes de almacenamiento de USDA para propósitos no autorizados.
- Divulgaré sin autorización, cualquier información personal de identificación (PII) que tenga acceso o aprenda como resultado de sus deberes y actividades de ser un usuario privilegiado.
- Publicaré sin autorización, cualquier información sensitiva, clasificada o confidencial o información fragmentada de USDA a la que tenga acceso o aprenda como resultado de *mis deberes y actividades de ser un usuario privilegiado.*

REGLAS DE COMPORTAMIENTO- RESPONSABILIDAD/ RENDICIÓN DE CUENTAS

En adición a continuar las directrices éticas, todos los usuarios serán responsables y rendirán cuenta de sus acciones relacionadas con los recursos de información que les han sido confiados.

Los usuarios deberán:

- Comportarse de una manera ética, informada y confiable cuando esté usando los sistemas.
- Estar alerta a las amenazas y vulnerabilidades tales como: programas maliciosos y virus.
- Participar en adiestramientos de seguridad en IT y programas de concienciación.
- No instalar o utilizar software no autorizado en equipos de USDA.
- Cumplir con todas las licencias de acuerdos de los softwares y no violar las leyes de derechos reservados federales.
- Conocer que su sistema puede ser monitoreado y que no hay expectativa de privacidad en los recursos IT de USDA.

En adición, los usuarios evitarán que otros utilicen sus cuentas cuando:

- Se desconecten o bloqueen su pantalla al salir del área de sus terminales o computadoras personales (PC).

- Programen una contraseña para el protector de pantalla automático.
- Estén ayudando a remediar las brechas de seguridad sin importar quien tenga la culpa.
- Notifiquen inmediatamente al administrador del sistema cuando haya un cambio en el rol, tareas o el estatus de un empleado cuando el acceso al sistema ya no sea requerido.
- Estén cumpliendo con las reglas de comportamiento cuando se tiene acceso a sistemas externos.
- Estén leyendo y entendiendo el encabezamiento de las páginas y los acuerdos de licencias.

REGLAS DE COMPORTAMIENTO- INTEGRIDAD

Los usuarios deben de proteger la integridad y la calidad de la información. Esto incluye, pero no está limitado a:

- Revisar la calidad de la información según sea colectada, generada y utilizada para asegurar de que es precisa, completa y actualizada.
- Tomar los adiestramientos adecuados antes de utilizar el sistema para aprender como entrar y cambiar la data correctamente.
- Proteger la información en contra de los virus y códigos malicioso cuando:
 - Usen un software anti-virus que esté actualizado.
 - Eviten el uso de un software que no haya sido aprobado tales como: un software de programa compartido o de dominio público.
 - Descontinúen el uso de un sistema cuando muestra la primera señal de una infección con un virus.
- Nunca entrar conscientemente a un sistema no autorizado, desconocido o con información falsa.

REVISIÓN DE CONOCIMIENTO # 11

Selecciona la respuesta correcta.

Peggy es una oficial de computadoras (gurú) y con frecuencia le resuelve los problemas a sus compañeros de trabajo antes de que IT pueda ayudarlos. Peggy, frecuentemente encuentra que puede hacer el trabajo más rápido descargando gratuitamente un programa compartido de herramientas (shareware) que con el software provisto en la computadora de la oficina. ¿Cuál de las siguientes políticas está violando Peggy?

1. Guías Básicas de Ética
2. Responsabilidad de las Reglas de Comportamiento
3. Integridad de las Reglas de Comportamiento
4. Todas las anteriores

La respuesta correcta puede ser encontrada en el Apéndice.

REGLAS DE COMPORTAMIENTO: USO APROPIADO DE CORREO ELECTRÓNICO

Las siguientes reglas se aplican en relación a la actividad de correos electrónicos:

- Los filtros automáticos pueden ayudar a prevenir que los mensajes ofensivos e inapropiados pasen a través del portal de correos electrónicos de USDA.
- Cualquier sistema de correo electrónico gubernamental es propiedad del gobierno y puede convertirse en un récord oficial.
- El uso de los recursos de IT constituye en el consentimiento de posible vigilancia y pruebas de seguridad. El monitoreo y las pruebas de seguridad aseguran que los procedimientos de seguridad adecuados y el uso apropiado para que sean observados por los recursos de IT de USDA.
- La supervisión del correo electrónico y otros recursos de IT por parte de la administración, se llevarán a cabo únicamente conforme con las políticas y directrices establecidas por USDA.
- Es prohibido que los usuarios de los recursos de USDA IT, envíen, reciban, retengan o proliferen cualquier mensaje o material que es fraudulento, inapropiado, ofensivo, de hostigamiento o de naturaleza sexual.

El correo electrónico es sólo para fines oficiales. Su organización puede ser que le permita el uso casual o incidental del correo electrónico.

Las directrices sobre los tipos del uso de correos electrónicos personales que puedan o no puedan ser autorizados son las siguientes:

- El correo electrónico no debe afectar adversamente la ejecución de las tareas oficiales.
- El uso del correo electrónico no debe reflejar mal al gobierno.
- Usted no debe utilizar el correo electrónico del gobierno para enviar pornografía, mensajes de racismo, sexismo, cualquier mensaje ofensivo, enviar correos de cadenas o vender algo.
- El correo electrónico no debe sobrecargar el sistema, como ocurre cuando se envían correos electrónicos en masa.
- Para mantener las redes abiertas y funcionando eficientemente, no reenvíe bromas, fotos o historias inspiradoras.
- Similarmente, evite el uso de “Responder a todos” a menos de que sea absolutamente necesario.
- El correo electrónico personal puede ser autorizado si la duración y la frecuencia son razonables. Preferiblemente, el correo electrónico debe ser utilizado durante el tiempo personal del empleado como lo es el receso de almuerzo.

El correo electrónico también puede ser permisible cuando sirve al interés público legítimo, tal como permitir a un empleado que busque un empleo en respuesta a los recortes en el gobierno federal.

INFRAESTRUCTURA PÚBLICA CLAVE

Los sistemas de información federal identifica y autentifica cada usuario, ya sea a través de un sistema de ingreso con una tarjeta inteligente, identificación (ID) de usuario o contraseña.

El método preferido de acceso a los sistemas de información es a través del uso de una infraestructura pública clave (O PKI por sus siglas en inglés), la cual le permite a su agencia a gestionar claves electrónicas llamadas certificados digitales para los usuarios autorizados.

PKI le permite a los usuarios a cifrar y digitalmente firmar correos electrónicos y documentos.

CONSEJOS PARA CREAR UNA CONTRASEÑA SEGURA

John piensa que cambiar su contraseña frecuentemente y memorizársela es complicado e inconveniente. Así que él la escribe y la deja debajo del teclado de su computadora. ¿A caso John necesitará algunos consejos para crear una contraseña segura que la pueda recordar?

Muchos sistemas de información federal aún identifican y certifican a sus usuarios por medio del uso de su ID de usuario y contraseña. Ambos determinan los derechos del mismo a tener acceso al sistema.

Recuerde, es su responsabilidad el asegurar que todas las practicas realizadas bajo su ID de usuario sean apropiadas para el uso de los recursos de los sistemas de información federal.

¿Qué usted necesita saber?

Es muy importante crear una contraseña compleja con el fin de proteger que los sistemas de gobierno federal no sean comprometidos.

- Combine letras, números y caracteres especiales (ejemplo: !,@,#,\$)
- Utilice combinaciones alfanuméricas o frases asociadas (ejemplo: P@\$w0rd T1p\$)
- Evite palabras o frases que puedan ser encontradas en diccionarios.
- Evite el uso de información personal. (ejemplo: cumpleaños, dirección residencial o número telefónico)
- Memorice su contraseña y absténgase de escribirla.
- Cambie su contraseña regularmente.

COPIAS DE RESPALDO, ALMACENAJE Y ROTULACIÓN

Una gran cantidad de información federal es almacenada en medios removibles tales como: CDs, USB portátiles o discos duros removibles y usted tiene que tener una precaución adicional para protegerlos de robos y no perderlos.

Para los archivos importantes se DEBE crear una copia de respaldo (backup) regularmente y almacenarlos en una localización segura para minimizar la pérdida de data si su disco duro no funciona o es infectado por un virus.

Almacene todos los medios removibles en contenedores tales como: gabinetes para protegerlos del fuego y el agua.

Es muy importante que rotule todos los medios removibles, incluyendo las copias de respaldo y los contenedores para reflejar la clasificación y el nivel de sensibilidad de la información que está contenida en los medios.

Los medios removibles o portátiles deben de estar propiamente marcados y almacenados de acuerdo a la clasificación de seguridad de la información que contienen.

Cuando ya no se necesite la información, usted no debe borrarla o “limpiarla”. Los medios removibles deben ser desmagnetizados o destruidos, si no son reusados al mismo tiempo o a un nivel de clasificación mayor al sistema para el cual fue utilizado inicialmente.

Siga las políticas de su agencia en relación al manejo, almacenamiento, rotulación y destrucción de medios removibles.

REGLAS DE COMPORTAMIENTO- COPIAS DE RESPALDO, ALMACENAJE Y ROTULACIÓN

Los sistemas de computadoras y medios removibles deben ser protegidos de ambientes peligrosos tales como: fuego, agua, calor y derrames de alimentos. Estos deben ser también protegidos de ser robados, alterados sin autorización y manejo negligente.

¿Qué usted debe saber?

Los usuarios deben:

- Utilizar las siguientes medidas físicas y lógicas para prevenir la pérdida de la disponibilidad de la información y los sistemas.
 - Asegurar que tiene una copia de respaldo para la información que usted es responsable.
 - Proteger a los sistemas y medios donde la información es almacenada.
 - Guardar los medios removibles con cubiertas protectoras.
- Mantener los medios lejos de otros que puedan producir campos magnéticos (tales como: teléfonos, radios y magnetos)
- Seguir los planes de contingencia.

REVISIÓN DE CONOCIMIENTO #12

Llena los espacios en blanco.

John está tratando de ser mejor trabajo con su contraseña de seguridad. Todas las siguientes son directrices para crear una contraseña segura excepto_____.

1. John reemplaza algunas de las letras de su contraseña con caracteres especiales tales como: @ and \$.
2. John utiliza su nombre y la calle donde vive en su contraseña para así poderla recordar con facilidad.

3. John utiliza combinaciones alfanuméricas y frases de asociación tales como: \$m311y C@t, para hacer su contraseña más compleja.
4. Ahora que John se ha impuesto un hábito, el cambia su contraseña cada par de semanas.

La respuesta correcta puede ser encontrada en el Apéndice.

REVISIÓN DE CONOCIMIENTO #13

Seleccione la respuesta correcta.

David quiere utilizar como ejemplo las nuevas directrices administrativas que han sido publicadas recientemente por su agencia para un escrito en su clase de negocios. No hay ningún señalamiento o directriz sobre la clasificación de seguridad. David debe:

1. Asumir que las directrices no están clasificadas y utilizarlas para su asignación.
2. Revisar las pautas para cualquier información personal sobre otros empleados de USDA y con un marcador negro ocultar esa información antes de utilizar las directrices para su asignación.
3. Contactar al punto de contacto de seguridad en su agencia para obtener permiso sobre el uso de las directrices para su asignación.
4. Remover todas las referencias del documento de las directrices antes de ser utilizado en su asignación.

La respuesta correcta puede ser encontrada en el Apéndice.

DESTINO: RECTA FINAL

SU RESPONSABILIDAD

La información es un activo crítico para el gobierno de los Estados Unidos. Es su responsabilidad el proteger la información sensitiva y clasificada del gobierno que le haya sido confiada.

Por favor contacte a su punto de seguridad para más información acerca del manejo o clasificación de la

RECONOCIMIENTO DE LAS REGLAS DE COMPORTAMIENTO DE USDA Y PRÓXIMOS PASOS

¡Felicidades!

Usted ya casi ha completado el adiestramiento “Año Fiscal (AF) 2017: Conciencia en la Seguridad Informática y Reglas de Comportamiento de USDA”. Sin embargo, USDA requiere por ley que para asegurar que quien utiliza la Información Tecnológica (IT) y los recursos de Información de Sistemas (IS por sus siglas en inglés) esté consciente de sus responsabilidades, cumplimiento y reconocimientos de esas responsabilidades como han sido delineadas en este adiestramiento, las políticas de USDA y el sistema específico de reglas requiere la firma de del reconocimiento de este adiestramiento, ya sea electrónica, impresa o firmando en la parte inferior, debe ser sometida al Administrador del Programa de Seguridad de Sistemas de Información (o ISSPM por sus siglas en inglés) de la agencia y mantenida en record.

“Entiendo que se me permite renunciar a la lectura de los materiales de capacitación obligatorios del adiestramiento Conciencia en la Seguridad Informática (o ISA por sus siglas en inglés) si tomo y paso antes el pre-examen, esto no me exime de mi responsabilidad de conocer y cumplir en todo momento con las políticas, procedimientos y Reglas de Comportamiento de USDA.”

Esto confirma que he leído y entendido las Reglas de Comportamiento como está detallado en este adiestramiento y entiendo que el mismo puede que no incluya todas las Reglas de Comportamiento incluidas en las políticas, procedimiento y reglas del sistema específico de USDA. Entiendo que el completar este adiestramiento no me exime de mi responsabilidad de saber y seguir en todo momento las políticas de USDA y los procedimientos de las Reglas de Comportamiento.

Yo entiendo que una vez USDA haya emitido mi tarjeta de LincPass o AltLinc, es mi responsabilidad en todo momento de utilizar la tarjeta de acceso de USDA o al sistema y red de la agencia y reportar cualquier problema en el uso de LincPass o AltLinc con el coordinador designado. También entiendo que debo regresar mi tarjeta de LincPass cuando ya no la necesite a mi coordinador de LincPass o persona designada en la agencia.

Firma: _____

Fecha: _____

Por la Regulación Departamental 3620-001, AgLearn es el sistema de adiestramiento oficial de USDA y la fuente para todos los recursos de data para auditorias, la culminación de adiestramientos mandatorios y archivos de examinación relacionados con las acciones del personal. Toda data incluida en AgLearn está sujeta a examinación en cualquier momento por parte del Inspector General de USDA y/o la Oficina de Manejo de Personal sin notificación previa. Las afirmaciones falsas de adiestramientos completados y sometidos por empleados utilizando AgLearn que hayan sido grabadas en el archivo de Historial de Aprendizaje, de ser comprobadas, pueden ser utilizadas para apoyar las acciones administrativas disciplinarias o de otra índole.

APÉNDICE- RESPUESTAS DE LA EVALUACIÓN

Revisión de Conocimiento #1

Llene el espacio en blanco.

Todos los siguientes son aspectos importantes para la Seguridad de los Sistemas Informativos excepto_____.

1. Protección de la información en las redes de las computadoras del gobierno.
2. Bloqueo al acceso no autorizado en las redes de las computadoras del gobierno.
3. Prevención de la modificación digital no autorizada en las redes de las computadoras del gobierno.
4. Restricciones específicas escritas para el uso de las redes en las computadoras del gobierno.

La respuesta correcta de la Revisión de Conocimiento #1 es: Restricciones específicas escritas para el uso de las redes en las computadoras del gobierno. Las guías escritas no cubren cada posible situación para el uso de una computadora del gobierno.

Revisión de Conocimiento #2

Seleccione la respuesta correcta.

¿Cuál de los siguientes sistemas no debería ser incluido en el programa de Protección de Infraestructura Crítica nacional?

1. Seguro Social
2. Planta Eléctrica
3. Escuela Elemental
4. La Reserva Federal

La respuesta correcta de la Revisión de Conocimiento #2 es: Escuelas elementales. La infraestructura crítica se refiere a los sistemas físicos y cibernéticos que son esenciales para las operaciones mínimas de la economía y el gobierno.

Revisión de Conocimiento #3

Selecciona la respuesta correcta.

Kate recibe una llamada telefónica de un hombre que dice está investigando un posible incidente de seguridad en el USDA Web TA o sistema de información de tiempo y asistencia y necesita que ella confirme su contraseña. ¿Qué puede hacer Kate para prevenir o desalentar esta llamada y no ser víctima de un hacker que está utilizando ingeniería social?

1. Verificar la identidad de la persona que llame y obtener su nombre y posición.
2. No dar a conocer su contraseña.
3. Tomar notas detalladas y reportar la llamada a su supervisor.
4. Todas las anteriores. Todas las repuestas son métodos para prevenir el ataque a las computadoras de parte de hackers que usan ingeniería social.

La respuesta correcta de la Revisión de Conocimiento # 3 es: Todas las anteriores. Todas las respuestas son métodos para prevenir que los hackers de las computadoras usen ingeniería social.

Revisión de Conocimiento #4

Llene el espacio en blanco.

Linda recibió un correo electrónico de su banco donde le pedían verificar los números de su cuenta y PIN para prevenir un robo de identidad. Esto podría ser una forma de un riesgo en la seguridad de la información conocido como_____.

1. Hoax (Broma)
2. Phishing (Fraude Electrónico)
3. Correo de Ingeniería
4. Robar Cookies

La respuesta correcta de la Revisión de Conocimiento # 4 es: Phishing (Fraude Electrónico). Phishing es un fraude altamente tecnológico que utiliza correos electrónicos o sitios web para convencer a los usuarios que divulguen números de tarjetas de crédito, información de cuenta bancaria, número de seguro social, contraseñas y otra información sensible.

Revisión de Conocimiento #5

Llene el espacio en blanco.

Mike quiere ver un enlace de un sitio web gracioso del cual le habló su amigo, pero él necesita instalar y ejecutar primero una aplicación de ActiveX. ActiveX es una forma de Código Móvil. Todas las siguientes son formas de Código Móvil excepto _____.

1. Ver audio clips.
2. Insertar un virus en la computadora.
3. Permitir la comunicación en un teléfono celular cifrado o codificado (encrypted).
4. Controlar la navegación en un sitio web.

La respuesta correcta de la Revisión de Conocimiento #5 es: Permitir la comunicación en un teléfono celular cifrado o codificado (encrypted). El código móvil incorporado en un sitio web puede reconocer y

responder al usuario ya sea moviendo su ratón, controlando la página de navegación, poniendo videos o ejecutando programas hostiles en su computadora.

Revisión de Conocimiento #6

Seleccione la respuesta correcta.

¿Cuál de los siguientes es un tipo de Malware?

1. Adware (programa de publicidad)
2. Spyware (programa espía)
3. Rootkit (juego de herramientas o programas)
4. Caballo de Troya (Trojan horse)
5. Keyloggers (registrador de teclas)
6. Todas las anteriores

La respuesta correcta para la Revisión de Conocimiento #6 es: Todas las anteriores. Sí el Malware o Código Malicioso es también conocido por diferentes nombres.

Revisión de Conocimiento #7

Seleccione la respuesta correcta.

¿Cuál de los siguientes es una señal de un malware en su computadora?

1. Lentitud
2. Reducción del espacio en el disco duro
3. Errores
4. Mensajes pop-ups
5. Todas las anteriores

La respuesta correcta para la Revisión de Conocimiento #6 es: Todas las anteriores. Sí el Malware o Código Malicioso es también aparece en diferentes formas.

Revisión de Conocimiento #8

Seleccione la respuesta correcta.

Phyllis recibe un correo electrónico del proveedor de su teléfono celular indicando que la cantidad que ella debe es diferente a la que debería ser. ¿Qué pasos no debería Phyllis seguir antes de abrir enlace en el correo electrónico?

1. Es apropiado que haga clic a cualquier enlace, ya que el correo electrónico proviene de su compañía de teléfonos.

2. Verificar si hay alguna referencia a su número de cuenta o número de teléfono móvil.
3. Filtrar todos los enlaces en el mensaje para asegurarse que todos vayan a un dominio válido.
4. Llamar al servicio al cliente de su proveedor o entrar en su sitio web escribiendo su dominio para verificar el mensaje de correo electrónico.

La respuesta correcta para la Revisión de Conocimiento #8 es: Es apropiado que haga clic a cualquier enlace, ya que el correo electrónico proviene de su compañía de teléfonos. Hacer clic en un link antes de verificar si es legítimo no es recomendado. Phyllis debe estar al tope sobre cualquier enlace en el mensaje para asegurarse que todos vayan a dominios válidos.

Revisión de Conocimiento #9

Llena los espacios en blanco.

Kyle, un empleado de USDA, está trabajando en su escritorio cuando se da cuenta que su billetera con su identificación del gobierno está perdida. La directriz de OMB para la protección de la Información Personal de Identificación requiere que Kyle reporte su billetera perdida al CERT_____.

1. Lo más pronto posible.
2. Dentro de una hora.
3. Cerca del finalizar su día de trabajo
4. Dentro 24 horas.

La respuesta correcta para la Revisión de Conocimiento #9: Dentro de una hora. OMB requiere que los objetos perdidos o robados con PII tienen que ser reportados entre una hora.

Revisión de Conocimiento #10

Selección Múltiple (Escoja todas las respuestas que apliquen)

¿Cuál no es PII?

1. Nombre y otros nombres usados
2. Número de Seguro Social completo y acortado
3. Número de teléfono del celular y el de la casa
4. La localización de la oficina
5. Información de Aplicación de la Ley

La respuesta correcta para la Revisión de Conocimiento #10 es: La localización de la oficina. La localización de la oficina generalmente no es considerada Información Personal de Identificación.

Revisión de Conocimiento # 11

Selecciona la respuesta correcta.

Peggy es una oficial de computadoras (gurú) y con frecuencia le resuelve los problemas a sus compañeros de trabajo antes de que IT pueda ayudarlos. Peggy, frecuentemente encuentra que puede hacer el trabajo más rápido descargando gratuitamente un programa compartido de herramientas (shareware) que con el software provisto en la computadora de la oficina. ¿Cuál de las siguientes políticas está violando Peggy?

1. Guías Básicas de Ética
2. Responsabilidad de las Reglas de Comportamiento
3. Integridad de las Reglas de Comportamiento
4. Todas las anteriores

La respuesta correcta para la Revisión de Conocimiento #11 es: Todas las anteriores. Instalar cualquier software que no ha sido aprobado en una computadora del gobierno, viola las guías básicas de ética del usuario y las reglas de comportamiento para la responsabilidad (rendición de cuentas) e integridad.

Revisión de Conocimiento #12

Llena los espacios en blanco.

John está tratando de ser mejor trabajo con su contraseña de seguridad. Todas las siguientes son directrices para crear una contraseña segura excepto_____.

1. John reemplaza algunas de las letras de su contraseña con caracteres especiales tales como: @ and \$.
2. John utiliza su nombre y la calle donde vive en su contraseña para así poderla recordar con facilidad.
3. John utiliza combinaciones alfanuméricas y frases de asociación tales como: \$m311y C@t, para hacer su contraseña más compleja.
4. Ahora que John se ha impuesto un hábito, el cambia su contraseña cada par de semanas.

La respuesta correcta para la Revisión de Conocimiento #12 es: John utiliza su nombre y la calle donde vive en su contraseña para así poderla recordar con facilidad. John debe evitar el uso de información personal para sus contraseñas. En vez, debe utilizar una frase de asociación reconocible.

Revisión de Conocimiento #13

Seleccione la respuesta correcta.

David quiere utilizar como ejemplo las nuevas directrices administrativas que han sido publicadas recientemente por su agencia para un escrito en su clase de negocios. No hay ningún señalamiento o directriz sobre la clasificación de seguridad. David debe:

1. Asumir que las directrices no están clasificadas y utilizarlas para su asignación.
2. Revisar las pautas para cualquier información personal sobre otros empleados de USDA y con un marcador negro ocultar esa información antes de utilizar las directrices para su asignación.
3. Contactar al punto de contacto de seguridad en su agencia para obtener permiso sobre el uso de las directrices para su asignación.
4. Remover todas las referencias del documento de las directrices antes de ser utilizado en su asignación.

La respuesta correcta para la Revisión de Conocimiento #13 es: Contactar al punto de contacto de seguridad en su agencia para obtener permiso sobre el uso de las directrices para su asignación. Debido a que David no puede decir si la información ha sido para aprobada para su publicación. Él debe contactar al contacto de seguridad de su agencia y buscar permiso para el uso de las guías.