

Subject: FW: OSI Trivia #001

From: Consulta OSI

Sent: Wednesday, August 30, 2006 4:14 PM

To: UPR-Usuarios; Aixa Ramírez; Edwin Martínez - RRP; Ernesto Soto - UPR CUH; Hector Morales - UPR Carolina; Ismael Villanueva; Juan Vega Vega - UPR Ponce; Omar Díaz - UPR Bayamon; Rafael Pagán; Rosa Ramírez - Cayey; Sandra Santos - UPR RCM; Victor Díaz - UPR RUM; Wilfredo de la Rosa - UPR Utuado

Subject: OSI Trivia #001

Adjunto el comienzo de una nueva serie informativa en herramientas y usos de las tecnologías. Esta serie llamada OSI Trivia, al igual que las Circulares Técnicas, será para uso y referencia de ustedes. Se ha establecido una vía de comunicación electrónica (consultaosi@upr.edu), la cual pueden utilizar para comunicarse y presentar sugerencias. Reciban un saludo cordial.

22 de agosto de 2006

001

OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información



USO DE CONTRASEÑAS



GUÍAS PARA UNA CONTRASEÑA CORRECTA

1. Mezclar caracteres alfabéticos, numéricos y caracteres especiales
2. Utilizar mayúsculas y minúsculas
3. Utilizar al menos 8 caracteres
4. Cambiar la contraseña con frecuencia

Buenas Prácticas

- PRIVADO: conocido por el usuario solamente
- SECRETO: debe ser construido, no debe ser palabra existente
- FÁCIL DE RECORDAR: para que no haya que escribirlo

AVISOS CONTRA UNA CONTRASEÑA INCORRECTA

1. NO compartir contraseñas
2. NO utilizar nombres, información personal, palabras del diccionario
3. NO utilizar la misma contraseña para todas las cuentas
4. NO utilizar secuencias repetitivas
5. NO utilizar el mismo patrón para cada contraseña (ej. misma contraseña y se añade número al final)
6. NO escribir contraseña en papel o en documentos en la computadora, y de tenerlo que hacer no tenerla visible
7. NO enviar contraseña electrónicamente
8. NO utilizar la clave de usuario ("user id") como contraseña
9. NO utilizar espacios en blanco ("spacebar")
10. NO utilizar la opción "Remember Password"

Prácticas Equivocadas

- Prestar cuentas, porque se le olvidó la contraseña a otro usuario
- Anotar la contraseña en un lugar visible
- Usar contraseñas disponibles en servidores de uso público

Para más temas de información diríjase a: <http://osi-ac.upr.edu/info/>

consultaosi@upr.edu

From: Consulta OSI
Sent: Thursday, September 28, 2006 5:02 PM
To: UPR-Usuarios
Subject: OSI Trivia #002
Attachments: netiquette.pdf; netiquette.jpg

22 de septiembre de 2006

OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información



Etiqueta en los Correos Electrónicos

BUENAS PRÁCTICAS

1. Ser claro y conciso
2. Aclarar preguntas y futuras preguntas
3. Utilizar gramática, puntuación y ortografía correctamente
4. Utilizar tono cordial y profesional
5. Contestar rápido
6. Utilizar "Reply" al contestar (mantiene historial)
7. Leer la respuesta antes de enviarla
8. Utilizar la opción Bcc ("Blind Carbon Copy") para proteger las direcciones de los destinatarios
9. Identificar el tema ("Subject") de manera significativa y apropiada
10. Utilizar verbos en su forma activa
11. Evitar oraciones demasiado largas
12. Mantener el lenguaje neutral
13. Utilizar el Cc ("Carbon Copy") en los casos que sean apropiados y justificados
14. Especificar el formato de los anejos
15. Utilizar listas de distribución en la medida que sea posible
16. Identificarse con su nombre, puesto, teléfonos y dirección electrónica al firmar

PRÁCTICAS EQUIVOCADAS

1. Anejar archivos innecesarios o demasiado grandes
2. Sobreutilizar la opción de alta prioridad
3. Escribir en MAYÚSCULAS (se interpreta como gritar)
4. Sobreutilizar la opción "Reply to All"
5. Utilizar abreviaciones inapropiadas (no todos las entienden)
6. Complicar el mensaje con colores y formatos
7. Reenviar ("Forward") mensajes en cadena
8. Solicitar recibo de entrega y lectura
9. Copiar un mensaje o anejo sin permiso del dueño
10. Utilizar el correo electrónico para información confidencial
11. Utilizar el correo electrónico en vez del teléfono para mensajes que requieren contestación inmediata
12. Utilizar el correo electrónico para propósitos que pueden percibirse como comerciales
13. Utilizar palabras como Urgente o Importante
14. Enviar mensajes difamatorios, ofensivos, racistas u obscenos
15. Contestar mensajes spam

NOTA: No todos los clientes de correo electrónico pueden mostrar mensajes en formato de HTML, en esos casos, los mensajes se mostrarán en formato de texto.

Para más temas de información diríjase a: <http://www.its.upr.edu/trivia/>

consultaosi@upr.edu

Rafael Pagán

From: Consulta OSI
Sent: Tuesday, October 31, 2006 11:41 AM
To: UPR-Usuarios
Subject: FW: OSI Trivia

Subject: OSI Trivia

20 de octubre de 2006



OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información

Listas de Correos Electrónicos

BUENAS PRÁCTICAS

1. Definir listado para grupos de personas a las que periódicamente se le remite un mismo correo electrónico de un tema asociado.
2. Revisar proactivamente la utilización de la lista, para cotejar que se utilice apropiadamente.
3. Notificar a OSI de incidentes de mal uso de una lista de correo electrónico.
4. Utilizar lista de distribución para enviar correo de un asunto relevante para los miembros de la lista.

PRÁCTICAS EQUIVOCAS

1. Enviar correos a listas de distribución para temas sean relevantes para todos sus miembros.
2. Enviar correos electrónicos a las listas institucionales previa autorización del supervisor inmediato.
3. Añadir participantes en las listas de correo electrónico sin la debida autorización.
4. Enviar archivos o anejos de gran tamaño a las listas de correo electrónico.
5. Enviar correos no relacionados a temas del trabajo tal como cadenas de correo.

Para más temas de información diríjase a: <http://osi-ac.upr.edu/info/>

consultaosi@upr.edu

*Maria T. Moreno Rivera
Analista Programador de Sistemas
Administración Central
Universidad de Puerto Rico
Tel. 787-250-0000 ext. 5495*

Subject: FW: OSI Trivia #4

From: Consulta OSI

Sent: Monday, December 04, 2006 5:15 PM

To: UPR-Usuarios

Subject: OSI Trivia #4

30 de noviembre de 2006

004



OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información

Resguardos ("Backup")

Buenas Prácticas

1. Hacer resguardos periódicamente: a diario o semanal.
2. Probar efectividad de resguardo, accediendo documentos del mismo para que se puedan utilizar en caso de emergencia.
3. Utilizar un dispositivo confiable para resguardar datos, preferiblemente disco compacto (CD, DVD) o "flash drives".
4. Rotular CD o DVD claramente con la fecha del resguardo y su contenido.
5. Almacenar documentos en un servidor de archivos, de haber uno disponible (contacte a su administrador de servidores).

Prácticas Equivocadas

1. No resguardar documentos de trabajo periódicamente.
2. Trabajar con documentos en "diskettes" o "pen drives" en lugar de usar estos dispositivos sólo como resguardo; ya que son más propensos a avería y puede resultar en la pérdida del documento.
3. Mantener una sola copia de resguardo.
4. Mantener resguardo en ambiente no adecuado: cerca de imanes, temperaturas extremas o áreas sucias.

Ventajas de Resguardo

1. De averiarse su computadora, le permite salvar su trabajo.
2. Si sus documentos se corrompen por virus, puede recuperarlos de un resguardo.
3. Almacenar archivos en un solo servidor, permite que el administrador del servidor resguarde los mismos.

Acceda versiones anteriores de OSI Trivia en: <http://osi-ac.upr.edu/info/>

Contáctenos en: consultaosi@upr.edu

Subject: FW: OSI Trivia #5
Attachments: OSI Trivia #5.pdf

From: Consulta OSI
Sent: Thursday, December 28, 2006 9:08 AM
To: UPR-Usuarios
Subject: OSI Trivia #5

28 de diciembre de 2006

005

OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información



CREACIÓN DE CONTRASEÑAS



La creación de una contraseña fuerte evitará que accedan la misma sin autorización.

BUENAS PRÁCTICAS

1. Utilice una palabra escrita en reverso como contraseña.
2. Utilice una palabra trasponiendo letras (anagrama) o sustituyendo letras por números o caracteres especiales.
Ejemplos:
 - "c3kur1dat" en vez de seguridad
 - "anesartnoc" en vez de contraseña
3. Utilice palabras de otros idiomas.
4. Repita letras adrede en la contraseña. Por ejemplo, "caandaddo"
5. En lo posible, elija una ristra de caracteres aleatorios (mientras menos común mejor)
6. Escriba intercalando caracteres de cuatro tipos: letras mayúsculas, letras minúsculas, dígitos y caracteres especiales.
7. Utilice términos de 8 caracteres o más para su contraseña (a mayor número, mejor)

PRÁCTICAS EQUIVOCADAS

1. Reutilizar una contraseña anterior.
2. Colocar un dígito al comienzo o final de la contraseña.
3. Utilizar la misma contraseña para diferentes sistemas.
4. Utilizar palabras asociadas a pasatiempos conocidos.
5. Verbalizar o mencionar en voz alta la contraseña mientras la escribe.
6. Utilizar su clave de usuario como contraseña.
7. Utilizar palabras como "password", "password1" o "contrasena".
8. Utilizar datos confidenciales tal como el número de seguro social o cualquiera porción de esto como contraseña.
9. Utilizar su nombre, el de parientes, amigos o mascotas en cualquiera combinación para la contraseña.
10. Utilizar fechas especiales (aniversarios, cumpleaños, etc.) en cualquier combinación para la contraseña.

Recuerde

Cambie su contraseña inmediatamente que ocurra alguna de las siguientes situaciones:

1. Posterior a brindar la contraseña a otra persona con el propósito de recibir apoyo técnico o para reparar su equipo.
2. Cuando la confiabilidad o confidencialidad de la contraseña queda en entredicho. En este caso, notifique a OSI inmediatamente para que se determine si amerita investigar el tema.

Acceda versiones anteriores de OSI Trivia en: <http://osi-ac.upr.edu/info/>

Contáctenos en: consultaosi@upr.edu

Subject: FW: OSI Trivia #006

From: Consulta OSI

Sent: Wednesday, January 31, 2007 11:58 AM

To: Consulta OSI

Subject: OSI Trivia #006

31 de enero de 2007

006

OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información



EVITE INFECCIÓN POR VIRUS Y PROGRAMACIÓN MALICIOSA

BUENAS PRÁCTICAS

1. Utilizar un programa de antivirus (ej. Symantec Antivirus)
2. Actualizar el programa de antivirus frecuentemente
3. Resguardar periódica y frecuentemente el contenido de su computadora
4. Orientar a los usuarios
5. Tener mecanismos de control al regresar a la institución un disco o medio de resguardo que fue sacado de la oficina
6. No abrir archivos adjuntos en los mensajes de correo electrónico o mensajes que se vean sospechosos
7. Cotejar con programas antivirus los discos y otros medios electrónicos de almacenaje utilizados, previo a insertar en su computadora
8. Evitar bajar programas o archivos a su computadora de fuentes desconocidas o dudosas

PRÁCTICAS EQUIVOCADAS

1. Utilizar discos y medios de resguardo infectados
2. Ejecutar programas infectados
3. Abrir documentos infectados
4. Acceder a una computadora infectada
5. Compartir archivos y programas infectados

FUENTES DE CONTAMINACIÓN

1. Mensajes desconocidos por correo electrónico
2. Archivos y programas bajados de páginas cuestionables en el Internet
3. Computadoras infectadas conectadas a la red
4. Acciones maliciosas de individuos

PASOS A SEGUIR EN CASO DE INFECCIÓN

1. Desconecte la computadora infectada del resto de la red.
2. Utilice resguardo del sistema operativo original para re-iniciar su computadora.
3. Determine con apoyo de OSI la gravedad de la infección.
4. Resguede archivos no ejecutables y directorios en otro medio o unidad que no esté infectado.
5. Restaure todos los programas utilizando los medios originales del producto y el contenido de su computadora de un resguardo reciente no infectado.
6. Identifique y ubique todos los medios insertados en su computadora a partir de su infección, para desinfectar los mismos.

Para más temas de información dirijase a: <http://osi-ac.upr.edu/info/>

consultaosi@upr.edu

Subject: FW: OSI Trivia #007

From: Consulta OSI

Sent: Monday, February 26, 2007 11:57 AM

To: Consulta OSI

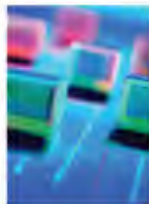
Subject: OSI Trivia #007

22 de febrero de 2007

007

OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información



Protección de Computadoras

BUENAS PRÁCTICAS

1. Proteger el equipo de riesgos ambientales tales como polvo, fuego y agua.
2. Suministrar ventilación adecuada al equipo en operación
3. Instalar regulador de voltaje y fuente de carga ininterrumpidas (UPS) para extender la vida útil del equipo
4. Desactivar y apagar el equipo al concluir el día
5. Notificar de inmediato cualquier falla de la computadora o en su acceso a la red, para mitigar el riesgo de perder información o acceso a servicios básicos
6. Coordinar con OSI la instalación de todo programa
7. Resguardar programas y datos periódicamente
8. Remover información confidencial de una computadora previo a enviarla para reparación; o asignar la reparación a una compañía que tiene acuerdo de no divulgación con la Universidad.

PRÁCTICAS EQUIVOCADAS

1. Fumar, comer o beber mientras utilice la computadora
2. Modificar la configuración del equipo o su programación; lo que puede interrumpir el uso de la computadora o el acceso a la red
3. No hacer "logoff" de su computadora cuando se aparte del equipo por periodos extendidos
4. Dejar su computadora desprotegida, a la vista y acceso de todos; propensa al robo
5. No informar de inmediato la pérdida o robo de equipo
6. Utilizar equipo módem independiente de la red de comunicaciones sin coordinarlo con OSI; lo cual expone la red al riesgo de ataques.
7. No codificar información confidencial previo a transmitir o almacenar la misma.
8. Eliminar versión de-codificada de datos, previo a probar que la información codificada se puede recuperar

Para más temas de información dirijase a: <http://osi-ac.upr.edu/info/>

consultaosi@upr.edu

Subject: FW: OSI Trivia #008

From: Consulta OSI

Sent: Wednesday, March 28, 2007 8:45 AM

To: Consulta OSI

Subject: OSI Trivia #008

19 de marzo de 2007

008

OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información



Compartir Archivos

BUENAS PRÁCTICAS

1. Compartir archivos y datos sólo con personas que estén autorizados a ellos
2. Utilizar programas Peer-to-Peer (tales como Kazaa, BitTorrent, Ares, Gnutella o EDonkey) con prudencia
3. Coordinar de antemano con la Oficina de Sistemas de Información, si requiere ejecutar programas Peer-to-Peer mientras se conecta a la red
4. Asegurar que sus datos, archivos y programas estén protegidos contra el acceso y copiado no autorizado desde otras computadoras
5. Desactivar programa Peer-to-Peer o apagar su computadora, si planifica estar alejado de su área de trabajo durante un período extendido

PRÁCTICAS EQUIVOCADAS

1. Tener activa la funcionalidad de compartir archivos ("File Sharing") al utilizar programas Peer-to-Peer, mientras está conectado a la red universitaria, sin tener necesidad y sin coordinarlo con la Oficina de Sistemas de Información
2. Copiar datos, archivos, programas, canciones o películas de video sin tener el permiso legal de hacerlo
3. Suministrar datos, archivos, programas, canciones o películas de video a terceros que no tienen autorización ni permiso legal a éstos

Para más temas de información dirijase a: <http://osi-ac.upr.edu/info/>

consultaosi@upr.edu

Subject: FW: OSI Trivia #009

From: Consulta OSI

Sent: Thursday, April 26, 2007 2:47 PM

To: UPR-Usuarios

Subject: OSI Trivia #009

23 de abril de 2007

009

OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información



Protección de Computadoras III

BUENAS PRÁCTICAS

1. Tener antivirus y actualizar el mismo periódicamente
2. Efectuar copias de resguardo periódicas
3. Actualizar periódicamente su sistema operativo y programados para asegurar que tengan los parchos y seguridad de los mismos
4. Utilizar sólo programas adquiridos legalmente
5. Desactivar cualquier programa "sospechoso" y cotejar en el panel de control si existe alguno que no haya instalado
6. Instalar programas de protección ("firewall", anti-spyware)
7. Crear y activar contraseñas fuertes para así evitar el acceso no autorizado al equipo
8. Correr el desfragmentador de disco duro para mejorar el desempeño del equipo
9. Conocer más sobre las infecciones y ataques a las computadoras para proteger mejor su equipo
10. Estar alerta ante nuevos virus y tomar las acciones recomendadas para proteger su computadora contra éstos.

PRÁCTICAS EQUIVOCADAS

1. Permitir que cualquier persona utilice su computadora
2. Activar en su computadora las opciones para compartir archivos e impresoras sin especificar quién estará autorizado a accederla.
3. Permitir que navegantes por Internet tengan acceso o borren archivos en su computadora
4. Abrir mensajes de correo electrónico o archivos adjuntos si desconoce su origen
5. No verificar archivos dudosos con el programa de antivirus
6. Guardar contraseñas en su equipo, especialmente si es utilizado por terceros
7. No desconectarse del Internet cuando no lo esté utilizando

Para más temas de información dirijase a: <http://osi-ac.upr.edu/info/>

consultaosi@upr.edu

Subject: FW: OSI Trivia #010

From: Consulta OSI

Sent: Monday, June 04, 2007 10:28 AM

Subject: OSI Trivia #010

1 de junio de 2007

039

OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información



Preparación de Contingencias

BUENAS PRÁCTICAS

1. Identificar, revisar y comprender el plan de emergencia de su oficina
2. Identificar Centro de Operaciones de Emergencia
3. Suministrar sus números de teléfono a la supervisión de la oficina, para que se puedan contactar con usted durante una emergencia
4. Ubicar en un lugar seguro y fuera de su oficina el listado de sus claves de usuario y contraseñas
5. Mantener resguardos actualizados de sus archivos críticos
6. Mantener expediente con copias de los documentos críticos de trabajo, para reubicarlos fuera de la oficina durante una emergencia
7. Mantenerse pendiente a los avisos y notificaciones de su oficina

PRÁCTICAS EQUIVOCADAS

1. No estar atento a los avisos de activación del plan de emergencia en su oficina
2. Mantener objetos sueltos sobre escritorio u otra superficie expuesta donde se puedan convertir en proyectiles
3. Dejar sin archivar documentos y medios electrónicos sobre su escritorio u otra superficie expuesta
4. No cubrir computadoras y otro equipo informático con toldos plásticos para protegerlos contra inclemencias
5. Dejar equipos electrónicos y documentos en el piso, cerca de ventanas o en áreas inundables
6. Dejar equipo electrónico conectado a receptáculos eléctricos y a la red

Para más temas de información dirijase a: <http://osi-ac.upr.edu/info/>

consultaosi@upr.edu

Subject: FW: OSI Trivia #011

From: Consulta OSI

Sent: Monday, June 25, 2007 2:52 PM

Subject: OSI Trivia #011

25 de junio de 2007

011

OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información



Después de una Emergencia

BUENAS PRÁCTICAS

1. Contactar su supervisión cuando haya pasado la emergencia
2. Inspeccionar su área de trabajo y la condición de los equipos informáticos al regresar a su oficina
3. Notificar a su supervisor y a la OSI de cualquier daño visible o percibido en los equipos informáticos
4. Inspeccionar su acceso a los diferentes sistemas y servicios; y notificar a la OSI de cualquier problema encontrado
5. Restaurar aquellos documentos electrónicos que trabajó durante la emergencia, luego de que haya verificado que los sistemas funcionan adecuadamente

PRÁCTICAS EQUIVOCADAS

1. Demorarse en notificar a su supervisor o a la OSI de cualquier daño visible o percibido de cualquier equipo o computadora
2. Reconectar el equipo informático en áreas inundadas o averiadas por la emergencia
3. Reconectar y encender su computadora sin confirmar que la OSI haya inspeccionado la red de comunicaciones
4. Intentar acceder o actualizar los datos a través de los sistemas sin que la OSI haya confirmado que las aplicaciones están disponibles

NOTA: En caso de dudas, consulte con su Oficina de Sistemas de Información (OSI)

Para más temas de información dirijase a: <http://osi-ac.upr.edu/info/>

consultaosi@upr.edu

Subject: FW: OSI Trivia #012

From: Consulta OSI

Sent: Monday, July 30, 2007 3:08 PM

Subject: OSI Trivia #012

30 de julio de 2007

012

OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información



Utilización Correcta de "Software"

BUENAS PRÁCTICAS

1. Utilizar sólo programas para los cuales posee una autorización o licencia legítima
2. Mantener prueba de autorización o copia de la licencia para los programas que tiene instalado en su computadora
3. Utilizar los programas que suministra la Universidad para funciones estándares tales como mensajería electrónica, procesamiento de texto, hojas de cálculo o presentaciones gráficas
4. Si administra un servidor, debe instalar y ejecutar programas nuevos o versiones nuevas de programas existentes en un ambiente de prueba, previo a instalarlo donde pueda impactar a los usuarios

PRÁCTICAS EQUIVOCADAS

1. Suministrar programas a terceros, en violación a los acuerdos contractuales y a los derechos de autor
2. Aceptar un programa de una fuente desconocida o que no es oficial sin tener la debida licencia de utilización
3. Bajar programas de fuentes desconocidas en el Internet, que pudieran exponer su computadora o la red a invasión de virus o programas nocivos

Para más temas de información dirijase a: <http://osi-ac.upr.edu/info/>

consultaosi@upr.edu

Subject: FW: OSI Trivia #07.01

From: Consulta OSI

Sent: Monday, August 27, 2007 4:13 PM

Subject: OSI Trivia #07.01

30 de agosto de 2007

07.01



OSI Trivia

Universidad de Puerto Rico / Oficina de Sistemas de Información

Protección de Computadoras Portátiles

BUENAS PRÁCTICAS

1. Asegurar la computadora portátil con dispositivos de seguridad en el área de trabajo
2. Guardar la computadora portátil en un lugar no visible y bajo llave cuando deba viajar sin ella
3. Rotular de manera permanente la computadora portátil y sus accesorios con el nombre del usuario y/u organización
4. Registrar marca, modelo, número de serie y número de propiedad de la computadora portátil; y almacenar esta información por separado, para usar en caso de robo
5. Si utiliza tarjeta módem para conectar al Internet, expulsarla de la computadora y llevarla consigo al apartarse de la computadora portátil

PRÁCTICAS EQUIVOCADAS

1. Almacenar la computadora portátil en un bulto ostentoso que llame la atención
2. Almacenar la computadora portátil en un bulto o saco que no esté debidamente amortiguado para protegerla de golpes
3. Dejar la computadora portátil desatendida y accesible a terceros
4. Colocar la computadora portátil sobre una superficie pequeña o desnivelada, donde esté propensa a caerse
5. Dejar la computadora portátil a plena vista dentro del auto
6. No informar de inmediato la pérdida, robo o intento de robo del equipo

Para más temas de información dirijase a: <http://osi-ac.upr.edu/info/>

consultaosi@upr.edu

Subject:

FW: OSI Trivia - Septiembre 2007 - Evite el Robo de Identidad

From: Consulta OSI

Sent: Tuesday, October 02, 2007 9:31 AM

To: Consulta OSI

Subject: OSI Trivia - Septiembre 2007 - Evite el Robo de Identidad

30 de septiembre de 2007

OSI TRIVIA

Universidad de Puerto Rico / Oficina de Sistemas de Información



EVITAR ROBO DE IDENTIDAD

BUENAS PRÁCTICAS

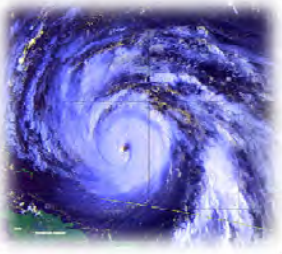
1. Evitar suministrar a terceros los siguientes elementos de su identidad: nombre, dirección, fecha de nacimiento y seguro social
2. Cotejar la seguridad de la página de Internet antes de entrar información sensible: prefijo "https" al comienzo de una dirección o el símbolo del candado en la parte inferior de la página
3. Proteger su información personal (seguro social, # tarjeta de crédito, etc.) de quien la solicite sin una justificación clara o necesidad real confirmada
4. Codificar ("encrypt") los archivos personales y privados para dificultar su lectura electrónica de forma no autorizada
5. Utilizar programas de seguridad para eliminar de forma segura archivos de una computadora que se vaya a desochar o ceder a terceros

PRÁCTICAS EQUIVOCADAS

1. Suministrar sus claves de usuario o contraseñas a terceras personas por teléfono, correo electrónico o Internet
2. Brincar su # seguro social - o los últimos 4 dígitos del mismo - a terceras personas por teléfono, correo electrónico o Internet
3. Proveer su fecha de nacimiento por el Internet
4. Responder a correos electrónicos no solicitados que venden productos o servicios
5. Emitir pagos electrónicos a través de páginas no aseguradas del Internet
6. No cotejar previamente la reputación de la compañía a la cual le suministra su número de tarjeta de crédito

Para ediciones anteriores, diríjase a <http://osi-ac.upr.edu/info>

consulta@osi.upr.edu



Preparación ante Contingencias

Buenas Prácticas

- Identificar, revisar y comprender el plan de emergencia de su oficina
- Identificar el Centro de Operaciones de Emergencia
- Suministrar sus números de teléfono a la supervisión de la oficina, para que se puedan contactar con usted durante emergencia
- Ubicar el listado de sus claves de usuario y contraseñas en un lugar seguro y fuera de su oficina
- Mantener resguardos actualizados de sus archivos críticos
- Mantener expediente con copias de los documentos críticos de trabajo, para reubicarlos fuera de la oficina durante una emergencia
- Mantenerse pendiente a los avisos y notificaciones de su oficina

Prácticas Equivocadas

- No estar atento a los avisos de activación del plan de emergencia en su oficina
- Mantener objetos sueltos sobre escritorio u otra superficie expuesta donde se puedan convertir en proyectiles
- Dejar sin archivar documentos y medios electrónicos sobre su escritorio u otra superficie expuesta
- No cubrir computadoras y otro equipo informático con toldos plásticos para protegerlos contra inclemencias
- Dejar equipos electrónicos y documentos en el piso, cerca de ventanas o en áreas que se puedan inundar
- Dejar equipo electrónico conectado a receptáculos eléctricos y a la red