ISO
BOLETÍN

www.utrgv.edu/is

The University of Texas Rio Grande Valley™
Information Security Office

VOLUMEN I, PUBLICACIÓN III ENERO 19, 2017

DENTRO DE ESTA PUBLICACIÓN:

EDITOR
Francisco Tamez
ISO Security Analyst

¡Feliz Año Nuevo!

La Oficina de Seguridad de la Información (ISO) de UTRGV desea desearle a usted y a sus familias un Feliz Año Nuevo. Esperemos que una de sus nuevas resoluciones de año nuevo involucre la seguridad de la información en casa y en el trabajo, en el caso de que no ha agregado esto a su lista no se preocupe, todavía hay mucho tiempo.

La ISO también quiere compartir algunos consejos de seguridad y esperamos que los compartas con amigos y familiares.

Algunos recordatorios básicos de seguridad para ayudarle a iniciar el año:

1. ¡Cuidado con las estafas fiscales! El IRS vio una oleada aproximada del 400 por ciento en incidentes de phishing y malware en la temporada de impuestos 2016. (www.irs.gov/uac/tax-scams-consumer-alerts)
2. Respaldo de datos y Sistema: Asegúrese de hacer copias de seguridad de documentos importantes, fotos y videos irreemplazables. No deje que los fallos de hardware, malware o criptografía obtengan sus datos. Los servicios de sincronización en la nube como OneDrive y Dropbox no es una solución para respaldos adecuada.Sistema operativo: busque actualizaciones y elimine programas innecesarios.
3. Higiene para Computadoras: Compruebe mensualmente las actualizaciones del sistema operativo (SO) y de los programas. Elimine todos los programas y servicios que no sean compatibles o innecesarios.
4. Cambie sus contraseñas regularmente: las contraseñas de UTRGV deben cambiarse al menos anualmente, pero puede cambiarlas más a menudo si es necesario. ¡Siga este consejo para sus cuentas bancarias y de redes sociales!
5. Empieza a organizar tus contraseñas con un administrador de contraseñas. (p. ej.: https://www.lastpass.com/es) donde puedes recordar todas tus contraseñas de forma segura para que usted no tenga que hacerlo.
6. Asegure sus dispositivos móviles (como ordenadores portátiles y tabletas) al no dejarlos visibles en su automóvil, protegiendo con contraseña el acceso a ellos y asegurándolos físicamente cuando no estén atendidos.

AVISOS DE SEGURIDAD

Informe Viernes Negro y Cyber Monday 2016:
Viernes Negro y Cyber Monday 2016 informe
Los ingresos de comercio electrónico de EE. UU. Informaron que el Viernes Negro del 2016 fue el primer día donde se generaron "más de mil millones de dólares en ventas en línea de dispositivos móviles, según Adobe." El Cyber Monday también registró un aumento de 12.1 por ciento alcanzando un nuevo récord con "$ 3.45 mil millones gastados en línea" (bit.ly/2iLmW4p).

Está claro que esta tendencia continuará probablemente para el nuevo año y como el acontecimiento de las ventas ocurra todavía sigue está la posibilidad de ventas fraudulentas y de anuncios falsos.

A pesar de las amenazas en línea al educarnos a nosotros mismos, compartir consejos entre familiares y amigos podemos combinar nuestros esfuerzos para estar seguros en línea. Además, la ISO siempre compartirá con el público cualquier vulnerabilidad en línea y cualquier otro tema de interés para usted.

Yahoo segunda violación de seguridad
Sobre la base de un análisis más profundo de los datos por los expertos forenses, Yahoo cree que un tercero no autorizado, en agosto de 2013, robó datos asociados con más de un billón de cuentas de usuarios.

Yahoo está notificando a los usuarios potencialmente afectados por correo electrónico y publicando información adicional en el sitio web de Yahoo. Además, Yahoo está pidiendo a los usuarios potencialmente afectados que cambien rápidamente sus contraseñas y adopten medios alternos de verificación de cuentas. La Oficina de Seguridad de la Información de UTRGV (ISO) recomienda encarecidamente que cualquier usuario de Yahoo cambie rápidamente sus contraseñas, preguntas de seguridad y respuestas.

Para las cuentas potencialmente afectadas, la información robada puede incluir nombres, direcciones de correo electrónico, números de teléfono, fechas de nacimiento, contraseñas hash (usando MD5) y, en algunos casos, preguntas y respuestas encriptadas o sin cifrar. (bit.ly/utrgvisonews2YDB)

Pros y contras de tu identificación médica en la aplicación de salud de tu iPhone

Si dispone de la última versión de iOS para su iPhone, puede configurar un ID médico en la aplicación Health para acceder a información importante de su salud. La identificación médica ayuda a los primeros auxilios a acceder a la información médica crítica (por ejemplo, medicamentos, condiciones médicas y alergias), sin necesidad de su código de acceso. (apple.co/2jbf7l7).

¿Las preguntas aquí serían quién tiene realmente acceso a su información médica crítica? ¿Y qué otra información se almacena en esta aplicación? Las respuestas serían: personas de los primeros auxilios, los compañeros de trabajo curiosos, los miembros de la familia, o cualquier persona que tenga acceso físico a su iPhone durante 15 segundos, y "además, los números de teléfono y los nombres de sus contactos de emergencia y su relación con usted También se pueden acusar, lo que introduce el robo de identidad o las preocupaciones de phishing. Por lo tanto, tendrá que sopesar los riesgos y beneficios de tener esta información fácilmente accesible a través de su iPhone." ((bit.ly/2j4xmNy)

¿Que aguarda este Semestre?

ISA Entrenamientos

Con la ayuda de los departamentos académicos en UTRGV la ISO comenzará a encontrado a los administradores de seguridad informática (ISA por sus siglas en inglés). Los ISA actuarán como un conducto entre la ISO y todos los departamentos y facultades. Esto ayudará a construir vías de comunicación para asegurar que los empleados y la ISO son informados de temas y problemas que afectan la seguridad informática.

Enero es el mes de la conciencia sobre el acoso (NSAM)

En enero de 2004, el Centro Nacional para las Víctimas del Crimen lanzó (NSAM por sus siglas en inglés) para aumentar la conciencia sobre el acoso. NSAM surgió de la labor del Centro de Recursos de Acecho, un programa del Centro Nacional financiado por la Oficina de Violencia contra la Mujer, Departamento de Justicia de los Estados Unidos, para aumentar la conciencia sobre el acoso y ayudar a desarrollar e implementar respuestas multidisciplinarias al crimen.

En 2011, la Casa Blanca emitió la primera Proclamación Presidencial sobre el Mes Nacional de Concientización sobre el Acoso. La proclamación del Presidente Obama enfatizó los millones de personas afectadas por el crimen, sus consecuencias a menudo devastadoras, la dificultad de identificar e investigar el crimen y el firme compromiso del gobierno federal de combatir el acoso. (stalkingawarenessmonth.org)

Proyectos actuales de ISO

Nuestra oficina está trabajando en varios proyectos que mejorarán la gestión de activos y la vulnerabilidad de las computadoras en nuestra Universidad. La ISO está optimizando los métodos de descubrimiento de activos, inventario, la clasificación de los datos, y la prevención de pérdida de datos.

Solución de cifrado para Mac

La versión actualmente instalada de SecureDoc, la solución de administración de cifrado de UTRGV para Mac OSX, no es compatible con la última versión de OSX Sierra. IT está investigando una mejor solución para gestionar el cifrado OSX y la administración de estas Macs, incluyendo OSX e iOS.

Retiro de dominios UTB y UTPA

Las credenciales UTPA y UTB se retirarán este verano y ya no podrás iniciar sesión con estos dominios heredados. En el caso de que todavía usted está utilizando estas credenciales, póngase en contacto con el Centro de ayuda de IT.

Día de la privacidad de datos

Respetar la privacidad y proteger los datos es el tema del Día de la privacidad de datos (DPD), un esfuerzo internacional que se realiza anualmente el 28 de enero para crear conciencia sobre la importancia de la privacidad y proteger la información personal.

DPD es un evento en un esfuerzo más grande para generar conciencia acerca de la privacidad y seguridad. La Alianza Nacional de Seguridad Cibernética (NCSA por sus siglas en inglés) educa a los consumidores sobre cómo pueden ser propietarios de su presencia en línea. La campaña sobre la privacidad de NCSA es un componente integral de STOP.THINK.CONNECT .-la campaña global de seguridad, privacidad y seguridad en línea. (www.staysafeonline.org/data-privacy-day/about)

ISO

ISO destacó a: es una entrevista de un individuo que forma parte de UTRGV o un juega un rol en la seguridad informática. En este boletín, conoceras a Daniel Ramirez, quien es *Senior Information Security Analyst*.

Daniel Ramirez
Senior Information Security Analyst
The University of Texas Rio Grande Valley

1. Cuéntanos como la seguridad informática ha cambiado desde que empezó en su papel.
La seguridad está en todas partes porque el Internet está en donde sea. A medida que más personas y más cosas se conectan a Internet, la seguridad se vuelve cada vez más importante. Un hacker, a miles de kilómetros de distancia, podría conectarse a una cámara de seguridad accesible a Internet dentro de un edificio y usarlo para romper la seguridad y acceder a áreas restringidas. Esto podría ser el hogar de alguien o la red eléctrica de las naciones. Vivimos en una nueva era ahora.

2. ¿Quiénes son sus clientes, y cual es una de las áreas más difíciles para usted?
Mis clientes son los estudiantes, profesores y personal de UTRGV. Una de mis áreas más desafiantes es asegurar que cada uno de mis clientes tenga el conocimiento necesario para mantener tanto los recursos de información de UTRGV como los recursos de información personal seguros y protegidos.

3. ¿Cómo es que llegaste al campo de seguridad informática?
Crecí con una fascinación por las computadoras y la programación, antes del Internet. A medida que las computadoras comenzaron a conectarse a Internet, me intrigaron las tecnologías que se requerían para proteger las computadoras de las amenazas. Las amenazas aumentaron exponencialmente a lo largo de los años a medida que el mundo aprendía a hackear y esto cambió mi fascinación por la piratería ética y la ciberseguridad.

4. Los tres logros mas importantes en su vida:
Encontrar a mi esposa
Nacimiento de mis hijos
Conseguir una carrera en el campo de la seguridad informática

5. La gente se sorprendería saber que:
Me gusta trabajar con carpintería.

6. ¿Qué CD tiene usted en su coche? ¿O qué estación de radio te gusta escuchar?
Una mezcla de más de 100 canciones de rap y hip-hop de los años 80 hasta el nuevo siglo.

7. Si pudieras entrevistar a una persona (viva o muerta) ¿quién sería?
Mi tatarabuelo. Sería impresionante saber sobre mi historia ancestral.

8. ¿Si se les da la oportunidad, que le gustaría ser por un día?
Mi niño de 6 años , ver el mundo a través de sus ojos, ser un niño una vez más, y ver cómo estoy haciendo como un papá.

9. ¿Cuál es el mejor consejo que has recibido y que ha utilizado?
La vida es corta, disfruta cada minuto de ella.

10. ¿Cuál sería su consejo para un nuevo profesional en la seguridad informática?
¡No lo hagas! LOL. No, con toda seriedad la seguridad es un gran campo, pero es muy dinámico. A medida que las tecnologías cambian, también lo hacen las amenazas potenciales y los profesionales de la seguridad necesitan estar siem-

Artículo destacado

Por Cesar Pastore
UTRGV Information Security Analyst

Proteger sus datos en su USB

Tal y como los USB se vuelven más económicos al mismo tiempo incrementan en almacenamiento, se han convertido en un elemento popular para comprar durante la temporada de vacaciones. Similarmente, durante los últimos años, los usuarios se han vuelto más precavidos en la seguridad de la información almacenada en sus dispositivos USB. Este cambio en la mentalidad puede ser impulsado por diferentes factores, incluyendo requisitos relacionados con el trabajo o experiencia personal con la pérdida de uno de estos dispositivos personales. Para los usuarios que buscan asegurar su dispositivo USB hay una serie de opciones disponibles para incluir la seguridad en los USB. Incluso la unidad USB sin protección puede protegerse adecuadamente tomando las medidas adecuadas para cifrar el contenido de la unidad. Al igual que cualquier otro producto, las opciones varían en la funcionalidad de la seguridad dependiendo del tipo de USB disponible para los usuarios basándose en factores simples como precio, capacidad de almacenamiento y facilidad de uso. En este breve artículo cubriré tres niveles generales de seguridad para USB, incluida la autenticación de PIN incorporada, la autenticación basada en software incorporada y, finalmente, la codificación basada en software de otra compañía.

El método preferido para el cifrado y la protección por contraseña es el cifrado basado en hardware con un teclado de seguridad incorporado. Estos dispositivos son normalmente los más caros en el mercado debido a su alto nivel de seguridad y compatibilidad entre plataformas. Estos dispositivos pueden ejecutarse en sistemas operativos como Windows, Mac o cualquier otro. Estos USB requieren el desbloqueo de la llave USB con un PIN de seguridad programable antes de que se pueda acceder a los datos almacenados. Un ejemplo de uno de estos dispositivos sería Apricorn Aegis USB. La desventaja de estos dispositivos de unidad flash USB es el mayor precio de la unidad en comparación con las unidades con cifrado simple. Esta diferenciación de precios se hace más pronunciada a medida que aumenta la capacidad de la unidad flash USB.

El segundo conjunto de dispositivos ofrece un nivel equivalente de cifrado basado en hardware, pero lo hace a un costo menor, especialmente para dispositivos con capacidades de almacenamiento más altas. Estas unidades USB no proporcionan ningún teclado visible y, en su lugar, deben estar conectadas a una computadora compatible para poder introducir una contraseña y desbloquear la unidad. La principal diferencia entre estos dispositivos es que el USB debe estar conectado a un PC / Mac compatible para que el programa de autenticación de contraseña ejecute y valide la contraseña correcta. Estos dispositivos tienden a ser más bajos en el precio, sin embargo, pueden no ser tan compatibles. Algunos ejemplos de este tipo de unidades USB incluyen el Kingston Digital Data Traveler o el Integral Crypto Drive.

Por último, si se encuentra en posesión de una unidad flash USB sin funciones de seguridad incorporadas, el cifrado y la protección por contraseña todavía se pueden obtener a través de la funcionalidad basada en un sistema operativo o software de aplicación por medio de otra compañía. Dependiendo del tipo de sistema operativo que esté ejecutando, es posible que pueda utilizar la funcionalidad de cifrado incorporada proporcionada por Microsoft o Apple. Microsoft utiliza bitlocker para su cifrado de unidad y Apple utiliza FileVault. El principal inconveniente de estas herramientas es que está restringido a usar un sistema basado en Windows o Mac. Una vez que los datos han sido cifrados la unidad no es compatible con ningún otro sistema operativo. La ventaja es que estas aplicaciones de cifrado no tienen costo adicional, siempre y cuando tengas una versión de Microsoft o Mac OS que soporte la funcionalidad. Por último, si no tiene soporte de cifrado basado en sistema operativo como bitlocker o FileVault, hay una serie de otras compañías que, con un cargo por licencias, ofrecerán protección de cifrado basada en software para sus unidades USB.

Estos tres niveles generales de cifrado para USB que he cubierto brevemente deberían dar a los usuarios una idea general de los diferentes niveles de seguridad para USB actualmente disponibles. Dadas las diferentes opciones para proteger los datos en los USB en caso de pérdida o robo, es más fácil que nunca cifrar su unidad USB y estar seguro de que sus datos están protegidos y seguros.

ISO - Invitado

THE UNIVERSITY OF TEXAS RIO GRANDE VALLEY

Departamento de Policía

Acerca del Departamento:

Protege y sirve a la comunidad universitaria de estudiantes, profesores, personal y visitantes en toda la región del Valle del Río Grande, proporcionando servicios profesionales de aplicación de la ley y promoviendo activamente la participación de la comunidad a través de estrategias progresivas de asociación policial comunitaria y un compromiso con la educación. Estamos abiertos las 24 horas del día, los 7 días de la semana.

¡Información importante sobre seguridad personal!

RESPUESTA CIVIL A UN TIROTEO

¿Estás preparado? La posibilidad de estar involucrado en un tiroteo es una amenaza de alto riesgo. Este taller proporciona los conocimientos, habilidades y actitudes requeridos para respuestas efectivas a tales amenazas. Te enseñaremos qué hacer y cómo responder de manera segura y decisiva si estás atrapado en el fuego cruzado.

¡Fechas del entrenamiento se anunciarán pronto! Para más información contactar al Oficial Antonio Zarzoza, 956 665-2988.

¿Algunas maneras en que te podemos ayudar?

Escolta con Policía

Las escoltas con la policía a los vehículos, dormitorios en el campus se encuentran disponibles 24/7 para los estudiantes, profesores y el personal.

Asistencia para un vehículo:

La Policía de la Universidad tiene unidades especialmente equipadas para pasar corriente y ayudarte a abrir un vehículo. Un Permiso de Estacionamiento UTRGV válido te da derecho a estos servicios, llámenos al 956-665-7151 o al 956 882-8232. Estamos abiertos 24/7 los 365 días del año.

¿Algunas otras maneras en que UTRGV PD te puede ayudar?

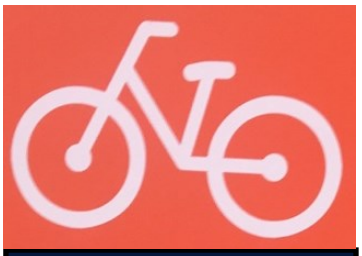
Información para cosas perdidas y encontradas:

Si ha perdido algo, infórmelo utilizando nuestra forma de cosas perdidas y encontradas. (www.utrgv.edu/police/services/lost-and-found)Usted puede reportar artículos perdidos por teléfono, pero recibirá **una respuesta más rápida reportándolo en línea**. Por favor, incluya cada detalle al describir el artículo que ha perdido para poder identificar el objeto. Los detalles útiles son: marca, color, tamaño, forma, número de modelo, cantidad, material (cuero, plástico, tela, metal, etc.), tamaño, características especiales,

Información útil

Prevención del robo de bicicletas

- Registra tu bicicleta con la Oficina de Estacionamiento y Transporte, 665-2738 (Edinburg) o 882-7051 (Brownsville)
- Mantenga las bicicletas con llave en cualquier momento que estén desatendidas con una buena cerradura tipo "U". La segunda opción sería un buen candado y cable. Asegúrese de que el candado o el cable "U" atraviesa la rueda delantera y el bastidor o la rueda trasera y el bastidor, y asegúrelo a un objeto fijo.
- Compruebe que está bien cerrado jalando del candado para asegurarse de que está bien seguro.
- Utilice un grabador para colocar una marca de identificación en los componentes principales sin pintar de la bicicleta.
- Durante el día en casa, mantenga la bicicleta fuera de vista, o al menos en la parte trasera de la casa.
- Por la noche y cuando no esté en casa, mantenga la bicicleta dentro de una estructura cerrada.
- Asegúrese de conservar todas las pruebas de compra incluyendo el número de serie.
- Ser capaz de identificar la bicicleta ... no sólo por su color, sino por sus características.
- Ten una o más fotografías a color de la bicicleta y de su dueño a mano.
- Nunca preste una bicicleta a extraños.
- Trate de evitar estacionarla en áreas desiertas o mal iluminadas.



Operación ID
Para la seguridad de su bicicleta una calcomanía de la bicicleta se requiere en su bicicleta (GRATIS). Estacione sólo en ubicaciones de bicis disponibles. Para obtener más información, póngase en contacto con el Departamento de Policía de UTRGV (956) 665-7151

Contáctos de UTRGV PD

Edinburg Campus

Ayuda En Campus : 4357
Emergencia En Campus : 911
Despacho y emergencia: (956) 665-7151

Estación de policía
Academic Services Facility Bldg.
501 N. Sugar Road
Edinburg TX 78539

Harlingen Campus

Despacho y emergencia: (956) 882-8232

Estación de policía
2102 Treasure Hills Blvd.
Harlingen, TX 78550

Brownsville Campus

Despacho : (956) 882-8232
Emergencia: (956) 882-2222

Estación de policía
One W. University Boulevard
Brownsville, TX 78520

Email: police@utrgv.edu

Web: www.utrgv.edu/police

Facebook: www.facebook.com/UTRGVPoliceDepartment

Twitter: www.twitter.com/utrgvpolice


DON'T
GET
SMACked
Check your
Social Media
Access Controls
utrgv.edu/is/en-us/
resources/social-media


WE
ARE
SOCIAL!
www.utrgv.edu/is
www.facebook.com/utrgviso

ARTÍCULOS DE SEGURIDAD INFORMÁTICA

La FDA emite una guía final para la seguridad de dispositivos médicos.
Con toda la preocupación actual de que el IOT (por sus siglas en inglés) sea inseguro debido a ataques cibernéticos, la Administración de Alimentos y Medicamentos de los Estados Unidos (FDA, por sus siglas en inglés) ha publicado la guía final de la agencia para la seguridad de dispositivos médicos. (bit.ly/2j8tGwE)

La FDA confirmó que los dispositivos cardíacos de St. Jude Medical tienen vulnerabilidades.
Esto podría permitir a un hacker acceder a un dispositivo. Una vez adentro, podrían agotar la batería o administrar cargas eléctricas, la FDA comento.
(bit.ly/2jvlU0f)

La universidad de Los Angeles paga $ 28,000 en ransomware.
(Los Ángeles Valley College en Valley Glen pagaron 28.000 dólares en bitcoins a los hackers, que habían utilizado software malicioso para obtener una variedad de sistemas, incluyendo computadoras importantes y correos electrónicos. bit.ly/2j5Afjj)

Ransomware - restaurar sus archivos de la manera desagradable
Los hackers están robando los archivos informáticos de las personas y sólo los devuelven si pagan dinero o aceptan infectar a otros dos usuarios con el virus. (cnb.cx/2ikI8QM)

Si necesitas reportar un incidente:

Visite nuestro sitio web (www.utrgv.edu/is) si necesita reportar un incidente de seguridad . Algunos incidentes pueden requerir informar tanto a la ISO y al Departamento de Policía de UTRGV (PD) o de tecnología de la información (IT) . Por ejemplo, cualquier pérdida o robo de una computadora de propiedad de la Universidad (ej. estación de trabajo, ordenador portátil, celular, tableta) tiene que ser reportado a la ISO y a UTRGV PD. Del mismo modo, en caso de computadoras infectadas con ransomware deben de ser reportadas a ISO y a IT.

REPORTA UN INCIDENTE

The University of Texas Rio Grande Valley™

Information Security Office

La misión de la Oficina de la Seguridad Informática es proporcionar apoyo a la Universidad en la logro de sus objetivos, garantizando la seguridad, integridad, confidencialidad y disponibilidad de los recursos de información.

Locations:
Sugar Road Annex (ESRAX) Building
R –167 Rusteberg Hall (BRUST) Building (*by appointment*)

Phone: (956)665-7823
Email: is@utrgv.edu

Visitanos en la web y en las redes sociales!
www.utrgv.edu/is www.facebook.com/utrgviso

Servicios que proporcionamos:

CONCIENCIA, RIESGO Y CUMPLIMIENTO

ACTIVOS Y ADMINISTRACIÓN DE LAS VULNERABILIDADES

INGENIERÍA Y RESPUESTA A INCIDENTS

CONCIENCIA, COMUNICACIÓN Y DIFUSIÓN

¡Danos tu opinion!
bit.ly/utrgvisonewsletterfeedback