ISO
BOLETÍN

www.utrgv.edu/is

The University of Texas Rio Grande Valley™
Information Security Office

VOLUMEN I, PUBLICACIÓN II NOVIEMBRE 23, 2016

DENTRO DE ESTA PUBLICACIÓN:

EDITOR
Francisco Tamez
ISO Security Analyst

¡Felices fiestas!

La Oficina de la Seguridad Informática (ISO por sus siglas en inglés) le gustaría desearte unas felices dietas. En el mes de Noviembre nos preparamos para comprar en aquellas tiendas con descuentos especiales for las fechas navideñas o también planeamos para visitar a nuestros seres queridos. A nosotros nos gustaría agradecerles por su apoyo, por leer este boletín, y por tomar un interés en seguridad informática.

A la ISO le gustaría compartir unas cuantas recomendaciones acerca de la seguridad informática y ojalá y los compartas con tus amigos y familiares.

1. Cuando estés comprando en línea asegúrate de tener la "s" en https:// por el hecho de que estos sitios toman medidas de seguridad mayores. Te puede proteger de muchas maneras de vigilancia y pirateo de tus cuentas, y algunas formas de censura.
2. Comparte con cuidado y no compartas tu localización en las redes sociales. Esto les dice a los ladrones que no te encuentras en casa. Visita nuestra campana de Controles de Acceso en las Redes Sociales (SMACked por sus siglas en inglés) (bit.ly/2fTPJSc) para aprender más de la privacidad en las redes sociales.
3. Para. Piensa. Conéctate. No conduzcas actividades sensibles como comprar en línea, ver tus cuentas bancarias, o trabajo clasificado utilizando a red Wi-Fi pública. (http://bit.ly/29ciR9h)
4. 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.
5. Actualiza tus información bancaria y contraseña, también pregúntale a tu banco si ellos ofrecen autentificación de dos factores para poder agregar mas seguridad a tu cuenta

ANUNCIOS

EOL Software

Las aplicaciones de software tienen un ciclo de vida. El ciclo de vida comienza cuando el software es anunciado y concluye cuando ya no es soportado por el proveedor, también llamado fin de vida (EOL por sus siglas en inglés). Cuando el software deja de ser apoyado por el proveedor, instantáneamente deja de recibir actualizaciones que permite mantener el software seguro.

EOL OS

Windows XP y Apple OSX 10.6 y versiones anteriores son consideradas EOL. Si actualmente está utilizando un sistema operativo EOL, debería actualizar su sistema operativo para mantener la seguridad de su equipo y sus datos. Ordenadores en propiedad, arrendados o gestionados por UTRGV deben cumplir con la Norma de Seguridad Informática, el cual requiere que se ejecuten solamente sistemas operativos que sean apoyados por el proveedor. Windows Vista será EOL en abril de 2017, planeé actualizar este sistema operativo pronto.

QuickTime EOL

Apple anunció que ya no lanzará soporte para QuickTime para Windows. Las computadoras con el sistema operativo de Windows y que están utilizando QuickTime pueden ser vulnerables al malware. ISO recomienda que todos los usuarios de Windows desinstalen QuickTime.

UTRGV Computer Domain Migration Project Update

This project entails transitioning all University computer from the legacy domains to the UTRGV domain.

- Si tu computadora está pendiente, por favor repuesta la migración a través de ServiceNow para agenda una cita. Cuando estés pidiendo el servicio, por favor asegúrate de incluir la siguiente información:
- Tu Correo electrónico de UTRGV
- El número de etiqueta de tu computadora
- Tu localización
- Teléfono
- Hora y fecha de cuando estés disponible para que IT te pueda contactar

Contacta a IT para cualquier problema técnico

956-665-2020 (Edinburg)

956-882-2020 (Brownsville/ Harlingen)

Office 365: característica de prevención de pérdida de datos (DLP por sus siglas en ingles) de seguridad y cumplimiento

El 15 de Noviembre, se implementó una nueva característica de seguridad para mejorar los esfuerzos de prevención de pérdida de datos (DLP) en UTRGV. Esta característica de seguridad proporciona iconos de archivos de advertencia y notificaciones por correo electrónico cuando se comparte información personal como números de tarjeta de crédito y / o números de seguro social a través de OneDrive, Office 365 o correo electrónico.
Los archivos no se leen pero se analizan para ver si los datos coinciden con el número de seguro social y / o los patrones de números de tarjeta de crédito. Esto no ocurre inmediatamente. El tiempo necesario para que aparezcan los iconos de advertencia y las notificaciones por correo electrónico que se reciben varían ya que OneDrive, SharePoint y el correo electrónico están alojados fuera de Microsoft.

Productos actuales con EOL

Considere la posibilidad de actualizar si utiliza los siguientes productos con estas versiones o con anteriores.

Producto	Versión	Producto	Versión
Adobe Acrobat X	10	Adobe Flash Player	19
Adobe Reader	9.x	Java SE	5
Adobe Flash Media	4.5		

¿Que fue lo que te perdesite?

Octubre NCSAM

Octubre fue el Mes Nacional de Concientización sobre Seguridad Cibernética (NCSAM por sus siglas en inglés), administrado por el Departamento de Seguridad Nacional.

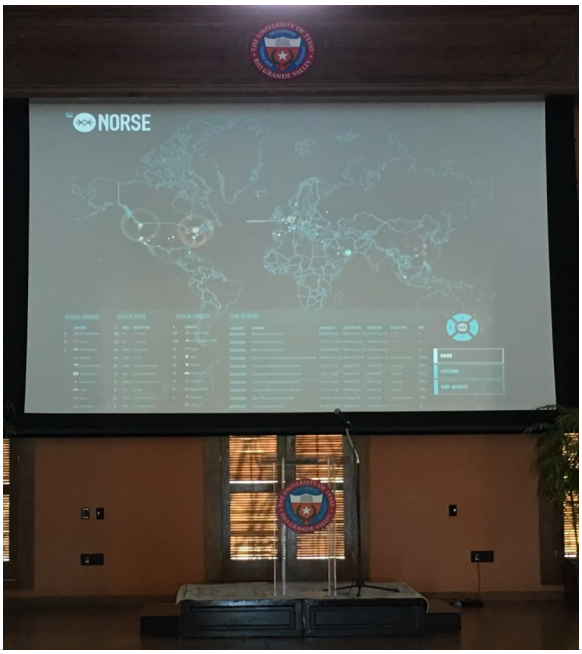
A lo largo del mes de Octubre, la ISO discutió varios temas de seguridad cibernética tales como el uso de malware por delincuentes en línea, robo de propiedad intelectual, fraude de Internet, fraude de identidad, acoso cibernético y más. Nuestra oficina proporcionó consejos cibernéticos semanales en Octubre a través de nuestro Blog de Noticias y las redes sociales.

Exposición de seguridad informática.

El 11 de octubre la ISO llevó a cabo la primera Expo de Seguridad Cibernética en el campus de Edinburg en el ballroom. Más de 110 estudiantes, profesores y personal de UTRGV asistieron al evento.

De manera similar, la ISO llevó a cabo la primera Expo de Seguridad Cibernética en el Campus de Brownsville en Plains Capital El Gran Salón el 31 de Octubre.

Más de 70 estudiantes de UTRGV, profesores y personal asistieron a este evento, 13 estudiantes del Instituto Tecnológico De Matamoros pudieron participar también en la Expo.



¿Que esperar para el siguiente año?

ISA Entrenamientos

La ISO comenzará a buscar a los administradores de seguridad informática (ISA por sus siglas en inglés) para cada departamento. 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.

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.

¿Planeas salir de vacaciones?

Si usted está planeando en sus vacaciones de invierno y no va a utilizar su computadora de oficina, entonces no se olvide de apagarla. ¡Al dejar su computadora apagada usted está protegiendo su información y usted está ahorrando energía al mismo tiempo!

¡Las compras en línea de los días festivos están aquí!

Ser más seguro y más seguro, mientras que las compras en línea es una alta prioridad durante la temporada de vacaciones, un momento clave para la compra de regalos en línea. El Lunes Cibernético de este año -que cae el 28 de noviembre- se prevé que será el mayor y el más activo de todos los tiempos, generando $ 3,36 mil millones en ventas con un crecimiento de 9,4 por ciento comparado con el 2015.
Read more: bit.ly/2fi50wu

Nuevo equipo, smartphone o tableta?

Tenga en cuenta los siguientes consejos ISO:

- Actualice su dispositivo y active la actualización automática.
- Preste atención al configurar su nuevo dispositivo por primera vez, especialmente las opciones de privacidad
- Tenga cuidado con las aplicaciones o características que permite sincronizar.
- Trate de entender qué información personal recoge el dispositivo, cómo se utiliza y cómo se almacena.
- Mantenga actualizado su antivirus.
- Cambie la contraseña en el dispositivo antes de usarlo.

Las contraseñas son como ...

- **Enigmas:** Debe ser difícil para los demás adivinar.
- **Frases:** Mientras más largas mejor.
- **Cepillo de dientes:** Utilice contraseñas diferentes para cada cuenta.
- **Ropa interior:** Nunca comparta su contraseña con otras personas.

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, tú vas a conocer a Dr. Jeffery A. Graham, quien es Chief Information Officer en UTRGV.

Dr. Jeffery A. Graham

Chief Information Officer
The University of Texas Rio Grande Valley

1. **¿Quiénes son sus clientes, y cuál es una de las áreas más difíciles para usted?**
   Facultad, estudiantes, personal y visitantes. Crea un desafío para darles servicios omnipresentes que esperan cuando cada uno tiene diferentes necesidades y habilidades.

2. **¿Qué te gusta más de tu trabajo?**
   La posibilidad de resolver los problemas, mientras más difícil más satisfecho me siento.

3. **Cuéntanos cómo ha cambiado la seguridad de la información desde que empezaste en tu rol.**
   La importancia de la seguridad de la información es mucho más reconocida y tomada más en serio al mismo tiempo que la complejidad de los ataques ha aumentado.

4. **¿Cuáles son los mejores momentos de su vida:**
   - Mi matrimonio con Rosario
   - El nacimiento de mis 3 hijas
   - Y mudarme al valle en 1988, ya que nada de eso hubiera sido posible si no hubiera tomado esa oportunidad

5. **La gente se sorprendería de saber:**
   Que me case en México y que aún no había aprendido español, así que no entendí la mayor parte de lo que sucedió en la ceremonia :J

6. **¿Qué CD tienes en tu auto? ¿O qué estación de radio escuchas?**
   La banda A de mi radio está configurada para escanear los repetidores locales y la Banda B escanea las frecuencias locales de control de Tránsito Aéreo.

7. **Si pudieras entrevistar a una persona (viva o muerta), ¿Quién sería?**
   Steven Hawkins, estoy fascinado con la astrofísica, la física cuántica, la relatividad, etc. Yo no entendería la conversación pero lo disfrutaría.

8. **Si se le da una oportunidad, ¿A quién le gustaría ser por un día?**
   Uno de los astronautas lunares, cuando yo era niño siempre asumí que un día caminaría sobre la Luna.

9. **¿Cuál es el mejor consejo que ha recibido y que ha utilizado?**
   Vestirse y actuar para el trabajo que deseas, no el trabajo que tienes.

10. **¿Cuál es una cosa con la que no podrías vivir?**
    Mi taza de café.

11. **¿Cuál sería su consejo para un nuevo profesional de IT?**
    La tecnología cambia muy rápidamente y si necesita seguir aprendiendo siempre habrá muchas oportunidades.

Asociación estudiantil sobresaliente

En este espacio podrás conocer a una asociación estudiantil sobresaliente que forma parte de UTRGV. En este boletín, conocerás a la Asociación de Profesionales en Tecnología de la Información.

Asociación de Profesionales en Tecnología de la Información

Asociación de Profesionales en Tecnología de la Información es una organización que se compromete a proporcionar a sus miembros con experiencia que mejorará sus carreras académicas y profesionales; Con actividades tales como participación comunitaria, capacitación práctica y competiciones. Como organización aquí en la Universidad de Texas - Rio Grande Valley, proporcionamos a nuestros miembros temas de discusión durante nuestras juntas generales para informarles sobre los temas más comunes e interesantes relacionados con nuestra carrera como análisis de protocolos, exploración de puertos, hacking de google , Eliminación de malware y líneas de comandos.

Visite nuestro Facebook para contactarnos (http://bit.ly/2g3TzZT)
Todas las carreras son bienvenidas a unirse.

Protégete a ti mismo

Por: AITP

Al entrar en la universidad, es un mundo completamente nuevo, lleno de emoción y peligro ... a través de Internet. Como estudiantes universitarios vamos a Starbucks o cualquier lugar donde hay Wi-Fi gratituo para hacer tareas, proyectos, leer o navegar por Internet. Sin embargo, la mayoría de nosotros no somos conscientes de los riesgos que atravesamos al conectarnos a redes públicas. Las exposiciones que pueden afectarte son robo, fraude, acecho y / o acoso, estos son clasificados como riesgos principales que pueden dañarte en todos los aspectos de tu vida. Es importante tener en cuenta los peligros que pueden ocurrir al navegar por la web. ¡Aquí están algunas cosas que hacer y qué no hacer que pueden ayudarte a mantenerte a salvo!

Hacer	No Hacer
Fuertes c0nTr@seña$	Descargar medios gratuitos
Obtenga protección contra virus y programas espías	Almacenar en línea tu información de pago
Consiga un bloqueadpr de ventanas emergentes	Compartir excesivamente tu información personal
Monitoreo de cuentas	Hacer clic en ligas (links) desconocidos
Respaldos	Compartir tu cuenta bancaria
	Compartir tu número de seguro social

Articulo destacado

Por: UTRGV CISO Thomas Owen

Con la explosión en las nuevas plataformas de comunicación, los piratas informáticos se están moviendo rápidamente para capitalizar en todas las formas posibles. Mientras que Facebook, MySpace, Twitter y otros sitios de redes sociales / blogging solían ser el dominio de Generación Y, la tendencia es ahora para personas de todas las edades a utilizar estos sitios para mantenerse en contacto y difundir información. Sin embargo, el problema es que nunca se sabe exactamente qué información se está difundiendo y a quién.

Por ejemplo, considere el caso de dos empleados de una gran firma financiera estadounidense que hizo noticias hace unos meses. Por simplicidad, los llamaremos Jack y Jill. Ambos tenían cuentas de Facebook, eran amigos de Facebook, y a veces se comunicaban fuera del trabajo. Suena como una amistad inocente, ¿verdad? Fue, hasta que los hackers fueron capaces de tomar el control de la cuenta de Facebook de Jack. Los hackers le enviaron a Jill un simple mensaje: "Mira las fotos que tomé de nosotros en el picnic de la compañía". Jill hizo clic en el enlace, esperando ver fotos del picnic. En su lugar, descargó software malicioso, permitiendo a que los hackers tomaran el control de la computadora portátil de su empresa. Estoy seguro de que usted puede ver a dónde se dirige: Los atacantes fueron capaces de utilizar sus credenciales para acceder a la red de la empresa. El incumplimiento pasó desapercibido por aproximadamente dos semanas.

Este ejemplo ilustra cómo el crecimiento de los medios de comunicación social, junto con la falta de conciencia entre los empleados y los empleadores con respecto al uso personal y potencial del negocio, puede aumentar la reputación de una institución, la responsabilidad y las exposiciones al riesgo operacional. Este aumento se puede atribuir a la institución que tiene una presencia de redes sociales para llegar a los clientes, a los empleados que acceden a los sitios de redes sociales en el trabajo y a los empleados que acceden a los sitios de redes sociales en las computadoras de su trabajo que se encuentran en el hogar.

¿Cómo pueden las organizaciones gestionar este riesgo?

Tratar a los medios de redes sociales como cualquier otro tipo de riesgo: Incluir las redes sociales en un proceso formal de evaluación de riesgos. Esta evaluación del riesgo debe ayudar a medir el nivel de riesgo, identificar los controles existentes, evaluar la necesidad de controles adicionales y, en última instancia, ayudar al banco a determinar su enfoque para el uso de las redes sociales por los empleados. Todas las decisiones deben basarse en este proceso basado en el riesgo.

¿Qué tipos de controles están disponibles?

Los controles varían según la organización, pero algunos ejemplos incluyen restricciones técnicas, incluyendo a las redes sociales en la Política de Uso Aceptable (AUP por sus siglas en inglés) o como una política específica, y el entrenamiento de concentimiento de seguridad para los empleados.

Los controles técnicos suelen proporcionar la mayor (pero a veces una falsa) tranquilidad. Los dispositivos de hardware o el software se pueden utilizar para filtrar sitios web por dirección web, contenido o categoría. Las organizaciones también pueden configurar un servidor proxy para obligar a los usuarios a través de un proceso de filtrado, incluso cuando los usuarios están físicamente fuera del sitio.

Identificar el uso de las redes sociales en el AUP o en una política específica ayudará a las organizaciones a proporcionar pautas para los empleados y a mitigar los riesgos, especialmente el riesgo de reputación. El marco de políticas debe abordar si las redes sociales pueden usarse en sistemas controlados por la organización (tanto en el trabajo como en el hogar) y qué información se le permite a un empleado divulgar con respecto a la organización y las actividades organizacionales.

El entrenamiento de concentimiento de seguridad para los empleados con respect a las redes sociales es un proceso en curso. No es adecuado esperar que los usuarios se siente en una sala por 8 horas una vez al año y retener ese conocimiento hasta el próximo entrenamiento anual. Carteles, notas y correos electrónicos con respecto a la evolución de las redes sociales pueden servir como recordatorios para ser vigilantes tanto en el lugar de trabajo y en casa. Si hay un brote de virus en sitios frecuentemente visitados (como el gusano Koobface en Facebook), utilice la ocasión para informar a los empleados sobre los peligros.

ARTÍCULOS DE SEGURIDAD INFORMÁTICA

Exposición seguridad informática
Al hablar de seguridad informática no nos referimos en exclusividad al tema de virusy spam, sino que vamos más allá, son muchos otros los factores a tener en cuenta. bit.ly/2fECX9W

Wi-Fi gratuito: ¿Que tan seguro es?
De acuerdo con una encuesta de Kaspersky Lab de viajeros de negocios internacionales, tres de cada cuatro personas se conectan a los servicios gratuitos de Wi-Fi en el extranjero, y el 82% de los viajeros se conectan a redes gratuitas, pero inseguras en lugares públicos como aeropuertos, cafeterías y hoteles. Por desgracia, esta práctica común puede poner en riesgo a los viajeros: la encuesta también indica que el 30% de los directivos de empresas han sido el blanco de la delincuencia informática cuando viajan al extranjero. bit.ly/2flMhwu

Un software chino espía 700 millones de «smartphones»
La firma de seguridad Kryptowire descubre una puerta trasera en miles de dispositivos móviles que transfiere información personal de los usuarios a servidors chinos. bit.ly/2f3Od2F

Estos y otros artículos se pueden encontrar en: http://www.utrgv.edu/is/es-es/noticies-y-alertas/index.htm

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.

1201 W. University Drive
Sugar Road Annex (ESRAX) Building
Edinburg, TX 78539

Phone: (956)665-7823
Fax: (956)665-3154
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