THE SHIELD

AGOSTO 28, 2017

VOLUMEN II, PUBLICACIÓN I

The University of Texas Rio Grande Valley

Information Security Office

¡Bienvenido!

La Oficina de Seguridad Informática (ISO) de UTRGV se enorgullece de presentar la nueva imagen y el nuevo nombre de nuestro boletín informativo. Este boletín se esforzará por mantenerle informado sobre noticias importantes de seguridad y temas que le ayudarán a mantenerse seguro tanto en el trabajo (para los empleados), en la escuela (para los estudiantes), como en casa (para todos). Sus comentarios, ideas y críticas son bienvenidos para asegurar que este boletín sirvira a la comunidad UTRGV de la mejor manera posible. ¡Bienvenido al otoño del 2017 y al inicio de otro gran año académico!

Algunos recordatorios básicos de seguridad para ayudarle a comenzar el nuevo semestre de otoño:

- Compruebe su correo electrónico de UTRGV - hoy en día la mayoría de los profesores y compañeros de clase se comunicarán por correo electrónico. Los empleados de UTRGV deben usar su correo electrónico de UTRGV para conducir negocios universitarios oficiales.
- No sea Phished — Tenga cuidado al hacer clic en los enlaces de correo electrónico y al descargar archivos adjuntos de correos electrónicos sospechosos; recuerde colocar siempre su ratón sobre la liga o link, esta técnica revelará el link verdadero. Si no está esperando un correo electrónico o si simplemente no se ve bien, no haga clic en ningún vínculo o archivo adjunto! Podría ser un intento de phishing. Para más información no dude en visitar nuestro sitio web: www.utrgv.edu/is/en-us/resources/training/phishing-page
- Actualice sus dispositivos — Verifique que los parches más recientes estén instalados. Asegúrese de que su sistema operativo (OS) está actualizado, así como las aplicaciones que ha instalado, especialmente Adobe, los navegadores web (IE, Edge, Safari, Chrome, Firefox, etc.) y los productos de Microsoft Office (Word, Excel, etc).
- Copia de seguridad: empiece a proteger su valioso trabajo y otra información digital haciendo una copia electrónica en One Drive for Business. One Drive for Business es un servicio gratuito de almacenamiento en la nube proporcionado por UTRGV a estudiantes y empleados, puede confiar en 1 Terabyte (TB) de almacenamiento en la nube.
- Conéctate con cuidado - Cuando compras en línea, comprueba que el sitio tenga seguridad habilitada. Busque direcciones web con "https: //", lo que significa que el sitio toma medidas adicionales para ayudar a proteger su información.

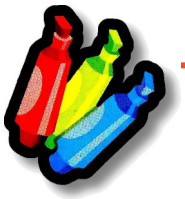
DENTRO DE ESTA PUBLICACIÓN:

EDITOR

Francisco Tamez

Security Analyst

www.utrgv.edu/is



AVISOS DE SEGURIDAD

NCSAM

Octubre es el mes nacional de concientización sobre seguridad cibernética (NCSAM por sus siglas en ingles), administrado por el Departamento de Seguridad Nacional. NCSAM se creó como un esfuerzo de colaboración entre el gobierno y la industria para garantizar que cada estadounidense tiene los recursos que necesitan para mantenerse más seguro y más seguro en línea.

NCSAM 2017 también marca el 7 ° aniversario de la STOP. THNK. CONNECT. ™. Cada año, NCSAM destaca el mensaje general de STOP. THINK. CONNECT ™ y los conceptos básicos de la campaña, como "Mantenga una máquina limpia", "Proteja su información personal", "Conéctese con cuidado", "Sea Web Wise", "Sea un buen ciudadano en línea".

Advertencia de fraude en ingeniería social

Una organización estatal utiliza SpawGlass como para proyectos de construcción. En junio, alguien registró un dominio spawglasscontractors.com y envió correos electrónicos a la oficina de negocios y, finalmente, ingeniería social para cambiar el número de enrutamiento bancario a otra cuenta. Enviaron grandes pagos a esta otra cuenta y no se dieron cuenta de que era fraudulenta hasta que el verdadero SpawGlass se puso en contacto con ellos para sus pagos.

Este es uno de varios incidentes en los últimos meses que involucran el cambio de números de enrutamiento bancario. Por favor, haga que sus oficinas de negocios sean conscientes de esto para que ninguna otra organización sea víctima de esta hazaña, y que tenga buenos controles para cambiar estos números.

Fecha de desactivación permanente para legado (UTPA / UTB) Conjunto de reenvío de correo electrónico para el 31 de Agosto de 2017

ATENCIÓN TODOS LOS TRABAJADORES LEGADOS:
El 31 de agosto de 2017, el reenvío de correo electrónico de las cuentas UTPA / UTB (legacy) se desactivará permanentemente. Actualmente, los mensajes de correo electrónico enviados a las cuentas UTPA / UTB se envían a las cuentas de correo electrónico de UTRGV. Los mensajes reenviados se indican mediante el uso de su dirección de correo electrónico heredada en la sección "Para" del mensaje. También incluyen una nota en la línea de asunto y la nota de abajo en el cuerpo del mensaje indicando que fue reenviada de UTPA / UTB.
**** Reenvío de correo electrónico desde UTPA / UTB ****
Por favor, lea el mensaje a continuación:
El reenvío de correo electrónico de las cuentas UTPA / UTB (legadas) a las cuentas UTRGV se desactivará permanentemente el 31 de agosto de 2017. Por favor, actúe ahora e infórmele a sus contactos que siguen utilizando su correo electrónico heredado para usar su dirección de correo electrónico UTRGV. Recibirá amplias notificaciones antes de la fecha de desactivación permanente del 31 de agosto de 2017. Sin embargo, le recomendamos que tome medidas ahora e informe a sus contactos que todavía utilizan su correo electrónico heredado para usar su dirección de correo electrónico de UTRGV.

Si tiene alguna pregunta o necesita asistencia técnica, póngase en contacto con la oficina de servicios de IT.
Brownsville / Harlingen / South Padre Island
956-882-2020
Main 1.212 (Brownsville)
Edinburg / McAllen / Rio Grande City
956-665-2020
Academic Services Building 1.102

Cybersecurity Expo 2017

¡Realizaremos nuestra segunda Exposición de Ciberseguridad en el campus de Brownsville y Edinburg!
A lo largo del mes de octubre, la ISO discutirá varios temas de seguridad cibernética tales como el uso de malware por delincuentes en línea, robo de propiedad intelectual, phishing, cyberstalking y más. Nuestra oficina estará ofreciendo consejos semanales de cyber en octubre a través de nuestro sitio web y medios sociales!

Adobe dejara de soportar Flash Player en 2020

Como los estándares abiertos como HTML5, WebGL y WebAssembly han madurado en los últimos años, la mayoría ahora proporcionan muchas de las capacidades y funcionalidades que los plugins fueron pioneros y se han convertido en una alternativa viable para el contenido en la web. Con el tiempo, Adobe ha visto cómo las aplicaciones de ayuda evolucionan para convertirse en plugins y, más recientemente, han visto que muchas de estas capacidades de plugins se incorporan a estándares web abiertos. Hoy en día, la mayoría de los vendedores de navegadores están integrando las capacidades una vez proporcionadas por los complementos directamente en los navegadores y los complementos de desestimación.

Adobe está planeando al final de su vida Flash. En concreto, dejaremos de actualizar y distribuir Flash Player a finales de 2020 y animaremos a los creadores de contenido a migrar cualquier contenido Flash existente a estos nuevos formatos abiertos.
bit.ly/Adobe-EOLFlashP

Software con fin de vida

EOL Software
Las aplicaciones de software tienen un ciclo de vida. El ciclo de vida comienza cuando el software se libera y termina cuando ya no es compatible con el proveedor, también llamado Fin de vida (EOL por sus siglas en inglés). Cuando el software deja de ser soportado por el proveedor, ya no recibe actualizaciones de seguridad.

EOL OS
Windows XP y Apple OSX 10.8 y anteriores son EOL. Si actualmente utiliza uno de estos sistemas operativos (OS por sus siglas en inglés) de EOL, debe actualizar su sistema operativo para mantener la seguridad de su computadora y sus datos. Las computadoras pertenecientes, arrendadas o administradas por UTRGV deben cumplir con el estándar de seguridad informática (bit.ly/UTRUTRGVISOComputerSecurityStandard), que requiere que ejecuten sólo sistemas operativos compatibles con proveedores. Vista será EOL en Abril del 2017, por lo tanto planee actualizar este sistema operativo pronto.

Actualice si está utilizando versiones **anteriores** de cualquiera de los siguientes productos:

Productos soportados

Producto	Versión	Producto	Versión	Producto	Versión	Producto	Versión
Windows	8	MacBook Pro	OS X 10.7	Java SE	8	Firefox	55.0.2
Windows	8.1	Adobe Flash Player	26.0	iPhone	iOS 8.1	Google Chrome	60.2
Windows	7	Adobe Reader	2017.012	Android	Jelly Bean	Internet Explorer	11
Windows	10	Adobe Acrobat X	2017.012				
iMac	OS X 10.7						

Para actualizar correctamente al sistema operativo más reciente, necesitará los siguientes requisitos de sistema. En el caso de que el hardware del equipo no sea capaz de soportar el último sistema operativo, entonces de acuerdo con el estándar de seguridad informática, el equipo tendrá que pasar por el excedente y una nueva con hardware capaz tomará su lugar.

Si utiliza para su actividad laboral una computadora que es propiedad universitaria con un sistema operativo con EOL, inicie sesión en my.utrgv.edu y envíe un ticket a través de Service Now o póngase en contacto con IT Service Desk lo antes posible.

Brownsville / Harlingen / Isla del Padre Sur 956-882-2020
Edinburg / McAllen / Río Grande City 956-665-2020

Una recomendación amistosa para estudiantes, maestros y empleados de UTRGV que utilizan computadoras personales o portátiles: revise los siguientes requisitos de sistema, inicie sesión en my.utrgv.edu, visite la aplicación vSoftware y compre ($ 9.95 USD) Windows 10; Es muy recomendable que realice una copia de seguridad de todos sus archivos, fotos y otros documentos importantes antes de actualizar su sistema operativo. En el caso de que su computadora personal no sea compatible con el sistema operativo, considere actualizar su máquina.

Para obtener una lista con más software EOL, visite: bit.ly/list-EOL2017

ESCRITORIO LIMPIO

BUENA SEGURIDAD

PRÁCTICA

Un ejemplo de mala práctica

Una práctica de escritorio limpio asegura que todos los materiales confidenciales o sensibles se eliminan de un área de trabajo y se ponen bajo llave cuando los elementos no se usan o un empleado sale de su estación de trabajo. Es una de las principales estrategias a utilizar cuando se intenta reducir el riesgo de violaciones de seguridad en el lugar de trabajo. Utilice la lista de verificación a continuación para asegurarse de que su área de trabajo (o hogar) es segura, organizada y compatible.

- ☐ Las contraseñas no deben dejarse escritas en ninguna ubicación accesible.
- ☐ Asegúrese de que toda la información confidencial o sensible en forma impresa o electrónica esté segura al final de la jornada de trabajo o cuando usted se haya ido por un período prolongado.
- ☐ Las pantallas de las computadoras (portátiles, tablets, teléfonos, etc.) deben bloquearse cuando el espacio de trabajo esté desocupado.
- ☐ Los dispositivos portátiles, como las tabletas y teléfonos móviles, deben asegurarse en un lugar bajo llave cuando no se estén utilizando o al final de la jornada de trabajo.
- ☐ Los dispositivos de almacenamiento externo, como los CD, DVD o unidades USB, deben protegerse en un almacenamiento bajo llave cuando no estén en uso.
- ☐ File cabinets, drawers and storage lockers containing Confidential or Sensitive information should be kept closed and locked when not in use or not attended.
- ☐ Llaves utilizadas para acceder información confidencial o sensible no deben dejarse en un escritorio desatendido.
- ☐ Todas las impresoras y máquinas de fax deben ser despejados de los papeles tan pronto como se impriman; Esto ayuda a garantizar que los documentos confidenciales o sensibles no se dejan atrás para que la persona equivocada los recoja.
- ☐ Tras la eliminación*, los documentos confidenciales y / o sensibles deben ser triturados o colocados en contenedores confidenciales bajo llave.

**Aseúrese de que las políticas de gestión y retención de registros de UTRGV se sigan al deshacerse de cualquier registro oficial de UTRGV [HOP ADM-10-102]*

ISO destacó a:

ISO destacó a: es una entrevista de un individuo que forma parte de UTRGV o juega un rol en la seguridad informática. En este boletín, conoceras a Jennifer Avila, *Network Security Analyst III*.

Jennifer Avila
Network Security Analyst III

1. Díganos cómo ha cambiado la seguridad de la información desde que empezó en su papel.
La priorización en la seguridad cibernética, ya que todo está basado en la nube. Sin duda, ha aumentado debido al elevado aumento del cibercrimen y al elevado precio de los datos personales.

2. ¿Quiénes son sus clientes y cuál es una de las áreas más difíciles para usted?
UTRGV personal de TI, alta dirección, asuntos legales, PD, HR. De acuerdo con la tarea de análisis forense y de vulnerabilidades para aplicaciones. La parte desafiante es obtener los datos que necesitan, los resultados; Cada tarea puede ser única, la mitad de las veces se siente que usted necesita para reinventar la rueda.

3. ¿Cómo es que llegaste al campo de seguridad informática?
Comencé (alrededor de 2001) yo era un director de TI para una pequeña organización, y yo estaba involucrado con el control de acceso, el administrador del servidor (intercambio de administración) con la asistencia de los consultores. De todos los diferentes papeles el campo de la seguridad era de gran interés para mí.

4. Los tres logros mas importantes en su vida:
- Casarme
- Obtener mi licenciatura y posgrado (MSIT)
- -reservare éste para los logros en el futuros-

5. La gente se sorprendería saber que:
- Por lo general, cuando no estoy en el trabajo, estoy tomando clases de baile
- Me encanta cocinar (pasteles y cualquier cosa en general)
- He estado en muchos conciertos y festivales

6. ¿Qué CD tiene usted en su coche? ¿O qué estación de radio te gusta escuchar?
Tengo en mi vehículo Sirius XM (Hard rock, Latin, 80's music)

7. Si pudieras entrevistar a una persona (viva o muerta) ¿Quién sería?
- Mi juez, el tipo que creó el silicon valley
- Tool (el cantante principal)

8. ¿Si se le da la oportunidad, quien le gustaría ser por un día?
Alguien que es súper rico y lo daria a la caridad.

9. ¿Cuál es el mejor consejo que has recibido y que ha utilizado?
Manténgase fiel a sí mismo y su primer instinto es la mayoría de las veces el camino correcto.

10. ¿Cuál sería su consejo para un nuevo profesional en la seguridad informática?
Obtenga sus certificaciones, esté abierto a aprender diferentes conceptos.

WannaCry Ransomware y Lecciones

Por Departamento de Recursos de Información
DIR.texas.gov

Una vulnerabilidad descubierta por primera vez por la Agencia de Seguridad Nacional y luego liberada por los piratas informáticos en Internet. El 12 de mayo de 2017, los blogs de tecnología y las noticias de SI se encendieron con la noticia de un nuevo ataque de ransomware que se propagaba como un incendio forestal a través de redes públicas y privadas, bloqueando a la gente de sus datos y exigiendo que pagaran un rescate o perdieran todo. Agencias como el British National Health Service (NHS) y Telefonia, el mayor proveedor de telecomunicaciones de España, fueron afectadas. Incluso empresas privadas como Fedex sintieron el peaje de este software malicioso. Sólo en las primeras horas, entre 230.000 y 390.000 computadoras en más de 150 países se infectaron con este ransomware recién descubierto. Su nombre era WannaCry (WNCRY / WannaCrypt).

Este mal negocio nos enseñó algunas lecciones difíciles.

1. **Parche.... ¡¡PARCHE!!** Todo el mundo siempre lo dice, pero claramente no todo el mundo lo hizo. Este ransomware atacó con éxito tantos sistemas debido a sistemas operativos no soportados o sin parches. ¡Como dije, remiendo!

2. **El olvido no es excusa.** Los sistemas dejados en el pasado a menudo significan puntos de acceso no supervisados. WannaCry demostró cuán importante es la gestión de activos consistente. Los malos actores se aprovechan de tu error humano. Es fundamental dar un paso atrás y mirar su sistema desde el exterior. Si estuviera tratando de colarse en sus sistemas, ¿dónde buscaría primero?

3. **Construir algunas paredes con segmentación de red.** Remendar viejos sistemas a menudo viene con una serie de desafíos técnicos. Por esta razón, los nuevos sistemas se construyen a menudo sobre el viejo y sin apoyo. Muchos no se dan cuenta del riesgo de los sistemas sin parche y la falta de segmentación de la red. La segmentación de la red y la arquitectura de red bien planificada podrían haber ahorrado a algunas organizaciones un mundo de dolor.

4. **La ciberseguridad protege la vida real.** Es importante recordar mientras la ciberseguridad es digital y usted puede estar luchando la buena lucha detrás de una pantalla de computadora, la vida de la gente cuelga en la balanza. El ataque de WannaCry a los servicios de atención de salud en el Reino Unido, fue una muestra clara de que hay consecuencias que van mucho más allá de bitcoin.

5. **¡No olvide la disponibilidad!** WannaCry dio a las organizaciones una rápida patada en la parte trasera y les recordó que la disponibilidad en el taburete de tres patas de la CIA, es esencial para el éxito de los negocios cotidianos. El costo de este ransomware se estima en más de $ 8 mil millones de dólares debido a la interrupción del negocio, la pérdida de ingresos y el tiempo de restauración gastado..

ISO Invitado

U.S. DEPARTMENT OF STATE
OVERSEAS SECURITY ADVISORY COUNCIL

Hacking sucede

Caso de estudio: Dendroid Malware

Las funciones maliciosas incluyen:

- Realizar y grabar llamadas
- Eliminar registros de llamadas
- Interceptar mensajes de texto
- Tome fotografías con la cámara del teléfono
- Descargar imágenes existentes
- Grabar y subir audio y video
- Abrir aplicaciones y páginas web
- Iniciar denegación de servicio

En los primeros meses de 2015, se descubrieron diariamente 5.000 nuevos ejes de malware para Android. Sólo uno de esos fue "Dendroid", un acceso remoto dinámico y difícil de detectar también, que al mismo tiempo fácilmente disponible en foros de malware por una módica tarifa de $ 300. Dendroid se esconde dentro de estas aplicaciones y evade el detector de malware de Google Play, permitiéndole operar durante períodos prolongados. Sus diversas capacidades -como encender el micrófono a voluntad- podrían utilizarse para facturas fuertes de números de tarifa premium o permitir que actores maliciosos recopilen información sobre el negocio y los contactos personales del propietario de Android. Los usuarios deben desconfiar de las aplicaciones que solicitan una amplia variedad De permisos, y puede descargar aplicaciones de seguridad móvil para protegerse contra diversas amenazas de malware.

Continúa de la página 7

Detección de una intrusión

¿Cómo sabes cuando has sido hackeado?

La mayoría de los encuestados no estaban seguros o eran incapaces de identificar un compromiso en sus dispositivos móviles. Esto aumenta de nuevo el riesgo de información, especialmente si los empleados continúan utilizando sus teléfonos con fines comerciales después de que un dispositivo sea hackeado. A menudo, el malware del smartphone es extremadamente difícil de detectar. Algunos signos de compromiso pueden incluir:

- Estado latente
- Batería con drenaje frecuente
- Mayor uso de datos
- Aparecer aplicaciones
- Aplicaciones que desaparecen

Desafortunadamente, muchos de los síntomas de compromiso también pueden confundirse con la conexión a través de un proveedor de servicios extranjero mientras viaja al extranjero. Ofrecer a los empleados un dispositivo de préstamo o asistencia técnica puede ser la mejor manera de mitigar los hacks no detectados de los teléfonos móviles.

\Todos los principales proveedores de teléfonos inteligentes ofrecen la posibilidad de limpiar a distancia dispositivos-un interruptor de matar virtual que permite la eliminación de datos sensibles en caso de que un teléfono se pierde o es robado. Aunque el borrado remoto no se ejecute si la batería del teléfono muere, una señal no está disponible o un hacker deshabilita las conexiones de red, sin embargo es una táctica de mitigación que todos los empleados deben activar y utilizar tan pronto como un teléfono desaparezca. Los siguientes enlaces ofrecen guías paso a paso sobre la eliminación remota de Android (support.google.com/a/answer/173390) y Apple (support.apple.com/kb/PH2701).

Siéntase libre de continuar leyendo el informe "Viajando con dispositivos móviles: Tendencias y mejores prácticas" visitando el sitio Web de OSAC: www.osac.gov/Pages/ContentReportDetails.aspx?cid=17989

Do **YOU** have an idea for a topic? Would you like to include something in particular to this newsletter? Any comments or suggestions are **ALWAYS** welcome!

Feel free to submit your thoughts by visiting our website:
bit.ly/utrgvisonewsletterfeedback

er.educause.edu/blogs/2015/12/january-guard-your-privacy-online

The University of Texas Rio Grande Valley
Information Security Office

FREE GIVEAWAY

Get a chance to WIN
one of our popular drawstring bag
WITH goodies!

LIKE
Our Facebook Page

SHARE
The Post

TAG
3 Friends

www.utrgv.edu/is

@UTRGViso

ARTÍCULOS DE SEGURIDAD

5,300 registros de la Universidad de Iowa Health Care expuestos durante dos años
Miles de pacientes de la Universidad de Iowa Healthcare (UIHC) tenían parte de su información privada inadvertidamente publicado por más de dos años en un sitio de desarrollo de aplicaciones web.

En mayo de 2015 la información del paciente sin cifrar fue guardada por un empleado de UIHC en un sitio público de intercambio de archivos que formaba parte de un programa de creación de aplicaciones web de código abierto que utilizaba la organización. Los archivos fueron dejados en el sitio desprotegido después de que el proyecto fue terminado.
Los archivos fueron detectados el 29 de abril por un profesional de ciberseguridad y reportados al oficial de privacidad de UIHC. Los archivos fueron removidos del sitio de intercambio de archivos antes del 1 de mayo. El 22 de junio UIHC comenzó a enviar cartas informando a los afectados de lo ocurrido.
bit.ly/UICHDB

SANS OUCH! Boletín de Agosto: Respaldo y recuperación
Si utilizas una computadora o un dispositivo móvil por mucho tiempo, tarde o temprano algo puede salir mal, resultando en la pérdida de tus archivos personales, documentos o fotografías. Por ejemplo, puedes eliminar archivos importantes accidentalmente, tener una falla de hardware, perder el dispositivo o infectarte con alguna especie de malware como ransomware. En casos como estos, los respaldos son a menudo la única forma de reconstruir tu vida digital. En este boletín, explicamos qué son los respaldos, cómo respaldar tus datos y desarrollar una estrategia simple que sea adecuada para ti.
bit.ly/SANSAgostoN

La Corte Suprema de Justicia de Nueva York cayó por un ataque de phishing de 1 millón de dólares
Lori Sattler, fue engañada por más de un millón de dólares mientras trataba de vender su apartamento en el Upper East Side y comprar otro. bit.ly/1MillionPhish

Universidad de Newcastle falsificada en estafa de phishing
Los ciberdelincuentes se esforzaron mucho para clonar el sitio web de la Universidad de Newcastle hasta llegar a crear docenas de subpáginas que explicaban los diferentes programas ofrecidos por la Universidad

Mientras que los defraudadores cometieron algunos errores en el sitio falso, los que no están familiarizados con el sitio real, como los estudiantes de intercambio de divisas fácilmente podría confundirlo de verdad. Los hackers se refirieron incorrectamente a la escuela en el sitio de phishing como la "Universidad Internacional de Newcastle" en lugar de como "Universidad de Newcastle" tanto en la URL como en todo el sitio.
bit.ly/UNewcastleSpoofed

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.

Servicios que proporionamos:

CONCIENCIA, RIESGO Y CUMPLIMIENTO

ADMINISTRACIÓN DE LAS VULNERABILIDADES

INGENIERÍA Y RESPUESTA A INCIDENTS

CONCIENCIA, COMUNICACIÓN Y DIFUSIÓN

Oficinas:

- Sugar Road Annex (ESRAX) Building
- R-167 Rusteberg Hall (BRUST) Building (*by appointment*)

Teléfono: (956)665-7823

Email: is@utrgv.edu

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

¡Danos tu opinion!
bit.ly/utrgvisonewsletterfeedback

Agradecimientos especiales a:

Information Technology

Jennifer Avila

The Overseas Security Advisory Council (OSAC)

www.osac.gov