Nuestra razón de ser

IT SECURITY FORENSIC, Es una empresa de ciberseguridad que tiene como objetivo brindar servicios enfocados en identificar posibles fallos en la seguridad de las infraestructuras tecnológicas de nuestros clientes, y para ello contamos con un grupo de consultores expertos en técnicas de Ethical hacking, analistas de vulnerabilidades, peritos informáticos forenses, auditores en ciberseguridad y expertos en infraestructura tecnológica y aplicaciones de redes de datos y servicios web, aplicando metodologías y estándares internacionales, para brindar a nuestros clientes servicios de calidad, con tiempos de respuesta óptimos y con costos acordes al mercado de la ciberseguridad.

Misión

Ofrecer servicios de consultoría especializada en ciberseguridad de la información, informática forense, Ethical hacking, análisis de vulnerabilidades, auditoría de seguridad de la información y capacitación, con los más altos estándares de calidad del mercado, lo que genera confianza y valor a nuestros clientes.

Visión

En cinco años ser líderes, generando conocimiento mediante los procesos de formación y capacitación, así como convertirnos en un centro de investigación cibernética en las líneas de la informática forense digital, el análisis de vulnerabilidades y las pruebas de seguridad “Ethical Hacking” o “Pentesting”, complementando con los servicios de auditoría de seguridad de la información, enmarcados en los estándares y normas internacionales vigentes.

Equipo de trabajo

Contamos con un equipo de trabajo multidisciplinar, con conocimientos específicos en las áreas asociadas a los servicios que ofertamos para nuestros clientes. Todo en aras de brindar calidad en el desarrollo de las actividades y procesos que requieren los servicios definidos en nuestro portafolio, con personal calificado y certificado en normas internacionales como: Auditores líderes en ISO-IEC 27001:2013, ISO-IEC 27001:2022, ISO 27032, ISO 31000, ITIL v4, TOGAF, Pentester Certified Offensive and Defensive Security Professional (CODSP), Scrum Master Professional Certificate (SMPC), Scrum Foundation Professional Certificate, IPv6 Avanzado, Investigadores Digitales Forenses (IDF) y Peritos Ciber Judiciales.

Portafolio de servicios

Detección, análisis y remediación de vulnerabilidades.

IT SECURITY FORENSIC SAS. Cuenta con expertos en materia de detección, análisis y remediación de vulnerabilidades, a nivel de sistemas operativos, aplicaciones, entornos web, bases de datos, dispositivos activos de red y artefactos tecnológicos tales como dispositivos móviles, sistemas de control de acceso y sistemas IoT.

Nos enfocamos en la identificación de los posibles riesgos que afectan la funcionalidad, disponibilidad, confidencialidad e integridad de estos. Para ello los expertos de nuestra entidad utilizan diferentes herramientas tecnológicas especializadas que permiten garantizar los procesos establecidos para el servicio.

Objetivos

- Utilizar las mejores prácticas y metodologías para identificar, clasificar y analizar las vulnerabilidades y riesgos que afectan los sistemas informáticos.
- Generar los planes de remediación más pertinentes para las vulnerabilidades y riesgos detectados.
- Diseñar planes de capacitación y concientización del uso de las herramientas tecnológicas de la organización.

Estructura del servicio.

1. **Detección de vulnerabilidades a nivel de software, hardware, y dispositivos móviles.**

IT SECURITY FORENSIC SAS, utiliza herramientas de software especializadas, de carácter licenciado como libre para la detección de vulnerabilidades en sistemas informáticos, a nivel de software, hardware y dispositivos móviles.

Actividades propuestas

- Definición de los objetivos de análisis.
- Diseño de las pruebas de detección de vulnerabilidades.
- Informe técnico de las vulnerabilidades identificadas.

2. Análisis de vulnerabilidades.

IT SECURITY FORENSIC SAS, utiliza metodologías enfocadas al proceso de análisis de vulnerabilidades en sistemas informáticos, a nivel de software, hardware y dispositivos móviles.

Actividades propuestas

- Clasificación de las vulnerabilidades identificadas.
- Informe técnico de las vulnerabilidades clasificadas.

3. Plan de remediación de vulnerabilidades y ejecución de este

Un equipo multidisciplinar de IT SECURITY FORENSIC SAS, genera los planes de remediación y mitigación de las vulnerabilidades identificadas y clasificadas, utilizando las mejores prácticas, normatividades y modelos definidos para el proceso. También acompaña a los dueños y administradores de los servicios y plataformas en la implantación del plan propuesta, con el objeto de garantizar la correcta ejecución.

Actividades propuestas:

- Plan de remediación para las vulnerabilidades identificadas y clasificadas.
- Acompañamiento en la ejecución del plan de remediación.
- Informe técnico del proceso de remediación definido y ejecutado.
- Nuevas pruebas de detección de vulnerabilidades de los sistemas parchados.
- Informe técnico del estado final del proceso.

Etical Hacking

El Etical hacking, es una técnica utilizada por los Pentester para evaluar la seguridad informática en los sistemas, infraestructura y todos los activos de información de la compañía. Mediante el uso adecuado de esta técnica es posible identificar las vulnerabilidades, falencia en los sistemas y programas, también se enfoca en realizar un análisis más metódico y profundo, ya que mediante diversas metodologías se realiza la explotación de los fallos encontrados, con el objeto de presentar el impacto real al que está expuesta la entidad.

IT SECURITY FORENSIC SAS. Utiliza metodologías eficientes que permiten obtener los mejores resultados en las pruebas de ciberseguridad y explotación de vulnerabilidades identificadas en los sistemas informáticos, de hardware e infraestructura tecnológica objeto de análisis.

Objetivos

- Utilizar las mejores metodologías para determinar los fallos, falencias y vulnerabilidades en los sistemas informáticos y de infraestructura tecnológica. Ejecutar diferentes técnicas de explotación de estas, para demostrar el estado real de los sistemas y el impacto que se puede generar si se materializa un evento.
- Hacer visibles las fallas de seguridad que pueden presentar los sistemas informáticos y concientizar a las directivas de la importancia de las medidas de seguridad y protección que deben implementar para evitar ser víctimas de los ciberdelincuentes informáticos.
- Generar los informes técnicos y ejecutivos pertinentes relacionados con el objeto de servicio de Etical Hacking realizado.

Estructura del servicio.

1. **Etical Hacking**

1.1. Servicios y aplicaciones Web.

IT SECURITY FORENSIC SAS, utiliza herramientas de software licenciado y libre especializadas para la detección de vulnerabilidades y explotación de estas en los sistemas, servicios y aplicativos webs, los cuales se encuentren expuestos en Internet. Este tipo de servicio se puede desarrollar mediante pruebas externas a la compañía o al interior de esta, obteniendo resultados que al ser comparados se obtendrá información específica que permitirá al Pentester generar recomendaciones adecuadas y ajustadas a las necesidades de inseguridad identificadas.

IT SECURITY FORENSIC SAS, utiliza herramientas y metodologías especializadas para la detección y explotación de las vulnerabilidades identificadas en las redes inalámbricas o wifi, las cuales permiten hacer visibles los riesgos y fallas en las configuraciones de los dispositivos activos y aplicaciones que los controlan. Con la información obtenida se generan las recomendaciones pertinentes para dar solución a los agujeros de seguridad identificados.

1.2. Ingeniería Social.

Es una técnica utilizada para revisar y evaluar la seguridad de los recursos informáticos de la compañía, se enfoca en técnicas que tratan de persuadir y adquirir información vital de las personas (empleados, clientes, proveedores) y personal que tiene algún tipo de vínculo con la organización. La ingeniería social busca identificar las falencias que tienen los usuarios a nivel de seguridad y tiene como objetivo primordial demostrar la importancia de la concientización y adopción de buenas prácticas en temas de seguridad por parte de todos los empleados de la organización.

1.3. Dispositivos activos de red perimetral.

Para el proceso de Etical hacking de dispositivos de red perimetral, IT SECURITY FORENSIC SAS, utiliza técnicas especializadas que permiten identificar y vulnerar la seguridad de los sistemas, haciendo evidente los fallos en

configuraciones y procesos de actualización adecuados del software utilizado por los activos de hardware.

Actividades propuestas para los servicios de Etical hacking

- Definición de los objetivos de análisis.
- Diseño de las pruebas de Etical hacking.
- Reconocimiento.
- Escaneo.
- Obtener acceso.
- Mantener acceso
- Informe técnico.
- Presentar informe.

Informática Forense.

IT SECURITY FORENSIC se encarga de analizar los sistemas informáticos en busca de evidencias que permitan llevar a cabo una causa judicial o una negociación extrajudicial, para ello se cuenta con herramientas especializadas, metodologías y recurso humano experto en el área de la informática forense.

Permitiendo realizar los procesos necesarios para la adquisición de información en cualquier tipo de dispositivo como: (equipos de cómputo o equipos móviles y servicios publicados en Internet (Correo electrónico, páginas web, etc.). La información obtenida de esta actividad es procesada y analizada, cumpliendo con los estándares de seguridad y protocolos de cadena de custodia establecidos. Con el objeto de garantizar a nuestros clientes la integridad y confiabilidad de la información.

Objetivos

- Recuperar información en dispositivos y medios digitales mediante técnicas avanzadas, garantizando la preservación de la data original.

- Tomar copias o imágenes digitales de medios electrónicos, de carácter sospechoso, involucrados en un evento informático, utilizando herramientas especializadas de software forense, para realizar la búsqueda y extracción de datos específicos y necesarios para un proceso judicial.
- Realizar un análisis detallado para una investigación digital forense a partir de una imagen que suministre un tercero.
- Utilizar herramientas y técnicas especializadas para levantar información de fuentes de datos abiertos y públicos, a partir de datos o perfiles básicos.
- Asegurar y preservar evidencia digital en tránsito o en reposo.
- Garantizar el almacenamiento temporal o permanente de evidencia digital forense.

Servicios de informática forense que ofrecemos

A partir de la toma de imágenes forenses, la recolección de evidencias, IT SECURITY FORENSIC, presta los siguientes servicios, mediante el uso de herramientas y técnicas específicas para la actividad.

- **Adquisición.** A partir de un medio de almacenamiento o dispositivo magnético original, se crea una imagen forense con sus respectivos hashes de integridad. También dentro del servicio es posible recuperar información perdida a partir de un medio o dispositivo de almacenamiento original.
- **Análisis.** Se realiza una investigación forense a partir de una imagen de un dispositivo de almacenamiento, la cual puede ser elaborada por los expertos forenses de la compañía y suministrada por un tercero. El análisis también puede realizarse a partir de datos o perfiles básicos, obtenidos de fuentes abiertas o privadas.
- **Preservación.** Permite el aseguramiento y preservación de evidencia digital en tránsito o en reposo. Como también el almacenamiento temporal o permanente de evidencia digital.
- **Borrado seguro de medios de almacenamiento.** Muchas entidades cuando realizar una actualización del parque tecnológico a nivel de equipos de cómputo, optan por desecharlo o realizar procesos de donación a entidades sin ánimo de lucro, sin tener en cuenta que en las

unidades de almacenamiento pueden entregar información corporativa que, al caer en manos criminales, puede ser perjudicial para la compañía.

Informes periciales

Para el servicio de informática forense se realizan informes específicos y de carácter jurídico, los cuales pueden ser presentados como evidencia en un proceso judicial. Las pruebas entregadas a los clientes se elaboran dando cumplimientos a las premisas establecidas por la ley y garantizando los debidos procesos de cadena de custodia y preservación de la información.

Diseño, estructuración y acompañamiento en la implementación de un modelo de seguridad enfocado en el sistema de gestión de seguridad de la información "SGSI" bajo las directrices del "MSPI" recomendado por MinTic.

IT SECURITY FORENSIC, desarrolla y acompaña a la organización en implantación del sistema de gestión de seguridad de la información "SGSI", enmarcado bajo la normativa ISO/IEC 27001:2013 e ISO-IEC 27001:2022.

Actividades propuestas

- Realizar una visita inicial a la organización, con el objeto de identificar si existe o no una estructura de seguridad de la información y definir el alcance del SGSI en caso de no contar con un modelo establecido.
- Colaborar con la definición de las políticas de seguridad de la información, acorde con la estructura organizacional.
- Estructurar los procedimientos necesarios para la correcta implementación del SGSI.
- Realizar el proceso de auditoría interna y plan de mejora continua del SGSI, una vez implantado el modelo desarrollado.

- Generar un plan de formación y concientización para los empleados de la organización enfocado al modelo de seguridad de la información y gestión de riesgos.

Objetivos

- Identificar los riesgos asociados a los activos de información y servicios misionales de la organización.
- Identificar y clasificar los niveles de seguridad para los activos de información existentes en la organización.
- Diseñar, estructurar y acompañar a la organización en el proceso de implementación de un modelo de seguridad de la información enmarcado bajo los estándares recomendados por el MinTic.
- Recomendar e implantar una metodología de gestión de riesgos informáticos acorde a la misión estratégica de la organización.
- Acompañar en el proceso de formación y capacitación para todo el personal de la organización en el sistema de gestión de seguridad de la información (SGSI), enmarcado bajo el modelo de seguridad y privacidad de la información (MSPI).

Diseño e implementación del protocolo IPv6 y servicios asociados

IT Security Forensic, es experta en el acompañamiento a las instituciones en el diseño, desarrollo, capacitación e implementación del plan de transición para la adopción del protocolo IPv6, (Internet Protocol versión 6). De IPv6 depende que más dispositivos, equipos de cómputo, teléfonos móviles o tabletas en cualquier institución, puedan conectarse a la red, abonando el camino para la implementación de redes de nueva generación, nuevos y más eficientes servicios sobre la red, así como acceso a contenidos exclusivos, que sólo están publicados mediante este protocolo.

Además del plan de adopción se incluye la construcción del plan de transición, la ejecución de la implementación y monitoreo para la adopción de IPv6 en la institución y las capacitaciones y sensibilizaciones necesarias para el proceso de transición en los sistemas de información de la institución.

Objetivos específicos

- Apropiar y capacitar al personal de TI de la institución en los conceptos y herramientas necesarias para la implementación de IPv6.
- Realizar el inventario institucional de equipos de red, equipos de cómputo, servicios de red y aplicación.
- Hacer un diagnóstico de la infraestructura de la entidad: aplicaciones, servicios, seguridad y topología de los servicios y la red de datos.
- Construir el plan de implementación para IPv6 con las acciones necesarias para alcanzar el nivel óptimo de direccionamiento en la entidad.
- Realizar la implementación y el plan de direccionamiento IPv6 para la entidad teniendo en cuenta los resultados obtenidos en el diagnóstico y plan de implementación.
- Llevar a cabo la socialización de resultados en el equipo de TI de la institución.

Alcance (fases para el proceso de adopción)

El alcance de cada acompañamiento será definido según el tamaño y las características tecnológicas de la institución. Se realizarán las siguientes Fases:

Capacitaciones y formación.

Capacitaciones.

IT SECURITY FORENSIC. Cuenta con un grupo de expertos dentro de los cuales se destacan profesiones y magíster en diferentes áreas del conocimiento tales como ingenieros en electrónica, sistemas, redes, ciberseguridad, eléctricos, así como licenciado, técnicos y tecnólogos.

Con este equipo de trabajo multidisciplinar se ha diseñado una gran variedad de cursos y programas de capacitación en áreas de las tecnologías de la información, sistemas informáticos, redes de datos, redes eléctricas, ciberseguridad de la información y normas tales como ISO 27001:2013, ISO 27032, ISO 27005 e ISO 31000. Utilizando metodologías eficientes que permiten obtener los mejores resultados en los procesos de aprendizaje.

Objetivos

- Utilizar las mejores metodologías para los procesos de enseñanza aprendizaje.
- Formar a los estudiantes en programas enfocados en áreas técnicas y normativas.
- Preparar al estudiante para presentar los exámenes de certificación en normas tales como ISO 27001 Auditor Líder, ISO 27032 Gerente de ciberseguridad, ISO 27005 Gestión de riesgos de IT e ISO 31000 Gestión de riesgos.

Curso de Implementación de servicios IPv6 Avanzado.

El curso avanzado de IPv6 tiene una duración de 40 horas y está concebido para capacitar a profesionales en el Área de Redes, Gerentes de Proyectos y de Tecnologías de la Información que tengan conocimiento en protocolo IPv4 y en el funcionamiento de internet, necesarios para entender el porqué de la migración hacia IPv6.

A raíz del agotamiento de direcciones IPv4, por el uso comercial de Internet, que se empezó a percibir en los años 80, hubo la necesidad de implementar nuevas estrategias que permitieran un mejor uso de estas direcciones (Subredes, VLSM, NAT y direccionamiento privado) y junto con el imparable crecimiento de usuarios y dispositivos, implicó en pocos meses que estas direcciones se agotan.

Por todo lo anterior, el organismo que se encarga de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), ha trabajado en los últimos años en una nueva versión del Protocolo de Internet, concretamente la versión 6 (IPv6), que posee direcciones con una longitud de 128 bits dando mayor cantidad de direcciones a enrutar y ofreciendo posibilidades de seguridad y calidad de servicio desde el mismo protocolo.

La implementación del protocolo IPv6 se está realizando a nivel mundial de manera gradual y en coexistencia con IPv4, pues su desplazamiento se hará de manera paulatina hasta tanto los dispositivos de cliente, equipos de red, aplicaciones, contenidos y servicios se adapten a la nueva versión del protocolo de Internet; por esta razón, se ha hecho indispensable contar con personas capacitadas que participen en la transición hacia IPv6, encargadas de desarrollar estrategias para el diseño e implementación de redes bajo los parámetros del nuevo protocolo.

Objetivo

Dar a conocer los conceptos tanto básicos como avanzados y las funcionalidades del protocolo IPv6 para su transición y convivencia en las redes de datos y comunicaciones de Colombia.

Metodología
El presente curso contará con elementos teórico-prácticos, que conducirán al estudiante a un aprendizaje significativo, después del cual, podrá realizar actividades de configuración del protocolo IPv6 en equipos de red y máquinas virtuales utilizando diferentes Sistemas Operativos.

Dirigido a
Profesionales del área de TI, área de redes, gerentes de proyectos y de tecnologías de la información.

Curso de Ethical Hacking.

El curso de Ethical hacking tiene una duración de 40 horas y está concebido para capacitar a profesionales en el área de redes de datos, ingenieros de sistemas, electrónicos, seguridad y encargados de garantizar la confidencialidad, autenticidad y disponibilidad de los servicios informáticos de las organizaciones y para todos aquellos interesados en aprender las técnicas y métodos del pentesting en todas sus estructuras.

El programa de formación está concebido con una metodología teórico-práctica la cual permite al estudiante adquirir las destrezas necesarias para ejecutar un test de penetración sobre diferentes entornos informáticos.

Objetivo.
Formar profesionales altamente competitivos en el área del Ethical hacking, con conocimientos específicos y el uso de técnicas y herramientas avanzadas para la identificación y vulneración de las falencias encontradas en los sistemas informáticos.

Metodología
El presente curso contará con elementos teórico-prácticos, que conducirán al estudiante a un aprendizaje significativo, después del cual, podrá realizar actividades de Etical hacking sobre dispositivos activos de red y máquinas virtuales utilizando diferentes Sistemas Operativos.

Dirigido a

profesionales en el área de redes de datos, ingenieros de sistemas, electrónicos, seguridad y encargados de garantizar la confidencialidad, autenticidad y disponibilidad de los servicios informáticos de las organizaciones y para todos aquellos interesados en aprender las técnicas y métodos del pentesting en todas sus estructuras.

Análisis Forense Informático

El curso está orientado a profesionales encargados de diseñar y/o implantar mecanismos de seguridad en sus empresas. Al finalizar el curso el alumno habrá adquirido los conceptos técnicos básicos necesarios en lo que respecta a las metodologías de análisis y el tratamiento y/o adquisición de la evidencia digital.

Objetivo

El objetivo de este curso es introducir al estudiante en los conceptos básicos del análisis forense informático. El curso está orientado a profesionales encargados de diseñar y/o implantar mecanismos de seguridad en sus empresas. Al finalizar el curso el alumno habrá adquirido los conceptos técnicos básicos necesarios en lo que respecta a las metodologías de análisis y el tratamiento y/o adquisición de la evidencia digital.

Metodología

El presente curso contará con elementos teórico-prácticos, que conducirán al estudiante a un aprendizaje significativo, después del cual, podrá realizar actividades de la Informática Forense Digital sobre dispositivos activos de red, equipos de cómputo, dispositivos móviles y máquinas virtuales utilizando diferentes Sistemas Operativos.

Dirigido a

Profesionales y estudiantes interesados en Seguridad Informática, y en particular, profesionales informáticos vinculados a la implantación o diseño de mecanismos de seguridad de la información para el aseguramiento de las organizaciones.

CONTACTENOS
Calle 33 # 24 B 171, Soacha Cundinamarca
Celular: 3163500451
E-mail: it.secu.forensic@gmail.com
www.it-sf.com.co