A continuación presentamos un esquema que detalla lo que propondríamos al realizar una propuesta para proveerles este servicio de consultoría.

INDICE

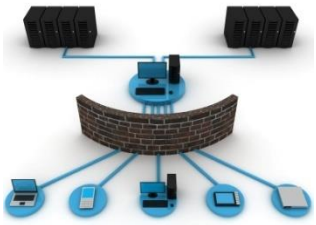
1. Objetivos del Análisis de vulnerabilidades a la Infraestructura Tecnológica.

technologyINT-S21sec se complacen en presentarle el esquema para la prestación del servicio de Evaluación de seguridad Externo a su infraestructura tecnológica. Para ello se ofrece principalmente un Análisis de Vulnerabilidades Externo y un Test de Intrusión externo para ser aplicados en su infraestructura tecnológica.

La propuesta que presentaríamos incluiría la realización de un análisis exhaustivo de la seguridad de los sistemas de información externos (expuestos en internet) de las diferentes instituciones donde se haría el análisis, los cuales se definirían en un alcance definidos en el alcance, incluyendo la identificación de posibles vulnerabilidades y potenciales amenazas y la elaboración de un plan de acción que contendrá recomendaciones y actuaciones priorizadas, para mejorar el nivel de seguridad de sus sistemas.

Las áreas objeto de auditoría se detallan a continuación:

ANÁLISIS EXTERNO DE VULNERABILIDADES



* Auditoria desde Internet, utilizando técnicas manuales y automáticas sobre las direcciones IP públicas de la institución a Auditar.
* Exhaustivo Análisis de Vulnerabilidades sobre los dispositivos infraestructura externa delimitada por la institución a auditar.
* Plan de revisión que permita verificar que las vulnerabilidades reflejadas en los distintos informes han sido resueltas, de manera que sea posible realizar un seguimiento de la resolución de las mismas (Certificación)

TEST DE INTRUSIÓN EXTERNO

* Análisis de la seguridad de la infraestructura de la institución a auditar, desde el punto de vista de un hacker externo a la organización.
* Pruebas técnicas limitadas a n jornadas de trabajo, aunque estas jornadas pueden variar, de acuerdo al tamaño de la institución a auditar, para cada una de las partes a analizar con el único objetivo de conseguir información sensible y/o escalada de privilegios sobre aquellos aplicativos o plataformas de la institución a auditar.
* A realizar en modalidad de Caja Negra (Pentest Externo). Únicamente se requerirá información por parte de la institución a auditar, para confirmar/delimitar el alcance y objetivos a atacar durante la fase de Pentest Externo.

  El equipo de auditores de S21sec evaluará el nivel de seguridad de los diferentes sistemas informáticos que componen la red, detectará posibles vulnerabilidades, intentará explotarlas, presentará los resultados obtenidos y propondrá las recomendaciones que considere más convenientes para proteger el sistema.

2. Nuestra Alianza con S21sec

S21sec es la primera compañía Europea por volumen de colaboración con agencias gubernamentales, cuerpos de seguridad del estado y compañías privadas en todo el mundo para garantizar un servicio de alta calidad a sus clientes en el sector de la seguridad.

3. Nuestras Referencias

S21sec es primera compañía Europea por volumen de colaboración con agencias gubernamentales, cuerpos de seguridad del estado y compañías privadas en todo el mundo para garantizar un servicio de **alta calidad** a sus clientes en el sector de la seguridad.

CNI y CCN-CERT: S21sec mantiene relaciones de estrecha colaboración tanto con CNI, como con CCN-CERT. Por las características de confidencialidad de la relación no se proporcionan más detalles por escrito.

Guardia Civil: S21sec colabora activamente con Guardia Civil en el ámbito de Inteligencia y Ciber-Terrorismo, compartiendo conocimiento que afecta a ambas partes y acudiendo conjuntamente a conferencias internacionales dedicadas a los delitos informáticos.

Europol: S21sec está en trámite de ser formador de Europol en aspectos tan diversos como malware y botnets orientados a los riesgos de los países miembros de UE, como seguridad en aplicaciones Web.

Interpol: S21sec es ponente en eventos de Interpol, especialmente sobre el fraude actual en Internet, y formamos parte de sus grupos de trabajo.

Ministerio de Defensa: S21sec es una compañía que dispone de acuerdo de seguridad en vigor con el Ministerio de Defensa y mantiene relaciones con varios de los principales cuerpos y unidades del ejército español.

Policía Nacional: S21sec colabora tanto con la Dirección General de la Policía en el área de sistemas, como con el área operativa dependiente de las Comisarías Generales en el ámbito de operaciones.

Mossos d'Esquadra: S21sec ha colaborado con el Área de Seguridad en Tecnologías de la Información de los Mossos d'Esquadra en proyectos de consultoría de seguridad lógica.

Ertzaintza: S21sec mantiene relación con Ertzaintza, inicialmente proporcionando servicios a su área de sistemas, y se colabora activamente con otros departamentos operativos en lo relacionado con el Fraude y gestión de incidentes de seguridad.

Policía Foral Navarra: S21sec está acometiendo proyectos con Policía Foral Navarra fundamentalmente en su área de sistemas.

S21SEC como CERT para Sector Financiero

S21sec está constituido como CERT para el sector financiero debido a su actividad por años en la lucha contra el fraude financiero en España. S21sec ha editado anualmente su informe de Fraude Online desde 2005 y dispone de +90% de cuota de mercado de este tipo de servicios anti-fraude en nuestro país.

Organismos Internacionales

Miembro de la BTF, Botnet Task Force (USA)

Miembro de Digital Phisnet (USA)

Miembro Colaborador de FIRST, Forum of Incident Response and Security Teams (USA)

Miembro de la , National Cyber-Forensic & Training Alliance (USA)

Miembro de Team Cymru (USA)

Miembro del APWG, Anti-Phishing Working Group

VeriSign iDefense

iDefense es la mayor compañía de Inteligencia en Seguridad existente a nivel mundial, tanto por volumen de información, como por volumen de agentes (+250), así como por volumen de descubrimientos de vulnerabilidades exclusivas llevadas a cabo.

La estructura organizativa de dicha compañía permite que la investigación de seguridad sea llevada a cabo en 12 idiomas permitiendo el conocimiento global de las tendencias y amenazas emergentes llegando a nivel de conocer que vulnerabilidades van a ser explotadas por que delincuentes, y en base a ese tipo de información tomar un nivel de exposición al riesgo u otro.

VeriSign es uno de los accionistas de **S21sec** en la actualidad, por lo que la relación con iDefense es más que estrecha y continuada en el tiempo. **S21sec** además de mantener relación con los más altos cargos de iDefense, participa como contribuidor en el programa de descubrimiento de nuevas vulnerabilidades como uno de los colaboradores más activos.

Microsoft

S21sec es la única empresa española que alimenta la información del servicio de Barra Inteligente de navegación de Internet Explorer (IE) versión 7.

4. Alcance

Cabe destacar que si bien durante todas las fases del trabajo a realizar se aplicarán buenas prácticas de seguridad y todas las medidas recomendadas por los fabricantes, factores como el número de personas que pueden tener acceso al sistema, la disponibilidad permanente de las conexiones y la transparencia tecnológica hacen que nos encontremos frente a un sistema potencialmente inseguro y expuesto a múltiples amenazas como, por ejemplo:

* Extraños que pueden acceder al sistema desde Internet o desde las redes del clientes (hackers, la competencia, …)
* Fallos en los procesos internos propios que pueden derivar en falta de calidad, falta de seguridad, sobrecargas, ...
* Socios y clientes autorizados a acceder al sistema pero que pueden aplicar políticas de seguridad diferentes a la nuestra
* Gestión incorrecta en el acceso de servicios y en la autenticación de usuarios

El servicio ofertado por **S21sec** pretende auditar la configuración de seguridad de la red externa y aplicativos web simulando las condiciones de un ataque proveniente de un intruso desde Internet para poner de manifiesto posibles vulnerabilidades existentes en la red que podrían llegar a ser explotadas y comprometer al sistema.

Para una correcta realización del proyecto, **S21sec** aplicará todas las técnicas de análisis que están a su alcance y, en particular, utilización de técnicas manuales de hacking ético durante la fase de intrusión, herramientas propietarias en la fase de análisis de vulnerabilidades y aplicación de técnicas desarrolladas en experiencias similares.

El alcance objeto de la auditoría sería el siguiente:

* **Análisis Externo de Vulnerabilidades:**
  Para un análisis Externo, trabajamos sobre un máximo de xxx direcciones IP publicadas en Internet. Estamos en capacidad para hacer análisis hasta de miles de direcciones IP para una sola instiucion.

* **Test de Intrusión externo:**
  Pentest Externo sobre direcciones IP expuestas en internet pertenecientes a la INSTITUCION EXTERNA A REALIZAR.

El servicio ofertado por **S21sec** pretende auditar la configuración de seguridad de la red y simular las condiciones de un ataque proveniente de un intruso desde Internet, para poner de manifiesto posibles vulnerabilidades existentes en la red que podría llegar a ser explotadas y comprometer la infraestructura tecnológica y por ende la seguridad nacional.

Para una correcta realización del proyecto, **S21sec** aplicará todas las técnicas de análisis que están a su alcance y, en particular, utilización de técnicas manuales de hacking ético durante la fase de intrusión, herramientas propietarias en la fase de análisis de vulnerabilidades y aplicación de técnicas desarrolladas en experiencias similares.

NOTAS IMPORTANTES:

-S21SEC CUENTA AMPLIA EXPERIENCIA EN ESTE TIPO DE SERVICIOS.

-CONTAMOS CON AUTORIZACION Y LICECNIAMIENTO DE QUALYS.

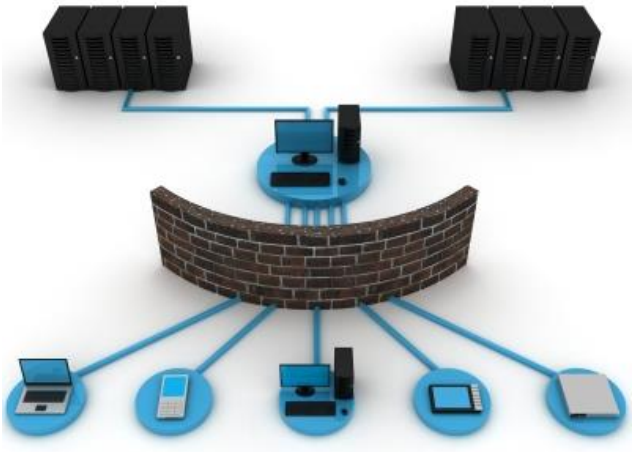
-ESTE SERVICIO ESTA ALINEADO A CUMPLIMIENTO PCI DSS.

-ADJUNTAREMOS UN EJEMPLO DE REPORTE TECNICO Y EJECUTIVO

5. Pruebas de Penetración y Explotación de Vulnerabilidades

TAREAS QUE SE REALIZARIAN EN LA AUDITORIA

Para realizar el test de intrusión externo, **S21sec** se basará en la experiencia profesional de sus auditores así como en metodologías reconocidas mundialmente como la Open Source Security Testing Methodology Manual (OSSTMM) y la Information System Security Assessment Framework (ISSAF) y realizaría sólo aquellos módulos que aplican a un test de intrusión.



Una vez definidos el alcance y los objetivos, se procede a la recolección de aquella información necesaria para llevar a cabo la auditoría.

En esta fase, se pretende obtener el máximo de información de la institución a auditar, que pueda servir para una posible intrusión. Para ello se realizaría una búsqueda para obtener los siguientes resultados:

* Obtención de un Mapa de Red externo
* Información ISP / ASP
* Propietarios del Sistema y del Servicio
* Localización en medios web.
* Nombres de Servidores

Información excesiva de los registros de dominio:

* Comprobación en los registros DNS
* Comprobación de Información Excesiva en los DNS
* Comprobación en las base de datos de SPAM

Identificación de los Servicios de Sistemas

Una vez recabada toda la información posible sobre el objetivo, se intentaría una aproximación más técnica donde se lleva a cabo un sondeo sobre los sistemas de la red de la institución a auditar. El objetivo es conocer el máximo posible sobre:

* Sistemas online
* Puertos y servicios disponibles
* Identificación de routers y firewalls
* Identificación de sistemas críticos
* Versión de sistema Operativo
* Identificación de rutas

Búsqueda y Verificación de Vulnerabilidades

En esta fase se emplean herramientas de software automáticas para realizar un análisis de las posibles vulnerabilidades en los sistemas definidos en el alcance. Para ello se utilizan:

* **Herramientas Comerciales.** El equipo de trabajo realiza un análisis inicial con dichas herramientas para localizar las vulnerabilidades visibles en sus sistemas a través de INTERNET. (15% del tiempo).

* **Herramientas Propietarias.** Se realiza un análisis complementario al anterior con Herramientas Propietarias desarrolladas a través de nuestro Dpto. de I+D+i. Este estudio complementario ayuda a cruzar resultados y a evitar falsos positivos, además es posible que se localicen vulnerabilidades no reportadas por las HHCC (85% del tiempo invertido).

* **Pruebas manuales.** Una vez finalizados todos los estudios automatizados, se procede a realizar un análisis manual de los resultados obtenidos y a ejecutar una serie de pruebas, con el objetivo de descubrir nuevas vulnerabilidades no detectadas por las herramientas software automáticas, así como para eliminar los falsos positivos que se hubiesen podido producir.

Testeo de Medidas de Contingencia

Se evaluarán la eficacia de las medidas de contingencia de los Sistemas de la institución que se encuentran expuestos a Internet, identificando mecanismos de seguridad y procedimientos de respuesta que necesiten ser revisados

Una vez realizadas estas pruebas se conocerá desde el punto de vista de la seguridad los siguientes aspectos de los Sistemas de la Organización:

* Capacidades Anti-Troyano
* Capacidades Anti-Virus
* Medidas de Contingencia
* Debilidades de Contingencia
* Intrusión/Escalada de privilegios

Utilizando las vulnerabilidades identificadas en las fases anteriores, y previo acuerdo con la institución, se procederá a realizar las siguientes acciones:

* **Simulación de Intrusión Externa**. Simular el ataque de una persona con intenciones maliciosas, pretenda introducirse en cualquiera de los Sistemas de la institucion (acceso a Sistemas Protegidos, accesos hacia la DMZ, accesos hacia la LAN, usurpación de datos críticos, etc).

* **Explotación de Vulnerabilidades**. Se intenta explotar las vulnerabilidades localizadas en la fase anterior, garantizando siempre que no influyan en el correcto funcionamiento de los servicios.

* **Generación de Exploits**. El grupo de trabajo encargado de desarrollar este proyecto planteará la generación de exploits propietarios y/o modificación de aquellos que sean públicos y que sirvan como herramientas adicionales para conseguir entrar en la red del cliente u obtener información sensible.

* **Intentos de Acceso**. A través de la explotación de éstas vulnerabilidades, se intenta acceder a las máquinas de cada una de los sistemas visibles, demostrando en cada caso las posibilidades de tomar el control de las mismas, usurpar datos confidenciales, e incluso dejarlas fuera de servicio (los ataques DoS no se llegan a hacer efectivos, pero se documenta la posibilidad de realizarlos, siempre y cuando esta exista).

* **Escalada de Privilegios**. Es interesante demostrar si es posible el realizar una escalada de privilegios (utilizando claves de acceso localizadas a lo largo del estudio o a través de herramientas específicas) que nos posibiliten acceder de una máquina a otra, e incluso llegar a otras redes del cliente.

* **Análisis de Entornos Restringidos (Autenticación).** Se analizan todas aquellas zonas que requieren de una autenticación para conseguir acceso a las mismas partiendo de ataques de “Fuerza Bruta”. Si tras un periodo prudente de tiempo no se consigue entrada a la aplicación a través de las técnicas anteriores, se les pide a los responsables de entorno unas claves de acceso (en aquellas zonas de las aplicaciones en las que sean requeridas) para no demorar el estudio. Dentro de la aplicación se estudia el grado de maniobra de un usuario autenticado, verificando que no se puede obtener información de otros usuarios, no hay cruce de sesiones, etc.

6. Elaboración de la documentación

Los informes entregables, una vez finalizada la auditoria, contendrán la siguiente información:

- **Información pública de los sistemas de la institución**. Se reflejará la información que se puede obtener de los sistemas de la institución cliente: información de dominios, direcciones IP, máquinas, sistemas operativos, información sensible en documentos públicos, cuentas de correo.
- **Descripción de las pruebas de ataques**. Se realizará una descripción de los escaneos automáticos y de las pruebas de ataque manuales realizadas, definiendo los pasos seguidos y las consecuencias que pudiesen tener si éste fuese real.
- **Recopilación de Vulnerabilidades**. A través de ésta fase se documentan las vulnerabilidades localizadas tanto por las herramientas comerciales como las detectadas a través de técnicas manuales.
- **Recomendaciones para la Corrección de Vulnerabilidades.** En el documento de Recopilación de Vulnerabilidades se definirán, asimismo, las recomendaciones técnicas y las propuestas para solventar las problemáticas detectadas. Además se detallarán recomendaciones que prevengan los efectos de los ataques que pudieran tener consecuencias negativas.

La documentación se estructurará con dos formatos diferenciados para facilitar su comprensión tanto por una audiencia técnica, como por una que no lo sea.

Informes Ejecutivos

El Informe Ejecutivo definirá de forma global y resumida el resultado del Test, destacando, entre otras cuestiones:

- Puntos Fuertes y Puntos débiles
- Volumen y catalogación (por riesgo) de las vulnerabilidades localizadas
- Valoración y exposición del estado de seguridad global
- Recomendaciones de **S21sec.**
- Cuadro de mando, que permita realizar un seguimiento de las distintas vulnerabilidades reportadas/solucionadas a lo largo del trabajo.

Informes Técnicos

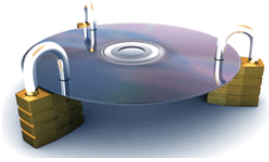
En dichos informes se detallarán todo el proceso seguido y servirá de “Manual Práctico” para realizar la corrección ante los problemas detectados, con independencia de la explicación adicional del workshop.

Entre otras cuestiones contendrá las siguientes:

- Metodología Empleada
- Obtención de Información Pública
- Mapa Topológico y Análisis Inicial
- Análisis de Máquinas / Hosts
  - Definición de las Pruebas Realizadas
  - Vulnerabilidades Detectadas
  - Descripción de las Intrusiones Perpetradas
  - Proposición de Soluciones
- Análisis de Aplicativo
  - Definición de las Pruebas Realizadas
  - Vulnerabilidades Detectadas
  - Descripción de las Intrusiones Perpetradas
  - Proposición de Soluciones
- Soluciones ante las Problemáticas Detectadas
- Incidencias
- Resumen de Vulnerabilidades
- Valoración y Recomendaciones **S21sec**

Documentación Electrónica

Todos los documentos se entregarán en formato electrónico (CD) o por correo electrónico, con extensión PDF y XLS, para que el propio cliente realice las copias y/o distribuciones que considere necesarias. La distribución de los mismos se realizará de manera cifrada y a la lista de personas, que en la reunión inicial mantenida para planificar el trabajo, se decida.



7. Certificación

S21sec cuenta con los certificados de calidad otorgados por la Asociación Española de Normalización y Certificación (AENOR). Esto demuestra la calidad de servicio en materia de seguridad que ofrece la compañía:

Certificado del Sistema de Gestión de la I+D+i, en base a la norma UNE 166002: 2006.
Certificado del Sistema de Gestión de Seguridad de la Información, en base a la norma UNE-ISO/IEC 27001: 2007.
Certificado del Sistema de Gestión de la Calidad, según la norma UNE-EN ISO 9001:2008.

8. Estructura Organizativa

Para la consecución del éxito en un proyecto como el que se identifica en la presente propuesta es necesario constituir desde el primer momento un equipo de trabajo organizado en los siguientes niveles:

NIVEL	**TECNOLOGYINT / INSTITUCION**	S21SEC
Dirección	Comité Director del Proyecto	
Coordinación	Jefe de Proyecto	Jefe de Proyecto Consultor de seguridad.
Ejecución	Responsables de áreas implicadas y personal asignado al proyecto	Auditores de Sistemas

Es imprescindible que la INSTITUCION garantice:

* La participación e implicación de su personal en el proyecto, sobre todo por parte de los responsables de las diversas áreas y funciones.
* Una comunicación fluida entre ambas partes para facilitar la toma de datos, particularmente al comienzo de las fases de Adquisición de conocimiento y acompañamiento.

9. Perfiles profesionales

S21sec pondrá a disposición de LA INSTITUCION un equipo de profesionales altamente cualificados que, entre otros conocimientos, podrán disponer de los siguientes (el tipo de perfil asignado dependerá del tipo de proyecto a realizar):

- **Auditores Especialistas en Técnicas de Hacking / Seguridad Telemática**: Se encargarán de las actividades de Intrusión y los análisis técnicos derivados del proyecto a realizar.
- **Jefe de Proyecto**: Realizará las actividades de coordinación de recursos e interlocución con el Cliente.
- **Responsable de alto nivel**: Realizará la interlocución de alto nivel con el cliente en los casos en que esta fuera necesaria.
- **Documentalista**: Llevará a cabo todas las labores de documentación del Proyecto.

10. Sobre S21sec

En **S21sec** avanzamos con el cambio, adelantándonos a él y generando soluciones eficaces a los retos que la nueva cultura y vida digital exigen a organizaciones y personas.

Contamos con una amplia gama de servicios y productos destinados a garantizar la seguridad de los sistemas de información de las organizaciones.

SERVICIOS:

>> COMPLIANCE

Servicios orientados a garantizar el cumplimiento de la legislación, normativas y estándares de seguridad aplicables a las organizaciones.

>> ASSESSMENT

Los servicios de auditoría de seguridad aumentan la integridad de los sistemas de información, eliminan los accesos ilegales y previenen robos de información, pérdidas de productividad o fraude en las organizaciones.

>> ECRIME

Servicios para la detección y resolución de los incidentes que afectan a las organizaciones, debido principalmente a la proliferación de actividades delictivas en Internet, cibercrimen y fraude online, las 24 horas los 365 días del año.

>> INTELLIGENCE

Servicios y tecnología encaminados a una mejor comprensión de las oportunidades y amenazas de los negocios, facilitan la optimización de los procesos de toma de decisiones y contribuyen a alcanzar una mayor competitividad a través del conocimiento y la capacidad de adaptación a cambios súbitos.

>> CERT

Servicios ofrecidos 24x7x365 desde el CERT de **S21sec** para una gestión proactiva de riesgos de seguridad, monitorización del cumplimiento de los estándares y normativas e identificación, análisis y mitigación de los efectos de las amenazas de seguridad.

>> TRAINING

Planes de formación y concienciación ajustados a los conocimientos y capacidades de los profesionales para proteger a las organizaciones y a la sociedad frente a amenazas y riesgos digitales.

>> RESEARCH

Con laboratorios especializados en fraude y delitos online, vigilancia digital, seguridad multimedia y en entornos SCADA, cloud computing y tecnologías inalámbricas, ofrecemos servicios de innovación para el desarrollo de soluciones, proyectos y metodologías y para dar respuesta a las necesidades actuales y futuras de empresas e instituciones.

TECNOLOGÍA

>> BITACORA

Bitacora es la plataforma que da respuesta a las crecientes necesidades de las organizaciones en materia de gestión de la seguridad y de cumplimiento normativo.

>> DIGITAL SURVEILLANCE

La tecnología de Vigilancia Digital de **S21sec** analiza en tiempo real la información disponible en Internet sobre directivos, productos, clientes y competidores con el objetivo de tomar decisiones para proteger las organizaciones.

11. Investigación y Desarrollo I+D

CENTROS Y LABORATORIOS PIONEROS ESPECIALIZADOS EN CIBERSEGURIDAD.

Apostamos por la investigación y el desarrollo, con una inversión de un 25% del presupuesto anual. Muestra de ello es la creación del primer **centro europeo de I+D+i especializado en ciberseguridad**, con laboratorios destinados a la protección de las últimas tecnologías y desde el que **S21sec** realiza proyectos de vanguardia a empresas e instituciones.

Para ofrecer la máxima protección a los clientes, prevenir el fraude online y poder detectar y actuar ante cualquier amenaza en todo el mundo, en **S21sec** contamos con un **CERT** desde el que se vela por la seguridad las 24 horas del día.

El **Centro de Inteligencia en Seguridad** cierra el ciclo necesario para poder dotar a las organizaciones del conocimiento de sus riesgos y amenazas y apoyar la toma de decisiones.

Desde **S21sec University** ofrecemos planes de carrera y cursos de especialización para la formación de los profesionales de seguridad y campañas de difusión y sensibilización del uso de las TIC para todos los usuarios.

12. Riesgos de estar vulnerables.

Al ser vulnerables, nuestro país puede ser blanco de ataques cibernéticos, de tal forma que el delincuente informático tendrá puertas abiertas para entrar y salir cuando quiera. A que entraría el delincuente cibernético a nuestra infraestructura?

- A robar bases de datos
  - Datos de los clientes
  - Datos financieros de la institución
  - Documentación confidencial de la institución
  - Correos electrónicos intercambiados por la alta gerencia
  - Planos y Formulas confidenciales
  - Propiedad Intelectual
  - Números de cédulas, tarjetas de crédito, contraseñas
- A controlar los sistemas PLC-SCADA desde el exterior
  - Logrando de esta forma controlar cualquier dispositivo desde el exterior.

13. Elaboración de un presupuesto.

Es nuestro interés poder preparar un presupuesto, sin compromisos, sea para una institución o para un grupo, de tal manera que puedan ver los costos y tiempos en que se harían estas auditorías y de esa forma poder incluirlos en los presupuestos del próximo año.

Estamos abiertos a cualquier tipo preguntas o inquietudes, y si están interesados podríamos preparar una audio conferencia en sus instalaciones, para que puedan hacer preguntas directamente a los auditores que harán los trabajos.

Para solicitar un presupuesto, por favor realice una comunicación expresando su interés y tramítala vía correo electrónico, o enviándola vía mensajería a nuestras oficinas, debajo nuestra ubicación.

El responsable y representante en la República Dominicana de S21sec es el Ing. Pedro Héctor Castillo, al cual pueden contactar en la oficina ubicada en la calle Luisa Ozema Pellerano #6, en Gazcue, Distrito Nacional, al número 809-685-8883 o llamarlo directo al 809-330-1586, también pueden enviar un correo a pcastillo@technologyint.net. Para ver más informaciones de quienes somos, servicios, clientes pueden entrar a nuestro sitio web www.technologyint.net.

Solicite hoy su presupuesto sin compromisos….