

**SVIS, S.A. DE C.V.**

**e-Business**

**Tecnología de Información en su Negocio.**



**Página Web**

[www.svis.com.mx](http://www.svis.com.mx)

**e-mail**

[svis@svis.com.mx](mailto:svis@svis.com.mx)

**Telefonos**

+52 (55) 5251 -22-29

+52 (55) 5251 -03-54

**Fax**

+52 (55) 5596 -48-09

Bosques de Duraznos No. 69  
Torre B Piso 5 Desp. 504  
Bosques de las Lomas  
11700 México, D.F.



## Servicios de Seguridad

Dado el entorno de los negocios electrónicos de la actualidad, SVIS S.A. de C.V. se da a la tarea de conformar una serie de servicios alrededor del tema de la Seguridad de la Información desde diversos aspectos y conformando los siguientes servicios:

**Evaluando la Seguridad de la Información Corporativa**

**Análisis de impacto de Negocio**

**Programa de medidas preventivas**

**Plan de Recuperación en caso de desastre**

**Respuesta a ataques cibernéticos**

**Verificando el cumplimiento de la seguridad corporativa**

**Desarrollo de la Arquitectura de Seguridad**

**Cuidando la seguridad de su organización**

**Políticas, procesos, cultura y Organización**

**Planeación estratégica de la seguridad de la información**

**Estándares de Seguridad**

**Concientización en Seguridad**

**Calidad y Experiencia a su alcance**

<p><b>Evaluando la Seguridad de la Información Corporativa</b></p>	<p>La realización del Análisis de Riesgos de Alta Penetración proporciona al cliente una lista detallada de vulnerabilidades en torno a la información contenida dentro y fuera de sus sistemas de información, estableciendo en cada caso el nivel de riesgo.</p> <p>En dicho Análisis no solo mostramos los hallazgos y vulnerabilidades a nivel técnico. A través de generar patrones de posibles ataques al crear escenarios de explotación sobre conjuntos de vulnerabilidades encontradas, el análisis busca demostrar que tan profundo se podría llegar a penetrar dentro de una organización a partir del aprovechamiento sistemático de varios de los huecos que quizá por si solos, no representan una gran amenaza para la continuidad del negocio. Esto permite a la organización que aplique el análisis, establecer un correcto orden de prioridades en la implementación de parches y soluciones, ya sean temporales o permanentes.</p> <p>En un tiempo reducido, se conoce el estado actual de riesgo de la información corporativa, analizando: redes, comunicaciones, aplicaciones críticas, bases de datos, seguridad física, además de revisar las prácticas en el manejo de la información por parte de los usuarios y verificar tanto la existencia como la aplicación de políticas y procedimientos relacionadas al manejo seguro de la información.</p> <p><b>Entregables:</b></p> <ul style="list-style-type: none"> <li>• Dictamen de Seguridad de Información</li> <li>• Resumen de vulnerabilidades y riesgos representativos</li> <li>• Conclusiones</li> <li>• Recomendaciones Generales</li> <li>• Plan de acción Sugerido</li> <li>• Detalle de vulnerabilidades y riesgos</li> <li>• Resumen Ejecutivo</li> </ul>
<p><b>Análisis de impacto de Negocio</b></p>	<p>A través de la implementación de un Análisis de Impacto de Negocio, se identifican los riesgos inherentes a la ejecución de los procesos críticos de negocio para la organización, evaluando el impacto de los mismos en términos de tiempo de recuperación y pérdidas económicas directas. Esto permite definir los requerimientos de seguridad que habrán de establecerse en torno a los procesos de operación más importantes, así como sobre valiosos activos de información del negocio.</p> <p>El Objetivo primordial del análisis, es detectar y priorizar los procesos y activos necesarios para el restablecimiento de la operación del negocio, con un nivel de servicio aceptable.</p> <p>La realización del Análisis de Impacto de Negocio se lleva a cabo a través de la ejecución de un estudio sobre los procesos propios del negocio, identificando procesos críticos, activos de información, posibles situaciones de corrupción de procesos y requerimientos de los procesos de misión crítica entre muchos otros.</p> <p>A través del BIA también se obtiene una clasificación de vulnerabilidades identificadas a través de un análisis de alta penetración, las cuales, se correlacionan de acuerdo a su nivel de criticidad en términos operativos y del valor de la información que manejan.</p> <p>El cliente obtiene una relación de los riesgos que corre la organización, así como la definición de una Estrategia de Recuperación para casos de contingencia, estableciéndose recomendaciones precisas, las cuales permitirán, la eventual implantación de una Arquitectura de Seguridad Robusta.</p>
<p><b>Programa de medidas preventivas</b></p>	<p>Las diferentes vulnerabilidades tecnológicas que se presentan dentro de las empresas son en ocasiones, eventos que sucedieron sin saber de donde vinieron o quien los originó y el daño causado es a veces devastador ya que los riesgos derivados de dichas vulnerabilidades atacan a las empresas en sus procesos de negocio, logrando inhabilitarlas parcial o totalmente; lo que puede resultar enormemente costoso.</p> <p>El equipo de consultores expertos con el que contamos, recomiendan y aplican la solución apropiada a cada riesgo de seguridad, en la cual su equipo de enlace designado dentro de la compañía, es guiado paso a paso en cada proceso de la aplicación de las contramedidas</p>

	<p>necesarias para solucionar parcial o totalmente los riesgos que lo ponen en inmediato e inminente peligro.</p> <p><b>El Servicio está conformado por los siguientes pasos:</b></p> <ul style="list-style-type: none"> <li>• Revisión inicial de reporte de huecos de seguridad</li> <li>• Búsqueda en Internet de información referente a las distintas vulnerabilidades y métodos de corrección a las mismas</li> <li>• Elaboración de documentos de adecuación a infraestructura por vulnerabilidad</li> <li>• Implementación de adecuaciones a infraestructura por parte de SVIS/GCP Global</li> <li>• Elaboración final de Reporte Ejecutivo y Técnico</li> </ul> <p>Los Beneficios obtenidos al contar con un servicio como éste, son innumerables; los principales, son que se eliminan los riesgos informáticos de manera pronta, como suele presentarse la vulnerabilidad.</p> <p>La guía de soluciones así como su aplicación, se hacen la mayoría de las veces utilizando las mismas técnicas avanzadas de hackeo que pudieron haberse manejado para vulnerar los sistemas.</p>
<p><b>Plan de Recuperación en caso de desastre</b></p>	<p>La conciencia de contar con la implementación de un Plan para la Recuperación de Desastres ha crecido considerablemente en los últimos años. La imperiosa necesidad de contar con planes contingentes en cada organización es fundamental. Después del ya tan citado once de septiembre donde el mundo entero presencio lo nunca antes concebido, se ha marcado la pauta para que empresas de todo tamaño contemplen planes de contingencia que les permitan reaccionar de forma tan rápida como les sea posible, ante un acontecimiento desastroso, sea este derivado de la malicia humana o bien por la naturaleza misma (incendios, terremotos, huracanes, etc.).</p> <p>Nuestro equipo experto, implementan corporativamente el plan a través del cuál habilita a sus clientes para responder ágilmente a situaciones inesperadas, de tal forma que las funciones críticas de negocio continúen casi de manera normal, minimizando el impacto en las operaciones.</p>
<p><b>Respuesta a ataques cibernéticos</b></p>	<p>Es un servicio diseñado para el Rastreo de Incidentes de Seguridad el cuál da respuesta a acontecimientos imprevistos que fueron causados deliberadamente o por negligencia, impactando la infraestructura de tecnología o de la información que ésta contiene, a través de la cuál se soportan los procesos de negocio que permiten a la empresa funcionar correctamente, poniendo en riesgo su integridad al ser violados.</p> <p>En tal caso, es probable que nunca se pueda saber que o quién fue lo que produjo el incidente que atentó contra la integridad de la organización, haciendo muy difícil la toma de medidas adecuadas para evitar que ocurra de nuevo. Simplemente, identificar el origen del incidente (interno o externo a la organización) implica la toma de medidas muy diversas.</p> <p>La mayoría de los incidentes pueden ser rastreados hasta su origen, dependiendo de la habilidad de quién lo ocasionó, así como de la prontitud con que éste le sea reportado a un experto para su rastreo. Dependiendo de la naturaleza del incidente, de la calidad de la información proporcionada por el cliente y de la prontitud del reporte, los miembros del equipo tienen la capacidad de identificar a través de un análisis forense, los eventos que derivaron en el incidente, identificando en un buen número de ocasiones al o los responsables del hecho. Sin embargo en ocasiones, la gran habilidad de quién comete la ofensa, impide llegar al origen de todo lo acontecido. No obstante, los miembros del ISET de SVIS/GCP Global® siempre entregan datos de gran valía para el cliente, los cuales le permitirán sentar las bases de prevención que lo lleven a evitar que dicho incidente se repita.</p> <p><b>Algunos beneficios que pueden alcanzarse a partir de la aplicación del programa son:</b></p> <ul style="list-style-type: none"> <li>• Respuesta rápida a incidentes.</li> <li>• Recopilación de evidencia electrónica y documental sobre el incidente.</li> <li>• Cierre de huecos de seguridad.</li> <li>• La entrega de un reporte técnico y ejecutivo de lo hallado.</li> </ul>

	<ul style="list-style-type: none"> <li>• Identificación de él o los causantes del incidente</li> </ul> <p>Para evitar pro-activamente estos incidentes, consulte con nuestros expertos las alternativas que tenemos para que, organizaciones como la suya, se protejan de este tipo de amenazas.</p>
<p><b>Verificando el cumplimiento de la seguridad corporativa</b></p>	<p>Este programa permite a las organizaciones definir si los esquemas de seguridad de información establecidos en el pasado continúan siendo viables aún tras los cambios sufridos por la empresa y su entorno. Situaciones donde hayan sucedido cambios significativos en el número de personal, número de equipos de cómputo, cambio en la plataforma tecnológica, o bien en la fusión entre dos o más organizaciones, introducen variables culturales capaces de invalidar los modelos de seguridad existentes.</p> <p>Es un servicio integral de investigación y análisis que provee información sobre todos los factores tecnológicos, estructurales, culturales y de procesos de negocios, que pueden afectar negativamente la confiabilidad, confidencialidad o disponibilidad de la información institucional.</p> <p>Abarca la evaluación conjunta o separada de los tres niveles de medidas de seguridad que deben existir en toda organización.</p> <p><b>Dichas medidas son:</b></p> <ul style="list-style-type: none"> <li>• Medidas de Prevención: Aquellas destinadas a impedir que se produzcan incidentes de seguridad capaces de causar un impacto a la operación del negocio.</li> <li>• Medidas de Detección: En esta categoría se evalúan aquellas medidas y mecanismos que permiten detectar intentos de penetración a los sistemas.</li> <li>• Medidas de Corrección: Permiten minimizar los efectos negativos ocasionados por problemas u omisiones ubicadas en el modelo de seguridad existente.</li> <li>• Permite conocer, sin dejar espacio a la especulación, el nivel de cumplimiento en el desarrollo de las operaciones diarias y de los estándares de seguridad establecidos por la organización.</li> <li>• Evalúa la vigencia del modelo de seguridad existente VS el modelo de seguridad que se debería tener debido a los cambios en la organización y en su entorno.</li> <li>• Facilita la comprensión sobre cómo es que el elemento humano, la estructura organizacional y los procesos de negocios pueden estar fungiendo como factores de riesgo para la continuidad y la estabilidad operativas. Así, no sólo se identifican vulnerabilidades derivadas de la aplicación de la tecnología, también se consideran las variables relacionadas con todo el entorno de negocio.</li> <li>• Se detectan las áreas de mejora potencial, obteniendo las bases para planear e implementar bajo un correcto orden de prioridades, las medidas preventivas y correctivas necesarias. Identificación de las fortalezas y debilidades de cada uno de los elementos auditados.</li> </ul>
<p><b>Desarrollo de la Arquitectura de Seguridad</b></p>	<p>El desarrollo de una Arquitectura de Seguridad de TI ahora, es más importante que nunca pues permite la interacción compleja y segura de diversos sistemas de computo, protocolos de comunicación e infraestructuras de sistemas sobre redes publicas y privadas, de forma que se maximice la productividad de los usuarios, garantizando la confidencialidad, integridad y disponibilidad de los activos de información corporativos.</p> <p>El servicio tiene por objetivo estudiar, diseñar e implementar una Arquitectura de Seguridad formal dentro de la organización, estableciendo mediante la utilización de tecnología de punta, un ambiente de cómputo seguro y acorde con los requerimientos funcionales de la organización, alineándose a la estrategia de seguridad corporativa, sin perder de vista los objetivos del negocio.</p> <p>La metodología para la implementación comienza por la recolección y análisis de la información centrados en los requerimientos del negocio, pasando por la revisión de la infraestructura actual, análisis de la normatividad existente, dictado de directrices para la evaluación de tecnologías entre otras actividades, hasta llegar al punto de generar un diseño conceptual apoyado de un plan de implementación.</p> <p>El beneficio principal de desarrollar una arquitectura de seguridad sólida es minimizar</p>

	<p>seriamente el riesgo de incidentes y daños a la información institucional.</p> <p>Antes de implementar un proyecto para el desarrollo de una Arquitectura de Seguridad de Información es necesario contar con los siguientes elementos:</p> <ul style="list-style-type: none"> <li>• Evaluando la Seguridad Corporativa.</li> <li>• Políticas de Seguridad.</li> <li>• Análisis de Riesgos de Alta Penetración.</li> </ul>
<p><b>Cuidando la seguridad de su organización</b></p>	<p>Hemos comprobado que pueden encontrarse las causas de posibles riesgos para la salud empresarial, incluso en la ausencia de síntomas claros, desde un primer sondeo. Este servicio cumple con ese propósito a través de un análisis de alto impacto de la seguridad de información, elemental para la prevención de amenazas y su posterior eliminación en la operatividad organizacional.</p> <p>Es un servicio que presenta y analiza los resultados de tal manera que se genera una conciencia colectiva sobre la responsabilidad de actuar y anticiparse, corporativamente, contra toda amenaza derivada de problemas en la seguridad de la información. Igualmente, los resultados establecen las bases para planear e instituir medidas concretas contra riesgos que comprometan la competitividad organizacional.</p> <p>Tome en cuenta que la información organizacional es un valioso activo. Las causas y posibles amenazas a la seguridad de dicha información pueden situarse en la cultura, la estructura y los procesos organizacionales.</p> <p><b>Objetivos que cumple:</b></p> <p><b>APRENDER a identificar pro-activamente amenazas que pongan en riesgo la operación y continuidad del negocio.</b></p> <p>Ayuda a comprender cómo el cambio tanto interno como el del entorno, puede impactar a la organización, exponiendo los elementos de la seguridad de información que pueden poner en riesgo la organización al amenazar sus resultados.</p> <p><b>UBICA los Puntos de Mejora Potencial.</b></p> <p>Agrupar las áreas de oportunidad previstas por la alta dirección, sobre los temas claves de carácter organizacional y operacional, mismos que pudieran verse impactados directa o indirectamente por factores de riesgo en el manejo de la información, los cuales debieran ser atacados para minimizar dramáticamente el nivel de vulnerabilidad de la organización e inclusive incrementar el desempeño de la misma. Los puntos acumulados se manejan de manera que el grupo crea una visión común de la situación real, así como de las prioridades.</p> <p><b>COMPRENDER la brecha que existe entre el nivel de riesgo actual y un nivel de riesgo tolerable.</b></p> <p>El ritmo al que evolucionan las organizaciones y su entorno, hace imposible eliminar de forma absoluta los riesgos y amenazas que la acechan. En este punto se realiza un análisis en el que expone como la cultura, estructura y procesos organizacionales pueden estar generando factores de riesgo que representen amenazas latentes así como llevar éstas a los niveles mínimos aceptables.</p> <p><b>IDENTIFICA las vulnerabilidades en la Infraestructura Tecnológica.</b></p> <p>Se determina el grado de vulnerabilidad de la organización desde los puntos de vista de manejo de datos, sistemas de información y telecomunicaciones.</p> <p><b>VISUALIZAR claramente la cadena de causas que dan origen a posibles e</b></p>

	<p><b>inaceptables niveles de riesgo.</b></p> <p>A través de la utilización de herramientas probadas en cientos de organizaciones alrededor del mundo, llevamos al grupo directivo no sólo a visualizar las principales amenazas que atentan contra la organización, si no a identificar sus raíces, obteniendo un análisis de causa-efecto de todos aquellos patrones problemáticos que pueden desencadenar en un (posible) estado de alta vulnerabilidad. De igual manera, se obtiene una visualización sobre CÓMO invertir dicha cadena a fin de crear una cadena de soluciones. Con ello, surge una mejor comprensión del grupo en relación a los riesgos y áreas de oportunidad existentes, proveyendo por tanto la habilidad para pronosticar los retos a los que se enfrentarán en un futuro, facilitando su capacidad de adaptación al cambio y logrando atacar los problemas antes que estos se presenten.</p> <p><b>LOCALIZA claramente las áreas de oportunidad más urgentes.</b></p> <p>Conduce a la organización a contar con un adecuado orden de prioridades, desarrollando una correcta valoración de su información, logrando la comprensión de la diferencia entre información confidencial, sensible y pública, identificando el impacto y consecuencias que los riesgos actuales pueden desencadenar, dando certidumbre a la toma de acciones concretas y específicas. A través del servicio se obtiene un resultado real sobre el nivel de riesgo a corto plazo que puede tener la empresa en cuanto a sus procesos de negocio más importantes.</p> <p><b>DEFINICIÓN del borrador de un Plan de Acción orientado a resolver las áreas de oportunidad en la seguridad, las cuales pudieran afectar seriamente a la organización.</b></p> <p>Basados en el cúmulo de resultados obtenidos en los puntos anteriores, así como en un orden de prioridades derivado de los patrones previamente identificados, se genera una guía práctica de solución inmediata sobre qué hacer en caso de contar con vulnerabilidades de alto riesgo que pongan en peligro los ingresos, utilidades y/o el prestigio de la organización.</p> <p><b>¿Qué caracteriza al servicio?</b></p> <ul style="list-style-type: none"> <li>• El servicio se aplica en muy corto tiempo; hasta en 6 días.</li> <li>• No es necesario que el cliente asigne un líder de proyecto o personal de apoyo dedicado.</li> <li>• No entorpece las actividades cotidianas del cliente durante su ejecución.</li> <li>• Precisa de la participación de la Alta Dirección tan sólo por un día.</li> <li>• Está basado en tecnología probada en cientos de organizaciones alrededor del mundo.</li> <li>• Se genera un reporte que contiene el análisis creado con el grupo ejecutivo, complementado con un reporte técnico preciso que señala las áreas de oportunidad para los departamentos técnicos y de sistemas.</li> </ul>
<p><b>Políticas, procesos, cultura y Organización</b></p>	<p>Proporcionamos una solución basada en estándares mundiales sobre la generación e implementación de políticas, procesos, así como la definición de la estructura organizacional que un área de seguridad de información debe tener, con base en la importancia que cada empresa le de a su "Información".</p> <p>Para saber si su empresa requiere de estos elementos, tendrá que preguntarse lo siguiente:</p> <ul style="list-style-type: none"> <li>• ¿Qué tan importante es su información y que tan segura esta en función a su importancia?.</li> <li>• ¿Qué tanto depende su empresa de sus sistemas de información y de comunicaciones en sus procesos de operación regular y en la toma de decisiones?.</li> <li>• ¿Qué tan disponible necesita que se encuentre su información y sus sistemas de operación así como los de producción?.</li> <li>• Su información estratégica, ¿cuenta con la confidencialidad necesaria?.</li> <li>• ¿Existen las políticas, procesos y controles necesarios que permitan un buen uso de la información corporativa?.</li> <li>• Y en caso de existir, ¿se llevan a cabo?</li> </ul>

	<p>Quizá desconoce de la existencia de estos elementos (políticas, procesos, cultura y estructura) o sabe que existen y que no se cumplen cabalmente. Si éste es el caso, quizá sea momento de hacer un alto en el camino y tomar en cuenta estos cuestionamientos.</p> <p>Hemos colaborado con un numeroso grupo de organizaciones alrededor del mundo en el Diseño e Implementación de una Organización de Seguridad de Información, respaldándonos años de experiencia así como una calidad excepcional. Un aspecto fundamental para que participemos en un proyecto de tal magnitud va condicionado a que exista una conciencia activa en los altos directivos de la organización de que el elemento cultural forma la base fundamental de un proyecto de tal envergadura. De no contar con su apoyo y patrocinio directo, es muy probable que prefiramos no participar en el desarrollo de una solución como esta, ya que su implementación sería difícilmente un éxito.</p> <p><b>Los principales beneficios de contratar el servicio son:</b></p> <ul style="list-style-type: none"> <li>• El Incremento sustancial en el nivel de Concientización sobre la importancia de la seguridad de la información.</li> <li>• Contar con proceso y controles más seguros y confiables.</li> <li>• Contar con Políticas apegadas a estándares internacionales, incluyendo mecanismos de aplicación.</li> <li>• La formación de una base "Cultural" de Seguridad de Información perdurable.</li> <li>• Aumento en la capacidad de adaptación al cambio interno y del entorno de manera pro-activa.</li> </ul>
<p><b>Planeación estratégica de la seguridad de la información</b></p>	<p>Poner en riesgo la Información Corporativa, hoy en día significa comprometer la continuidad y la supervivencia de casi cualquier empresa. La información es un activo cuyo valor es incalculable. La pérdida de la confidencialidad o de la confiabilidad de ésta puede dañar seriamente la capacidad organizacional de producir resultados. La definición e implantación de una Estrategia de Seguridad de Información Corporativa es indispensable para anticiparse a las amenazas y minimizar los riesgos derivados del mal uso de la inteligencia organizacional. Un esfuerzo de tal magnitud reclama la participación de todas las áreas de la organización, toda vez que su alcance va más allá del ámbito de la aplicación tecnológica.</p> <p>Hemos diseñado este servicio de asesoría estratégica altamente especializado el cuál tiene por objetivo facilitar la creación de la Estrategia Maestra de Seguridad de Información, de forma coherente con los objetivos y exigencias del negocio y del mercado a donde se desenvuelven las operaciones de cada uno de nuestros clientes. Bajo este marco, la organización puede decidir de manera inteligente y pro-activa sobre la realización de inversiones en infraestructura, desarrollo de planes de contingencia, entre otras medidas, mediante una oportuna identificación de los objetivos operacionales de seguridad, mismos que ayudarán a la gestión de los recursos informáticos, manteniéndolos bajo control.</p> <p>El Desarrollo de la Estrategia de Seguridad Corporativa comprende perspectivas de prevención (pro-activo), detección (reactivo), así como de monitoreo y respuesta a incidentes.</p> <p><b>Beneficios del Plan:</b></p> <ul style="list-style-type: none"> <li>• Se comprende el problema de la seguridad de la información como una condicionante para la capacidad operativa de la organización.</li> <li>• Se sientan las bases para generar una conciencia colectiva sobre la importancia de salvaguardar los activos de información, permeando dicha noción a todos los niveles de la organización.</li> <li>• Se entiende que la capacidad para reaccionar ante incidentes de seguridad representa una alternativa de solución inaceptable, es decir, se reconoce que al reaccionar, el daño ya ha sido infringido.</li> <li>• Se institucionaliza un plan estratégico de acción pro-activa que opera permanentemente, dando respuesta a los continuos cambios tecnológicos, culturales, estructurales y de proceso.</li> </ul>
<p><b>Estándares de</b></p>	<p>Es un servicio de alta tecnología en el cuál se desarrollan, actualizan e implementan las metodologías de seguridad para el control de proyectos y el control de cambios en las áreas</p>

<p><b>Seguridad</b></p>	<p>de IT, buscando desarrollar e incluir los requerimientos para calificar la seguridad de la información conforme a modelos de clase mundial, evaluando los requerimientos de seguridad de la información relacionados a los procesos de control de cambios en las aplicaciones y sistemas de información empresariales.</p> <p>Toda organización condiciona su operación a cambios constantes. Los sistemas y aplicaciones que la soportan deben realinearse continuamente con el negocio debido a causas tales como: la generación o el acopio de nuevos tipos de datos, el desarrollo de nuevos productos y servicios, las modificaciones legales y fiscales, las fusiones, la apertura de sucursales, la concesión de franquicias, etc. El manejo de la infraestructura de sistemas y de la información corporativa se ve desafiado con cada transformación, de modo que el cumplimiento de estándares de seguridad se convierte en un reto permanente. Es necesaria la aplicación de una Metodología centrada en Estándares de Seguridad para poder identificar las amenazas y minimizar los riesgos derivados del desarrollo de nuevos proyectos de TI así como del mantenimiento de sistemas ya existentes. Mediante un control y una gestión adecuada de los cambios originados por nuevos proyectos, pueden mantenerse niveles adecuados en la seguridad de la información sin comprometer la continuidad de la operación. El fondo de este esfuerzo consiste en prever posibles contingencias.</p> <p><b>Beneficios del servicio:</b></p> <ul style="list-style-type: none"> <li>• Evaluar la sensibilidad de la información durante la iniciación del desarrollo o la modificación de nuevos sistemas.</li> <li>• Poder definir los requerimientos de seguridad y control interno incluidos en el diseño conceptual de cada sistema (ya sea nuevo o modificado) lo más tempranamente posible.</li> <li>• Poder establecer estándares adecuados para la definición y la documentación de los requerimientos de seguridad para cada nuevo proyecto o para cualquier modificación en los sistemas.</li> <li>• Capacidad para identificar los controles de seguridad que garantizan la precisión, la suficiencia y la autorización de entradas y salidas de información para asegurar la integridad y confidencialidad de la información.</li> <li>• Planear la administración de la seguridad en la realización de proyectos de TI usando: puntos de revisión, calidad, inspecciones, pruebas y revisiones de procesos automatizados.</li> <li>• Evaluar los riesgos y las contingencias de la realización de proyectos, tomando en cuenta factores técnicos y no técnicos.</li> </ul>
<p><b>Concientización en Seguridad</b></p>	<p>El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.</p> <p>De ahí, que la disciplina de la seguridad debe ser entendida y practicada por todos y cada uno de los elementos de una organización moderna. Este servicio cubre esta expectativa.</p> <p>Nos dimos a la tarea de conformar un seminario de Concientización de seguridad que estuviera al alcance de todos los niveles de la organización, sin importar su grado de conocimiento sobre el tema de Seguridad Informática.</p> <p>El servicio consta de los siguientes temas:</p> <p><b>Introducción</b></p> <ul style="list-style-type: none"> <li>• Evolución del término Seguridad</li> </ul> <p><b>Seguridad Física</b></p>

- Tipos de desastres
- Acciones hostiles
- Control de accesos

### **Seguridad Lógica**

- Controles de acceso
- Niveles de Seguridad Informática

### **Delitos Informáticos**

- La información y el delito
- Tipos de delitos informáticos
- Delincuente y víctima
- Legislación Nacional
- Legislación Internacional

### **Amenazas Humanas**

- Hackers
- Personal

### **Comunicaciones**

- Objetivo de las redes
- Protocolos de red
- Estructura básica de la Web

### **Amenazas Lógicas**

- Acceso – uso - autorizado
- Detección de intrusos
- Identificación de amenazas
- Tipos de ataques

### **Políticas de Seguridad**

- Políticas de Seguridad Informática
- Evaluación de Riesgos

### **Ingeniería Social**

- Métodos
- Quien es el enemigo?

### **Conclusiones**

Si el personal de nuestra empresa se encuentra capacitado y conciente de la necesidad y utilidad de la seguridad, el éxito esta asegurado.

“En la actualidad, ninguna organización se encuentra inmune a incidentes de seguridad, lo mejor es estar preparado”