SISTESEG

Seguridad y Continuidad para su Negocio

SERVICIOS EN SEGURIDAD DE LA INFORMACION

BOGOTA/COLOMBIA

Perfil Corporativo

Somos una empresa especializada en la prestación de servicios dirigidos a mejorar la capacidad de manejar el riesgo sobre la información dentro de las organizaciones, con el objetivo de poder generar un conjunto de controles lógicos, físicos y administrativos, como resultado de nuestro proceso de evaluación.

Contamos con un equipo humano profesional, en el área de Ingeniería de Sistemas e Ingeniería Eléctrica, con estudios de postgrado en reconocidas universidades del país.

Nuestro personal además posee experiencia laboral en al área de consultoría, desarrollada en compañías multinacionales y nacionales, reconocidas en área de Comunicaciones, Desarrollo de Software y Seguridad de la Información: 3Com, Extreme Networks, Sonicwall, además somos CISSP Certified del ISC^2, CISA de ISACA, ABCP del DRI, miembros de ASIS Internacional, ISACA, IP usergroup e IEEE.

Nuestros Recursos

Los servicios de seguridad de la información que ofrecemos buscan garantizar un tiempo mínimo de ejecución, seguridad integral e integración del recurso humano, para lograr continuidad en la operación del negocio, contamos con:

- Consultores con experiencia Internacional.
- Integración de fabricantes lideres en sus áreas.
- Auditores PCI, Auditores 052, Auditores ISO 27001.
- Somos una empresa orientada en Seguridad de la Información.
- Servicios de instalación de:
  - firewalls,
  - IPS,
  - GAV
  - Mail Security,
  - Control de contenido
  - VPN(IPSEC)
  - VPN(SSL)
- Ingenieros con experiencia en Sistemas Operativos, Bases de Datos, Comunicaciones, Seguridad de la información.
- Modelo de seguridad SGSI cumpliendo con el estándar ISO 17799/ISO 27001, COBIT e ITIL.
- Manejo Integral del Riesgo^{TM}: Seguridad física + Seguridad Lógica + Factor Humano.

- Experiencia en la elaboración y seguimiento de planes estratégicos de los sistemas de información.

Nuestra **Misión.**

Proveer servicios de calidad en el área de la Seguridad de la Información, con personal altamente calificado, cumpliendo con los requerimientos de nuestros clientes y la rentabilidad de nuestros accionistas.

Portafolio de **Servicios**

Seguridad **de la Información.**

La seguridad de la información es un componente crítico de la estrategia de negocio de cualquier organización. Nuestros servicios de seguridad de la información le permiten identificar los riesgos asociados a la información dentro de su organización, definir políticas y procedimientos de acuerdo a los requerimientos de su negocio, identificar las herramientas de tecnología que apoyen las políticas y controles, e implementar un plan de concientización y entrenamiento a los usuarios de acuerdo a los roles dentro de la organización.

Para el desarrollo de los servicios de seguridad utilizamos estándares y recomendaciones de las mejores prácticas tales como: ISO 17799/ISO 27001, COBIT, Circular 052, PCI e ITIL.

Evaluación **de Riesgos**

La evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

La evaluación cubre los siguientes aspectos:

- GAP Analysis con relación a ISO 27001
- Evaluación con respecto a la norma ISO 27001
- Administración de la seguridad de la información.
- Seguridad Física
  - Según el NFPA 75
  - EIA/TIA 942
- Redes de Comunicaciones.
- Pruebas de Penetración (Hacking Ético)
  - Sistema operativos(GFI LanGuard)
  - Equipos de red
  - Acceso físico y lógico

- Telefonía.
- Bases de Datos.
- Sistemas Operativos
- Aplicaciones.
  - Metodología de desarrollo
  - Cumplimiento ISO 17799/ISO 27001
  - Lista de verificación.
- Firewalls.

Con base en los riesgos encontrados se define un plan de implementación de los controles para mitigarlos a corto, mediano y largo plazo. Este plan es la verdadera carta de navegación para la inversión en tecnología.

Definición de Políticas, Procedimientos y Estándares de Seguridad de la Información. (SGSI)

La base de cualquier modelo de seguridad de la información son las Políticas y Procedimientos. Basados en una evaluación de riesgos definimos políticas y procedimientos de Seguridad de acuerdo a los requerimientos de su negocio, siguiendo la recomendación ISO 17799/ISO 27001.

El servicio le ofrece a su organización los siguientes beneficios:

- Definición de las políticas de seguridad de acuerdo a los objetivos y requerimientos de su negocio.
- Estandarización de todos los sistemas de cómputo y comunicaciones dentro de su red.
- Documento en donde constan las políticas de seguridad de la información que la compañía debe seguir.
- Procedimientos de seguridad de la información
  - Procedimientos de respaldo
  - Gestión de cambios
  - Gestión de la capacidad
  - Gestión de contraseñas
  - Gestión del antivirus

Diseño de Arquitectura de Seguridad.

Diseñamos la arquitectura de seguridad necesaria de acuerdo a los requerimientos de su negocio. El diseño incluye herramientas tales como:

- Autenticación.
- Cifrado
- Antivirus y Gateway antivirus
- Control de Acceso Físico.
- Mail security
- PKI
- Control de Contenido.

- Manejo de Ancho de Banda.
- VPN(SSL o IPSEC)
- Políticas del Firewall
- Unified Threat Management UTM[TM Sonicwall]

Auditorías en **Seguridad ISO 27001, Circular 052, PCI**

El servicio de Auditoria de la seguridad, identifica las vulnerabilidades con los riesgos correspondientes y define un plan de acción de los controles para mitigar dichos riesgos. Se trata pues, de si estamos cumpliendo con nuestro modelo de seguridad relacionándolo directamente con los controles establecidos por ISO 27001, Circular 052, PCI y generar un reporte de cumplimiento para que se tomen las medidas correctivas adecuadas.

Los entregables del servicio incluyen un reporte con las vulnerabilidades, riesgos encontrados y las acciones para reducirlos. Este servicio verifica el cumplimiento de acuerdo a lo definido en ISO 27001, CIRCULAR 052 Y PCI y sirve de apoyo en la obtención de la certificación ofrecida por Icontec o PCI.

Para realizar la auditoría PCI nos basamos en las recomendaciones del consorcio PCI fue formado by American Express, Discover Financial Services, JCB, MasterCard Worldwide y Visa International en Sept. 7, 2006. PCI DSS quiere decir Payment Card Industry Data Security Standard y busca proteger la información de los usuarios y luchar contra la suplantación y otros fraudes que se producen en Internet sobre las transacciones electrónicas.

Por otra parte, el servicio de Auditoria de seguridad Circular 052 identifica los controles sobre los cuales no se tiene cumplimiento al momento de la realización de la auditoría. Se busca en este proceso identificar de manera concisa y veraz si se está cumpliendo con el modelo de seguridad alineado directamente con los controles establecidos por la circular 052. Una vez realizado este estudio, es decir, la identificación de los controles sin soporte, se debe generar entonces un reporte de cumplimiento para que se tomen las medidas correctivas adecuadas de acuerdo a un plan de acción definido y aprobado por las directivas.

ITEMS A REVISAR

1. Definiciones y criterios de seguridad y calidad
2. Obligaciones Generales
3. Obligaciones Adicionales por Tipo de Canal
4. Reglas sobre Actualización de Software
5. Obligaciones Específicas por Tipo de Medio – Tarjetas débito y crédito
6. Análisis de Vulnerabilidades

Entrenamiento a usuarios en Seguridad

El servicio de entrenamiento a usuarios ayuda a las organizaciones a reducir de manera importante los riesgos sobre la información, al integrar la seguridad en las tareas diarias de los empleados.

Diseñamos e implementamos el plan de concientización y entrenamiento a usuarios de acuerdo a los roles dentro de la organización. Dentro de los módulos a incluir como parte del entrenamiento a usuario final tenemos:

- ISO 27001, mejores prácticas seguridad.
- Seguridad Sistema Operativo.
- Correo electrónico.
- Seguridad Internet.
- Ingeniería Social
- Manejo de Incidentes.
- Seguridad organizacional y operativa.
- Seguridad Física.
- Ataques a la red.
- Manejo de Contraseñas.

FIN