www.cydesys.com

CYDESYS

CONSULTORIA EN SEGURIDAD INFORMÁTICA

CONSULTORIA PARA IMPLEMENTACIÓN EN SISTEMAS DE GESTIÓN EN SEGURIDAD INFORMÁTICA (SGSI) ORIENTADOS A CERTIFICACIÓN EN PCI DSSV.3.0. E ISO 27001

www.cydesys.com

CYDESYS

SISTEMAS DE GESTIÓN EN SEGURIDAD INFORMÁTICA

SGSI: Un SGSI es un elemento para administración relacionado con la seguridad de la información, implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información.
Si bien gran parte de la información se vincula con computadoras y redes, hay otra parte que no se representa en forma de bits, sino por ejemplo en papeles, en la memoria de las personas, en el conocimiento y experiencia de la organización misma, en la madurez de sus procesos, etc. En ambos casos, la información debe ser protegida de manera diferente, por eso es importante un SGSI.

Solución:

- Repositorios de información: Se establecen los repositorios de información y se establece el grado de confidencialidad.
- Diagnosticó: Conociendo el tipo de información y su clasificación se define el riesgo sobre estos repositorios.
- Diseño del SGSI: Conociendo el nivel de riesgos de la información se establecen los controles necesarios, su periodicidad y se establece el control interno.
- Plan de Continuidad de Negocio: Se establece el plan de continuidad de negocio más acorde a las necesidades de la empresa.
- Documentación: Manuales, procedimientos e instructivos.
- Implementación: Seguimiento y control de los planes establecidos.
- Acompañamiento: Se acompaña a la empresa en el proceso de certificación.

Beneficios:

- SGSI permite obtener una visión global del estado de los sistemas de información.
- Poder observar las medidas de seguridad aplicadas y los resultados obtenidos, para poder mejores decisiones estratégicas.
- Debe estar documentado y ser conocido a distintos niveles por todo el personal.

www.cydesys.com

PCI DSS V3.0.

Evaluación de seguridad PCI DSS

Mejore la seguridad de los datos de las tarjetas de pago evaluando la seguridad de sus procesos bajo PCI Data Security Standard (PCI DSS)
El estándar PCI DSS provee una base de requisitos técnicos y operativos diseñados para proteger los datos de los usuarios de tarjetas. Este estándar es aplicable a todas las entidades involucradas en los procesos de pago mediante tarjeta - comercios, entidades de proceso, adquisición, emisión de tarjetas y proveedores de servicios, así como cualquier otra entidad que almacene, procese o transmita datos de los titulares de una tarjeta. Para cumplir con PCI DSS, se debe evaluar el entorno de pago físico/lógico de la entidad, así como sus políticas, procedimientos y sistemas de configuración.

Solución
Cydesys S.A.S.es consultor en seguridad informática lleva a cabo la evaluación de la conformidad con PCI DSS v 3.0.

Alcance del servicio:

- Pre-evaluación PCI DSS
  o Gap Analysis según PCI DSS
- Consultoría PCI DSS con soluciones integradas
  o Soporte al cliente para cumplir con los requisitos PCI DSS.
- Escaneado PCI (GFI LAN)
  o Usando la herramienta de escaneo más completa en evaluaciones de seguridad o Reportes de escaneo localizados.
- Ensayos de penetración en sistemas, en redes o en aplicaciones.
- Establecimiento de un sistema de gestión acorde con los requisitos PCI DSS
  o Consultoría del sistema de documentación
- Evaluación PCI DSS
  o Auditoría neutral e independiente

Beneficios

- Reducir los riesgos financieros y de marca derivados de problemas en la seguridad de los datos de las cuentas de pago.
- Mejorar su reputación ante entidades de adquisición y marcas de pago.
- Cydesys S.A.S., un solo interlocutor para obtener todas las certificaciones de sistemas de pago necesarias para su negocio.

www.cydesys.com

CYDESYS

ISO 27001

ISO 27001:

Actualmente la información es el objeto de mayor valor para las organizaciones, es por ello que surge la necesidad de diseñar mecanismos que permitan garantizar la seguridad de la misma, la seguridad de la organización es el resultado de operaciones realizadas por personas soportadas por tecnología.

Solución:
La implementación de un sistema de seguridad de información basado en la norma ISO 27001 Comienza por el compromiso de la alta Gerencia en el desarrollo del proceso.
Luego se realiza la valoración de la información y se establecen las tablas de acceso a la información en la empresa.
Se determinan cual es la información más sensible que debe ser protegida y como serán los mecanismos de control para garantizar la confidencialidad, integridad y disponibilidad de la información.

BENEFICIOS

- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

- Confianza y reglas claras para las personas de la organización.
- Aumento de la seguridad con base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.