

CONSULTORÍA TRATAMIENTO DE DATOS CIRCULAR 2 SIC

FASE 2

De acuerdo con la circular externa 02 del 2015 de la superintendencia de industria y comercio con enfoque a la seguridad del tratamiento de datos para el cumplimiento de la norma ISO 27001 versión 2013 y PCI V 3.0.

Con el desarrollo de las tecnologías de la información y la comunicación cada día la información tiene un mayor valor como activo empresarial, en este sentido se puede apreciar como las grandes empresas han sido víctimas de ataques que han tenido altos costos no solamente a nivel económico sino también la imagen de la compañía, en este sentido podemos ver unos ejemplos de los ataques cibernéticos más importantes en la época actual:

1. Panamá Papers: 1,2 Millones de usuarios y 3,8 billones de dólares.
2. El gran hack de EE.UU.: 160 millones de usuarios
3. Adobe: 152 millones de usuarios
4. eBay: 145 millones de usuarios
5. Heartland: 130 millones de usuarios
6. TJX: 94 millones de usuarios
7. AOL: 92 millones de usuarios
8. Sony PlayStation Network: 77 millones de usuarios
9. Veteranos de EE.UU.: 76 millones de usuarios
10. Target: 70 millones de usuarios

Teniendo en cuenta los riesgos informáticos presentes, los diferentes entes gubernamentales están comenzando a desarrollar leyes para garantizar la seguridad de la información, en este sentido el gobierno Colombiano ha establecido el siguiente marco legal.

MARCO LEGAL VIGENTE



Para no solamente cumplir con los requisitos de ley y enfocados a certificaciones como ISO 27001 del 2013 y PCI V3.0. Nosotros presentamos el siguiente proceso de consultoría enfocado a garantizar la seguridad de su información como uno de los activos más importantes de su empresa.

ESTRUCTURA DE LA CONSULTORIA.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

- Diagnostico de las funciones de la información.
- Clasificación de la información.
- Definición de los compromisos de la empresa de acuerdo al marco legal correspondiente.

SERVIDORES

- Inventario de servidores.
- Definición de funciones realizadas en el centro de datos.
- Arquitectura de funciones en servidores

SEGURIDAD FÍSICA

- Revisión de procedimientos.
- Verificación y actualización de datos de empleados.
- Revisión de la funcionalidad del control de acceso.

DIAGNÓSTICO DE RED

- Inventario de equipos periféricos.
- Certificación de puntos de red

ANÁLISIS DE APLICACIONES

- Se evalúa la funcionalidad de cada una de las aplicaciones en la empresa.
- Usuarios, privilegios y contraseñas.

ADMINISTRACIÓN DEL RIESGO

- Identificación de vulnerabilidades.
- Propuesta para controles .
- Implementación de controles.
- Gestión de incidentes.

CIFRADO DE COMUNICACIONES

- Definir las comunicaciones de confidencialidad.
- Establecimiento de método para la realización de comunicaciones cifradas

PLAN DE CONTINUIDAD DE NEGOCIO

- Redundancia.
- Política de back ups
- Centro operativo alternativo

ACTUALIZACIÓN DE REGISTRO NACIONAL DE BASES DE DATOS

- Actualización en marco legal para cambios en registro.
- Consultoría para cumplimiento de los requisitos

PRODUCTOS

DIAGNOSTICO DE CENTRO DE DATOS

- Inventario
- Funciones
- Propuesta de arquitectura

SEGURIDAD FÍSICA

- Revisión y actualización de datos.
- Revisión de procedimientos.
- Auditoria de control de acceso.

SUGERENCIAS

- Estructuración de SGSI Enfocado a certificaciones en normas ISO 27001 y PCI V.3.0.
- Sistema de gestión y detección de vulnerabilidades.