Sheet

¿Qué es Seguridad de la Información y por qué hablamos de prevención de pérdida de datos?

¿Qué es seguridad de información? Pasos, reglas que permiten custodiar la información

La seguridad de información es un valor estratégico y va más alla de la infraestructura, va de un enfoque iterativo y resiliente.

Busca garantizar

- Confidencialidad: Solo pueden acceder las personas autorizadas
- Integridad: La información es inalterada
- Disponibilidad: La información se encuentra disponible y segura

¿Para que sirven las técnicas de prevención de perdida de datos? Permiten garantizar los datos para que podamos estar protegidos en caso suceda algún problema dentro de nuestro sistema y sus datos.

Estudios de Casos: Riesgos materializados que han afectado a grandes empresas

- Yahoo (2013): Pérdida de 2 billones de datos de sus usuarios
- Mariott (2018): Pérdida de 500 millones de datos
- Finder (2016): Perdió datos de sus tarjetas y direcciones

El peligro de conectarlo todo: una ciudad lleva un mes "hackeada" por un peligroso "ransomware"
https://www.abc.es/tecnologia/redes/abci-baltimore-ciudad-lleva-hackeada-peligroso-ransomware-robbinhood-201906070334_noticia.html

Hacking the Russian Power Grid
https://www.nytimes.com/2019/06/18/podcasts/the-daily/trump-russia-cyber-grid.html

Más de mil millones de cuentas afectadas en la nueva megafiltración de Yahoo, la más grande en la historia
https://www.xataka.com/seguridad/los-problemas-para-yahoo-aumentan-una-nueva-megafiltracion-afecto-los-datos-de-mas-de-mil-millones-de-cuentas

Quién está tras el hackeo de Sony Pictures y otros ciberataques
https://www.kaspersky.es/blog/operation-blockbuster/7797/

Más de 5 mil millones de documentos y 229 empresas afectadas: así han sido los mayores robos de datos de la historia
https://www.xataka.com/privacidad/mas-de-5-mil-millones-de-documentos-y-229-empresas-afectadas-asi-han-sido-los-mayores-robos-de-datos-de-la-historia

The 14 biggest data breaches of the 21st century
https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Iniciación: Planeación y Compromiso Interno para adelantar un proceso de Gestión de Riesgos de Seguridad

Gestión de riesgos de seguridad - Momentos

Planeacion y compromiso interno: Fundamental pues debemos incorporar seguridad. Debemos mantener un compromiso alto para que este proceso sea exitoso. Si la alta dirección no se encuentra involucrada, algo no está bien.

Identificacion de Activos de información: Información que se está usando, la que tenemos y como está fluyendo dentro de la organización. Cada activo y cada flujo de información tendrá un control diferencial.

Identificacion de riesgos, amenazas y/o vulnerabilidades: Identificar riesgos y amenazas que pueden afectar estos activos. Qué hacer ante eventualidades.

Identificacion de controles, indidentes a incidentes: Identificar que controles ante un eventual hecho, garantizar que no perderemos la información.

Ejecución - Monitoreo y Evaluación: Realizar los controles, monitorear, evaluar nuestros procesos que estamos realizando para mantener esta seguridad.

Debemos pensar en cómo podemos llegar a vernos afectados.

¿Qué son los activos de Información? Cuál es su valor y cómo identificar los controles a implementar de acuerdo a su nivel de criticidad

Activos de información: Todos los recursos que apoyan el modelo del negocio (BD, archivos, manuales, hardware, software, recursos humanos). Estan directamente relacionados con la administración de la información y de los datos.

Todo es importante dentro de materia de seguridad

Identificar:

- Donde tenemos nuestros servidores alojados
- Como se hace la custodia de información
- Quienes tienen acceso a los datos alojados
- Se depende de una fuente externa
- Qué datos recopilamos de los usuarios
- Los datos recopilados son realmente necesarios
- Donde se encuentra ubicada la empresa

¿Cómo identificar Activos de Información?

1. Hacer un inventario de activos
2. Identificar su responsable
3. Determinar su Nivel de Importancia
4. Clasificar los activos identificados
    1. Infraestructura
    2. Infraestructura crítica

3. Personal

https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

¿Qué son los riesgos digitales? Cómo identificarlos y tratarlos

Identificar riesgos digitales:

1. **Tipo de Activos:** Determinar esto nos permite saber el nivel de importancia del activo de información. Dependiendo si afecta a la disponibilidad, integridad o disponibilidad se califica como sensible o no sensible
    1. Sensible
    2. No sensible
2. **Amenazas:** Factor externo que otra persona o entidad puede explotar para generarme un riesgo para perder datos.
3. **Vulnerabilidades:** Factores internos que pueden exponerme para perder datos o activos de información.
    1. **Riesgos inherentes a la seguridad digital:** Puede ser de dos tipos
        1. **Inherente:** Problemas inherentes de cada negocio
        2. **Residual:** Lo que cada uno puede soportar
    2. **Valoración de impacto:** Que tanto impacto tendría la materialización de este riesgo.
    3. **Valoración de la probabilidad de ocurrencia:** Qué tan probable que este riesgo de seguridad se materialice
4. **Definición de controles**
    1. Definición de controles específicos para prevenir pérdida de datos
        1. Controles en la recolección
        2. Controles en el flujo de la información
        3. Controles en el alojamiento y disposición

5. **Calificar y evaluar controles:** Mantener un sistema de auditorías para poder mantener evaluando las formas de controlar los riesgos de perdida de datos
6. **Gestión y tratamiento del riesgo**
7. **Seguimiento:** Siempre debemos estar dando seguimiento a las formas de seguridad de los datos

https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

Prevención de pérdida de datos, una visión estratégica y proactiva, no solo técnica y reactiva

La prevención de datos es una estrategia. Debemos intentar anticiparnos a los acontecimientos.

No nos diferenciaremos si es que no realizamos una gestión adecuada de los datos de nuestros usuarios.

Debemos mantener una visión estratégica sobre la protección de los datos.

- Diferenciarnos de los demás
- Brindar a nuestros usuarios la seguridad que los datos están mantenidos de forma segura y ordenada

Modelo de Gestión de Riesgos de Seguridad Digital y su relación con la Protección de Datos Personales

Reglamento europeo de proteccion de los datos personales.

Vincula a toda la union europea, pero tambien a todas las empresas que esten haciendo negocios con paises de la union europea y esten administrando datos de personas de estos paises.

Tenemos que implementar:

- Controles de proteccion de datos personales y de proteccion de prevencion de perdida de esos datos
- Seudonomización y cifrado de datos personales
- Capacidad para garantizar confidencialidad, disponibilidad e integridad de nuestra información
- Garantizar resiliencia de los sistemas
- Capacidad para restaurar la disponibilidad de la información

https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en

Diferenciación de la Visión Europea de protección de datos personales, a la visión Norteamericana

Estados unidos y la unión Europea poseen visiones distintas acerca de la protección de los datos. Mientras que por un lado, la Unión Europea se ve influenciada por la Alemania Nazi donde los datos eran usados para poder hacer perfilamientos sobre las personas, en estados Unidos se vio como una manera para poder ayudar al Estado a ejercer sus funciones.

Por ello mientras que en la union europea lo toman como un derecho la protección de los datos de las personas, en estados unidos simplemente se ve como un derecho del consumidor.

Roles, Responsabilidades, Recursos y Criterios para la Gestión de Riesgos de Seguridad Digital

Roles:

- **Líder:** Define la finalidad de tratar los datos. Dice qué deben hacer para establecer sus procesos de negocio.
- **Oficiales de Cumplimiento:** Persona independiente dentro o fuera de la organización que se encarga de evaluar los controles de seguridad y privacidad
- **Responsables y Encargados:** Decide como vamos a tratar los datos personales e identificar los datos que vamos a tratar.

Es importante que tanto el oficial de cumplimiento como el responsable y encargado hallan estado presentes en la etapa de planeación debido a que tienen que tener seguro que los controles se encuentran correctamente implementados y garantizar que los controles se estén haciendo.

Se debe evitar que ambos cargos tengan una persona distinta para que de esa forma puedan darse cuenta de los errores.

La prevención de pérdida de datos, como factor de crecimiento y cumplimiento regulatorio

Cualquiera que quiera hacer negocio con la Union Europea, tendrá que implementar la GDPR para que podamos realizarlo.

El líder es parte fundamental dentro de este proceso.

Debemos clasificar la información y monitorear el flujo de los datos y establecer controles de acceso y/o intercambio. Adicionalmente, es necesario que eliminemos la información que no sea requerida por nuestra empresa.

Además también debemos restringir y controlar de forma automática el acceso a datos personales por parte de terceros no autorizados. Generar alertas automaticas y controles de seguridad de los datos y restaurar la disponibilidad y el acceso a los datos de forma rápida en caso de incidente físico o técnico.