MUST UNIVERSITY
FLORIDA - USA

TECHNOLOGY AND CYBERSECURITY - CYT683 - 2.2

Sistema de gestión de la seguridad de la información

Sistema de gestión de la seguridad de la información

Contenido organizado por **Dallas Morais de Almeida** en 2022 a partir del libro ***Fundamentals of Information Security: based on ISO 27001 and ISO 27002***, publicado en 2018 por Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H.

Objetivos de Aprendizaje

- Comprender el concepto de sistema de gestión de la información.
- Introducir con relación a la implementación de un sistema de seguridad de la información.

Introducción

La seguridad de la información es un elemento imprescindible para que las empresas estén protegidas de las diversas amenazas que existen en el mercado. Desarrollar políticas de seguridad de la información ha sido una estrategia eficaz para que las empresas consigan garantizar que sus datos no se pierdan o adulteren. En esas políticas se establece una serie de actitudes que deben adoptan la organización, colaboradores, proveedores, clientes y los demás involucrados.

El desarrollo de una política de seguridad de la información es una actitud esencial, y dentro de esa política es preciso que haya un sistema de gestión de la seguridad de la información. En ese sistema se abordarán diversos aspectos elementales y específicos de cada proceso organizacional que de alguna forma sea relevante para la empresa en el contexto de la seguridad de la información. El mundo vive una realidad donde las empresas están cada vez más conectadas entre sÍ, siendo así, es importantísimo que haya una gestión adecuada de las informaciones, en el sentido de protegerlas contra las amenazas.

Principales aspectos de la seguridad de la información

El profesor Edison Fuentes, en su libro "*Praticando a Segurança da Informação*", destaca por lo menos diez aspectos elementales que se deben considerar en lo que dice respecto a la seguridad de la información:

1- **No es una cuestión solamente de tecnología:** para que haya un sistema eficaz de protección de la seguridad de la información no basta apenas invertir en soluciones tecnológicas o en equipos de última generación. Es necesario también evaluar y potencializar otros elementos que son tan importantes como la protección tecnológica.

2- **Es una decisión empresarial:** cuando se protege una información, hay una protección del negocio de la empresa. Una empresa puede dejar de existir en caso de que una información extremamente importante sufra algún tipo de daño.

3- **No pasa por milagro:** no adelanta contar con la suerte o tener un pensamiento optimista de que no va a pasar nada. Es necesario invertir recursos, conocimiento y tiempo para obtener un nivel satisfactorio de seguridad de la información.

4- **Debe formar parte de los requisitos del negocio:** una empresa precisa considerar los costos con seguridad de la información en el momento de componer los precios de sus productos o servicios. Seguridad de la información no se puede ver como un elemento trivial, se debe encarar como algo de extrema importancia para la supervivencia del negocio de la empresa.

5- **Exige una postura profesional de las personas:** garantizar la seguridad de la información organizacional requiere que todos estén comprometidos con ella. Para eso es necesario establecer procedimientos, reglas, normas y reglamentos para todos.

6- **Es liberar informaciones apenas para quien precisa:** para proteger la información con eficiencia, solamente el usuario que necesita la información para desempeñar sus funciones puede tener acceso a ellas. En ese sentido, si la información no dice respecto a la actividad de un empleado, no se le debe poner a disposición.

7- **Es implementar el concepto de gestor de la información:** ese concepto dice respecto al efectivo dueño de la información. En ese caso, son los propietarios de la información los que deben establecer quien podrá tener o no tener acceso a las informaciones.

8- **Debe contemplar todos a los colaboradores:** el concepto de colaboradores aquí va más allá de los empleados internos. Terceros, proveedores, clientes, prestadores de servicios, consultores, en fin, todos son colaboradores y se deben comprometer con la seguridad de la información.

9- **Es considerar a las personas como un elemento vital:** el capital humano es fundamental para el desarrollo adecuado de la seguridad de la información en el contexto de la organización. Son las personas las que efectivamente harán con que las cosas sucedan, siendo así, es importantísimo que todos sepan y estén comprometidos con el proceso de seguridad de la información.

10- **Exige alineación con el negocio:** no se puede desempeñar políticas y sistemas de seguridad de la información sin que ellos estén alineados a los objetivos de la empresa, sin embargo, de la misma forma, no es posible desarrollar el negocio de la empresa sin considerar la seguridad de la información..

Sistema de gestión de seguridad de la información

El sistema de gestión de seguridad de la información es un sistema de gestión organizacional, que abarca todos los procesos internos y externos de la empresa, sin embargo, se desarrolla específicamente para proteger las informaciones de la organización.

El desarrollo de un sistema de gestión de seguridad de la información es una tarea compleja, que exige un amplio análisis de la organización. En esos análisis es necesario integrar diversas áreas, equipos, departamentos y conocimientos para que, a través del cambio de conocimientos se establezcan los riesgos, detectando las amenazas y desarrollando las acciones de gestión.

La complejidad de desarrollar un sistema de gestión de la seguridad de la información no se limita apenas al volumen de actividades que se deben ejecutar, sino abarca también la efectiva implementación en la empresa. Es necesario comprender que no adelanta establecer medidas extremamente eficientes en el papel si en el momento de colocarlas en práctica no hay una adherencia por parte de los involucrados. Tampoco adelanta pensar que la seguridad de la información es un elemento separado de las demás áreas.

CONOZCA MÁS

Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática https://www.redalyc.org/articulo.oa?id=378345292002

Definiendo el alcance del sistema de gestión de la seguridad de la información

El establecimiento de un sistema de gestión de la seguridad de la información no sucede de forma aleatoria, pero es bien planificado y demarcado. La empresa debe determinar los límites y funcionalidad del sistema de gestión de la seguridad de la información con el objetivo de definir su alcance. Esa delimitación es extremamente importante y necesaria, pues el alcance es la base para la toma de decisiones con relación al sistema de seguridad.

En el alcance se definen todos los elementos que se deben considerar y contemplar en el sistema de gestión de la seguridad de la información. En el alcance se definen los activos relevantes para el sistema, tales como maquinaria, colaboradores, aliados, tipos de servicios, estructuras, categorización de las informaciones y procesos internos y externos, por ejemplo.

Delimitar el alcance es crucial para un sistema de seguridad de la información, pues cuanto más amplio sea, más complejo es el sistema. Eso significa que el alcance deberá contemplar apenas las cuestiones que realmente son relevantes en lo que dice respecto a la seguridad de la información. No tiene sentido que una organización invierta recursos financieros y de tiempo para desarrollar una serie de medidas que no sean significativas con relación a la protección de la información.

CONOZCA MÁS

ISO 27001 - Seguridad de la Información

https://www.youtube.com/watch?v=BNdPQU32p2Y

En resumen

Las informaciones de la organización son extremamente preciosas y garantizar que ellas se protejan demanda una serie de acciones por parte de las empresas. Para que esas acciones sean realmente efectivas, el cuerpo directivo precisa estar consciente de los aspectos de la seguridad de la información y estar dispuesto a desarrollar un sistema de gestión de la seguridad de la información.

En la punta de la lengua

Referencias Bibliográficas

Fazenda, R., & Fagundes, L. (2015, May). Análise dos desafios para estabelecer e manter sistema de gestão de segurança da informação no cenário brasileiro. In *Anais do XI Simpósio Brasileiro de Sistemas de Informação* (pp. 307-314). SBC.

Fontes, E. (2008). *Praticando a segurança da informação*. Brasport.

Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H. (2018). *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. Brasport.

Martins, A. B., & Santos, C. A. S. (2005). Uma metodologia para implantação de um sistema de gestão de segurança da informação. *JISTEM-Journal of Information Systems and Technology Management*, *2*(2), 121-136.

Libro de referencia:

Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002

Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H.

Brasport, 2018.

MUST UNIVERSITY
FLORIDA - USA

Imagens: Shutterstock