Riesgos de seguridad de la información

MUST UNIVERSITY
FLORIDA - USA

Riesgos de 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 riesgo; amenaza, vulnerabilidad, exposición y contramedida en el contexto de la seguridad de la información.
- Aprender sobre la evaluación de riesgos.

Introducción

En el contexto empresarial es muy importante que las organizaciones estén siempre bien posicionadas en el mercado y ejecutando acciones que les permitan crecer, manteniendo sus capacidades competitivas. Entre los muchos procedimientos adoptados para ese fin, la seguridad de la información se destaca por tener la misión de resguardar todos los datos estratégicos de la empresa. Perder, violar, exponer o adulterar cualquiera de esos datos puede traer enormes pérdidas y perjuicios a la organización. Siendo así, es imprescindible que las empresas estén cada vez más empeñadas en evaluar los riesgos y adoptar acciones de control y protección de datos.

¿Qué es riesgo?

Riesgo es la posibilidad de que un agente amenazador se aproveche de una fragilidad y las consecuencias que los negocios de las empresas pueden sufrir a partir de eso. En lo que dice respecto a la seguridad de la información, el riesgo está constantemente presente y puede tener origen en los más variados lugares:

- Desastres naturales; inundaciones, lluvia de granizo, terremotos, huracanes, etc.
- Accidentes no previstos; incendios, caídas de energía, etc.
- Actos de espionaje.
- Ataques hacker.

Los ejemplos citados anteriormente son apenas algunos de los muchos agentes amenazadores que pueden causar serios daños a las informaciones de la empresa y, consecuentemente, perjuicios al negocio.

Como se dijo, el riesgo sucede cuando el sistema no es totalmente seguro, siendo así, es más probable que las amenazas se concreticen cuando el sistema de seguridad está vulnerable.

¿Qué es amenaza?

Amenaza dice respecto a cualquier persona o cosa que indeseablemente puede explotar las vulnerabilidades del sistema de seguridad de la información. Aquellos que sacan provecho de una fragilidad en el sistema se conocen como agentes amenazadores. Esos agentes amenazadores pueden ser invasores digitales, profesionales no cualificados que no cumplen los protocolos de seguridad, entre otros.

¿Qué es vulnerabilidad?

La vulnerabilidad es el nivel de fragilidad que un sistema de seguridad tiene, siendo, por lo tanto, la puerta de entrada de los agentes amenazadores. Un sistema de seguridad de la información es vulnerable cuando no tiene o no ofrece una protección adecuada contra las amenazas. La vulnerabilidad se puede ejemplificar por la utilización de antivirus desactualizados, *hardwares* sin contraseñas de acceso, falta de sistemas de seguridad físicos (porteros, vigilantes, trancas, etc.) y muchas otras situaciones que facilitan la entrada de un agente amenazador.

¿Qué es exposición?

La exposición es la condición en que una empresa está cuando el agente amenazador consigue explotar las vulnerabilidades del sistema de seguridad y acceder a las informaciones. Cuando sucede eso, la organización queda expuesta a pérdidas, perjuicios, desfalques, etc.

O que é uma contramedida?

Contramedidas son acciones utilizadas para amenizar el riesgo inminente. Las contramedidas se pueden desarrollar de manera preventiva o correctiva, pero tienen la finalidad de fortalecer el sistema de seguridad de la información, para eliminar las vulnerabilidades y reducir la probabilidad de que un agente amenazador acceda a las informaciones.

Entendendo na Prática

Supongamos que una empresa tiene una computadora en el medio de la fábrica con acceso ilimitado a las informaciones de todos los departamentos y la contraseña de entrada está pegada en su monitor. Esa es la ***vulnerabilidad***, la empresa está vulnerable a accesos no autorizados. La ***amenaza*** es un empleado, proveedor, cliente o cualquier persona que se conecta y obtiene informaciones sigilosas. La probabilidad de que una persona no autorizada acceda a las informaciones es el ***riesgo***. En caso de que alguien concretice esa acción, la vulnerabilidad se exploró y la empresa está ***expuesta*** a perjuicios. Una ***contramedida*** que se debería ejecutar en el ejemplo anterior podría ser limitar el acceso de esa computadora a informaciones específicas y no sigilosas.

CONOZCA MÁS

¿En qué consiste el derecho a la protección de datos personales?
https://www.youtube.com/watch?v=-zn6vEbRl0s

Evaluando riesgos de seguridad

Los riesgos pueden tener innumerables fuentes y, para que una organización pueda establecer un proceso robusto de seguridad de la información, es necesario que ella sepa como evaluar esos riesgos. Esa evaluación tiene como objetivo la identificación, dimensionamiento y ranking de los riesgos según los objetivos de la empresa.

La evaluación de los riesgos se debe analizar con periodicidad para ajustar los posibles cambios del proceso de seguridad de la información. Esas evaluaciones de riesgos deben suceder de forma disciplinada y tener la capacidad de indicar resultados pasibles de cotejo y multiplicación.

Análisis de riesgos

El propósito de elaborar un análisis de riesgos es elucidar cuales son las amenazas significativas para los procesos de la operación y detectar cuales son los riesgos pertinentes. Una vez que se haya hecho el análisis de riesgos, es posible definir el tipo de acción necesaria para garantizar la seguridad de la información. Los análisis de riesgos también tienen el papel de hacer con que las medidas a adoptar para la garantía de la seguridad de la información sean económicamente viables.

Ponderando que la seguridad es la capacidad de resistir a daños y que las amenazas potenciales son constantes, perseverantes, mutables e innovadoras, las organizaciones precisan considerar que el nivel de seguridad de sus sistemas puede variar todos los días. Siendo así, los análisis de riesgos se precisan actualizar constantemente para evitar procesos obsoletos e ineficientes.

Los cuatro objetivos principales de un análisis de riesgos son:

1- Definir y establecer el costo de cada activo de la organización

2- Establecer las vulnerabilidades y amenazas

3- Especificar el riesgo de que una amenaza pase a ser real y comprometa los procesos de operación

4- Determinar la relación entre los costos de un daño y los costos de las acciones proyectivas, buscando un equilibrio entre los dos.

Análisis cuantitativo del riesgo

Analizar de forma cuantitativa un riesgo tiene como objetivo el cálculo del nivel de la pérdida monetaria y la probabilidad de que una amenaza se concretice, teniendo por base el efecto del riesgo. En otras palabras, el análisis cuantitativo del riesgo busca definir los perjuicios financieros que una organización tendría con el suceso de un incidente y también la probabilidad de que ese incidente suceda.

En el análisis cuantitativo de los riesgos, los gestores buscan atribuir los valores de cada proceso, insumo, estructura, herramientas, en fin, todo lo que dice respecto a las operaciones de la empresa. Una vez que se hayan establecido esos valores, es posible entonces determinar el riesgo del agujero financiero de forma clara y objetiva.

Aunque sea un tipo de evaluación directa y transparente de los riesgos, los análisis cuantitativos no son cien por ciento precisos, pues es prácticamente imposible medir y dar valor al impacto de todos los tipos de información que una empresa posee.

Análisis cualitativo del riesgo

El análisis cualitativo del riesgo difiere del cuantitativo en el sentido de no establecer cálculos financieros de posibles pérdidas, sino por evaluar las distintas circunstancias y probabilidades de riesgo, clasificando la magnitud de las amenazas y la eficacia de las probables contramedidas. Este tipo de análisis no se basa en las ciencias exactas, sino en el buen sentido y vivencia de la organización.

Para desarrollar el análisis cualitativo de los riesgos es necesario, por lo tanto, que las personas involucradas tengan vivencia organizativa y conocimiento de las amenazas que se deben evaluar. En este tipo de análisis se consulta al grupo con relación a una hipótesis de amenaza y los potenciales perjuicios y cada participante da su opinión con relación a la probabilidad de suceso y las dimensiones del daño, teniendo como base su experiencia e instinto.

En Resumen

En esta clase usted conoció los conceptos de riesgo, amenaza, vulnerabilidad, exposición y contramedida, además pudo verificar la importancia de evaluar los riesgos de la seguridad de la información y aplicar esa evaluación.

Identificar los riesgos es una acción fundamental para que la seguridad de las informaciones esté garantizada. Es necesario, por lo tanto, que las organizaciones se empeñen en desarrollar métodos de análisis eficaces para conseguir establecer procesos eficientes de seguridad de datos. Los daños asociados a una violación de la seguridad pueden ser incalculables y, por eso, evaluar con cuidado *y de forma metódica* cada riesgo constituye acciones que garantizan la estabilidad y supervivencia de la empresa en el mercado.

En la punta de la lengua

Referencias Bibliográficas

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

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