UNIVERSIDAD DEL CENTRO DEL BAJIO.

LICENCIATURA EN SISTEMAS COMPUTACIONALES.

TÍTULO:

“ANALISIS DE RIESGOS VS ADMINISTRACION DE RIESGOS”.

MATERIA:

SEGURIDAD INFORMATICA.

DOCENTE:

FILIBERTO DURAN GARCIA.

PRESENTA

PABLO SÁNCHEZ UGALDE.

Celaya, Guanajuato , 23 de Febrero del año 2019.

Análisis de riesgos vs administración de riesgos.

El primer paso en la Gestión de riesgo es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

La clasificación de datos tiene el propósito de garantizar la protección de datos (personales) y significa definir, dependiendo del tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso a los datos e informaciones. Considerando el contexto de nuestra misión institucional, tenemos que definir los niveles de clasificación como por ejemplo: confidencial, privado, sensitivo y público. Cada nivel define por lo menos el tipo de persona que tiene derecho de acceder a los datos, el grado y mecanismo de autenticación.

Una vez clasificada la información, tenemos que verificar los diferentes flujos existentes de información internos y externos, para saber quienes tienen acceso a que información y datos.

Clasificar los datos y analizar el flujo de la información a nivel interno y externo es importante, porque ambas cosas influyen directamente en el resultado del análisis de riesgo y las consecuentes medidas de protección. Porque solo si sabemos quienes tienen acceso a que datos y su respectiva clasificación, podemos determinar el riesgo de los datos, al sufrir un daño causado por un acceso no autorizado.

La valoración del riesgo basada en la formula matemática

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

Para la presentación del resultado (riesgo) se usa una gráfica de dos dimensiones, en la cual, el eje-x (horizontal, abscisa) representa la “Probabilidad de Amenaza” y el eje-y (vertical, ordenada) la “Magnitud de Daño”. La Probabilidad de Amenaza y Magnitud de Daño pueden tomar condiciones entre Insignificante (1) y Alta (4). En la practica no es necesario asociar valores aritméticos a las condiciones de las variables, sin embargo facilita el uso de herramientas técnicas como hojas de calculo.

Se habla de un Ataque, cuando una amenaza se convirtió en realidad, es decir cuando un evento se realizó. Pero el ataque no dice nada sobre el éxito del evento y sí o no, los datos e informaciones fueron perjudicado respecto a su confidencialidad, integridad, disponibilidad y autenticidad.

Estimar la Magnitud de Daño generalmente es una tarea muy compleja. La manera más fácil es expresar el daño de manera cualitativa, lo que significa que aparte del daño económico, también se considera otros valores como daños materiales, imagen, emocionales, entre otros. Expresarlo de manera cuantitativa, es decir calcular todos los componentes en un solo daño económico, resulta en un ejercicio aun más complejo y extenso.

REFERENCIAS.

7. ANÁLISIS DE RIESGO

En el texto: ("7. Análisis de Riesgo", 2019)

Bibliografía: 7. Análisis de Riesgo. (2019). Retrieved from https://protejete.wordpress.com/gdr_principal/analisis_riesgo/