Gestión de Riesgos

Transcribed on July 5, 2025 at 1:16 PM by Minutes AI

Speaker 1 (00:03)

Bienvenidos a esta nueva sesión donde vamos a hablar de la ISO 27001 y el Análisis y Gestión del Riesgo.

En esta sesión lo que vamos a trabajar es definir qué es la ISO 26001 como estándar, como norma, lo que proporciona una organización.

Vamos a definir lo que es un sistema gestor de Seguridad de información, lo que nos aporta, lo que puede aportarnos dentro de la organización y vamos a hablar también del concepto de Evaluación y Análisis de riesgo.

Este concepto es importante porque es una de las herramientas fundamentales a la hora de poder medir en qué estado nos encontramos dentro de la parte del ciclo de seguridad.

Al final tenemos que entender que la seguridad es un proceso totalmente cíclico.

Esto son herramientas que nos permiten poder evaluar, medir cómo estamos en un momento determinado y poder mejorar en caso de necesidad.

Además, estudiaremos también conceptos básicos acerca de la evaluación del riesgo.

Vamos a comenzar hablando de lo que es la ISO 27001.

La ISO 27001 es una norma que nos va a permitir, va a especificar los requisitos que debemos que debemos cumplir para establecer, para poder implantar, para poner en funcionamiento, para controlar, para revisar, para mantener y poder mejorar un sistema gestor de seguridad de información totalmente documentado dentro del contexto que nos encontramos en una organización de negocio o diferentes tipos de riesgos.

Al final, si nos damos cuenta, la ISO 27001 lo que nos aporta es una gestión de riesgos más una mejora continua.

Si nos damos cuenta, la seguridad de información es un proceso en el cual necesitamos gestionar, identificar y gestionar los riesgos a los que nos enfrentamos como organización y poder disponer de herramientas que nos permitan medir en qué momento estamos, si estamos mejor o estamos peor en cuanto a seguridad para poder tomar decisiones y poder invertir lo adecuado en caso de necesidades de tener que mejorar la seguridad de la empresa.

Bien, si queremos hablar también de, por ejemplo, el sistema gestores de seguridad de información, podemos decir que este sistema es un framework, es una especie de marco de trabajo que está compuesto de personas, está compuesto de salvaguardas, controles, protecciones, por así decirlo, está compuesto también de documentación políticas en un proceso en el que se busca continuamente la mejora de la protección de la confidencialidad, la integridad y la disponibilidad de la información.

Es decir, un SGSI al final es un sistema en el cual participan personas, participan procesos, participa en documentación políticas y todo ello lo que busca es mejorar la seguridad para proteger la conciencia, la integridad y la disponibilidad de la información.

Si entendemos esto, veremos que USGSI no es una aplicación al uso, sino un SGSI es un conjunto de herramientas donde participan personas, donde habrá documentación, donde habrá procesos, habrá procedimientos con el objetivo de mejorar la seguridad, que es el objetivo constante de una organización.

¿Cómo se consigue esa mejora?

Pues a través de implantar controles, hacer un seguimiento de esos controles.

Los controles al final vamos a llamarlos salvaguardas o protecciones.

Implantaremos controles, haremos un seguimiento de controles, haremos una auditoría Pentest, en el futuro podemos llamarlos hacia Kinetic, podemos llamarlos de diferentes maneras.

Haremos auditoría a esos controles y decidiremos si tenemos que mejorar esos controles en algún momento.

Aquí tenéis una imagen donde se puede ver un poco la definición de la política de seguridad en el paso inicial, la definición del ámbito del sistema gestor de seguridad de información y fijaros cómo hay una evaluación 1 Gestión del riesgo.

Es un proceso fundamental dentro de un SGSI, esa identificación de riesgos, ese análisis, esa gestión, esa evaluación para poder seleccionar controles después controles son salvaguarda, son protecciones y poder aplicarlos en caso de necesidad para mejorar la seguridad a nivel global.

Esto veremos un poco más después.

Vamos a ir ahora con el análisis de riesgos.

Vamos dentro del capítulo apartado de evaluación del riesgo.

Un análisis de riesgos intenta que los criterios en los que vamos a apoyar sean lo más objetivo posible.

Para ello vamos a tener una parte donde vamos a identificar esos riesgos, vamos a ver a través de los riesgos, vamos a intentar llevar a cabo esa gestión y nos va a permitir apoyarnos para tomar decisiones en caso de que tengamos que solventar dichos riesgos.

¿Qué nos va a permitir el análisis de riesgos?

Lo que acabo de comentar un poco en resumen, identificar los diferentes riesgos a los que estamos expuestos simplemente por el hecho de existir o de una actividad de negocio en Internet, cómo podría afectar también dichas amenazas o qué impacto pueden tener dichas amenazas o dichos riesgos que estamos identificando en el caso de llevarse a cabo, de materializarse.

Eso también lo vamos a identificar con el análisis de riesgo.

Y podemos decir también que nos aporta la posibilidad de tomar decisiones en cuanto sepamos si tenemos que mejorar la seguridad o no tenemos que mejorar la seguridad.

Es decir, tenemos los elementos, las características adecuadas para poder tomar decisiones.

¿Gracias a este análisis evaluación del riesgo podemos tomar decisiones de tengo que mejorar los controles?

¿Tengo que mejorar las protecciones?

¿Tengo que invertir en seguridad?

Entonces, haciendo un breve resumen de todo esto, lo que es la evaluación y el análisis del riesgo es una herramienta, un proceso que nos permite identificar los riesgos a los que estamos expuestos, poder medir si ese riesgo tiene un impacto grave contra mi organización, poder tomar la decisión de qué controles tengo que aplicar, esos controles me permitirán mitigar ese impacto, en el caso de que ese riesgo se materialice tendremos un nuevo valor para ese riesgo y si tenemos que mejorar en algún momento esa inversión en esos controles en esas protecciones para poder llevarla a cabo, mejorar.

Y como se puede entender, es un cíclico, es un proceso totalmente cíclico.

Volveremos a identificar riesgos, volveremos a evaluar cómo se encuentra ese riesgo respecto al control de los controles que tenemos aplicados, volveremos iterar de nuevo en un proceso totalmente cíclico.

Esto nos lo permite el análisis de riesgos y es una herramienta fundamental dentro de un sistema gestor de seguridad de la información.

Bien, vamos a pasar al apartado de conceptos básicos acerca de la evaluación del riesgo.

Tenemos el primer concepto que vamos a estudiar, es el Minasset.

¿Qué es un activo?

Es cualquier cosa que tenga un valor para la organización.

Por ejemplo, puede ser un servicio que tengamos montado dentro de la organización, una página web, un servidor web, puede ser un sistema de información, también podría ser un recurso con valor para organización, es decir, cualquier información, cualquier servicio, cualquier elemento dentro de la organización que tenga un valor.

Tenemos también el concepto de riesgo.

El riesgo para nosotros va a ser la probabilidad de que se produzca un impacto en un activo, por ejemplo.

Es decir, es la probabilidad de que ocurra o que se materialice una amenaza contra un activo, eso supone un impacto.

Es verdad que el impacto puede provocar un daño de varias maneras, pero en el momento que se materializa un riesgo sufriremos un impacto.

La probabilidad de que ocurra también es importante, tenemos que tenerla en cuenta.

Como valor tenemos la evaluación del riesgo.

Aquí tenemos la protección.

La protección al final pues es un salvaguarda o control, se puede llamar de varias maneras, es un elemento, un elemento que va a disminuir el impacto, que tiene un riesgo en caso de materializarse.

Es decir, yo tengo un riesgo identificado sobre un activo, yo coloco una salvaguarda, lo que estoy haciendo es disminuir la probabilidad de ocurrencia o disminuir el impacto que va a tener ese riesgo en caso de materializarse gracias a esa salvaguarda.

De forma que estamos generando como dos tipos de tengo un riesgo inicial, yo le aplico un control a ese riesgo inicial, el riesgo disminuirá, ya sea en probabilidad de ocurrencia o ya sea impacto y tendría un riesgo secundario, un riesgo residual que veremos.

Entonces, el control o protección es un elemento fundamental y es al final, si lo llevamos al plano de ácido de Segovia, pues podemos decir que hablamos de un firewall, un IPS, un antivirus, es decir, si tenemos un antimabuen en el sistema, en caso de tener una infección, el impacto seguramente sea menor que si no tenemos el antimabue.

Entonces estamos viendo cómo, llevándolo a un plano más práctico, cómo disminuye ese impacto de la amenaza.

Vamos a pasar al siguiente.

Tenemos el concepto de riesgo potencial.

Y el riesgo residual, lo he comentado antes un poco por encima, el riesgo potencial es el riesgo que identificamos sobre un activo antes de que apliquemos un control, una salvaguarda, una protección o un conjunto de salvaguardas.

Y en riesgo residual es el riesgo resultante.

Tengo un riesgo identificado, le aplico un control, una protección o varias, el riesgo disminuye y ese es el riesgo residual.

Los valores de riesgo se pueden identificar de manera cuantificativa o cualitativa.

Entonces eso para el análisis lo podemos hacer de diferente manera.

El concepto de Evaluación del Riesgo, al final es todo este proceso que estamos comentando, estamos identificando y estamos llevando a cabo esa evaluación, midiendo con los controles, viendo el riesgo inicial, el riesgo final y llevando a cabo el impacto, la probabilidad de ocurrencia que llevaría a cabo esa amenaza en caso de materializarse.

Por último, el concepto de amenaza.

Concepto de amenaza lo podemos definir como una situación que puede provocar un incidente de seguridad.

Lógicamente esas situaciones producen daños a los activos.

Un ejemplo podría ser un empleado, un insider, que ya es un concepto que hemos visto, que consigue acceso a cierta información, la roba y la vende en un mercado negro, por ejemplo, en un mercado.

Bien, pues ahí tendríamos una amenaza.

Otra amenaza podría ser una vulnerabilidad que tengo en el sistema, alguien externo, un atacante externo, me explota esa vulnerabilidad, un error, otra amenaza que puede ocurrir.

Bien, como conclusiones, esta sesión hemos tratado el sistema gestor de seguridad de información definido, recordar el marco de trabajo donde tenemos personas, documentos, procedimientos que están de forma cíclica trabajando para proteger la confidencialidad, la disponibilidad, la integridad de la información.

La evaluación del riesgo, recordamos, identificamos riesgos sobre activos de la organización, tenemos un riesgo potencial, riesgo inicial, aplicamos controles, salvaguardas, protecciones, disminuimos ese riesgo extra, un riesgo residual, tendremos que ver si ese riesgo es aceptable por la organización.

Si aceptamos ese mínimo riesgo, recordad que la seguridad 100 % no va a existir, con lo cual habrá un valor de riesgo umbral que se llama, que se acepta y que es el que tenemos que definir en esa evaluación del riesgo.

Y luego el análisis de riesgo nos permite medir la eficiencia de nuestras inversiones en seguridad.

Al final las empresas invierten en seguridad y este análisis de riesgo y evaluación del riesgo lo que hacemos son procesos que nos permiten identificar, medir cómo eficiente y eficaz está siendo este proceso y si tenemos que mejorar.

El análisis y evaluación del riesgo es la herramienta que utiliza un sistema gestor de seguridad de información para poder retroalimentarse y poder saber en qué momento nos encontramos en términos de seguridad en la organización.

1 SGSI, al final es el objetivo de la norma ISO 27001 nos indica, nos especifica qué requisitos debemos cumplir para poder implantar este tipo de sistemas.

Bien, con esto finalizamos la sesión.

Espero que es una temática más de seguridad de información, no de ciber, pero fijaros cómo tiene una rama donde en el momento que empezamos a hablar de protecciones, en el momento que empezamos a ver cómo medir esos controles, entrará la parte de ciberseguridad.

Ahí empezamos a hilarlo.

La seguridad de información tiene una rama que es ciberseguridad y empezamos a hilar, empezamos a hilar toda esa parte de ciberseguridad me permite medir la eficiencia y eficacia de los controles para evitar riesgos.

Y ahí es donde empezamos a ver la importancia de la ciberseguridad desde el punto de vista técnico.

Hay un hilo conductor donde se juntan los dos mundos, lógicamente, y es justamente en este punto.

Nos vemos en la siguiente sesión.