ANALISIS DE RIESGOS EN SISTEMAS

Unidad I: Análisis y gestión de riesgos

Objetivo específico 1: El alumno aprenderá como analizar y gestionar el riesgo así como debe de tratar los riesgos evaluando las situaciones a las que se enfrenta realizando una auditoria y acreditación del riesgo en sistemas

.

Conceptos a desarrollar en la unidad: Introducción al análisis y gestión de riesgos, el análisis y tratamiento de los riesgos, evaluación, certificación, auditoría y acreditación de los riesgos.

TEMA 1. ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

Introducción

El uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios.

La gestión de los riesgos es una piedra angular en las guías en una organización, pública o privada, donde se considera un principio fundamental que las decisiones de empresa y se fundamenten en el conocimiento de los riesgos que implican:

Se insiste recurrentemente en el necesario equilibrio entre riesgos y oportunidades para tomar las mejores decisiones.

En pocas palabras, la gestión de los riesgos es nuclear a la dirección de las organizaciones. En particular, los riesgos que tienen su origen en el uso de tecnologías de la información deben trasladarse a los órganos de dirección y contextualizarse en la misión de la organización.

El conocimiento de los riesgos permite calibrar la confianza en que los sistemas desempeñarán su función como la Dirección espera, habilitando un marco equilibrado de Dirección, Gestión de Riesgos y Cumplimiento (GRC), tres áreas que deben estar integradas y alineadas para evitar conflictos, duplicación de actividades y zonas de nadie.

1.1 Introducción al análisis y gestión de riesgos

Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que compro metan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.[5]

El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

Disponibilidad:

Es la disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad:

Es el mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad:

Es que la información llegue solamente a las personas autorizadas. Contra la

confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que nos acerquen a la percepción de los usuarios de los sistemas de información:

Autenticidad:

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

Trazabilidad:

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual que haya que poner medios y esfuerzo para conseguirlas. A racionalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición:

Riesgo:

Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema:

Análisis de riesgos:

proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Sabiendo lo que podría pasar, hay que tomar decisiones:

Tratamiento de los riesgos

proceso destinado a modificar el riesgo.

Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (típicamente contratando un servicio o un seguro de cobertura), o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.

Nótese que una opción legítima es aceptar el riesgo. Es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio. Es más, a veces aceptamos riesgos operacionales para acometer actividades que pueden reportarnos un beneficio que supera al riesgo, o que tenemos la obligación de afrontar. Es por ello que a veces se emplean definiciones más amplias de riesgo:

Como todo esto es muy delicado, no es meramente técnico, e incluye la decisión de aceptar un cierto nivel de riesgo, deviene imprescindible saber en qué condiciones se trabaja y así poder ajustar la confianza que merece el sistema. Para ello, qué mejor que una aproximación metódica que permita tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.

1.2 El análisis y el tratamiento de los riesgos en su contexto

Las tareas de análisis y tratamiento de los riesgos no son un fin en sí mismas sino que se encajan en la actividad continua de gestión de la seguridad.

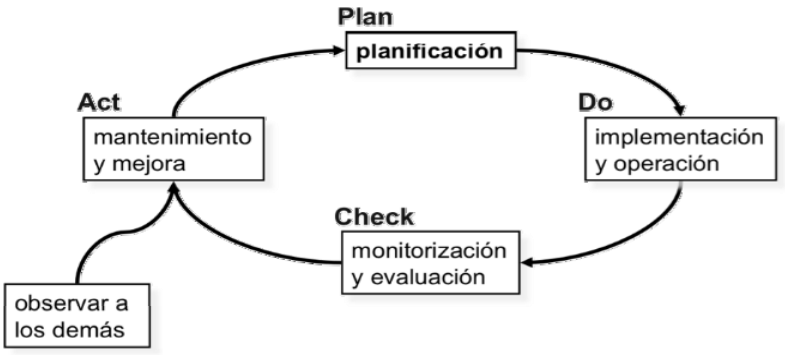
El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos.

La implantación de las medidas de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con el sistema de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

Este esquema de trabajo debe ser repetitivo pues los sistemas de información rara vez son inmutables; más bien se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto.

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento. La fase de tratamiento estructura las acciones que se acometen en materia de seguridad para satisfacer las necesidades detectadas por el análisis.

Los sistemas de gestión de la seguridad de la información (SGSI) formalizan cuatro etapas cíclicas:



Ciclo PDCA

El análisis de riesgos es parte de las actividades de planificación, donde se toman decisiones de tratamiento. Estas decisiones se materializan en la etapa de implantación, donde conviene desplegar elementos que permitan la monitorización de las medidas desplegadas para poder evaluar la efectividad de las mismas y actuar en consecuencia, dentro de un círculo de excelencia o mejora continua.

Concienciación y formación

El mejor plan de seguridad se vería seriamente hipotecado sin una colaboración activa de las personas involucradas en el sistema de información, especialmente si la actitud es negativa, contraria a las medidas, o tienen la percepción de pasarse el día “luchando contra las medidas de seguridad”. Es por ello que se requiere la creación de una “cultura de seguridad” que, emanando de la alta dirección, conciencie a todos los involucrados de su necesidad y pertinencia.

Son tres los pilares fundamentales para la creación de esta cultura:

- una política de seguridad corporativa que se entienda (escrita para los que no son expertos en la materia), que se difunda y que se mantenga al día
- una normativa se seguridad que, entrando en áreas específicas de actividad, aclare la postura de la Organización; es decir, defina lo que es uso correcto y lo que es incumplimiento
- una formación continua a todos los niveles, recordando las cautelas rutinarias y las actividades especializadas, según la responsabilidad adscrita a cada puesto de trabajo

A fin de que estas actividades cuajen en la organización, es imprescindible que la seguridad sea:

- mínimamente intrusiva: que no dificulte innecesariamente la actividad diaria ni hipoteque alcanzar los objetivos de productividad propuestos,
- sea "natural": que no de pie a errores gratuitos[6], que facilite el cumplimiento de las buenas prácticas propuestas y
- practicada por la Dirección: que dé ejemplo en la actividad diaria y reaccione con presteza a los cambios e incidencias.

Incidencias y recuperación

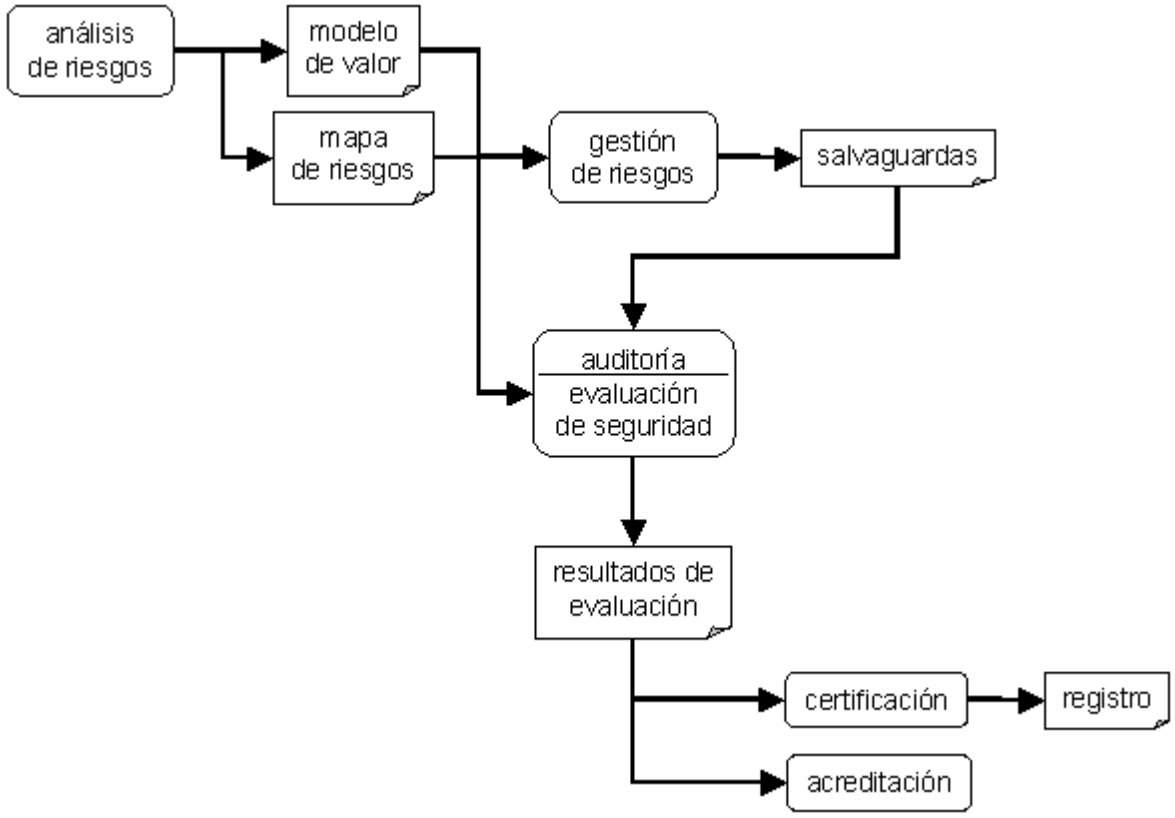
Las personas involucradas en la utilización y operación del sistema deben ser conscientes de su papel y relevancia continua para prevenir problemas y reaccionar cuando se produzcan. Es importante crear una cultura de responsabilidad donde los potenciales problemas, detectados por los que están cercanos a los activos afectados, puedan ser canalizados hacia los puntos de decisión. De esta forma el sistema de seguridad responderá con presteza a las circunstancias de cada momento.

Cuando se produce una incidencia, el tiempo empieza a correr en contra del sistema: su supervivencia depende de la agilidad y corrección de las actividades de reporte y reacción. Cualquier error, imprecisión o ambigüedad en estos momentos críticos, se ve amplificado convirtiendo lo que podía ser un mero incidente en un desastre.

Conviene aprender continuamente, tanto de los éxitos como de los fracasos, e incorporar lo que vamos aprendiendo al proceso de gestión de riesgos. La madurez de una organización se refleja en la pulcritud y realismo de su modelo de valor y, consecuentemente, en la idoneidad de las salvaguardas de todo tipo, desde medidas técnicas hasta una óptima organización.

1.3 Evaluación, certificación, auditoría y acreditación

El análisis de riesgos es una piedra angular de los procesos de evaluación, certificación, auditoría y acreditación que formalizan la confianza que merece un sistema de información. Dado que no hay dos sistemas de información iguales, la evaluación de cada sistema concreto requiere amoldarse a los componentes que lo constituyen. El análisis de riesgos proporciona una visión singular de cómo es cada sistema, qué valor posee, a qué amenazas está expuesto y de qué salvaguardas se ha dotado. Es pues el análisis de riesgos paso obligado para poder llevar a cabo todas las tareas mencionadas, que se relacionan según el siguiente esquema:



Contexto de certificación y acreditación de sistemas de información

En esta sección se hace una presentación conceptual de las actividades citadas.

Evaluación

Es cada vez más frecuente la evaluación de la seguridad de los sistemas de información, tanto internamente como parte de los procesos de gestión, como por medio de evaluadores independientes externos. Las evaluaciones permiten medir el grado de confianza que merece o inspira un sistema de información.

Certificación

La evaluación puede llevar a una certificación o registro de la seguridad del sistema. En la práctica se certifican productos y se certifican sistemas de gestión de la seguridad. La certificación de productos es, de alguna forma, impersonal: "esto tiene estas características técnicas". Sin embargo, la certificación de sistemas de gestión tiene que ver con el "componente humano" de las organizaciones buscando el análisis de cómo se explotan los sistemas[7].

Certificar es asegurar responsablemente y por escrito un comportamiento. Lo que se certifica, producto o sistema, se somete a una serie de evaluaciones orientadas por un objetivo ¿para qué lo quiere?[8]. Un certificado dice que un sistema es capaz de proteger unos datos de unas amenazas con una cierta calidad (capacidad de protección). Y lo dice en base a que ha observado la existencia y el funcionamiento de una serie de salvaguardas. Es decir que detrás de un certificado no hay sino los conceptos de un análisis de riesgos.

Antes de proceder a la certificación, debe haberse realizado un análisis de riesgos a fin de conocer los riesgos y de controlarlos mediante la adopción de los controles adecuados, además, será un punto de control de la gestión del producto o sistema.

Acreditación

Algunas certificaciones tienen como objetivo la acreditación del producto o sistema. La acreditación es un proceso específico cuyo objetivo es legitimar al sistema para formar parte de sistemas más amplios. Se puede ver como una certificación para un propósito específico.

Auditorías

Aunque no sea lo mismo, no están muy lejos de este mundo las auditorías, internas o externas, a las que se someten los sistemas de información

- unas veces requeridas por ley para poder operar en un cierto sector (cumplimiento),
- otras veces requeridas por la propia Dirección de la Organización,
- otras veces requeridas por entidades colaboradoras que ven su propio nivel de riesgo ligado al nuestro.

Una auditoría puede servirse de un análisis de riesgos que le permita (1) saber qué hay en juego, (2) saber a qué está expuesto el sistema y (3) valorar la eficacia y eficiencia de las salvaguardas.

Frecuentemente, los auditores parten de un análisis de riesgos, implícito o explícito, que, o bien realizan ellos mismos, o bien lo auditan. Siempre en la primera fase de la auditoría, pues es difícil opinar de lo que no se conoce. A partir del análisis de riesgos se puede analizar el sistema e informar a la gerencia de si el sistema está bajo control; es decir, si las medidas de seguridad adoptadas están justificadas, implantadas y monitorizadas, de forma que se puede confiar en el sistema de indicadores de que dispone la gerencia para gestionar la seguridad de los sistemas.

La conclusión de la auditoría es un informe de insuficiencias detectadas, que no son sino incoherencias entre las necesidades identificadas en el análisis de riesgos y la realidad detectada duran- te la inspección del sistema en operación.

Las auditorías deben repetirse regularmente tanto para seguir la evolución del análisis de riesgos (que se debe actualizar regularmente) como para seguir el desarrollo del plan de seguridad determinado por las actividades de gestión de riesgos.

1.4 ¿Cuándo procede analizar y gestionar los riesgos?

Un análisis de riesgos TIC es recomendable en cualquier Organización que dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión. En particular en cualquier entorno donde se practique la tramitación electrónica de bienes y servicios, sea en contexto público o privado. El análisis de riesgos permite tomar decisiones de gestión y asignar recursos con perspectiva, sean tecnológicos, humanos o financieros.

El análisis de riesgos es una herramienta de gestión que permite tomar decisiones. Las decisiones pueden tomarse antes de desplegar un servicio o con éste funcionando. Es muy deseable hacerlo antes, de forma que las medidas que haya que tomar se incorporen en el diseño del servicio, en la elección de componentes, en el desarrollo del sistema y en los manuales de usuario. Todo lo que sea corregir riesgos imprevistos es costoso en tiempo propio y ajeno, lo que puede ir en detrimento de la imagen prestada por la Organización y puede suponer, en último extremo, la pérdida de confianza en su capacidad. Siempre se ha dicho que es mejor prevenir que curar y aquí se aplica: no espere a que un servicio haga agua; hay que prever y estar prevenido.

Realizar un análisis de riesgos es laborioso y costoso. Levantar un mapa de activos y valorarlos requiere la colaboración de muchos perfiles dentro de la Organización, desde los niveles de gerencia hasta los técnicos. Y no solo es que haya que involucrar a muchas personas, sino que hay que lograr una uniformidad de criterio entre todos pues, si importante es cuantificar los riesgos, más importante aún es relativizarlos. Y esto es así porque típicamente en un análisis de riesgos aparecen multitud de datos. La única forma de afrontar la complejidad es centrarse en lo más importante (máximo impacto, máximo riesgo) y obviar lo que es secundario o incluso despreciable. Pero si los riesgos no están bien ordenados en términos relativos, su interpretación es imposible.

En resumen, que un análisis de riesgos no es una tarea menor que realiza cualquiera en sus ratos libres. Es una tarea mayor que requiere esfuerzo y coordinación. Por tanto debe ser planificada y justificada.

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

En conclusión

Procede analizar y gestionar los riesgos cuando directa o indirectamente lo establezca un precepto legal y siempre que lo requiera la protección responsable de los activos de una organización.