Universidad Nacional Autónoma de México

Facultad de Estudios Superiores Aragón

Administración de la Seguridad de la Información

TESIS

Para obtener el grado de Ing. Mecánico Electricista

Autor: José Daniel Ramos Guzmán

Asesor: Ing. Narciso Acevedo Hernández

México, D.F. 2013

Contenido

Justificación

En la actualidad la mayoría de las organizaciones (privadas o de gobierno) han tenido o tendrán algún problema de seguridad que podría ser la perdida, robo o modificación de información no autorizada así como la falta de disponibilidad de algún servicio que requiera un usuario, el clásico "No hay sistema".

Muchas organizaciones no toman en cuenta que la seguridad de esta información (activo*), ya sea almacenada de manera física y/o lógica, debe ser resguardada con la aplicación de controles que mantengan la confidencialidad e integridad* de estos activos para que la misión de la organización sea llevada con éxito.

Además la Seguridad de la Información toma en cuenta que no todos los riesgos de seguridad están relacionados con la tecnología de la información.

¿Cómo es esto? La mayor parte de problemas en cuestiones de Seguridad Informática son causados por personal interno o por el mismo usuario, ya sea por falta de conocimiento, descuido, falta de pericia o ingeniería social.

Todas estas problemáticas son tomadas en cuenta al momento de realizar la "Administración de la Seguridad de la Información" por lo que es necesario que las organizaciones tengan al personal adecuado para la realización de todo el proceso de fortalecimiento, seguimiento y actualización de la infraestructura y sistemas de información en materia de seguridad.

La inquietud de realizar esta tesis titulada "Administración de la Seguridad de la Información" es con el fin de tener una herramienta que brinde el conocimiento de los pasos básicos necesarios que se deben realizar al momento de estar al frente de una organización como personal de seguridad informática.

Objetivos

Objetivo General

Dar a conocer a usuarios con poca experiencia en materia de seguridad de la información los diferentes elementos que constituyen la Administración de la Seguridad de la Información visto desde una perspectiva muy general, tomando en cuenta que el lector quisiera no entrar en detalles técnicos de todo lo que constituye la Administración de la Seguridad.

Objetivo. Panorama Actual e Importancia de la Seguridad de la Información

Crear conciencia de las problemáticas actuales que viven las organizaciones Privadas y de Gobierno en materia de seguridad de la información además de los tipos de ataques y hackers famosos y sus hazañas para tener un panorama de las vulnerabilidades explotadas y con esto concientizar al lector acerca de la importancia que tiene la Seguridad de la Información no solo para las Organizaciones, sino también a nivel de usuario.

Objetivo. Análisis y Evaluación de Riesgos

Dar a conocer una forma de identificar, analizar y evaluar los riesgos de seguridad en una Organización basándose en la misión y sus políticas de seguridad.

Objetivo. Implementación de Controles de Seguridad

Conocer referencias que ayuden con la implementación de controles de seguridad para la mitigación de riesgos en los que la organización se vea involucrada.

Objetivo. Poniendo a Prueba los Controles

Identificar pruebas que ayuden con el monitoreo y seguimiento de los controles implementados para realizar las acciones preventivas o correctivas correspondientes para el fortalecimiento del sistema de Administración de la Seguridad de la Información.

Introducción

La información electrónica y los sistemas automatizados son esenciales para casi todas las operaciones de organizaciones públicas y privadas. Si las Organizaciones no pueden proteger la disponibilidad, integridad y, en algunos casos, la confidencialidad de esta información, su capacidad para llevar a cabo sus misiones y objetivos se verá seriamente afectada. Sin embargo, a pesar de la enorme dependencia de la información y de los sistemas electrónicos, las auditorías siguen revelando serias debilidades en la seguridad de la información.

Como resultado, miles de millones de pesos en recursos están en riesgo de pérdida, grandes cantidades de datos sensitivos están en riesgo de divulgación no autorizada y las operaciones críticas se vuelven vulnerables a perturbaciones graves.

Los sectores gubernamentales al igual que muchas organizaciones del sector privado están empezando a reconocer la importancia de los riesgos y comienzan a apreciar plenamente la importancia de proteger sus recursos de información. La apertura del problema de la seguridad de la información, coloca a la administración de seguridad de la información en el contexto de otras cuestiones de administración de información de tecnológica.

A pesar de que se ha utilizado la tecnología desde hace años, las organizaciones en todo el mundo están experimentando una explosión en el uso de los datos electrónicos y sistemas informáticos conectados en redes. Como resultado, las Organizaciones se han vuelto enormemente dependientes de estos sistemas y datos para apoyar sus operaciones.

Las redes que son utilizadas en las Organizaciones mayormente se utilizan para el intercambio de mensajes electrónicos por los cuales igualmente se envía información, obtener datos de sitios remotos y mantener registros críticos. Cada vez existe más dependencia a la automatización de actividades que a menudo se interconectan con sistemas con salida a Internet para apoyar sus operaciones.

A pesar de que la tecnología promete agilizar las operaciones y mejorar la prestación de los servicios, también exponen estas actividades a mayores riesgos. Esto se debe a que los sistemas automatizados están reemplazando rápidamente a los procedimientos manuales y a los documentos en papel que en muchos casos ya no están disponibles como "copia de seguridad" si los sistemas automatizados fallan.

Este riesgo se agrava porque, cuando los sistemas están conectados entre sí para formar redes o son accesibles a través de sistemas públicos, se vuelven mucho más vulnerables a intrusiones anónimas desde ubicaciones remotas. Además, gran parte de la información mantenida por las organizaciones, aunque no se encuentra debidamente clasificada se sabe que es extremadamente sensitiva y cualquier otra operación automatizada es blanco atractivo para individuos u organizaciones con fines maliciosos, como podrían ser las actividades de fraude para obtener beneficios personales o sabotear las operaciones con

fines activistas. Varias Organizaciones han experimentado intrusiones en sus sistemas y los indicadores utilizados como pruebas son el número de ataques que son cada vez mayores y que muchos de estos ataques no son detectados.

Hay que centrarse principalmente en el marco de gestión que las organizaciones han establecido y no en los controles específicos que han elegido, porque se ha identificado a la Administración de la seguridad como un problema de fondo en las Organizaciones.

Los controles técnicos como son los relacionados con el cifrado son cada vez más accesibles y ayudan a facilitar la seguridad de la información pero la aplicación efectiva requiere que estas técnicas sean cuidadosamente seleccionadas y que su utilización sea administrada y controlada de forma continua. Además, hay muchos aspectos de la seguridad de la información como son la evaluación de riesgos, el desarrollo de políticas y la planeación de recuperación de desastres que requieren atención de la administración coordinada de la Organización llámese personal operativo y alta dirección.

1. Panorama Actual e Importancia de la Seguridad de la Información

El flujo de información que se maneja actualmente tanto en organizaciones como en el uso personal de las tecnologías es bastante alto y esta tendencia seguirá subiendo debido a los nuevos dispositivos para el intercambio de información que se ha vuelto más rápido y transparente para el usuario y las organizaciones, además de que cada vez más personas están en contacto con tecnologías que ayudan a facilitar su vida y/o también para el entretenimiento.

Si miramos a nuestro alrededor y hacemos reflexión de las actividades que se realizaron al final del día, nos daremos cuenta que tan sumergidos estamos en la tecnología de la información, tan fácil como recordar cuantos correos electrónicos enviamos, cuantos mensajes de texto a través del celular mandamos y recibimos, pagos de cuenta al banco, cobrar el sueldo por nomina, hacer reservación de boletos para viajes o conciertos vía internet, consultar la cartelera por internet, pagar el súper con tarjeta de crédito o débito, guardar y trasladar información utilizando memorias USB, buscar información en internet para realizar la tarea, etc.

Estas son actividades que de manera cotidiana realizan usuarios con muy poco o nada de conocimiento acerca de la informática, a estos usuarios no les interesa saber cómo es que se guarda, cuida y utiliza la información que diariamente envía por diversos medios,

lo único que le importa es no tener problemas ni retrasos en cada una de estas actividades.

Ahora bien, debemos tomar en cuenta que las organizaciones realizan estas mismas actividades a través de sus empleados y además habría que sumar a todo esto que en sus instalaciones muchas veces cuentan con impresoras en red, intranets, servidores, páginas web, flujo de información a nivel nacional o internacional, dispositivos de red, etc., por lo que el riesgo de tener un incidente de seguridad es mucho mayor.

Desafortunadamente en muchos lugares la seguridad de la información se toma muy a la ligera y únicamente se realizan acciones de seguridad cuando se ha presentado algún incidente y cuando esto sucede se toman decisiones muy precipitadas y sin contar con un procedimiento para que el negocio continúe o se recupere.

Este tipo de problemas son más comunes de lo que pensamos y siempre se ha pensado que los mayores desastres son causados por virus informáticos o por hackers, pero lamentablemente muchos de estos incidentes son causados desde el interior de la organización.

1.1. México y los Acuerdos Internacionales

El Consejo de Europa realizó la Conferencia de Cooperación contra el Cibercrimen en Estrasburgo, Francia, donde se reunieron 280 expertos en cibercrimen de 80 países, 15 organizaciones e iniciativas internacionales, y 30 participantes del sector privado y académico para mejorar la cooperación contra el cibercrimen en todos los niveles.

En esta variopinta reunión, en la cual se discutió el estado de la legislación de los diferentes países en relación al cibercrimen, la protección de menores contra la explotación sexual, las políticas e iniciativas internacionales existentes y las diversas modalidades de lucha contra los delitos informáticos, entre otros temas, resaltó nuevamente para México las ventajas de la incorporación del país al Convenio de Budapest sobre Cibercriminalidad.

Si bien nuestro país ya ha sido observador durante la firma del citado convenio, la adhesión de México al mismo aún no ha sido ratificada, a pesar de las ventajas que podría traer en la labor de reforzar políticas, definir estrategias, establecer una legislación adecuada y aplicar medidas prácticas sobre el cibercrimen y la seguridad cibernética en el país.

¿Por qué? Porque el Convenio de Budapest es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional) y trata con carácter prioritario una política penal contra la ciberdelincuencia en cada uno de los países miembros. Y uno de los problemas que los investigadores digitales enfrentamos en muchos casos es, precisamente, el de la trasnacionalidad de los delitos informáticos y la falta de tratados internacionales que nos permitan traspasar fronteras al perseguir a los delincuentes.

El Convenio de Budapest, pues, nos permitiría no solo avanzar en temas de cooperación internacional contra delitos informáticos, sino también fortalecer nuestras leyes y regulaciones contra el cibercrimen de todo nivel.

Adicionalmente, durante la Conferencia Octopus se discutió también el vincular la protección de datos personales con las estrategias contra el cibercrimen que se establezcan en cada país, debido a la alta incidencia del robo de información personal con fines delictivos a nivel mundial.

Solo para darnos una idea de la magnitud de información de la cual hablamos aquí, de acuerdo con el Instituto Federal de Acceso a la Información y Protección de Datos de México (IFAI), solo a nivel Federal, el gobierno mexicano tiene un total de 3,097 bases de datos registradas, el 97% de las cuales contienen solo información básica de identidad, en tanto el otro 3% reúne datos personales sensibles como origen étnico, de salud o información genética, religión, preferencias sexuales, creencias políticas, entre otros datos.

Asimismo, nueve de cada 10 usuarios de Internet han brindado datos de identificación (nombre, foto, edad, dirección, género, RFC y CURP) por Internet, y casi cuatro de cada 10 usuarios han dado también información sensible en redes sociales (79%), sitios de banca en línea (65%) o tiendas online (62%).

Por eso, tanto la ciberseguridad como las políticas de protección de datos deben ser consistentes con los derechos fundamentales de los ciudadanos, esenciales en las sociedades democráticas.

Jacqueline Peschard, comisionada presidenta del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), en busca de alcanzar este objetivo en México, manifestó interés en sumarse al Convenio 108 del Consejo de Europa (CE) para la “Protección de las Personas con Respecto al Tratamiento Automatizado de Datos Personales”.

El 108 garantiza a los ciudadanos de los Estados contratantes el respeto de sus derechos y libertades. Principalmente el derecho a la vida privada frente a los tratamientos de datos personales, conciliando de esa forma el respeto a la vida privada con la libre circulación de información entre los países.

Además el convenio contiene conceptos relativos a los principios de calidad de la información y a los derechos de los titulares de los datos. Señala criterios que regulan el tratamiento de datos y su flujo transfronterizo.

El Convenio, también llamado de Estrasburugo, consta de 27 artículos agrupados en 7 capítulos y su objeto es garantizar el respeto de los derechos y libertades fundamentales de toda persona física, sin importar su nacionalidad, con respecto al trato automatizado de sus datos, sensibles o comunes, ya sea en el sector público o privado.

En 2005, en Madrid, España, fueron estipulados los estándares internacionales para la protección de datos personales, y se estableció el papel de los titulares y responsables de la información, los gobiernos en el mundo y terceros implicados.

Años más tarde, los diputados Gustavo Parra y Adolfo Mota, militantes del PAN y PRI, respectivamente, presentaron el proyecto para la Ley Federal de Protección de Datos Personales, la cual está basada en lo que fue estipulado en la capital española.

Uno de los valores que vale la pena destacar de la ley de protección de datos personales en México es justamente la clasificación de los datos (en patrimoniales, financieros y sensibles), división que ha resultado benéfica para la normatividad.

Las autoridades a cargo de vigilar el cumplimiento de la Ley Federal de Protección de Datos Personales son el Instituto Federal de Acceso a la Información y Protección de Datos (Ifai) y la Secretaría de Economía, las cuales están atentas a infracciones como el incumplimiento de las solicitudes del titular, la transferencia de datos sin consentimiento del titular, el recabo de datos a través de engaños y la creación de bases de datos sensibles sin justificación, entre otras.

1.2. Simulación de Ataques Cibernéticos en México

México simulará ser víctima de una serie de embates informáticos como parte de una serie de ejercicios organizados por la Organización de Estados Americanos (OEA) con la finalidad de concientizar a los gobiernos y sociedad civil sobre cómo reaccionar frente a dicha contingencia.

Los supuestos embates serán realizados por un laboratorio móvil de simulación, que permite llevar a cabo ejercicios de detección y mitigación de ciberataques. Dicho laboratorio es gestionado por el Comité Interamericano contra el Terrorismo (CICTE) de la OEA y será puesto a disposición de las naciones participantes.

El laboratorio permitirá a las naciones realizar simulacros ante un embate informático y elaborar procesos de respuesta ante una crisis, indicó un comunicado liberado por el propio organismo.

El nuevo laboratorio permitirá incrementar el alcance de los ensayos, pues congregará en un mismo lugar al sector privado, la academia, la sociedad civil y autoridades gubernamentales. Ello redundará en una capacitación de más alcance y mayor calidad de los funcionarios públicos, líderes sociales y empresariales, expertos y académicos.

De acuerdo a la OEA, los simulacros servirán para conocer las debilidades y fortalezas de las naciones con respecto a la protección de su infraestructura crítica y sistemas de información.

Colombia y Argentina son las otras naciones que participarán junto a México en la simulación de los embates informáticos.

1.3. Actividad Maliciosa en América Latina

Brasil y México se encuentran entre los países de América Latina con el mayor registro de actividad cibernética maliciosa, ambas naciones son acompañadas por Colombia y Argentina, que también destacaron en este ramo, reveló el Informe sobre Amenazas a la Seguridad en Internet (ISTR, por sus siglas en inglés) de Symantec.

De acuerdo con el estudio, Brasil es el país de América Latina donde más actividad maliciosa se registra, seguido por Argentina en segundo lugar, Colombia en tercero y México en cuarto sitio.

El reporte señala que Brasil y México son las naciones con la mayor producción y distribución de código malicioso en la región, siendo los responsables de la creación del 39 y 21%, respectivamente.

Por su parte, Argentina domina junto a Brasil en el campo relacionado con el correo electrónico no deseado. El estudio señala que la nación carioca es responsable del 40% del spam, mientras que el país del Cono Sur se ubica en segundo puesto con 15%.

Con respecto al hospedaje de sitios relacionados con la ingeniería social, Brasil nuevamente domina con 39%, seguido por Colombia con 32% y Argentina con sólo 8%.

Finalmente el estudio sentencia que Brasil y México son las naciones de la región con el mayor número de ataques vía web, es decir, los países en los que más sitios legítimos son infectados por algún virus para atacar a los visitantes de los mismos.

1.4. Protección de Información en México

La pérdida de información en empresas e instituciones ha afectado a más de 500 millones de personas en los últimos tres años. De acuerdo con él un estudio realizado por KPMG México "Data Loss Barometer", el 21 % de los incidentes de pérdida de datos se ha dado por culpa de una persona interna en la Organización. Este estudio también revela que en 2010 más de 10 millones de personas perdieron o les fueron robados datos de su identidad personal.

Según un estudio, la primera causa de fugas de información desde el 2007 es la incursión y ataques de intrusos cibernéticos, con aproximadamente 250 millones de personas afectadas. En segundo lugar se encuentra el robo o pérdida de medios portátiles, con alrededor de 114 millones de número de incidentes, seguido por la eliminación incorrecta de información, con 78 millones de casos.

1.4.1. Situación actual en México

Recientemente se realizó un sondeo entre altos directivos de empresas de diferentes sectores. Los resultados fueron muy interesantes, y revelan que las empresas aún tienen mucho por hacer para proteger su información.

El 83% de los encuestados dijo que el costo de oportunidad en caso de perder información de su organización sería muy elevado. Ante la pregunta de si conoce con precisión dónde están sus vulnerabilidades de tecnología, el 75 % contestó que no del todo, mientras que el 22% aseguró conocerlas al 100%.

Otro dato muy importante que este sondeo reveló fue que el 94% desconoce cuál es el costo de oportunidad de no analizar las vulnerabilidades de la organización, pero anticipa que es muy elevado. Ver Ilustración 1.

Ilustración 1

Ante la pregunta de si su negocio puede desaparecer en caso de que deje de operar debido a alguna fuga de información, 63% dijo que sí y que es algo que deben resolver urgentemente, mientras que 37% considera que su empresa no corre el riesgo de poder desaparecer debido a esta crisis.

Ilustración 2

Aunque muchos consideraron que la seguridad es un tema que debe ser prioritario, no es de sorprenderse que esto no sea una realidad. El 58% de las organizaciones no considera a la información como una parte integral dentro del proceso de planeación estratégica, a pesar de que sabe de su importancia, mientras que el 36% si lo hace.

Por otro lado, 13% de las compañías encuestadas anticipa sus acciones a desarrollar en caso de que se presenten problemas de seguridad. El 70% tiene una idea, aunque no certera y reacciona al sucedido, mientras que el 17% responde en el momento.

Para 27% de las organizaciones, el aspecto más importante a considerar en tema de seguridad de la información es desarrollar y ligar la estrategia de seguridad al negocio. El 21% piensa que es asegurar la continuidad del negocio y 15% entender el impacto en el negocio de presentar algún problema en materia de seguridad.

Ilustración 3

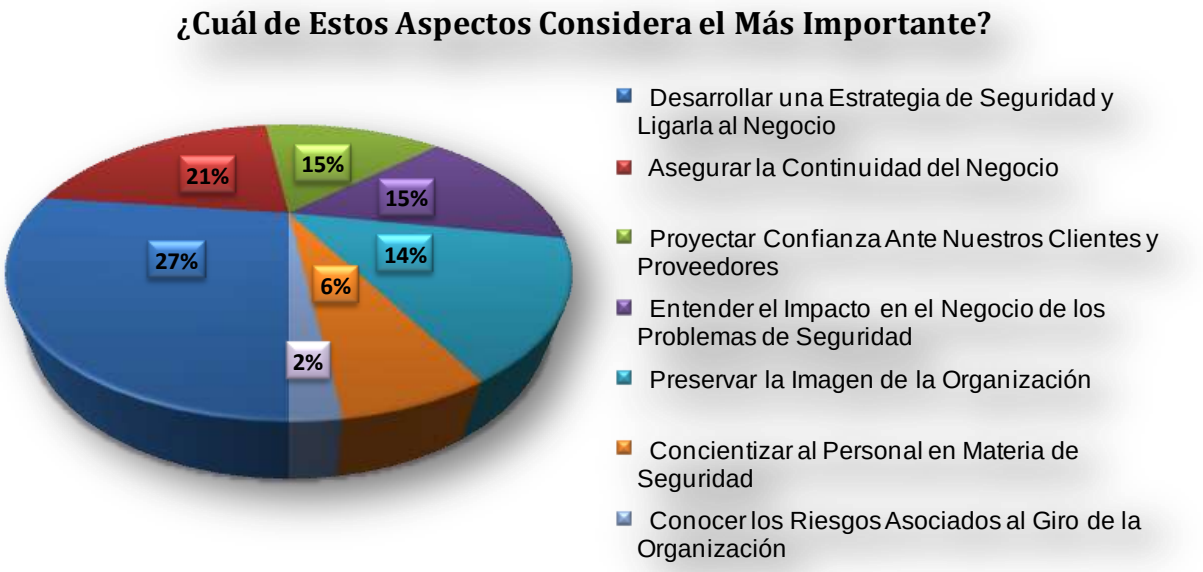


Ilustración 4

1.4.2. Retos en el manejo de la información

Una característica de la información es que esta no es estática. Está en constante movimiento y es un flujo desde que se crea hasta que se destruye. Por esto es importante conocer como la trasferimos y a través de qué canal, pero sobre todo cuestionarnos si el medio es seguro y quién tiene acceso a éste.

Otra de sus particularidades es que constantemente se va procesando y transformando dentro de la organización. Ante esto debemos tener siempre presente cuánto tiempo se puede conservar y en dónde. Sin embargo también es importante considerar que una vez que esta información ya no se necesite, es necesario deshacernos de ella de la manera más conveniente. Si la información está almacenada electrónicamente, se puede hacer a través de un software especial, pero si es física (papel) se deberá llevar a cabo una destrucción de los documentos para evitar que estos lleguen a manos de personas que puedan hacer mal uso de ellos.

Otro reto importante al que se enfrentan las compañías es la Ley Federal de Protección de Datos Personales en Posesión de Particulares, ya que su alcance afecta a todas las empresas, aunque no manejen datos de clientes, pues la Ley abarca inclusive la información de los empleados.

Por esto, las organizaciones deben proteger tanto la información que es crítica para su negocio, como aquella que tiene un interés privado.

1.4.3. Protegiendo la Información

La tecnología nos ayuda a ser mejores y a comunicarnos más rápido, pero su reto es que constantemente nos presenta nuevos desafíos. Es común que las estrategias de seguridad en las empresas estén enfocadas a prevenir lo que entra a la compañía, pero no lo que sale de la misma.

Debido a esto es prioritario tomar medidas preventivas para estar protegidos y preparados, pues es mejor antes que después. El contar con políticas controles tecnológicos, métricas y procedimientos bien establecidos para saber qué hacer en caso de pérdida de información hará que respondamos mejor ante una situación crítica.

Para poder proteger la información de la empresa, primero debemos definir los parámetros que indiquen qué es información sensitiva y cuál es confidencial.

Posteriormente hay que hacer un inventario de los activos de información. Esto significa que no solamente se debe hacer una lista de información (ya clasificada) con la que se cuenta, sino que también hay que definir que se va a hacer para protegerla. Finalmente podremos definir los controles adecuados para esa información.

Hay cosas por hacer que no pueden esperar. Entre ellas se encuentra el desarrollar estrategias para prevenir fugas de información, hacer un análisis de las vulnerabilidades e impacto que tendrá la pérdida de información en nuestro negocio, entre otras.

2. Análisis y Evaluación de Riesgos

En la Administración de la Seguridad de la Información, es crucial que el análisis y evaluación de riesgos se realice de forma sistemática, solo de esta forma es posible identificar y evaluar los riesgos asociados con los activos de información. De esta manera se puede dar seguimiento de la evolución de los niveles de riesgo de los activos y su influencia en toma de decisiones relacionadas con la Seguridad de la Información.
Para que el riesgo sea correctamente tratado, la Organización debe comenzar por conocer los riesgos que afecten sus actividades diarias. Los análisis de riesgos son una herramienta que nos brinda ese conocimiento.
El análisis de riesgos nos ayuda a aproximar de manera metódica los niveles de riesgo tanto para los activos como para la organización y algunos de los pasos que se tienen que realizar de manera general son los siguientes (sin seguir una metodología específica y definiendo actividades generales).

- Definir alcance de análisis (limitado por áreas, procesos o tipos de activos de una Organización).
- Identificar e inventariar los activos relevantes para la organización
- Identificar las amenazas (pudiendo identificarse el agente de amenaza si la metodología lo pide).
- Identificar las vulnerabilidades

- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar la probabilidad de materialización de la amenaza
- Determinar las contra medidas y su eficacia frente al riesgo

2.1. Activos

Se denominan activos a todo aquello que es considerado de importancia para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección, su misión y visión de negocio.

El activo más importante de una organización es la "Información" que puede estar presente de manera tangible o intangible (papel, conocimiento del personal, procesos, procedimientos, etc.). Otra manera de identificar los activos es a través de lo que se llaman "Activos de Información" que son todos aquellos medios que se utilizan para procesar, transferir o almacenar la información.

No existe como tal una clasificación estándar para los activos ya que hay metodologías que utilizan una clasificación propietaria e incluso otras que no los clasifican, pero en general se tiene el entendido de que el activo puede ser de tipo tangible o intangible. Los casos más comunes para los activos intangibles son la reputación y la información por si misma (mencionada en la norma ISO 27001). Ya que este documento no pretende ser una metodología de análisis de riesgos, los ejemplos que aquí se utilicen serán solo informativos

De igual manera, dependiendo la metodología se podrán realizar mapas o diagramas de dependencias entre activos ya que hay activos que únicamente procesan la información y sus salidas son las entradas de otro activo o incluso un activo no puede operar hasta que arranque otro activo. Dependiendo la metodología que se utilice, estas dependencias podrán ayudar a realizar cálculos de índice de riesgo acumulado.

Un ejemplo de la dependencia entre activos es como el siguiente:

- Capa 1: el entorno: activos que se precisan para garantizar las siguientes capas
  - Equipamiento y suministros: energía, climatización, comunicaciones
  - Personal: de dirección, de operación, de desarrollo, etc.
  - Otros: edificios, mobiliario, etc.
- Capa 2: el sistema de información propiamente dicho
  - Equipos informáticos (hardware)
  - Aplicaciones (software)
  - Comunicaciones
  - Soportes de información: discos, cintas, etc.

- Capa 3: la información
  - Datos
  - Meta-datos: estructuras, índices, claves de cifra, etc.

- Capa 4: las funciones de la Organización, que justifican la existencia del sistema de formación y le dan finalidad
  - Objetivos y misión
  - Bienes y servicios producidos

- Capa 5: otros activos
  - Credibilidad o buena imagen
  - Conocimiento acumulado
  - Independencia de criterio o actuación
  - Intimidad de las personas
  - Integridad física de las personas

Otro ejemplo de dependencias en tres capas puede ser el utilizado por metodologías basadas en Gestión de Procesos de Negocio o Procesos tal como lo hiciera la ISO/IEC 9001. Ver Ilustración 5.

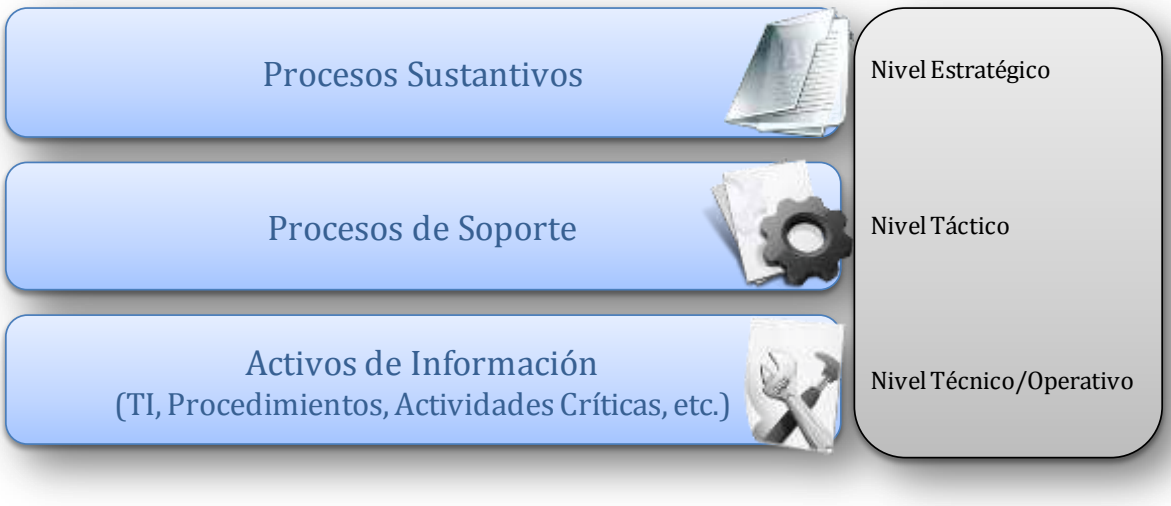


Ilustración 5

2.2. Valoración

En este caso no solo se habla acerca de lo que cuesten las cosas, sino también de la relevancia que representan para la organización. Para los análisis de riesgos, si algo no vale nada, se debe prescindir de eso, pero si no se puede prescindir impunemente de un activo, entonces quiere decir que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos utilizando cálculos que pudieran ser operaciones probabilísticas (utilizando comúnmente la media y moda) y/o sumatorias, dependiendo el modelo matemático que utilice la metodología.

2.2.1. Valoración cualitativa

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás, Es frecuente plantear estas escalas como "órdenes de magnitud" y en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

Pros;

- Los cálculos, si los hay, son simples y fáciles de entender y ejecutar.
- No es necesario determinar el valor monetario de la información.
- No es necesario determinar la frecuencia.
- No es necesario estimar el costo de las medidas recomendadas de reducción de riesgos y calcular el costo- beneficio.

Contras;

- La evaluación del riesgo y los resultados son esencialmente subjetivos tanto en el proceso y las métricas.
- No se hace ningún esfuerzo para desarrollar una base objetiva monetaria por el valor de los activos de información. Por lo tanto, la percepción de valor no es realista pudiera no reflejar el valor real de riesgo.
- No existe una base que proporcione un análisis de costo / beneficio de las medidas de mitigación de riesgo, sólo la indicación subjetiva de un problema.
- No es posible dar seguimiento al desempeño de gestión de riesgos objetivamente cuando todas las medidas son subjetivas.

2.2.2. Valoración cuantitativa

Las valoraciones numéricas absolutas cuestan mucho esfuerzo pero no adolecen de los problemas de las valoraciones cualitativas. Sumar valores numéricos es absolutamente natural y la interpretación de las sumas no es nunca motivo de controversia.

Pros;

- La evaluación y los resultados se basan sustancialmente en procesos y métricas de manera independiente. Por lo tanto, es compatible y significativo realizar un análisis estadístico.
- El valor de la información (disponibilidad, confidencialidad e integridad) expresado en términos monetarios tiene un mejor entendimiento. De esta manera, la pérdida esperada es más entendible para la organización.
- Se obtiene una base creíble para la evaluación de costo-beneficio de las medidas de mitigación de riesgo. Por lo tanto, la toma de decisiones para el presupuesto de la seguridad de la información es más coherente y compatible.
- La gestión de riesgos puede ser monitoreada y evaluada.
- Los resultados de evaluación de riesgos se expresan en el lenguaje de la administración, el valor monetario, los porcentajes, y la probabilidad anualizada. Por lo tanto, el riesgo se entiende mejor.

Contras;

- Los cálculos son complejos. Si no se entiende o se explica con eficacia, se podría desconfiar de los resultados.
- No es práctico para intentar ejecutar una evaluación cuantitativa del riesgo sin utilizar una herramienta automatizada reconocida y bases de conocimientos asociados. Un esfuerzo manual, incluso con el apoyo de la hoja de cálculo y software estadístico genérico, puede tomar de diez a veinte veces el esfuerzo de trabajo que se requiere con el apoyo de una buena herramienta automatizada de evaluación de riesgos.
- Se debe recopilar una cantidad sustancial de información sobre la información de destino y de su entorno de TI.
- Todavía no existe un estándar, inventario o base de conocimiento de amenazas completo que contenga información de su frecuencia de materialización. De este modo, los usuarios deben confiar en la credibilidad de los proveedores que desarrollan y apoyan las herramientas automatizadas o hacer investigación de amenazas por su propia cuenta.

2.3. Vulnerabilidades

Típicamente una vulnerabilidad es reconocida por ser una debilidad o falla de algún activo, de la organización, algún diseño, implementación o procedimiento que pudiera ser explotado por usuarios internos o externos con acciones mal intencionadas o bien, por desconocimiento, ignorancia o falta de capacitación.

Cabe señalar que los tipos de vulnerabilidades que existen, y la metodología necesaria para determinar si las vulnerabilidades están presentes, generalmente variarán dependiendo de la naturaleza del activo de información.

Para la identificación de vulnerabilidades se recomienda lo siguiente;

- Si el sistema informático aún no ha sido diseñado, la búsqueda de vulnerabilidades debe centrarse en las políticas de seguridad de la organización, los procedimientos de seguridad previstos y las definiciones de los requisitos del sistema y análisis de los vendedores o los desarrolladores de seguridad de productos.

- Si el activo de información está por implementarse, la identificación de las vulnerabilidades debe ser ampliada para incluir información más específica, como por ejemplo las características de seguridad planificadas descritas en la documentación del diseño de la seguridad y los resultados de la prueba del sistema de certificación y evaluación.

- Si el activo de información ya está operando, el proceso de identificación de las vulnerabilidades debe incluir un análisis de las características de seguridad de los sistemas de TI y los controles de seguridad, técnicos y de procedimiento que se utiliza para proteger el sistema.

2.4. Amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las Amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

Existen incidentes naturales (terremotos, inundaciones, tormentas, etc.) e incidentes causados por el hombre como (contaminación, fallos eléctricos, etc.) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos. Hay amenazas causadas por las personas, debido a errores de operación, administración, configuración o bien ataques intencionados como pueden ser los causados por hackers.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

2.4.1. Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

- Degradación (impacto): cuán perjudicado resultaría el activo
- Frecuencia (probabilidad): cada cuánto se materializa la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.
La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción". Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias

2.5. Determinación del impacto

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

2.5.1. Impacto acumulado

Es el calculado sobre un activo teniendo en cuenta

- Su valor acumulado (el propio mas el acumulado de los activos que dependen de él)
- Las amenazas a que está expuesto

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

- El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.
- El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las contra medidas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc

2.5.2. Impacto repercutido

Es el calculado sobre un activo teniendo en cuenta

- Su valor propio
- Las amenazas a que están expuestos los activos de los que depende

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

- El impacto es tanto mayor cuanto mayor es el valor propio de un activo.
- El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.
- El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.
- El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información.

2.6. Determinación del riesgo

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

2.6.1. Riesgo acumulado

Es el calculado sobre un activo teniendo en cuenta

- El impacto acumulado sobre un activo debido a una amenaza y
- La frecuencia de la amenaza

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la frecuencia de la amenaza.

El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las contra medidas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

2.6.2. Riesgo repercutido

Es el calculado sobre un activo teniendo en cuenta

- El impacto repercutido sobre un activo debido a una amenaza y
- La frecuencia de la amenaza

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la frecuencia de la amenaza.

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

2.7. Modificación del Riesgo a Través del Impacto

En los pasos anteriores no se han tomado en consideración las contramedidas desplegadas. Por lo tanto se miden los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las contra medidas presentes.

Se definen contra medidas como procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se invocan simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otros, seguridad física y por último, está la política de personal.

Hay que planificar el conjunto de contra medidas pertinentes para atajar tanto el impacto como el riesgo, reduciendo bien la degradación del activo (minimizando el daño), bien reduciendo la frecuencia de la amenaza (minimizando sus oportunidades).

Toda amenaza debe ser requerida profesionalmente para su evaluación, lo que quiere decir que hay que:

- Establecer una política de la Organización al respecto; o sea, unas directrices generales de quién es responsable de cada cosa
- Establecer una norma; o sea, unos objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada
- Establecer unos procedimientos; o sea, instrucciones paso a paso de qué hay que hacer
- Desplegar contra medidas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas
- Desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto A este conjunto de elementos se le encasilla habitualmente bajo el nombre de Sistema de Gestión de la Seguridad de la Información (SGSI), aunque se está gestionando tanto como actuando.

El párrafo anterior puede llamar a engaño si el lector interpreta que hay que llevar a cabo todos y cada uno de los puntos para cada amenaza. No. En la práctica lo dicho se traduce en desarrollar una política, unas normas y unos procedimientos junto con el despliegue de una serie de contra medida y controles y, ahora sí, verificar que todas y cada una de las amenazas tienen una respuesta adecuada.

De los puntos anteriores, el más “abierto” es el de determinación de las contra medidas apropiadas. Es realmente un arte que requiere personal especializado aunque en la práctica las situaciones más habituales están perfectamente documentadas en la literatura y basta elegir de entre un catálogo en función de la magnitud del riesgo.

2.8. Procedimiento Metodológico

Las organizaciones utilizan la evaluación de riesgos para determinar el alcance y potencial de las amenazas en los sistemas de tecnologías de la información, lo que permite realizar una adecuada identificación de controles de seguridad para reducir la exposición de los sistemas.

Riesgo.- Es la función de la probabilidad de que una amenaza explote una vulnerabilidad resultando en un impacto negativo para la organización.

2.8.1. Caracterización del Alcance

La principal actividad de la Caracterización del Alcance es determinar el propósito de la seguridad de la información. Con esta información se crean los criterios necesarios para la evaluación de riesgos que debieran incluir de igual manera los límites y restricciones dentro de la evaluación.

Entre los principales requerimiento para el aseguramiento de la información y sus activos de información se pueden tomar en cuenta los siguientes puntos:

- Establecer un Sistema de Gestión de Seguridad de la Información.
- Estar en conformidad con regulaciones nacionales e internacionales.
- Estar en conformidad con regulaciones internas de la organización.
- Realizar planes de continuidad de negocio.
- Cumplir con cláusulas contractuales.

Para realizar esta identificación se toma en cuenta tanto la información que constituyen los sistemas así como los sistemas mismos que son también nombrados activos de información.

2.8.2. Identificación del Inventario

La identificación de los componentes que se incluirán para determinar los niveles de riesgo debe tomar en cuenta lo siguiente:

- Identificación de Activos
- Identificación de Amenazas
- Identificación de Vulnerabilidades
- Identificación de controles de seguridad existentes

Activos

La identificación de activos requiere el apoyo del personal operativo de la organización y del personal que entiende adecuadamente los procesos que componen a las áreas.

Se debe tomar en cuenta para la identificación de activos todo lo que se encuentra dentro del alcance en términos de Personal, Tecnología y Procesos.

Existen diferentes técnicas que ayudan en la identificación de activos entre las cuales están:

- Diagramas de flujo de actividades, procesos, procedimientos, etc.
- Identificación de los activos de tecnología, personas y procesos que son críticos para mantener la operación de las actividades tácticas.
- Identificar el inventario de activos de la organización.
- Entrevistas o talleres con los responsables de áreas.
- Revisión de documentación de la organización.
- Herramientas de escaneo automáticas.

Amenazas

Una amenaza tiene el potencial de hacer daño a los activos, tales como información, procesos y sistemas y por lo tanto a las organizaciones. Las amenazas pueden ser de origen natural o humano, y puede ser accidental o deliberada. Las fuentes de amenazas tanto accidental como intencionada deben ser identificadas. Una amenaza puede surgir desde el interior o desde el exterior de la organización. Las amenazas deben ser identificadas de forma genérica y por tipo (por ejemplo, las acciones no autorizadas, daños físicos, fallas técnicas). Esto significa que ninguna amenaza se pasa por alto, incluso lo inesperado.

Algunas amenazas pueden afectar a más de una vulnerabilidad y por lo tanto a más de un activo. En tales casos, pueden causar efectos diferentes dependiendo del lugar donde este el activo y la información que en él se almacene, procese o transfiera.

Las entradas que se debieran tomar en cuenta para la identificación de las amenazas son las siguientes:

- Propietarios de los activos o los usuarios
- Personal de recursos humanos
- Especialistas en seguridad de la información
- Expertos de seguridad física
- El departamento jurídico
- Autoridades meteorológicas
- Compañías de seguros
- Autoridades de Gobierno
- Aspectos del medio ambiente
- Incidentes documentados

Además de las categorías antes señaladas vale la pena consultar catálogos de amenaza para completar la lista de amenazas genéricas. Cuando se utilizan catálogos de amenazas se debe ser consciente de que hay un cambio continuo de las amenazas importantes, sobre todo si el entorno empresarial cambia continuamente.

Atendiendo a su origen, existen dos tipos de amenazas:

- Externas, que son las causadas por alguien (hackers, proveedores, clientes, etc.) o algo que no pertenece a la organización. Ejemplos de amenazas de este tipo son los virus y las tormentas.

- Internas, estas amenazas son causadas por alguien que pertenece a la organización, por ejemplo errores de usuario o errores de configuración.

Las amenazas también pueden dividirse en dos grupos según la intencionalidad del ataque en deliberadas y accidentales:

- Deliberadas: Cuando existe una intención de provocar un daño, por ejemplo un ataque de denegación de servicio o la ingeniería social.

- Accidentales: Cuando no existe tal intención de perjudicar, por ejemplo averías o las derivadas de desastres naturales: terremotos, inundaciones, fuego, etc.

Para valorar las amenazas en su justa medida hay que tener en cuenta cual sería el impacto en caso de que ocurrieran y a cuál o cuáles son los parámetros de seguridad que afectaría, si a la confidencialidad, la integridad o la disponibilidad.

Vulnerabilidades

El objetivo de este paso es realizar un listado completo de las diferentes vulnerabilidades que pueden estar presentes en el inventario de activos y que pudieran ser explotadas por las amenazas identificadas anteriormente.

Los métodos recomendados para la identificación de vulnerabilidades son a través de:

- Fuentes de vulnerabilidades (sitios especializados en vulnerabilidades en internet, evaluaciones de riesgo anteriores, etc.)

- Pruebas de seguridad (análisis de vulnerabilidades, pruebas de penetración, auditorias de configuración, etc.)

- Listas de verificación de requerimientos de seguridad de la organización (checklist de configuración, checklist de auditoría, checklist de pruebas, procedimientos y manuales de operación, políticas de seguridad, verificación de controles de seguridad, etc.)

Cabe señalar que los tipos de vulnerabilidades que existen, y la metodología necesaria para determinar si las vulnerabilidades están presentes, generalmente varía dependiendo de la naturaleza de los activos de información.

- Si el activo de información aún no ha sido diseñado o implementado, la búsqueda de vulnerabilidades debe centrarse en las políticas de seguridad de la

organización, los procedimientos de seguridad previstos y las definiciones de los requerimientos de sistema, y el de los proveedores o desarrolladores.

- Si el activo de información ya está implementado, la identificación de las vulnerabilidades debe ser ampliada para incluir información más específica, como por ejemplo las características de seguridad planificadas descritas en la documentación del diseño de la seguridad y los resultados de la prueba del sistema de certificación y evaluación.

- Si el activo de información ya se encuentra en producción, el proceso de identificación de las vulnerabilidades debe incluir un análisis de las características de seguridad de los sistemas de TI y los controles de seguridad, técnicos y de procedimiento, que se utiliza para protegerla.

La información catalogada del inventario de activos, vulnerabilidades y amenazas se relaciona directamente con la identificación de los riesgos asociados a un determinado grupo de activos que por su característica misma se ven expuestos por la falta de mantenimiento o incluso por las actividades mismas de una organización.

Un ejemplo gráfico de esta caracterización del riesgo se entiende de una manera más sencilla con la siguiente imagen. Ver Ilustración 6.

Ilustración 6

Para realizar un análisis de riesgos se parte del inventario de activos. Si es razonablemente reducido, puede decidirse hacer el análisis sobre todos los activos que contiene. Si el inventario es extenso, es recomendable escoger un grupo relevante y manejable de activos, bien los que tengan más valor, los que se consideren estratégicos o todos aquellos que se considere que se pueden analizar con los recursos disponibles. Se puede tomar cualquier criterio que se estime oportuno para poder abordar el análisis de riesgos en la confianza de que los resultados van a ser útiles, Ver Ilustración 7.

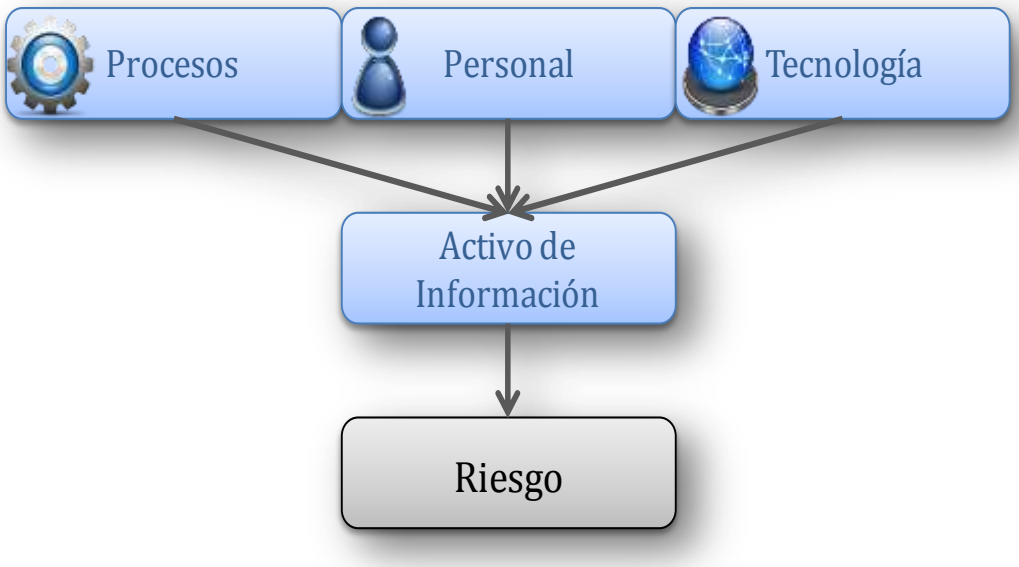


Ilustración 7

Hay que tener en cuenta que la realización de un análisis de riesgos es un proceso laborioso. Para cada activo se van a valorar todas las amenazas que pueden afectarle, la vulnerabilidad cada una de las amenaza y el impacto que causaría la amenaza en caso de ocurrir. Con todos esos datos, se calcula el valor del riesgo para ese activo.

Independientemente de la metodología que se utilice, el análisis de riesgos debe ser objetivo y conseguir resultados repetibles en la medida de lo posible, por lo que deberían participar en él todas las áreas de la organización que estén dentro del alcance de la Administración de la Seguridad de la Información. De esta manera quedarán plasmados varios puntos de vista y la subjetividad, que es inevitable, quedará reducida. Además contar con la colaboración de varias personas ayuda a promover el desarrollo de la Administración de la Seguridad de la Información como una herramienta útil para toda la organización y no sólo para la dirección o el área que se encarga del proyecto. Se puede abordar el análisis de riesgos con varios enfoques dependiendo del grado de profundidad con el que se quiera o pueda realizar el análisis.

2.8.3. Valoración de Riesgo

En una ejecución resumida de un análisis de riesgos cualitativo se tomará en cuenta el cálculo básico para la determinación del riesgo con la siguiente fórmula:

- **Riesgo** = Probabilidad x Impacto
- **Impacto** = Vulnerabilidad && Amenaza

Para el anterior cálculo debemos tomar en consideración los siguientes criterios de Probabilidad y de Impacto.

Valor	Probabilidad de Ocurrencia	Guía
1	Muy Baja	Ha ocurrido una vez en cinco años
2	Baja	Ha ocurrido una vez en tres años
3	Media	Ha ocurrido una vez al año
4	Alta	Ha ocurrido por lo menos dos veces al año
5	Muy Alta	Ha ocurrido tres veces o más en un año

Valor	Impacto	Guía
1	Muy Bajo	Es irrelevante su afectación para la Confidencialidad, Integridad y Disponibilidad
2	Bajo	La Confidencialidad, Integridad y Disponibilidad tienen una importancia baja para el activo
3	Medio	La Confidencialidad, Integridad y Disponibilidad puede ser comprometida y la importancia del activo es relevante para la Organización
4	Alto	La Confidencialidad, Integridad y Disponibilidad se ve afectada y tendría una consecuencia de importancia para la Organización
5	Muy Alto	La Confidencialidad, Integridad y Disponibilidad se ve seriamente afectada y puede dañar la operación de la organización, comprometer la seguridad de la información y/o incurrir en una no conformidad regulatoria interna o externa

Valor	Nivel de Amenaza	Guía
1	Muy Baja	La amenaza es obsoleta y de fácil control
2	Baja	La amenaza es conocida y existen controles para retenerla
3	Media	La amenaza se puede materializar y su retención causaría un aumento en el esfuerzo operativo
4	Alta	La amenaza puede degradar la seguridad de la organización
5	Muy Alta	La amenaza puede causar un daño severo a la Organización

Valor	Exposición a la Vulnerabilidad	Guía
1	Baja	Existen controles de seguridad definidos y monitoreados que dificultan la explotación de la vulnerabilidad
2	Media	Existen controles de seguridad pero no se monitorea su efectividad
3	Alta	No existen un procedimiento de identificación de vulnerabilidades

		Amenaza				
		Muy Baja	**Baja**	**Media**	**Alta**	**Muy Alta**
Vulnerabilidad	**Baja**	1	1	2	3	4
	Media	1	2	3	4	5
	Alta	2	3	4	5	5

Tomemos como ejemplo un activo de tipo Aplicativo cuya Vulnerabilidad es:

- Falta de seguridad en el protocolo de autenticación

Y cuyas amenazas asociadas a la vulnerabilidad pudieran ser:

- Robo de información
- Acceso no autorizado

Primero hay que valorar el nivel de exposición de la vulnerabilidad.

	Nivel de Exposición	
Falta de seguridad en el protocolo de autenticación	Baja	1
	Media	2
	Alta	**3**

A continuación se valoran las amenazas asociadas a la vulnerabilidad.

		Amenaza				
		Muy Baja	Baja	Media	Alta	Muy Alta
Falta de seguridad en el protocolo de autenticación	Robo de Información	1	**2**	3	4	5
	Acceso no Autorizado	1	2	3	**4**	5

Utilizando la tabla de Vulnerabilidad VS Amenaza, determinamos el valor final de los Impactos.

		Amenaza				
		Muy Baja	Baja	Media	Alta	Muy Alta
Vulnerabilidad	**Baja**	1	1	2	3	4
	Media	1	2	3	4	5
	Alta	2	**3**	4	**5**	5

- **Impacto** 1 = {3 && 2} = 3
- **Impacto** 2 = {3 && 4] = 5

Se determina la Probabilidad tomando en cuenta los criterios descritos anteriormente (vulnerabilidad y amenaza asociada) y el histórico de incidentes con los escenarios de las Vulnerabilidades y Amenazas. Normalmente para esta actividad se deben realizar entrevistas e identificar si ha habido acciones correctivas, preventivas o el resultado de auditorías pasadas.

Probabilidad		Muy Bajo	Bajo	Medio	Alto	Muy Alto
Falta de seguridad en el protocolo de autenticación	Robo de Información	1	**2**	3	4	5
	Acceso no Autorizado	1	2	3	**4**	5

Con la información anterior se puede realizar la estimación del riesgo utilizando la fórmula de este ejemplo.

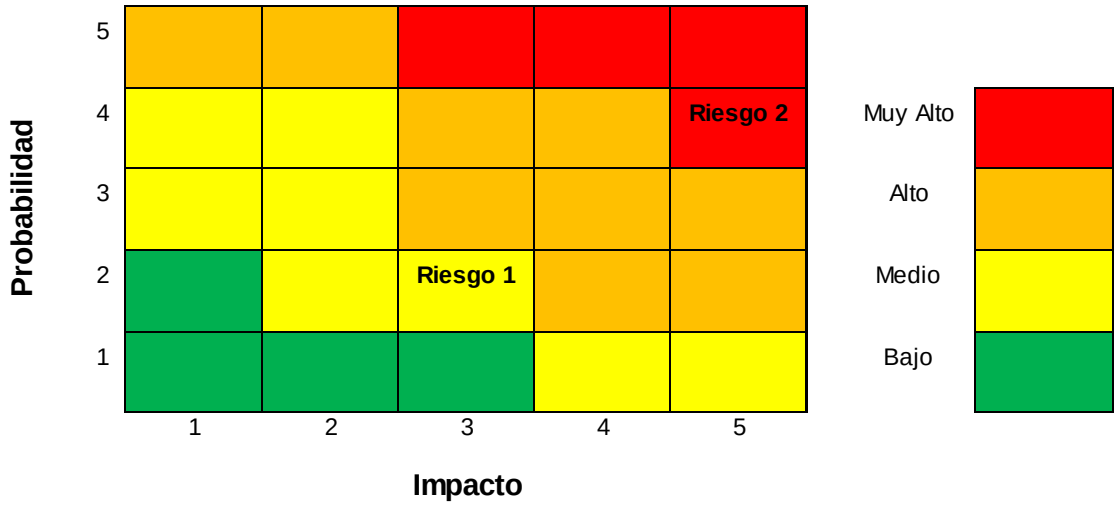
- **Riesgo** 1 = Probabilidad (2) x Impacto (3) = 6
- **Riesgo** 2 = Probabilidad (4) x Impacto (5) = 20

La fórmula de la presente metodología se puede utilizar en una matriz de niveles de riesgo que ayudará a corroborar el correcto valor de riesgo asociado al activo.

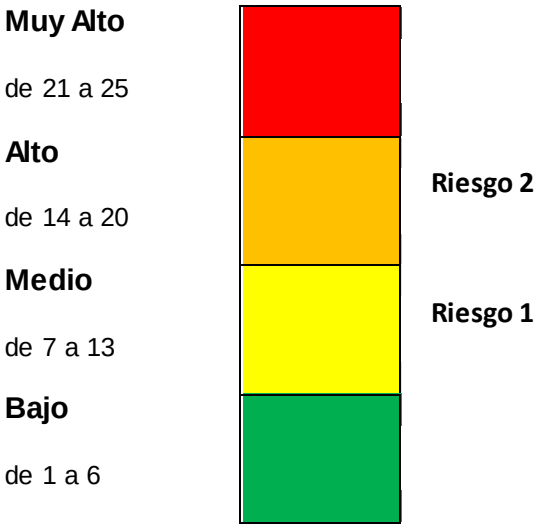
Probabilidad	MB					B					M					A					MA				
Amenaza																									
Vulnerabilidad	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA
Baja	1	1	2	3	4	2	2	4	6	8	3	3	6	9	12	4	4	8	12	16	5	5	10	15	20
Media	1	2	3	4	5	2	4	6	8	10	3	6	9	12	15	4	8	12	16	20	5	10	15	20	25
Alta	2	3	4	5	5	4	6	8	10	10	6	9	12	15	15	8	12	16	20	20	10	15	20	25	25

Una vez obtenidos los niveles de riesgo, se debe determinar un criterio llamado Tolerancia al Riesgo que puede ser determinado por una Matriz de Calor o simplemente determinando los niveles usando límites inferiores y superiores.

Usando una Matriz de Calor para determinar la Tolerancia al Riesgo, el resultado del estudio anterior quedaría de la siguiente manera.



Utilizando una Tolerancia al Riesgo de niveles inferiores y superiores el estudio anterior quedaría de la siguiente manera.



Dependiendo el nivel de madurez de la organización en Gestión de Riesgos es posible determinar diferentes maneras de definir un criterio de Tolerancia al Riesgo y normalmente este criterio es definido en conjunto con la Alta Dirección y se realiza una carta donde se aceptan los niveles y en algunos casos se realiza una descripción de los diferentes niveles de riesgo.

A partir del análisis de los riesgos de los diferentes escenarios de la Organización, se priorizan en un orden descendente, con el escenario de mayor al de menor nivel. Para las intervenciones se deben tomar decisiones sobre cómo actuar sobre los mismos. Las metodologías pretenden actuar sobre los riesgos que estén por fuera del rango aceptable, es decir, intervenir sobre los niveles altos de riesgo.

En la intervención de los riesgos se utiliza distintas medidas que disminuyan la Probabilidad (Medidas de Prevención) o que disminuyen el impacto (Medidas de Protección o Mitigación), o una combinación de ambas.

El siguiente paso de la Gestión de Riesgos es determinar los criterios de tratamiento del riesgo que, en este caso utilizaremos los sugeridos por ISO/IEC 27001 que son los siguientes.

- Aceptar.- En este caso se debe definir un criterio sólido para aceptar un riesgo ya que la organización está dispuesto a aceptar todos los riesgos que tienen un nivel Bajo o en su defecto que su mitigación causaría un gasto mayor al valor del activo.

- Mitigar.- Todos los riesgos que se decidan mitigar deberán someterse a una evaluación para determinar las opciones de controles de seguridad que ayuden a disminuir ya sea la probabilidad, el impacto o incluso ambos.

- Transferir.- Muchas veces los activos son del proveedor o el dueño del activo pertenece a otra área de la Organización y no se tiene forma de realizar actividades de mitigación, por lo que los controles de seguridad los debe aplicar un tercero y en estos casos únicamente se pueden realizar estudios de cumplimiento, auditorías o monitoreo del activo y sus riesgos asociados.

- Evitar.- Está forma de tratamiento es la más radical ya que para evitar un riesgo se debe eliminar la fuente del mismo, eso quiere decir que se deberá prescindir del activo o de ciertas actividades de la Organización.

Es importante tomar en cuenta que muchas organizaciones ligan la aceptación al riesgo con la tolerancia al riesgo, es decir, aceptan todos los riesgos que tengan el nivel más bajo de riesgo que en nuestro ejemplo serían todos los que están en color verde en la Matriz de Calor o todos los que se encuentran en los límites entre 1 y 6.

Esta actividad de aceptación al riesgo es también llamada Apetito al Riesgo, ya que se pudieran aceptar únicamente los niveles de riesgo más bajos y los más altos, se pudieran aceptar los que tengan únicamente un nivel de impacto bajo, etc. En resumen, el Apetito al Riesgo es el umbral de aceptación que la organización pretende asumir sin realizar actividades de control.

3. Implementación de Controles de Seguridad

En la aplicación de controles recomendados para mitigar el riesgo, una organización debería considerar la implementación de controles Técnicos, Administrativos y Operativos o una combinación de estos controles para maximizar la eficacia en la disminución al riesgo. Una correcta implementación de controles de seguridad logra impedir, limitar o frenar una amenaza o disminuir la exposición de la vulnerabilidad de tal forma que se asegurará la misión, visión y objetivos estratégicos de la Organización.

El proceso recomendado para la implementación de controles implicará elegir entre una combinación de controles Técnicos, Administrativos y Operativos que ayudarán a mejorar la postura de la organización en materia de seguridad. Las ventajas y desventajas que una organización tendrá que considerar se ilustran mediante la visualización de las decisiones involucradas en la aplicación. Como ejemplo, un Control Técnico que requiere software adicional de seguridad puede ser más complejo y costoso que un Control de tipo Procedimiento, pero el Control Técnico es probable que sea más eficaz debido a que la aplicación está automatizada. Por otro lado, un Procedimiento podría aplicarse simplemente por medio de un memorando a todas las personas interesadas y haciendo uso de concienciaciones sobre las directrices de seguridad de la Organización para garantizar que los usuarios siempre sigan las políticas vigentes.

Se debe tomar en cuenta que la aplicaciones de los controles por nivel (Administrativo, Operativo y Técnico) debe ser en concordancia con el nivel inferior. La aplicación de estos controles está sujeta a la siguiente gráfica. Ver Ilustración 8.

Ilustración 8

3.1. Controles de Seguridad Técnicos

Los Controles de Seguridad Técnicos para la mitigación de riesgos pueden ser configurados para proteger contra ciertos tipos de amenazas. Estos controles pueden ser simples o complejos y por lo general implican arquitecturas de sistemas, disciplinas de ingeniería y paquetes de seguridad con una combinación de hardware, software y firmware. Todas estas medidas deben trabajar juntas para asegurar los datos críticos y sensitivos, la información y las funciones del sistema de TI. Los controles técnicos pueden agruparse en las siguientes categorías principales, según el propósito principal:

- **Soporte**.- Controles de apoyo son de carácter genérico y subyacen la mayoría de las capacidades de seguridad de TI. Estos controles deben estar en su lugar con el fin de implementar otros controles.
- **Preventivo**.- Los controles preventivos se centran en la prevención de las violaciones de seguridad que se produzcan en el primer lugar.
- **Detectivos**.- Estos controles se centran en la detección y recuperación de un fallo de seguridad.

Ver Ilustración 9.

Ilustración 9

3.1.1. Controles de Soporte Técnicos

Identificación. Este control proporciona la capacidad de identificar de forma única a los usuarios, procesos, y recursos de información. Para llevar a cabo otros controles de seguridad (por ejemplo, control de acceso discrecional DAC, control de acceso obligatorio MAC), es esencial que tanto los sujetos y los objetos sean identificables.

Administración Criptográfica. Las claves criptográficas deben estar bien administradas cuando las funciones criptográficas se implementan en varios otros controles. La Administración Criptográfica incluye la generación, distribución, almacenamiento y mantenimiento de claves.

Administración de Seguridad. Las características de seguridad de un sistema informático deben estar configuradas (ejemplo, activado o desactivado) para satisfacer las necesidades de una instalación específica y dar cuenta de los cambios en el entorno operativo (control de cambios). La seguridad del sistema se puede realizar directamente en el sistema operativo o las aplicaciones.

Protecciones de Sistemas. El fundamento de diversas capacidades de un sistema de seguridad funcional es la base de la confianza en la ejecución técnica. Esto representa la calidad de la aplicación desde la perspectiva tanto del diseño de los procesos utilizados y de la manera en la cual se realizó la aplicación. Algunos ejemplos de las protecciones del sistema son la protección de la información residual (también conocida como la reutilización de objetos), como mínimo privilegio (o "necesidad de saber"), proceso de separación, modularidad, capas, y la minimización de lo que hay que confiar.

3.1.2. Controles Preventivos Técnicos

Autenticación. El control de autenticación proporciona los medios para verificar la identidad de una entidad para asegurar que es quién dice ser. Los mecanismos de autenticación incluyen típicamente son por algo que se sabe, algo que se tiene o algo que se es, recientemente se habla de un tipo de autenticación por posición geográfica Para precisar estos tipos de autenticación, se puede dar como ejemplo que algo que se sabe puede ser una contraseña, algo que se tiene puede ser una tarjeta de proximidad o token, algo que se es se refiere a dispositivos biométricos y por posición geográfica está ligado a coordenadas geográficas o IP.

Autorización. El control de autorización permite la especificación y posterior gestión de las acciones permitidas para un determinado sistema (por ejemplo, el propietario de la información o el administrador de base de datos determina quién puede actualizar un archivo compartido visitada por un grupo de usuarios).

Control de Acceso. La integridad de datos y confidencialidad son aplicadas por los controles de acceso. Cuando un acceso haya sido autorizado para ciertos procesos, es necesario hacer cumplir la política de seguridad definida. Estos controles basados en políticas se aplican a través de mecanismos de control de acceso distribuidos por todo el sistema (por ejemplo, etiquetas MAC sensibilidad del CAD; conjuntos de permisos de archivos, listas de control de acceso, funciones, perfiles de usuario). La eficacia y la fuerza del control de acceso dependerá de la exactitud de las decisiones de control de acceso (por ejemplo, cómo están configuradas las reglas de seguridad) y la implementación de control de acceso (por ejemplo, el diseño de la seguridad del software o hardware).

No repudio. O también dicho rendición de cuentas depende de la capacidad de garantizar que los remitentes no pueden negar el envío de información y que los receptores no pueden negar que lo recibieron. No repudio se extiende tanto a la prevención y detección. Se ha colocado en la categoría de prevención debido a que los mecanismos implementados evitan exitosamente el repudio de una acción (por ejemplo, el certificado digital que contiene la clave privada del propietario y que es conocida sólo por él). Como resultado, este control se aplica típicamente en el punto de transmisión o recepción.

Protección de Comunicaciones. En un sistema distribuido, la capacidad de lograr los objetivos de seguridad es altamente dependiente de las comunicaciones fiables. El control de protección de las comunicaciones garantiza la integridad, disponibilidad y confidencialidad de la información sensitiva y crítica mientras se encuentra en tránsito. Las comunicaciones protegidas utilizan métodos de cifrado de datos (por ejemplo, VPN e IPSEC), y de tecnologías de cifrado (por ejemplo, DES, TDES, RAS, MD4, MD5 y Secure Hash Standard) para minimizar las amenazas de red, tales como el reenvío no autorizado, la interceptación, la detección de paquetes y sniffing

Privacidad de Transacciones. Tanto Gobierno como el sector privado están cada vez más obligados a mantener la privacidad de las personas (por ejemplo LFPDPPP). Los controles de privacidad de transacción (por ejemplo, SSL, secure shell) protegen contra la pérdida de privacidad con respecto a las operaciones realizadas por una entidad.

3.1.3. Controles Detectivos y de Recuperación Técnicos

Auditoría. La auditoría de eventos de seguridad relevantes, el monitoreo y el seguimiento de anomalías de los sistemas son elementos clave en la detección posterior a un hecho, recuperación de fallos de seguridad.

Detección de intrusos y la contención. Es esencial para detectar brechas de seguridad (por ejemplo, intrusión de red, actividades sospechosas) para que se pueda dar respuesta de una manera oportuna. Es de poca utilidad detectar una violación de seguridad si no hay una respuesta eficaz para el evento. Los controles de detección de intrusiones y contención proporcionan estas mismas capacidades.

Prueba de Integridad. El control de prueba de integridad analiza la integridad de los sistemas y sus irregularidades para la identificación de riesgos y amenazas potenciales. Este control no impide que violaciones a las políticas de seguridad, pero las detecta y ayuda a determinar el tipo de acción correctiva necesaria.

Restauración de Estado. Este servicio permite a un sistema volver a un estado que se sabe que es seguro después de una violación de la seguridad.

Detección y Eliminación de Virus. Detección y eliminación de virus y software malicioso instalado en servidores y equipos de cómputo de usuario, identifica y elimina los virus de software para garantizar la integridad del sistema y los datos.

3.2. Controles de Seguridad Administrativos

Los controles de seguridad administrativos en conjunto con los controles técnicos y operativos, se llevan a cabo para gestionar y reducir el riesgo de pérdida y proteger a la misión de una organización. Los controles administrativos se centran en la estipulación de la política de protección de la información, pautas y normas, que se llevan a cabo a través de procedimientos operativos para cumplir con las metas de la organización y las misiones.

Estos controles incluyen lo siguiente:

3.2.1. Controles Preventivos Administrativos

- Asignar los roles y responsabilidades en materia de seguridad para garantizar el cumplimiento de la misión crítica de los sistemas de TI.
- Desarrollar y mantener los planes de seguridad y documentar los controles de seguridad actuales para soportar las actividades operativas a través de un seguimiento al apoyo de la misión de la organización.
- Implementar controles de seguridad al personal, incluyendo la segregación de funciones, implementación de privilegios mínimos y registro de asignación y retiro de privilegios de uso de tecnología de la organización.
- Realizar concienciación sobre la seguridad y realizar capacitación técnica para garantizar que los usuarios finales y los usuarios del sistema son conscientes de las reglas de comportamiento y sus responsabilidades en la protección de la misión de la organización.

3.2.2. Controles Detectivos Administrativos

- Los controles de seguridad al personal, incluyen la liquidación de personal al término de contratación, investigación de antecedentes y rotación de actividades.
- Realizar una revisión periódica de los controles de seguridad para garantizar que los controles son efectivos.
- Realizar auditorías periódicas.
- Llevar a cabo la gestión de riesgos para evaluar y mitigar los riesgos
- Autorizar y aceptar el riesgo residual.

3.2.3. Controles de Recuperación Administrativos

- Proporcionar continuidad de soporte y desarrollar, probar y mantener la continuidad de las operaciones para proporcionar la reanudación del negocio y garantizar la continuidad de las operaciones durante emergencias o desastres
- Establecer la capacidad de respuesta a incidentes y preparar al personal para reconocer, reportar y responder al incidente y devolver el sistema el estado operativo normal.

3.3. Controles de Seguridad Operativos

La normatividad de seguridad de una organización debe establecer controles de seguridad y guías que aseguren la correcta ejecución de procedimientos implementados en los activos y recursos para forzar una armónica operación de acuerdo a las metas y misión de la Organización. La alta dirección juega un papel fundamental en la supervisión de la implementación de políticas y para garantizar el establecimiento controles operativos apropiados.

Los controles operativos aplicados de acuerdo con un requerimiento básico (por ejemplo, controles técnicos) y las buenas prácticas de la industria, se utilizan para corregir las deficiencias operativas que pueden ser ejercidos por las amenazas potenciales de los recursos. Para garantizar la coherencia y uniformidad en las operaciones de seguridad, se deben realizar procedimientos y métodos paso a paso claramente definidos, documentados y mantenidos.

3.3.1. Controles Preventivos Operativos

- Control de acceso a medios y eliminación de los mismos (por ejemplo, control acceso físico y métodos de desecho de información).
- Limitar la distribución de información (por ejemplo, el uso de etiquetado).
- Control de virus.
- Salvaguardar la instalación informática (por ejemplo, guardias de seguridad, procedimientos para la recepción de visitantes, sistemas de tarjetas electrónicas, accesos biométricos de control, gestión y distribución de llaves y cerraduras, barreras y vallas).
- Aseguramiento de cajas de cableado.
- Copias de seguridad (por ejemplo, procedimientos para disponer regularmente de datos y copias de seguridad del sistema de archivos, registros que guardan todos los cambios de base de datos que se utilizarán en diversos escenarios de recuperación).
- Establecer procedimientos fuera de las instalaciones de almacenamiento y seguridad.
- Proteger las laptops, y PC's.
- Proteger los activos de TI del fuego (por ejemplo, requisitos y procedimientos para el uso de extintores, lonas, sistemas de aspersión en seco, sistema de extinción de incendios).

- Fuente de energía de emergencia (por ejemplo, los requisitos para sistemas de alimentación ininterrumpida).
- Controles de humedad y temperatura en los centros de datos, archivo, PBX y bóvedas (por ejemplo, el funcionamiento de los acondicionadores de aire, la dispersión de calor).

3.3.2. Controles Detectivos Operativos

- Proporcionar seguridad física (por ejemplo, el uso de detectores de movimiento, control de circuito cerrado de televisión, sensores y alarmas)
- Garantizar la seguridad del medio ambiente (por ejemplo, el uso de detectores de humo y fuego, sensores y alarmas).

3.4. Costo-Beneficio

Para asignar recursos y poner en práctica el costo-beneficio de los controles, las organizaciones, después de haber identificado todos los posibles controles y evaluar su viabilidad y eficacia se realiza un análisis coste-beneficio por cada control propuesto para determinar qué controles son necesarios y apropiados para sus circunstancias.

El análisis costo-beneficio puede ser cualitativo o cuantitativo. Su propósito es demostrar que los costos de aplicación de los controles pueden ser justificados por la reducción en el nivel de riesgo. Por ejemplo, la organización puede no querer gastar $1,000 en un control para reducir el riesgo de $200.

Un análisis de costo-beneficio para propuestas de nuevos controles o controles mejorados abarca lo siguiente:

- Determinar el impacto de la implementación de los controles nuevos o mejorados
- Determinar el impacto de la no aplicación de los controles nuevos o mejorados
- La estimación de los costes de la implementación. Estos pueden incluir, pero no se limitan a lo siguiente:
  - Equipamiento técnico y las compras de software
  - Reducción de la eficacia operativa si el rendimiento del sistema o la funcionalidad se reduce para aumentar la seguridad
  - El costo de la implementación de políticas y procedimientos adicionales
  - El costo de la contratación de personal adicional para implementar las políticas propuestas, procedimientos o servicios

- Los costos de formación
- Los costos de mantenimiento

- Evaluación de los costos de implementación y los beneficios contra la criticidad de los sistemas y los datos para determinar la importancia de la organización en la implementación de nuevos controles teniendo en cuenta sus costos y su impacto.

La organización tendrá que evaluar los beneficios de los controles en términos de mantener una postura aceptable para la misión de la organización. Así como hay un costo en la implementación de un control necesario, hay un costo no implementarlo. Al relacionar el resultado de no implementar el control, las organizaciones pueden determinar si es factible renunciar o no a la implementación.

Ejemplo de análisis: Se cuenta con un sistema X con información privada de los empleados, información crítica y sensitiva que es utilizada para el cumplimiento de la misión de la organización. Sin embargo, el sistema no está habilitado para generar pistas de auditoría y se requiere determinar el costo-beneficio de esta funcionalidad.

Los puntos 1 y 2 al impacto intangible (por ejemplo, los factores de disuasión) para implementar o aplicar el nuevo control. El punto 3 enumera los elementos tangibles (por ejemplo, el costo real).

1) Impacto de activar la función de auditoría del sistema: La función de auditoría del sistema permite al administrador del sistema de seguridad monitorear las actividades de los usuarios, pero el rendimiento del sistema se verá afectado y por lo tanto afectará la productividad del usuario. Asimismo, se requerirán recursos adicionales, tal como se describe en el punto 3.

2) Impacto de no activar la función del sistema de auditoría: Las actividades de los usuarios y las violaciones a las políticas de seguridad no podrán ser monitoreadas y rastreadas si la función de auditoría está desactivada. La seguridad no se puede maximizar para proteger los datos confidenciales y la misión de la organización.

3) Estimación del costo de la habilitación de la generación de pistas de auditoría.

Consideraciones de Implementación	Costo
Costo de habilitar la característica de auditoría	$ 0
Personal requerido para monitoreo y resguardo de las pistas de auditoría	$ XX,XXX
Capacitación del personal a cargo	$ XX,XXX
Agregar software que soporte la generación de filtrado y reporteo	$ XX,XXX
Espacio de almacenamiento requerido	$ XX,XXX
Total	$ XX,XXX

Los directivos de la organización deben determinar lo que constituye un nivel aceptable de riesgo para la misión. El impacto de un control puede entonces ser evaluado y se determinará si el control será incluido o excluido.

Después la organización determina un rango de niveles de riesgo factibles. Este rango puede variar entre las organizaciones, sin embargo, las siguientes reglas se aplican para determinar el uso de los nuevos controles:

- Si el control reduciría el riesgo más de lo necesario, y si existe una alternativa menos costosa
- Si el control costaría más que la reducción del riesgo proporcionado
- Si el control no reduce el riesgo suficientemente, de ser el caso, busque más controles o un control diferente
- Si el control proporciona una reducción de riesgo aceptable y está en balance con el costo beneficio, de ser así, el control es adecuado.

Con frecuencia, el costo de implementar un control es más tangible que el costo de no implementarlo. Como resultado de ello, la alta dirección juega un papel crítico en las decisiones relativas a la aplicación de medidas de control para proteger la misión de la organización.

3.5. Identificación de Controles de Seguridad

Continuando con el ejemplo utilizado para la identificación del nivel de riesgo del Capítulo II Análisis y Evaluación de Riesgos, se realizará una matriz de identificación de controles a muy alto nivel de acuerdo a la norma ISO/IEC 27002 donde se demostrará de manera informativa una técnica utilizada para la identificación de controles de seguridad.

La primera actividad será la de identificar los once dominios de la ISO/IEC 27002 y relacionarlos con el activo tipo Aplicativo de nuestro ejemplo para determinar cuáles son los que aplican y descartar desde un principio el resto. Para realizar esta identificación, se deberá entender el objetivo de cada dominio y el alcance que tiene sobre la infraestructura de la organización y los dominios tecnológicos de la misma.

Dominio ISO 27002	Objetivo del Dominio
A.5 Política de Seguridad de la Información.	Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.
A.6 Organización de la Seguridad de la Información.	Manejar la seguridad de la información dentro de la organización. Mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos.
A.7 Gestión de Activos de Información.	Lograr y mantener una apropiada protección de los activos organizacionales. Asegurar que la información reciba un nivel de protección apropiado.
A.8 Seguridad de los Recursos Humanos.	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios. Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus

	responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano. Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada.
A.9 Seguridad Física y Ambiental.	Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización. Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.
A.10 Gestión de las Comunicaciones y Operaciones.	Asegurar la operación correcta y segura de los medios de procesamiento de la información. Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros. Minimizar el riesgo de fallas en el sistema. Proteger la integridad del software y la integración. Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información. Asegurar la protección de la información en redes y la protección de la infraestructura de soporte. Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales. Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa. Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro. Detectar las actividades de procesamiento de información no autorizadas.
A.11 Control de Accesos.	Controlar el acceso a la información.

	Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información. Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información. Evitar el acceso no autorizado a los servicios de la red. Evitar el acceso no autorizado a los sistemas operativos. Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación. Asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móviles.
A.12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.	Garantizar que la seguridad sea una parte integral de los sistemas de información. Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones. Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos. Garantizar la seguridad de los archivos del sistema. Mantener la seguridad del software y la información del sistema de aplicación. Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.
A.13 Gestión de Incidentes en la Seguridad de la Información.	Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna. Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.
A.14 Gestión de Continuidad del Negocio.	Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna

A.15 Cumplimiento.	Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad. Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional. Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

La identificación de los dominios se puede realizar utilizando una simple matriz donde se marcaran los dominios aplicables.

Activo	Vulnerabilidad	Amenaza	5.- Política de Seguridad	6.- Organización de la Seguridad de la Información	7.- Administración de Activos	8.- Recursos Humanos	9.- Seguridad Física/Ambiental
Aplicativo	Falta de seguridad en el protocolo de autenticación	Robo de Información	✗	✗	✗	✗	✗
		Acceso no Autorizado	✗	✗	✗	✗	✗

Activo	Vulnerabilidad	Amenaza	10.- Comunicaciones y Operaciones	11.- Control de Acceso	12 Adquisición, Desarrollo y Mantenimiento de Sistemas	13 Gestión de Incidentes	14 Continuidad del Negocio	15 Cumplimiento
Aplicativo	Falta de seguridad en el protocolo de autenticación	Robo de Información	✗	✓	✓	✗	✗	✗
		Acceso no Autorizado	✓	✓	✓	✗	✗	✗

El paso a seguir será la identificación de los controles de seguridad de cada uno de los dominios de la norma que se escogieron como aplicables de acuerdo a las características del activo, del tipo de vulnerabilidad y de la amenaza.

Activo	Vulnerabilidad	Amenaza	10.10.1 Registro de auditoría	10.10.2 Uso del sistema de monitoreo	11.2.2 Gestión de privilegios	11.6.1 Restricción del acceso a la información	12.1.1 Análisis y especificación de los requerimientos de seguridad	12.3.1 Política sobre el uso de controles criptográficos
Aplicativo	Falta de seguridad en el protocolo de autenticación	Robo de Información	✗	✗	✗	✓	✓	✓
		Acceso no Autorizado	✓	✓	✓	✓	✓	✗

En la tabla anterior se pueden ver que existen ocho controles de seguridad aplicables para la mitigación de los riesgos identificados, esto no quiere decir que se van a aplicar todos los controles, únicamente nos ayudará a resaltar los controles que mitiguen más riesgos.

Se tiene la falsa creencia que entre más controles de seguridad se implementen, la certidumbre del riesgo disminuirá considerablemente e incluso el impacto a la organización será prácticamente nulo, pero, en realidad, entre más controles de seguridad se apliquen, se generarán más puntos de explotación y el esfuerzo para monitorear estos puntos podría ser mucho más elevado que las actividades operativas normales.

Los criterios recomendados para la implementación de controles serán los siguientes y serán únicamente informativos más no limitativos.

- Identificar los controles por tipo de activo.
- Identificar los controles que mitiguen la vulnerabilidad como punto principal y se afine su elección de acuerdo al tipo de amenaza.
- Identificar los controles que mitiguen más vulnerabilidades (utilizando la matriz anterior).
- Identificar los controles de acuerdo a su tipo y agruparlos para su monitoreo (Operativos, Administrativos y Técnicos).

La selección de los controles que se hará para el presente ejemplo será utilizando los controles que mitiguen más riesgos, debido a esto tenemos que los controles 11.6.1 y

12.1.1 son los que cumplen con dicho requisito y de esta manera limitamos el exceso de actividades de mitigación además de reducir los esfuerzos y costos de monitoreo de efectividad y eficiencia.

Activo	Vulnerabilidad	Amenaza	11.6.1 Restricción del acceso a la información	12.1.1 Análisis y especificación de los requerimientos de seguridad
Aplicativo	Falta de seguridad en el protocolo de autenticación	Robo de Información	✔	✔
		Acceso no Autorizado	✔	✔

La implementación de los controles de seguridad se puede realizar de diferentes maneras, pero es necesario que se tenga debidamente documentado el tipo de control y los objetivos primordiales que deberá cumplir, así como un responsable de implementación.

No existe una manera genérica de realizar fichas de definición para la implementación de controles de seguridad, pero para fines ilustrativos se utilizará una que se recomienda por experiencia propia.

Control	Objetivo del Control	Nivel del Control	Tipo de Control
11.6.1 Restricción del acceso a la información	Limitar el acceso de los usuarios finales y del personal de soporte a la información y las funciones de los activos en concordancia con la política de acceso definida.	Operativo	Preventivo
12.1.1 Análisis y especificación de los requerimientos de seguridad	Los requerimientos de seguridad para aplicaciones comerciales, para el desarrollo de sistemas nuevos realizados In-House o las mejoras a los sistemas ya existentes, se debieran especificar de manera previa a realizar cualquier actividad de desarrollo o adquisición	Administrativo	Preventivo

Las fichas de definición de controles son utilizadas con el propósito de tener claramente documentadas las actividades necesarias que se deberán llevar a cabo por los responsables de control y para tener una trazabilidad correcta de los niveles de seguridad e incluso para apoyar en la definición de métricas de seguimiento y monitoreo de la eficacia y eficiencia en el cumplimiento del objetivo descrita en cada ficha.

Una vez definidas las fichas se desarrollan los controles de acuerdo a los requerimientos descritos en el objetivo, el nivel de control y el tipo de control.

3.6. Desarrollo de los Controles de Seguridad

Se deberá tomar como supuesto para el presente ejercicio el hecho de que existe un manual de políticas de la Organización en el que ya se encuentra definida una Política de Control de Acceso (Un tipo de Control de Seguridad Preventivo Administrativo).

Control ISO 27002	11.6.1 Restricción del acceso a la información
Objetivo	Limitar el acceso de los usuarios finales y del personal de soporte a la información y las funciones de los activos en concordancia con la política de acceso definida.
Nivel de Control	Operativo
Actividad	Identificar la existencia de procedimientos de asignación de derechos de acceso al momento de crear perfiles de usuario. Es importante crear perfiles de acceso definidos dentro de una matriz en la que se asignen los derechos que tienen sobre las características de la información y los sistemas que las procesan, transmiten y almacenan.
Guía de Implementación	a) Controlar los derechos de acceso de los usuarios, por ejemplo leer, escribir, borrar y ejecutar b) Controlar los derechos de acceso de todas las aplicaciones c) Asegurar que las entradas y salidas se envían sólo a las terminales autorizadas.
Descripción	Se mejorarán y/o crearan procedimientos específicos para la asignación de derechos de acceso conforme a un legítimo requerimiento para el cumplimiento de los deberes y responsabilidades considerando los principios de: • Segregación de Funciones • Need to Know • Least Privilege
Responsable	Nombre del responsable del control

Control ISO 27002	12.1.1 Análisis y especificación de los requerimientos de seguridad
Objetivo	Declarar los requisitos mínimos de seguridad de acuerdo a las actividades de negocio para la creación de nuevos sistemas de información, mejoras a los sistemas de información existentes o para la adquisición de sistemas comerciales.
Nivel de Control	Administrativo
Actividad	Reflejar el valor comercial de los activos de información involucrados, y el daño comercial potencia que podría resultar de una falla o ausencia de seguridad. Implementar la seguridad debiera ser integrado en las primeras etapas de los proyectos de sistemas de información.
Guía de Implementación	a) Se deben considerar controles de seguridad automatizados en los sistema de información para apoyar los controles manuales existentes b) Los requisitos de seguridad de la información y procedimientos para implementar la seguridad deben incluirse en las primeras etapas de los proyectos. Los controles incluidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación c) Si los productos son comprados se deberá formalizar un proceso de pruebas y adquisición. Los contratos con los proveedor deberán satisfacer los requisitos de seguridad de la Organización
Descripción	Se considera apropiado, por ejemplo que por razones de costo la gerencia puede desear hacer uso de productos evaluados y certificados independientemente. Los requerimientos de seguridad en la fase de requerimientos de un proyecto y debieran ser justificados, acordados y documentados como parte del caso comercial general para un sistema de información.
Responsable	Nombre del responsable del control

4. Poniendo a Prueba los Controles

Se deberán realizar actividades de medición de forma planificada y documentando adecuadamente la selección de controles y objetivos de control para su medición, especificando métricas y definiendo una recopilación de datos, análisis y presentación de informes. La planificación debe incluir la identificación de los recursos financieros, humanos y de infraestructura (física y herramientas).

Las metas de medición deben especificar claramente las razones y objetivos de acuerdo a aciertas consideraciones entre las que se pueden incluir las siguientes:

- El rol que tiene la Seguridad de la Información en una Organización para el cumplimiento de su misión y objetivos de negocio
- Mejora continua de objetivos y metas
- Requerimientos legales, contractuales y regulatorios aplicables
- Estructura organizacional
- Costo-beneficio de implementación de mediciones de control de la Seguridad de la Información

El alcance del proceso de medición se genera en términos del alcance de la Administración de la Seguridad, que comúnmente se define de acuerdo a ISO/IEC 27001

para garantizar un nivel adecuado de rendición de cuentas y capacidad de administración de actividades de medición.

La medición implica un proceso de obtención de información acerca de la efectividad de la Administración de la Seguridad.

Los controles y objetivos de control utilizan un método de medición, una función de medición, un modelo de análisis y evaluación de esa información contra los criterios de decisión para llevar a cabo una mejora continua de la Administración de la Seguridad.
Ver Ilustración 10.

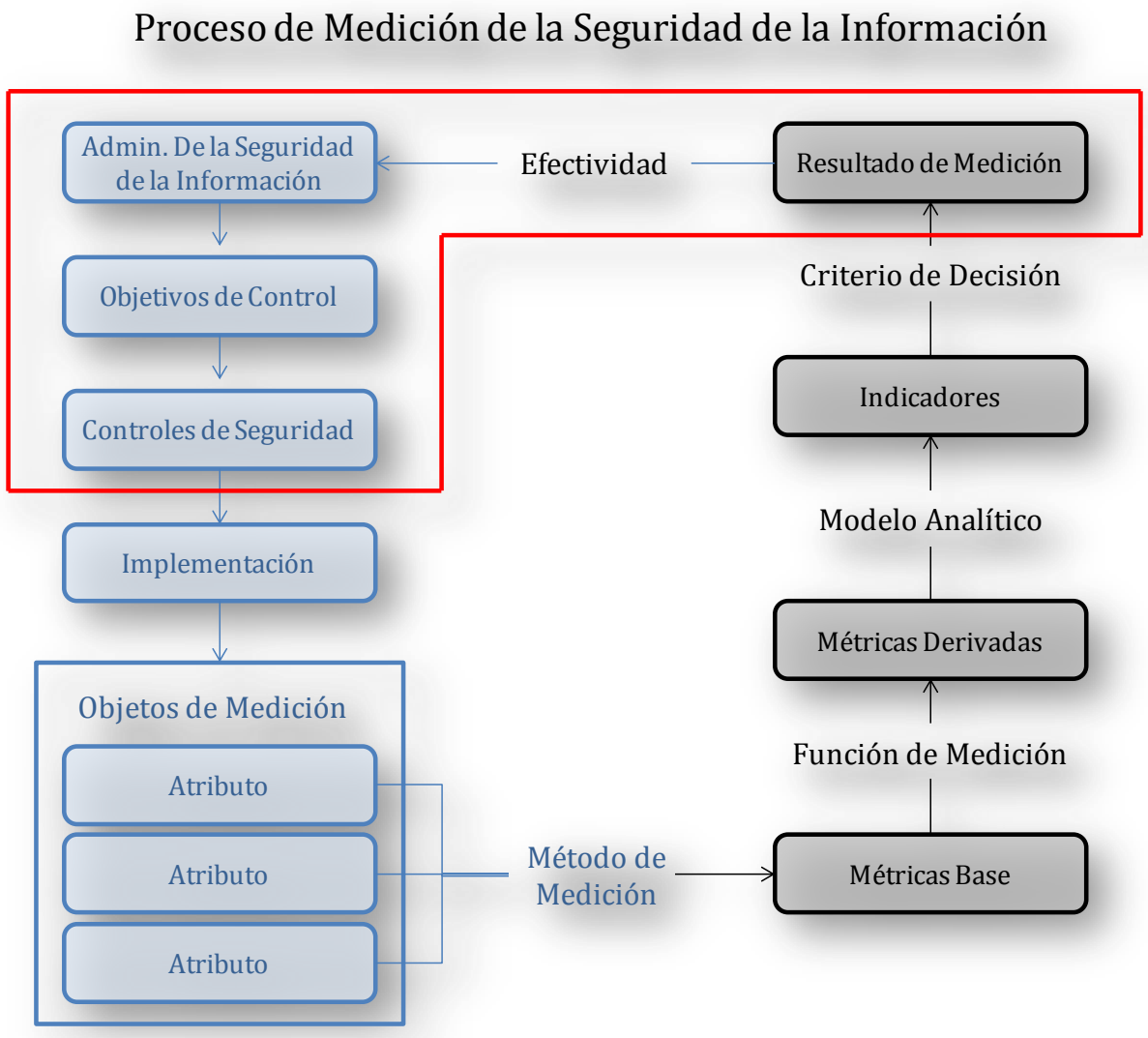


Ilustración 10

El proceso de medición consiste en lo siguiente:

- Identificación de la métrica base mediante el uso de un método de medición relevante para recoger atributos aplicables de los objetos de medición.

  Cada objeto de medición de los controles que han aplicado puede tener muchos atributos, algunos de los cuales pueden ser de interés para la medición.

  Un atributo dado puede ser utilizado para varias mediciones diferentes. El número de usuarios que han recibido concientización acerca de la seguridad es un ejemplo de una métrica base.

- Definición de métrica derivada por aplicación de una función de medición de métrica base

  Cuando la función de medición se aplica a una métrica de una sola base, la métrica derivado será igual a la métrica base aplicable. Una métrica base individual puede ser utilizada para varias métricas derivadas diferentes. En algunos casos, las métricas base pueden ser insumos en el modelo de análisis incluyendo las métricas derivadas

  El porcentaje de usuarios que recibieron concienciación sobre seguridad es un ejemplo de métrica derivada

- Obtener indicadores mediante la aplicación de un modelo analítico a las métricas derivadas utilizando la aplicación de criterios de decisión.

  Los indicadores individuales proporcionan información sobre cómo comparar las métricas derivadas contra los criterios de decisión para cada indicador individual.

  La combinación de porcentaje de usuarios que recibieron concienciación sobre la seguridad de la formación y el porcentaje de usuarios que han firmado un acuerdo de usuario produciría un indicador.

- Interpretación de los indicadores mediante la aplicación de criterios de decisión para proporcionar un insumo en la toma de decisiones de las partes interesadas.

  Basado en un criterio de decisión específico de la organización que defina porcentajes aceptables para las métricas derivadas (en el ejemplo de la concienciación), se tomará una decisión si el resultado de la medición indica una mejora en la concienciación de seguridad y eficacia de la formación.

- Producir resultados de medición para obtener una evaluación general de la eficacia de la Administración de la Seguridad y de los controles de seguridad a través de la comparación de indicadores contra los criterios de decisión aplicables.

  En este ejemplo, la conciencia de seguridad de la información y el indicador de formación se combina con otros indicadores para comprender la evaluación global de la eficacia de la Administración de la Seguridad.

4.1. Selección de Controles de Seguridad Incluidos en la Medición

Dependiendo de los recursos y capacidades de una Organización, el alcance inicial de la medición de los controles de la seguridad de la información deberá limitarse a la identificación de las actividades, productos y servicios a los que se les dan mayor prioridad por la alta dirección. Al paso del tiempo el alcance deberá ampliarse para alinearse a las actividades, productor y servicios de prioridad menor pero que son igualmente importantes para el cumplimiento de las metas de la organización.

La selección de mediciones para los controles y objetivos de control incluirá algunos de los siguientes puntos:

- Identificar los controles y objetivos de control seleccionados para su implementación como resultado de la Evaluación de Riesgos
- Priorizar los controles y objetivos de control basándose en los siguientes criterios
  - Recursos y capacidades de la Organización
  - Requerimientos solicitados por las partes interesadas de la Organización (gerencias, alta dirección, etc.)
  - Política de Seguridad de la Información
  - Información específica de los requerimientos legales, contractuales y regulatorios.
- Valor de la información en relación con los costos de medición

4.2. Identificación de los Objetos de Medición

La medición de la Seguridad de la Información puede ser aplicada a distintos objetivos de negocio dentro del contexto de la Administración de la seguridad.

- Usando metas de medición seleccionadas para objetivos de negocio específicos
- Especificando entidades y atributos únicos de cada entidad que ayudarán a proporcionar información que ayudará a la implementación y efectividad de los controles y objetivos de control

Los datos de los objetivos de negocio y sus correspondientes entidades servirán como insumo para mediciones individuales.

- Unidades de negocio
- Locaciones geográficas
- Productos y servicios
- Procesos y Sub procesos
- Activos de información

El tamaño de los objetivos de negocio debe ser cuidadosamente seleccionado para asegurar que los resultados de las mediciones sean coherentes. Si los objetivos son muy amplios, los resultados de las mediciones podrían ser muy vagos si es que las entidades son muy pequeñas y el costo de la medición de cara al beneficio sería muy alto.

4.3. Desarrollo y Selección de Métricas

Las organizaciones deben utilizar una variedad de recursos disponibles para identificar y adaptar las medidas de seguridad de la información.

Cada medida debe ser documentada en detalle según las necesidades de la organización. La documentación debe incluir al menos lo siguiente:

- Nombre y código de la métrica
- Eficacia del control u objetivo de control que se medirá
- Tipo de métrica para indicar si es una medida de cumplimiento o desempeño
- Objetivo de la métrica
- Método de medición: Objeto de la medición y atributos que proporcionan los datos de medida, fórmula de la métrica y criterios de validación de atributos

- Para las métricas base, los datos de medición obtenidos incluidas las escalas y unidades de medida serán utilizados para definir el método de métrica.
- Para las medidas derivadas, las funciones de medición se agregan a las métricas base.

- Procedimientos de recolección de datos.
- Los interesados en las métricas, como pueden ser los propietarios de la información, información del cliente, recolector de información y revisor métricas
- Ciclo de vida de la métrica: frecuencia de ejecución de la métrica, análisis y generación de informes
- Objetos de negocio relevantes
- Criterios
- Indicadores correspondientes y formatos de informes

4.3.1. Verificación del Método de Medición

Un método de medición específico se debe aplicar a cada objeto de medición en combinación con un atributo crítico para extraer información específica que se puede utilizar como base para el cálculo de la medición base. El método define los atributos del objeto de medición en la métrica.

Las métricas de medición pueden ser subjetivas u objetivas. Los métodos subjetivos implican la cuantificación usando juicio humano, mientras que los métodos objetivos implican la cuantificación basada en reglas numéricas tales como contar que puede ser implementado a través de medios humanos o automatizados.

Los métodos de medición pueden usar fuentes de datos como las siguientes:

- Reportes de auditoría internos o externos
- Resultados de análisis de riesgos
- Resultados de cuestionarios e investigaciones
- Registros de eventos como logs, reportes estadísticos y pistas de auditoría
- Reportes de incidentes, principalmente de aquellos que tuvieron un impacto
- Estadísticas

- Resultados de pruebas como pruebas de penetración, ingeniería social, herramientas de cumplimiento y herramientas de seguridad

Las operaciones de los métodos de medición pueden involucrar actividades como el conteo de eventos u observando el desempeño de los controles al paso del tiempo. El mismo método de medición puede ser aplicado a múltiples atributos.

El método de medición mapea la magnitud del atributo medido a un valor. El tipo de escala depende de la naturaleza de la relación entre los valores de la escala. El método de medición por lo general afecta al tipo de escala que se pueden utilizar sin problemas con un atributo dado. Como un ejemplo de escala, los métodos subjetivos de medición por lo general sólo son compatibles con escalas ordinales o nominales.

Una unidad de medición a menudo se asocia con una escala. Sólo cantidades expresadas en las mismas unidades de medición son directamente comparables.

Los criterios de verificación deberán ser definidos y documentados para cada método de medición.

Ya sea basándose en métodos manuales (por ejemplo, investigación, observación, autoevaluación) o métodos basados en el uso de fuentes de datos automatizados, los métodos de medición requieren la verificación sustantiva para establecer un nivel de confianza en el valor del atributo. Los métodos de medición pueden ser verificados mediante pruebas con las entidades con valores de atributos conocidos o mediante el uso de otros métodos de ensayo.

La verificación de los métodos de medición debe tener lugar durante un período de tiempo y debe incluir un número suficiente de ensayos individuales para proporcionar una muestra estadísticamente válida de los atributos para la creación y análisis de las métricas base.

Dentro de un ambiente de operación normal el tamaño de las muestras de prueba dependerán de:

- La frecuencia con la que el control es ejecutado
- El riesgo de fallo de un control

Los métodos de medición deben ser consistentes al paso del tiempo por lo que las métricas base tomadas en diferentes etapas de tiempo deben ser comparables y esas mediciones e indicadores basados en las métricas sean igualmente comparables. Por ejemplo, las métricas deben ser comparables y consistentes entre departamentos o entidades diferentes de la misma organización.

4.3.2. Función de Medición

Una función de medición se debe aplicar a dos o más métricas base para crear métricas derivadas. En algunos casos, las métricas base pueden ser insumo del modelo de análisis además de las métricas derivadas. Cuando una métrica derivada se basa en una métrica de una sola base la función de medición es innecesaria.

Las funciones de medición definen como las métricas base se pueden agrupar en métricas derivadas. Varias métricas derivadas pudieran utilizar la misma función.

Las funciones de medición pueden implicar una variedad de técnicas, tales como promedio de todas las medidas de base, la aplicación de ponderaciones a métricas base, o la asignación de valores cualitativos a las métricas base antes de reunirlos en métricas derivadas. Las funciones de medición podrán prever la combinación de métricas base que utilizan diferentes escalas, tales como porcentajes y resultados cualitativos de evaluación.

Una fórmula para el cálculo de cada métrica debe ser definida y documentada. Una fórmula para una métrica derivada se basa en las métricas base que componen la métrica derivada y la función de medición usada para obtener métricas derivadas.

4.3.3. Partes Interesadas

Para cada métrica se deberá identificar de manera apropiada a todas las partes interesadas y se deberán documentar.

- Responsable de la métrica. Persona u Organización que es propietaria de la información de las entidades y atributos usados para la creación de las métricas base y que además es responsable de la métrica
- Clientes (internos o externos). Persona u Organización que requiere y exige las métricas para realizar sus actividades de negocio
- Recolector. Persona u Organización responsable de recolectar, registrar y almacenar la información de los atributos de entidades.
- Comunicador. Persona u Organización responsable de analizar la información y comunicar las métricas
- Revisor. Persona u Organización que revisa los criterios de evaluación de métricas para verificar su efectividad

4.3.4. Validación de la Selección de Atributos

Un objeto de medición puede tener varios atributos de Seguridad de la Información. A fin de que las métricas de cumplimiento o desempeño se realicen correctamente, se deberán evaluar ciertos atributos de los objetos para su selección.

Los atributos deben ser validados con el fin de garantizar que sean los seleccionados han sido los más apropiados para la medición. Además, debe realizarse una prueba para determinar si es un número apropiado de atributos los que se han seleccionado para asegurar una medición eficaz.

La característica de estos atributos determinan los tipos de métodos de medición se utilizarán para determinar las métricas de base (por ejemplo, cualitativa o cuantitativa).

El proceso de selección de atributos y validación debe garantizar métricas resultantes del atributo seleccionado o atributos que son útiles para indicar la efectividad de la Administración de la Seguridad. La selección de atributos no debe hacerse únicamente en los datos fáciles de obtener o atributos fáciles de medir.

4.3.5. Modelo Analítico

Para cada métrica, debe definirse un modelo analítico con el fin de transformar una o más métricas derivadas en un indicador. En algún momento un modelo analítico puede tan simple como la transformación de una sola métrica derivada en un indicador. Se debe tener en cuenta que los criterios de decisión que se aplican a un indicador también deben ser considerados cuando se define el modelo analítico. El modelo analítico combina medidas de una manera que produce una salida que puede evaluarse utilizando criterios de negocio significativos para los interesados en la Administración de la Seguridad.

4.3.6. Indicadores y Formatos de Reportes

Para cada indicador que será reportado a los clientes (internos o externos) se deberá definir un formato específico de tal manera que quede documentado y sea utilizado las veces que sea necesario para homologar la entrega de información.

Los indicadores se producirán mediante la agregación de métricas derivadas e interpretándolas basándose en criterios de decisión. Los formatos de reportes representarán visualmente las métricas con la ayuda de explicaciones verbales acerca de los indicadores. Los formatos de presentación de informes se deberán personalizar para satisfacer las necesidades de la información.

4.3.7. Criterios de Decisión

Para cada indicador, deben ser identificados y documentados los criterios de decisión para orientar acciones concretas para los clientes con respecto a las expectativas del progreso de la métrica y los umbrales para iniciar acciones de mejora basados en las métricas. Los criterios de decisión establecen una meta de éxito. El grado de éxito se basa en la proximidad del resultado hacia los criterios establecidos. La mecánica de los criterios de decisión establecidos difiere de los indicadores derivados de cumplimiento y métricas de desempeño.

Para los indicadores derivados de las métricas de cumplimiento, los criterios se establecen para presentar la realización de tareas específicas o de la aplicación de controles específicos previstos en la seguridad de la información. La Administración tendrá que aplicar el razonamiento cualitativo y subjetivo para determinar los criterios apropiados para los indicadores a partir de métricas de desempeño.

Aunque todas las organizaciones desean una implementación efectiva de los controles y los objetivos de control, entregas eficientes de servicios de seguridad e impacto mínimos de los eventos de seguridad en su misión, los indicadores asociados serán diferentes para los objetivos de negocio. Una organización deberá establecer criterios de decisión para estos indicadores y deberá estar listo para ajustar los criterios, sobre la base de indicadores reales, una vez que se obtienen.

La organización también puede decidir no establecer metas de los indicadores hasta que se recojan los datos iniciales y se puedan utilizar como base de referencia de rendimiento. Una vez que la línea de base se obtiene y se determinaron las medidas correctivas, los criterios de decisión y fases de aplicación podrán definirse de manera realista. Si los criterios de decisión no se pueden establecer aun habiendo obtenido una línea base, la gerencia deberá evaluar si los objetivos en la medición y las métricas están proporcionando el valor esperado para la organización.

El establecimiento de criterios de decisión y líneas de base de métricas pueden facilitar los datos históricos que se refieran a estas métricas disponibles. Las tendencias observadas en el pasado, darán una idea de los rangos de rendimiento que han existido anteriormente y orientan la creación de criterios de decisión reales.

4.4. Validación de Métricas

Las métricas deben ser validadas para asegurar su usabilidad y el costo contra su efectividad. Se recomienda considerar los siguientes criterios:

- Estratégico. Alineado a los objetivos de negocio de la Organización y las necesidades de las partes interesadas
- Cuantitativo. Proporcionar información objetiva y empírica
- Interpretativo. Insumos objetivos que apoyarán con la interpretación de la información
- Costo-efectividad. El costo de la recopilación de información debe ser balanceada contra las pérdidas potenciales a los que el valor de la métrica se relaciona
- Verificable. Revisores externos o terceras partes deberán poder evaluar la información y concordar con los resultados
- Significativo. La información debe proporcionar datos significativos acerca de la aplicación efectiva de los controles y los objetivos de control al paso del tiempo para permitir realizar una evaluación del impacto de los cambios o la consistencia de los resultados
- Usabilidad. Los resultados deben soportar las decisiones significativas de negocio
- Indivisible. La información debe ser copilada de la forma más discreta en un nivel no analizado de ser posible
- Bien definido. Se deberán documentar características como la frecuencia, fórmulas, evidencias e indicadores
- Repetible. Las métricas deben producir resultados comparables y reproducibles

4.5. Recolección de Información, Análisis y Reportes

Análisis de datos y presentación de informes de las métricas. Los procedimientos deben especificar el método de análisis de datos, la frecuencia, el formato y los métodos para informar sobre los productos de información. Se debe especificar la gama de herramientas necesarias para llevar a cabo el análisis de los datos.

- Recopilación de datos, incluido el almacenamiento y la verificación. Los procedimientos deben especificar cómo serán recogidos y clasificados los datos, así como la forma en la que se almacenará. La verificación de datos puede llevarse a cabo a través de una auditoría. Las herramientas automatizadas pueden ser utilizadas para apoyar estos procedimientos.

- Análisis de datos y presentación de informes de las métricas. Los procedimientos deben especificar el método de análisis de datos, la frecuencia, el formato y los métodos para informar sobre los productos de información. Se debe identificar la gama de herramientas que serán necesarias para llevar a cabo el análisis de la información.

4.6. Documentación

El enfoque general de las métricas debe ser documentado en un plan de implementación. El plan de implementación debe incluir la siguiente información, como mínimo;

- Controles y objetivos de controles que serán medidos
- Metas de las métricas
- Objetivos de negocio bajo medición
- Métricas individuales que serán recolectadas y usadas
- Recolección de información y procedimientos de análisis
- Procedimiento de reporte y formatos
- Roles y responsabilidades de las partes interesadas
- Ciclo de actualización de métricas para asegurar su implementación en relación a la Administración de la Seguridad y los objetivos de negocio

4.7. Operación de Métricas

La operación de métricas de Seguridad de la Información implica la recolección y análisis de los datos utilizados para crear métricas de seguridad. Se trata de actividades que son esenciales para asegurar que las mediciones recolectadas se utilicen para obtener una comprensión de la efectividad de la Administración de la Seguridad y para identificar las acciones adecuadas de mejora. Esta fase incluye las siguientes actividades:

- Integrar los procedimientos de las métricas dentro de la operación de la Administración de la Seguridad

- Recolectar, almacenar y verificar la información

En el diseño de los controles de seguridad es conveniente haber tomado en cuenta lo siguiente para facilitar su seguimiento:

- Si el control tiene como fin ser preventivo, detectivo o de recuperación

- Momento en el que dado un incidente se ejecutará el control

- En el caso de los controles que su objetivo es la detección y recuperación, ¿Cuánto tiempo tienen para ejecutarse antes de que ocurra un impacto adverso?

Si está información está disponible, entonces la efectividad de los controles se podrá medir directamente

4.8. Integración de Procedimientos

El programa de métricas de seguridad de la información debe ser completamente integrado y utilizado dentro de la Administración de la Seguridad, donde se recomienda incluir lo siguiente:

- Definición y documentación de las funciones y responsabilidades relacionadas con el desarrollo, implementación y mantenimiento de las Métricas de Seguridad en el contexto de la Administración de la Seguridad

- La generación de datos y recolección incluyendo el cambio de los procesos actuales para dar cabida a la generación de información y actividades de recolección. La integración supone un equilibrio entre el grado de impacto en los procesos existentes que pueden ser toleradas y las necesidades del proceso de medición. Deberían reducirse al mínimo los cambios necesarios para recopilar datos deberían reducirse al mínimo

- La comunicación de los cambios en las actividades de recolección de datos con las partes interesadas para asegurar la correcta recolección de información, incluyendo la comprensión del tipo de datos, herramientas de recopilación de datos y los procedimientos de recolección de datos. La adecuada competencia de los recolectores de información facilitará la calidad de los datos recogidos y la utilidad de las medidas para la organización

- Los análisis de datos y la presentación de informes deban integrarse en los procesos pertinentes para garantizar un rendimiento normal de estos procesos

- Las políticas y procedimientos definirán el uso de las métricas dentro de la organización, la difusión de la información de métricas, auditoría y revisiones del proceso de medición
- Procedimiento de seguimiento de métricas para evaluar su uso
- Procedimiento de eliminación de métricas por salir y procedimientos de adición de nuevas métricas para garantizar su uso en la organización.

4.9. Recolección de Datos

El Proceso de recolección de datos integra la siguiente información:

- Los datos de los atributos requeridos deben ser recolectados en intervalos regulares utilizando el método designado de acuerdo con los procedimientos definidos en el plan de implementación. La recolección de datos se debe documentar al menos lo siguiente:
  - Fecha, hora y lugar de recolección de datos
  - Información del recolector
  - Información del propietario de los datos
  - Cualquier problema que se produjera durante la recolección de datos que pueda proporcionar información útil para la validación de datos y validación del proceso de medición
- Consolidar los datos recolectados y resguardar en un formato para el análisis de datos y presentación de informes
- Verificar los datos recolectados contra los criterios de validación de atributos

4.10. Almacenamiento de Datos

Los datos recopilados deben ser almacenados incluyendo cualquier información de contexto necesaria para verificar, comprender o evaluar los datos. Los datos no debieran ser almacenados en una herramienta automatizada, la necesidad de automatización se define por el volumen y la complejidad de los datos recolectados, analizando y reportando cada ciclo de recolección.

4.11. Desarrollo de las Métricas

El desarrollo de las métricas para el ejemplo de la Administración del presente documento se va a realizar tomando los controles de seguridad desarrollados en el capítulo anterior.

Control	Objetivo del Control	Nivel del Control	Tipo de Control
11.6.1 Restricción del acceso a la información	Limitar el acceso de los usuarios finales y del personal de soporte a la información y las funciones de los activos en concordancia con la política de acceso definida.	Operativo	Preventivo

Para comenzar con la actividad se deberán identificar los objetos de medición que componen al control de seguridad tomando como primicia aquellas características sustantivas que son el motivo de su funcionamiento.

De igual manera se deberá identificar la Métrica Base/Derivada que serán los insumos para el desarrollo de los cálculos de medición.

Tipo de Insumo Requerido	Descripción del Insumo
Objetos de Medición	Atributo 1. Lista de perfiles. Atributo 2. Lista de usuarios con acceso a aplicaciones e información almacenada en activos de información.
Métricas Base	Total de usuarios con acceso a las aplicaciones. Total de desviaciones en la asignación de permisos de acuerdo al perfil de usuario.

Requerimiento	Descripción
Métrica	Derechos de acceso de aplicaciones e información
Código	ASI.11.6.1
Objetivo de Control / Control	11.6 Control de Acceso para Aplicaciones e Información 11.6.1 Restricción de los Accesos a la Información
Tipo de Métrica	Cumplimiento
Métrica Base / Derivada	Base
Propósito	Identificar el grado de desviación de la asignación de los derechos de acceso de acuerdo al tipo de perfil requerido para cada usuario
Detalles del Cálculo de Medición	La función de cálculo está expresada por la siguiente función: ASI.11.6.1 = (TU / TD) x 100 Dónde: TU = Total de usuarios con acceso a las aplicaciones TD = Total de desviaciones en la asignación de derechos de acceso
Valor	Porcentaje
Escala	0 – 100
Procedimiento de Recolección	ASI.11.6.1_Procedimiento
Frecuencia de Recolección	Semestral
Recolector	Grupo de Auditoría de la Organización

Control	Objetivo del Control	Nivel del Control	Tipo de Control
12.1.1 Análisis y especificación de los requerimientos de seguridad	Los requerimientos de seguridad para aplicaciones comerciales, para el desarrollo de sistemas nuevos realizados In-House o las mejoras a los sistemas ya existentes, se debieran especificar de manera previa a realizar cualquier actividad de desarrollo o adquisición	Administrativo	Preventivo

De igual manera se deberá identificar la Métrica Base/Derivada que serán los insumos para el desarrollo de los cálculos de medición.

Tipo de Insumo Requerido	Descripción del Insumo
Objetos de Medición	Atributo 1. Anexos Técnicos Atributo 2. Checklist de Verificación de Seguridad Atributo 3. Contratos Atributo 4. Casos de Uso Atributo 5. Casos de Prueba Atributo 6. Procedimientos de Control de Cambios
Métricas Base	Clausulas no cumplidas por el software de conformidad con el Anexo Técnico Total de cláusulas de seguridad del Anexo Técnico Desviaciones con las recomendaciones del Checklist de Seguridad Total de requerimientos del Checklist de Seguridad

Requerimiento	Descripción
Métrica	Requerimientos de seguridad de sistemas/aplicaciones
Código	ASI.12.1.1
Objetivo de Control / Control	12.1 Requerimientos de Seguridad de los Sistemas de Información 12.1.1 Análisis y especificación de los requerimientos de seguridad
Tipo de Métrica	Cumplimiento
Métrica Base / Derivada	Base
Propósito	Identificar el nivel de desviación de los Sistemas/Aplicaciones de conformidad con los requerimientos de seguridad específicos para cada etapa de adquisición o desarrollo de los mismos
Detalles del Cálculo de Medición	La función de cálculo está expresada por la siguiente función: ASI.12.1.1 = $\bar{X}$ { (CC / TC) , (DCHK / TCHK) } X 100 Dónde: CC = Clausulas no cumplidas TC = Total del cláusulas de seguridad del Anexo Técnico DCHK = Desviación de acuerdo al Checklist de Seguridad TCHK = Total de requerimientos del Checklist de Seguridad
Valor	Porcentaje
Escala	0 – 100
Procedimiento de Recolección	ASI.12.1.1_Procedimiento
Frecuencia de Recolección	Anual
Recolector	Grupo de Auditoría de la Organización

Un tablero con un conjunto de valores puede ofrecer a los administradores la evolución o tendencias durante el ciclo de mejora continua y el cumplimiento de Administración de la Seguridad de la Información. Para una representación gráfica de una organización se pueden seleccionar una o más de los siguientes tableros:

- El uso de Scorecards para proporcionar información al más alto nivel con información estratégica mediante indicadores

- Tableros ejecutivos y operativos. Un tablero de instrumentos está menos centrado en un objetivo estratégico y más ligado a los controles y procesos específicos. Dentro de un cuadro de mando, la eficacia de los controles y procesos se convierte en el foco. Se puede utilizar una amplia gama de colores para entender los resultados [por ejemplo, desde el negro (0%) hasta el verde brillante (100%)]

- Uso de informes. Los informes pueden ser muy simples y estáticos, tales como una lista de medidas para un período de tiempo determinado, a más sofisticados como informes de referencias cruzadas con agrupaciones anidadas y la dinámica llamada Drill-Down. Los informes se utilizan cuando el usuario tiene que analizar los datos brutos en un formato fácil de leer

- Indicadores para representar un valor dinámico de datos adicionales, incluyendo alertas elementos gráficos y etiquetado de los puntos finales

5. Conclusiones

Seguramente muchas personas que no se encuentran relacionadas con la seguridad de la información pudieran desconocer los peligros de no realizarse una autoevaluación pensando que las actividades que se realizan no están relacionadas con amenazas que pudieran dañar su imagen o su operación. Está forma de pensar es más común de lo que creemos ya que México es un país que hasta hace poco comenzó esforzarse en asegurar su operación y blindar sus objetivos de negocio con controles de seguridad que no son bien vistos por el usuario que está mal informado.

¿A qué se debe este descontento con la seguridad?

Simple, es bien sabido por los especialistas en seguridad que la misma entorpece el rendimiento de las actividades e incluso de los sistemas debido a que muchas operaciones manuales están sujetas a un proceso de "tramitología" y documentación sin dejar a un lado el cumplir con los requerimientos de seguridad que muchas veces hacen más extenso un procedimiento.

En el ámbito de las actividades automatizadas, el "performance" se ve afectado por una serie de validaciones de integridad de la información y el aseguramiento de la misma utilizando medidas de procesamiento extra que tienen como fin el poder entregar las salidas de un proceso o servicio tal y como se espera y en el momento que se solicita.

Es aquí cuando se hace imprescindible adoptar una cultura de Administración de Seguridad en las organizaciones para crear una conciencia colectiva en la que participen todos los trabajadores activamente, siendo respetuosos de las políticas y alineándose a las regulaciones y lineamientos en los que se rige el negocio al que pertenecen.

Debido a esto, se debe hacer extensiva la publicación de una política de seguridad bajo la que se dirigirán los esfuerzos de la organización y donde la participación de la alta dirección tiene un papel fundamental para hacer valer las necesidades de los recursos humanos y materiales, que den seguimiento y control en la planeación ejecución y mejora continua de un sistema que sea alimentado de manera constante y con lo que se pueda crear un histórico de necesidades de las que la organización aprenderá sobre sus mismos pasos para no reaccionar a un evento de seguridad cuando es demasiado tarde.

Afortunadamente en México la creación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) ha hecho que, organizaciones particulares estén al pendiente de los requerimientos de la ley donde se incluye la identificación de los datos sensitivos de una persona que recaban a través de una necesidad de entrega o solicitud de un servicio y por el que están sujetos a resguardar la información a través de medidas de seguridad que pudieran ser auditadas de manera sorpresiva por la Secretaría de la Función Pública.

Este simple requisito conlleva aplicar las actividades descritas en la presente Tesis con sus respectivas variantes de implementación de acuerdo al tamaño de la empresa, la

cantidad de información que manejan, el tipo de almacenamiento o procesamiento que realizan con la información y principalmente los recursos que deberán asignar para cumplir con dicha ley.

Por el lado del sector Gobierno se expidió el Manual Administrativo de Aplicación General en Materia de TIC´s y Seguridad de la Información (MAAGTICSI) en donde se incluyen diversas metodologías de gestión para las tecnologías de la información entre las cuales destaca la implantación de un Sistema de Gestión de la Seguridad de la Información. En las organizaciones que están certificadas en ISO/IEC 27001 están sobradas para los requerimientos de MAAGTICSI por lo que únicamente se deberán alinear a procesos referidos a la administración de proyectos, entrega de servicios, etc.

Como se puede observar en el presente trabajo de Tesis, el punto más importante para para la Administración de la Seguridad de la Información es realizar una Administración de Riesgos adecuada debido a que con esta actividad se puede justificar la implementación de controles de seguridad y tener trazabilidad de las acciones y deficiencias en materia de seguridad de la Organización.

6. Bibliografía

ISO/IEC 27001.- Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requerimientos

ISO/IEC 27002.- Tecnología de la Información. Técnicas de Seguridad, Código para la Práctica de la Gestión de la Seguridad de la Información

ISO/IEC 27003.- Tecnología de la Información. Técnicas de Seguridad. Guía de Implementación para la Gestión de Sistemas de Seguridad de la Información

ISO/IEC 27004.- Tecnología de la Información. Técnicas de Seguridad. Gestión de Métricas de Seguridad de la Información

ISO/IEC 27005.- Tecnología de la Información. Técnicas de Seguridad. Administración de Riesgos de la Seguridad de la Información

ISO/IEC 31000.- Administración de Riesgos. Principios y Guías

MAGERIT Versión 2.- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Octave S Versión 1.- Metodología de Administración de Riesgos, Carnegie Mellon, Software Engineering Institute

Octave Allegro Guidebook.- Metodología de Administración de Riesgos, Carnegie Mellon, Software Engineering Institute

Special Publication 800-30. - Risk Management Guide for Information Technology Systems. National Institute of Standars and Technology

Special Publication 800-37. - Guide for Applying the Risk Management Framework to Federal Information Systems. National Institute of Standars and Technology

Special Publication 800-39. - Managing Information Security Risk (Organization, Mission and Information System View. National Institute of Standars and Technology

7. Glosario

Término	Descripción
Actitud de Riesgo	Enfoque de la organización para evaluar y eventualmente llevar a cabo, mantener, tomar o alejarse de riesgo
Activo	Algo que tenga valor para la organización
Amenaza	Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización
Análisis de Riesgos	Procesar a comprender la naturaleza de riesgo para determinar la magnitud de riesgo NOTA 1: El análisis de riesgos es la base para la evaluación del riesgo y las decisiones sobre el tratamiento del riesgo NOTA 2: El análisis del riesgo incluye la estimación del riesgo.
Apetito al Riesgo	Cantidad y tipo de riesgo que la organización está dispuesta a perseguir, conservar o llevar
Aversión al Riesgo	Actitud de alejarse de riesgo
Criterios de Riesgo	Términos de referencia contra el cual la magnitud de un riesgo se evalúa NOTA 1: Los criterios de riesgo se basan en los objetivos de la organización, y externo y el contexto interno NOTA 2: Los criterios de riesgo se pueden derivar de las normas, leyes, políticas y otros requisitos.

Término	Descripción
Comunicación y Consulta	Proceso continuo e iterativo que una organización lleva a cabo para proporcionar, compartir u obtener información y para entablar un diálogo con las partes interesadas y otros con respecto a la gestión del riesgo NOTA 1: La información puede relacionarse con la existencia, la naturaleza, la forma, la probabilidad, la gravedad, la evaluación, la aceptabilidad, tratamiento u otros aspectos de la gestión del riesgo. NOTA 2: La consulta es un proceso de dos vías de comunicación informada entre una organización y sus grupos de interés u otras personas sobre un tema antes de tomar una decisión o determinación de una dirección en un tema en particular. La consulta es: • Un proceso que repercute en una decisión a través de la influencia en lugar de poder, y • Un insumo para la toma de decisiones, no la toma de decisiones conjunta.
Confidencialidad	La propiedad de que la información no se haga disponible o divulgada a personas no autorizadas, entidades o procesos
Consecuencia	Resultado de un evento que afecta a los objetivos NOTA 1: Un evento puede llevar a una serie de consecuencias NOTA 2: Una consecuencia puede ser cierto o incierto y puede tener efectos positivos o negativos en los objetivos NOTA 3: Las consecuencias pueden ser cualitativas o cuantitativas
Contexto Externo	Entorno externo en el que la organización busca lograr sus objetivos NOTA: contexto externo puede incluir: • El entorno cultural, social, político, jurídico, reglamentario, financiero, tecnológico, económico, natural y competitivo, ya sea internacional, nacional, regional o local; • Factores clave y las tendencias que tienen impacto en los objetivos de la organización, y • Las relaciones con los y las percepciones y valores de los grupos de interés externos.

Término	Descripción
Contexto Interno	Ambiente interno en el que la organización busca alcanzar sus objetivos NOTA: contexto interno puede incluir: • Gobierno, estructura organizativa, funciones y responsabilidades; Las políticas, los objetivos y las estrategias que están en marcha para alcanzarlos; • Las capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías); • Las percepciones y valores de los grupos de interesados internos; • Los sistemas de información, flujos de información y procesos de toma de decisiones (tanto formales como informales); • Las relaciones con los y las percepciones y valores de los grupos de interés, internos; • La cultura de la organización
Control de Seguridad	Medida que está modificando al riesgo NOTA 1: Los controles incluyen cualquier proceso, la política, dispositivo, práctica u otras acciones que modifican el riesgo. NOTA 2 Los controles no siempre pueden ejercer el efecto deseado
Disponibilidad	La propiedad de ser accesible y utilizable a petición por una entidad autorizada
Dueño del Riesgo	Persona o entidad que tiene la responsabilidad y autoridad para gestionar el riesgo
Establecimiento de Contexto	Definición de los parámetros externos e internos que deben tenerse en cuenta en la gestión de riesgos, definición del alcance y criterios de riesgo la administración de la política de gestión de riesgos
Evaluación de Riesgos	Proceso de comparación de los resultados de análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable NOTA: Evaluación de riesgos ayuda a la decisión sobre el tratamiento del riesgo

Término	Descripción
Evento	Ocurrencia o cambio de un conjunto particular de circunstancias NOTA 1: Un evento puede ser una o más ocurrencias y puede tener varias causas NOTA 2: Un evento puede consistir en algo que no sucedía NOTA 3: Un acontecimiento a veces puede ser referido como un "incidente" o "accidente"
Evento de seguridad de la información	Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.
Fuente de Riesgo	Elemento que solo o en combinación tiene el potencial intrínseco para dar lugar al riesgo NOTA: Una fuente de riesgo puede ser tangible o intangible
Gestión de Riesgos	Actividades coordinadas para dirigir y controlar una organización en lo que respecta al riesgo
Identificación de Riesgos	Proceso de encontrar, reconocer y describir los riesgos NOTA 1: La identificación de riesgos consiste en la identificación de las fuentes de riesgo, eventos, sus causas y sus posibles consecuencias NOTA 2: La identificación de riesgos puede implicar datos históricos, análisis teórico, opiniones informadas de expertos y de grupos de interés
Impacto	Cambio adverso en el nivel de los objetivos de negocio alcanzado
Impacto Repercutido	Se considera únicamente el valor propio del impacto. Este valor se combina con la frecuencia estimada de la amenaza
Impacto Residual	Impacto remanente en el sistema tras la implantación de los controles de seguridad determinados
Incidente de seguridad de la información	Un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información
Información de Eventos de Seguridad	Una ocurrencia identificada de un estado de los sistemas, servicios o redes que indica una posible violación de la política de seguridad de la información, la falta de garantías o una situación previamente desconocida

Término	Descripción
Información Sobre Incidentes de Seguridad	Una serie de eventos de seguridad no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar a la seguridad informática
Integridad	La propiedad de salvaguardar la exactitud e integridad de los activos
Interesados	Persona u organización que pueden afectar, ser afectado o percibe a sí mismo de ser afectado por una decisión o actividad NOTA: Un tomador de decisiones puede ser un interesado.
Lineamiento	Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas
Marco de Gestión del Riesgo	Conjunto de componentes que proporcionan los fundamentos y modalidades de la Organización para el diseño, implementación, monitoreo, revisión y mejora continua de la gestión del riesgo en toda la organización NOTA 1: Los fundamentos incluyen la política, los objetivos y el compromiso con la gestión del riesgo NOTA 2: Las disposiciones de una Organización incluyen planes, relaciones, responsabilidades, recursos, procesos y actividades NOTA 3: El marco de gestión de riesgos se inserta dentro de las políticas generales estratégicas y operativas de la Organización
Monitoreo	Continua comprobación, supervisión, para observar o determinar el estado con el fin de identificar el cambio en el nivel de rendimiento requerido o esperado NOTA: El seguimiento se puede aplicar a un marco de gestión de riesgo, el proceso de gestión del riesgo, riesgo o control
Nivel de Riesgo	Magnitud de un riesgo, expresado en términos de la combinación de consecuencias y su probabilidad
Perfil de Riesgo	Descripción de cualquier conjunto de riesgos NOTA: El conjunto de riesgos puede incluir aquellas que se refieren a la organización en su conjunto, que forma parte de la organización, o como se defina lo contrario.

Término	Descripción
Plan de Gestión de Riesgo	Esquema dentro del marco de gestión de riesgo que especifica el método, los componentes de gestión y los recursos que deben aplicarse a la gestión de riesgo NOTA 1: Los componentes de administración incluyen típicamente procedimientos, prácticas, asignación de responsabilidades, la secuencia y el calendario de actividades.
Política	Intención y dirección general expresada formalmente por la gerencia
Política de Gestión de Riesgo	Declaración de las intenciones globales y orientación de una Organización relacionada con la gestión del riesgo
Probabilidad	Posibilidad de que algo suceda NOTA 1: En la terminología de gestión de riesgos, la palabra "probabilidad" se utiliza para referirse a la posibilidad de que algo suceda, ya sea definido, medido o estimado de manera objetiva o subjetiva, cualitativa o cuantitativamente y se describe el uso de términos generales o matemáticamente (como una probabilidad o una frecuencia durante un periodo de tiempo dado) NOTA 2: El término Inglés "likelihood" no tiene un equivalente directo en algunas lenguas, en lugar de eso se utiliza el equivalente del término "Probabilidad" el cuál es usado muy a menudo. Sin embargo, en inglés, "Probability" es a menudo una interpretación estricta como un término matemático. Por lo tanto, en el riesgo de gestión terminológica, "likelihood" se utiliza con la intención de que debe tener la misma interpretación del término "Probability" en muchos idiomas distintos al inglés.
Proceso de Gestión del Riesgo	Aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación, consulta, estableciendo el contexto y la identificación, análisis, evaluación, tratamiento, seguimiento y la revisión de riesgo
Revisión	Actividad realizada para asegurar la conveniencia, adecuación y eficacia para alcanzar los objetivos establecidos Se puede aplicar a un marco de gestión de riesgo, el proceso de gestión del riesgo, riesgo o control

Término	Descripción
Riesgo	Efecto de la incertidumbre sobre los objetivos NOTA 1: Un efecto es una desviación de lo que se espera (positivo y/o negativo) NOTA 2: Los objetivos pueden tener aspectos diferentes (por ejemplo, financieros, sanitarios y de seguridad, y las metas ambientales) y se puede aplicar a diferentes niveles (como estratégicos, proyectos, productos y procesos) NOTA 3: El riesgo se caracteriza a menudo por eventos potenciales y sus consecuencias, o una combinación de estos NOTA 4: El riesgo se expresa a menudo en términos de una combinación de las consecuencias de un acontecimiento (incluyendo cambios en las circunstancias) y la probabilidad asociada de ocurrencia
Riesgo Acumulado	El valor propio de un activo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma
Riesgo de Seguridad de la Información	Potencial que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto cause daño a la organización NOTA 1 En términos generales, el riesgo es un efecto de la incertidumbre sobre los objetivos NOTA 2 Se mide en términos de una combinación de la probabilidad de un evento y su consecuencia
Riesgo Repercutido	Se considera únicamente el valor propio de un activo. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma, medidas ambas sobre activos de los que depende
Riesgo Residual	Riesgo que queda después del tratamiento del riesgo NOTA 1: El riesgo residual puede contener el riesgo identificado. NOTA 2: El riesgo residual también puede ser conocido como "riesgo retenidos".
Seguridad de la Información	Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades como la autenticidad, responsabilidad, no repudio y la fiabilidad

Término	Descripción
Sistema de Gestión de la Seguridad de la Información (SGSI o ISMS)	Basado en un enfoque de riesgo empresarial para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información NOTA: El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.
Tercera persona	Esa persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión
Tratamiento del Riesgo	Proceso para modificar el riesgo NOTA 1: El tratamiento del riesgo puede incluir, • Evitando el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo; • La eliminación de la fuente de riesgo • Cambiando la probabilidad • Cambiar las consecuencias • Compartiendo el riesgo con la otra parte o partes (incluyendo los contratos de riesgo y financiamiento), y • Retención del riesgo por elección informada. NOTA 2: El tratamiento del riesgo puede crear riesgos nuevos o modificar los riesgos existentes.
Trazabilidad	Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento
Valor Acumulado	Considera tanto el valor propio de un activo como el valor de los activos que dependen de él
Vulnerabilidad	La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas