Gestión de Riesgo

Introducción

La Gestión de Riesgo es un método que se puede aplicar en diferentes contextos donde se debe incluir y trabajar con las consideraciones de la seguridad.

El propósito es mostrar como se puede aplicar el enfoque de la Gestión de Riesgo en la Seguridad Informática y particularmente en el ámbito de las organizaciones sociales o empresas. Al mismo tiempo señala los puntos críticos y claves que se debe reconsiderar, para que la gestión de riesgo sea más exitosa.

1. Definición de Seguridad Informática

La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su **confidencialidad**, **integridad** y **disponibilidad**

Considerar aspectos de seguridad significa

a) conocer el peligro,

b) clasificarlo

y c) protegerse

de los impactos o daños de la mejor manera posible. Esto significa que solamente cuando estamos consientes de las potenciales amenazas, agresores y sus intenciones dañinas (directas o indirectas) en contra de nosotros, podemos tomar

medidas de protección adecuadas, para que no se pierda o dañe nuestros recursos valiosos.

En este sentido, la Seguridad Informática **sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.**

2. **Gestión de Riesgo en la Seguridad Informática**

La Gestión de Riesgo es un método **para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo**.

En su forma general contiene cuatro fases

- **Análisis**: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
- **Clasificación**: Determina si los riesgos encontrados y los riesgos restantes son aceptables.
- **Reducción**: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.
- **Control**: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de

- Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.
- Orientar el funcionamiento organizativo y funcional.
- Garantizar comportamiento homogéneo.
- Garantizar corrección de conductas o prácticas que nos hacen vulnerables.
- Conducir a la coherencia entre lo que pensamos, decimos y hacemos.

3. Seguridad de la Información y Protección de Datos

En la Seguridad Informática se debe distinguir dos propósitos de protección, la **Seguridad de la Información y la Protección de Datos**.

Se debe distinguir entre los dos, porque forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección.

Sin embargo hay que destacar que, aunque se diferencia entre la Seguridad de la Información y la Protección de Datos como motivo o obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

Para ilustrar un poco la diferencia entre los dos, se recomiendo hacer el siguiente ejercicio.

Ejercicio: Seguridad de la Información y Protección de Datos

Este ejercicio sirve para mostrar la diferencia entre la Seguridad de la Información y la Protección de Datos y su importancia para la decisión y justificación, cuales de los elementos de información requieren una mayor atención en su cuido.

La lista de los elementos usados y los resultados obtenidos en el ejercicio salen como resumen de los talleres "Sensibilización y evaluación de riesgo para el manejo seguro de la Información" y solo son de carácter demostrativo, tampoco son completos.

Suponiendo que todos contamos con una cuenta bancaria, se hace la pregunta a los participantes **¿Cuáles son los datos, informaciones que maneja el banco sobre mí?** y se presenta las respuestas en tarjetas.

(Consejo metodológico: una respuesta por tarjeta)

Números de cuentas bancarias	Patrimonio	Firma	Hábitos de consumo (restaurantes, tiendas)
Número de identificación	Dirección domicilio	Profesión, Cargo laboral	Contraseñas de cuenta
Transacciones bancarias	Consumo servicio de teléfono, electricidad, etc	Nombre y Apellido	Salario
Números telefónicos	Deudas y créditos	Lugar de estudio de hijos	Capacidad de consumo

A continuación preguntamos,

¿Cuáles de los elementos se considera como Información confidencial?,

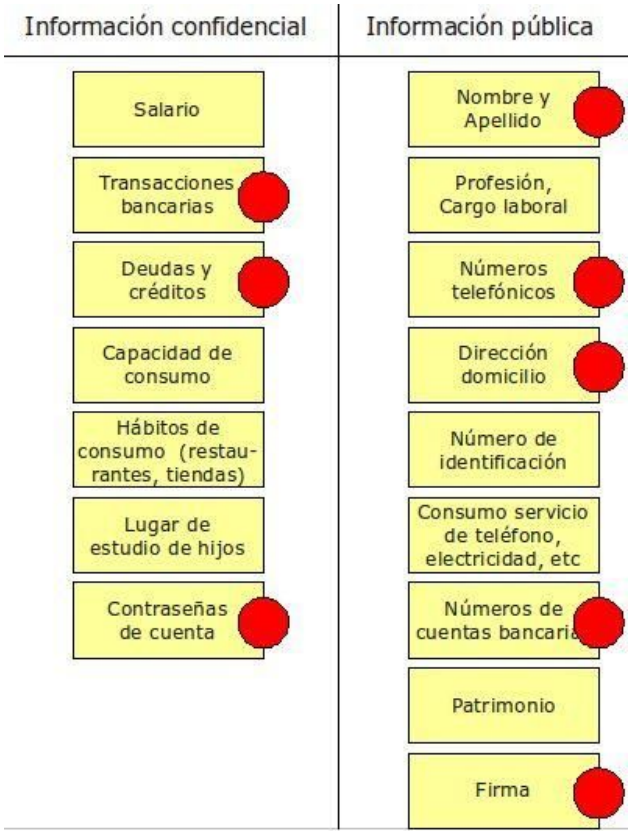
las cuales el banco debería tratar de tal manera, que no terminen en manos ajenas.

(Consejo metodológico: es importante que se aplique una **visión crítica**, porque a primera vista todos los elementos nos parecen "privados", sin embargo, reflexionando un poco sobre nuestro propio estilo de difusión de la información, nos damos cuenta que muchos de

los elementos mencionados, se maneja en un ámbito bastante público).

Como último paso

¿Cuáles de los elementos son de interés propio del banco, para que sea capaz de manejar mi cuenta? y los marcamos por ejemplo con un punto rojo.



Conclusiones:

- Existe una divergencia en la percepción de la gente, cuales de los elementos deben ser calificados como confidencial y por tanto recibir un tratamiento más cuidadoso por parte de la institución que lo maneja (el banco).
- Los elementos que se puede considerar como confidenciales, del punto de vista de la persona que aparece en ellos, y por consecuencia merecen un manejo más cuidadoso por parte del banco, no coinciden con los elementos que son críticos para este, para garantizar el buen manejo de mis recursos económicos. Entonces hay una probabilidad que exista una diferencia en la opinión, entre el propietario de la cuenta y el banco, sobre la importancia y atención en el manejo de los diferentes elementos informativos.
- Dentro del marco de la Seguridad Informática, los elementos que definimos como confidenciales, requieren una atención especial, porque están ligados al concepto de la Protección de Datos y los que son de interés propio del banco (con punto rojo) a lo de la Seguridad de la Información.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación non-autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros.

El motivo o el motor para implementar medidas de protección, que responden a la Seguridad de la Información, es el propio interés de la institución o persona que maneja los datos, porque la perdida o modificación de los datos, le puede causar un daño (material o inmaterial). Entonces en referencia al ejercicio con el banco, la perdida o la modificación errónea, sea causado intencionalmente o simplemente por negligencia humana, de algún récord de una cuenta bancaria, puede resultar en perdidas económicas u otros consecuencias negativas para la institución.

En el caso de la **Protección de Datos**, el objetivo de la protección no son los datos en si mismo, **sino el contenido de la información sobre personas,** para evitar el abuso de esta.

Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información.

En muchos Estados existen normas jurídicas que regulan el tratamiento de los datos personales, como por ejemplo en España, donde existe la "Ley Orgánica de Protección de Datos de Carácter Personal" que tiene por objetivo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Sin embargo el gran problema aparece cuando no existen leyes y normas jurídicas que evitan el abuso o mal uso de los datos personales o si no están aplicadas adecuadamente o arbitrariamente.

Existen algunas profesiones que, por su carácter profesional, están reconocidos o obligados, por su juramento, de respetar los datos personales como por ejemplo los médicos, abogados, jueces y también los sacerdotes.

Pero independientemente, si o no existen normas jurídicas, **la responsabilidad de un tratamiento adecuado de datos personales y las consecuencias que puede causar en el caso de no cumplirlo, recae sobre cada persona que maneja o tiene contacto con tal información,** y debería tener sus raíces en códigos de conducta y finalmente la ética profesional y humana, de respetar y no perjudicar los derechos humanos y no hacer daño.

Si revisamos otra vez los resultados del ejercicio con el banco y en particular los elementos que clasificamos como "Información Confidencial", nos podemos preguntar,
¿de que manera nos podría perjudicar un supuesto mal manejo de nuestros datos personales, por parte del banco, con la consecuencia de que terminen en manos ajenas?

Pues, no hay una respuesta clara en este momento sin conocer cuál es la amenaza, es decir quién tuviera un interés en estos datos.

4. Retos de la Seguridad

La eficiente integración de los aspectos de la Seguridad Informática en el ámbito de las organizaciones sociales y empresas enfrenta algunos retos muy comunes que están relacionados con el funcionamiento y las características de estas.

- Los temas transversales no reciben la atención que merecen y muchas veces quedan completamente fuera de las consideraciones organizativas: Para todas las organizaciones y empresas, la propia Seguridad Informática no es un fin, sino un tema transversal que normalmente forma parte de la estructura interna de apoyo.
  Nadie vive o trabaja para su seguridad, sino la implementa para cumplir sus objetivos.

- Carencia o mal manejo de tiempo y dinero: Implementar medidas de protección significa invertir en recursos como tiempo y dinero.

- El proceso de monitoreo y evaluación, para dar seguimiento a los planes operativos está deficiente y no integrado en estos: Implementar procesos y medidas de protección, para garantizar la seguridad, no es una cosa que se hace una vez y después se olvide, sino requiere un control continuo de cumplimiento, funcionalidad y una adaptación periódica, de las medidas de protección implementadas, al entorno cambiante.

Todas estás circunstancias juntas, terminan en la triste realidad, que la seguridad en general y la Seguridad Informática en particular no recibe la atención adecuada. El error más común que se comete es que no se implementa medidas de protección, hasta que después del desastre, y las escusas o razones del porque no se hizo/hace nada al respecto abundan.

Enfrentarse con esta realidad y evitando o reduciendo los daños a un nivel aceptable, lo hace necesario trabajar en la "Gestión de Riesgo", es decir

a) conocer el peligro,

b) clasificarlo y

c) protegerse de los impactos o daños de la mejor manera posible.

Pero una buena Gestión de riesgos no es una tarea única sino un proceso dinámico y permanente que tiene que estar integrado en los procesos (cotidianos) de la estructura institucional, que debe incluir a todas y todos los funcionarios

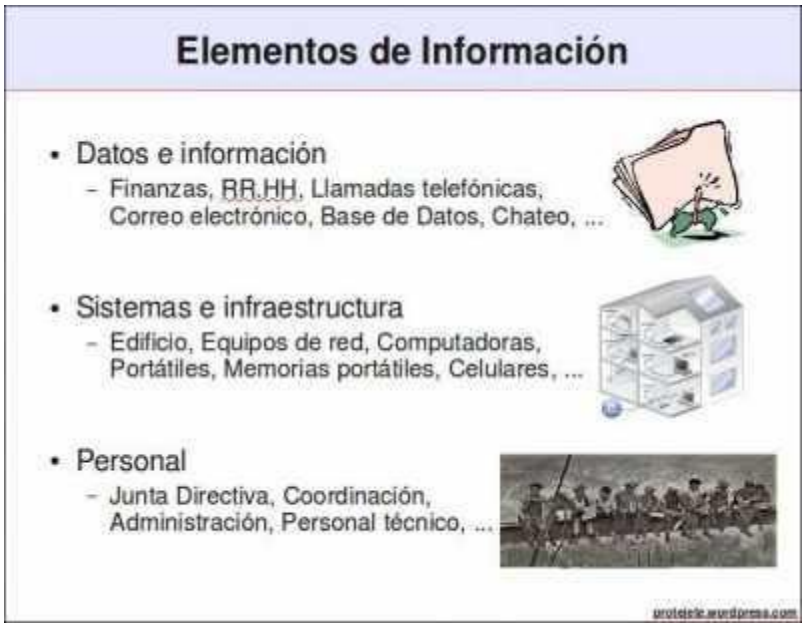
-¡¡la falla es el eslabón más débil de la cadena!!-

y que requiere el reconocimiento y apoyo de las directiva.

Sin estas características esenciales no están garantizados, las medidas de protección implementadas no funcionarán y son una perdida de recursos.

5. **Elementos de Información**

Los Elementos de información son todos los componentes que contienen, mantienen o guardan información. Dependiendo de la literatura, también son llamados **Activos o Recursos**.



Son estos los Activos de una institución que tenemos que proteger, para evitar su perdida, modificación o el uso inadecuado de su contenido, para impedir daños para nuestra institución y las personas presentes en la información.

Generalmente se distingue y divide tres grupos

- **Datos e Información**: son los datos e informaciones en si mismo
- **Sistemas e Infraestructura**: son los componentes donde se mantienen o guardan los datos e informaciones
- **Personal**: son todos los individuos que manejan o tienen acceso a los datos e informaciones y son los activos más difíciles de proteger, porque son móviles, pueden cambiar su afiliación y son impredecibles

6. **Amenazas y Vulnerabilidades**

Amenazas

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un

evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

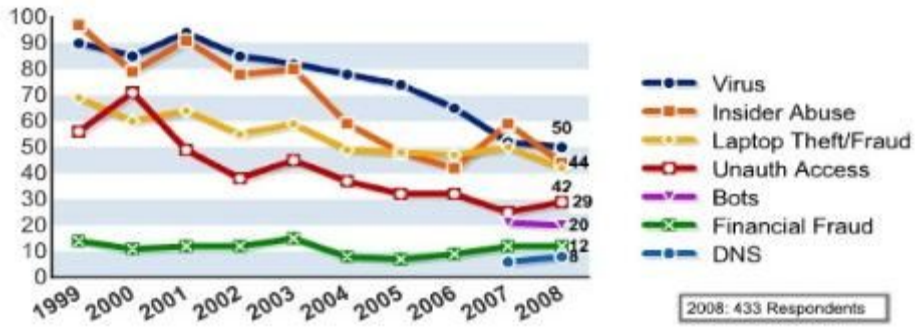
Desde el punto de vista de la entidad que maneja los datos, existen amenazas de origen externo como por ejemplo las agresiones técnicas, naturales o humanos, sino también amenazas de origen interno, como la negligencia del propio personal o las condiciones técnicas, procesos operativos internos (Nota: existen conceptos que defienden la opinión que amenazas siempre tienen carácter externo!)

Generalmente se distingue y divide tres grupos

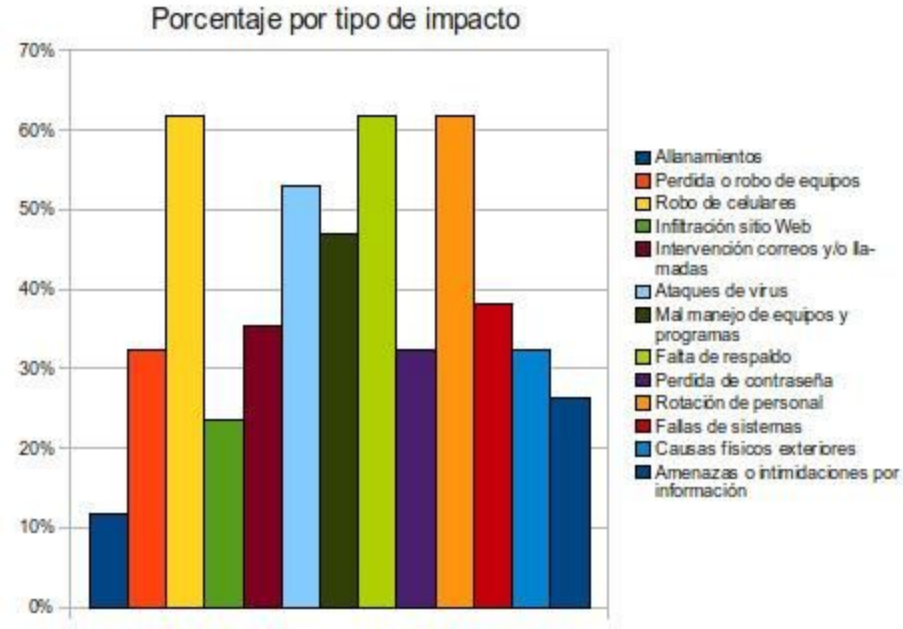
- **Criminalidad**: son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.
- **Sucesos de origen físico**: son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.
- **Negligencia y decisiones institucionales**: son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

Existen amenazas que difícilmente se dejan eliminar (virus de computadora) y por eso es la tarea de la gestión de riesgo de preverlas, implementar medidas de protección para evitar o minimizar los daños en caso de que se realice una amenaza.

Para mostrar algunas de las amenazas más preocupantes, consultamos dos estadísticas, el primer grafo sale de la "Encuesta sobre Seguridad y Crimen de Computación – 2008" del Instituto de Seguridad de Computación (CSI por sus siglas en inglés) que base en 433 respuestas de diferentes entidades privadas y estatales en los EE.UU



El segundo tiene su origen en una encuesta que se hizo en el año 2007, con 34 organizaciones sociales a nivel centroamericano



Ambos grafos, muestran el porcentaje de todos los encuestados que sufrieron ese tipo de ataque.

Como se observa, existen algunas similitudes respecto a las amenazas más preocupantes

- Ataques de virus (>50%)
- Robo de celulares, portátiles y otros equipos (>40%)

Pero también existen otras amenazas que, aunque no aparezcan en ambas encuestas, son muy alarmantes y que se debe tomar en consideración

- Falta de respaldo de datos
- Perdida de información por rotación, salida de personal
- Abuso de conocimientos internos
- Mal manejo de equipos y programas
- Acceso no-autorizado
- etc

Vulnerabilidades

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

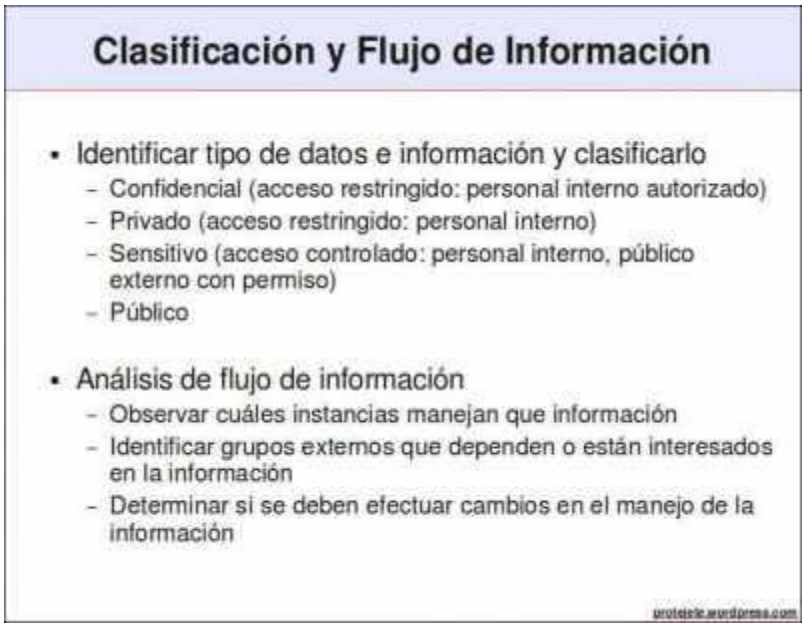
Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos característicos: **Ambiental**, **Física**, **Económica**, **Social**, **Educativo**, **Institucional** y **Política**.

7. **Análisis de Riesgo**

El primer paso en la Gestión de riesgo es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección,

sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

Clasificación y Flujo de Información

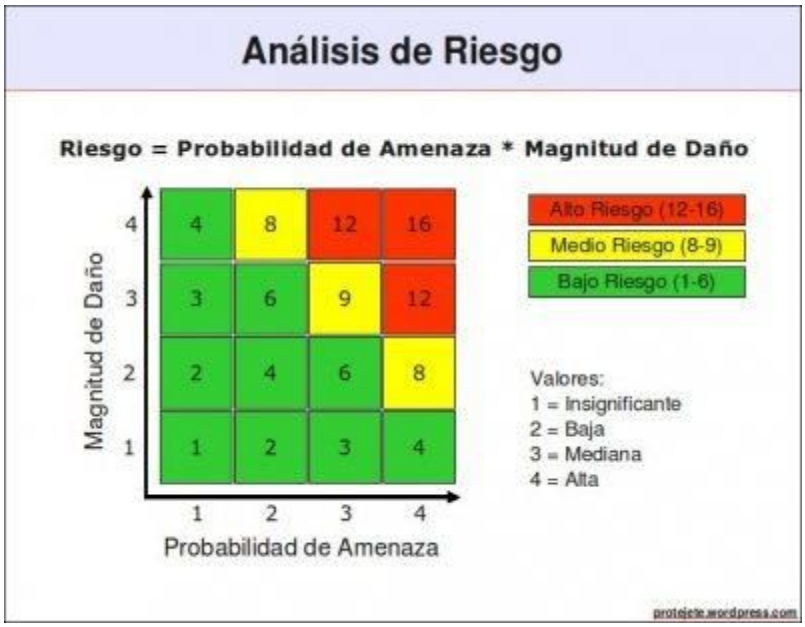


La clasificación de datos tiene el propósito de garantizar la protección de datos (personales) y significa definir, dependiendo del tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso a los datos e informaciones. Considerando el contexto de nuestra misión institucional,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

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

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

Análisis de Riesgo



Existen varios métodos de como valorar un riesgo y al final, todos tienen los mismos retos -las variables son difíciles de precisar y en su mayoría son estimaciones- y llegan casi a los mismos resultados y conclusiones.

En el ámbito de la Seguridad Informática, el método más usado es el Análisis de Riesgo.

La valoración del riesgo basada en la formula matemática

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

Para la presentación del resultado (riesgo) se usa una gráfica de dos dimensiones, en la cual, el eje-x (horizontal, abscisa) representa la "Probabilidad de Amenaza" y el eje-y (vertical, ordenada) la "Magnitud de Daño".

La Probabilidad de Amenaza y Magnitud de Daño pueden tomar condiciones entre Insignificante (1) y Alta (4). En la practica no es necesario asociar valores aritméticos a las condiciones de las variables, sin embargo facilita el uso de herramientas técnicas como hojas de calculo.

Nota: La escala (4 condiciones) de la Probabilidad de Amenaza y Magnitud de Daño no es fijo y puede ser adaptada y afinada a las necesidades propias. En diferentes literaturas, particularmente la Probabilidad de Amenaza puede tomar hasta seis diferentes condiciones.

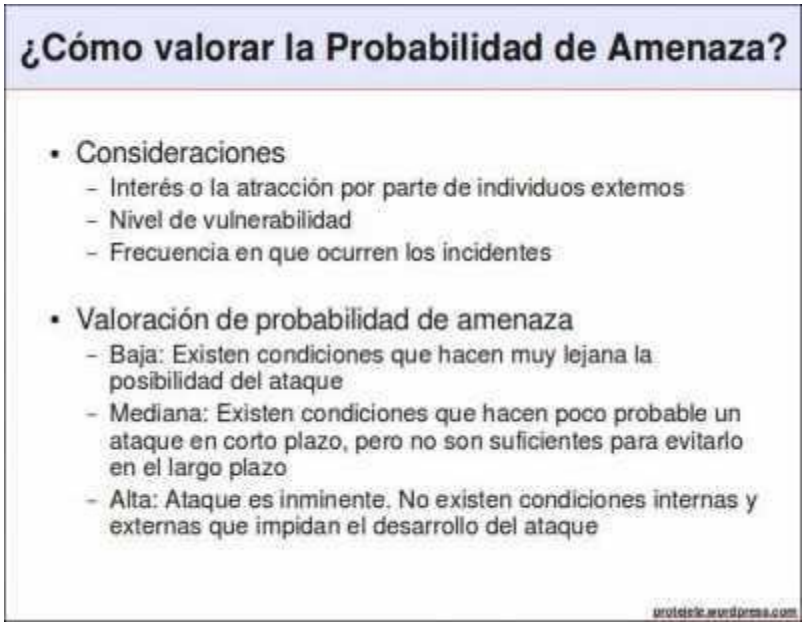
Como mencioné, el reto en la aplicación del método es precisar o estimar las condiciones (valores) de las dos variables, porque no basen en parámetros

claramente medibles. Sin embargo, el análisis de riesgo nos permite ubicar el riesgo y conocer los factores que influyen, negativa- o positivamente, en el riesgo.
En el proceso de analizar un riesgo también es importante de reconocer que cada riesgo tiene sus características:

- Dinámico y cambiante (Interacción de Amenazas y Vulnerabilidad)
- Diferenciado y tiene diferentes caracteres (caracteres de Vulnerabilidad)
- No siempre es percibido de igual manera entre los miembros de una institución que talvez puede terminar en resultados inadecuados y por tanto es importante que participan las personas especialistas de los diferentes elementos del sistema (Coordinación, Administración financiera, Técnicos, Conserje, Soporte técnico externo etc.)

El modelo se pude aplicar a los diferentes elementos de manera aislado, sino también al sistemas completa, aunque en el primer caso, el resultado final será más preciso pero también requiere más esfuerzo.
Entre más alta la Probabilidad de Amenaza y Magnitud de Daño, más grande es el riesgo y el peligro al sistema, lo que significa que es necesario implementar medidas de protección.

Probabilidad de Amenaza



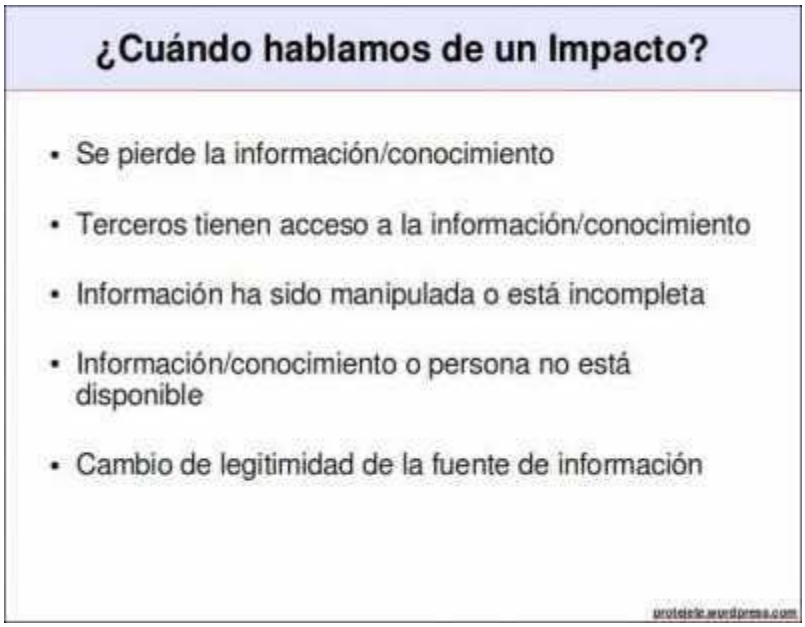
Se habla de un Ataque, cuando una amenaza se convirtió en realidad, es decir cuando un evento se realizó. Pero el ataque no dice nada sobre el éxito del evento y sí o no, los datos e informaciones fueron perjudicado respecto a su confidencialidad, integridad, disponibilidad y autenticidad.

Para estimar la Probabilidad de Amenaza nos podemos hacer algunas preguntas

- **¿Cuál es el interés o la atracción por parte de individuos externos, de atacarnos?** Algunas razones pueden ser que manejamos información que contiene novedades o inventos, información comprometedora etc, tal vez tenemos competidores en el trabajo, negocio o simplemente por el imagen o posición pública que tenemos.
- **¿Cuáles son nuestras vulnerabilidades?** Es importante considerar todos los grupos de vulnerabilidades. También se recomienda incluir los expertos, especialistas de las diferentes áreas de trabajo para obtener una imagen más completa y más detallada sobre la situación interna y el entorno.
- **¿Cuántas veces ya han tratado de atacarnos?** Ataques pasados nos sirven para identificar una amenaza y si su ocurrencia es frecuente, más grande es la probabilidad que pasará otra vez. En el caso de que ya tenemos implementadas medidas de protección es importante llevar un registro, que muestra los casos cuando la medida se aplico exitosamente y cuando no. Porque de tal manera, sabemos en primer lugar si todavía existe la amenaza y segundo, cuál es su riesgo actual.

Considerando todos los puntos anteriores, nos permite clasificar la Probabilidad de Amenaza. Sin embargo, antes tenemos que definir el significado de cada condición de la probabilidad (Baja, Mediana, Alta). Las definiciones mostradas en la imagen anterior solo son un ejemplo aproximado, pero no necesariamente refleja la realidad y la opinión común y por tanto se recomienda que cada institución defina sus propias condiciones.

Magnitud de Daño



Se habla de un Impacto, cuando un ataque exitoso perjudicó la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

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

Aunque conozcamos bien el impacto de un ataque exitoso, sus consecuencias pueden ser múltiples, a veces son imprevisibles y dependen mucho del contexto

donde manejamos la información, sea en una ONG (derechos humanos, centro de información etc.), en una empresa privada (banco, clínica, producción etc.), en una institución Estatal o en el ámbito privado. Otro factor decisivo, respecto a las consecuencias, es también el entorno donde nos ubicamos, es decir cuales son las Leyes y prácticas comunes, culturales que se aplica para sancionar el incumplimiento de las normas.

Un punto muy esencial en el análisis de las consecuencias es la diferenciación entre los dos propósitos de protección de la Seguridad Informática, la Seguridad de la Información y la Protección de datos, porque nos permite determinar, quien va a sufrir el daño de un impacto, nosotros, otros o ambos. En todo caso, todos nuestros comportamientos y decisiones debe ser dirigidos por una conciencia responsable, de no causar daño a otros, aunque su realidad no tenga consecuencias negativas.

Otras preguntas que podemos hacernos para identificar posibles consecuencias negativas causadas por un impacto son:

- **¿Existen condiciones de incumplimiento de confidencialidad (interna y externa)?** Esto normalmente es el caso cuando personas non-autorizados tienen acceso a información y conocimiento ajeno que pondrá en peligro nuestra misión.
- **¿Existen condiciones de incumplimiento de obligación jurídicas, contratos y convenios?** No cumplir con las normas legales fácilmente puede culminar en sanciones penales o económicas, que perjudican nuestra misión, existencia laboral y personal.
- **¿Cuál es el costo de recuperación?** No solo hay que considerar los recursos económicos, tiempo, materiales, sino también el posible daño de la imagen pública y emocional.

Considerando todos los aspectos mencionados, nos permite clasificar la Magnitud del Daño. Sin embargo, otra vez tenemos que definir primero el significado de cada nivel de daño (Baja, Mediana, Alta). Las definiciones mostradas en la imagen anterior solo son un ejemplo aproximado, pero no necesariamente refleja la realidad y la opinión común y por tanto se recomienda que cada institución defina sus propios niveles.

8. **Matriz para el Análisis de Riesgo**

Introducción

La Matriz para el Análisis de Riesgo, es producto del proyecto y fue punto clave en analizar y determinar los riesgos en el manejo de los datos e información de las

organizaciones sociales participantes. La Matriz, que basé en una hoja de calculo, no dará un resultado detallado sobre los riesgos y peligros de cada recurso (elemento de información) de la institución, sino una mirada aproximada y generalizada de estos.

Hay que tomar en cuenta que el análisis de riesgo detallado, es un trabajo muy extenso y consumidor de tiempo, porque requiere que se compruebe todos los posibles daños de cada recurso de una institución contra todas las posibles amenazas, es decir terminaríamos con un sinnúmero de grafos de riesgo que deberíamos analizar y clasificar. Por otro lado, hay que reconocer que la mayoría de las organizaciones sociales y empresas, ni cuentan con personal técnico específico para los equipos de computación, ni con recursos económicos o mucho tiempo para dedicarse o preocuparse por la seguridad de la información que manejan y en muchas ocasiones tampoco por la formación adecuada de sus funcionarios en el manejo de las herramientas informáticas.

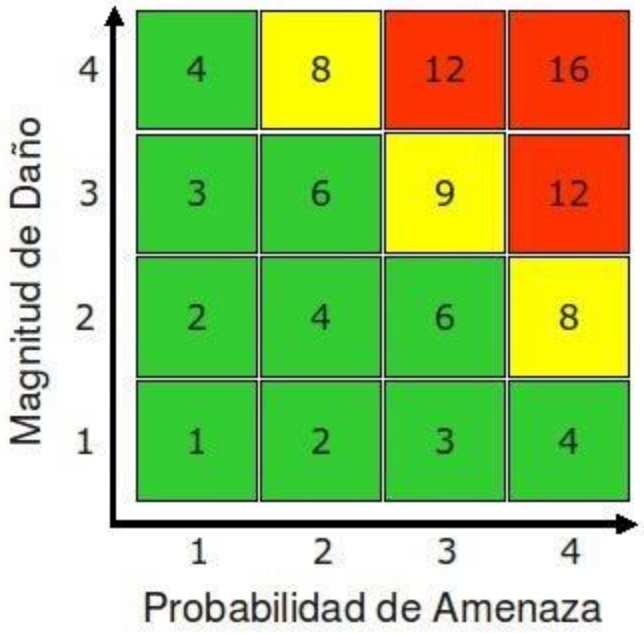
Entonces lo que se pretende con el enfoque de la Matriz es localizar y visualizar los recursos de una organización, que están más en peligro de sufrir un daño por algún impacto negativo, para posteriormente ser capaz de tomar las decisiones y medidas adecuadas para la superación de las vulnerabilidades y la reducción de las amenazas.

Fundamento de la Matriz

La Matriz la basé en el método de Análisis de Riesgo con un grafo de riesgo, usando la formula **Riesgo = Probabilidad de Amenaza x Magnitud de Daño**

La Probabilidad de Amenaza y Magnitud de Daño pueden tomar los valores y condiciones respectivamente

- 1 = **Insignificante** (incluido Ninguna)
- 2 = **Baja**
- 3 = **Mediana**
- 4 = **Alta**



El Riesgo, que es el producto de la multiplicación Probabilidad de Amenaza por Magnitud de Daño, está agrupado en tres rangos, y para su mejor visualización, se aplica diferentes colores.

- **Bajo Riesgo** = 1 – 6 (verde)
- **Medio Riesgo** = 8 – 9 (amarillo)
- **Alto Riesgo** = 12 – 16 (rojo)

Uso de la Matriz

La Matriz verdadera la basé en un archivo con varias hojas de calculo que superan el tamaño de una simple pantalla de un monitor. Entonces por razones demostrativas, en las siguientes imágenes solo se muestra una fracción de ella.
La Matriz contiene una colección de diferentes Amenazas (campos verdes) y Elementos de información (campos rojos). Para llenar la Matriz, tenemos que estimar los valores de la Probabilidad de Amenaza (campos azules) por cada Amenaza y la Magnitud de Daño (campos amarillas) por cada Elemento de Información.

Matriz de Análisis de Riesgo		Probabilidad de Amenaza					
Elementos de Información	Magnitud de Daño	Criminalidad		Sucesos físicos		Negligencia	
		Robo	Virus	Incendio	Falta de Corriente	Compartir contraseñas	No cifrar datos críticos
Datos e Información							
RR.HH							
Finanzas							
Sistema e Información							
Computadoras							
Portátiles							
Personal							
Coordinador							
Personal técnico							

Para la estimación de la Probabilidad de amenazas, se trabaja con un valor generalizado, que (solamente) está relacionado con el recurso más vulnerable de los elementos de información, sin embargo usado para todos los elementos.

Si por ejemplo existe una gran probabilidad de que nos pueden robar documentos y equipos en la oficina, porque ya entraron varias veces y no contamos todavía con una buena vigilancia nocturna de la oficina, no se distingue en este momento entre la probabilidad si robarán una portátil, que está en la oficina (con gran probabilidad se van a llevarla), o si robarán un documento que está encerrado en una caja fuerte escondido (es menos probable que se van a llevar este documento).

Este proceder obviamente introduce algunos resultados falsos respecto al grado de riesgo (algunos riesgos saldrán demasiado altos), algo que posteriormente tendremos que corregirlo. Sin embargo, excluir algunos resultados falsos todavía es mucho más rápido y barato, que hacer un análisis de riesgo detallado, sobre todo cuando el enfoque solo es combatir los riesgos más graves.

En el caso de que se determine los valores para la Probabilidad de Amenaza y Magnitud de Daño a través de un proceso participativo de trabajo en grupo (grande), se recomienda primero llenar los fichas de apoyo para los Elementos de Información y Probabilidad de Amenaza, y una vez consolidado los datos, llenar la matriz.

Dependiendo de los valores de la Probabilidad de Amenaza y la Magnitud de Daño, la Matriz calcula el producto de ambos variables y visualiza el grado de riesgo.

Matriz de Análisis de Riesgo		Probabilidad de Amenaza					
Elementos de Información	Magnitud de Daño	Criminalidad		Sucesos físicos		Negligencia	
		Robo	Virus	Incendio	Falta de Corriente	Compartir contraseñas	No cifrar datos críticos
		3	4	2	3	4	3
Datos e Información							
RR.HH	3	9	12	6	9	12	9
Finanzas	4	12	16	8	12	16	12
Sistema e Información							
Computadoras	2	6	8	4	6	8	6
Portátiles	3	9	12	6	9	12	9
Personal							
Coordinador	4	12	16	8	12	16	12
Personal técnico	3	9	12	6	9	12	9

Dependiendo del color de cada celda, podemos sacar conclusiones no solo sobre el nivel de riesgo que corre cada elemento de información de sufrir un daño significativo, causado por una amenaza, sino también sobre las medidas de protección necesarias

- Proteger los datos de RR.HH, Finanzas contra virus
- Proteger los datos de Finanzas y el Coordinador contra robo
- Evitar que se compartan las contraseñas de los portátiles
- Etc, etc

También, como se mencionó anteriormente, existen combinaciones que no necesariamente tienen mucho sentido y por tanto no se las considera para definir medidas de protección

- Proteger el Personal (Coordinador y Personal técnico) contra Virus de computación
- Evitar la falta de corriente
- Etc, etc
-

Elementos de la Matriz

La Matriz la basé en una hoja de calculo
La Matriz está compuesto por 6 hojas

- **1_Datos**: Es la hoja para valorar el riesgo para los Elementos de Información "Datos e Informaciones", llenando los campos "Magnitud de Daño" y "Probabilidad de Amenaza" conforme a sus valores estimados (solo están permitidos valores entre 1 y 4). Los valores de Probabilidad de Amenaza solo se aplica en está hoja, porque las demás hojas, hacen referencia a estos.

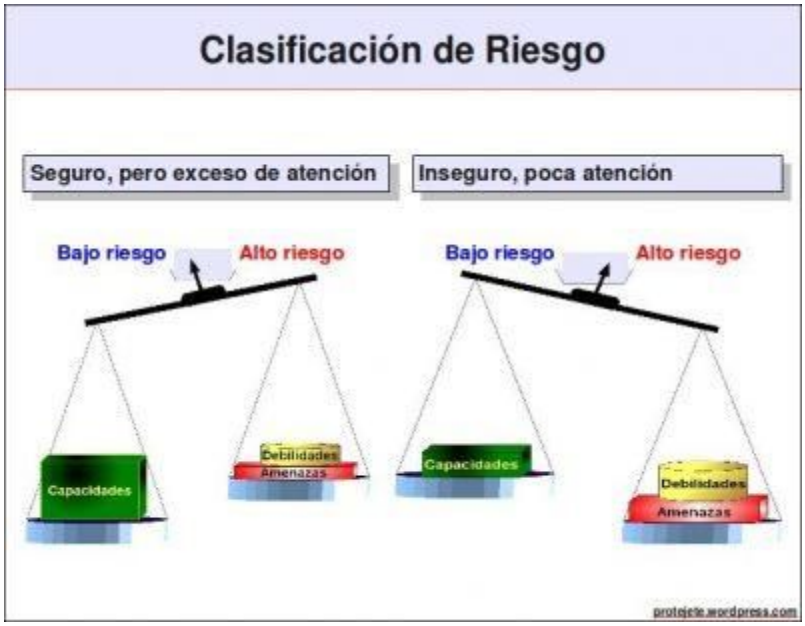
- **2_Sistemas**: Es la hoja para valorar el riesgo para los Elementos de Información "Sistemas e Infraestructura". Hay que llenar solo los valores de Magnitud de Daño, debido a que los valores de Probabilidad de Amenaza están copiados automáticamente desde la hoja "1_Datos". Igual como en "1_Datos", los tres campos de "Clasificación" (Acceso exclusivo, Acceso ilimitado, Costo de recuperación…).
- **3_Personal**: Es la hoja para valorar el riesgo para los Elementos de Información "Personal". Igual como en "2_Sistemas", solo hay que llenar los valores de Magnitud de Daño. Otra vez, los tres campos de "Clasificación" (Imagen pública…, Perfil medio…, Perfil bajo…) solo sirven como campo de apoyo.
- **Análisis_Promedio**: Esta hoja muestra el promedio aritmético de los diferentes riesgos, en relación con los diferentes grupos de amenazas y daños. La idea de esta hoja es ilustrar, en que grupo (combinación de Probabilidad de Amenaza y Magnitud de Daño) hay mayor o menor peligro. No hay nada que llenar en esta hoja.
- **Análisis_Factores**: Esta hoja tiene el mismo propósito como la hoja "Análisis_Promedio", con la diferencia que esta vez el promedio aritmético de los grupos está mostrado en un grafo, dependiendo de la Probabilidad de Amenaza y Magnitud de Daño. La linea amarilla muestra el traspaso de la zona Bajo Riesgo a Mediano Riesgo y la linea roja, el traspaso de Mediano riesgo a Alto Riesgo. La idea de esta hoja es ilustrar el nivel de peligro por grupo y la influencia de cada factor (Probabilidad de amenaza, Magnitud de Daño).
- **Fuente**: Esta hoja se usa solo para la definición de algunos valores generales de la matriz.

Adaptación de la Matriz a las necesidades individuales

La Matriz trabaja con una colección de diferentes Amenazas y Elementos de información. Ambas colecciones solo representan una aproximación a la situación común de una organización, pero no necesariamente reflejan la realidad de una organización especifica. Entonces si hay necesidad de adaptar la Matriz a la situación real de una organización, solo hay que ajustar los valores de las **Amenazas** en la hoja "**1_Datos**" (**solo en esta**) y los **Elementos de información en su hoja correspondiente**. Pero ojo, si hay que insertar, quitar filas o columnas, se recomienda hacerlo con mucho cuidado, debido a que se corre el peligro de introducir errores en la presentación y el calculo de los resultados.

9. Clasificación de Riesgo

El objetivo de la clasificación de riesgo es determinar hasta que grado es factible combatir los riesgos encontrados. La factibilidad normalmente depende de la voluntad y posibilidad económica de una institución, sino también del entorno donde nos ubicamos. Los riesgos que no queremos o podemos combatir se llaman riesgos restantes y no hay otra solución que aceptarlos.



Implementar medidas para la reducción de los riesgos significa realizar inversiones, en general económicas. El reto en definir las medidas de protección, entonces está en encontrar un buen equilibrio entre su funcionalidad (cumplir con su objetivo) y el esfuerzo económico que tenemos que hacer para la implementación y el manejo de estas.

De igual manera como debemos evitar la escasez de protección, porque nos deja en peligro que pueda causar daño, el exceso de medidas y procesos de protección, pueden fácilmente paralizar los procesos operativos e impedir el cumplimiento de nuestra misión. El caso extremo respecto al exceso de medidas sería, cuando las inversiones para ellas, superen el valor del recurso que pretenden proteger.

Entonces el estado que buscamos es, que los esfuerzos económicos que realizamos y los procesos operativos, para mantener las medidas de protección, son suficientes, ajustados y optimizados, para que respondan exitosamente a las amenazas y debilidades (vulnerabilidades) que enfrentamos.

Con Riesgo restante se entiende dos circunstancias, por un lado son estas amenazas y peligros que, aunque tenemos implementados medidas para evitar o mitigar sus daños, siempre nos pueden afectar, si el ataque ocurre con una magnitud superior a lo esperado. Podemos protegernos de cierto modo contra los impactos de un terremoto común, sin embargo cuando ocurre con una fuerza superior o antes no conocido, el impacto general será mucho más grande y muy probablemente afectará también a nosotros.

La otra situación es cuando aceptamos conscientemente los posibles impactos y sus consecuencias, después de haber realizado el análisis de riesgo y la definición de las medidas de protección. Las razones para tomar esta decisión pueden ser varias, sea que evitar los daños no está dentro de nuestra posibilidad y voluntad económica o porque no entendemos que no tenemos suficiente poder sobre el entorno. Sea lo que sea la razón, el punto importante es que sabemos sobre la amenaza y decidimos vivir con ella y su posible consecuencia.

10. **Reducción de Riesgo**

La reducción de riesgo se logra a través de la implementación de Medidas de protección, que basen en los resultados del análisis y de la clasificación de riesgo.

Las medidas de protección están divididos en medidas **físicas y técnicas**, **personales** y **organizativas**.

En referencia al Análisis de riesgo, el propósito de las medidas de protección, en el ámbito de la Seguridad Informática, solo tienen un efecto sobre los componentes de la Probabilidad de Amenaza, es decir aumentan nuestra capacidad física, técnica, personal y organizativa, reduciendo así nuestras vulnerabilidades que están expuestas a las amenazas que enfrentamos. Las medidas normalmente no tienen ningún efecto sobre la Magnitud de Daño, que depende de los Elementos de Información y del contexto, entorno donde nos ubicamos. Es decir, no se trata y muy difícilmente se puede cambiar el valor o la importancia que tienen los datos e informaciones para nosotros, tampoco vamos a cambiar el contexto, ni el entorno de nuestra misión.

La fuerza y el alcance de las medidas de protección, dependen del nivel de riesgo

- **Alto riesgo**: Medidas deben **evitar el impacto y daño**.
- **Medio riesgo**: Medidas solo **mitigan la magnitud de daño** pero no evitan el impacto.

Considerando que la implementación de medidas de protección están en directa relación con inversiones de recursos económicos y procesos operativos, es más que obvio, que las medidas, para evitar un daño, resultarán (mucho) más costosas y complejas, que las que solo mitigan un daño.

Para que las medias sean exitosas, es esencial que siempre verificamos su factibilidad, es decir que técnicamente funcionan y cumplen su propósito, que están incorporadas en los procesos operativos institucionales y que las personas se apropian de estás. Es indispensable que están respaldadas, aprobadas por aplicadas por la coordinación, porque sino, pierden su credibilidad. También significa que deben ser diseñadas de tal manera, que no paralizan o obstaculizan los procesos operativos porque deben apoyar el cumplimiento de nuestra misión, no impedirlo.

Otro punto clave es, que las personas que deben aplicar y apropiarse de las medias saben sobre su existencia, propósito e importancia y son capacitadas adecuadamente en su uso, de tal manera, que las ven como una necesidad institucional y no como otro cortapisa laboral.

Debido a que la implementación de las medidas no es una tarea aislada, única, sino un proceso continuo, su manejo y mantenimiento debe estar integrado en el funcionamiento operativo institucional, respaldado por normas y reglas que regulan su aplicación, control y las sanciones en caso de incumplimiento.

11. Control de Riesgo

El propósito del control de riesgo es analizar el funcionamiento, la efectividad y el cumplimiento de las medidas de protección, para determinar y ajustar sus deficiencias.

Las actividades del proceso, tienen que estar integradas en el plan operativo institucional, donde se define los momentos de las intervenciones y los responsables de ejecución.

Medir el cumplimiento y la efectividad de las medidas de protección requiere que levantemos constantemente registros sobre la ejecución de las actividades, los eventos de ataques y sus respectivos resultados. Estos tenemos que analizados frecuentemente. Dependiendo de la gravedad, el incumplimiento y el sobrepasar de las normas y reglas, requieren sanciones institucionales para los funcionarios.

En el proceso continuo de la Gestión de riesgo, las conclusiones que salen como resultado del control de riesgo, nos sirven como fuente de información, cuando se entra otra vez en el proceso de la Análisis de riesgo.