

ANÁLISIS DE RIESGOS EN SISTEMAS

Unidad 2: Método de análisis de riesgos

Objetivo específico 2: El alumno aprenderá el método de análisis de riesgos y conocerá cuales son los activos, las amenazas, determinara el impacto y el riesgo potencial y como utilizar las salvaguardas y el impacto y riesgo residual que existe

Conceptos a desarrollar en la unidad: Conceptos paso a paso del método de análisis de riesgos los activos, las amenazas, la determinación del impacto potencial y determinación del riesgo potencial, los salvaguardas, el Impacto residual y riesgo residual

TEMA 2. MÉTODO DE ANÁLISIS DE RIESGOS

Introducción

En este tema abordaremos el método de análisis de riesgos, considerando y llevando a cabo el concepto paso a paso de el método, así como identificar los riesgos de los activos, las amenazas que se presentan, teniendo la manera de determinar tanto el impacto potencial como la determinación del riesgo potencial que se presentan en los sistemas, además la integración y formas de salvaguardas que no ayudan a aminorar el impacto y el riesgo residual al que se enfrentan en las organizaciones

2.1 Conceptos paso a paso

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. determinar a qué amenazas están expuestos aquellos activos
3. determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Con el objeto de organizar la presentación, se introducen los conceptos de “impacto y riesgo potenciales” entre los pasos 2 y 3. Estas valoraciones son “teóricas”: en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

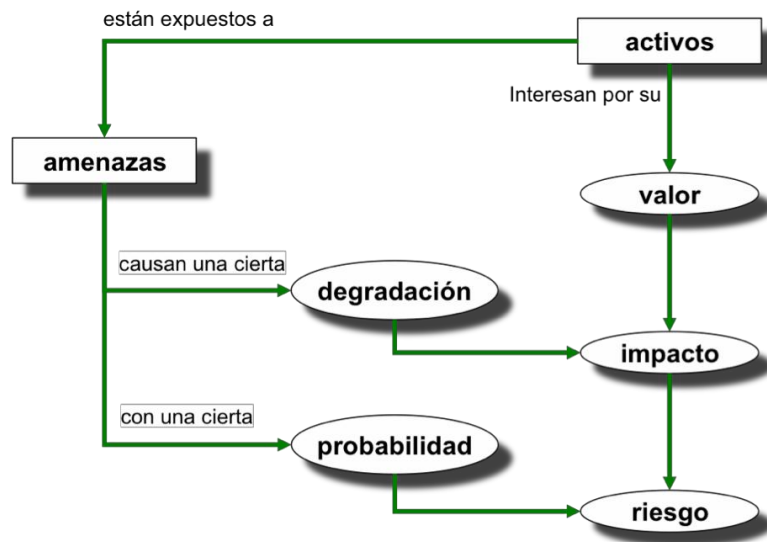


Ilustración 7. Elementos del análisis de riesgos potenciales

2.1.1 Paso 1: Activos

En un sistema de información hay 2 cosas esenciales:

- la **información** que maneja
- y los **servicios** que presta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Subordinados a dicha esencia se pueden identificar otros activos relevantes:

- **Datos** que materializan la información.
- **Servicios** auxiliares que se necesitan para poder organizar el sistema.
- **Las aplicaciones informáticas** (*software*) que permiten manejar los datos.
- **Los equipos informáticos** (*hardware*) y que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar** que complementa el material informático.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
- **Las personas** que explotan u operan todos los elementos anteriormente citados.

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes

Dependencias

Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.

De manera que los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o 'superiores' depende de los activos que se encuentran más abajo o 'inferiores'. Estas estructuras reflejan de arriba hacia abajo las dependencias, mientras que de abajo hacia arriba la propagación del daño caso de materializarse las amenazas.

Por ello aparece como importante el concepto de "dependencias entre activos" o la medida en que un activo *superior* se vería afectado por un incidente de seguridad en un activo *inferior*¹¹.

Se dice que un “activo superior” depende de otro “activo inferior” cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

Aunque en cada caso hay que adaptarse a la Organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

- activos esenciales
 - información que se maneja
 - servicios prestados
- servicios internos
 - que estructuran ordenadamente el sistema de información
- el equipamiento informático
 - aplicaciones (*software*)
 - equipos informáticos (*hardware*)
 - comunicaciones
 - soportes de información: discos, cintas, etc.
- el entorno: activos que se precisan para garantizar las siguientes capas
 - equipamiento y suministros: energía, climatización, etc.
 - mobiliario
- los servicios subcontratados a terceros
- las instalaciones físicas
- el personal
 - usuarios
 - operadores y administradores
 - desarrolladores

Valoración

¿Por qué interesa un activo? Por lo que vale.

No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescídase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

La valoración se puede ver desde la perspectiva de la ‘**necesidad de proteger**’ pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

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.

El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial.

Por otra parte, los sistemas de información explotan los datos para proporcionar servicios, internos a la Organización o destinados a terceros, apareciendo una serie de datos necesarios para prestar un servicio. Sin entrar en detalles técnicos de cómo se hacen las cosas, el conjunto de información y servicios esenciales permite caracterizar funcionalmente una organización. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios.

Dimensiones

De un activo puede interesar calibrar diferentes dimensiones:

- su **confidencialidad**: ¿qué daño causaría que lo conociera quien no debe?
Esta valoración es típica de datos.
- su **integridad**: ¿qué perjuicio causaría que estuviera dañado o corrupto?
Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
- su **disponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
Esta valoración es típica de los servicios¹².

En sistemas dedicados a servicios de la sociedad de la información como puedan ser los de administración electrónica o comercio electrónico, el conocimiento de los actores es fundamental para poder prestar el servicio correctamente y poder perseguir los fallos (accidentales o deliberados) que pudieran darse. Así pues, en los activos esenciales, frecuentemente es útil valorar:

- la **autenticidad**: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)
- la **trazabilidad** del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?
- la **trazabilidad** del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Se reconocen habitualmente como dimensiones básicas la confidencialidad, integridad y disponibilidad. En esta metodología se han añadido la autenticidad y el concepto de trazabilidad, que a efectos técnicos se traducen en mantener la integridad y la confidencialidad de ciertos activos del sistema que pueden ser los servicios de directorio, las claves de firma digital, los registros de actividad, etc.

En un árbol de dependencias, donde los activos superiores dependen de los inferiores, es imprescindible valorar los activos superiores, los que son importantes por sí mismos. Automáticamente este valor se acumula en los inferiores, lo que no es óbice para que también puedan merecer, adicionalmente, su valoración propia.

¿Cuánto vale la “salud” de los activos?

Una vez determinadas qué dimensiones (de seguridad) interesan de un activo hay que proceder a valorarlo. La valoración es la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo. Hay muchos factores a considerar:

- coste de reposición: adquisición e instalación
- coste de mano de obra (especializada) invertida en recuperar (el valor) del activo
- lucro cesante: pérdida de ingresos
- capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- sanciones por incumplimiento de la ley u obligaciones contractuales
- daño a otros activos, propios o ajenos
- daño a personas
- daños medioambientales

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes a respetar son:

- la **homogeneidad**: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra
- la **relatividad**: es importante poder relativizar el valor de un activo en comparación con otros activos

Ambos criterios se satisfacen con valoraciones económicas (coste dinerario requerido para "curar" el activo) y es frecuente la tentación de ponerle precio a todo. Si se consigue, excelente. Incluso es fácil ponerle precio a los aspectos más tangibles (equipamiento, horas de trabajo, etc.); pero al entrar en valoraciones más abstractas (intangibles como la credibilidad de la Organización) la valoración económica exacta puede ser escurridiza y motivo de agrias disputas entre expertos.

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.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

Valoración cuantitativa

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente "natural". La interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es dineraria, además se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución respondiendo a las preguntas:

- ¿Vale la pena invertir tanto dinero en esta salvaguarda?
- ¿Qué conjunto de salvaguardas optimizan la inversión?
- ¿En qué plazo de tiempo se recupera la inversión?
- ¿Cuánto es razonable que cueste la prima de un seguro?

La "Guía de Técnicas" presenta un modelo de análisis basado en valoraciones cuantitativas.

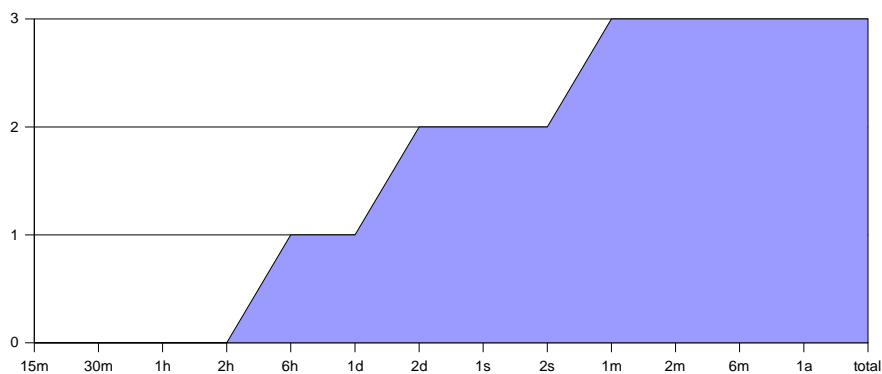
El valor de la interrupción del servicio

Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad.

No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido suponga la terminación de la actividad. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias.

En consecuencia, para valorar la [interrupción de la] disponibilidad de un activo hay que usar una estructura más compleja que se puede resumir en algún gráfico como el siguiente:

donde aparece una serie de escalones de interrupción que terminan con la destrucción total o permanente del activo. En el ejemplo anterior, paradas de hasta 6 horas se pueden asumir sin consecuencias. Pero a las 6 horas se disparan las alarmas que aumentan si la parada supera los 2 días. Y si la parada supera el mes, se puede decir que la Organización ha perdido su capacidad de operar: ha muerto. Desde el punto de vista de los remedios, la gráfica dice directamente que no hay que gastarse ni un euro por evitar paradas de menos de 6 horas. Vale la pena un cierto gasto por impedir que una parada supere las 6 horas o los 2 días. Y cuando se valore lo que cuesta impedir que la parada supere el mes, hay que poner en la balanza todo el valor de la Organización frente al coste de las salvaguardas. Pudiera ser que no valiera la pena.



Coste de la [interrupción de la] disponibilidad

2.1.2 Paso 2: 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.

Identificación de las amenazas

De origen natural

Hay accidentes naturales (terremotos, inundaciones, ...). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

Del entorno (de origen industrial)

Hay desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

Defectos de las aplicaciones

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, ‘vulnerabilidades’¹³.

Causadas por las personas de forma accidental

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

Causadas por las personas de forma deliberada

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

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.

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 valorar su influencia en el valor del activo, en dos sentidos:

degradación: cuán perjudicado resultaría el [valor del] activo

probabilidad: cuán probable o improbable es que se materialice 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 probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal:

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Degradación del valor

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia¹⁵ como medida de la probabilidad de que algo ocurra. Son valores típicos:

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

. Probabilidad de ocurrencia

2.1.3 Determinación del impacto potencial

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 se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias.

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 salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

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. 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.

Agregación de valores de impacto

Los párrafos anteriores determinan el impacto que sobre un activo tendría una amenaza en una cierta dimensión. Estos impactos singulares pueden agregarse bajo ciertas condiciones:

- puede agregarse el impacto repercutido sobre diferentes activos,
- puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común,
- no debe agregarse el impacto acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el impacto al incluir varias veces el valor acumulado de activos superiores,
- puede agregarse el impacto de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,
- puede agregarse el impacto de una amenaza en diferentes dimensiones.

2.1.4 Determinación del riesgo potencial

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 probabilidad de ocurrencia.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (que veremos más adelante):

- zona 1 – riesgos muy probables y de muy alto impacto
- zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo
- zona 3 – riesgos improbables y de bajo impacto
- zona 4 – riesgos improbables pero de muy alto impacto

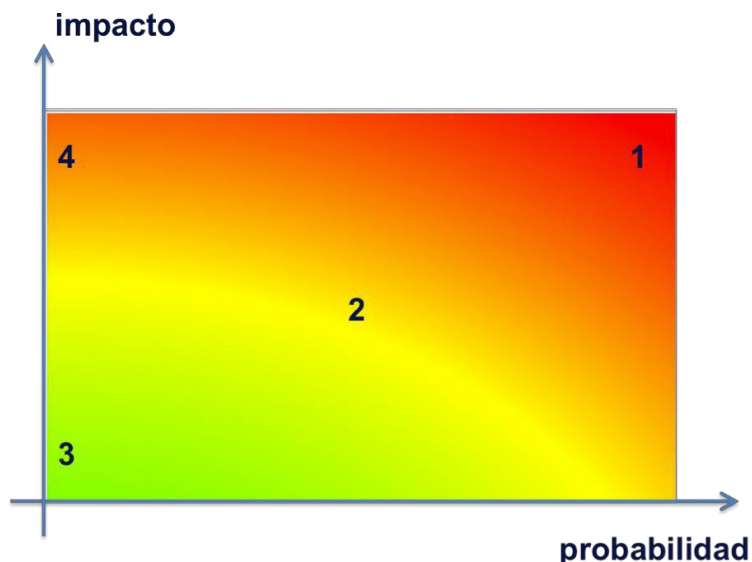


Ilustración 9. El riesgo en función del impacto y la probabilidad

Riesgo acumulado

Es el calculado sobre un activo teniendo en cuenta

- el impacto acumulado sobre un activo debido a una amenaza y
- la probabilidad 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 probabilidad de la amenaza.

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

Riesgo repercutido

Es el calculado sobre un activo teniendo en cuenta

- el impacto repercutido sobre un activo debido a una amenaza y
- la probabilidad 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 probabilidad 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.

2.1.5 Paso 3: Salvaguardas

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, 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 salvaguardas presentes.

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

Selección de salvaguardas

Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

1. tipo de activos a proteger, pues cada tipo se protege de una forma específica
2. dimensión o dimensiones de seguridad que requieren protección
3. amenazas de las que necesitamos protegernos
4. si existen salvaguardas alternativas

Efecto de las salvaguardas

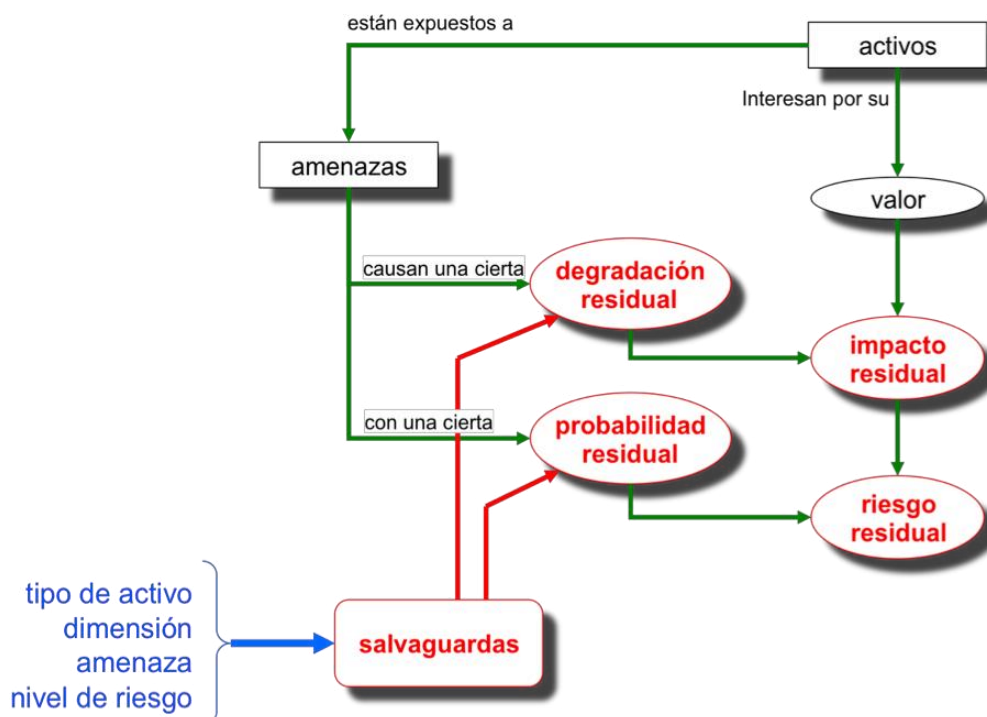
Las salvaguardas entran en el cálculo del riesgo de dos formas:

Reduciendo la probabilidad de las amenazas.

Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

Limitando el daño causado.

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.



Elementos de análisis del riesgo residual

Tipo de protección

Esta aproximación a veces resulta un poco simple, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

[PR] prevención

Diremos que una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los

mismos.

Ejemplos: autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, metodología segura de desarrollo de software, pruebas en pre-producción, segregación de tareas, ...

[DR] disuasión

Diremos que una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados caso de que el atacante realmente se atreva.

Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente, ...

[EL] eliminación

Diremos que una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

Ejemplos: eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, ...; en general, todo lo que tenga que ver con la fortificación o bastionado, ..., cifrado de la información, ..., armarios ignífugos, ...

[IM] minimización del impacto / limitación del impacto

Se dice que una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente.

Ejemplos: desconexión de redes o equipos en caso de ataque, detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente

[CR] corrección

Diremos que una salvaguarda es correctiva cuando, habiéndose producido un daño, lo repara. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.

Ejemplos: gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes, ...

[RC] recuperación

Diremos que una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo.

Ejemplos: copias de seguridad (back-up)

[MN] monitorización

Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posteriori, podemos aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro.

Ejemplos: registros de actividad, registro de descargas de web, ...

[DC] detección

Diremos que una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños.

Ejemplos: antivirus, IDS, detectores de incendio, ...

[AW] concienciación

Son las actividades de formación de las personas anexas al sistema que pueden tener una

influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación.

Ejemplos: cursos de concienciación, cursos de formación, ...

[AD] administración

Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que hayan puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo.

Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad, ...

Eficacia de la protección

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, eficacia que combina 2 factores:

desde el punto de vista técnico

- es técnicamente idónea para enfrentarse al riesgo que protege
- se emplea siempre

desde el punto de vista de operación de la salvaguarda

- está perfectamente desplegada, configurada y mantenida
- existen procedimientos claros de uso normal y en caso de incidencias
- los usuarios están formados y concienciados
- existen controles que avisan de posibles fallos

Vulnerabilidades

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

Traducido a los términos empleados en los párrafos anteriores, son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre un activo. A veces se emplea el término "insuficiencia" para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza.