Unidad 2
Análisis de Riesgo – Medidas de Solución

En un Sistema informático los riesgos son muchos y, además, de variada naturaleza. Para la toma de decisiones basadas en elementos de juicio que posibiliten, hasta donde resulte factible, la eliminación de la incertidumbre, resultará necesario un análisis de los riesgos que permita su conocimiento, probabilidad de ocurrencia y cuantificación. Es necesario determinar:

A)) Qué se necesita proteger?
B)) De qué debo protegerlo?
C)) En qué grado se necesita proteger?

En respuesta a la primera interrogante, o sea determinar cuáles son los elementos componentes del sistema a proteger, se debe realizar una lista minuciosa del sistema informático y sus interrelaciones, haciendo incapie en el conjunto de datos críticos 1) para el desembolvimiento de la organización y 2) para el funcionamiento del sistema en sí.

A partir de esta respuesta, podemos, partiendo de una clasificación básica de los riesgos, determinar de qué debemos proteger el sistema de la organización.

Clasificación de riesgos

< Riesgos de origen natural

Catástrofes climáticas o tectonicas o atmosféricos: solo determinadas zonas de una región so propensas a terremotos, vulcanismo, tornados, inundaciones, grandes lluvias, napas freaticas, etc., que representan en general un riesgo para la operatividad del sistema, que en su extremo puede ocasionar la imposibilidad de seguir operando el sistema.

< Riesgos de origen técnico

Las contingencias debidas a fallas de origen técnico en un sistema informático pueden provenir del mismo sistema (fallas de hardware o de software) o de sistemas externos vinculados o no con aquel (incendios, alimentación eléctrica, aire acondicionado, telecomunicaciones).

En estas situaciones, difíciles de preveer no solo en su ocurrencia sino también en su magnitud,

El objetivo esencial del control y de la seguridad de los sistemas informáticos es mantener la autenticidad, integridad, operatividad y confidencialidad de la información manejada o almacenada en computadoras, frente a contingencias que pueden generar la pérdida de archivos, o de registros o bien la alteración de uno o más registros, o que alteren la prestación de un servicio o la rentabilidad de la organización.

Para la seguridad informática, un sistema informático está formado por las personas, computadoras, papeles, medios de almacenamiento digital, el entorno donde actúan y sus interacciones.

Para eliminar o disminuir el riesgo de ocurrencia o bien para limitar las consecuencias

de una contingencia, existen distintos tipos de actividades o funciones de control o seguridad.

Es conveniente aclarar que el nivel de seguridad de un sistema informático nunca puede llegar al 100 % y lo que se trata de alcanzar es el menor grado de inseguridad, aunque este es variable y depende del tipo de sistema de que se trate.

Las funciones esenciales del control o seguridad son:

1) DISUADIR; para impedir los errores, omisiones, abusos, siniestros y violaciones de secreto, previo a las operaciones de entrada de datos. En este caso se trata de contar con medidas de protección que inspiren respeto (temor) como para mover a alguien a desistir de sus propósitos.El fin de EVITAR; parte incluso de analizar si alguna actividad del sistema informático debería interrumpirse por cuanto se corren importantes riesgos.

2) PREVENIR mediante la adopción de medidas que actúan conjuntamente con el ingreso de datos, rechazando los inválidos y obligando a su corrección. Esta es una función clásica de la seguridad y la más conocida.

3) DETECTAR para que, mediante diversos procedimientos, se advierta sobre errores ocurridos. Detectando un evento no deseado, es necesario que se informe de la falla. Por otra parte, la sola ubicación es de por sí insuficiente. Debe tenderse a una adecuada combinación de prevención y detección.

4) RECUPERAR Y CORREGIR; comprende aquellas acciones que permiten a un sistema recuperar en el menor tiempo posible su capacidad de procesamiento y brindar la información necesaria. Deberá estudiarse la necesidad de hacer frente a una emergencia máxima. (Plan de Desastre).

Un ordenador autónomo, sin enlaces de comunicaciones externas y con todos sus terminales y periféricos dentro de una sala segura y apantallada, únicamente es vulnerable a la entrada de usuarios no autorizados dentro del sistema, y a los accesos de usuarios a información que no están autorizados a recibir. Estos riesgos se pueden reducir mediante medios eficientes de identificación de usuarios y con acceso controlado a la sala de ordenador, siendo estos aspectos de la seguridad física de los ordenadores.

Hay tres maneras principales de atacar la seguridad del ordenador:

Obtención no autorizada de información.
Modificación no autorizada de la información.
Denegación no autorizada de servicio normal a los usuarios.

La obtención no autorizada de información se denomina ataque pasivo y la modificación no autorizada de la información o la denegación de servicios se denomina ataque activo.

Ambas formas de ataque pueden tener lugar en cualquier punto del enlace de comunicaciones o de red, que puedan transportar información relevante.

Los objetivos principales de las contramedidas contra los ataques a la seguridad son:

_ Minimizar la probabilidad de una intrusión proporcionando dispositivos y

procedimientos de protección.
_ Detectar cualquier intrusión tan pronto como sea posible.
_ Identificar la información objeto del ataque e identificar la información de control y estado necesaria para recuperarse del ataque.

ATAQUES PASIVOS

Los ataques pasivos pueden resultar en la obtención del contenido de determinados mensajes, pero si los datos están cifrados todavía pueden ser de valor para el intruso para obtener la localización e identidades de los interlocutores; esta información esta generalmente disponibles en los encabezamientos de lo mensaje o de bloque. La longitud de los mensajes y su frecuencia de transmisión pueden revelar la naturaleza de los mensajes que pueden estar siendo transmitidos. Estas formas de ataque pasivo (que no causan la obtención del contenido del mensaje), conocidas como violaciones de la seguridad de la transmisión, se pueden utilizar como parte de una intrusión más sofisticada.

ATAQUES ACTIVOS

Un ataque activo en un enlace de comunicaciones puede tomar muchas formas, como por ejemplo:

_ Modificación selectiva de los encabezamientos o de los datos.
_ Borrado de mensajes o de los datos.
_ Retraso de mensajes.
_ Reordenamiento de mensajes.
_ Duplicación de mensajes.
_ Insertación de mensajes adicionales.

Los ataques activos se pueden subdividir en tres categorías:

Modificación de mensajes.
Negación de servicio de mensajes.
Iniciación de asociación espuria.

La modificación de mensajes incluye ataques sobre:

_ La autenticidad (modificando la información de control de protocolos y haciendo que el mensaje sea enviado hacia un destino equivocado, o mediante la inserción de mensajes ficticios.
_ La integridad (mediante la modificación de los datos).
_ La ordenación (mediante el borrado de mensajes o la modificación de la información

de secuenciamiento en el protocolo).

La denegación del servicio de mensajes incluye los ataques en los cuales el intruso descarta o retrasa mensajes. La iniciación de asociación espuria incluye los ataques en los cuales se emiten secuencias de mensajes previamente grabados o se hacen intentos de establecer un acceso bajo una identidad falsa.

CONTRAMEDIDAS

Se pueden tomar muchas precauciones para reducir la probabilidad de fallos en la seguridad de las comunicaciones. Estas contramedidas pueden, en algunos casos, ser caras e incómodas, y es necesario seleccionar aquellas que sean adecuadas al nivel de riesgo y al tipo de amenaza que se prevé.

La gestión de riesgo es un método para la identificación, medida y control de sucesos inciertos, y se puede aplicar a la seguridad de las comunicaciones. Los elementos de gestión de riesgo son:

- Análisis de riesgo, que es una investigación sistemática de las amenazas potenciales y una cuantificación del impacto producido por acciones potenciales.
- Diseño alternativo de contramedidas que consiste en el diseño de varias contramedidas para cada amenaza, de modo que se satisfagan los requerimientos de seguridad especificados.
- Implementación y monitorización, que implementa un sistema de seguridad efectiva y monitoriza el sistema para garantizar una efectividad continua.

<u>Análisis de riesgo Vs. Valoración de Riesgo</u>

Los objetivos de la valoración de riesgo se enfocan en los siguientes aspectos:

1. Ayudar en la identificación de exposiciones
2. Ayudar en la cuantificación de los valores de las exposiciones.

Mientras que un análisis de riesgo es más amplio y su finalidad además de la valoración de riesgos incluye

3. Permitir un ranking de exposiciones por prioridad
4. Servir como base para el análisis del coste eficaz.

Las exposiciones implican puntos de riesgo para los datos y en general determinan puntos de control para los mismos.

Todo proceso de Análisis de riesgo debe basarse en los siguientes factores:

* Factor Crítico de Éxito

Si un estudio es suficientemente importante para hacerlo, es suficientemente importante hacerlo correctamente - y eso empieza con un apoyo total y compromiso de la Cabeza estratégica de una organización.

* Elementos de riesgo

Básicamente hay dos elementos principales de riesgo: *P*, la probabilidad de números de veces por año que ocurra una exposición, y *C*, el costo o pérdida atribuido a tal exposición. Los que se relacionan mediante la expresión

$R = P \times C$ donde el riesgo *R* esta expresado en términos de pérdidas por año.

* Valor de la probabilidad (P)

La mejor forma de expresar este factor de clasificadores de tiempo es como Tasas de ocurrencia esperadas.

Tiempo de frecuencia subjetiva	**Valor (P)**	**Multiplicador de Pérdidas (P_l)**	**Anualizado por año**
Una vez en 300 años	1	1/300	0,00333
Una vez en 30 años	2	1/30	0,03333
Una vez en 3 años	3	1/3	0,33333
Una vez en 100 días	4	365/100	3,65000
Una vez en 10 días	5	365/10	36,50000
Una vez al día	6	365/1	365,00000
10 veces al día	7	365/0.1	3650,00000
100 veces al día	8	365/0.01	36500,00000

Asignar valores de costo

Se debe elegir entre los siguientes tipos de coste (pérdidas) más conveniente para una determina exposición

1) El costo del material activo
2) El costo para reparar el activo (daños, menos el seguro)
3) El costo para reinstalar el activo (Incluye pedido, fletes e instalación)

4) El costo para operar sin el activo (incluye pérdida general, pérdida aplazada, pérdida confidencial del negocio y oportunidad de pérdida)
5) El costo de la capacidad de retroceso/recuperación
6) El costo del seguro.

Pérdida Potencial por Incidente (P.P.P.I)

Representa un índice que intenta acercar un valor que relaciona una estimación de la pérdida económica en que se incurriría por la ocurrencia de una contingencia y la probabilidad de ocurrencia de la misma:

$$PPPI = \frac{Perdida\_Estimada}{\Pr obabilidad\_de\_ocurrencia}$$

Conviene a veces utilizar un enfoque holístico al valorar las posibles contingencias, ya que pueden existir costos ocultos o no inmediatamente obvios que no hayamos considerado.

- **Evaluación de riesgos**
- **Evaluación de Costos**
- **Estrategia de Protección**

Evaluación de riesgos

El primer paso a dar es establecer qué es lo que se desea proteger, por qué y cuál es su valor, así como de quién se desea proteger. El objetivo que perseguimos no es otro que lograr que un ataque a nuestros bienes sea más costoso que su valor, invirtiendo menos de lo que vale.

El motivo es muy sencillo: si proteger nuestros bienes es más caro de lo que valen, entonces nos resulta más conveniente obtenerlos de nuevo que protegerlos, e igualmente, si atacarlos es más caro de lo que valen, a los atacantes les merecerá más la pena obtenerlos por sí mismos que atacarnos.

De esta simple ecuación se pueden derivar fácilmente las normas básicas en la evaluación de los riesgos, que podemos desglosar en dos partes:

- **Valor Intrínseco del producto a proteger**
- **Costo derivados de su pérdida**

Ambos conceptos son fundamentales, y ambos deben extenderse por toda la gama de posibilidades. Para ello lo mejor es observar el objeto de protección fría y metódicamente:

Valor intrínseco

Es probablemente el elemento más fácil de valorar: nadie mejor que Ud. para saber cuánto vale. Sólo necesita asegurarse de que valora todos los costos afectados, examinando minuciosamente todos los componentes a proteger.

Por ejemplo: un servidor de un departamento donde trabajan varios grupos de investigación podría valorarse -muy simplemente - de esta forma:

- **valor del ordenador**
- **valor del software**
- **valor de los resultados de investigación, patentes, etc., almacenados**
- **costo del esfuerzo y materiales invertidos en obtener esos datos**
- **valor de la información personal que contiene**

Costos derivados

Una vez más, hay que intentar abarcar todas las posibilidades. Aquí es bueno a menudo contar con un experto en temas de seguridad, pues pueden existir costos derivados que Ud. no conozca o imagine. Podemos seguir el ejemplo anterior:

- **valor de sustituir el hardware**
- **valor de sustituir el software**
- **valor de los resultados**
- **costo de reproducir los experimentos significativos**
- **costo de regenerar la información personal**

Estos parecen los costos más obvios. Pero puede haber mucho más. Por ejemplo, los resultados pueden ser públicos y tener un valor aparente nulo, pero en un entorno bajo las últimas propuestas de leyes internacionales de derechos de copia, su pérdida a manos de una compañía comercial podría suponer su desaparición del dominio público y el que esa información deje de ser gratuita y pase a ser comercial con un costo -incluso para quien originalmente la desarrolló- notoriamente elevado.

Más aún, información aparentemente inocua puede resultar tremendamente sensible: unos datos personales en apariencia inocentes podrían permitir a alguien suplantar a otra persona, otorgándole impunidad para cometer crímenes que al final serán imputados a la persona cuyos *inocentes* datos fueron comprometidos.

Un análisis detallado del sistema podría revelar que además existen datos confidenciales, o acuerdos con empresas, o información privilegiada que un agresor avezado podría usar en su beneficio y -probablemente- en nuestro detrimento. Es decir, no sólo se trata del valor del elemento perdido -si es que algo se pierde- si no también del valor añadido que gana el atacante y la repercusión de esa ganancia sobre nosotros.

Esta evaluación debe afectar todos los aspectos: además de los bienes, está en nuestro ejemplo el tiempo que fue necesario para obtenerlos. Un atacante podría intentar acceder a ellos sólo por ahorrarse el costo de realizar un desarrollo propio o el tiempo que éste supuso, o para obtener la experiencia y conocimientos que se ganó en su obtención.

En resumen, aunque en principio pueda parecer fácil la valoración de los bienes protegidos, pueden existir numerosos costos ocultos inherentes a su pérdida o compromiso que sólo un análisis detallado puede revelar y que a menudo requieren una valoración por alguien con experiencia en seguridad en conjunción con expertos especializados en el tratamiento de los bienes protegidos.

Evaluación de costos

La evaluación de los costos debe seguir las normas del sentido común Esto supone una serie de normas o reglas derivadas:

- **La seguridad debe cubrir todos los posibles métodos de ataque**
- **La máxima seguridad obtenible es la del elemento más débil del sistema**
- **La solución de seguridad constituye un sistema complejo**
- **Deben evaluarse tanto las medidas individuales como las interacciones entre todos los componentes del sistema**

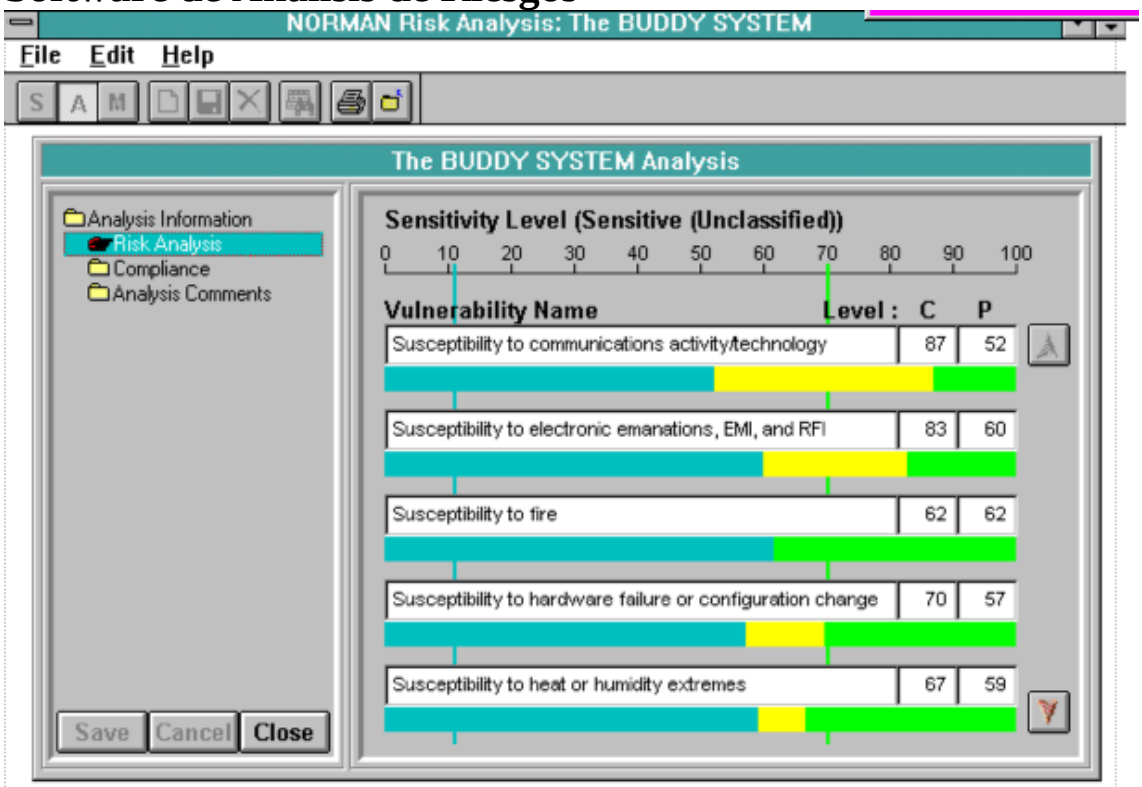
Recordemos que nuestro objetivo es minimizar el costo de la protección manteniéndolo por debajo del de los bienes protegidos maximizando el costo de los ataques manteniéndolo por encima del de los bienes protegidos, lo que nos lleva a esta otra regla:

- **Toda medida de seguridad debe contrastarse con el costo asociado a intentar romperla.**

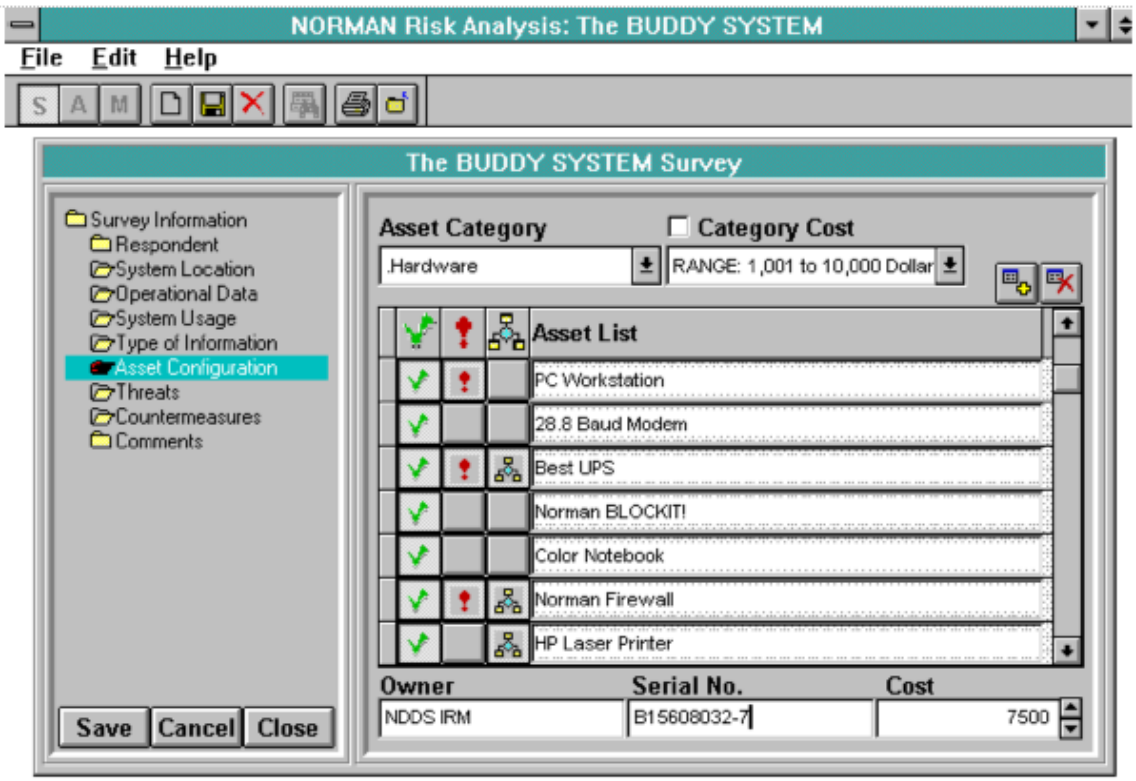
Conviene en general ser metódicos al evaluar las medidas de seguridad, y buscar un compromiso que asegure la protección sin dañar excesivamente la funcionalidad del sistema.

Y **siempre** recordar la norma principal: **la evaluación debe ajustarse al sentido común**. Si bien los comerciales, ejecutivos y demás integrantes de la organización ajena a la materia es muy propensa a engrosar los costos para aparentar una mayor importancia y enriquecer su autoestima promocionando su imagen personal, el profesional de la seguridad debe ser capaz de ver más allá de estas mezquindades y saber mantener un punto de referencia sensato en su evaluación.

Software de Análisis de Riesgos



Se calculan vulnerabilidades automáticamente basado en contramedidas del lugar. Los niveles aceptables son fijados en base a la sensibilidad de los datos como se establecido por el estudio.



El módulo de colección de datos (releva miento) colecciona del sistema, rápidamente y fácilmente, la información especifica. Identificación del recurso y la valoración es un paso importante.