ANALISIS DE RIESGOS EN SISTEMAS

Unidad 9: Consejos prácticos

Objetivo específico 9: El alumno aprenderá como es el desarrollo, alcance y profundidad de los riesgos, realizara la valoración de activos e identificar las amenazas dándoles un valor para poder seleccionar los salvaguardas para obtener una protección básica.

Conceptos a desarrollar en la unidad: Consejos prácticos, Alcance y profundidad, Para identificar activos, Para descubrir y modelar las dependencias entre activos, Para valorar activos, Para identificar amenazas, Para valorar amenazas, Para seleccionar salvaguardas, Aproximaciones sucesivas, Protección básica

Introducción

El planteamiento puede quedar un poco abstracto y no permitir al analista progresar con solvencia a través de los pasos indicados si confundiera lo importante con lo esencial. Por ello se ha considerado conveniente incluir algunos comentarios que puedan servir de guía para avanzar.

Se recomienda también que se recopilen tipos de activos, dimensiones de valoración, guías de valoración, catálogos de amenazas y de salvaguardas.

9.1 Alcance y profundidad

Se cubre un espectro muy amplio de intereses de sus usuarios. En el planteamiento de estas guías se ha seguido un criterio “de máximos”, reflejando todo tipo de activos, todo tipo de aspectos de seguridad; en definitiva, todo tipo de situaciones. En la práctica, el usuario puede encontrarse ante situaciones donde el análisis es más restringido. Siguen algunos casos prácticos frecuentes:

- sólo se requiere un estudio de los ficheros afectos a la legislación de datos de carácter personal
- sólo se requiere un estudio de las garantías de confidencialidad de la información
- sólo se requiere un estudio de la seguridad de las comunicaciones
- sólo se requiere un estudio de la seguridad perimetral
- sólo se requiere un estudio de la disponibilidad de los servicios (típicamente porque se busca el desarrollo de un plan de contingencia)
- se busca una homologación o acreditación del sistema o de un producto
- se busca lanzar un proyecto de métricas de seguridad, debiendo identificar qué puntos interesa controlar y con qué grado de periodicidad y detalle
- etc.

Estas situaciones, frecuentes, se traducen en un ajuste del alcance del análisis. Una estrategia frecuente es identificar como servicio a proporcionar el ámbito que deseamos analizar en detalle y usarlo como perímetro exterior de los activos, incorporando directamente valoraciones inferidas de la información que se maneja y la calidad que se espera del servicio.

Además de cubrir un dominio más o menos extenso, pueden darse situaciones en las que se requieren análisis de diferente calado:

- un análisis urgente para determinar los activos críticos
- un análisis global para determinar las medidas generales
- un análisis de detalle para determinar salvaguardas específicas para ciertos elementos del sistema de información
- un análisis de detalle cuantitativo para determinar la oportunidad de un gasto elevado

En resumen, las tareas que a continuación se detallan hay que adaptarlas

1. horizontalmente al alcance que se requiere
2. verticalmente a la profundidad oportuna

9.2 Para identificar activos

Conviene repetir que sólo interesan los recursos de los sistemas de información que tienen un valor para la Organización, bien en sí mismos, bien porque sobre sus hombros descansan activos de valor.

A título de ejemplo, un servidor de presentación web es un activo de escaso valor propio. Esto puede asegurarse porque no es normal que una Organización despliegue un servidor de presentación web salvo que lo necesite para prestar un servicio. Todo su valor es imputado:

- la indisponibilidad del servidor supone la interrupción del servicio; el coste que suponga la interrupción del servicio es el valor de disponibilidad que se le imputará al servidor
- el acceso no controlado al servidor pone en riesgo el secreto de los datos que presenta; el coste que suponga la pérdida de confidencialidad de los datos es el valor de confidencialidad que se le imputará al servidor
- ... y así con las diferentes dimensiones en consideración

Los intangibles

Ciertos elementos de valor de las organizaciones son de naturaleza intangible:

- credibilidad o buena imagen
- conocimiento acumulado
- independencia de criterio o actuación
- intimidad de las personas
- integridad física de las personas

Estos elementos pueden incorporarse al análisis de riesgos como activos o como elementos de valoración. La cuantificación de estos conceptos es a menudo difícil; pero de una u otra forma nunca puede olvidarse que lo que hay que proteger en última instancia es la misión de la Organización y el valor de ésta reside en estos intangibles. .

Identificación de activos

Quizás la mejor aproximación para identificar los activos sea preguntar directamente:

- ¿Qué activos son esenciales para que usted consiga sus objetivos?
- ¿Hay más activos que tenga que proteger por obligación legal?
- ¿Hay activos relacionados con los anteriores?

Lo esencial es siempre la información que se maneja y los servicios que se prestan. A veces nos interesa singularizar la diferente información y los diferentes servicios, mientras que otras veces podemos agrupar varias informaciones o varios servicios que son equivalentes a efectos de requisitos de seguridad. Incluso es frecuente hacer paquetes de { información + servicios } que la Dirección entiende como un uno.

No siempre es evidente qué es un activo en singular.

Es habitual y práctico identificar lo que podríamos llamar subsistemas. Un subsistema típico es un equipo informático, que bajo ese nombre contiene el *hardware*, los soportes de información (discos), periféricos, sistema operativo y aplicaciones (*software*) de base tales como ofimática, antivirus, etc. Si es posible, trate ese conglomerado como un activo único.

Si por ejemplo en su unidad tiene 300 puestos de trabajo PC, todos idénticos a efectos de configuración y datos que manejan, no es conveniente analizar 300 activos idénticos. Baste analizar un PC genérico que cuya problemática representa la de todos. Agrupar simplifica el modelo. Una buena idea es tener tantos activos como perfiles de configuración de equipos personales.

Otras veces se presenta el caso contrario, un servidor central que se encarga de mil funciones: servidor de ficheros, de mensajería, de la intranet, del sistema de gestión documental y ... En este caso conviene segregar los servicios prestados como servicios (internos) independientes. Sólo cuando se llegue al nivel de equipamiento físico habrá que hacer confluir en un único equipo todos los servicios. Si en el futuro se consigue segregar servicios entre varios servidores, entonces es fácil revisar el modelo de valor y dependencias.

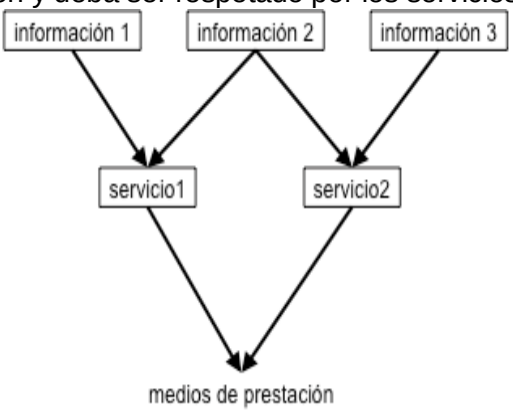
Durante la fase de identificación de activos es frecuente que haya ciclos de expansión en los que los activos complejos se desagregan en activos más sencillos, y fases de compresión, en las que muchos activos se agrupan bajo un activo único (es frecuente hablar de subsistemas). Estos ciclos se repiten recurrentemente hasta que

- el conjunto de activos sea lo bastante detallado como para no olvidarnos de nada
- el número de activos no sea tan grande que nos perdamos
- la denominación de los activos no sea ambigua y recoja la terminología habitual en la Organización

en pocas palabras, el modelo debe ser manejable y **fácil de explicar** a los que van a tomar decisiones a partir de nuestras conclusiones.

9.3 Para descubrir y modelar las dependencias entre activos

Siempre hay que empezar poniendo en lo más alto la información y los servicios. Depende de cada circunstancia el que sea antes la información o los servicios; pero lo más frecuente es que el valor esté en la información y deba ser respetado por los servicios que la manejan.



Dependencias al nivel superior

A veces es más difícil de lo esperado porque los responsables de los activos suelen estar más preocupados por el encadenamiento funcional entre activos que por la dependencia en el sentido de propagación de valor (requisitos de seguridad).

Es necesario transmitir al interlocutor que no se busca qué es necesario para que el sistema funciones, sino al revés, se busca dónde puede fallar el sistema o, más precisamente, dónde puede verse comprometida la seguridad de los activos.

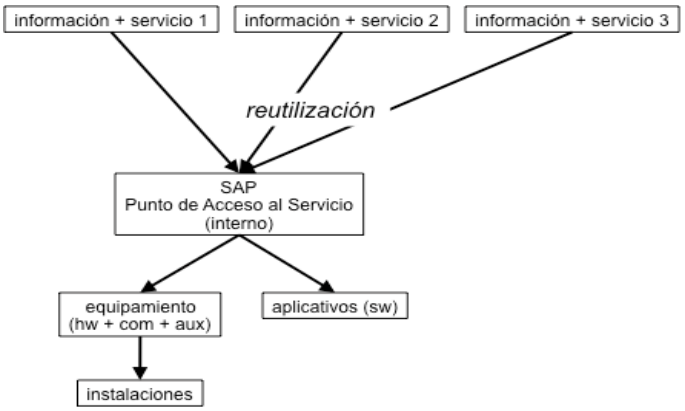
- Si unos datos son importantes por su confidencialidad, se necesita saber en qué sitios van a residir dichos datos y por qué lugares van a circular: en esos puntos pueden ser revelados.
- Si unos datos son importantes por su integridad, se necesita saber en qué sitios van a residir dichos datos y por qué lugares van a circular: en esos puntos pueden ser alterados.
- Si un servicio es importante por su disponibilidad, se necesita saber qué elementos se usan para prestar dicho servicio: el fallo de esos elementos detendría el servicio.

Estas consideraciones pueden plantearse con argumentos del tipo:

- si usted quisiera acceder a estos datos, ¿dónde atacaría para robarlos?
- si usted quisiera detener este servicio, ¿dónde atacaría para estropearlo?

Este planteamiento de "póngase en el lugar del atacante" es el que da pie a las técnicas denominadas "árboles de ataque"[29] que van parejas a lo que en esta metodología se denominan dependencias. En efecto, un activo puede ser atacado directamente o indirectamente a través de otro activo del que dependa.

Las anteriores consideraciones pueden desembocar en un diagrama "plano" de dependencias que se puede (y conviene a efectos prácticos) convertir en un árbol más compacto. Así, es normal decir que los servicios dependen del equipamiento, que depende a su vez de los locales donde se ubican los equipos, sin necesidad de explicitar que los servicios dependen de los locales. Es frecuente identificar "servicios internos" o "servicios horizontales" que son agrupaciones de activos para una cierta función. Estos servicios intermedios son eficaces para compactar el grafo de dependencias, pues las dependencias de dichos servicios se interpretan sin ambigüedad como dependencia de todos los elementos que prestan el servicio.



Servicios internos

Cuando se usen diagramas de flujo de datos o diagramas de procesos, no debe preocupar tanto la ruta que siguen los datos como el conjunto (desordenado) de elementos que intervienen. Un proceso depende de todos los activos que aparecen en su diagrama. Unos datos dependen de todos los sitios por donde pasen. Tanto en unos como en otros diagramas es frecuente encontrar descripciones jerarquizadas donde un proceso se subdivide en niveles de mayor detalle. Estas jerarquías de diagramas pueden ayudar a elaborar el grafo de dependencias.

Hay organizaciones donde está muy clara la información que hay que tratar y a partir de ella podemos identificar los servicios que la tratan y el equipamiento desplegado.

Hay organizaciones más centradas en los servicios que prestan, pudiendo partir de una enumeración de servicios para asociarles la información que manejan y el equipamiento desplegado.

Hay veces que el análisis empieza por el inventariado de equipamiento y luego se va buscando qué servicios se prestan y qué información se trata en el sistema.

Errores típicos

No es correcto decir que una aplicación depende de la información que maneja. El razonamiento de quien tal afirma es que "la aplicación no funcionaría sin datos", lo que es correcto; pero no es lo que interesa reflejar.

Más bien es todo lo contrario: la [seguridad de la] información depende de la aplicación que la maneja. En términos de servicio, se puede decir que la aplicación no vale para nada sin datos. Pero como el valor es una propiedad de la información, y la información es alcanzable por medio de la aplicación, son los requisitos de seguridad de la información los que hereda la aplicación. Luego la información depende de la aplicación. En otras palabras: a través de la aplicación puede

accederse a la información, convirtiéndose la aplicación en la vía de ataque.

Dado que datos y aplicaciones suelen aunar esfuerzos para la prestación de un servicio, el valor del servicio se transmite tanto a los datos como a las aplicaciones intervinientes.

mal	***bien***
aplicación → información	información → aplicación

Dependencias de la información y las aplicaciones

En este contexto, a veces conviene distinguir entre los datos y la información. La información es un bien esencial, siendo los datos una concreción TIC de la información. La información es valiosa, lo demás es valioso en la medida en que contiene información.

La información que maneja un sistema o bien se pone por encima de los servicios, o bien se agrupa

1. información → servicios → equipamiento (incluyendo datos, aplicaciones, equipos, …)
2. { información + servicios } → equipamiento (incluyendo datos, aplicaciones, equipos, …)

No es correcto decir que una aplicación dependa del equipo donde se ejecuta. El razonamiento de quien tal afirma es que “la aplicación no funcionaría sin equipo”, lo que es correcto; pero no es lo que interesa reflejar. Si tanto la aplicación como el equipo son necesarios para prestar un servicio, se debe decir explícitamente, sin buscar caminos retorcidos.

mal	***bien***
• servicio → aplicación • aplicación → equipo	• servicio → aplicación • servicio → equipo

Dependencias de los servicios

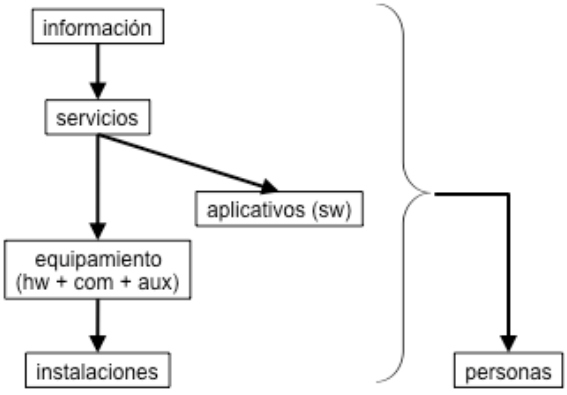
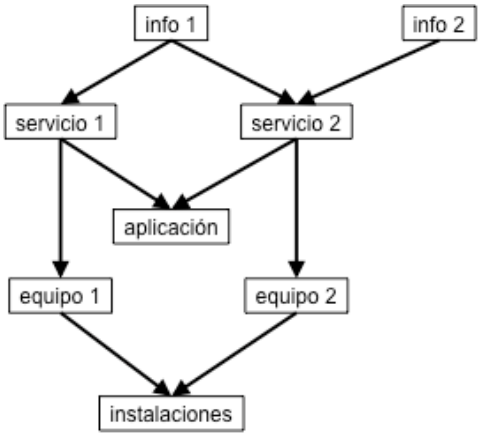


Ilustración 20. Jerarquía de dependencias

Los errores comentados a veces pasan desapercibidos mientras el sistema es muy reducido (sólo hay un servicio, una aplicación y un equipo); pero aparecen en cuanto el sistema crece. Por ejemplo, una aplicación X puede ejecutarse en diferentes equipos con diferentes datos para prestar diferentes servicios. Resulta entonces imposible relacionar la aplicación con uno o más equipos, salvo considerando cada caso



Dependencias entre activos para la prestación de unos servicios

¿Están bien modeladas las dependencias?

Establecer dependencias es una tarea delicada que puede acabar mal. Antes de dar por bueno un modelo de dependencias hay que trazar para cada activo todos los activos de los que depende directa o indirectamente. Y se debe responder positivamente a las preguntas de si

- ¿Están todos los que son? Es decir, si se han identificado todos los activos en los que puede ser atacado indirectamente el activo valorado.
- ¿Son todos los que están? Es decir, si realmente el activo valorado puede ser atacado en todos esos activos de los que depende

Como la relación de dependencia propaga el valor acumulado, encontrar un activo sin valor acumulado es síntoma de que las dependencias están mal modeladas o, simplemente, que el activo es irrelevante.

En otras palabras: para saber si las dependencias están bien establecidas, estudie el valor acumulado.

9.4 Para valorar activos

Siempre conviene valorar la información que constituye la razón de ser del sistema de información.

Si se han modelado servicios esenciales (prestados a usuarios externos al dominio de análisis), conviene valorarlos igualmente.

Es fácil identificar activos de tipo información y valorarlos siguiendo clasificaciones pautadas como su carácter personal o su clasificación de seguridad. Pero pasa a ser mucho más delicado valorar datos de tipo comercial u operacional porque hay que ir a las consecuencias del daño sufrido. Por ello en las metodologías de gestión de riesgos se requiere que la Organización establezca unos criterios para valorar, criterios que trascienden a los analistas y que deben proceder de los órganos superiores que son los encargados de valorar el sistema y de recibir los resultados del análisis.

El resto de los activos puede frecuentemente pasar sin valorar, pues su valor más importante es soportar la información y/o los servicios y de ese cálculo se encargan las relaciones de dependencias.

No obstante, si considera oportuno valorar otro tipo de activos ...

Los activos más sencillos de valorar son aquellos que se adquieren en un comercio. Si se avería, hay que poner otro. Esto cuesta dinero y tiempo (o sea, más dinero). Se habla de un coste de reposición. Salvo notorias excepciones, frecuentemente ocurre que el coste de los activos físicos es despreciable frente a otros costes, pudiendo obviarse.

Es difícil valorar las personas, en general; pero si un puesto supone una formación lenta y trabajosa, hay que tener en cuenta que la persona que desempeña ese puesto se convierte en

muy valiosa, pues su “coste de reposición” es notable.

En cualquier caso, para valorar un activo se debe identificar al responsable, que será la persona adecuada para valorar el activo. A este responsable hay que ayudarle con tablas de valoración como las del capítulo 4 del "Catálogo de Elementos" que, adaptadas al caso concreto, permitan traducir la percepción de valor en una medida cualitativa o cuantitativa del mismo.

A menudo no existe el responsable único y singular de un activo y/o servicio, sino que varias personas dentro de la Organización tienen opinión cualificada al respecto. Hay que oírlas todas. Y llegar a un consenso. Si el consenso no es obvio, puede requerir

un careo: junte a los que opinan e intente que lleguen a una opinión común

un Delphi: mande cuestionarios a los que opinan e intente que converjan a una opinión común

En los procesos de valoración de activos es frecuente recurrir a personas diferentes para valorar activos diferentes. Y es frecuente que cada entrevistado considere sus activos como de la máxima importancia; tanto más frecuente cuanto más especializado esté el entrevistado. Como muchas valoraciones son estimaciones de valor, hay que cuidar que todo el mundo use la misma escala de estimar.

Por ello es importante usar una tabla, directamente o adaptada al caso concreto. Y es importante que tras haber preguntado a los que entienden de cada activo, todos reciban una copia de la valoración global del sistema para que aprecien el valor relativo de “sus activos” y opinen en contexto.

Datos de carácter personal

Los datos de carácter personal están tipificados por leyes y reglamentos, requiriendo de la Organización que adopte una serie de medidas de protección independientes del valor del activo.

La forma más realista de enfrentarse a los activos de carácter personal es caracterizarlos como tales en el nivel que corresponda y, además, determinar su valor: el daño que supondría su revelación o alteración indebida. Con esta aproximación, el análisis de impactos y riesgos permitirá proteger los datos tanto por obligación legal como por su propio valor.

9.5 Para identificar amenazas

La tarea aparece como imposible: para cada activo, en cada dimensión, identificar amenazas.

Se puede partir de la experiencia pasada, propia o de organizaciones similares. Lo que ha ocurrido puede repetirse y, en cualquier caso, sería impresentable no tenerlo en cuenta.

Complementariamente, un catálogo de amenazas como el incluido en el "Catálogo de Elementos" ayuda a localizar lo que conviene considerar en función del tipo de activo y de las dimensiones en las que tiene un valor propio o acumulado.

A menudo se recurre a idear escenarios de ataque que no son sino dramatizaciones de cómo un atacante se enfrentaría a nuestros sistemas. Esta técnica es la que a veces se denomina “árboles de ataque”. Póngase en la piel del atacante e imagine qué haría con sus conocimientos y su capacidad económica. Puede que tenga que plantearse diferentes situaciones dependiendo del perfil técnico del atacante o de sus recursos técnicos y humanos. Estas dramatizaciones son interesantes para poder calcular impactos y riesgos; pero además serán muy útiles a la hora de convencer a la alta dirección y a los usuarios de por qué una amenaza no es teórica sino muy real. Es más, cuando evalúe las salvaguardas puede ser conveniente revisar estos escenarios de ataque.

Es habitual que las herramientas de soporte al análisis de riesgos aporten perfiles típicos para apoyar en esta tarea.

9.6 Para valorar amenazas

La tarea es desmoralizadora: para cada activo en cada dimensión, determinar la degradación que

causarían y la probabilidad de ocurrencia.

Siempre que sea posible conviene partir de datos estándar. En el caso de desastres naturales o accidentes industriales, se puede disponer de series históricas, genéricas o del lugar en el que se ubican los equipos de nuestro sistema de información bajo estudio. Probablemente también se disponga de un historial que informe de lo que es frecuente y de lo que "no pasa nunca".

Más complicado es calificar los errores humanos; pero la experiencia permite ir aquilatando valores realistas.

Y lo más complejo es calificar los ataques deliberados pues dependen de la suerte, buena o mala.

Hay muchos motivos que agudizan el peligro de una amenaza:

- que no requiera grandes conocimientos técnicos por parte del atacante
- que no requiera gran inversión en equipo por parte del atacante[34]
- que haya un enorme beneficio económico en juego (que el atacante puede enriquecerse)
- que haya un enorme beneficio en juego (que el atacante pueda salir fuertemente beneficiado, en su estima, en su conocimiento por todo el mundo, ...); por lo que más quiera, evite los retos y jamás alardee de que su sistema de información es invulnerable: no lo es y no tiene gracia que se lo demuestren
- que haya un mal ambiente de trabajo, semilla de empleados descontentos que se vengan a través de los sistemas, simplemente para causar daño
- que haya una mala relación con los usuarios externos, que se vengan a través de nuestros sistemas

Partiendo de un valor estándar, hay que ir aumentando o disminuyendo sus calificaciones de frecuencia y degradación hasta reflejar lo más posible el caso concreto. A menudo no es evidente determinar el valor correcto y es necesario recurrir a simulaciones que orienten. El uso de algún tipo de herramienta es muy útil para estudiar las consecuencias de un cierto valor, lo que algunos autores denominan la sensibilidad del modelo a cierto dato.

Si se aprecia que los resultados cambian radicalmente ante pequeñas alteraciones de una estimación de frecuencia o degradación, hay que (1) ser realistas y (2) prestar extrema atención a por qué el sistema es tan sensible a algo tan concreto y tomar medidas orientadas a independizar el sistema; es decir, a no hacer crítica una cierta amenaza.

Recuerde que la frecuencia no afecta al impacto, por lo que estudiando el impacto se puede ajustar la degradación y, posteriormente, estudiando el riesgo se puede ajustar la frecuencia.

Nunca se debe aceptar un valor injustificado de degradación en la esperanza de compensarlo con la frecuencia, pues la estimación del impacto es importante en sí misma, además de la de riesgo.

Sea cual sea la decisión final que se tome para estimar un valor, hay que documentarla pues antes o después se pedirán explicaciones, sobre todo si como consecuencia se van a recomendar salvaguardas costosas.

Es habitual que las herramientas de soporte al análisis de riesgos aporten perfiles típicos para apoyar en esta tarea.

9.7 Para seleccionar salvaguardas

Probablemente la única forma es tirar de catálogo. Use un (sistema) experto que le ayude a ver qué solución es adecuada para cada combinación de

- tipo de activo
- amenaza a la que está expuesto
- dimensión de valor que es motivo de preocupación
- nivel de riesgo

A menudo encontrará muchas soluciones para un problema, con diferentes calidades. En estos casos debe elegir una solución proporcionada a los niveles de impacto y riesgo calculados.

Muchas salvaguardas son de bajo coste, bastando configurar adecuadamente los sistemas u organizar normativa para que el personal haga las cosas de forma adecuada. Pero algunas contra medidas son realmente costosas (en su adquisición, en su despliegue, en su mantenimiento periódico, en la formación del personal a su cargo, ...). En estos casos conviene ponderar si el coste de la salvaguarda no supera el riesgo potencial; es decir, tomar siempre decisiones de gasto que supongan un ahorro neto.

Por último, y no menos importante, a la hora de desplegar salvaguardas hay que considerar su facilidad de uso. Lo ideal es que la salvaguarda sea transparente de forma que el usuario no tenga que hacer nada o, en su defecto, cuanto menos haya que hacer, mejor. Simplemente porque una salvaguarda de complejo manejo requiere personal especializado y añade a las amenazas que ya tenía el sistema la amenaza que supone su defectuosa utilización.

9.8 Aproximaciones sucesivas

El lector ya se habrá percibido de que el análisis de riesgos puede ser muy laborioso, requiriendo tiempo y esfuerzo. Además, hay que introducir muchos elementos que no son objetivos, sino estimaciones del analista, lo que implica que haya que explicar y consensuar lo que significa cada cosa para no estar expuestos a impactos o riesgos que se ignoran o se infravaloran, ni convertir la paranoia en un dispendio de recursos injustificados.

Si hay que ser prácticos y efectivos, conviene realizar aproximaciones sucesivas. Se empieza por un análisis somero, de alto nivel, identificando rápidamente lo más crítico: activos de gran valor, vulnerabilidades manifiestas o, simplemente, recomendaciones de libro de texto porque no hay nada más prudente que aprender en cabeza ajena, aprovechando la experiencia de los demás. Este análisis de riesgos es imperfecto, evidentemente; pero cabe confiar en que lleve en la dirección correcta. Los párrafos siguientes dan indicaciones de cómo orientarse rápidamente hacia el objetivo final: tener impactos y riesgos bajo control.

Nótese que estas aproximaciones imperfectas permiten desplegar rápidamente sistemas razonablemente protegidos cuando no hay tiempo para un análisis de riesgos en toda su plenitud. Cuando, con tiempo, se llegue a la fase de gestión de riesgos tras un análisis exhaustivo, muy probablemente ocurra que muchas salvaguardas están ya dispuestas, necesitándose sólo la introducción de algunas nuevas y/o la mejora de la eficacia de las existentes. No es pues trabajo perdido seguir estas aproximaciones informales.

9.8.1 Protección básica

Es frecuente oír hablar de medidas básicas de protección *(baseline)* que deberían implantarse en todos los sistemas, salvo que se demuestre que no son pertinentes a algún caso particular.

Por favor, no discuta; ni lo dude: a sus sistemas de información no debe poder acceder cualquiera en cualquier momento. Puede protegerlos física o lógicamente, poniéndolos en una sala donde no entra cualquiera, o imponiendo una identificación de acceso lógico. Pero ¡protéjalos!

Este tipo de razonamientos se pueden aplicar con frecuencia y llevan a desplegar un mínimo de salvaguardas “de puro sentido común”. Una vez avanzado lo que es obvio y no se debería nunca discutir, se puede avanzar a niveles más elaborados, específicos de cada sistema.

Para aplicar un tratamiento básico se requiere un catálogo de salvaguardas. Existen numerosas fuentes, entre las que cabe destacar:

- normas internacionales, por ejemplo [ISO 9000]
- normas sectoriales
- normas corporativas, especialmente frecuentes en pequeñas delegaciones de grandes organizaciones

Las ventajas de protegerse por catálogo son:

- es muy rápido

- cuesta menos esfuerzo que ponerse a analizar y decidir
- se logra un nivel homogéneo con otras organizaciones parecidas

Los inconvenientes de protegerse por catálogo son:

- el sistema puede protegerse frente a amenazas que no padece, lo que supone un gasto injustificado
- el sistema puede estar inadecuadamente protegido frente a amenazas reales

En general, con la protección básica no se sabe lo que se hace y, aún estando probablemente en la senda correcta, no hay medida de si falta o si sobra. No obstante, puede ser un punto de partida útil para refinar posteriormente.

La protección por catálogo puede refinarse un poco considerando el valor y la naturaleza de los activos o cuantificando las amenazas.

En base a la tipificación de los activos

Si usted tiene datos de carácter personal calificados de nivel alto, tiene que cifrarlos.

Si usted tiene datos clasificados como confidenciales, tiene que etiquetarlos y cifrarlos.

Aparte de cumplir con la legislación y normativa específica, habrá llevado a cabo una especie de "vacunación preventiva" de activos que seguro que son importantes.

Si usted tiene una red local conectada al exterior, tiene que poner un cortafuegos en el punto de conexión.

etc.

En base al valor de los activos

Si usted tiene todos los datos operacionales en soporte informático, tiene que hacer copias de seguridad.

Si usted tiene equipos informáticos, manténgalos al día con las actualizaciones del fabricante.

Lo que vale hay que cuidarlo, por si le pasara algo, sin entrar en muchas precisiones de qué les puede pasar exactamente.

En base a las amenazas

Si se trata de un sistema de la llamada administración electrónica (tramitación administrativa no presencial) o si los sistemas se usan para comerciar electrónicamente (compras y ventas no presenciales), registre cuidadosamente quién hace qué en cada momento pues se enfrentará a incidencias con los usuarios, teniendo que determinar quién tiene razón y quien paga los perjuicios. También habrá quien quiera usar sus servicios sin tener derecho a ello (fraude).

Lo que se puede necesitar, es necesario, y parte de las responsabilidades del responsable de seguridad es disponer de la información correcta cuando haga falta.

En base a la exposición

Si usted tiene una red de equipos antiguos y se conecta a Internet, debe instalar un cortafuegos.

Si tiene usted una aplicación en producción, debe mantenerla al día aplicando mejoras y corrigiendo los defectos anunciados por el fabricante.

Cuando se sabe que los sistemas de información son vulnerables, hay que protegerlos.