

Definición de una politica de Seguridad

Tabla de Contenidos

2. Definición de una politica de seguridad.....	2
2.1 Evaluación de Riesgos.....	2
Valor intrínseco.....	3
Evaluación de costes.....	4
2.2 Estrategia de protección.....	5
La persona directamente responsable.....	7
Personas que deben utilizar el sistema.....	8
Personas relacionadas que no usan el sistema.....	9
Personas ajenas al sistema.....	11
Reparto de responsabilidad.....	14
Control de acceso.....	15
Nivel logístico.....	16



2. Definición de una política de seguridad.

La **primera regla** y la más importante es que toda política de seguridad debe de ser holística. Esto es, debe cubrir todos los aspectos relacionados con la misma. Un ejemplo lo mostrará claramente: de nada sirve poner una reja corrediza de barras de titanio de quince centímetros de grosor para proteger la entrada de un establecimiento si además no se le pone un candado para cerrarla.

Por tanto, al elaborar una política de seguridad es preciso definir todos los aspectos de la misma, sin descuidar ninguno. Idealmente deberíamos prevenir todas las eventualidades, pero en la realidad no siempre es posible.

Esta es la **segunda regla** importante: la política debe adecuarse a nuestras necesidades y recursos. Una vez más un ejemplo puede mostrarlo claro: parece evidente que habitualmente no tiene sentido adquirir una caja de caudales para proteger una piruleta chupada de fresa (1).

Se trata por tanto de valorar los costes en que podemos incurrir en caso de una catástrofe, y contrastarlos con el coste de las medidas de seguridad. Sin embargo, también aquí conviene utilizar un enfoque holístico al valorar las posibles contingencias, ya que pueden existir costes ocultos o no inmediatamente obvios que no hayamos considerado.

- Evaluación de riesgos
- Evaluación de costes
- Estrategia de protección

2.1 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 -a la postre- 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.
- **Costes 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 Vd. para saber cuánto vale. Sólo necesita asegurarse de que valora todos los costes 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
- coste del esfuerzo y materiales invertidos en obtener esos datos
- valor de la información personal que contiene
- Costes 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 costes derivados que Vd. no conozca o imagine. Podemos seguir el ejemplo anterior:

1. valor de sustituir el hardware
2. valor de sustituir el software
3. valor de los resultados
4. coste de reproducir los experimentos significativos
5. coste de regenerar la información personal

Estos parecen los costes más obvios. Pero puede haber mucho más. Por ejemplo, los resultados pueden ser públicos y tener un valor aparente nulo, pero en un entorno ultracapitalista y 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 coste - incluso para

quien originalmente la desarrolló- notoriamente elevado. Véase si no el caso de las primeras versiones del popular editor de textos EMACS.

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 coste 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 costes 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 costes

La evaluación de los costes 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 coste de la protección manteniéndolo por debajo del de los bienes protegidos maximizando el coste 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 coste asociado a intentar romperla.

Una vez más, es útil contar con la ayuda de alguien con experiencia para evaluar las medidas de seguridad: debe recordarse que una política de seguridad constituye un sistema y todas las interacciones entre sus componentes deben

ser consideradas.

La mejor forma de tener seguridad es no tener nada que proteger. Una forma de conseguirlo es impidiendo todo acceso posible a los bienes protegidos. Esta solución es válida para cajas de seguridad bancarias, en que el objetivo es limitar todo acceso entre dos puntos de tiempo. Pero este no es el caso habitual, en que se debe permitir un acceso controlado pero mantenido a los bienes protegidos y es preciso hallar un compromiso: **una política de seguridad constituye un sistema dentro de un sistema y por tanto también debe evaluarse su interacción con el entorno del que debe formar parte.**

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.** Situaciones como la de ATT acusando en un juicio a un muchacho e incluyendo en su evaluación del valor de un panfleto el de un PDP-11 (un servidor departamental de muy elevado coste) empleado para pasarlo a máquina, son cuando menos irrisorias por no decir patéticas, sobre todo considerando que el mencionado panfleto estaba a la venta al público por 25 centavos (4). Si bien los comerciales, ejecutivos, yuppies y demás fauna ajena a la materia es muy propensa a engrosar los costes 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.

2.2 Estrategia De Protección.

Es conveniente pensar al establecer una política de protección en los distintos niveles que ésta debe abarcar:

- Físico
- Humano
- Lógico
- Logístico

Todos ellos son sumamente importantes, y el prescindir de cualquiera de ellos puede resultar en funestas consecuencias.



Nivel Físico

El primer factor a considerar, y el más evidente debe ser asegurar el sustrato físico del objeto de nuestra protección. No entraremos en muchos detalles, ya que abundan las compañías de seguridad especializadas en el tema, que constituye por sí toda una disciplina. Baste notar que es preciso establecer un perímetro de seguridad a proteger, y que esta protección deberá adecuarse a la importancia de lo que queremos proteger.

Cuando menos debe asegurarse el acceso físico inmediato. Esta es siempre una necesidad primordial. En el caso de la seguridad informática, es un paradigma omnipresente. Desde las precauciones básicas para evitar que agentes dañinos afecten a un ordenador (5) hasta la protección del acceso a personas ajenas (6).

La defensa contra agentes nocivos conlleva tanto medidas proactivas (limitar el acceso) como normativas de contingencia (p. ej. que hacer en caso de incendio) o medidas de recuperación (realizar copias de seguridad). El grado de seguridad solicitado establecerá las necesidades: desde el evitar el café y el tabaco en las proximidades del ordenador y prohibir a los niños el acceso al despacho, hasta el establecimiento de sistemas de protección redundantes, control de acceso a la sala de ordenadores y mantenimiento de personal de vigilancia con equipamiento sofisticado.

Esto incluye entre otras cosas:

- condiciones medioambientales (temperatura, humedad, polvo, etc...).
- prevención de catástrofes (incendios, tormentas, cortes de fluido eléctrico, sobrecargas, tormentas, terremotos, etc...).
- limitación de acceso (llaves, control de personal, listas de acceso, etc...).
- vigilancia (cámaras, guardias jurados, etc...).
- sistemas de contingencia (extintores, fuentes de alimentación ininterrumpida, estabilizadores de corriente, fuentes de ventilación alternativa, etc...).
- sistemas de recuperación (copias de seguridad, redundancia, sistemas alternativos geográficamente separados y protegidos, etc...).
- entradas y salidas de material (elementos desechables, consumibles, material anticuado, etc...).
- interacciones entre los componentes del sistema.

Lo más importante es recordar que quien tiene acceso físico a un ordenador tiene control absoluto del mismo. Por ello sólo deberían acceder al mismo aquellas personas que sea estrictamente necesario. Y como en el caso de los costes, pueden existir ramificaciones insospechadas en este terreno, por lo que es conveniente -si la seguridad es un tema importante- consultar con un profesional.

Nivel Humano

Con las últimas consideraciones hemos empezado a entrar en un terreno nuevo y altamente arriesgado: los seres humanos implicados en la seguridad del sistema. De ellos no basta considerar sólo su relación con el mismo, sino también todos sus aspectos personales, humanos y psicológicos así como sus posibles motivaciones en su interacción.

En este área podemos considerar varios sub-niveles:

- el administrador o responsable directo del sistema
- las personas que deben tener acceso al sistema como usuarios del mismo
- las personas relacionadas con el mismo pero que no necesitan usarlo
- las personas ajenas al sistema

Veamos cada caso por separado:

La persona directamente responsable

Esta persona debe tener acceso directo al sistema ya que el buen estado del mismo depende de ello. En principio **debería ser la única persona con acceso**, y si es preciso, debería haber más de uno para cubrir emergencias (gripe, vacaciones, etc...). Dentro de su área **debe tener un control absoluto** ya que es quien asume la responsabilidad última de su funcionamiento, sin éste no la puede asumir y, en cualquier caso, si tiene acceso físico el control absoluto no se le puede quitar.

Debe recordarse que esta persona tiene acceso físico y los conocimientos precisos, y por tanto control absoluto irremisible, lo que supone que debe ser una persona equilibrada y de la máxima confianza, con todo lo que ello conlleva. La ley exige de esta persona el secreto profesional, lo que es una garantía más. Además, al tener control absoluto debe ser el responsable último de una parte importante de su seguridad.

Es por tanto fundamental asegurar a esta persona tan bien como se asegure el resto del sistema: de nada sirve disponer el sistema más sofisticado si esta persona puede fallar en cualquier momento. La única forma de conseguirlo es cultivando su fidelidad, tanto mediante recompensas como penalizaciones adecuadas y proporcionadas al valor de los bienes que custodia. No hacerlo así es como poner un zorro a guardar gallinas: un salario insuficiente o inapropiado y una penalización insuficientes le harán más susceptible al chantaje o al soborno, mientras que unas penalizaciones excesivas pueden llevar a la desesperación y pérdida del miedo a las consecuencias o a un nerviosismo artificioso que disminuya su capacidad.

Es frecuente observar sitios donde se establece una vigilancia férrea de éstas personas, sometiéndolas a

escrutinios exhaustivos todos los días. Este es uno de los errores más comunes a evitar: olvidar el factor humano. Estos escrutinios son inútiles por cuanto no impiden que la información más importante, que está en la cabeza de las personas, entre y salga libremente, y además minan la confianza de las personas destruyendo su lealtad, facilitando así la generación de brechas en la línea de seguridad.

Es posible reducir nominalmente la responsabilidad de estas personas transfiriéndola a otras distintas que la asuman, normalmente sus jefes, reduciendo aparentemente la necesidad de cultivarlas. Pero esta es una transferencia ficticia: todo el que tiene acceso físico al ordenador tiene en última instancia control absoluto, y este traslado una vez más refleja una falta de confianza notoria que rompe de nuevo la necesaria relación de confianza y fidelidad, masacrando una vez más el sistema de seguridad.

Personas que deben utilizar el sistema

Como decíamos más arriba, la mejor seguridad es eliminar todo acceso, pero este no es el caso habitual, que exige que muchas personas puedan acceder a los recursos protegidos.

En principio, nadie más que el administrador del sistema debería tener acceso físico al mismo. Esto no siempre es factible, y cuando sea así, debe considerarse a toda persona que tenga acceso como si fuera un administrador más, con las mismas responsabilidades de seguridad y las mismas capacidades (véase epígrafe anterior). Un error común es creer que la categoría oficial de una persona refleja sus capacidades y las de todas las personas con las que se relaciona. Este enfoque clasista y decimonónico ignora la capacidad del ingenio humano, las posibilidades del afán de superación y la eventualidad de que alguien se relacione con personas que no son de su clase (9, 10).

Para evitar tener que dar la posibilidad de un control absoluto a muchas personas, la solución generalmente usada es establecer sistemas de acceso parciales con menores requisitos de seguridad. En este caso, los usuarios siguen teniendo control absoluto sobre su sistema, pero la responsabilidad y valor del sistema al que tienen acceso es mucho menor, disminuyendo la repercusión de un eventual compromiso y la importancia de la responsabilidad con la que tienen que cargar.

Casa con dos puertas mala es de guardar. Esta es la máxima más importante a considerar en estos casos: con el fin de limitar el acceso físico al sistema central estamos creando nuevos puntos de entrada, multiplicando el número de puertas del mismo y generando posibles agujeros en nuestro perímetro de seguridad. Es por ello importante comprobar que todas y cada una de ellas está debidamente asegurada, es necesaria, y que no sacrifica la seguridad global más allá de lo necesario.

En este sentido se deben establecer distintos niveles de importancia de los usuarios en base al grado en que comprometen la seguridad, tratando a cada uno de ellos correspondientemente. Es también imprescindible que todos ellos sean conscientes del grado en que son responsables de la seguridad del sistema, hasta qué punto pueden comprometerla y cuál es su grado de responsabilidad. Nadie que no esté dispuesto o pueda asumir esa responsabilidad debería tener acceso al sistema bajo ningún concepto.

Según esto, serían responsables de sistemas con responsabilidad limitada a la parte del sistema a que tienen acceso.

Un ejemplo puede aclarar estos puntos: en las oficinas de administración la persona responsable puede tener acceso a todos los datos administrativos, mientras que los administrativos y secretarías solamente deben acceder a una parte de esa información. Ocasionalmente, puede ser preciso más personal y emplear a personal eventual. Bien, en un entorno tal, es tristemente frecuente que el personal eventual se contrate deprisa y corriendo, sin control ni garantías. El jefe de personal no debería compartir sus privilegios de acceso con los demás, y bajo ningún concepto con el personal eventual. Sin embargo, es tristemente famoso el caso de los Servicios Secretos británicos, en que por dejadez o desidia, muchos miembros del personal oficial tenían anotadas sus claves de acceso en sitios visibles, permitiendo que durante un traslado en que hubo que contratar personal temporal cualquiera pudiera acceder a información de alto secreto.

Personas relacionadas que no usan el sistema

Básicamente, estas se dividen en dos ramas: el **personal ejecutivo** de rango superior que delega en personal subordinado las tareas de trabajar con el ordenador y el personal de mantenimiento general.

Respecto al **personal ejecutivo de rango medio** en mi opinión, bajo ningún concepto debería acceder al sistema nadie que no lo necesite de forma imprescindible, incluyendo especialmente al personal ejecutivo. Estas son personas que no lo precisan, y por tanto su acceso supone una ruptura seria de seguridad. Sin embargo, siendo como son las tecnologías de la información un tema de moda y a menudo caro, es inevitable que despierten la curiosidad, el orgullo y la vanidad, dando lugar a que todo el mundo quiera ver la máquina, mostrarla, presumir de ella o simplemente mostrar su poder, ascendiente y estatus paseando libremente por sus señoríos. Este es un problema importante cuando se trata del personal ejecutivo, dado que al tener un rango superior pueden poner en un apuro a las personas encargadas de la seguridad forzando una nueva brecha.

Si el responsable de seguridad no puede detener estas incursiones entonces el sistema de seguridad es inaceptable, ya que bajo la arrogancia disfrazada de inocencia pueden ocultarse designios nefastos que burlen así (regodeo, mofa y befa) todo el sistema.

Lo que esto implica es que nadie de rango superior debería acceder al sistema a menos que esté en condiciones de asumir la responsabilidad de su compromiso y lo haga formalmente: es obvio que el propietario de la empresa puede asumir esa responsabilidad, pero sería estúpido por parte del responsable de la seguridad permitírsele sin dejar constancia de cuanto haga y sin que la asuma formalmente primero. Entre otras cosas porque al final la responsabilidad será del responsable de seguridad si así no lo hace y es una situación muy tentadora incluso para el propietario el poder aporvecharse de la descarga en otro de esa responsabilidad.

Son las personas de rangos superiores, pero que no pueden o no quieren asumir esa responsabilidad muy probablemente el principal agujero de seguridad en todos los sistemas. Para solucionarlo es preciso eliminar su

ascendencia sobre el personal de seguridad, lo que exige un compromiso serio por parte del personal del más alto nivel.

Un consejo para todo responsable de seguridad es que se nieguen bajo ningún concepto a trabajar o asumir ninguna responsabilidad en entornos donde ejecutivos de rango medio puedan tener ningún ascendiente sobre ellos, sea éste cual sea.

La forma de establecer esta independencia puede variar según el entorno:

- El responsable de seguridad podría poseer un rango superior a cualquier persona que no pueda o deba sobrepasar sus funciones.
- Puede establecerse una jerarquía paralela completamente separada para el personal de seguridad (tratándolo como una entidad independiente).
- Puede establecerse un protocolo de acceso y vigilancia del personal de rango medio.
- Se puede establecer un filtro independiente a nivel físico (por ejemplo control de acceso por una empresa independiente).
- Se puede separar el entorno protegido del rango de acción de los mandos medios.

De estas soluciones sólo las dos primeras son recomendables. En la medida en que pueda existir alguna dependencia del personal de seguridad respecto a personal ejecutivo que no debe o puede sobrepasar sus funciones todo el sistema es inútil. Una persona interesada siempre puede encontrar un modo directo o indirecto de forzar a un subordinado a realizar cualquier tarea que desee, y así superar las barreras de seguridad. Esto además libera una nube de humo de falsa seguridad al poner el agujero en un eslabón oculto y aparentemente no relacionado.

La última solución, separar el entorno protegido, es posiblemente un buen paliativo: uno de los trucos más útiles que siempre conviene recordar es intentar poner -si es posible- unos buenos ventanales que den al sistema central. Esto no sólo facilita su vigilancia, también permite su supervisión a mandos medios reduciendo su sensación de inseguridad, y facilita la realización de visitas guiadas sin acceso real para quienes deseen presumir ante los invitados, eliminando así las excusas más frecuentes para exigir el acceso. Aunque sigue siendo necesario contar con el apoyo del personal de alto nivel frente a posibles interferencias.

Respecto al **personal de mantenimiento** general, es importante tenerlos en cuenta: suelen ser personas con quien estamos tan familiarizados que casi siempre se ignora su existencia. Su labor puede parecer o ser incluso imprescindible, especialmente por cuanto comporta de molesta. Su acceso al perímetro protegido debería ser lo más restringido posible y sólo autorizarse si es necesario.

En estas personas confluyen además circunstancias especiales: por un lado suelen ser personas no técnicas, no relacionadas con los equipos, y por tanto es más probable que cometan errores comprensibles en su interacción con ellos. Por otro lado, el que no se les exija cualificaciones relacionadas para desempeñar su trabajo no quiere decir

que no puedan poseerlas. Por ello, si deben acceder al sistema, es recomendable que lo hagan bajo supervisión por la persona responsable.

Esta responsabilidad debe hacerse extensiva a los demás usuarios en la medida en que también son responsables parciales de una parcela de la seguridad global del sistema: como vigilantes de su puerta de entrada deben supervisar que la misma no pueda resultar dañada o comprometida por nadie, y si alguien distinto debe acceder a su terminal, conviene que se aseguren de que no puede comprometerlo.

Una característica de este tipo de personas es que a menudo su función es considerada como de un rango inferior por el resto del personal. Ello a menudo les convierte en objeto de iras injustificadas y malos tratos, casi siempre irracionales, por parte del otro personal. Este es un serio peligro psicológico a evitar: su función habitualmente les da también acceso a casi todos los rincones del centro de trabajo, y como decíamos tienden a ser ignorados y pasar desapercibidos con gran facilidad. Si a esto sumamos las escasas responsabilidades que tienen que asumir (y se les pueden exigir) y la siempre plausible excusa de la ignorancia, nos encontramos con un elemento para quien romper la seguridad es sumamente fácil, las exigencias de responsabilidad son casi nulas, la motivación es fuerte y la excusa inmediata.

En conclusión, no debemos olvidar nunca la naturaleza humana, ni dejar de tratar a nuestros semejantes con humanidad.

Personas ajenas al sistema

En principio, estas personas deberían ser tratadas siempre como elementos intrusos y probablemente agresivos, lo que no debe impedir el que se les trate con la debida cortesía y guarde el respeto en todo momento.

Volviendo al principio general de que nadie que no lo precise debe acceder al sistema, estas personas nunca deberían acceder. De hecho, son estas personas la justificación de la existencia de todo el sistema de seguridad. Sin embargo pueden existir circunstancias especiales.

Una de tales circunstancias es la anteriormente mencionada situación en que se desea mostrar el sistema de protección por motivos psicológicos (orgullo) o políticos a alguien ajeno. En la medida de lo posible, debería restringirse este tipo de accesos, pero si son inevitables, nunca deberían autorizarse sin el consentimiento formal de alguna persona con un grado de responsabilidad y compromiso con el sistema de seguridad que lo garantice. La visita deberá ser siempre guiada y el visitante deberá ser sometido durante la misma a un férreo pero discretísimo marcaje para asegurar que en ningún momento la seguridad resulte comprometida.

Una alternativa honorable en ocasiones puede ser el establecer una sala alternativa de demostración, ocultando la sala real. Esta podría consistir simplemente en ordenadores viejos que adicionalmente son más grandes, ruidosos, tienen más lucecitas y son más impresionantes. Si el visitante no es técnico puede resultar suficiente e incluso más

productivo, sirviendo al objetivo sin dañar la seguridad.

Como de costumbre, es importante considerar todos los aspectos humanos implicados en estas personas: sus motivos para acceder, justificados o no, pueden surgir por múltiples razones, y el análisis de las mismas puede arrojar diáfana luz sobre las necesidades de seguridad y las soluciones más apropiadas. De hecho, éste es el abordaje mas efectivo y seguro para la protección de cualquier objeto, y a menudo también el más barato -si bien en ocasiones también puede ser insosteniblemente costoso.

En todo caso, sin un análisis detallado de las personas de quienes nos queremos proteger y de sus interacciones con nosotros, el entorno, y el resto de personas implicadas, es muy difícil, si no imposible, desarrollar estrategias defensivas efectivas. Ya hemos visto algunos ejemplos en los epígrafes anteriores. Veamos alguno más:

Durante la década de los 80 y primeros de los 90 (s. xx) surgió un gran número de penetradores de sistemas en las universidades. El problema surgía en muchos casos debido a estudiantes que deseaban acceder a más recursos de computación, aprender más cosas de las que se les enseñaba en clase, o acceder a nuevas tecnologías que eran fundamentales para su carrera pero les eran denegadas. El problema se recrudecía con la presencia de muchos profesores y administradores de sistemas (en la Universidad y empresas) que o bien desconocían las tecnologías que manejaban -y no querían que se notara- o bien deseaban mantener una sensación de alto sacerdocio elitista de la tecnología. Adicionalmente, el compromiso (en Universidad y empresas) del personal directivo con el mantenimiento de los equipos y la seguridad era escaso, dando lugar a que los recursos de contención fueran insuficientes. En tales circunstancias los estudiantes tenían la ventaja de disponer de un tiempo y tesón del que los responsables de seguridad carecían y constantemente penetraban los sistemas, a menudo generando problemas por su falta de conocimiento. Como reacción muchos administradores desarrollaron un miedo cerval y casi místico a los mismos, aunque usaran técnicas a menudo simples y primitivas. El miedo cerval generó medidas mas restrictivas, forzando a los estudiantes emprendedores a buscar caminos mas sofisticados y generando una peligrosa espiral.

En esta historia es posible detectar varios problemas: si los estudiantes hubieran dispuesto de un medio de satisfacer su curiosidad y hubieran podido acceder a las tecnologías que necesitaban y les eran negadas, muchos de ellos -la inmensa mayoría- no sólo no hubieran recurrido a penetrar sistemas de seguridad, también habrían estado mucho más ocupados en explorar aquellas que en buscar problemas. Es interesante también observar que los motivos pueden no siempre ser meramente económicos o nocivos, y basarse en algo tan básico como la curiosidad.

Más interesante aún es analizar las medidas de contención: claramente insuficientes, no podían desarrollarse debido a la falta de apoyo por el personal directivo. Y la ignorancia y sobrecarga de trabajo degeneraron en conductas supersticiosas, y en medidas más restrictivas de lo preciso. El resultado fué en conjunto peor para todos y la causa fué fundamentalmente psicológica.

De aquí podemos derivar otra conclusión importante: **aprendamos de nuestros errores.**

La otra cara de la moneda es la segunda mitad de los 90 (s. xx) en que la disponibilidad de sistemas operativos

avanzados de dominio público permitió el acceso a entornos profesionales, avanzados y sofisticados a toda persona interesada, y las limitaciones de acceso a tecnologías de comunicaciones se eliminaron casi totalmente: esto redujo la necesidad de explorar, y dio acceso a problemas complejos e interesantes en que invertir el tiempo, proporcionando objetivos constructivos. Sin embargo, y como contrapartida, los medios de comunicación de masas habían hincado el diente en el filón de la seguridad, promoviendo una falsa imagen mitificada del penetrador como un héroe romántico promoviendo los ataques destructivos como un fin en sí mismo que convertía automáticamente al perpetrador de los mismos en un mito objeto de la admiración de sus amigos e ídolo indiscutible del sexo contrario. Como resultado lógico la penetración de sistemas se convirtió en un objetivo por sí misma, sin justificación, irracional.

Una lectura interesante de esta situación es observar la necesidad del tratamiento holístico del problema: un análisis reducido que no considere la terrible influencia social ejercida por medios de comunicación de masas irresponsables no podría identificar la raíz del problema. Nos sirve también para ver como un abordaje tardío a la solución de un problema -la curiosidad y deseo de aprendizaje- puede llegar cuando este ya ha degenerado en un problema intratable -la presión social- por ser demasiado tarde.

Es decir, no hay que dormirse en los laureles ni dejar las cosas para mañana.

Nivel Lógico

Este nivel incluye las medidas de acceso y políticas de empleo de los recursos protegidos, así como la distribución de la responsabilidad correspondiente a las personas con responsabilidades parciales.

Este nivel es preciso en todos los entornos donde se debe proteger un recurso al que deben acceder muchas personas. Por ejemplo, un edificio de oficinas no puede permanecer cerrado: se pueden establecer privilegios de acceso, permitiendo a algunas personas un acceso total, a otras acceso a zonas sensibles, a empleados normales sólo a oficinas, y a visitantes sólo al área de recepción. Cada persona puede disponer de una llave o juego de llaves especial y será responsable de ellas, pudiendo comprometer aquellas zonas a las que tiene acceso.

Una política de distribución de los privilegios de acceso adecuada puede asegurar que cada persona acceda y pueda comprometer solamente aquellas áreas que sean imprescindibles.

El establecimiento de políticas de acceso y reparto de la responsabilidad a este nivel es muy importante por cuanto va a definir las necesidades informáticas de seguridad. Podemos centrarnos en dos aspectos fundamentales:

- Reparto de responsabilidad.

- Control de acceso.

Reparto de responsabilidad

El primer aspecto a decidir es cómo se va a repartir la responsabilidad en el acceso a los recursos, es decir, qué personas van a tener acceso, y en qué medida.

Se pueden establecer varias categorías en cuanto a las políticas más comunes, véase por ejemplo la documentación de seguridad informática del arco iris (14).

- Todo el mundo tiene acceso a todo.
- Dos niveles de acceso: privilegiado y normal.
- Varios niveles de acceso.

El primer caso es desgraciadamente uno de los mas comunmente utilizados, a menudo incluso involuntariamente. Es el caso, por ejemplo de una tienda pequeña en que todos los empleados tienen la llave, o el de un grupo de trabajo que comparte todos los recursos por igual entre todos los usuarios. Todos los usuarios tienen acceso al sistema con todos los privilegios y son por tanto administradores del mismo con poder absoluto sobre él. No hace falta decir que éste es el sistema menos seguro y más peligroso y que hay que intentar evitarlo siempre que sea posible.

En el segundo caso, una persona o grupo de personas tienen acceso absoluto, mientras que el resto de personas sólo puede acceder a un conjunto limitado de recursos determinado por los administradores con privilegios. En este caso, el riesgo máximo reside en las personas con acceso privilegiado y conviene reducir el número de las mismas al mínimo. Sin embargo, también existe un riesgo asociado a los usuarios normales, éste directamente proporcional al espectro de recursos al que tienen acceso y que pueden controlar. Es muy importante pues en este caso disponer de administradores cualificados que definan cuidadosamente a qué recursos acceden los usuarios y verifiquen que no puedan tener acceso a nada que no sea estrictamente necesario.

Finalmente, en ocasiones el problema puede ser complejo, siendo necesario disponer de varios niveles jerárquicos: por ejemplo, en una empresa el jefe de un departamento podría tener privilegios para decidir qué miembros de su departamento tendrán llave del mismo, pero no podrá proporcionar acceso a todo el edificio. Podrían establecerse así varios niveles de delegación de la responsabilidad. En éste caso, cada persona es administradora de un dominio de seguridad, asumiendo la responsabilidad del mismo y tomando parte en la responsabilidad total de manera proporcional a la importancia del dominio que controla.

El problema con cada uno de estos enfoques es que a medida que se intenta obtener un control más fino es preciso usar sistemas más complejos, disponer de una mayor cantidad de personal debidamente formado, y que la evaluación del grado de responsabilidad de cada persona se dificulta consecuentemente. Una consecuencia de este

problema es que proliferan los sistemas de seguridad inapropiados al ser difícil evaluar hasta qué punto un sistema se adecúa al modelo y necesidades que uno ha definido.

Por eso es muy importante elegir con sumo cuidado el sistema sobre el que se va a implementar la seguridad de un Centro. Especialmente, es importante escapar a las trampas que tienden muchos comerciales y a las técnicas agresivas de marketing: la seguridad es un tema candente y muchos vendedores se encuentran con un tema para el que no están preparados, pero no quieren perder ventas ni retrasarlas, por lo que a menudo recurren a medias verdades y a comparaciones y juegos de palabras engañosas. Por ejemplo: un famoso vendedor de software comercializa un producto que define como catalogado para un nivel dado de seguridad, pero omite indicar que la certificación se obtuvo para un sistema aislado, dejando al comprador creer que también es válido en un entorno de red: ellos no engañan a nadie, pero usan una terminología incompleta y omiten información para que el comprador pueda sacar conclusiones erróneas (e incidentalmente beneficiosas para el vendedor).

Es muy importante huir de comparaciones genéricas del tipo es como una máquina tipo X (p. ej. Unix) que omiten aclarar que hay muchas variedades de ese tipo o familia, y confían en una comparación vaga para aparentar mayor seguridad de la que ofrecen en realidad.

Y también es crucial evitar como al demonio a quienes ofrecen bajo términos genéricos sistemas derivados de otro pretendiendo aparentar que esa derivación es una mejora sin detallarla. Por ejemplo, hay un sistema que se vende como derivado de VMS (un sistema clásicamente conocido por su sólida seguridad) dando a entender que es un VMS mejorado y por tanto más seguro, cuando en realidad es un sistema distinto que incorpora algunas ligeras nociones del original, mucho más simple y menos poderoso, y desde luego infinitamente menos seguro .

En cualquier caso, una vez decidido cómo se va a repartir el acceso y responsabilidad sobre los dominios de seguridad, es relativamente fácil -si uno no se deja engatusar por vendedores ávidos de beneficios- elegir un sistema adecuado para la política elegida. Una buena ayuda a la hora de determinar las especificaciones técnicas del equipo necesario la constituyen las llamadas guías del arco iris, en especial el libro naranja disponibles en la red.

La recomendación más importante que puede hacerse en este capítulo es leer estas guías, y usarlas al determinar el sistema de seguridad más adecuado, pero no limitándose a pedir una catalogación determinada -que es donde más a menudo se usan técnicas engañosas- sino revisando paso a paso todos los detalles del nivel elegido para verificar que realmente los cumple hasta el final y a satisfacción de nuestras necesidades.

Control de acceso

Una vez definida la forma en que se va a distribuir la responsabilidad el siguiente paso es definir de qué forma se va a implementar la misma, y qué ambitos se deberán controlar.

La delegación de autoridad puede hacerse en muchas formas, y es preciso decidir cuál de ellas es la más apropiada, definiendo a qué dominios de información accede cada persona sobre la que se ha delegado

responsabilidad y cómo se controla el que cada una de ellas no pueda acceder a nada fuera de su dominio.

En ese sentido se pueden distinguir varias estrategias básicas:

- Delegación absoluta para un ámbito geográfico limitado.
- Delegación de un área de responsabilidad funcional.
- Mezclas de las dos anteriores.

Para entenderlo mejor podemos usar unas analogías: la delegación geográfica es similar a una empresa organizada por sucursales, donde cada sucursal es relativamente autónoma, y gestiona todos los aspectos de seguridad de su área de influencia, mientras que la delegación funcional sería como una factoría en que cada departamento asume responsabilidad sobre una parcela determinada del proceso de generación del producto final. Finalmente, podrían darse casos mixtos, como podría ser una Universidad que delega la responsabilidad de la seguridad de cada facultad sobre un Centro de Cálculo local en que cada persona se encarga de un aspecto de la misma (p. ej. una persona podría ser responsable de seguridad en red de una facultad).

Obviamente, el sistema más cómodo para delegar es el primero, ya que requiere un mínimo de configuración, lo justo para definir parcelas aisladas y que funcionan autónomamente. El problema es que puede dar demasiada autonomía a una persona o entidad que no debería tenerla. Además favorece la proliferación de políticas locales de seguridad que pueden ser conflictivas o contradictorias.

Una parcelación funcional requiere una disección minuciosa y un conocimiento detallado del sistema para definir compartimentos funcionales estancos y asignar privilegios en un área sin comprometer otras. Por otro lado, favorece la dispersión de una política común, aunque requiere un mayor esfuerzo de coordinación para mantener la armonía del sistema.

Los enfoques mixtos son los más versátiles, y bien manejados pueden ser los mas poderosos facilitando una división jerárquica de la responsabilidad administrativa, pero también requieren un mayor esfuerzo de configuración y coordinación para evitar que acaben convirtiéndose -con gran facilidad- en un monstruo anárquico, desorganizado e incontrolable.

Nivel logístico

Como hemos ido viendo, el problema de establecer cuál es la mejor forma de proteger algo es relativamente complejo. Un tratamiento adecuado debe no sólo tratar todos sus aspectos individuales, sino también considerar las interacciones entre sus elementos y la coordinación de los mismos. La forma de hacerlo es mediante el establecimiento de protocolos de trabajo y políticas comunes para coordinar la labor.

Esta labor logística de coordinación de todos los elementos involucrados para generar un sistema armónico es fundamental para el buen funcionamiento final del sistema, y debe también adecuarse a las necesidades existentes

para no resultar en un sistema demasiado laxo para mantener la seguridad necesaria ni en un tan rígido que dificulte el funcionamiento normal del trabajo.

Elaborar una política de coordinación de recursos es una tarea que no debe tomarse a la ligera: requiere un estudio detallado del sistema global que tenga en cuenta aspectos como, entre otros:

- El sustrato físico del sistema.
- La dinámica laboral.
- La dinámica de grupos de personal.
- Las necesidades físicas de los usuarios.
- Las necesidades psicológicas.
- El grado de formación de las personas implicadas.
- El grado de implicación en el complejo de seguridad.
- El entorno externo del que nos queremos proteger.

No entraremos en detalles de todos ellos y de las interacciones de cada posible presentación de cada aspecto con las demás ya que ello resultaría bastante complejo. Nos limitaremos en cambio a presentar algunos ejemplos de cada aspecto para mostrar en qué manera pueden influir en la concepción global, dejando su integración final como un ejercicio para el lector. De cualquier manera, también aquí conviene recordar que la mejor receta es una buena dosis de sentido común si bien, al final, la elaboración definitiva de una estrategia ajustada es todavía en buena medida una cuestión de arte.

El sustrato físico es el primer factor que salta a la vista: un entorno reducido a un despacho puede arreglarse con un sistema de aislamiento local, podrá aprovechar la proximidad para establecer comunicaciones orales y personales rápidas, y podrá cargar bastante peso en las relaciones interpersonales.

En cambio, una entidad que se expanda por una amplia área geográfica deberá considerar además problemas derivados de establecer una red de comunicaciones ancha, donde los contactos personales son escasos, a través de la red, y no se puede depositar confianza personal en alguien a quien no se conoce, por lo que será importante establecer directrices generales y distribuirlas, así como métodos de verificación de su cumplimiento. Además, habrá que considerar no sólo la protección de los sistemas diana, sino también de toda la infraestructura de comunicaciones.

Independientemente del ámbito físico, la dinámica laboral impone sus restricciones: un ambiente relajado puede permitir un mayor cuidado de los detalles, y definir normas de índole genérica confiando en que en caso de necesidad se dispondrá de tiempo suficiente para reaccionar y analizar la situación para elegir la respuesta adecuada.

Sin embargo, un entorno de producción frenética no puede permitirse el lujo de retrasar las consideraciones hasta el momento de tratar con los problemas, y exige una serie de normas estrictas y muy bien delimitadas que no dejen lugar alguno a la duda o la indecisión. El tiempo de respuesta es crucial, por lo que deben establecerse políticas

de redundancia y eficiencia que aseguren la máxima eficacia al tratar las emergencias.

La dinámica de grupos es también importante por cuanto define en qué medida y de qué se puede delegar la responsabilidad. También define las vías de comunicación disponibles para distribuir la información y notificar la aparición de problemas. Esto nos identifica además puntos sensibles en la cadena de control. Si el sistema no se ajusta, pueden generarse serios problemas y dilaciones que inhabiliten el sistema de seguridad. Por ejemplo, en una topología de estrella el nodo central (podría ser la oficina de notificación de problemas) soporta todo el peso de las comunicaciones, y requeriría recursos apropiados para su sobrecarga, pero también permitirá un sistema de control centralizado. En cambio una ramificación jerárquica o lineal con muchos escalones puede funcionar con menos personal de coordinación, y los retrasos en transmitir problemas o decisiones a lo largo de las cadenas aconsejan una mayor dispersión de la responsabilidad para acercarla a los puntos problemáticos y mejorar el tiempo de respuesta.

Algo similar sucede con las necesidades físicas de los usuarios: estas definen límites a lo que se puede realizar: en un entorno escaso de espacio no se pueden introducir soluciones muy sofisticadas, o varios tomos de manuales de seguridad. Un ambiente tropical necesitará ventanas por si falla el aire acondicionado, y si hay ventanas se pueden forzar o quedar abiertas. Y un ambiente gélido puede imponer otras limitaciones (vease la nota 8) que deben considerarse. Un entorno abierto (como una oficina de recepción o información) requerirá mayores precauciones y de un tipo distinto que un entorno claustrofóbico e inaccesible.

Respecto a las necesidades psicológicas individuales, se trata de un problema distinto al de las interacciones de grupos: en ciertos ambientes (como las oficinas de desarrollo donde se hace un trabajo creativo) no se pueden forzar horarios y se necesita una sensación de libertad, que exigen una menor carga de responsabilidad sobre el usuario, así como una vigilancia más laxa y mayor permisividad de horarios: un intento de acceso fallido de un programador trasnochador no puede valorarse igual que el ocurrido en una oficina donde nadie trabaja fuera de horarios. En un caso es una ocurrencia normal, y en el otro un aviso serio de un posible problema.

Por otro lado hay entornos donde es crucial el mantener una sensación de vigilancia constante para asegurar el correcto comportamiento de usuarios agresivos o potencialmente peligrosos (como podría ser un grupo de personal contratado temporalmente para realizar tareas potencialmente sensibles).

Con eso y todo, sigue siendo preciso descansar cierto grado de responsabilidad sobre algunas personas que necesitarán el conocimiento técnico preciso. El grado en que podemos delegar la responsabilidad por tanto depende sobremedida de el grado en que podamos confiar en dichas personas para realizar correctamente las tareas a encomendar. Así sería absurdo, por mucho que la organización de la empresa favorezca la descentralización de la responsabilidad el transferirla a personas o grupos carentes de los conocimientos necesarios. En tales circunstancias puede ser preferible asumir una relativa ineficacia en la transmisión de información a delegar actividades sensibles que serán mal desempeñadas. A veces se puede desarrollar una estrategia que contemple la formación de las personas implicadas, en especial si la dinámica laboral no impone grandes presiones. Pero también puede suceder que esta no permita a nadie dejar sus obligaciones para aprender. Este factor, la formación, influencia claramente pues hasta que

punto otros se pueden considerar.

El grado de implicación, que hemos dejado para el final, es probablemente el más importante: de nada sirven la mayoría de las estrategias si las personas implicadas no están dispuestas a asumir su responsabilidad, o si no se les puede exigir que lo hagan. Así en un entorno involucrado, será mas fácil confiar en que las personas hagan su parte, estén dispuestas a aprender y a colaborar. Lo que no quiere decir que vayan a poder hacerlo o tener el tiempo preciso, o que las condiciones vayan a permitirlo: por ejemplo, con personal interesado, geográficamente próximo, y con una dinámica laboral que permita dedicar el tiempo necesario, se podría plantear trasladar a un grupo de especialistas que eduquen a los usuarios, pero si el sistema exige una producción ininterrumpida, o la distancia es muy grande, tal vez sea preferible desplazar a algunos usuarios a un punto central para formarlos allí y que luego transmitan los conocimientos recién adquiridos localmente.

La otra cara de la moneda es, como indicamos, un grupo de usuarios poco concienciado: en estos casos la política debe dejar menor libertad y delegar menor confianza, y debería incluir, además de la formación técnica necesaria, programas agresivos de concienciación de los usuarios, que deberán adecuarse a los demás aspectos mencionados. En el peor de los casos puede ser preciso llegar a imponer frecuentes cambios de claves de acceso, limitaciones draconianas en las acciones permitidas, supervisión continua y detallada de toda acción posiblemente conflictiva, vigilancia estricta, verificación proactiva de toda actividad sensible (p. ej. preselección de claves), etc...

Todo ello, como es natural, sin dejar de evaluar, en todos los casos, el grado de presión externa al que estamos sometidos por los posibles atacantes. Por ejemplo, aun en un entorno escasamente motivado, puede ser innecesario establecer las medidas draconianas mencionadas si el interés externo por el mismo es anecdótico, en cuyo caso estas medidas serán mas una molestia innecesaria que una necesidad. Y en cambio, incluso en un entorno cerrado, muy limitado, con un grupo coherente de profesionales altamente cualificados y concienciados, puede ser preciso llegar a estrategias altamente restrictivas si el objeto de la protección es suficientemente precioso como para que haya una presión constante de ataques metódicos, determinados y fuertemente agresivos.

Con estos últimos ejemplos hemos ido viendo también hasta qué punto están unos y otros imbricados y porqué es tan importante no descuidar ningún aspecto ni las interacciones entre ellos. Para concluir podemos decir que hay tantas estrategias como posibles necesidades, oscilando desde las más laxas en entornos acogedores, controlados, concienciados y bien formados a las más fascistas en entornos descuidados, ignorantes, dispersos y sometidos a fuertes ataques externos.

En resumen, todo se reduce, como decíamos al principio, a emplear un enfoque holístico, que no descuide ning n detalle y se adapte a las necesidades y circunstancias del entorno en que ha de desenvolverse. Todo ello sazonado con una buena dosis de sentido com n, experiencia y sensibilidad est tica constituye la receta fundamental para la elaboraci n de una pol tica apropiada de seguridad para cualquier entorno.

