Auditoría Pública nº 61 (2013), pp. 111 - 117

NUEVAS TECNOLOGÍAS

Ángel Carrasco Núñez
Técnico de sistemas y seguridad
Servicio de Informática
Cámara de Cuentas de Andalucía

Conceptos de seguridad informática y su reflejo en la Cámara de Cuentas de Andalucía

RESUMEN/ABSTRACT:

El objetivo de este artículo es explicar los conceptos en los que se basa la capa técnica de la gestión de la seguridad informática de la forma más asequible posible. De esta manera, se podrán entender mejor las ventajas de invertir en ella, así como, el proceso de su aplicación junto con sus implicaciones, tanto para el implantador como para los usuarios a los que va destinada.

La gestión de la seguridad informática tiene otros aspectos como la aplicación o la adecuación a la normativa como la ISO 27000, etc. que no son objeto de este artículo.

Lejos de ser un artículo académico, se trata de una reflexión personal basada en mis quince años de experiencia profesional, en mi participación en asociaciones relacionadas con esta rama de las tecnologías de la información como ISMS Forum y además en estar certificado en hacking ético –C|EH- de EC-Council.

The objective of this article is to explain the concepts on which the technical layer of information security management is based in the most accessible way possible. As such, the advantages of investing in it may become better understood, as well as the application process along with its implications, both for the implementer and the users to whom it is targeted.

Information security management has other aspects such as the application or adaptation to legislation such as ISO 27000, etc., which are not the object of this article.

Far from being an academic article, it is a personal reflection based on my fifteen years of professional experience, my participation in associations related to this branch of information technologies such as ISMS Forum and also on account of my CEH certificate in ethical hacking from the EC-Council.

PALABRAS CLAVE/KEYWORDS:

SEGURIDAD, AMENAZA, VULNERABILIDAD, RIESGO, GESTIÓN DE SEGURIDAD
SECURITY, THREAT, VULNERABILITY, RISK, SECURITY MANAGEMENT

I. INTRODUCCIÓN

En los últimos años está habiendo una creciente preocupación por la seguridad de los activos informáticos, en todos los ámbitos y organizaciones, tanto públicas como privadas e incluso en el usuario particular. Este interés ha sido catalizado por:

- Los numerosos ataques informáticos, en donde los atacantes han obtenido datos confidenciales que han supuesto costosas pérdidas económicas, legales y de imagen.
- Las legislaciones nacionales e internacionales, como el Esquema Nacional de Seguridad, establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, sobre el acceso electrónico de los ciudadanos a los servicios públicos, y regulado en el Real Decreto 3/2010, de 8 de enero, que surgen para dar respuesta, entre otras cosas, a estos incidentes.

Desde el punto de vista de los especialistas en seguridad, a los usuarios de las tecnologías de la información, el público en general y los profesionales en particular, todavía nos quedan algunos mitos por derribar y algunos conceptos por clarificar. En mi opinión, cuánto más conocimiento haya en este aspecto, mejor podrán evaluarse sus inversiones, y viceversa. Asimismo, se logrará una mayor conciencia de que todos los implicados son también responsables, en mayor o en menor medida, de la seguridad de los activos y valorarán los esfuerzos y los condicionantes que han de sopesar los técnicos a la hora de implantar un nuevo servicio informático.

II. CONCEPTOS DE SEGURIDAD

El mundo de las tecnologías de la información nace de un entorno empresarial donde cada organización y/o compañía establece sus propias definiciones, las cuales, van evolucionando constantemente y normalizándose a través de organismos internacionales o asociaciones profesionales. Un ejemplo sería International Organization for Standardization que son los desarrolladores de las normas ISO y en especial una que nos afecta, la "ISO/IEC 27001 - Sistema de Gestión de Seguridad de la Información". Por lo que resulta imprescindible estar informados sobre sus cambios porque repercuten a todos los niveles.

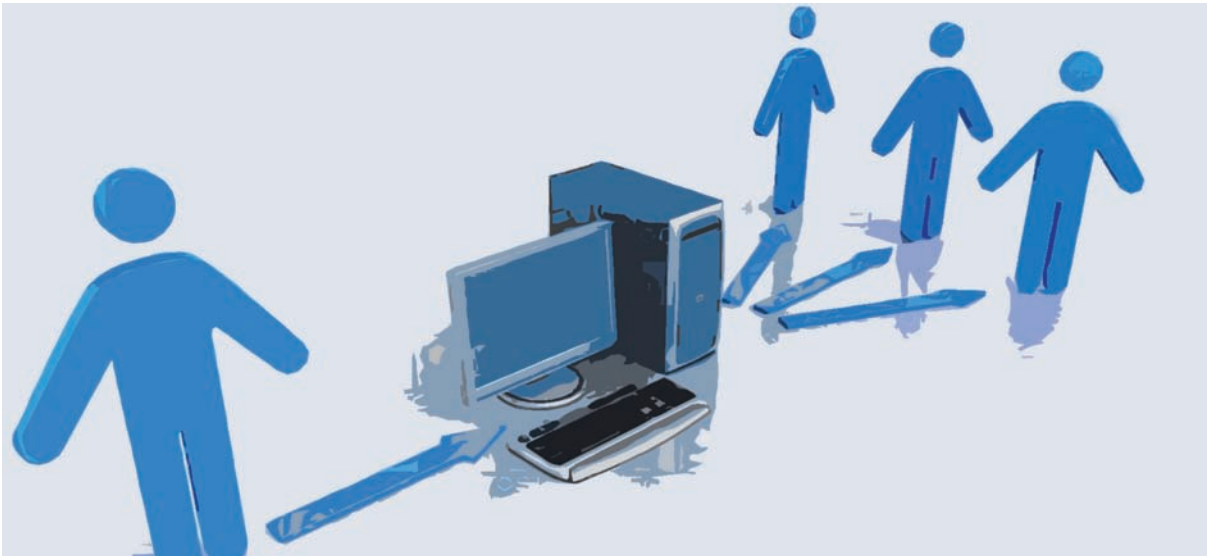
Por otro lado, cuando se habla de conceptos de seguridad, se corre el riesgo de pensar en productos y no en soluciones. Por ejemplo, cuando queremos garantizar el acceso y el contenido de nuestros ficheros, directamente se puede pensar en usar un antivirus. Aunque, sería conveniente contemplar un sistema de copias de seguridad por si se borra o altera la información, un sistema que compruebe la trazabilidad –tal como nos dice el Esquema Nacional de Seguridad- para verificar por donde ha pasado la documentación, etc. Como podemos ver, el antivirus podría ser una de las medidas necesarias para alcanzar la solución a nuestro objetivo, sin embargo, requiere de otras para realmente cumplir con la meta en el mayor porcentaje posible. Por eso, es más importante tener claro lo que buscamos, estudiar sus casuísticas y analizar qué productos responden a las mismas.

El concepto de **seguridad** es el primero que ha de ser consensuado y entendido. Bajo mi prisma, se trata de un concepto subjetivo más cercano a la psicología humana que a una ingeniería, ya que, estar seguro, es la sensación de conocer y controlar el entorno. Lo contrario, sentirse inseguro, es la impresión de que hay un elemento desconocido y cuyas acciones son impredecibles; y la inmensa mayoría de la humanidad, detesta o siente angustia ante este sentimiento.

Al ser un concepto subjetivo, para que nos sea útil debemos llegar a poderlo evaluar y medir porque de él derivarán soluciones técnicas, que necesitará inversiones y provocará cambios en el modelo de trabajo. Así que hasta poder establecer la definición de la **gestión de la seguridad**, deberemos analizar, previamente, tres conceptos básicos que serán su base.

Citando textualmente del glosario de la ISO 27000, la **amenaza** "es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización". Existen muchos tipos pero a continuación describimos las principales:

- Amenaza lógica: Es aquella que afecta a la información almacenada en los activos. A su vez, hay dos casos especialmente importantes:
  - Amenaza estructurada: Producida por alguien que posee una metodología formal, un posible patrocinador y sobre todo, un objetivo definido. Un buen ejemplo de ello son los famosos espionajes industriales.
  - Amenaza no estructurada: El atacante no posee una metodología formal, tampoco tiene patrocinador y no tiene un objetivo. Suelen ser intrusos "ociosos", efectos del malware o empleados descontentos.
- Amenaza física: En la cual, el atacante tiene diferentes tipos de acceso físico a la organización y puede ocasionar problemas. Ejemplos hay desde una persona buscando información confidencial en la papelera o seguir a un empleado y entrar con él por la puerta como si fuera un compañero.



Sabiendo qué tipo de amenazas existen y que puedan darse en nuestro entorno tecnológico, se pueden establecer las contramedidas técnicas y laborales necesarias ya que:

- Las amenazas lógicas estructuradas buscan comprometer un sistema a largo plazo y por lo tanto, tratan de evitar dejar cualquier rastro del ataque.
- A los atacantes que emplean las amenazas lógicas no estructuradas, en cambio, les es indiferente dejar rastro y lo que buscan es notoriedad. Por ejemplo, modificar el contenido de una web pública.
- Las amenazas físicas se exceden del objetivo de este artículo.

La **vulnerabilidad**, a diferencia de la amenaza, se produce a través de una programación negligente o de una mala utilización del software.

- Mala programación: El producto tiene bugs, en otras palabras, fallos de programación que permite bloquear el funcionamiento de la aplicación o acceder a información protegida y confidencial.
- Mala utilización: A pesar de la documentación aportada por el fabricante, el usuario es el responsable de utilizar el producto con todas sus consecuencias. Por ejemplo, un usuario que se olvida de la contraseña que ha puesto a un fichero o que guarda un documento confidencial en una carpeta pública.

El tercer concepto general es el **valor del bien** que es la medida del tiempo y los recursos necesarios para reemplazarlo, o para devolverlo a su estado anterior cuando haya habido un ataque exitoso. Cada vez más, también han de evaluarse los costes asociados al bien, tan subjetivos como la pérdida de la reputación o de la confianza que tenía la organización antes del incidente.

Una vez explicados los conceptos de amenaza, vulnerabilidad y valor del bien, estas se relacionan mediante el concepto del riesgo. El **riesgo** define una medida del peligro que corre cualquier bien y se suele expresar por medio de la **ecuación del riesgo**:

$$\text{Riesgo} = \text{Amenaza} \times \text{Vulnerabilidad} \times \text{Valor del Bien}$$

Gracias a esta ecuación, puede representarse todos los riesgos que hemos encontrado en la plataforma, en otras palabras, puede trazarse un mapa de riesgos.

Una vez familiarizados con el concepto de riesgo, podemos definir la **gestión de seguridad** como un proceso de mejora continua donde se mantiene un nivel aceptable de riesgo percibido.

Se dice que se debe mantener un nivel aceptable de riesgo porque la seguridad es la réplica al riesgo, sin embargo, debe responderse de una forma equilibrada sin que se agoten los recursos de la organización porque es imposible garantizar un nivel de seguridad total.

Y se dice percibido porque es imposible establecer contramedidas a los riesgos desconocidos.

III. VISIÓN GLOBAL DE LA SEGURIDAD

Generalmente cuando queremos asegurar una plataforma, es preferible hablar de riesgos que de seguridad ya que gracias a conocer el riesgo, se puede establecer una contramedida que lo mitigue o erradique. De ahí que el mapa de riesgos permita tener una imagen pormenorizada del estado en que se encuentra la platafor-

ma en un momento dado. Sin embargo, si no se interpreta bajo una visión global, se corre el peligro de no asegurar los elementos más expuestos o querer blindar todos los elementos, produciéndose un fuerte desequilibrio entre presupuesto y esfuerzos.

La visión global es de suma importante porque toda plataforma tecnológica es un sistema donde cada elemento está relacionado e interactúa con otros, por lo que, si se modifica o altera su comportamiento, cambia el sistema por completo. Actualmente, no es raro que un servicio complejo se encuentre en diferentes servidores y ubicaciones, y que se accedan a él desde cada vez más diversos dispositivos. Un ejemplo puede ser la plataforma de la Cámara de Cuentas de Andalucía donde la Rendición Telemática depende de más de una decena de servicios que se encuentran en diversos servidores y a donde acceden diferentes perfiles de usuario, tanto desde dentro como desde fuera de la Institución.

Uniendo el mapa de riesgos y la visión global, podemos darle un carácter relativo a los riesgos que hemos encontrado y gracias a esta visión holística, la gestión de seguridad, además de ser un proceso de mejora continua por sí mismo, debe impulsar mejoras cuando el mapa de riesgos cambie. En este caso, lo más eficiente y eficaz es seguir los pasos descritos por la Teoría de las Limitaciones propuesta por el Dr. Eliyahu M. Goldratt que nos ayudará a mitigar o reducir los riesgos más prioritarios siguiendo los siguientes pasos:

I. Identificar los activos, sus dependencias y sus riesgos. De ahí, señalar aquellos riesgos que más exponen a la plataforma.

II. Decidir cómo solucionarlos.

III. Subordinar todos los elementos a la decisión anterior.

IV. Mitigar o eliminar el riesgo.

V. Si se ha conseguido, se ha de volver al paso primero.

El quinto paso es imprescindible para evitar toda inercia que posee cualquier sistema, además, así se logra mantener la seguridad bajo un nivel aceptable, en otras palabras, controlable o asumible, de riesgos.

IV. INVERSIÓN FRENTE A LA INSEGURIDAD

La seguridad requiere una inversión debido a la necesidad de implantar hardware, adquirir licencias de software, los costes de sus mantenimientos y de formar a administradores y a usuarios. Además, es un gasto progresivo porque cada vez las necesidades son mayores y van incrementando su coste.

En relación con lo anterior, si se conciencia a los usuarios de las políticas y procedimientos de seguridad que hay implantados, reducimos algunas necesidades de inversión e incluso, permite optimizarlas porque serán los propios usuarios quienes nos retroalimentarán con la información más directa. Además, los usuarios prefieren comprender el porqué de las cosas a que les sea impuesto, ya que puede producir una sensación de resistencia y de rechazo.

En caso de no invertir en seguridad, seremos víctimas de los siguientes incidentes:

- Pérdida de reputación y confianza. Aunque es un intangible al que se le ha buscado diversas formas de valoración, es un sentimiento que una vez que el usuario se identifica con él, rara vez se modifica. Un ejemplo puede ser un ataque a una web de pago de tasas. Si el usuario percibe, siente o ha visto cómo ha sido atacada, su confianza no se recupera fácilmente.
- Interrupciones de servicio. Se puede dar el caso de que hayan atacado con éxito el sistema de correo corporativo, paralizando en gran medida las comunicaciones de la organización.
- Pérdidas de información y de trabajo por parte de los usuarios. Cualquier virus acompañado de un mal sistema de copia de seguridad puede causar un verdadero desastre en la información.

En todo incidente hay imputables una serie de costes directos y otros indirectos. Los directos siempre son el valor de los bienes afectados y los costes salariales de los trabajadores que no pueden desarrollar su labor. Los indirectos pueden ser los costes de imagen y reputación que derivan del éxito del ataque. La campaña de nueva imagen y el tiempo para vencer la reticencia de los usuarios, provocará retrasos y la utilización de otros medios para interactuar con la institución. Otro coste indirecto que, a veces, se olvida es el coste legal porque hayamos sido denunciados por haber perdido información confidencial o que haya sido expuesta públicamente.

Así que, por un lado, está la inversión en los riesgos más graves bajo una visión global y por otro, está el coste de asumir el riesgo. Generalmente, todas las instituciones tienen más que ganar que perder en invertir en seguridad y máxime si la gente está concienciada.

Como ejemplo más intuitivo, se puede contemplar el siguiente escenario: Si se emplea un servidor con sólo un disco duro para guardar los ficheros de la institución. La inversión para convertirlo en un sistema redundado, es decir, donde si se rompe un disco duro esté la información en otro y dando servicio, se puede estimar en unos 500 euros más la instalación y pruebas, un total de 650 euros.

Si contamos con copias de seguridad de la información, podríamos realizar el siguiente calculo para obtener el potencial coste de un fallo en el disco del servidor que comentamos.

Supongamos que la organización tiene 50 trabajadores cuyo sueldo medio es de 10 euros/hora y dos técnicos cuyo sueldo medio es 15 euros/hora. Seguidamente hay que contar con el tiempo y coste de la instalación y pruebas de los discos duros -esta vez en redundado-, la implementación del sistema operativo y el software en ese servidor de nuevo y la restauración total de los datos. Para que este escenario sea lo más real posible, se aplicará un coeficiente corrector del 20% al sueldo de los trabajadores porque se considera que pueden hacer otras tareas mientras se está recuperando el sistema.

Trabajadores	50
Sueldo	10,00 €
Horas/Jornada	8
Factor de corrección	20%
Coste diario del personal	**3.200,00 €**
Técnicos	2,00 €
Sueldo	15,00 €
Horas hasta corregir el problema	16
Coste diario del personal técnico	**480,00 €**
Coste total diario del personal	**3.680,00 €**
Sistema de discos redundados	500,00 €
Precio/Hora	45,00 €
Horas/Recuperación del sistema	24
Coste total de la puesta en pie del servidor	**1.580,00 €**
Coste total	**5.260,00 €**

Este ejemplo ha sido extraído de una pyme que sufrió un incidente similar en 2012 y que demuestra con claridad que invertir en seguridad es rentable, 650 euros de inversión frente a 5.260,00 € de gasto. Aquí no se ha evaluado los costes de imagen al tener la empresa parada y otros costes indirectos, como no poder atender a proveedores y clientes.

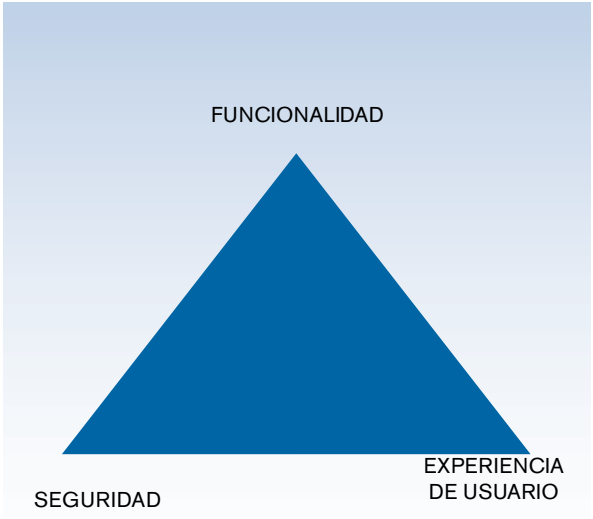
V. TRIÁNGULO DE LA SEGURIDAD

En aras de una mejor comprensión, el especialista traza un triángulo donde cada vértice señala un aspecto muy importante del servicio a implantar: la funcionalidad, la seguridad y la experiencia del usuario.

Este triángulo es muy controvertido para los usuarios y a la vez, es la causa de un gran esfuerzo, tanto en recursos como en tiempo, para todos los técnicos relacionados con la implantación de un nuevo servicio.

Aunque lo ideal es que este triángulo sea equilátero, la realidad demuestra que cada vez que se hace hincapié en uno de los vértices, se aleja produciéndose una fuerte merma de los otros dos.

Figura 1. Triángulo de la seguridad



VI. EJEMPLOS REALES

En base a todo lo anteriormente expuesto, se van a exponer algunos ejemplos reales dentro de la plataforma de Cámara de Cuentas de Andalucía.

Lo primero de todo, la gestión de l**a seguridad es un proceso de mejora**. Tras un serio análisis se comprobó que todo el tráfico de la red pasaba a través de los cortafuegos, por lo que había grandes posibilidades de que se convirtieran en cuello de botella. A la vez, la necesidad de adaptarse a los nuevos entornos, trabajo fuera de la sede o desde cualquier dispositivo, y nuevas aplicaciones, era cada vez mayor.

Así que, cuando tuvimos que sustituirlos, tras analizar muchos productos, se recurrió a cortafuegos de nueva generación, en concreto PA-500 de Palo Alto Networks. Gracias a él, se obtuvo una gran ventaja técnica: La autorización se vinculaba al usuario y a los servicios, estuvieran donde estuvieran.

En el caso de la Cámara de Cuentas de Andalucía, donde se contempla que el 65% de los funcionarios trabajan fuera de la oficina, donde entidades públicas han de enviar sus contabilidades desde sus sedes, donde ciudadanos pueden consultar información sobre la institución y donde proveedores pueden consultar la plataforma de contratación, era importante que este elemento garantizara los accesos de la forma más eficiente y por otro lado, se asegurase que no hubiera resquicios por dónde introducirse desautorizadamente.

Por otro lado, **la seguridad debe ser transparente al usuario**. Desde el 2003, el acceso al Portal corporativo es seguro a través de comunicaciones cifradas. A raíz de la buena experiencia que se ha tenido, se solicitó un certificado digital a la Fábrica Nacional de Moneda y Timbre debido a su calidad técnica y de reconocimiento legal, por lo que, ha acabado siendo empleado en la implantación de todos los nuevos servicios.

Tercero, cuando se aplica la seguridad, **la funcionalidad incluso puede aumentar**. Así que el siguiente paso consiste en firmar y encriptar digitalmente el correo electrónico. De esta forma, se puede identificar claramente al remitente, se hace accesible el contenido sólo a los destinatarios concretos y se garantiza la integridad ya que, cualquier manipulación del certificado invalida el contenido del correo.

En la Cámara de Cuentas de Andalucía, se ha optado por acceder al correo vía web para evitar los problemas de seguridad de los clientes pesados (Outlook, Thunderbird, etc.) y facilitar la movilidad de los usuarios. Siempre se tuvo la necesidad de encriptar y/o firmar digitalmente los correos pero hasta que no se implantó el software de CommuniGate que lleva el Webmail llamado Pronto!, no ha habido dicha posibilidad. Actualmente, antes del paso definitivo a producción, se están revisando los últimos detalles para mejorar la facilidad al usuario final, tomando siempre como criterio fundamental de actuación el equilibrio del triangulo de la seguridad.

Antes de acabar con los ejemplos, quisiera hacer una mención económica. Tanto en el caso de los cortafuegos como en el sistema de correo, sus precios se encontraban en la misma banda que productos similares pero sin las características descritas anteriormente. Por lo tanto, a la hora de elegir, estaba claro que haciendo un esfuerzo similar, podíamos optar a un producto mejor. Por otro lado, establecer comunicaciones seguras empleando el

certificado de la Fábrica Nacional de Moneda y Timbre es gratuito para instituciones públicas. Con esto quiero desterrar la idea de que implantar un nivel de seguridad aceptable incrementa notablemente los costes de explotación de la plataforma.

VII. RECAPITULACIÓN FINAL

Para entender el concepto de seguridad, previamente se han explicado los conceptos de amenaza, vulnerabilidad, valor del bien y del riesgo, para acabar definiendo la capa técnica de la gestión de seguridad como un proceso de mejora continua, donde se mantiene un nivel aceptable de riesgo percibido y que ha de aplicarse a la hora de implantar y mantener un servicio.

Sin embargo, se ha dado un paso más dándole un carácter holístico al sistema, en el cual cada elemento se relaciona con otros a diferentes niveles. El estudio de estas implicaciones y las limitaciones presupuestarias y técnicas hacen que la aplicación de la teoría de las limitaciones sea la más eficaz y eficiente forma de encarar la reducción del nivel de riesgos.

En relación a esto último, se han dado unas pautas intuitivas para evaluar la inversión teniendo en cuenta los costes tangibles, intangibles y legales.

A continuación, se ha descrito cómo hacer hincapié en la seguridad puede causar una merma de funcionalidades o de facilidad de uso, por lo que se propone trazar un triángulo de seguridad lo más equilátero posible.

Por último, se han expuesto una serie de ejemplos reales fundamentados en que la seguridad ha de ser un proceso de mejora, transparente al usuario e incluso debería ofrecer más funcionalidades. De forma que la seguridad deja de ser algo molesto y limitante para el usuario y refuerza su sensación de seguridad y confianza en el sistema.

BIBLIOGRAFÍA

Richard Bejtlich (2008): "El Tao de la monitorización de seguridad en redes". Pearson Educación S.A.

Gilbert Ramirez, Brian Caswell, Noam Rathaus, Hay Beale (2005): " *Nessus, Snort, and Ethereal Power Tools: Customizing Open Source Security Applications*". Syngress Media.

Eliyahu M. Goldratt, Eli Schragenheim, Carol A. Ptak (2009): "Necesario pero no suficiente". Díaz de Santos.

Eliyahu M. Goldratt (2005): "La meta: un proceso de mejora continua". Díaz de Santos.

CONCEPTOS

Comprometer: Es la acción por la cual un atacante pone en riesgo un equipo o dispositivo determinado.

Malware: Software cuyo comportamiento es hostil, molesto o intrusivo.

Bug: Fallo de programación dentro de un programa.