Preservación documental digital y seguridad informática

Juan Voutssas M. *

Artículo recibido:
3 de diciembre de 2009.
Artículo aceptado:
6 de abril de 2010.

Resumen

Se analiza la problemática actual de la producción y acumulación mundial de información en forma de documentos electrónicos o digitales, así como los problemas derivados del acceso de esa información, sobre todo en red, dado que esto podría implicar riesgo y pérdida de esa información. Se determinan los riesgos, amenazas vulnerabilidades, etcétera, que afectan a esa información, así como diversas estrategias para establecer la seguridad informática y la relación de ésta con la preservación confiable de esa información. Se estudian y establecen con detalle los factores que inciden a favor y en contra de los documentos digitales.

* Centro Universitario de Investigaciones Bibliotecológicas de la UNAM, México. voutssas@servidor.unam.mx

Palabras clave: Bibliotecología; Archivística; Ciencias de la Información; Bibliotecas y Archivos Digitales Electrónicos; Preservación Documental Digital: Seguridad Informática.

Abstract

Documentary, digital and security information
Juan Voutssas M.

Today's problematic situation with respect to the world production and accumulation of information in electronic or digital document format is analyzed, as well as the problems associated with access to their content, especially via the Internet since this could imply the risk of losing such information,. The risks, threats, vulnerabilities, etc. which affect this information are determined, as well as diverse strategies to establish computer security, and the relation this has with reliable preservation of information. The factors which have a bearing in favor of or against the security of digital documents, are studied in detail.

Keywords: Library Science: Archivistics; Information Science; Electronic and Digital Library Science and Archives; Digital Documental Preservation; ComputerSecurity.

"La sabiduría consiste en poder reconocer diversos peligros y escoger de entre ellos el menos dañino".

Niccolo Machiavelli, en *El Príncipe.*

El ambiente de los *sistemas de información* que predominó hasta principios de la década de los noventa, –previo a la globalización de las telecomunicaciones, las redes mundiales de teleproceso, la *Internet*, etcétera– tuvo como una de sus características más relevantes la de poseer entornos informáticos en los que se operaba de manera aislada o en redes privadas en las cuales, la seguridad impuesta por el acceso físico y algunas simples barreras informáticas bastaban para que la seguridad de la información en ellos contenida estuviese garantizada. Por lo mismo, no había mucha preocupación al respecto ni estrategias al efecto. En 1977, el senador Abraham A. Ribicoff, de Connecticut, EUA, propuso una iniciativa de "Acta de Ptotección de los

Sistemas de Cómputo Federales", la cual buscaba por primera vez definir cibercrímenes y recomendar sanciones por dichos delitos. La iniciativa no prosperó en esa ocasión [1].

En la actualidad, los sistemas de información han sido sustituidos casi en su totalidad por Tecnologías de Información y Comunicaciones (TIC) convergentes, por inmensas y cada vez más complejas redes institucionales locales y regionales, por servidores y computadoras personales que cada vez tienen mayor capacidad de proceso y de acceso a otros computadores, y cuya interconexión se extiende mundialmente. Al mismo tiempo, la *Internet* forma ya parte de la infraestructura operativa de sectores estratégicos de todos los países como el comercial, energía, transportes, banca y finanzas, –por mencionar algunos– y desempeña un papel fundamental en la forma en que los gobiernos proporcionan sus servicios e interactúan con organizaciones, empresas y ciudadanía, y es un factor cada vez más creciente de intercambio de información de manera individual por parte de los ciudadanos toda vez que se forman redes sociales cada vez más complejas.

La naturaleza y el tipo de tecnologías que constituyen la infraestructura de la información y comunicaciones también han cambiado de manera significativa. El número y tipo de dispositivos, servicios y variedades que integran la infraestructura de acceso se ha multiplicado, e incluye ya variados elementos de tecnología fija, inalámbrica y móvil, así como una proporción creciente de accesos que están conectados de manera permanente. Como consecuencia de todos estos cambios el volumen, naturaleza, disponibilidad y sensibilidad de la información que se intercambia a través de esta infraestructura se ha modificado y ha aumentado de manera muy significativa.

Por lo mismo, hoy en día la información es un activo muy valioso para casi todas las organizaciones; para algunas de ellas es su activo más valioso y por ello se invierten considerables recursos en crearla, administrarla, mantenerla, distribuirla, etcétera. De la capacidad de que esa información sea administrada correcta y eficientemente depende en gran medida el poder mantener la competitividad, credibilidad, flujo de liquidez, retorno de la inversión, rentabilidad, cumplimiento de la legalidad e imagen de la mayoría de empresas y organizaciones.

Aparte de su valor, por la misma convergencia de variados sistemas tecnológicos se produce, procesa, almacena y distribuye cada vez más y más información en formatos digitales, proveniente a su vez de procesos informáticos, acumulándose ya a lo largo de los años cantidades muy considerables

1 "Timeline: The US Government and Cybersecurity". 2003. Compiled by *The Washington Post*. Diponible noviembre 19, 2009 en: http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html

de este insumo. Como consecuencia vemos en las organizaciones modernas acumularse información depositada y almacenada en estas formas digitales, la que por lo general debe ser operada, distribuida y consultada por muchos en forma remota.

Pero precisamente por sus condiciones de ser digital, multiaccesible y necesariamente operada en red, la información se enfrenta a riesgos de daño o pérdida. Como resultado de esa creciente interconexión masiva y global, los sistemas y las redes de información se han vuelto más vulnerables ya que están expuestos a una cantidad creciente así como a una mayor variedad de amenazas. Esto hace a su vez que surjan nuevos retos que deben abordarse en materia de seguridad. La *seguridad informática* pretende eliminar o contener estos daños o pérdidas.

No toda la información que administra y utiliza una organización deberá ser preservada; mucha de ella es transitoria y por tanto tiene un tiempo de vida efímero; otra parte deberá ser preservada sólo por ciertos periodos que podríamos llamar de "corto plazo" –algunos años o menos– y cierta parte deberá ser preservada a largo plazo –por eones–. La preservación implica entonces una permanencia y autenticidad predeterminadas. Toda la información valiosa debe estar contemplada por la seguridad informática. La información a preservar es información valiosa: por lo tanto debe estar desde un principio y por siempre contemplada bajo esa óptica.

¿Por qué afirmamos que la información a preservar debe estar contemplada *desde un principio* por la seguridad informática? La respuesta es simple: pretender aplicar estas medidas a posteriori a una información que ya está almacenada es mucho más caro y difícil; y muchas veces inútil, puesto que ya está dañada o no es confiable.

Nada mejor para ilustrar esto que el postulado de Gene Spafford, experto en seguridad, quien en octubre del 2000, durante la "23ª Conferencia Nacional Acerca de Seguridad de los Sistemas de Información" –*23rd National Information Systems Security Conference*– hizo una analogía entre los esfuerzos de los especialistas en seguridad informática y los de los médicos cardiólogos:

> Nuestros pacientes están conscientes que la falta de ejercicio, la dieta rica en grasas y el tabaco son dañinos para todos ellos; no obstante, continúan fumando, comiendo grasa y viviendo sedentariamente hasta que llega el infarto. Entonces, todos ellos claman por una píldora mágica que los cure inmediatamente, sin ningún esfuerzo. Todos además afirman que su condición no es su culpa: es defecto genético heredado de sus padres, o es culpa de las compañías tabacaleras o de hamburguesas, etcétera. Los culpables siempre son terceros; nunca ellos. De pasada

> nos reprochan el no haberlos cuidado mejor y evitado el infarto. ¿esto les suena familiar? Pero no tiene por qué ser así; podemos hacerlo mejor. Necesitamos dejar de hacer las cosas como lo hacemos usualmente y comenzar a enfocarnos en una calidad de principio a fin. La seguridad informática debe ser construida desde el mismísimo principio, y no tratar de tapar el pozo después del accidente.

Subrayo entonces que preservación documental *no es* sinónimo de seguridad informática: la preservación de documentos de archivo se define como:

> el conjunto de principios, políticas, reglas y estrategias que rigen la estabilización física y tecnológica así como la protección del contenido intelectual de documentos de archivo adquiridos, con objeto de lograr en ellos una secuencia de existencia a largo plazo continua, perdurable, estable, duradera, ininterrumpida, inquebrantada, sin un final previsto.[2]

Esto es válido tanto para documentos de archivo sobre soportes "tradicionales" como para documentos de archivo digitales. Sólo que en este último caso habría que agregar a la definición:

> en el caso de preservación documental digital debe establecerse específicamente cómo esos documentos serán conservados durante y a través de las diferentes generaciones de la tecnología a través del tiempo, con independencia de donde residan —sus soportes— y de cómo estén representados —sus formatos—.

Defino "Seguridad Informática" como:

> el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos.

Conscientes de esta diferencia, es de suma importancia reflexionar acerca del hecho de que no puede haber ni gestión documental –corto a mediano plazo– ni preservación documental –mediano a largo plazo– sin que la información haya sido contemplada bajo los conceptos de la seguridad informática

2 "Glosario Interpares". Sitio Web oficial del Proyecto "Interpares. Disponible noviembre 19, 2009 en inglés: http://www.interpares.org/ip2/ip2_term_pdf.cfm?pdf=glossary En castellano; Sitio Web del TEAM México de Interpares: http://www.interpares.org/display_file.cfm?doc=ip3_mx_glosario_interpares_v1-2.pdf

desde un principio, desde su mismísima creación. La seguridad informática nos maximiza la probabilidad de que la información –entre otros recursos informáticos– se mantenga libre de daños y por tanto opere cotidiana y correctamente. Es una herramienta que puede ser utilizada en reservorios de corto-mediano plazo y que a su vez nos permitirá que la parte de esa información que así establezcamos se pueda preservar a largo plazo. Por lo mismo podemos concluir que la seguridad informática forma parte de la preservación documental digital y no al revés. La primera es subconjunto de la otra.

Conceptos fundamentales de la seguridad informática:

Para poder comprender el concepto integral de la seguridad informática, es indispensable entender los diversos conceptos básicos que la rigen, ya que de otra forma no es posible establecer una base de estudio. Los enunciaré a continuación y los desarrollaré con más detalle más adelante.

- *Recursos Informáticos*: el equipo de cómputo y telecomunicaciones; los sistemas, programas y aplicaciones, así como los datos e información de una organización. También se les conoce como "activos informáticos"
- *Amenaza*: fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los recursos informáticos de la organización.
- *Impacto*: la medida del efecto nocivo de un evento.
- *Vulnerabilidad*: característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza.
- *Riesgo*: la probabilidad de que un evento nocivo ocurra combinado con su impacto en la organización.
- *Principio básico de la seguridad informática*: la seguridad informática no es un producto, es un proceso.

El objetivo primario de la *seguridad informática* es el de mantener al mínimo los riesgos sobre los recursos informáticos, –todos los recursos– y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable. Para ello utilizaremos estructuras organizacionales técnicas, administrativas, gerenciales o legales.

El objetivo secundario de la *seguridad informática* –y subrayo que es de nuestro especial interés desde el punto de vista de la preservación documental–

consiste en garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su confiabilidad total. Este concepto varía de acuerdo a distintos autores, a los contextos documentales y al tipo de organización a la que la información esté asociada. En un contexto archivístico y en donde tratamos de interoperar un enfoque de seguridad informática con uno de preservación digital, podemos establecer esa confiabilidad como la unión de seis características esenciales:

- permanencia
- accesibilidad
- disponibilidad
- confidencialidad (privacidad)
- autenticidad (integridad)
- aceptabilidad (no repudio)

La característica de *permanencia* estará asociada a la medida en la que podemos asegurar que el documento existirá y estará disponible por un lapso considerable, si es necesario, eternamente. Está asociada con su presencia, su existencia, y ellas dependen obviamente de su protección, su salvaguarda y por supuesto, de la duración y continuidad de su soporte físico. Es común confundir esta característica con la de *accesibilidad*, la cual tiene que ver con que el documento, existiendo, pueda ser accedido por nosotros y sea visible. Son dos conceptos distintos. Distingamos bien entre almacenamiento permanente seguro –la "permanencia"– y el acceso futuro –la "accesibilidad"–.

Respecto al primer concepto, la permanencia depende del *almacenamiento permanente seguro*. Para asegurar este almacenamiento de objetos digitales, –en este caso documentos de archivo– se requiere de estrategias, procedimientos y técnicas adecuadas para crear, operar y mantener archivos documentales a largo plazo. Tales estrategias deben permitir preservar la *cadena de bits*[3] y sus formatos. Por lo mismo se deben diseñar y llevar a cabo meticulosamente esas técnicas y procedimientos para la conservación tanto de los soportes documentales como de sus contenidos digitales: la información del documento en sí misma y los metadatos asociados a él. La preservación del soporte, la cadena de bits, su estructura y su formato nos da la permanencia.

El acceso futuro de los objetos digitales almacenados es otra cuestión. ¿Cómo asegurarnos de que –después de haberse conservado en buen estado– vamos a poder ver o reproducir estos documentos dentro de los archivos

3 Cadena de bits: datos digitales codificados en una secuencia estructurada de bits o dígitos binarios y que son transmitidos, almacenados o recibidos como una unidad. Glosario "Interpares".

dentro de veinte, cincuenta o doscientos años? Es decir: ¿cómo garantizaremos nuestra capacidad de interpretar y reproducir correctamente las *cadenas de bits* correctamente conservadas? Debemos asegurarnos de que –habiéndose conservado en buen estado– vamos a poder acceder: ver y/o reproducir estos documentos dentro de veinte, cincuenta o doscientos años; es decir: deberemos poder reproducir correctamente esa *cadena de bits* correctamente conservada.

La capacidad futura de poder reproducir el documento correctamente nos da la medida de la accesibilidad. Pongamos por ejemplo:

Si usted posee un disco fonográfico de acetato de 78 r.p.m. conservado en buen estado, requiere de un dispositivo tecnológico para accederlo: en este caso será simplemente un fonógrafo. Si usted posee un casete con una película en formato "Beta" *en buen estado*, requiere como artilugios tecnológicos para accederla un videocasetera que opere ese formato en especial, además de una televisión que pueda recibir y desplegar la señal del videoreproductor. Ha habido permanencia de los documentos ya que se hallan en buen estado y el fonógrafo y videocasetera nos permiten la accesibilidad. Si usted tiene un documento de texto dentro de un archivo en "Word 5.1" grabado en un disquete de ocho pulgadas, y asumiendo que este documento y su soporte se encuentran en perfecto estado de conservación, requiere de un equipo lector adecuado, esto es, una unidad de disquetes de ocho pulgadas conectado a una computadora; requiere además del programa *Office* o alguno semejante que pueda acceder a ese archivo y que ese programa sea operable bajo un cierto sistema operativo que también posee y que opera correctamente en su computador; varios requerimientos para acceder al documento.

Si usted tiene un archivo procesado en "Lotus 1-2-3" *grabado* en una cinta magnética de computadora de media pulgada, 7 o 9 canales, asumiendo que el documento y su soporte se encuentran en perfecto estado de conservación, tiene usted otro documento que ha permanecido a lo largo del tiempo: existe sin duda; ha tenido "permanencia". Pero usted requiere para accederlo al igual que el ejemplo anterior un lector de cintas de carrete abierto compatible con una cierta computadora, que contenga un sistema operativo donde corra un programa que pueda leer e interpretar correctamente ese archivo. Requerimientos muy complejos en la actualidad.

Para acceder a cada uno de los documentos de los ejemplos anteriores hemos requerido de un accesorio tecnológico del cual dependemos para lograr esa acción. En el caso del disco fonográfico lo único que necesitamos es físicamente un equipo, un reproductor de estos discos, es decir un fonógrafo y ya está. La accesibilidad es relativamente sencilla; en el caso del archivo *Word*, los requerimientos crecieron y se complicó más y en el caso del archivo Lotus el acceso se volvió un verdadero problema.

Como podemos concluir, una cosa es que un documento exista, permanezca en buen estado, y otra cosa es que se pueda acceder y se pueda ver y analizar su contenido. Dependiendo de nuestra capacidad de disponer de esos artefactos, programas, sistemas operativos, formatos, etcétera, tendremos acceso a esos documentos. Habrá o no "accesibilidad", independientemente de su "permanencia". Esta es la acepción de usabilidad que deberá usarse en lo relativo a preservación y seguridad. No debe confundirse este término con el concepto de "accesibilidad" como "usabilidad" en el sentido de las facilidades que se le agregan a ciertos sitios *Web* para que puedan ser accedidos más fácilmente por personas con capacidades visuales diferentes, tales como fuentes de letras más grandes, contrastes de colores más pronunciados, "lentes de aumento" virtuales sobre la pantalla, etcétera. Ése es otro concepto de "accesibilidad" o "usabilidad" que no tiene que ver con seguridad o preservación de información y no deben ser confundidos.

Hoy en día ya se maneja el concepto de "archivo permanente", el cual consiste en una serie de estrategias y técnicas tendientes a lograr la interoperabilidad máxima, es decir, que la arquitectura de los sistemas de archivos de información digital para preservación sea independiente de la tecnología usada para crearlos, precisamente para reducir el problema de la accesibilidad. La técnica archivística conocida como: "preservación de objeto persistente" –*persistent object preservation* o "POP"– tiene como propósito asegurar que los documentos de archivo digitales permanezcan accesibles por medio de la autodescripción hecha de ellos, incluyendo formatos, características estructurales y tecnológicas, etcétera, hecha de manera independiente del equipo o programas en donde operen.

La característica de *disponibilidad* tiene que ver con la facilidad de poder acceder al documento cuando, como sea y por quien sea necesario. Subrayo: la *accesibilidad* nos brinda una capacidad tecnológica de acceso; la *disponibilidad* nos da una medida acerca de: quién, cómo, dónde y cuándo puede accederse al documento. *Disponibilidad* no significa obligatoriamente que todos los documentos deban estar disponibles todo el tiempo en-línea para todo el mundo. De acuerdo a ciertas reglas establecidas por cada organización es necesario que el documento esté disponible en los tiempos, bajo las condiciones y para las personas preestablecidas. La *disponibilidad* consiste en la capacidad de la organización de poder acceder a un documento conforme a esas condiciones preestablecidas. En la medida que podemos establecer y cumplir esas condiciones –tiempo, requisitos, soporte, restricciones, etcétera– diremos que un cierto documento tiene mayor o menor disponibilidad.

La característica de la *confidencialidad* o privacidad tiene que ver con el hecho de que los registros documentales deben estar disponibles siempre,

pero sólo para las personas autorizadas, durante las circunstancias y bajo condiciones válidas y preestablecidas. No deberá ser posible obtener ninguna información de los archivos fuera de esas condiciones.

La característica de *autenticidad* o *integridad* es sumamente importante. Algunos autores lo consideran uno de los elementos más importantes de la preservación. Tiene que ver con la confianza de un documento de archivo como tal; esto es, la cualidad de un documento de archivo de ser lo que pretende ser sin alteraciones o corrupciones. Los documentos auténticos son los que han mantenido su identidad e integridad al paso del tiempo[4].

Este concepto es directamente proporcional al grado en que el documento digital refleja al original, no en su apariencia física, sino en su esencia, su espíritu, su intención. Un documento *íntegro* es el que refleja totalmente la esencia del original; es decir, no ha sido corrompido en su contexto: alterado, mutilado, interpretado, aumentado, recortado, deformado, censurado, etcétera: es confiable y por tanto aceptable. Su mensaje, autoría, fechas asociadas, lugares, etcétera, son en realidad las consignadas en el documento desde siempre; en suma: es auténtico. Aunque hubiese cambiado físicamente, en su esencia refleja de manera completa lo que se estableció en el documento original.

El original de un documento electrónico –llamado la primera instanciación (representación de una abstracción a través de una instancia concreta)– desaparece en el ambiente digital la primera vez que es salvado. Lo que se recupera *siempre* es una copia. En realidad no se puede preservar documentos digitales: sólo se puede preservar la capacidad de reproducirlos una y otra vez[5]. Lo importante al poder acceder y reproducir una y otra vez un documento, es la condición de que sea íntegro, auténtico. Es necesario subrayar que un cierto documento no tiene que ser idéntico al documento que le dio origen para ser íntegro; de hecho, es perfectamente natural que los documentos electrónicos sean modificados de tiempo en tiempo, para actualizar su formato, versión, sistema operativo, código de caracteres, etcétera. Pero si no se puede preservar en realidad a largo plazo un documento digital y lo que se preserva es nuestra capacidad de reproducirlo correctamente es necesario por tanto garantizar de alguna forma que aunque su estructura física

4 "Glosario Interpares". Sitio Web oficial del Proyecto "Interpares. Disponible noviembre 19, 2009 en inglés: http://www.interpares.org/ip2/ip2_term_pdf.cfm?pdf=glossary. En castellano; Sitio Web del TEAM México de Interpares: http://www.interpares.org/display_file.cfm?doc=ip3_mx_glosario_interpares_v1-2.pdf

5 Luciana Duranti and Thibodeau, Kenneth. 2005. "The concept of record in interactive, experiential and dynamic environments: The view of InterPARES", en: *Archival Science*. Springer Netherlands. ISSN:1389-0166 (Print) 1573-7519 (Online). Vol. 5 Nums. 2-4. December 2005. DOI 10.1007/BF02660804. pp. 13-68.

cambie, su contenido sea el mismo, y sus "contextos" sean documentados; esto es, todavía sea íntegro, auténtico. En la medida que se pueda garantizar esa autenticidad se podrá afirmar que nuestro documento sigue siendo "íntegro", "auténtico" a lo largo del tiempo, al margen de los cambios y adaptaciones tecnológicas sufridas.

La "esencia" de un documento puede extraerse de sus "contextos" de creación: es decir: cómo fue hecho. Estos contextos provienen de varias fuentes que es necesario identificar y consignar junto con el documento: el contexto de procedencia –la instancia creadora, así como su mandato, estructura y funciones–; el contexto jurídico-administrativo –la normatividad que ampara o rige a ese documento–; el contexto procedimental –las reglas para crearlo, procesarlo, modificarlo, etcétrera–; el contexto documental –las reglas de representación según las cuales el contenido de un documento de archivo son comunicados– y finalmente el contexto tecnológico –los formatos, sistemas y otras reglas técnicas bajo las cuales existe la representación digital del contenido de un documento de archivo–. Finalmente, deben documentarse también los cambios que los documentos hayan experimentado desde su creación. No es necesario que estos contextos estén escritos documento por documento; son inherentes a todo un archivo. Pero es indispensable que cada documento mantenga esa "esencia" esos contextos así consignados, para que cada documento del archivo sea auténtico. En este contexto, un documento digital preservado es considerado auténtico si puede declararse que es una copia auténtica por parte del custodio quien de fe de su identidad y de su integridad a lo largo del tiempo a partir del momento en que lo ingresó a su acervo, y ese custodio puede documentar además correctamente el proceso de conservación segura –inclusive cualquier migración posterior y sus consecuencias tanto en forma como en contenido–.

La característica final de la información segura implica la *aceptabilidad* o "no repudio". En lo relativo a documentos sobre soportes *tradicionales,* la autenticidad fue establecida siempre a través del objeto mismo, del documento, así que el custodio sólo necesitó preocuparse de que el usuario analizase el objeto y sacara sus propias conclusiones acerca de su autenticidad. Con los medios digitales, lo que el usuario necesita para analizar y concluir la aceptabilidad es conocer la calidad del proceso de creación de un documento, la autoridad y capacidad –competencia– del custodio, así como la calidad de la documentación del proceso de conservación y su seguridad. El custodio a su vez requiere contar con los elementos que le permitan dar fe o establecer que la información contenida en ese archivo es auténtica y que ya hemos mencionado.

La consecuencia final de la unión de las seis características antes descritas en un documento y/o archivo que los contenga es la de la fiabilidad, entendida

esta como la confianza en un documento de archivo como establecimiento de un acto o declaración de un hecho. Implica que un documento de archivo puede sostener al hecho del que es relativo y es establecida examinando la completud lograda en las características que dan forma al documento de archivo así como el nivel de control ejercido durante su proceso de creación y preservación.

El medio para lograr el objetivo secundario de la *seguridad informática* consiste entonces en que los documentos, registros y archivos informáticos que son propiedad de la organización cumplan ahora y en un futuro en la medida más completa posible con estas seis características esenciales de los mismos, y como consecuencia obtendremos su *fiabilidad total.*

Amenazas informáticas

Las amenazas, como ya hemos mencionado, consisten en la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los insumos informáticos de la organización y ulteriormente a ella misma. Entre ellas, identificamos como las principales:

- El advenimiento y proliferación de "malware" o "malicious software", programas cuyo objetivo es el de infiltrase en los sistemas sin conocimiento de su dueño, con objeto de causar daño o perjuicio al comportamiento del sistema y por tanto de la organización.
- La pérdida, destrucción, alteración, o sustracción de información por parte de personal de la organización debido a negligencia, dolo, mala capacitación, falta de responsabilidad laboral, mal uso, ignorancia, apagado o elusión de dispositivos de seguridad y/o buenas prácticas.
- La pérdida, destrucción, alteración, sustracción, consulta y divulgación de información por parte de personas o grupos externos malintencionados.
- El acceso no autorizado a conjuntos de información.
- La pérdida, destrucción o sustracción de información debida a vandalismo.
- Los ataques de negación de servicio o de intrusión a los sistemas de la organización por parte de ciber-criminales: personas o grupos malintencionados quienes apoyan o realizan actividades criminales y que usan estos ataques o amenazan con usarlos, como medios de presión o extorsión.
- Los "phishers", especializados en robo de identidades personales y

otros ataques del tipo de "ingeniería social".[6]

- Los "spammers" y otros mercadotecnistas irresponsables y egoístas quienes saturan y desperdician el ancho de banda de las organizaciones.
- La pérdida o destrucción de información debida a accidentes y fallas del equipo: fallas de energía, fallas debidas a calentamiento, aterrizamiento, desmagnetización, rayadura o descompostura de dispositivos de almacenamiento, etcétera.
- La pérdida o destrucción de información debida a catástrofes naturales: inundaciones, tormentas, incendios, sismos, etcétera.
- El advenimiento de tecnologías avanzadas tales como el cómputo *quantum,* mismas que pueden ser utilizadas para desencriptar documentos, llaves, etcétera al combinar complejos principios físicos, matemáticos y computacionales.

Vulnerabilidades informáticas

Una vulnerabilidad es alguna característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza, intencional o accidentalmente. Las vulnerabilidades pueden provenir de muchas fuentes, desde el diseño o implementación de los sistemas, los procedimientos de seguridad, los controles internos, etcétera; se trata en general de protecciones inadecuadas o insuficientes, tanto físicas como lógicas, procedimentales o legales de alguno de los recursos informáticos. Las vulnerabilidades al ser explotadas resultan en fisuras en la seguridad con potenciales impactos nocivos para la organización. Más detalladamente, provienen de:

- Fallas en el diseño o construcción de programas, sobre todo en aquellos que provienen de un mercado masivo; por ejemplo sistemas operativos, programas de aplicación, el protocolo de comunicaciones TCP/IP, etcétera.
- Uso de computadoras, programas y equipos de red de tipo genérico en aplicaciones críticas.
- Atención insuficiente al potencial error humano durante el diseño, implementación o explotación de sistemas, particularmente debidas a

6 Sarah Granger. 2009. "Social Engineering Fundamentals, Part I: Hacker Tactics". Security Focus. Disponible noviembre 19, 2009, en: http://www.securityfocus.com/infocus/1527

desviaciones u omisiones de buenas prácticas en estas etapas.
- Confianza excesiva en algún único dispositivo u oficina de seguridad.
- Relajamiento de las políticas y procedimientos de seguridad, debidos a falta de seguimiento de los mismos, producidas por un desempeño de seguridad adecuado durante cierto lapso.
- Fallas de seguimiento en el monitoreo o indicadores de seguridad.
- Pobre o nula gobernanza de los activos informáticos, debida principalmente a un mal seguimiento de esos activos y sus contextos de seguridad asociados de forma integral.
- Cambio frecuente de elementos de la plataforma informática.
- Falla en la adjudicación o seguimiento de responsabilidades.
- Planes de contingencia nulos o pobres, tanto para situaciones cotidianas como extremas.
- Ignorancia, negligencia o curiosidad por parte de usuarios en general de los sistemas.
- Equipos, programas y redes "heredados" de generaciones tecnológicas anteriores.
- Errores inherentes al diseño de microprocesadores y microcódigos que se encuentran en rutinas básicas o "núcleo" de los sistemas, o en el encriptado o virtualización.
- Falta de concientización del personal en general acerca de la importancia de la seguridad y responsabilidades compartidas e integrales.

Riesgos informáticos

Como se mencionó también, riesgo se define como la probabilidad de que un evento nocivo ocurra combinado con su impacto o efecto nocivo en la organización. Se materializa cuando una amenaza actúa sobre una vulnerabilidad y causa un impacto. Los principales riesgos se agrupan como:

- Sustracción de datos personales para usos malintencionados.
- Fugas de información, extracción o pérdida de información valiosa y/o privada.
- Introducción de programas maliciosos a los sistemas de la organización, que pueden ser utilizados para destruirlos u obstaculizarlos, usurpar recursos informáticos, extraer o alterar información sin autorización, ejecutar acciones ocultas, borrar actividades, robo y detentación de identidades, etcétera.
- Acciones de "ingeniería social" malintencionada: "phishing", "spam",

espionaje, etcétera.
- Uso indebido de materiales sujetos a derechos de propiedad intelectual.
- Daño físico a instalaciones, equipos, programas, etcétera.

Impactos

Los impactos son los efectos nocivos contra la información de la organización al materializarse una amenaza informática. Al suceder incidentes contra la seguridad informática pueden devenir en:

- Disrupción en las rutinas y procesos de la organización con posibles consecuencias a su capacidad operativa.
- Pérdida de la credibilidad y reputación de la organización por parte del consejo directivo de la organización, público en general, medios de información, etcétera.
- Costo político y social derivado de la divulgación de incidentes en la seguridad informática.
- Violación por parte de la organización a la normatividad acerca de confidencialidad y privacidad de datos de las personas.
- Multas, sanciones o fincado de responsabilidades por violaciones a normatividad de confidencialidad.
- Pérdida de la privacidad en registros y documentos de personas.
- Pérdida de confianza en las tecnologías de información por parte del personal de la organización y del público en general.
- Incremento sensible y no programado en gastos emergentes de seguridad.
- Costos de reemplazo de equipos, programas, y otros activos informáticos dañados, robados, perdidos o corrompidos en incidentes de seguridad.

Cada uno de estos efectos nocivos puede cuantificarse de tal forma de ir estableciendo el impacto de ellos en la información y consecuentemente en la organización. En resumen, la seguridad informática pretende identificar las amenzas y reducir los riesgos al detectar las vulnerabilidades nulificando o minimizando así el impacto o efecto nocivo sobre la organización. Si analizamos y juntamos todo lo anterior creo que estamos ya en posibilidad de comprender porqué la "seguridad informática" se definió entonces como "el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas,

guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos".

Estrategia y metodologías para la gestión de la seguridad informática

En los últimos años se han ido desarrollando diversas metodologías para la creación de una infraestructura de seguridad informática al interior de una organización y para revisar el estado que guarda la seguridad de la información en esa organización. Bajo los nuevos enfoques se destaca el hecho de que estas metodologías no sólo deben abarcar –como se hacía antes– las problemáticas de la seguridad interna de los sistemas; hoy en día deben hacer una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de la organización en cuanto a la seguridad de la información que maneja. Esta aproximación marca la diferencia del anterior concepto conocido como "seguridad de sistemas" hacia el nuevo concepto de "seguridad informática de Tecnologías de Información y Comunicaciones (TIC)". El nuevo enfoque considera también los riesgos organizacionales, operacionales, normativos y físicos de una organización, con todo lo que esto implica.

El contexto mundial acerca de esta problemática recomienda como primera etapa diseñar para cada organización una "estrategia de seguridad informática". Esto se hace generalmente en dos pasos:

Paso 1) Establecer los requisitos de seguridad. Para ello se estudian tres fuentes:

a) Los principios, objetivos, políticas, procedimientos y requisitos que la organización ha desarrollado para apoyar sus operaciones y que conforman el tratamiento de la información.

b) El conjunto de requisitos legales, estatutos, contratos y regulaciones que deben satisfacer tanto la organización en sí misma como sus socios, usuarios, contrapartes, contratistas y proveedores de servicios.

c) La valoración de los riesgos de la información en la organización, a partir de sus objetivos y estrategias generales. Con ellos se identifican las amenazas a los activos, se evalúa la vulnerabilidad, la probabilidad de su ocurrencia y se estima su posible

impacto. Para el análisis de riesgos es prática generalizada seleccionar alguna metodología ya probada al efecto. Existe un buen número de ellas a nivel mundial, pero si se desea abundar en el conocimiento de este tipo de metodologías, recomiendo estudiar en particular la denominada OCTAVE – *Operationally Critical Threat, Asset, and Vulnerability Evaluation*[7].

Este análisis o valoración de riesgos permite estar en capacidad de:

- Identificar, evaluar y manejar los riesgos de seguridad informática.
- Establecer la probabilidad de que un recurso informático quede expuesto a un evento, así como el impacto que ese evento produciría en la organización.
- Determinar las medidas de seguridad que minimizan o neutralizan ese riesgo a un costo razonable.
- Tomar decisiones preventivas y planeadas en lo tocante a seguridad.

Los elementos que un análisis de riesgos debe cubrir son:

- Análisis de los activos que son de valor.
- Análisis de amenazas cuya ocurrencia pueda producir pérdidas a la organización.
- Análisis de vulnerabilidades en los controles de seguridad y en los sistemas.
- Análisis de todos los riesgos y sus impactos en las operaciones de la organización.
- Análisis de las medidas de seguridad que actuarían como una protección total o parcial contra cada riesgo.

Paso 2) Establecer una estrategia para la construcción de la seguridad informática dentro de la organización.

Para el establecimiento de una estrategia destinada a construir la seguridad informática dentro de la institución es prática generalizada seleccionar una metodología ya probada al efecto. Si bien existe un buen número de ellas a nivel mundial, es una práctica muy utilizada y altamente recomendada optar por alguna de las metodologías que se han convertido gradualmente en estándares en los últimos años. Existen varias ventajas en usar una metodogía aprobada para este propósito:

7 OCTAVE – *Operationally Critical Threat, Asset, and Vulnerability Evaluation*. Disponible 19 noviembre, 2009 en: http://www.cert.org/octave/

- Da certeza y continuidad operacional a la organización
- Da certeza en los costos de seguridad, además de su justificación.
- Permite que la seguridad se convierta en parte de la cultura de la organización, al incrementar la conciencia de seguridad en todos los niveles.
- Permite determinar y planear las acciones preventivas y correctivas en materia de seguridad.
- Brinda criterios para el diseño, operación y evaluación de planes de contingencia.
- Facilita la toma de decisiones en toda la organización que atañan a la seguridad.
- Incrementa la productividad de los recursos humanos, financieros, de equipo, etcétera dedicados a la seguridad.

Las limitantes generalmente observadas en estas metodologías son:

- Es un proceso analítico con un gran número de variables.
- Una sola metodología no es aplicable a todos los ambientes.
- Inversión considerable de tiempo y recursos dedicados a las actividades.
- Las soluciones al problema de seguridad no son instantáneas ni permanentes; el análisis de riesgos y sus soluciones es un proceso cíclico y continuo que involucra no sólo al área de tecnologías de la información sino a la organización en general.
- La seguridad informática requiere de la participación de todos los niveles de la organización y es una responsabilidad compartida.

Los estándares metodológicos iso en seguridad informática

Para realizar algún estudio acerca de la seguridad de la información dentro de alguna organización, podemos seleccionar entre varios estándares que siguen estas metodologías modernas al efecto. Si bien existen varios al efecto, dependiendo de épocas, regiones, costos, etcétera, para ilustrar este documento utilizaremos como base algunos de los estándares para la seguridad de la información

provenientes de la Organización Internacional de Estándares (ISO). En particular el estándar ISO/17799 o los estándares ISO/IEC 27001 y 27002 *(Information technology – Security techniques – Information security management systems – Requirements)*. Todos estos estándares consisten en normas internacionalmente aceptadas que ofrecen recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

El estándar metodológico ISO/17799 fue aprobado en al año 2000. Es a su vez descendiente de la norma británica BS 7799-2:2002 del –*Information Security Management Standard– del British Standard Institute* quien publicó su primera versión de ellas en Inglaterra en 1995, con actualizaciones realizadas en 1998 y 1999, consistentes de dos partes: 1.- Código de prácticas y 2.- Especificaciones del sistema de administración de seguridad de la información.

Los estándares ISO/IEC 27001 y 27002 fueron aprobados como estándar internacional en 2005 por la *International Organization for Standarization* (ISO) y por la *International Electrotechnical Commission* (IEC). Estas normas provienen de la norma ISO/17799:2000. Si bien las versiones ISO 27001 y 27002 son las más actualizadas, dado que son muy recientes todavía es muy utilizado el ISO/17799. Resulta muy adecuado utilizar alguna de ellas para el diseño de la estrategia para la seguridad informática de una cierta organización ya que ello indica que se sigue un proceso metodológico estandarizado, moderno y de amplia aceptación mundial para la construcción de la seguridad organizativa. Esto además facilitará el proceso de revisión de la seguridad ya que de todas formas la revisión debe hacerse también siguiendo un estándar metodológico. Algunas de las razones prácticas para utilizar este estándar son:

- Conceptualiza la información como activo con su correspondiente valor para la organización.
- Consiste en una guía metodológica para la autocreación de la infraestructura de seguridad por parte de la organización, basada en encuestas, diagnósticos, análisis, sugerencias, etcétera.
- Su enfoque está dirigido a la protección de la información con miras a la continuidad de la organización y retorno de las inversiones.
- Es una herramienta de alto valor para construir y evaluar una infraestructura para la seguridad de la información dentro de la organización.
- Pretende asegurar la permanencia, disponibilidad, accesibilidad, integridad, confidencialidad y aceptabilidad de la información.
- Integra controles que incluyan las mejores prácticas relativas a la seguridad de la información.

- Ofrece a la organización un punto de referencia estandarizado y reconocido mundialmente, con una metodología totalmente estructurada.
- Es una herramienta de alto valor para construir y evaluar una infraestructura para la seguridad de la información dentro de la organización.
- Facilita la creación de un entorno confiable y único dentro de la organización donde fluye la comunicación y las operaciones.
- Permite establecer procesos definidos para diseñar, implementar, evaluar, mantener y administrar la seguridad de la información.
- Permite establecer claramente un conjunto de políticas, estándares, procedimientos, buenas prácticas y guías relativos a la seguridad al interior de la organización.
- En las próximas versiones permitirá obtener niveles de certificación informando a la organización de su estado en ese momento en cuanto a seguridad, así como posibles mejoras a la misma y retroalimentaciones.
- Permite llegar hasta el detalle en los conceptos de seguridad de la información.
- Produce un conjunto de procedimientos, controles y medidas de evaluación aplicables y medibles.
- Finalmente, y de suma importancia, organiza la seguridad en diez dominios o áreas principales específicas perfectamente diferenciadas. De estos diez dominios se derivan 36 objetivos de control, esto es, los resultados que se espera alcanzar mediante la implementación de los controles, y 127 acciones de control, esto es, prácticas, procedimientos o mecanismos que reducen el nivel de riesgo.

Los diez dominios o áreas del estándar son:

- *Políticas de seguridad.* Es indispensable en toda organización que posea activos informáticos contar con políticas de seguridad documentadas y procedimientos internos de la organización acerca de las estrategias y disposiciones que guíen los principales rubros y áreas relacionados con la seguridad del los bienes informáticos y que permitan su actualización y revisión por parte de un comité de seguridad interno.

  Algunos de los principales objetivos de control y acciones dentro de este dominio son:

  - Políticas y procedimientos internos generales de seguridad informática.

    - Políticas de acceso a instalaciones sensibles.
    - Políticas y procedimientos de inventarios de bienes informáticos
    - Políticas y procedimientos de respaldo de datos.
    - Políticas y procedimientos de resguardo de información.
    - Políticas y procedimientos para asignación de usuarios y lineamientos normativos de acceso
    - Políticas y procedimientos para la creación y mantenimiento de *software*.
- *Aspectos formales para la seguridad organizacional*. La existencia de un marco formal de seguridad que debe integrar la organización, formados por una oficina o comité de administración de la seguridad de la información, un oficial de seguridad —*Information System Security Officer*— ISSO, un equipo de recuperación contra desastres, auditorías y revisiones externas a la infraestructura de seguridad así como controles a los servicios de tercerización –*outsourcing*–, entre otros aspectos.
  Algunos de los principales objetivos de control y acciones dentro de este dominio son:
    - Elaboración de diagnósticos de seguridad
    - Establecimiento de personas, áreas o comités específicamente creados para la seguridad informática.
- *Clasificación y control de activos*. El análisis de riesgos utiliza un inventario de activos de información —instalaciones, equipos, programas, datos, personas—, que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado respecto de la información; es decir, los activos deben ser etiquetados de acuerdo con su nivel de confidencialidad y sensibilidad.
  Algunos de los principales objetivos de control y acciones dentro de este dominio son:
    - Definición de políticas y procedimientos claramente establecidos y distribuidos para la realización de inventarios de equipos, programas y procesos, así como para cambios, modificaciones y baja de los mismos.
    - Realización de inventarios y clasificación de activos informáticos en cuanto a infraestructura de equipo de cómputo de alto rendimiento, equipo de comunicaciones, equipo donde se procesa o genera información sensible, equipo cotidiano.
    - Realización de un inventario completo de bases de datos y sistemas y aplicaciones informáticos.

- Establecer y dar seguimiento a la periodicidad de estos inventarios.

- *Seguridad de las acciones del personal.* En este aspecto, la seguridad se orienta a diseñar, implementar y proporcionar controles a las acciones del personal que opera con los activos de información. El objetivo de esta área es contar con los elementos necesarios para mitigar el riesgo de dolo, negligencia o accidente inherentes a la acción humana; es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información. Debe tomarse en cuenta que, según los expertos, las personas son en general el eslabón más débil en la cadena de seguridad informática y son responsables de la mayoría de las fallas [Schneier, 2000].

  Algunos de los principales objetivos de control y acciones dentro de este dominio son:

  - Elaboración de los "perfiles de usuario" con acceso a cada una de las diversas bases de datos y recursos de información de la organización, tanto para el personal como para otros usuarios externos.
  - Establecimiento de normas y políticas de uso correcto de las instalaciones, de los recursos y de la información por parte del personal y usuarios externos, así como correcta difusión de las mismas.
  - Establecimiento de normas y políticas para el uso correcto de las redes y la *Internet*.
  - Establecimiento de normas, políticas y procedimientos para asignación, uso e inhabilitación de cuentas del personal de la organización, así como de otros usuarios.
  - En su caso, diseño y uso de cartas compromiso de confidencialidad –*non disclosure agreement*– con el personal que maneja información confidencial o sensible.
  - Establecimiento de políticas, procedimientos y bitácoras de acceso a las instalaciones y uso de equipo de cómputo para usuarios externos (personal de mantenimiento enviado por proveedores, visitantes, etcétera).

- *Seguridad física y de entorno.* Identificar las instalaciones y los perímetros de seguridad, de forma que se puedan establecer controles del acceso físico a las distintas áreas con equipo, infraestructura y sistemas sensibles, de acuerdo con el tipo de seguridad preestablecida.

  Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- Establecimiento de normas, políticas y procedimientos para regular el acceso restringido a instalaciones, equipos e infraestructura sensibles.
- Establecimiento de normas, políticas y procedimientos para adquirir, instalar y supervisar los elementos recomendados universalmente para seguridad física: energía ininterrumpida, baterías, planta de energía de respaldo, pararrayos, tierras físicas, cortafuegos, climatización, ductos adecuados, restringidos y señalizados, separando los de potencia de los de red; redes redundantes, pisos falsos, circuitos cerrados de televisión, detectores de humo y sistemas profesionales de extinción de incendios, etcétera.

- *Administración de operaciones, comunicaciones y equipo.* Integrar los procedimientos bajo los que opera la infraestructura tecnológica así como los controles de seguridad inherentes documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, control de código malicioso, etcétera.

  Algunos de los principales objetivos de control y acciones dentro de este dominio son:

  - Establecimiento de normas, políticas y procedimientos para regular el acceso a los sistemas y redes: listas de acceso en ruteadores, equipos cortafuegos con programación interna de las políticas que facilitan o deniegan acceso a los usuarios, etcétera.
  - Establecimiento de normas, políticas y procedimientos para regular el acceso a redes estándares, así como a las inalámbricas, las cuales se recomienda que estén todas bajo la modalidad de acceso protegido WPA –*Wi-fi Protected Access*– o semejante.
  - Monitoreo frecuente del acceso a sistemas, aplicaciones y bases de datos.
  - Monitoreo de enlaces a la red y *logs* o bitácoras de memoria de usos y accesos a sistemas operativos y bases de datos, tanto de sus administradores –DBA– como de personal y usuarios en general.
  - Establecimiento de normas, políticas y procedimientos para verificar de la integridad de la información que se crea y almacena.
  - Establecimiento de normas, políticas y procedimientos para

depurar y auditar periódicamente la calidad de los datos contenidos en las bases de datos y archivos digitales de la organización.
    - Establecimiento de normas, políticas y procedimientos para llevar registros de control de acceso a aplicaciones informáticas a través de identificación y autenticación y registros de auditoría.
    - Establecimiento de normas, políticas y procedimientos para llevar bitácoras y controles de fallas de equipos y sistemas.
- *Control de acceso a los sistemas*. Habilitar los mecanismos que permitan monitorear el acceso a los activos lógicos de información, que incluyen los procedimientos de administración de usuarios y sus privilegios, definición de responsabilidades o perfiles de seguridad y el control de acceso y cambios a las aplicaciones y bases de datos.
  Algunos de los principales objetivos de control y acciones dentro de este dominio son:
    - Establecimiento de normas, políticas y procedimientos para regular el acceso a todas las bases de datos y sistemas de información
    - Establecimiento de normas, políticas y procedimientos para creación de cuentas de usuarios de las bases de datos.
    - Establecimiento de normas, políticas y procedimientos para asignación, modificación y baja de contraseñas o *passwords*.
    - Establecimiento de normas, políticas y procedimientos para validación e integridad de datos, así como para depuraciones, descartes / disposiciones periódicas.
    - Establecimiento de normas, políticas y procedimientos para llevar bitácoras de memoria de usos y accesos a las bases de datos.
    - Establecimiento de normas, políticas y procedimientos para acceso a los sistemas y aplicaciones informáticos a través de identificación y autenticación.
    - Establecimiento de normas, políticas y procedimientos para establecer y llevar registros de auditorías informáticas, en especial de la seguridad..
- *Desarrollo de sistemas y su mantenimiento*. La organización debe disponer de procedimientos que garanticen la calidad y seguridad de origen de los sistemas desarrollados para tareas específicas de la organización, así como su mantenimiento periódico.
  Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- Establecer y seguir una metodología estándar para el desarrollo de sistemas de información, como por ejemplo RUP —*Rational Unified Process*— o Proceso Racional Unificado .
- Establecer y llevar procedimientos normados para la etapa de pruebas y liberación de nuevas versiones de sistemas de información.
- Diseñar y establecer un *laboratorio de pruebas* para el monitoreo y evaluación de desarrollos informáticos. Cabe subrayar que estos laboratorios no son instalaciones físicas propiamente, sino ambientes especializados, mayormente procedimentales y estandarizados para las pruebas.
- Establecimiento de procedimientos estandarizados para la creación de manuales de usuario y manuales técnicos de todos los sistemas de información y mantenerlos actualizados.
- Establecimiento de procedimientos estandarizados para el mantenimiento de programas y aplicaciones, control de versiones, gestión del cambio, etcétera.
- Establecimiento de procedimientos estandarizados de permiso a modificaciones y mantenimiento de los sistemas y aplicaciones informáticos a través de identificación y autenticación así como registros de auditorías informáticas.

- *Control de incidentes de seguridad de la información y continuidad de las operaciones de la organización*. La organización debe disponer de procedimientos que garanticen la detección oportuna de incidentes dentro de la seguridad de la información así como los procedimientos para contender con estas contingencias; el sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias graves, garantizando la operación de la organización desde el punto de vista de la información. Estos planes deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar los alcances y eficacia de los mismos.

  Algunos de los principales objetivos de control y acciones dentro de este dominio son:

  - Diseñar y establecer uno o varios "centros maestros" de procesamiento de datos acordes al tamaño de la organización los cuales integren todo tipo de seguridades lógicas, físicas y organizativas construidos o adaptados ex-profeso para manejo adecuado y seguro de bases de datos y archivos de la organización.
  - Diseñar y establecer "centros espejo" o "bases de datos espejo"

o "archivos espejo", supervisando su actualización rigurosa de acuerdo a lo estipulado por la organización del RFE.
- Establecimiento de procedimientos estandarizados en todas las áreas para que lleven reportes de eventos relacionados con la seguridad.
- Establecimiento de procedimientos estandarizados en todas las áreas respecto a la solución de incidentes o escalamiento de los mismos a instancias superiores.
- Recordar periódicamente a todas las áreas que el programa de seguridad es permanente.
- Establecimiento de planes de contingencia, salvaguarda y recuperación de datos

- *Aspectos legales y normativos de la seguridad informática*. La organización acatará las leyes, normas y reglamentos establecidos, y/o establecerá los pertinentes, con que debe cumplir internamente en materia de seguridad, así como los requerimientos de seguridad derivados de estos con los que deben cumplir todos sus proveedores, socios, contratistas y usuarios.

  Algunos de los principales objetivos de control y acciones dentro de este dominio son:
  - Conocer y difundir las leyes, reglamentaciones, normas, etcétera dentro del marco jurídico que rigen y/o afectan a la organización.
  - Revisar y difundir periódicamente las normas y procedimientos específicos relacionados con la seguridad así como sus actualizaciones, tanto al interior de la misma como con proveedores y usuarios externos.
  - Establecer y aplicar procedimientos normativos que rijan la adquisición y/o contratación de bienes y servicios informáticos, especialmente los dedicados a la seguridad informática.
  - Diseñar, establecer y supervisar los mecanismos para verificar el correcto seguimiento de normas, políticas y procedimientos de seguridad informática en todas las áreas de la organización.

Resumen final

Es necesario recordar siempre que en el medio informático, en realidad no existe la "seguridad informática" total ya que el riesgo o probabilidad de

que un evento nocivo ocurra nunca es cero. Hoy en día no existe en el planeta ninguna organización cien por ciento segura y por ello los expertos en el tema prefieren manejar en la actualidad el principio de "administración calculada del riesgo". Esto significa que el proceso de lograr la seguridad informática *nunca está concluido, y nunca es total y absoluto*. Por más que la organización se esfuerce, cada día surgen nuevas amenazas, riesgos y vulnerabilidades dentro de los activos informáticos y por lo mismo el proceso debe ser permanente y evolutivo: siempre será perfeccionable. El riesgo crecerá en proporción al tiempo en el que las medidas de seguridad funcionen adecuadamente y no haya incidentes mayores. La confianza lleva a bajar la guardia y nuevas vulnerabilidades aparecen. Por ello debe continuarse en este esfuerzo permanentemente para mantener al día la metodología, las políticas de seguridad, los procedimientos, los controles y las medidas de seguridad de los activos informáticos manteniendo siempre así un nivel de seguridad adecuado y una *administración del riesgo* razonable; todo ello a un costo proporcional y razonable al valor de los bienes informáticos guardados.

Algunas de las recomendaciones puntuales a este propósito:

- Revisar periódicamente mediante un plan al efecto las normas, políticas, procedimientos y controles de la seguridad informática para perfeccionarlos y mantenerlos actualizados.
- Consolidar un grupo o comité oficial de seguridad informática con personas, funciones y responsabilidades perfectamente establecidas.
- Migrar periódicamente hacia las nuevas versiones de los estándares metodológicos; siguiendo con nuestro ejemplo esto significaría migrar del ISO / 17799 hacia al ISO / IEC 27002 y sus derivados: 27001, 27003, etcétera. Pero ello debe hacerse en cualquier estándar que se hubiese adoptado en la organización. Esto debe hacerse cuando aparezcan y se estabilicen las nuevas ediciones del mismo.
- De los inventarios, auditorías, bitácoras, etcétera se obtienen siempre mediciones acerca de algunas estrategias y controles que siempre faltan de implementar en toda organización o que deben perfeccionarse; debe hacerse una revisión equivalente para evaluar los riesgos y actuar al efecto.
- Establecer los dominios de acción y objetivos que no satisfagan del todo a lo estipulado por la organización e incidir con mayor rigor en ellos.
- Deben implantarse métricas estandarizadas para evaluar a futuro el estado y los avances de la seguridad informática. En este sentido serán útiles metodologías tales como el ISO 27004 o semejantes.

- Todavía es prematuro, pero la tendencia es que en un futuro cercano se buscarán certificaciones de organizaciones acreditadas al efecto. Para el estudio, toma de decisiones y conveniencia de hacerlo, se recomienda revisar los estándares EA-7 03 (de la European Accreditation) así como los nuevos ISO 27006, ISO 27001, ISO 19011 e ISO 17021. Independientemente de que la certificación sea deseada o no por la organización, las metodologías mencionadas serán muy útiles para las actividades de la persona o grupo interno de seguridad de la organización.

Finalmente, es muy importante que recordemos que podemos diseñar entornos de seguridad informática para cualquier organización que no necesariamente requerimos que desemboquen en la preservación de archivos digitales a largo plazo, pero no podemos, –y no debemos– diseñar y construir ambientes de preservación de archivos digitales a largo plazo sin contemplar en ese proyecto y desde el principio la seguridad informática de la organización.

"En Dios confiamos; a todos los demás los escanearemos en busca de virus."

Proverbio de la sabiduría popular

Referencias bibliográficas

* *Todas las referencias electrónicas han sido verificadas como existentes y exactas hasta el 19 de noviembre del 2009.*

"BS 7799-1:1995. Code for Practice for Information Security Management". British Standards Institute. 1995.

"BS 7799-2:1999. Specification for Information Security Management Systems". British Standards Institute. 1999.

"BS 7799-3:2006. Information Security Management Systems. Guidelines for Information Security Risk Management". British Standards Institute. 2006.

Carnegie Mellon. Software Enginnering Institute. 2005. "OCTAVE Methodology - (Operationally Critical Threat, Asset, and Vulnerability Evaluation)". Disponible 19 noviembre, 2009 en: http://www.cert.org/octave/

Duranti, Luciana, and Thibodeau, Kenneth. 2005. "The concept of record in interactive, experiential and dynamic environments: The view of InterPARES". en: *Archival Science*. Springer Netherlands. ISSN:1389-0166 (Print) 1573-7519 (Online). Vol. 5 Nums. 2-4. December 2005. DOI 10.1007/BF02660804. pp. 13-68.

Granger, Sarah. 2009. "Social Engineering Fundamentals, Part I: Hacker Tactics". Security Focus. Disponible 19 noviembre, 2009, en: http://www.securityfocus.com/infocus/1527

Interpares. International Research for Permanent Authentic Records in Electronic Systems. 2005. "Glosario Interpares". Sitio Web oficial del Proyecto "Interpares. Disponible noviembre 19, 2009 en inglés:

http://www.interpares.org/ip2/ip2_term_pdf.cfm?pdf=glossary

En castellano; Sitio Web del TEAM México de Interpares:

http://www.interpares.org/display_file.cfm?doc=ip3_mx_glosario_interpares%2820090318%29.pdf

"ISO / IEC 17799:2000. "nformation technology - Security techniques - Code of practice for information security management". International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). 2000.

"ISO / IEC 17799:2005. Information technology - Security techniques - Code of practice for information security management". International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). 2005.

"ISO / IEC 27001:2005. Information technology - Security techniques - Information security management systems - Requirements". International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). 2005.

"ISO / IEC 27002:2005. Information technology - Security techniques - Code of practice for information security management". (anterior ISO/IEC 17799:2005). International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). 2005.

OCDE. Organización Para la Cooperación y Desarrollo Económico. 2002. "Lineamientos Para la Seguridad de los Sistemas y Redes de Información – Hacia una Cultura de la Seguridad". París: OCDE. 2002. Disponible 19 noviembre, 2009 en: http://www.oecd.org/dataoecd/15/29/34912912.pdf

Schneier, Bruce. 2000. *Secrets & Lies : Digital Security in a Networked World*. John Wiley & Sons, 2000. 432 p. ISBN: 0-471-25311-1.

Voutssas M., Juan. 2007. *Preservación del Patrimonio Documental Digital en México*. México: UNAM, Centro Universitario de Investigaciones Bibliotecológicas. 207 p. ISBN: 978-607-02-583-5.