

Seguridad Informática (Informe)

*Alejandra T. Chavez Flores¹
Octubre 2009*

Resumen

Con la aparición de Internet y su ubicuidad en la vida profesional y privada de las personas, aparecen asociados nuevos riesgos que es necesario evitar o al menos, minimizar. Emerge así el asunto de la Seguridad Informática, que no existe en términos absolutos, se debe tener bien en claro que sólo es posible reducir las oportunidades de que un sistema sea comprometido o minimizar la duración y daños provocados a raíz de un ataque. Cuando se produce un ataque entran en juego tres elementos clave: la confidencialidad, la integridad y la disponibilidad de los datos, junto al impacto en los equipos físicos y en un tema no menor, la reputación de la persona o de la institución. El impacto incluye temas desde posibles pérdidas económicas hasta implicancias legales.

Si bien el tema está internalizado en el ambiente del personal informático capacitado, en muchas oportunidades no se cuenta en las instituciones con una política escrita, formal, de Seguridad Informática. Además, los usuarios finales no están suficientemente concientizados de este asunto. Se hace necesario fortalecer una campaña de alfabetización al respecto, ya iniciada por ejemplo, para el área de la Administración Pública Nacional, por ArCERT (Coordinación de emergencias en redes teleinformáticas).

Los profesionales de la información, no necesariamente están bien instruidos en asuntos de la tecnología de la información. En la opinión de la autora de este informe, sería importante que los mismos contaran, al menos, con una capacitación básica sobre estos temas para poder así enfrentar adecuadamente las situaciones que puedan presentarse durante el desarrollo de sus tareas. Asimismo estarían en mejores condiciones de poder interaccionar con los sectores de informática, sistemas o como se los denomine en cada institución y reclamar la implantación de una política de seguridad formal, en aquellos lugares donde no la hubiera, ya que la misma, siempre y cuando se cumpla, permite estar en una mejor posición para evitar o al menos mitigar, los impactos negativos de un ataque informático.

El presente informe intenta reunir en forma breve, los aspectos más relevantes del asunto, pero la actualización sobre el tema, debe ser de carácter permanente.

¹ Bibliotecaria. Desde 1995 se desempeña como Jefa del Centro de Información del Centro Atómico Constituyentes, Comisión Nacional de Energía Atómica (Argentina). Sus actividades, orientadas a temas de gestión de la información en CyT, incluyen la participación como Coordinadora nacional en la Red Regional de Información en el Área Nuclear y como Oficial de Enlace ante el International Nuclear Information System (INIS). Ha participado en la creación y desarrollo de la Biblioteca Electrónica de CyT del Ministerio de Ciencia, Tecnología e Innovación Productiva de la República Argentina desde el año 2002 hasta el 2006. *chavezflores@gmail.com*

No se han incluido los temas referidos a seguridad física de las instalaciones y amenazas naturales o humanas, únicamente por razones de extensión del informe. Los mismos sin duda alguna, constituyen un elemento importante en el tema de la Seguridad Informática.

Introducción

El presente informe ha sido realizado dentro del trabajo comprendido en la Práctica profesional realizada en CLACSO durante 2009, requisito para acceder al título de Licenciada en Bibliotecología y Ciencia de la Información, orientación Tecnología de la Información, de la Facultad de Filosofía y Letras de la Universidad Nacional de Buenos Aires. Su objetivo es el de presentar en forma sucinta, los aspectos más relevantes de la temática, buenas prácticas, leyes y normativa relacionada, así como también, la bibliografía consultada para su redacción.

La finalidad principal de este documento es la de colaborar en la concientización de personas que no son específicamente de formación informática, para el presente caso profesionales bibliotecarios, de la importancia de saber acerca de los alcances de la Seguridad Informática y cómo este asunto tiene alto impacto tanto en el quehacer diario en el ámbito de trabajo como en las actividades privadas debido a la ubicuidad de Internet. Es necesario entender, por lo tanto, la relevancia de contar, al menos, con una formación básica al respecto.

Cabe aclarar que el presente informe no pretende de manera alguna ser exhaustivo en la temática, sobre todo por ser un asunto que requiere una constante actualización. Por otro lado, no han sido incluidos los temas referidos a seguridad física de las instalaciones y amenazas naturales (fuego, inundaciones, terremotos, etc.) o humanas (maliciosas: fraude, sabotaje, vandalismo o no maliciosas: impericia). Asimismo, si bien fueron consultadas varias fuentes, es de destacar que la mayor información fue recabada de la documentación producida por ArCERT que se encuentra disponible para su consulta en: <http://www.arcert.gov.ar/index.html>

Seguridad Informática

Al abordar el tema de Seguridad Informática, se debe tener muy en claro que no existe una seguridad en términos absolutos. Sólo se pueden reducir las oportunidades de que un sistema sea comprometido o minimizar la duración y daños provocados a raíz de un ataque.

Al tratar el asunto, se está considerando que se encuentran en riesgo tres elementos:

a) Los datos: información guardada en las computadoras.

Ellos tienen tres características a proteger:

- Confidencialidad
- Integridad
- Disponibilidad

b) Los recursos: el equipamiento en sí mismo

c) La reputación

Una de las actividades iniciales es el Análisis de riesgos, para lo cual, se debe realizar un modelado de amenazas. Se trata de una actividad de carácter recurrente.

Un riesgo es una combinación de activos, vulnerabilidades y atacantes.

Elementos

- Lo que se quiere proteger: los activos
- Objetivos de seguridad: niveles y tipos de protección que requiere cada activo.
 - **confidencialidad** de los datos: se garantiza que la información es accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
 - **integridad** de datos y sistemas: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
 - **disponibilidad** del sistema/red: se garantiza que las personas usuarias autorizadas tengan acceso a la información y recursos relacionados con la misma toda vez que se requiera.
- Amenazas²
- Motivos: financieros, políticos, personales/sicológicos.

Bauer propone utilizar por ejemplo:

- **Análisis simple de riesgos:** cuando se han identificado los activos, vulnerabilidades y algunos posibles atacantes, se deberá correlacionarlos y cuantificarlos. Una forma sencilla es calcular las Expectativas de Pérdidas Anualizadas (ALEs, *Annualized Loss Expectancies*) donde para cada vulnerabilidad asociada a sus activos se debe estimar:
 - Su Expectativa de Pérdida Individual (SLE, *Single Loss Expectancy*) donde se estima el coste de sustituir o recuperar ése activo.
 - El Ratio Anual de Ocurrencias esperadas (ARO, *Annual Rate of Occurrence*)

Luego se multiplican esto ratios para obtener las Expectativas de Pérdidas Anualizadas de esa vulnerabilidad (ALE)

Es decir, para cada vulnerabilidad se calcula:

$$\text{SLE} \times \text{ARO} = \text{ALE (coste/año)}$$

Se estima luego las Ocurrencias Anuales Esperadas (EAO, *Expected Annual Occurrence*) que se expresan en número o fracción de incidentes por año. Este valor se multiplica con el obtenido anteriormente de donde se obtendrá, para el incidente considerado, el coste por año.

En este tipo de análisis será de gran utilidad añadir ALEs asociados a una misma vulnerabilidad.

² Ver: Cohen, F. et al: *A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model.*

<http://www.all.net/journal/ntb/cause-and-effect.html>

Si bien este método involucra un elemento de subjetividad es muy útil para enumerar, cuantificar y valorar riesgos como así también, para focalizar los gastos de seguridad informática y preparar los presupuestos correspondientes.

- **Árboles de ataque:** desarrollados por Bruce Schneier. Se trata de una representación visual formal y metódica sobre la seguridad de los sistemas basados en las variantes de los ataques (los ataques posibles contra un determinado objetivo). Se representan mediante estructuras de árboles donde se denomina nodos raíz a la meta (el objetivo a atacar) y las diferentes maneras de lograr dicha meta se denominan nodos hojas. Una vez diseñado, se añaden los costes al árbol para estimar las pérdidas que podrían suponer los diferentes ataques.

Hay que tener en consideración que los ataques pueden ser direccionados a:

- Servidores
- Red
- Aplicaciones web

Estrategias generales para minimizar los ataques

- ✓ Observar el principio del menor privilegio
- ✓ Defensa a fondo o en profundidad
- ✓ Redundancia: utilizar más de un mecanismo de seguridad
- ✓ Punto de choque
- ✓ Eslabón más débil
- ✓ Postura de falla segura
- ✓ Definición y uso de políticas y procedimientos
- ✓ Mantenerse informado/actualizado

SERVIDORES

Ataques a servidores

- Servidores Web: Utilización de vulnerabilidades conocidas que posibilitan ejecutar código arbitrario, acceso no autorizado a archivos o denegación de servicio (DoS).
- Servicios de administración remota: Telnet, SSH, Microsoft Terminal Server.
- Servicios de administración de contenidos: FTP, SSH/SCP, etc.
- Servidores de Nombres: ataque al servidor, modificación de zonas, *cache poisoning*, etc.
- Servidor de correo electrónico: interceptación de datos confidenciales; *spam*; propagación de virus, apropiación del servidor de correo para lanzar otros tipos de ataque, etc.
- Servidor de bases de datos: problemas tales como compromiso del servidor (por ej. por desbordamientos de búfer); robo de datos; corrupción de datos o pérdida, denegación de servicio (DoS), etc.

- Navegadores: fallas que permiten ejecutar código arbitrario en el cliente, controlando parcial o totalmente el equipo: *Cross site scripting*, manipulación de *cookies*, robo de código fuente, etc.

Como protegerse

Utilización de buenas prácticas:

- ✓ Fortalecimiento (*hardening*) o aseguramiento de las instalaciones del sistema operativo
- ✓ Deshabilitación de servicios y cuentas no utilizados
- ✓ Administración remota segura. Cifrado del tráfico
- ✓ Utilizar sistemas de búsqueda automática de vulnerabilidades: por ej. NISSUS
- ✓ Actualizaciones del sistema operativo y aplicaciones (parches)
- ✓ Utilización de herramientas que buscan y detectan problemas de seguridad; detectan intrusos y controlan cambios.
- ✓ Análisis periódico de *logs*

RED

Como protegerse

- ✓ Uso de arquitectura de red seguras: buen diseño de perímetros de red
- ✓ Separar los sistemas que tienen un alto riesgo de ser comprometidos: creación de zona desmilitarizada (DMZ), de arquitectura “fuerte”, con servidores fortalecidos y monitoreados.
- ✓ Redundancia
- ✓ Filtrado de paquetes incluso en enrutadores externos
- ✓ Instalación de cortafuegos (*firewalls*) configurados cuidadosa y minuciosamente.
- ✓ Atención y vigilancia continua y sistemática

APLICACIONES

Aplicaciones Web

Ataques a mecanismos de seguridad

- Obtención de usuario y clave con diccionario o fuerza bruta

Como protegerse:

- ✓ Utilización de contraseñas “fuertes”
- ✓ Política de cambio frecuente de contraseñas
- ✓ Mecanismos de deshabilitación temporal de la cuenta

Ataques a las aplicaciones (mal desarrolladas)

- Ataques de entrada no validada. Por ej.: modificación de atributos enviados por el servidor, inyección de comandos SQL, inyección LDAP, explotación de *Buffer overflow*, *Cross Site Scripting* (XSS), etc.

Como protegerse:

- ✓ Desarrollo seguro de aplicaciones: uso de buenas prácticas y principios de diseño, tener en cuenta la seguridad desde el inicio, construcción de distintas capas de defensa, manejo apropiado de los errores, fallo en forma segura,
- ✓ Desconfiar siempre de la información enviada por el cliente y por lo tanto asegurar que toda la información que envíe sea validada por la aplicación en el servidor antes de ser utilizada.
- ✓ Definir estrictamente que datos/formato de entrada están permitidos y chequear cada parámetro que entra contra dichas definiciones.
 - Por ej.: caracteres permitidos, tipo de datos (entero, cadena, fecha), longitud mínima y máxima, rango numérico, según patrones, etc.

Ataques a mecanismos de autenticación

- Robo de cookies (via XSS), predicción de ID de sesión, inyección de comandos SQL para saltar formularios de *login* de la aplicación, etc.

Lo mencionado anteriormente es responsabilidad específica de personal informático capacitado, sin embargo, es necesario asegurar que el personal que no sea informático tenga al menos una noción general del tema de seguridad informática para tener mayor conciencia y compromiso, desde su rol y puesto de trabajo dentro de la organización. Existen buenas prácticas que como usuarios/as deberían ser observadas en las tareas diarias:

Manejo responsable de claves de acceso:

- ✓ selección de claves “fuertes”, difíciles de descifrar
- ✓ mantenerlas en secreto
- ✓ no transferirlas
- ✓ no escribirlas en papeles de fácil acceso, en archivos sin cifrar.
- ✓ no habilitar la opción “recordar clave en este equipo”, que ofrecen los programas
- ✓ no enviarla por correo electrónico
- ✓ cambiarla frecuentemente

Práctica de “escritorio limpio”

- ✓ evitar dejar información sensible³ a disposición de personas no autorizadas
- ✓ guardar bajo llave documentación importante
- ✓ evitar de dejar en lugares visibles y fácilmente accesibles *pendrives*, CDs, etc. con información sensible

Resguardo de la pantalla

- ✓ No dejar desatendido el equipo
- ✓ Bloquear la PC si se abandona, aunque sea momentáneamente, el puesto de trabajo.

Navegación en Web, buenas prácticas.

³ Información sensible: datos de empleados, contratos, números de cuentas, claves, etc.

- ✓ Evitar acceder a sitios desconocidos o no confiables.
- ✓ No aceptar la instalación automática de software.
- ✓ No descargar archivos ejecutables.
- ✓ No dejar información sensible en páginas o foros.
- ✓ Si debe enviar información sensible:
- ✓ Solo hacerlo en sitios seguros (https)
- ✓ Verificar el certificado del sitio.
- ✓ Consulte con su administrador sobre configuración segura del navegador.
- ✓ Verificar el destino de los enlaces

Uso responsable y seguro del correo electrónico

Se debe estar informado de las diferentes maneras en que se puede generar situaciones donde se pone en peligro la seguridad. Por ejemplo:

Ingeniería Social

Es un conjunto de trucos, engaños o artimañas que permiten confundir a una persona para que entregue información confidencial, ya sea los datos necesarios para acceder a ésta o la forma de comprometer seriamente un sistema de seguridad.

Código Malicioso: virus, troyanos, gusanos, etc.

Programa de computadora escrito para producir inconvenientes, destrucción, o violar la política de seguridad

Buenas prácticas

Archivos adjuntos

- ✓ No abrir archivos adjuntos de origen desconocido.
- ✓ No abrir archivos adjuntos que no esperamos recibir, aunque nos parezca que su origen es conocido.
- ✓ No abrir adjuntos que tengan extensiones ejecutables.
- ✓ No abrir adjuntos que tengan más de una extensión.
- ✓ Chequear con el remitente la razón por la cual nos envió un archivo adjunto.
- ✓

Reenvío de correo electrónico

- ✓ Borrar la/s dirección/es de correo del/los remitente/s
- ✓ mejor aún: copiar el contenido del correo original y armar uno nuevo
- ✓ Si se reenvía a más de una persona, utilizar la opción de enviar "Copia Oculta"
- ✓ No ser un reenviador compulsivo de correos electrónicos

SPAM: mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas.

- ✓ No dejar la dirección de correo electrónico en cualquier formulario o foro de Internet.
- ✓ No responder correos no solicitados. Lo más seguro es borrarlos.
- ✓ En general, no conviene enviar respuesta a la dirección que figura para evitar envíos posteriores.

- ✓ Configurar filtros o reglas de mensaje en el programa de correo para filtrar mensajes de determinadas direcciones.
- ✓ Nunca configurar “respuesta automática” para los pedidos de acuse de recibo.
- ✓ No responder a los pedidos de acuse de recibo de orígenes dudosos

Pishing: solicitud de datos confidenciales

- ✓ Comunicarse telefónicamente con la Empresa, para confirmar el supuesto pedido.
- ✓ Nunca enviar por correo información confidencial sin cifrar.
- ✓ Verificar el origen del correo.
- ✓ Verificar el destino de los enlaces.

Cadena de correo electrónico

Una de las herramientas que se utilizan comercialmente para obtener direcciones de correo electrónico y armar bases de datos con las mismas es armar cadenas de correos electrónicos.

Conforman también una oportunidad a los piratas informáticos, pues obtienen blancos reales a los que enviarles virus y todo tipo de software malicioso.

Hoax: engaño/broma.

Se presentan por ejemplo como:

- ✓ Alertas sobre virus “incurables”
- ✓ Mensajes de temática religiosa
- ✓ Cadenas de solidaridad
- ✓ Cadenas de la suerte
- ✓ Leyendas urbanas
- ✓ Métodos para hacerse millonario
- ✓ Regalos de grandes compañías

Políticas de seguridad

Existen dos posturas fundamentales respecto de las decisiones y políticas de seguridad:

- a) Postura de negociación preestablecida: se especifica sólo lo que se permite y se prohíbe todo lo demás. Es decir: *lo que no está permitido expresamente, está prohibido*, constituyendo por lo tanto una postura de falla segura. Los diferentes servicios se van activando según el caso.
- b) Postura de permiso preestablecido: se especifica sólo lo que se prohíbe y se permite todo lo demás.

Con referencia a el establecimiento de políticas en materia de seguridad informática, en el ámbito de la administración pública nacional, la ONTI (Oficina Nacional de Tecnología de la Información dependiente de la Secretaría de la Función Pública) aprobó mediante la [Disposición N° 006](#) del 3 de agosto de 2005 la Política de Seguridad de la Información Modelo (versión 1), en el cual deben basarse los Organismos para dictar o adecuar sus

políticas de seguridad, de acuerdo a lo dispuesto por la [Decisión Administrativa 669/2004](#) y la [Resolución SGP 45/2005](#).

<http://www.arcert.gov.ar/politica/modelo.htm>

http://www.arcert.gov.ar/politica/Presentacion_DA_669-04.ppt

Enlaces de interés:

Coordinación de emergencias en redes teleinformáticas. ArCERT

<http://www.arcert.gov.ar/index.html>

Dirección Nacional de Protección de datos personales:

<http://www.jus.gov.ar/dnppd>

Ministerio de Justicia, Seguridad y Derechos Humanos. Dirección Nacional de Protección de datos personales.

<http://www.jus.gov.ar/dnppdnew/>

<https://seguridadinformatica.sgp.gob.ar/>

Cybsec Security Systems S. A. (privado)

<http://www.cybsec.com/ES/>

Legislación

Importante: los enlaces son a los textos de las normas consultadas entre agosto y octubre de 2009, por lo tanto se recomienda confirmar actualizaciones realizando la búsqueda en Infoleg:

<http://www.infoleg.gov.ar/>

Política de Seguridad de la Información

Decisión Administrativa 669/2004

<http://infoleg.mecon.gov.ar/infolegInternet/anexos/100000-104999/102188/norma.htm>

Protección de datos personales:

Constitución Nacional, Art. 43.

Ley 26.343 (Ley N° 25.326. Modificación)

<http://www.infoleg.gov.ar/infolegInternet/anexos/135000-139999/136483/norma.htm>

Ley 25.326 y su decreto reglamentario 1558/2001

Disposiciones de la DNPDP (Dirección Nacional de Protección de datos personales)

<http://www.jus.gov.ar/dnppdnew/>

Ley 26.388 Delito informático (Modificación al Código Penal)

<http://www.infoleg.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm>

Firma digital:

Firma digital argentina

<http://www.pki.gov.ar/>

Ley 25.506

<http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm>

Decreto 2628/2002

<http://infoleg.mecon.gov.ar/infolegInternet/anexos/80000-84999/80733/norma.htm>

Decreto 724/2006

<http://infoleg.mecon.gov.ar/infolegInternet/anexos/115000-119999/116998/norma.htm>

(Ver normativa completa en el sitio de Firma digital argentina)

Protección jurídica del software y las bases de datos:

Ley 24.766, llamada de confidencialidad de la información, que protege a ésta sólo cuando importa un secreto comercial.

<http://www.infoleg.gov.ar/infolegInternet/anexos/40000-44999/41094/norma.htm>

Ley 24.769, de delitos tributarios, que brinda tutela penal a la información del Fisco Nacional a fin de evitar su supresión o alteración.

<http://www.infoleg.gov.ar/infolegInternet/anexos/40000-44999/41379/texact.htm>

Ley 11.723 luego de sanción de la ley 25.036 ha extendido la protección penal al software.

<http://www.infoleg.gov.ar/infolegInternet/anexos/40000-44999/42755/texact.htm>

Derecho de autor:

Ley 24.870

Modificación de los artículo 5° y 84 de la Ley 11.723.

<http://www.infoleg.gov.ar/infolegInternet/anexos/45000-49999/45758/norma.htm>

Otras leyes de interés

Ley 25.164 Ley Marco de Regulación del Empleo Público Nacional

Obligaciones de los funcionarios públicos

<http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/60458/norma.htm>

Convenio Colectivo de Trabajo General.

Ley 25.188 Ética en el ejercicio de la Función Pública

<http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/60847/texact.htm>

Código de ética de la Función Pública

<http://www.infoleg.gov.ar/infolegInternet/anexos/55000-59999/55841/norma.htm>

<http://www.anticorrupcion.gov.ar/41-99.pdf>

Ley 24.624 Art. 30

<http://infoleg.mecon.gov.ar/infolegInternet/anexos/30000-34999/31692/norma.htm>

Decisión Administrativa 43/96

<http://www.mecon.gov.ar/digesto/decadm/1996/decadm43.htm>

Normas

Serie ISO/IEC 27000 se resalta:

ISO/IEC 27001 Sistema de Gestión de Seguridad de Información

Antecedente de la serie: **ISO 17799**

Esta familia de normas tiene relación con las series:

ISO 9000

ISO 14001

<http://www.iso.org>

Otras normas de interés:

Serie ISO/IEC-13335-1 (2004): Conceptos y modelos para la seguridad de TI.

Entrevistas

La siguiente sección registra la información recabada a través de tres entrevistas.

A) Entrevista con personal del sector de Informática del Dpto. de Física de la Comisión Nacional de Energía Atómica (CNEA)

Ing. Luis Rémez

Lic. Norberto De Luca

Durante esta primera entrevista no se trabajó en base a preguntas ya establecidas, sino que fue abierta y tuvo como finalidad entrar en tema y ver que asuntos no considerados podían surgir durante la interacción, es decir, un objetivo exploratorio.

Se focalizó en los temas de aseguramiento de servidores, uso del SSH, conocimiento de los usuarios finales acerca de problemas de seguridad, entre otros.

De dicha interacción se destaca lo siguiente:

Se recomienda el uso de formularios Web en lugar de conexiones SSH, para todos aquellos casos en que se trata de acciones predeterminadas por parte del usuario, y conocidas de antemano. Sin embargo se debe tener especial atención a los problemas de seguridad tales como *SQL Injection*.

De ser necesario conexiones de control remoto cuando no se conocen de antemano las acciones del usuario, como por ejemplo control de experimentos a distancia, se recomienda la colocación de un servidor a donde obligatoriamente primero deban entrar y registrarse todos los usuarios, servidor que estará fortalecido y por lo tanto controlado en cuanto a configuración, actualización de parches, etc., lo que evita la entrada directa desde múltiples equipos de los que se desconoce si están bien configurados, actualizados y fortalecidos.

Se mencionó, asimismo, la importancia de contar con usuarios alertados sobre los problemas de seguridad dado que muchas veces, son víctimas de su ingenuidad.

Si bien es difícil contar con una política de seguridad escrita, se destacó la importancia del uso de buenas prácticas, del monitoreo y de la permanente actualización por parte de los administradores.

B) Entrevista con personal del Dpto. Tecnología de la Información de CNEA
Lic. Patricia Binaghi. Jefa del Grupo Transmisión de Datos.

Se tuvo como base para esta entrevista un primer listado breve de preguntas que se presentan a continuación con las respectivas respuestas. La interacción se centró más en los aspectos de lo que deber ser cumplido en los organismos de gobierno. También se conversó sobre el rol del ArCERT (Coordinación de Emergencias en Redes Teleinformáticas)

1) ¿En su experiencia, como se comportan los sectores informáticos de instituciones en la Argentina? Están plenamente concientizados del tema de seguridad?

Están concientizados pero deben luchar para lograr la implantación de una cultura de la seguridad informática sobre todos con los niveles superiores, de dirección institucional.

Esto implica en lo formal, la implantación de una Política de Seguridad Informática, para la Administración Pública (APN), de acuerdo a la Decisión Administrativa 669/2009.

El porcentaje de instituciones de la APN que han cumplido, es bajo.

2) ¿A nivel académico, como se trata el tema en los cursos de instalación de Linux, por ejemplo?

Los temas de seguridad en general no se dan desde el principio, aunque sería importante hacerlo desde el inicio para fijar la importancia del asunto.

3) ¿Es necesario tener una política de seguridad, escrita?

Sí, en los organismos de la APN está formalizado por la Decisión Administrativa 669/2004. Todo deber estar por escrito: la filosofía, responsabilidades, procedimientos, etc.

4) ¿Cuál podría ser el papel del sector de servicios de información (biblioteca, centro de documentación, biblioteca digital, etc.) con respecto a los temas de seguridad y hasta donde debe recabar información del sector informático?

Deberían tener el rol de usuarios, pero en la realidad, por falta de personal informático, se produce una descentralización donde cada sector tiene su propio personal, resultando difícil la observación de buenas prácticas y su control.

No deberían tener que preocuparse por aquellos temas seguridad reservados al personal informático pero sí en la observancia de buenas prácticas de seguridad informática como usuarios.

5) Que es ArCERT?

ArCERT, creado en 1999 por Resolución SFP Nro 81/99, dentro del ámbito de la Secretaría de la Gestión Pública, es un organismos cuyas funciones principales son es actuar en respuesta ante incidentes de seguridad (ataques o intentos de penetración) en redes donde se haya afectado a recursos informáticos de la Administración Pública Nacional (APN) así como también difundir información para neutralizar dichos incidentes ya sea de manera preventivo o correctiva y capacitar a personal técnico que trabaja en redes de las instituciones del sector público a nivel nacional. Asimismo centraliza la información, promoviendo su intercambio, sobre incidentes de seguridad ocurridos en la APN, asesora sobre los temas de su incumbencia y promueve la coordinación entre las instituciones para la prevención, detección, manejo y recupero de incidentes de seguridad.

Durante la entrevista se conversó también, sobre posibles diseños de arquitectura segura para la provisión de servicios de información (por ej. bibliotecas digital, repositorios institucionales, etc.).

C) Entrevista al Ing. Juan A. Jolís (EducAR)

En este caso, la entrevista se realizó en forma conjunta con el Lic. Fernando López, de la Biblioteca Virtual de CLACSO. Se tomó como base una segunda lista de preguntas, más extensa que la primera.

1) En su experiencia ¿cómo se comportan los sectores informáticos de instituciones en la Argentina? ¿Están plenamente concientizados del tema de seguridad?

Hablando de las instituciones con las cuales he tenido contacto, las áreas técnicas conocen los riesgos, tanto en el sector público como en el privado. Luego, dentro de cada institución es diferente el grado de aplicación que le asigna al asunto o que se le puede asignar. A partir del año pasado se inició desde el Sector de la Administración Pública, la Semana de la Seguridad Informática, tratando de fomentar, en especial, en el ámbito gubernamental, la concientización sobre el tema a través de seminarios, capacitación interna, etc.

A nivel de usuario es muy bajo el nivel de concientización, sólo un 5%. La realidad es que aún dentro de las áreas de sistemas no hay por lo general una política de seguridad escrita, existen recomendaciones y sólo comenzó siendo una obligación en las instituciones bancarias. Un tema a tener muy en cuenta es el de la Ley de datos personales, tema delicado incluso para los bibliotecarios. Cuando se administran datos personales hay que tener en cuenta ciertas normas. Hay una responsabilidad legal con respecto a los datos sensibles, tales como afiliación a un sindicato, religión, etc. Se los puede tener registrados (ya sea en papel, una planilla electrónica, una base de datos) pero se debe garantizar que se hace todo lo necesario y posible para protegerlos. Aunque se tenga datos personales no sensibles, hay que tener el compromiso de informar al usuario que se guardan dichos datos, y que tiene el derecho a saber cuales son, que puede solicitar su modificación, pedir que se borren, etc. El usuario cede los datos, pero sigue siendo el dueño, y sólo para un determinado fin. Sino, puede reclamar ante la Comisión de Protección de Datos Personales la que se contactará con el organismo en cuestión. Las bases que contienen datos personales sensibles, deben ser declaradas ante dicha Comisión. Hubo un plazo para que las entidades bancarias, privadas, organismos públicos, etc. regularizaran su situación. Hay que tener en cuenta que se deben resguardar también aquellas en papel, hojas firmadas por empleados, etc. es decir, lo que aún no esté informatizado.

El dueño de los datos, de ser necesario, puede presentar una demanda si considerar que sus derechos han sido violados.

Por lo que, en cada organismo, se debería tener acuerdos por escrito donde se estipule: que datos se aportan, como se aportan, que derechos hay, que responsabilidades, etc.

2) ¿Es necesario tener una política de seguridad escrita?

Dentro del ámbito público el Modelo de política de seguridad informática, del ONTI contiene los lineamientos de la misma, el ABC del tema, organizado en secciones comenzando por la capa física. Dichas recomendaciones básicas, generales constituyen en puntapié inicial luego el límite, hasta donde se quiere y se puede llegar lo determina cada institución.

Lo básico para exigir a los informáticos es tener redactada una política, que debe ser algo vivo, un documento escrito, consensado por los jefes, con amplia participación del área de Sistemas. Lo que suele pasar en la realidad, es que por lo general no existe dicha política por escrito en las instituciones, tan sólo existen políticas orales.

Es recomendable tener una persona específica cuando el plantel de personal de Sistemas ya es muy grande.

Con respecto a software libre, Linux por ejemplo, todo lo referido a capacitación en seguridad se puede encontrar en Internet, pero demanda muchas horas de trabajo y pruebas, un curso de capacitación es una inyección de conocimientos, luego hay que continuar.

En el caso de los licenciados se puede llamar y hay respaldo, sin embargo no recomendaría colocar un servidor expuesto a Internet con un software comercial.

Debería estar en claro cual es el alcance, cuales son las incumbencias del informático, si le toca decidir las políticas, por ley los administradores de sistemas son punibles penalmente, por ejemplo si atentan contra la comunicación entre los usuarios, esto es:

leer los correos electrónicos o eliminar los correos de un usuario constituye una interferencias en la comunicación entre dos personas. Sin embargo pueden presentarse casos donde el administrados deba borrar correos que están "en cola" y que ponen al sistema en situación de inminente colapso.

Por otro lado, si hubiera sospecha de envío hacia afuera de información confidencial, se deberá presentar un recurso y solicitar un allanamiento.

Debería sin embargo, haber un documento de la institución donde se detalle por escrito todo lo que es propiedad de la institución, por ejemplo si los contenidos de los correos electrónicos del personal se consideran como propiedad de dicha institución, por ejemplo.

Este tipo de documentos debe ser conocido por todo el personal, que podrá estar o no de acuerdo.

3) ¿Cual sería la mejor forma de abordar el tema de un seguimiento de los temas de seguridad informática cuando se dispone de poco personal? ¿A quien "sobrecargar"?: a los que hacen el soporte técnico y administran los servidores o al que está con tareas de desarrollo/localización de soft?

A ambos:

Los desarrolladores deberán tener en cuenta los mecanismos necesarios para hacer seguras las aplicaciones que desarrollan o bien "customizan" (adaptan) para su uso.

Soporte técnico deberá supervisar los temas relacionados con seguridad de acceso en las estaciones de trabajo, actualizaciones del sistema operativo de un puesto, y gestión de antivirus como mínimo.

Los administradores de servidores y redes deberán estar atentos a las actualizaciones de firmware o de sistema operativo al margen de custodiar, controlar y resguardar la información que se transmite o deposita en los equipos de su dominio.

4) ¿Es posible conocer el diseño de la red institucional por parte del sector de Biblioteca?

En realidad el conocer como es la arquitectura es patrimonio del área de Sistemas y debe ser algo confidencial, saber la arquitectura no es conveniente, pues hay estadísticas de casos en donde personal interno, de la propia institución, es el que ha causado problemas.

Si existe una política de seguridad por escrito y si dice, por ejemplo, que debe haber una barrera, y además se cuenta con auditorías, se debería estar tranquilo.

5) ¿Que puntos clave se deberían tener en cuenta en la selección de un software de biblioteca digital/Repositorio institucional, desde el punto de vista de la seguridad informática?

Por ejemplo usuario y clave no debe ser accesible para nadie; el usuario de aplicación, debe estar enmascarado en un único usuario que se comunica con la base de datos; abrir sólo lo que sea necesario; observancia de buenas prácticas para el desarrollo de software.

6) ¿Sería buena idea proponer actividades de tipo seminario para tratar el tema de seguridad informática orientadas a bibliotecarios?

Siempre es buena idea, cualquier usuario de un equipamiento informático debe recibir un mínimo de capacitación. En el caso de los bibliotecarios hay que determinar que es lo que sería más conveniente para dicha capacitación.

7) Sistema de copias de seguridad (*backup*): recomendaciones, cosas que se debe olvidar.

Nosotros utilizamos software "Bacula". Lo más importante: los datos, los fuentes, compilados y los instaladores de todo software involucrado incluyendo en todos los casos los entornos que existieran (desarrollo, test y producción). Se debe hacer una prueba periódica para garantizar la disponibilidad de los mismos o bien auditarlos.

8) ¿Es recomendable y en que casos, frecuencia, alcance, etc., realizar una auditoria de seguridad informática?

Toda vez que el bien involucrado así lo justifique.

Durante la entrevista se conversó también, sobre posibles diseños de arquitectura segura para la provisión de servicios de información (por ej. bibliotecas digitales, repositorios institucionales, etc.).

Bibliografía consultada:

ArCERT. Fundamentos de la seguridad de la información. (Reuniones 1-3). En: Manual del Instructor de Seguridad de la Información. 2007.

http://www.arcert.gov.ar/webs/manual/arcert_manual_instruct_seginf.zip

ArCERT. Reforzando la instalación de Debian GNU/Linux. ArCERT, Subsecretaría de la Gestión Pública, 2006.

ArCERT. Recomendaciones para el uso seguro del correo electrónico, ArCERT, Subsecretaría de la Gestión Pública, 2006.

http://www.arcert.gov.ar/webs/tips/recomendaciones_email.pdf

ArCERT. Recomendaciones para evitar ser victima del "phishing", ArCERT, Subsecretaría de la Gestión Pública, 2006.

http://www.arcert.gov.ar/webs/tips/recomendaciones_phishing.pdf

ArCERT. Manual de seguridad en redes. Buenos Aires, ArCERT, 1999.
www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

Bauer, Michael. Seguridad en servidores Linux. Madrid, Anaya Multimedia, 2005.

Biscioni, Fernando. Panorama de riesgos en el uso de las tecnologías. Buenos Aires, ArCERT, 2009.

[http://www.arcert.gov.ar/ncursos/material/Panorama de Riesgos Tecnologias v4.pdf](http://www.arcert.gov.ar/ncursos/material/Panorama_de_Riesgos_Tecnologias_v4.pdf)

OCDE. Directrices de la OCDE para la seguridad de sistemas y redes de información. Hacia una cultura de seguridad.

http://www.csi.map.es/csi/pdf/ocde_directrices_esp.pdf

Oficina Nacional de Tecnologías de la Información. Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional. Buenos Aires, ONTI, 2005.

http://www.arcert.gov.ar/politica/PSI_Modelo-v1_200507.pdf

Oppliger, Rolf. Internet Security: Firewalls and Beyond. Communications of the ACM. May v. 40, no. 5, 1997.

OWASP. Las diez vulnerabilidades más críticas en aplicaciones Web. 2004.

http://www.arcert.gov.ar/webs/textos/OWASP_Top_Ten_2004_Spanish.pdf

Toxen, Bob. The Seven Deadly Sins of Linux Security. ACM QUEUE, May-June 2007, p. 39-43

Zwicky, Elizabeth. Construya firewalls para internet. México, McGraw-Hill, 1997.