No.21 / junio-julio 2014 ISSN: 1251478, 1251477

.Seguridad 21

Cultura de prevención para TI

Java y otras tecnologías

Renovación para viejos conocidos

Criptografía en hardware | Autorregulación y privacidad | (In)seguridad en Java | Cómo superar Windows XP | Concienciar para prevenir | Dispositivos móviles

Contenido

.Seguridad
Cultura de prevención para TI

Editorial

Java y otras tecnologías

Renovación para viejos conocidos

México es una comunidad consolidada en el uso de tecnologías de la información y aún así no tenemos una cultura de seguridad establecida, aprendemos a usar un dispositivo antes de aprender sobre seguridad y privacidad. Cuando niños, antes de cruzar la calle por uno mismo, nos enseñaron a mirar los semáforos, voltear a ambos lados de la carretera y después cruzar. En el caso del uso de tecnologías de información, hemos llegado a la madurez sin pasar por la etapa de la prevención. No aprendimos a mirar a ambos lados pero vamos y venimos de todas las carreteras.

En esta edición hacemos una reflexión sobre tecnologías que son ya bien conocidas en el ámbito de TI pero que siguen provocando dolores de cabeza a usuarios y profesionales cada vez que se habla de seguridad informática. La información corporativa en dispositivos móviles ha cobrado gran auge este año, conocemos Java desde mediados de los 90, a raíz de las declaraciones de Edward Snowden la criptografía se volvió tendencia, Windows XP estuvo en el mercado durante 12 años y como CERT de la UNAM, hemos predicado la cultura de seguridad desde nuestros inicios.

Te invitamos a conocer estas propuestas de renovar a los viejos conocidos, de transformar la tecnología de nuestro quehacer diario y sobre todo, de evolucionar nuestra conciencia de seguridad informática.

L.C.S Jazmín López Sánchez
Editora
Coordinación de Seguridad de la Información

.Seguridad
Cultura de prevención para TI

.Seguridad Cultura de prevención TI M.R. / Número 21 / junio - julio 2014 / ISSN No. 1251478, 1251477 / Revista Bimestral, Registro de Marca 129829

Criptografía basada en hardware

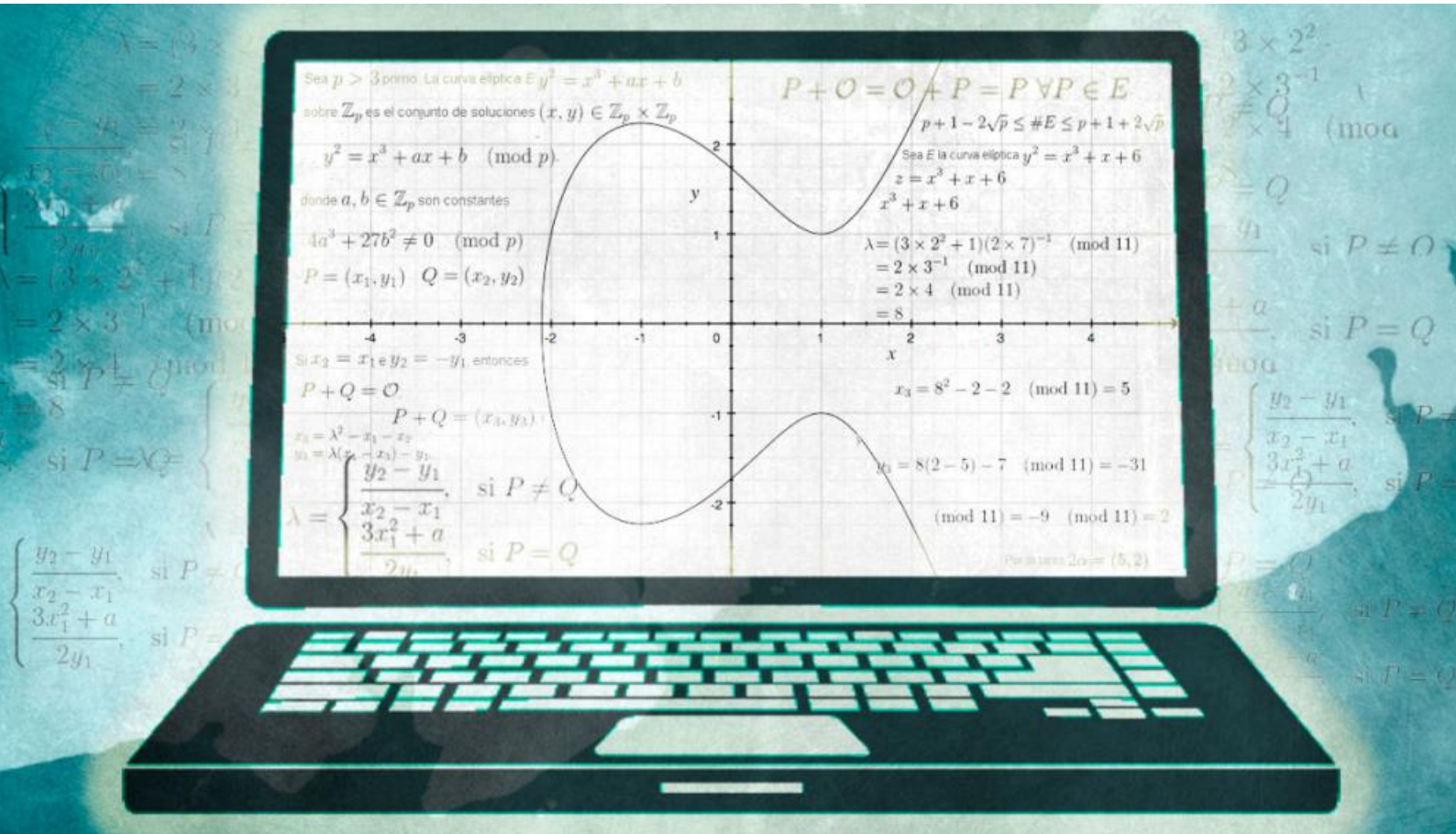
Eduardo Palma Ávila

Hoy en día la criptografía juega un papel fundamental en la protección de datos. Esta ciencia que data de hace miles de años es utilizada para proporcionar confidencialidad, integridad, autenticación y no repudio a la información que se encuentra almacenada en cualquier medio electrónico, que viaja a través de una red de datos o que está siendo utilizada en tiempo real.

Su evolución ha sido marcada por la necesidad de ocultar la información y hacerla visible sólo a personas autorizadas, asimismo, por atacantes no autorizados que analizan métodos y algoritmos matemáticos en busca de la clave que les permita tener acceso a los datos para obtener algún beneficio. Es por ello que se busca utilizar algoritmos más robustos, para hacer la tarea más difícil (más no imposible) a los criptoanalistas que trabajan día a día en vulnerar estos métodos matemáticos.
El poder computacional que tenemos en la actualidad nos permite realizar implementaciones de ciertos métodos matemáticos en cualquier PC. Lenguajes de programación como Java, C# y .NET poseen rutinas ya desarrolladas de algoritmos como DES, TripleDES, AES y RSA, lo cual facilita enormemente el uso de la criptografía. A la vez, este mismo poder computacional está siendo utilizado para romper los algoritmos.

Se recomienda utilizar llaves de longitud cada vez mayor para dificultar esta tarea a los criptoanalistas. Para elegir el tipo de criptografía (cifrado simétrico, cifrado asimétrico o de llave pública y firma digital) es indispensable considerar lo siguiente:

- Importancia de los datos que se desean proteger
- Cantidad de información
- Medio de almacenamiento y/o transmisión
- Infraestructura y recursos computacionales



con los que se cuenta
- Políticas de seguridad

Utilizar algoritmos robustos como 3DES, AES y RSA con llaves de longitud "grande" representa un consumo de recursos considerable. Por tal motivo, en una implementación criptográfica, debe ponerse en la balanza el costo contra el beneficio.

El área de seguridad de la información de cualquier organización debe presentar esta evaluación a su junta directiva para tomar la decisión correcta. Si el riesgo de pérdida de la información es alto y si los posibles daños económicos, reputacionales y penales, así como las sanciones por parte de las instituciones reguladoras son considerables, entonces es muy recomendable invertir en una buena solución criptográfica.

Cuando la opción es utilizar algún lenguaje de programación, es importante tener en consideración que la llave está compuesta por un sólo componente (cadena hexadecimal o texto codificado en base64) y que en algún momento debe especificarse, es decir, que esta información puede ser visible por cualquier usuario que tenga acceso al sistema de archivos. Con acceso a la llave simétrica, un atacante podría descifrar los datos y hacer mal uso de los mismos. El desarrollador debe trabajar junto con el área de seguridad para implementar los controles necesarios en el resguardo de la o las llaves criptográficas, protegiendo los archivos a nivel Sistema Operativo, almacenando las llaves en base de datos, utilizando una llave adicional para proteger las llaves, etc.

Otro punto importante es el poder computacional ya que el cifrado por software es relativamente lento al consumir bastantes recursos del procesador. Si la cantidad de datos a cifrar y/o descifrar no es muy grande y el tiempo de respuesta no es un factor determinante, puede utilizarse sin problemas.

Por el contrario, si la información es crítica, la cantidad de datos a procesar es considerable y el tiempo de respuesta es importante en el proceso, una buena opción es utilizar criptografía basada en hardware.

Los módulos de seguridad por hardware, denominados Hardware Security Modules (HSM), son dispositivos físicos cuya principal función es el almacenamiento y manejo de llaves criptográficas, además realizan operaciones de cifrado, descifrado y firma digital por medio de algoritmos como AES, TripleDES, RSA, DSA, Curvas Elípticas, SHA 1 y 2. Por la criticidad de su operación, estos equipos cuentan con certificaciones de seguridad como FIPS 140-2 (Federal Information Processing Standards), Common Criteria EAL 4+ o PCI DSS (Payment Card Industry Data Security Standards), esto hace imposible que las llaves criptográficas puedan ser exportadas fuera de los dispositivos y que el almacenamiento y transmisión de datos estén protegidos. En caso de que el equipo fuese abierto, toda la información que almacena se borraría automáticamente.

Estos equipos pueden realizar miles de operaciones criptográficas por segundo y permiten que el manejo de las llaves se lleve a cabo por control dual, bajo autenticación por tarjetas inteligentes, dispositivos USB o contraseñas, además es posible establecer una segregación de responsabilidades (custodios, administradores y operadores).

En el proceso de cifrado por software la llave reside en algún archivo del sistema operativo y está compuesta por un solo componente.
A diferencia de éste, si se usa HSM, todas las llaves residen dentro del dispositivo y es imposible extraerlas. La llave puede dividirse en tantos componentes como se requiera, resguardados por personas denominados custodios, por lo que para tener acceso no autorizado a la llave se requiere de la complicidad de todo el personal involucrado.

Para hacer uso de las rutinas de cifrado, descifrado y firma basta utilizar las API proporcionadas por el fabricante del HSM. Estas rutinas pueden embeberse en código Java, C, C# o .NET.

Existen varios tipos de Hardware Security Modules, dependiendo de su funcionalidad:

- **Propósito general**. Estos equipos son utilizados para cifrar cualquier tipo de información, por ejemplo cadenas de texto o archivos; también se utilizan para generar firmas digitales o facturas electrónicas. Existen modelos similares a servidores (cajas), otros son tarjetas que se insertan en la ranura PCI o PCIe del servidor y otros que se conectan por un puerto USB.

- **Sistemas de pagos**. Utilizados generalmente por instituciones financieras. Un ejemplo de estos equipos es cuando se ingresa una tarjeta de crédito en un cajero automático, al ingresar el PIN se genera un bloque de información que se cifra automáticamente con el teclado del cajero.

Este bloque de información viaja hacia el HSM de la institución financiera. El dispositivo recibe la petición, descifra el bloque y envía de regreso al cajero si el PIN del tarjetahabiente es válido o inválido. De esta manera, la información nunca viaja en claro y en caso de que sea interceptada por algún atacante ésta no le será útil pues la llave reside en el HSM y sin ella no es posible obtener el PIN del usuario.

- **Dedicados a servicios de Firma Electrónica Avanzada de documentos y facturación electrónica.**

- **HSM para firma digital y cifrado de correo electrónico.**

- **Dedicados al manejo de Infraestructura de Llave Pública (PKI)**. Firma digital, sellado de tiempo, cifrado de datos y transacciones electrónicas.

- **Módulos que inyectan llaves criptográficas a los cajeros automáticos de manera remota y automática.**

Existen diversas opciones a elegir de acuerdo a las necesidades de cada organización. Entre los fabricantes más reconocidos a nivel mundial se encuentran Thales, SafeNet, Hewlett Packard, Realsec y Futurex.

Una desventaja al utilizar estos equipos podría ser el costo, ya que representa una inversión de algunos miles de dólares, sin embargo, como se precisó anteriormente, si el costo e impactos por la pérdida de información lo ameritan, es muy recomendable adquirir estos dispositivos.

Existen órganos reguladores que obligan a las instituciones que norman a manejar los procesos criptográficos usando HSM. En México, por ejemplo, el Servicio de Administración Tributaria (SAT) establece que los Proveedores Autorizados de Certificación (PAC) deben utilizar módulos criptográficos para cifrar la información y resguardar las llaves de los clientes de facturación electrónica. Los PAC proporcionan el servicio de validación, asignación de folio e incorporación del sello digital correspondiente a las facturas electrónicas también conocidas como Comprobantes Fiscales Digitales por Internet (CFDI) generados por los contribuyentes.

A nivel mundial, Visa establece que sus socios comerciales deben utilizar dispositivos HSM que cumplan con ciertos estándares de seguridad para el manejo de las transacciones que involucran pagos con tarjetas bancarias.

En Estados Unidos, la ley HIPAA (The Health Insurance Portability and Accountability Act of 1996) obliga a las instituciones del sector salud a proteger todos los registros que incluyen identificadores individuales como nombre, dirección, detalles de contacto, número de seguridad social y datos sobre la salud física y mental de los usuarios. Los HSM juegan un papel fundamental para la protección de este tipo de información.

Finalmente, para que una infraestructura de HSM sea eficiente, es indispensable establecer las políticas de seguridad que requiera la organización, por ejemplo, definir quienes serán los custodios de las llaves, quienes los administradores, en cuántas partes se dividirán las llaves, cómo se resguardarán los componentes, bajo qué condiciones se realizará algún cambio en los HSM o en las claves, entre otros. Deben definirse procedimientos funcionales y confiables para el manejo de llaves criptográficas.

De nada sirve tener dispositivos que cumplen con todos los estándares de seguridad globales si un solo custodio resguarda todos los componentes de la llave en el cajón de su escritorio.

Si quieres saber más consulta:

- Criptografía y criptoanálisis: la dialéctica de la seguridad
- Criptografía cuántica
- Violaciones de datos impulsan interés en cifrado, dice estudio

Referencias

Security Requirements for Cryptographic Modules. Recuperado de http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

PCI SSC Data Security Standards Overview. Recuperado de: https://www.pcisecuritystandards.org/security_standards/

Common Criteria Recognition Arrangement. Recuperado de: https://www.niap-ccevs.org/ccra/index.cfm?&CFID=23446544&CFTOKEN=8d9ab5badbcb1b30-B97A9C09-F9DA-7D32-1B6A8553ECB9F763

Sistema de Administración Tributaria - Factura Electrónica. Recuperado de: http://www.sat.gob.mx/informacion_fiscal/factura_electronica/Paginas/default.aspx

Visa PIN security. Recuperado de: https://usa.visa.com/download/merchants/pin-security-080507-final.pdf

Visa PIN Security Requirements. Recuperado de: http://www.visaeurope.com/en/businesses__retailers/payment_security/idoc.ashx?docid=849b2be1-10b9-4bb5-8b8e-74f546777440&version=-1

Securing Electronic Health Records and Meeting HIPAA Requirements. Recuperado de: http://www.safenet-inc.com/uploadedFiles/About_SafeNet/Resource_Library/Resource_Items/Solution_Briefs_EDP/SafeNet_Solution_Brief_HIPAA.pdf?n=1398

Thales e-Security: https://www.thales-esecurity.com/products-and-services/products-and-services/hardware-security-modules

SafeNet: http://www.safenet-inc.com/data-encryption/hardware-security-modules-hsms/

Hewlett Packard: http://www8.hp.com/us/en/software-solutions/atalla-payments-and-data-security/

Realsec: http://www.realsec.com/en/

Futurex: http://www.futurex.com/

Eduardo Palma Ávila

Egresado de la carrera de Ingeniería en Computación de la Facultad de Ingeniería de la UNAM. Formó parte de la segunda generación del Plan de Becarios de Seguridad en Cómputo impartido por la Coordinación de Seguridad de la Información/UNAM-CERT a través de la DGTIC de la UNAM.

Actualmente labora en HSBC México S. A. en el área de Seguridad en la Infraestructura, responsable del equipo de Authentication Services and Encryption Key Management.

Modelo de autorregulación como parte del sistema de protección de datos personales – Parte I

Humberto David Rosales Herrera

En junio de 2006 se publica en el Diario Oficial de la Federación la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), incorporando la protección de datos personales en el campo de estudio del derecho informático mexicano y considerando como sujetos obligados a los poderes de la unión, los órganos constitucionales autónomos o con autonomía legal y a cualquier otra entidad federal. En julio de 2010 se publica la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) considerando como sujetos obligados a los particulares de carácter privado, sean personas físicas o morales, que lleven a cabo el tratamiento de datos personales.

El tratamiento de datos personales se refiere a la obtención, uso, divulgación o almacenamiento de datos personales por cualquier medio. Su uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Ambas leyes tienen como objeto garantizar privacidad de nuestros datos personales y nos otorga el derecho y control sobre nuestra propia información personal frente a la posesión por terceros, para que su tratamiento sea legítimo sin importar si es automatizado, manual o por parte de las entidades del sector público o privado. Es decir, no sólo aplica sobre aquella información albergada en sistemas computacionales, sino en cualquier medio (soporte) que permita su utilización a través de la generación, acceso, almacenamiento, procesamiento, transferencia y disposición final.

En este artículo nos referiremos en particular al

marco jurídico vigente para la protección de datos personales en posesión de los particulares, el cual está integrado por:

- Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)
- Reglamento de la LFPDPPP
- Criterios Generales para la Instrumentación de las Medidas Compensatorias sin la Autorización Expresa del IFAI
- Lineamientos sobre el Contenido y Alcance de los Avisos de Privacidad
- Parámetros para el Correcto Desarrollo de los Esquemas de Autorregulación Vinculante
- Recomendaciones en Materia de Seguridad de Datos Personales:

Imagen 1 Marco jurídico para la protección de datos personales en posesión de los particulares

Como punto de partida tomaremos el artículo 44 de la LFPDPPP que establece que los particulares responsables de datos personales podrán convenir entre ellos o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante, una actividad a través de la cual los responsables se comprometen a la protección de datos personales mediante el cumplimiento con lo dispuesto por la Ley, el Reglamento y demás disposiciones aplicables.

Dichos esquemas de autorregulación vinculante deberán contener mecanismos para medir su eficacia en la protección de los datos y las posibles consecuencias, así como las medidas correctivas eficaces en caso de incumplimiento. Se debe contar con reglas o estándares específicos que permitan armonizar los tratamientos de datos personales efectuados por los adheridos, facilitar el ejercicio de los derechos de los titulares de los datos personales, además de prever consecuencias y medidas correctivas eficaces en caso de incumplimiento.

Los esquemas deben estar constituidos por dos elementos básicos: por un lado, el tipo de esquema de autorregulación vinculante en el que se recogen los principios, normas y procedimientos que los miembros adheridos se comprometen a observar y cumplir y, por otro lado, los mecanismos de control necesarios para la aplicación de tales normas.

El Reglamento en su Capítulo VI: Incentivos establece que la incorporación de esquemas de autorregulación como parte de las medidas de protección de datos personales será tomada en consideración para determinar la atenuación de sanciones. El IFAI podrá determinar mecanismos que faciliten procesos administrativos ante el mismo, así como otros incentivos.

En el Capítulo VI indica que los objetivos de la autorregulación están orientados a coadyuvar al cumplimiento del principio de responsabilidad, establecer procesos y prácticas para la protección de datos, además de establecer políticas, procesos y buenas prácticas. De forma voluntaria, el responsable puede obtener certificaciones o constancias de cumplimiento de la Ley para identificar si cuenta con políticas de privacidad alineadas al cumplimiento de la LFPDPPP.

También indica que la adopción de estos esquemas facilita la coordinación entre esquemas de autorregulación reconocidos internacionalmente, promueve el compromiso de los responsables, encauza mecanismos de solución alternativa de controversias y permite las transferencias de datos personales entre responsables con esquemas de autorregulación como *puerto seguro*.

Puerto Seguro consta de siete principios básicos: i) notificación (información a los afectados), ii) opción (posibilidad de oposición de los afectados), iii) transferencia a terceros, iv) seguridad, v) integridad de los datos, vi) aplicación (procedimientos para la satisfacción de los derechos de los afectados) y vii) derecho de acceso.

Imagen 2 Aspectos que debe cubrir el esquema de autorregulación vinculante para dar cumplimiento con la ley en materia de protección de datos personales

Estos parámetros incluyen:

- **Contenido mínimo**. Complementariedad, armonización, normatividad aplicable, requisitos, forma de administración, sistema de supervisión y vigilancia, consecuencias, medidas correctivas y compromisos adicionales.
- **Contenidos complementarios**. Mecanismos alternativos de solución de controversias, medidas de seguridad adicionales a las establecidas en la Ley y el Reglamento, cláusulas tipo para la obtención del consentimiento, ya sea para el tratamiento o la transferencia de los datos personales, cláusulas tipo para informar a los titulares del tratamiento de sus datos personales cuando éstos no sean obtenidos de manera personal o directa; o avisos de privacidad estándar que resulten aplicables a un sector o industria y cuya única diferencia sea el tipo de tratamientos exclusivos a los que los responsables someten los datos personales de los titulares.
- **Relacionado al sistema de certificación en materia de protección de datos personales.**

Un esquema de autorregulación en materia de protección de datos personales se puede considerar como máxima expresión del cumplimiento de la LFPDPPP, ya que es un sistema de aseguramiento integrado por mecanismos para medir la eficacia en la protección de los datos, determina las consecuencias del incumplimiento de las medidas de protección y establece medidas correctivas eficaces.

El esquema de autorregulación puede traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos, asimismo puede contener reglas o estándares específicos que permitan armonizar los tratamientos de datos y facilitar el ejercicio de los derechos de los titulares.

El enfoque que debemos dar a la creación de un esquema de autorregulación vinculante en materia de protección de datos personales es principalmente el de establecer las medidas que nos van a permitir direccionar, sensibilizar, establecer, supervisar, mantener e incrementar la efectividad de las medidas de protección físicas, técnicas y administrativas para la protección de los datos personales y a su vez, asegurar el cumplimiento de las obligaciones establecidas por la LFPDPPP.

Los principios torales (principios que sostienen el modelo de autorregulación) que deben ser

observados en el esquema de son:

I. Voluntariedad en la adhesión o adopción del esquema de autorregulación vinculante.

II. Obligatoriedad, ya que el esquema de autorregulación vinculante constriñe a quien se adhiere o lo adopta.

III. Transparencia relativa a las prácticas que siguen en materia de protección de datos personales, salvo aquellos aspectos que los responsables señalen como confidenciales o reservados.

IV. Responsabilidad, materializa la obligación de velar por el cumplimiento de los principios de protección de datos personales previstos por la LFPDPPP (licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad) en relación con los datos personales que posee o que haya comunicado.

V. Imparcialidad, los esquemas de autorregulación vinculante deben organizarse y operar de forma que salvaguarden la objetividad e imparcialidad de sus actividades.

Imagen 3 Principios torales del esquema de autorregulación vinculante

Los objetivos mínimos que debe buscar el esquema de autorregulación son:

- Consolidar una cultura de autoevaluación y autorregulación en materia de protección de datos personales.
- Desarrollar un sistema de evaluación permanente con referencia a la protección de datos de carácter personal.
- Fortalecer permanentemente los mecanismos físicos, tecnológicos y administrativos establecidos para la protección de datos de carácter personal y obtener el reconocimiento por parte de los *grupos de interés*[1] como una empresa que protege los datos personales que le son confiados.
- Dar a conocer a la comunidad de la empresa las acciones encaminadas al cumplimiento de la LFPDPPP y la protección de datos de carácter personal.
- Conocer las áreas de oportunidad o mejora para posteriormente priorizarlas y desplegar planes de acción.
- Articular los resultados de la evaluación con análisis de brecha (gap analisys) sobre el cumplimiento y el plan director para instrumentar de forma ordenada las acciones de mejora encaminadas a la protección de los datos de las personas.
- Mejorar la protección de los datos personales en forma continua y creciente mediante acciones tendientes a reforzarlas.

Informar al grupo responsable de la gestión de la protección de los datos personales y al grupo directivo sobre cómo se está gestionando la protección de datos personales.

- Conocer en qué situación está la organización con relación al cumplimiento de la LFPDPPP y su reglamento a través de diagnósticos de cumplimiento y auditorías.

Para lograr estos objetivos mínimos, es necesario implementar un plan de acción en tres fases, éstas se detallarán en la próxima entrega de este artículo, junto con una serie de recomendaciones finales y conclusiones.

Si quieres saber más consulta:

- Ley Federal de Protección de Datos Personales en Posesión de Particulares
- Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I
- Infografía: Protección de datos personales

[1] El término grupo de interés (stakeholders) se ha ido imponiendo progresivamente para designar a todas las personas, grupos u organizaciones que mantienen una relación directa o indirecta con la empresa; están dentro y fuera de la empresa y pueden afectar o ser afectadas por las actividades de la empresa, positiva o negativamente. Las empresas con su actividad generan impacto directo o indirecto que afecta a sus grupos de interés, a los cuales es necesario identificar y analizar. (http://rse.xunta.es/index.php?option=com_content&view=article&id=19&Item...)

Humberto David Rosales Herrera

Su experiencia profesional se ha enfocado en la administración áreas de tecnología de misión crítica y seguridad integral con más de veinticinco años de experiencia internacional como consultor, auditor, gerente y subdirector. Desarrolle un método para generar métricas sobre la evolución de efectividad en la administración de TI.

Cuenta con el PhD Computer Science (1990) de la Pacific Western University de Los Angeles, California y con las certificaciones CISSP, CCNA DE CISCO NETWORKS (instructor), MICROSOFT CERTIFIED PROFESSIONAL (instructor), PMP.

(In)Seguridad en Java: La biografía no autorizada

Romeo A. Sánchez López

El otro día fui a una cafetería, de esas donde escriben tu nombre en el vaso y pedí mi tradicional café frappuccino Java Chip. Me dijeron que ya no se llama Java Chip, sino solamente Chip, así que me resigné a tomarlo así, sin Java, y me fui de ahí pensando en una nueva metáfora: muchos se están deshaciendo de Java, la popular plataforma de desarrollo, no saben por qué, pero lo están desinstalando.

Algo ha estado pasando últimamente con Java (la plataforma de cómputo diseñada pensando en la seguridad) que ha sido el blanco perfecto para explotar una serie de vulnerabilidades encontradas hace apenas unos meses. Siendo precisos, Java no sólo es un lenguaje de programación sino una de las tecnologías con mayor presencia en el mundo, lo que le ha valido ser uno de los objetivos más codiciados por los creadores de *malware* en los últimos años.

Un poco de historia

La plataforma Java fue creada por Sun Microsystems a mediados de los 90, no sólo pensando en que tuviera la capacidad de ejecutarse en cualquier plataforma sino también en que fuera segura. Se incorporaron características de seguridad que no tenía ningún otro lenguaje o plataforma de su época, como el verificador de clases (Class Verifier), que se asegura de usar versiones de los programas sin alterar, o el administrador de seguridad (Security Manager) que ayuda a controlar quiénes tienen acceso a ciertos métodos o recursos de la aplicación. Incluso la interfaz para programación de aplicaciones (API) de Criptografía de Java incluyó las implementaciones de los algoritmos criptográficos más importantes en su momento. Es más, el famoso criptógrafo Whitfield Diffie fue CSO de Sun Microsystems en ese tiempo, lo que

criptográficos más importantes en su momento. Es más, el famoso criptógrafo Whitfield Diffie fue CSO de Sun Microsystems en ese tiempo, lo que refuerza la idea de que Java fue diseñado con la seguridad en mente. Fui un instructor certificado por Sun Microsystems casi desde los inicios de Java y puedo dar fe de que existía un curso llamado Implementing Java Security, donde enseñábamos cómo aprovechar las características de seguridad del lenguaje. Todo indicaba que tendríamos una plataforma segura para rato[1], hasta que un día Oracle compró Sun Microsystems y algo cambió.

Mientras leo mi nombre escrito en el vaso, que ya muestra evidencias de la condensación por el calor intenso, llego a la conclusión de que se trata del precio de la fama.

El precio de la fama

En realidad las vulnerabilidades en Java no son tema nuevo. Han estado presentes desde el principio, pero con dos diferencias importantes con respecto a las actuales: la plataforma recién comenzaba a popularizarse y Sun Microsystems tenía una capacidad de respuesta muy buena para corregir las vulnerabilidades reportadas. Sin embargo, es de esperarse que cuando algo (o alguien) adquiere fama, se vuelva blanco inherente de ataques, entonces la motivación por encontrar nuevas vulnerabilidades en la plataforma aumenta.

Cada año se descubren nuevas vulnerabilidades pero, coincidentemente desde el año de la compra, el número de vulnerabilidades en Java ha incrementado su búsqueda, no sólo por parte de los investigadores, también por aquellos que buscan una oportunidad para lucrar aprovechando una combinación paradójicamente peligrosa: Internet y la capacidad de Java de ejecutarse en un navegador.

Por tal motivo, hay quienes se han dado a la tarea de informarnos cuando ocurre alguna vulnerabilidad de día cero (*zero-day*)[1] o de los detalles de tales vulnerabilidades encontradas[2]. Sin embargo, la pregunta hasta este momento sigue siendo ¿Qué es vulnerable en Java?

Imagen 1. La gráfica representa la cantidad de vulnerabilidades que se han encontrado en la plataforma

Imagen 1 Java desde los primeros años hasta ahora. Es evidente el aumento tan pronunciado en los últimos años

El regreso de los *applets*

¿Alguna vez escuchó hablar de los *applets* de Java? Los *applets* fueron una buena idea al principio, la manera ideal de distribuir programas Java a prácticamente cualquier usuario con una conexión a Internet, pero pronto fueron reemplazados por otras tecnologías más ligeras y con mejor desempeño, por lo que fueron relegados poco a poco, condenados al destierro y al olvido, hasta que alguien les encontró un nuevo uso. Un *applet* no es otra cosa más que un programa hecho en Java que se coloca en un servidor web y se asocia con una etiqueta <*applet*> en una página HTML.

Cuando un usuario entra a un sitio web que tiene una página con un *applet* asociado, el *applet* se descarga junto con la página HTML y, una vez descargado en el navegador de la computadora del usuario, se ejecuta siempre y cuando el navegador tenga la configuración suficiente para permitirlo. Es aquí donde el *applet*, si fue programado de manera que explote una vulnerabilidad, se ejecuta y arruina la diversión de navegar en Internet.

Es importante aclarar que en condiciones normales un *applet* sigue un estricto control de seguridad, pues no permite la ejecución de código nativo en la computadora del usuario, ni puede conectarse a un servidor diferente a aquél de donde fue descargado. El problema está cuando el programador del applet ha descubierto cómo

el programador del *applet* ha descubierto cómo burlar esos controles.

De esta manera, los *applets* han constituido un excelente vector de ataque, porque pueden ser descargados desde Internet y ejecutados en un navegador. Haciendo un poco de memoria, en los 90 algunos *applets* se hicieron famosos, por ejemplo “Jumping the Firewall”, que lograba evadir *firewalls*, o “Big attacks come in small packages” que, irónicamente, podía hacer mucho daño a través de pequeños paquetes de datos. Ya no he encontrado referencias válidas a estas vulnerabilidades antiguas; más bien estoy haciendo un esfuerzo por recordar aquellos primeros casos.

Por lo pronto veo con cierta ansiedad que mi frappé comienza a derretirse y me apresuro a terminarlo antes de que pierda su consistencia. Creo que así mismo pasa con las vulnerabilidades de Java, son aprovechadas tan pronto las descubren, antes de que alguien logre corregirlas.

El lado obscuro de los *applets* de Java

La explotación de vulnerabilidades de Java no se hizo esperar. Evidentemente resulta atractivo poder distribuir un *applet* malicioso (*malware*) que se descarga automáticamente (siempre hay emprendedores que encuentran nichos de mercado). Una de esas oportunidades de negocio se encuentra en el mercado negro de *applets*.

¿Qué pensaría si alguien le ofrece la posibilidad de clonar un sitio, el que usted quiera, hospedado en un servidor de ellos (ni siquiera tiene que exponer el suyo), con un *applet* a la medida y, mejor aún, personalizable, polimórfico y que le brinde estadísticas de descargas para cuantificar el éxito de una "campaña de infección" por *malware*?[3] Suena ridículamente atractivo, ¿no es así? Sin embargo, así es como se está haciendo, a la manera de “hágalo usted mismo”. Lo único que hay que hacer después de cerrar el trato es lograr convencer, directa o indirectamente, a todos los incautos posibles para que entren al sitio malicioso y esperar a que se descargue el *applet* maligno en sus navegadores. Eso es todo, ni siquiera es necesario pedirles sus credenciales (a menos que se desee una ganancia adicional) pues el *applet* que ejecuta el código Java vulnerado podría leer la información por sí mismo, sin restricciones, incluso transmitirla sigilosamente a donde se quiera, mientras el ingenuo espera a que algo aparezca en la pantalla.

El problema específico

Hablando de las últimas vulnerabilidades descubiertas, éstas se presentan en Java Standard Edition 7 (Java SE 7), específicamente en una interfaz de programación (API) llamada Reflection, que es el mecanismo a través del cual un programa puede examinar o hasta modificar el comportamiento de una aplicación en tiempo real. El problema radica en que ciertas vulnerabilidades permiten que se explore y modifique la aplicación durante la ejecución, sin pasar por las restricciones del administrador de seguridad (Security Manager).

Ya sin restricciones, se pueden transferir, cargar y ejecutar clases modificadas sin validar y, por lo tanto, hacer prácticamente lo que se quiera. No obstante, aunque el problema parece estar limitado únicamente a los *applets*, la realidad es que, al estar presente la vulnerabilidad en la API de Java, todos los productos que usen dicha API son vulnerables también. Por ejemplo, pensemos en que más de 1,000 millones de computadoras

usan Java, junto con más de 3,000 millones de dispositivos móviles y todos los reproductores Blu-ray del mundo, entre muchas otras cosas, como receptores de televisión satelital, sistemas de navegación de automóviles, máquinas de lotería o dispositivos médicos, por mencionar sólo algunos.[4]

Ejemplo de código vulnerable

He sido programador desde los 80 en el siglo pasado y sé de seguridad, así que, para salir de dudas, decidí comprobar por mí mismo qué tan fácil era explotar las vulnerabilidades de Java 7. Ahora hay una gran cantidad de documentación sobre cómo hacerlo. Incluso sin tener mucha experiencia, programar los *applets* no fue tarea difícil. Una de las vulnerabilidades en la que me enfoqué consistía en deshabilitar el Security Manager de la Máquina Virtual de Java[2] (JVM), y una vez deshabilitado, ejecutar una aplicación nativa en el sistema operativo, es decir, fuera de Java (algo que los *applets* tienen prohibido hacer, a menos que cuenten con un certificado válido y firmado). Para hacer la historia corta, terminé ejecutando una aplicación nativa de Windows: la calculadora (es curioso ver cómo en muchas pruebas de concepto de análisis de vulnerabilidades, muchos investigadores coinciden en ejecutar siempre la calculadora, tanto que hasta parece formar parte de las herramientas de hackeo).

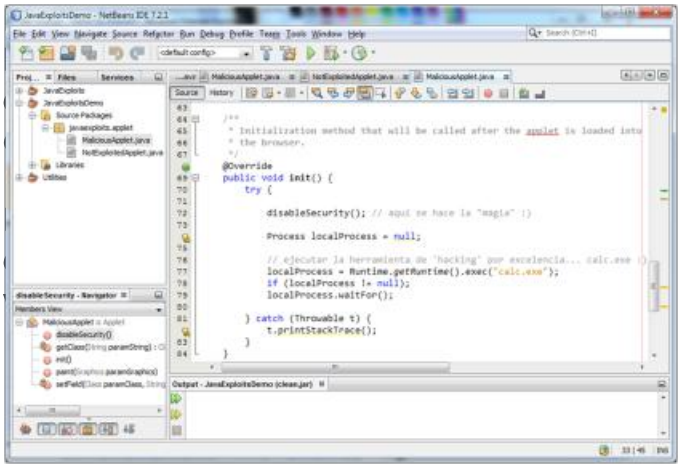


Imagen 2 Código de ejemplo que ejecuta la calculadora de Windows después de deshabilitar el Security Manager gracias a una vulnerabilidad de Java 7

En un escenario seguro, cualquier intento de hacer eso haría que el validador de applets lo descargara de la memoria, para que no se ejecutara.

Mientras pienso en esto, un poco de café se derrama en mi camisa. ¡Qué ironía! Acabo de ser víctima de mi propio café.

```
<!doctype html>
<html>
    <head>
        <meta charset="utf-8" />
        <title>Café amargo - Demo by Knaverit</title>
    </head>
    <body>
        <h1>bSecure 2013... enjoy!<h1>
        <img src="java_hero.png" width=30% height=30%>

        <!--Este es sólo un ejemplo de ejecución de Applet que explota
            una vulnerabilidad de JRE 7

            ¡En realidad *NO* realiza ningún tipo de infección! :) -->

        <applet code="javaexploits.applet.MaliciousApplet.class"
                archive="JavaExploitsDemo.jar" width="100" height="100">

    </body>
</html>
```

Imagen 3 Código HTML para enviar el applet *malicioso al navegador del usuario*

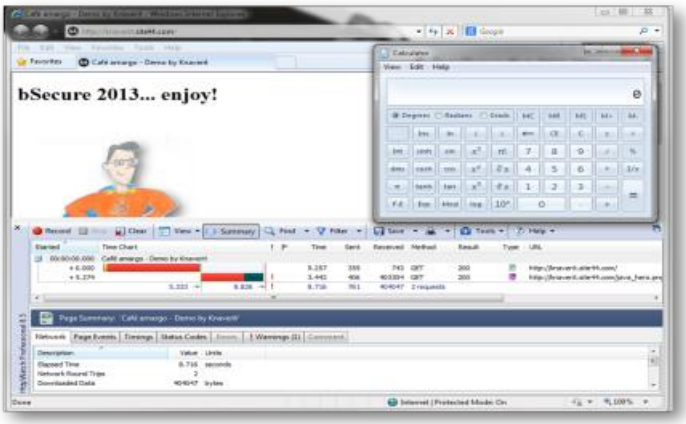


Imagen 4 La calculadora de Windows se ejecuta al entrar al sitio que aloja al applet *malicioso*

Recomendaciones

Casi termino mi café (antes de tiempo, gracias a lo que derramé), pero no puedo hacerlo sin dejar algunas recomendaciones:

1. Si eres un **programador**, debes esforzarte por aprender y aplicar técnicas de programación segura en tus desarrollos. Es cierto; es importante que el programa haga lo que tiene que hacer, pero también es importante que lo haga con seguridad, no dando oportunidad de encontrar y aprovechar un error dejado por descuido o por ignorar las consecuencias.

2. Si eres **administrador de sistemas** y tus usuarios necesitan usar el *plugin* de Java en sus navegadores para sus tareas cotidianas en la empresa, es crucial que distribuyas las actualizaciones más recientes del *plugin* de Java.
3. En todos los casos, usa siempre la versión más actualizada de tu navegador de Internet y de los *plugins* que uses (hay otros *plugins* con historial de vulnerabilidades, no sólo Java). Si no usas algún *plugin*, deshabilítalo o desinstálalo. El único inconveniente ocurre cuando un *applet* de Java requiere ejecutarse en una versión específica de Java, pues en ese caso se requiere tener instalada dicha versión. Si eso ocurriera, conviene activar el *plugin* únicamente cuando se use la aplicación y desactivarlo nuevamente al salir.

Aunque Oracle ha estado trabajando en solucionar las vulnerabilidades, y ha logrado mantener la situación bajo control en los últimos meses, hay que tomar medidas inmediatas, como desinstalar o deshabilitar Java ¡Pero sólo en los navegadores! No quiero imaginarme a un administrador de sistemas desinstalando un servidor de aplicaciones Java sólo por desconocer dónde está la vulnerabilidad. Es mejor informarse.

Finalmente miro el vaso de café, ahora vacío. No estuvo mal, pero siento que le faltó algo. Tal vez debería llamarse nuevamente Java Chip o de lo contrario, la próxima vez pediré solo café, café amargo.

Referencias

[1]Days since last known Java 0-day exploit. Recuperado de: http://java-0day.com/ 2013.

[2]Oracle Java Exploits and 0days Timeline. Recuperado de: http://eromang.zataz.com/uploads/oracle-java-exploits-0days-timeline.html 2013.

[3]Danchev, Dancho. "Inside AnonJDB – a Java based malware distribution platforms for drive-by downloads". Recuperado de: http://www.webroot.com/blog/2012/01/17/inside-anonjdb-a-java-based-malware-distribution-platforms-for-drive-by-downloads/ 2012.

[4]Oracle. "Learn About Java Technology". Web site: http://www.java.com/en/about/ . 2014..

[1] Las versiones de la edición estándar de Java van desde la 1.0 liberada en 1996, hasta la versión 8 (Java 8) en 2014, han incluido numerosas actualizaciones y mejoras al lenguaje. Los programadores usan una distribución de Java conocida como JDK (Java Development Kit) que incluye las herramientas de compilación y depuración de código, mientras que los usuarios de las aplicaciones utilizan una versión que se instala en los navegadores de Internet conocida como JRE (Java Runtime Environment).

[2] La Máquina Virtual de Java (Java Virtual Machine) es un proceso que ejecuta el sistema operativo, a su vez permite ejecutar una aplicación en ella de manera que dicha aplicación no necesite conocer los detalles subyacentes de la plataforma o sistema operativo en el que se ejecuta la máquina virtual, permitiendo además, que el código no requiera adaptarse para cada plataforma. De otra manera, sin una máquina virtual, el código debería modificarse y compilarse cada vez para cada plataforma diferente.

Romeo A. Sánchez López

Ingeniero en Seguridad Computacional con Maestría en Educación especializado en Razonamiento Matemático y en proceso de obtener el grado de Maestro en Ciencias en Sistemas Inteligentes por el Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) especializándose en aprendizaje automático y agentes inteligentes. Su experiencia en IT comenzó a mediados de los 80 como programador BASIC, y posteriormente desempeñando actividades de administración de redes y sistemas, ingeniero de software y desarrollador de aplicaciones empresariales en diferentes plataformas y lenguajes, pero principalmente en JAVA.

En la actualidad se desempeña a cargo del equipo Enterprise Technical Architecture en CEMEX, en Estrategia de IT, donde es responsable del diseño de arquitectura de los sistemas de información.

Cómo superar a Windows XP (sin fallar en el intento)

Sergio Andrés Becerril

"Mejorar es cambiar; la perfección requiere cambios constantes."

- Winston Churchill

Doce años es una cantidad considerable de tiempo, más cuando hablamos de informática. Sin embargo, a Windows XP se le contaron 12 años, 5 meses y 14 días antes de formalizar su *fin de vida*: el momento en que Microsoft decidió finalizar el soporte y por ende, las actualizaciones para el sistema operativo, esto incluye aquellas de seguridad.

Ocurrió el 8 de abril de 2014, unos días antes de publicarse esta edición. Sin embargo, aún hay muchas organizaciones e individuos que siguen utilizando alguna variante de Windows XP en sus equipos de cómputo: 26.29% de los equipos a nivel mundial (de acuerdo a la firma de análisis Net Applications). Y es que a lo largo de su vida, XP se distinguió por brindar a sus usuarios estabilidad, eficiencia y familiaridad, ventajas que son difíciles de abandonar para saltar a un nuevo (y desconocido) sistema operativo.

Esta transición hacia la finalización de soporte implica importantes desventajas. Principalmente la falta de actualizaciones de seguridad, que deja a los usuarios en un punto muy frágil pues cualquier vulnerabilidad que sea posteriormente descubierta no recibirá un parche de corrección.

El primer caso de este tipo se dio el 26 de abril, cuando la firma de seguridad FireEye descubrió un ataque que ha sido utilizado de forma exitosa contra diferentes versiones de Internet Explorer. Aunque el ataque se realizó contra las versiones 9, 10 y 11, la vulnerabilidad afecta a versiones previas que van desde la 6. Microsoft eventualmente liberó un parche específicamente para esta debilidad, argumentado que fue descubierta a escasos días del fin oficial de soporte, pero el "martes de actualizaciones" del mes de mayo efectivamente dejó de tratar

actualizaciones para XP, excluyendo otra falla descubierta en los días intermedios.

Todo lo anterior puede resumirse en lo siguiente: es tiempo de cambiar. A continuación ofrezco varias recomendaciones para

migrar tus equipos de Windows XP dependiendo de tus requerimientos personales o los de tu organización.

La ruta preferida: actualización

En la mayoría de los casos, es posible realizar una transición ordenada a nuevas tecnologías sin perturbar tus procesos personales o de negocio.

La primera posibilidad es una actualización de software. De los tres sistemas operativos que Microsoft liberó posteriores a Windows XP, Windows 7 es la alternativa más realista para el proceso de actualización en equipos existentes. Windows Vista es ya considerado como obsoleto (como muestra de ello ya ha finalizado su periodo de soporte generalizado) y Windows 8 suele requerir de características avanzadas que sólo se encuentran en los procesadores más modernos. Puedes checar los requerimientos de Windows 7 con la herramienta oficial de Microsoft y de igual manera para Windows 8.

En algunos casos las herramientas podrían indicar que los equipos actuales son inviables y requieren actualización de hardware. En este caso debemos evaluar si esta opción es la mejor. Por ejemplo, muchos equipos anteriores al año 2010 utilizan memoria RAM del tipo DDR2, la cual es cada vez más difícil de obtener debido a la saturación del mercado con equipos que utilizan DDR3. Esto conlleva un aumento en el precio de

Saneamiento de información

Si decides cambiar de equipo de cómputo, recuerda que es importante realizar un borrado seguro de tu información antes de desechar cualquier medio de almacenamiento.

La razón de esto es que cuando borras un archivo en tu computadora, en realidad la información no desaparece; tu computadora simplemente marca como disponible el espacio que tus archivos ocupaban y sigue trabajando. Si en algún momento otros archivos requirieran ese espacio, pueden utilizarlo, sólo entonces se borra realmente la información que existía ahí.

Si quieres enfocarte en archivos específicos hay muchas opciones. En Windows por ejemplo, existe Eraser (entre muchas otras), que también cuenta con versión portátil. Mac OS cuenta con una opción en Finder, Secure empty trash, que te permite borrar definitivamente tus archivos. Finalmente, para Linux puedes utilizar Secure-delete.

Por otro lado, tal vez sea más eficiente formatear completamente el disco. Pero recuerda que el formateo tradicional no es suficiente, debes realizar un formateo de bajo nivel. Diferentes sistemas operativos le llaman a este proceso de manera diferente (formateo completo, formateo seguro) pero la mejor clave para saber que está realizando el procedimiento correcto es el tiempo: un formateo de este tipo suele durar varias horas. Por ejemplo, un análisis determinó un tiempo de 0.31 minutos por gigabyte (aproximadamente 1 hora 30 minutos para un disco de 500 GB).

Si prefieres ahorrarte el tiempo y tu disco es magnético, siempre existe la opción de desmagnetizarlo. Este proceso puede ser utilizado para borrar masivamente y de manera segura cientos de discos que serán descartados, haciéndolo un proceso óptimo para grandes organizaciones.

los módulos de RAM de tipo DDR2, obligando a realizar una evaluación detallada de costo-beneficio.

Yo suelo seguir los siguientes lineamientos para determinar si un equipo es actualizable:
1. Tipo de actualización. Hace 15 años no era raro actualizar tu procesador a un modelo más moderno. Los procesadores eran en mayor o menor medida intercambiables y su costo era mucho menor en proporción al de un equipo nuevo. Actualmente cambiar de procesador implica cambiar , la *motherboard*, lo que a su vez suele implicar cambiar la RAM. En conjunto, estas tres piezas pueden representar entre el 30% y el 80% del costo de un equipo nuevo.
Por ello, suelo actualizar únicamente tres componentes: RAM, disco duro y cualquier dispositivo externo, como mouse, teclado o monitor. En particular, una actualización de disco duro a uno de estado sólido y un incremento de RAM pueden respirar nueva vida a equipos ligeramente obsoletos.

2. Antigüedad. Debido a lo anterior, un equipo mayor a 5 años usualmente no es candidato a actualizaciones, generalmente sólo uno menor a 3 años de antigüedad brindará un retorno de inversión justificable.

3. Tipo de computadora. En general, las portátiles son menos susceptibles a actualización que los equipos de escritorio.
En cualquier caso, las licencias de Windows 7 y 8 tienen costos diferentes para actualización y para versión completa. La única diferencia es que para poder instalar la versión de actualización es necesario que el equipo tenga instalada una versión de Windows XP o Vista, por ejemplo, una actualización de disco duro nos obligaría a adquirir licencias completas. El ahorro de una versión de actualización es de alrededor del 25%.

Si es imprescindible adquirir equipo nuevo

Queda la opción de actualizar tus equipos de cómputo adquiriendo nuevos. Aunque el costo definitivamente es superior al de actualizaciones por partes, el tiempo de vida probablemente será mucho mayor al contar con características más modernas a lo largo de todo el hardware y software. Además, muchos equipos nuevos cuentan con beneficios adicionales, como licencias de prueba para software, hardware adicional sin costo (como impresoras), cupones de descuento, etc.

Si vas a comprar aparatos nuevos, la mejor relación costo-beneficio te la dan aquellos que están ligeramente por debajo del líder en cada categoría. Por ejemplo, procesadores de penúltima generación. Recuerda también que la memoria RAM suele ser más cara si ya viene instalada. Casi siempre es más barato comprar más RAM después de adquirido el equipo e instalarla por tu cuenta. La mayoría de las garantías actuales permiten este tipo de actualizaciones sin perder su validez, aunque como siempre, te recomiendo verificar esta información previamente con el fabricante.

El cambio de hardware da pie a grandes posibilidades de replantear objetivos y optimizar los recursos. Si vas a reemplazar tu equipo personal, puedes aprovechar este momento para adquirir un equipo de cómputo mejor orientado a tus necesidades. Desde la salida de Windows XP han salido al mercado varias nuevas tecnologías y otras han evolucionado al punto de ameritar una revisión. ¿Sabías que desde 2001 han salido al mercado 4 nuevos estándares de conectividad Wi-Fi? El último soporta velocidades de hasta 866.7 Mbps (más de 10 veces el máximo de velocidad del estándar 802.11g liberado en 2003). Adquirir un equipo nuevo te permite obtener esta tecnología lista para usar.

En el ambiente corporativo es similar. Por ejemplo, Windows 8.1 no permite acceder a dominios de Windows ni la aplicación de políticas, mientras que Windows 8.1 Pro sí. Otras tecnologías, como BitLocker (para el cifrado de discos) podrían ser esenciales en tu organización o críticas para el alcance de metas a mediano y largo plazo, como la certificación ante algún estándar. Además te permite homologar los equipos, lo que aumenta tremendamente la eficiencia del equipo técnico para la resolución de incidentes.

Respaldo y restauración de datos

Si estás pensando en cambiar tu equipo personal por uno nuevo, la solución más sencilla es evitar realizar un respaldo. En vez de ello te sugiero que (una vez adquirido el nuevo) saques el disco duro de tu computadora actual y lo conectes mediante USB al nuevo por medio de un gabinete para discos duros. Puedes adquirir uno de estos artefactos en cualquier tienda que venda accesorios de cómputo, ellos mismos pueden ayudarte a realizar la extracción de tu disco. Una vez que esté listo, funcionará como una memoria USB (sólo que ya tendrá todos tus datos). De esta manera, podrás realizar la transferencia de tu información a tu nueva computadora y al mismo tiempo, contar con un respaldo portátil y eficiente. Si tu disco ya presenta fallas, puedes realizar este procedimiento para copiar tu información y una vez terminado, desechar el disco.

Si en cambio, estás pensando en una actualización de equipos a nivel de organización, puedes ayudarte de varias herramientas. De manera similar al caso anterior, puedes conectar a algún servidor los diferentes discos duros de los equipos que se están reemplazando, incluso puedes utilizar uno de esos equipos como servidor de migración. Alternativamente, si trabajas en un entorno con dominio de Windows, puedes utilizar la opción de perfiles móviles para realizar el respaldo y restauración de datos de manera automática.

Reusar los discos duros de esta manera permite mitigar otra consideración de seguridad al reemplazar equipo de cómputo: el saneamiento de los medios de almacenamiento. Si retienes los discos para tu uso continuo, puedes ahorrarte horas (o hasta semanas en ambientes corporativos grandes) de formateos de

Reciclaje tecnológico: instala Linux

Si tu equipo no es compatible con Windows 7 u 8, pero quieres exprimirle otro año (o 5, o 10) más de funcionamiento, tal vez te interese considerar Linux.

Debido a sus (usualmente menores) requerimientos de hardware, Linux es una solución ideal para equipos con varios años de antigüedad que no requieran grandes cantidades de procesamiento. Afortunadamente, muchas de nuestras tareas cotidianas son posibles sin estresar demasiado a la computadora: navegar por Internet, enviar y recibir correo electrónico, escuchar música, editar documentos, etc.

Linux es gratuito y puedes descargar gratuitamente gran cantidad de software para una enorme variedad de usos. Sin embargo, debes estar consciente de que Linux requiere que tomes decisiones importantes sobre qué y cómo utilizarás tu equipo de cómputo. Puedes descargar gratuitamente la suite de oficina de Linux, LibreOffice (o cualquiera de sus competidores también gratuitos). En general funcionan de manera muy similar al Office de Microsoft, pero no son iguales. Y aunque mucho del software de Windows puede ser utilizado en Linux, para esto requieres herramientas de terceros que pueden o no ser gratuitas, por ejemplo Wine o Crossover.

Si te interesa más información, publicaré en breve un artículo con información más a detalle sobre Linux.

los discos antes de desecharlos (ver sección barra lateral).

Finalmente, recuerda que los archivos que estarás restaurando pueden estar contaminados con *malware*. No olvides escanear los archivos que restaures con un antivirus actualizado.

Si tienes aplicaciones críticas dependientes de XP.

En algunos casos, te encontrarás con que existen aplicaciones en tu organización que dependen de Windows XP para seguir funcionando y que son críticas para las operaciones de tu organización. Usualmente es por una de estas dos razones:

1. Tus aplicaciones utilizan bibliotecas de Windows o de lenguajes como Visual Basic de versiones anteriores a XP. Aunque Windows XP aún las puede ejecutar, las nuevas versiones de Windows ya no son capaces de ello.
2. Tus aplicaciones web requieren Internet Explorer y de sólo ciertas versiones (usualmente 6 o 7).

En este caso, una solución transitoria es la virtualización de equipos con Windows XP para permitir la interacción con estos sistemas. Esto permite añadir varias capas de seguridad:

- En caso de una infección o vulneración de los equipos virtualizados, es posible contener la amenaza dentro del entorno virtual sin afectar a otros servicios.
- Los equipos virtuales pueden ser respaldados fácilmente, permitiendo su inmediata restauración ante cualquier incidente.

Sin embargo, debe enfatizarse que ésta es una medida **transitoria** y que debe trabajarse en la migración de servicios obsoletos de los sistemas a mediano plazo.

Sergio Andrés Becerril

Es un profesionista informático con 15 años de experiencia en proyectos de la iniciativa privada, académicos y docentes. Actualmente labora en el Departamento de Cómputo del Centro de Enseñanza de Lenguas Extranjeras de la UNAM, y como Director de Tecnología de una consultora privada especializada en seguridad informática. Puedes encontrarlo en twitter: @dolphone.

Concienciar para prevenir

Edgar Ríos Clemente

¿Cuántos de nosotros hacemos actividades de prevención en nuestro día a día? ¿Cuántas de éstas son relacionadas a nuestra salud? ¿Y a nuestra ciberseguridad?

De acuerdo al diccionario de la Real Academia Española, prevenir es la "preparación y disposición que se hace anticipadamente para evitar un riesgo o ejecutar algo", también significa "anticiparse a un inconveniente, dificultad u objeción".

Por lo que se refiere a prevención en la salud, uno debe preguntarse ¿Cuántos de nosotros vamos al doctor o al dentista de forma preventiva? Estoy seguro de que no somos unos cuantos los que nos esperamos hasta que ya no podemos soportar más algún dolor para hacer la visita obligada. Lo mismo sucede con los usuarios dentro de las organizaciones cuando hablamos de la prevención de riesgos de seguridad, ¿cuántos se acercan a sus áreas de seguridad de forma preventiva?, ¿a cuántos conoces que lleguen al área de soporte porque no tienen actualizada su firma de antivirus o en busca de las últimas actualizaciones de su sistema operativo? Todo esto no es más que el reflejo de la falta de cultura de prevención en nuestra sociedad.

Todavía hay muchas organizaciones que apenas están reaccionando ante los temas de seguridad, es decir, formando equipos de respuesta robustos o identificando servicios requeridos. Sin embargo, todas lidian con uno de los temas más difíciles de implementar en toda empresa, la administración de cambios organizacionales. Uno de estos es crear la costumbre de la prevención. Pero, ¿qué podemos hacer cada uno de nosotros para crear conciencia de los riesgos de seguridad de la información? Puedo decir que quienes saben de la importancia de la prevención, saben también las dificultades de implementarla.

Es importante resaltar que a la fecha se siguen presentando las mismas amenazas básicas de seguridad que desde hace más de una década. De acuerdo al reporte de la empresa Verizon, publicado en las noticias de seguridad de la CSI/UNAM-CERT el 23 de abril de 2014, es un

hecho que los esfuerzos realizados no han sido suficientes y que deben crearse mejores programas de prevención.

Parece que las nuevas generaciones nacen con una habilidad asombrosa para operar cualquier dispositivo que se les ponga enfrente, por esto mismo, el tema de concienciación de la seguridad toma más relevancia, para que la prevención de riesgos en la seguridad sea un hábito.

Generar y promover iniciativas de prevención reducirá riesgos como fuga de información por ingeniería social, por citar un ejemplo. Está en cada uno de nosotros hacer los cambios necesarios para que los incidentes de seguridad no sean los mismos año tras año.

La concienciación para la prevención constituye un pilar importante para el cambio de la cultura organizacional en cuanto a temas de seguridad. Para que cumpla su objetivo, cada una de las actividades que propongamos en el marco de esta concienciación deberá estar dirigida a un sector específico, deberá contar con una serie de recomendaciones para su aplicación y de ser posible, estar relacionadas a la cotidianeidad de los usuarios. Trabajando la concienciación de este modo, será más fácil que unos padres puedan orientar a sus hijos dentro de sus hogares, por dar un ejemplo.

Crear conciencia de la importancia de la prevención y convertirla en un hábito nos beneficiará a todos. Pero si los esfuerzos no son bien dirigidos y la comunicación no es clara, se le restará atención a todo el proceso y el resultado podría ser adverso.

Concienciar para prevenir los riesgos de seguridad en ambientes digitales nos evitará muchos dolores de cabeza, incidentes en algunos casos, y explicaciones a la alta dirección.

Para crear una cultura proactiva en toda la población y en las organizaciones, se debe acelerar la disponibilidad de información, de recursos educativos y de concienciación, proporcionando las herramientas adecuadas para los usuarios

Como un inicio básico, si eres un usuario casero debes proteger tu información y tus dispositivos electrónicos. Para hacerlo puedes encontrar información en el sitio de Usuario casero de la CSI/UNAM-CERT, en los sitios web de los mismos dispositivos o en las páginas de tus redes sociales, en éstas se indica qué hacer para configurarlos adecuadamente. En cuanto a recomendaciones de seguridad en servicios financieros, cada entidad tiene la obligación de proporcionarlas en sus páginas.

Si eres responsable de proporcionar servicios de seguridad, no olvides aprovechar las herramientas tecnológicas con las que tu organización cuenta en favor de la concienciación, como cursos de entrenamiento (internos y externos), bases de conocimiento, redes sociales (Twitter, Facebook, Instagram, Pinterest, entre otras), correo electrónico, herramientas de colaboración, posters, tableros de avisos, etc. Posteriormente deberás verificar que realmente se apliquen los cambios propuestos, es decir, revisar la eficacia de la campaña de concienciación mediante los incidentes de seguridad identificados. Puedes encontrar más información de cómo crear una campaña de entrenamiento en la publicación del National Institute of Standards and Technology NIST 800-50 "Building an Information Technology Security Awareness and Training Program" (Cómo construir una campaña de conciencia y entrenamiento para la cultura de seguridad).

La siguiente es una lista de recomendaciones básicas de prevención por la que debemos iniciar:

Utilizar contraseñas seguras

Utiliza diferentes combinaciones para usuarios y contraseñas y evita escribirlas. Recurre a frases fáciles de recordar o nombres de canciones, puedes utilizar la primera letra de cada palabra combinándolas con caracteres especiales.

Protege tus dispositivos móviles

Recuerda que también pueden ser blancos de malware y de usuarios malintencionados. Para protegerte habilita la contraseña de acceso y descarga aplicaciones sólo de sitios de confianza.

En la computadora y dispositivos móviles

Mantén actualizado el sistema operativo y las aplicaciones, de preferencia activa la opción de actualizaciones automáticas. Utiliza un antivirus/antimalware y configúralo para que realice las actualizaciones automáticas.

Protege tu identidad digital

Se precavido al proporcionar información personal en medios digitales. Verifica que los sitios que visitas sean seguros y habilita configuraciones de privacidad.

En los medios sociales

Asegúrate de que la configuración de tu perfil sea en su mayoría privada y ten cuidado con la información que publicas.

Asegura tu red inalámbrica

Las redes inalámbricas, si no son configuradas adecuadamente, pueden ser vulnerables, sobre todo las redes públicas, debes evitar realizar transacciones financieras en estas redes.

Evita navegar en sitios y archivos desconocidos

Si no has solicitado esa información, evita abrir los mensajes desconocidos que te llegan.

Solicita la ayuda correcta

Cuando eres víctima o sospechas de un incidente de seguridad, contacta al equipo de atención a incidentes de seguridad de tu organización o solicita servicios profesionales, la UNAM cuenta con el UNAM-CERT.

Si requieres apoyo en la instalación de aplicaciones, consulta a tus proveedores o contacta a un técnico profesional.

Si quieres saber más consulta:

- Usuario casero
- Comic Liga Super-Seg
- Noticias UNAM-CERT
- 2014 Data Breach Investigations Report
- NIST Special Publication 800-50 - Building an Information technology Security Awareness and training Program
- NIST Bulletin - Information Technology Security Awareness, Training, Education, and Certification

Edgar Ríos Clemente

Ingeniero en Computación de la UNAM, becario de la segunda generación del Programa de Tecnología en Cómputo (PROTECO) de la División de Ingeniería Eléctrica de la Facultad de Ingeniería y de la segunda generación de seguridad Informática (CSI/UNAM-CERT).

Cuenta con más de 9 años de experiencia en Seguridad de la Información en los sectores de telecomunicaciones y financiero. Ha realizado cursos y diplomados en administración de proyectos, derecho en TICs y administración de negocios en la UNAM, ITESM e ITAM. Actualmente labora en un banco líder internacional como consultor regional de seguridad.

Dispositivos móviles: un riesgo de seguridad en las redes

María del Rocío Sánchez Saavedra

A través del presente artículo, se abordarán tres aspectos importantes referentes a la seguridad en el uso de dispositivos móviles dentro de las redes corporativas, los cuales tienen que ver con el establecimiento de políticas empresariales, mecanismos de seguridad a instrumentar y recomendaciones para su uso. Como mencionan Murgante, Gervasi, Iglesias, Taniar y Apduhan (2011), muchas empresas están adoptando el uso de *smartphones* para la implementación de un ambiente de trabajo inteligente u oficina inteligente. A través de su artículo, muestran que la implementación de VPN entre la empresa y el cliente móvil representa una tecnología de seguridad eficaz para la protección de la red entre los sistemas de información corporativos y los *smartphones*.

Por otra parte, informes presentados por compañías como CISCO, Juniper y Symantec sobre el uso y seguridad de dispositivos móviles, también coinciden en el crecimiento en este ámbito desde el año 2011, la tendencia responde a la necesidad de acceder a la información de la compañía estando fuera de ella.

Como señala Carey Nachenberg, Vicepresidente de Symantec Corporation, en muchas ocasiones los usuarios sincronizan sus dispositivos a servicios públicos de nube, quedando fuera del control de los administradores de la red; por lo que es importante que las compañías definan políticas de seguridad y estrategias de control para el uso de dichos dispositivos en la red corporativa.

Estrategias y políticas empresariales

Hoy en día, el uso de teléfonos inteligentes y tabletas tanto a nivel personal como empresarial se ha convertido en una práctica creciente debido

a las múltiples funcionalidades que proporcionan estos equipos así como a las aplicaciones que pueden ser instaladas en los mismos. Me refiero a su utilización en el entorno de las compañías, las cuales han adoptado como una práctica laboral su incorporación a fin de que el personal pueda acceder a los sistemas de información, bases de datos, correo electrónico, telefonía y otros recursos corporativos tanto desde el interior como desde el exterior de la empresa. Lo que se busca es obtener una mayor productividad.

Es importante que antes de implementar y proporcionar una mayor movilidad a través de dichos dispositivos, se diseñen e instrumenten políticas y estrategias de uso que salvaguarden la integridad de la información de la compañía así como la seguridad de todos los recursos tecnológicos con los que cuenta.

De acuerdo a Saro y Fernández (2013), la estrategia y las políticas de seguridad para el uso de dispositivos móviles deben ser definidas por una comisión integrada por personal de las áreas de TIC, recursos humanos, jurídica y directivos, con el objetivo de planear, diseñar, implementar y dar a conocer las mismas al personal de la compañía. Se deben tomar en cuenta todos los aspectos que puedan representar un riesgo de seguridad para la información corporativa y por otra parte, deben estar dentro del marco del SGSI[1] de la organización.

Al definir una estrategia y políticas de seguridad para los equipos móviles alineadas al sistema de gestión de la seguridad de la información, la empresa contará con procedimientos acordes a los objetivos institucionales, además definirá e implementará controles de seguridad basados en un análisis de riesgos. En el blog Negocios Bajo Control, específicamente en el artículo titulado Gestión de la Seguridad de la Información Corporativa en Dispositivos Móviles[2] (2013), el autor presenta una tabla en donde se sugieren posibles factores de riesgos y estrategias de control a instrumentar para cada uno de ellos a fin de que la seguridad de la información corporativa no se vea amenazada por el uso de dispositivos móviles.

Establecer políticas y estrategias de seguridad adecuadas no es una tarea fácil, pero sí necesaria e indispensable para las compañías que adoptan el uso de estas tecnologías pues se debe considerar que cada dispositivo móvil es un activo más que representa un riesgo de seguridad en las redes corporativas.

Mecanismos de seguridad para el uso de dispositivos móviles

Empresas tecnológicas como Symantec, Cisco, Juniper, Enterasys y Citrix, por mencionar algunas, son conscientes de la inminente preocupación por parte de las compañías y del personal de los departamentos de TI por proteger la integridad de los datos corporativos. Al considerar los riesgos que representa el uso de dispositivos móviles, ofrecen actualmente soluciones para implementar diversos mecanismos de seguridad.

Profundizando en estas estrategias, las empresas pueden adoptar varias de ellas a fin de proteger sus recursos. Entre los principales mecanismos se encuentran:

• **MDM (Mobile Device Management)**. Mecanismo orientado a la gestión y al control centralizado de los dispositivos móviles corporativos o personales. Permite contar con toda la información referente al aparato, monitorizarlo, configurar políticas, aplicaciones y tener un historial de cada equipo, entre otras funcionalidades.

• **MDP (Mobile Device Protection)**. Mecanismo utilizado para la protección del propio dispositivo móvil a través de la instalación de un cliente VPN/SSL[3], un antivirus, del uso de cifrado y de métodos de autenticación robustos.

• **NAC (Network Access Control)**. Mecanismo para controlar el acceso a la red corporativa de cada dispositivo móvil. Permite, entre otras cosas, determinar si el equipo es personal o de la compañía, aplicar políticas de seguridad para operaciones sensibles realizadas a través del dispositivo y reparar dispositivos por medio de la instalación y actualización de aplicaciones por medio de VLAN[4] y considerando el perfil de autenticación del mismo.

• **MAM (Mobile Application Management).** Gestiona las aplicaciones a partir de listas negras y blancas, provee entornos virtuales, aplica políticas P2P[5], entre otras funcionalidades.

• **MDS (Mobile Data Security)**. Mecanismo encargado de la seguridad de los datos, la protección de los puertos Wi-Fi, Bluetooth y mini USB del dispositivo, así como la instalación de un cliente DLP[6] (para controlar y evitar la pérdida de datos) y el uso de IRM[7] (para administrar los derechos sobre la información).

Un punto importante para la instrumentación de estos mecanismos de seguridad es que se pueden implementar utilizando los servicios de nube pública que ofrecen los distintos fabricantes de soluciones, o bien, utilizar una nube privada. Dicha decisión dependerá de las necesidades específicas y recursos de cada compañía.

Recomendaciones

La concienciación del personal es un aspecto importante de seguridad para que la red corporativa no sea vulnerable por el uso de dispositivos móviles, personales o corporativos, contribuye a la adopción de las políticas y estrategias de seguridad establecidas para el acceso a los datos y recursos de la compañía.

En el caso de que el personal vaya a utilizar sus dispositivos propios, se le debe concienciar en aspectos tales como el uso de contraseñas complejas de bloqueo/desbloqueo de sus equipos, utilizar firewalls, realizar respaldos, uso de antivirus para el análisis de datos y aplicaciones, configurar opciones de bloqueo y/o borrado de datos del dispositivo en caso de pérdida o robo, entre muchas otras buenas prácticas que en la actualidad existen para un uso seguro de los dispositivos en las redes empresariales.

Como recomendación final, Symantec a través de su portal plantea cinco pilares clave que deben considerarse en el establecimiento de una estrategia móvil al interior de las compañías, las he representado en la siguiente imagen:

Imagen 1 Pilares clave para establecer una estrategia móvil.

Como podemos ver, gestionar la seguridad de los dispositivos móviles para su uso en las redes corporativas implica una serie de consideraciones por parte de las compañías y un reto más para los departamentos de TIC, lo importante es tener conciencia de ello y comenzar a instrumentar medidas para disminuir los riesgos asociados.

Si quires saber más consulta:

- Normatividad en las organizaciones: Políticas de seguridad de la información - Parte I
- Dispositivos móviles
- Riesgo tecnológico y su impacto para las organizaciones parte I

Referencias

Murgante, Beniamino. Gervasi, Osvaldo. Iglesias, Andrés. Taniar, David. Apduhan, BernadyO. (2011). Security Enhancement of Smart Phones for Enterprises by Applying Mobile VPN Technologies. Computational Science and Its Applications – ICCSA. ISBN 10.1007/978-3-642-21931-3_39

Traynor, P., Amrutkar, C., Rao, V., Jaeger, T., McDaniel, P. and La Porta, T. (2011), From mobile phones to responsible devices. Security Comm. Networks, 4: 719–726. doi: 10.1002/sec.218

Carey Nachenberg. (2011). Una mirada a la Seguridad de los Dispositivos Móviles. Symantec Corporation.

CISCO (2014). CISCO 2014 Annual Security Report. Recuperado de: http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html?keycode=000350063

Javier Saro Luna / Javier Fernández Martín (2013). La gestión segura de la información en movilidad ante el fenómeno BYOD: ¿Bring Your Own Device = Bring Your Own Disaster? SiC, 104, 65-73 pp.

http://www.viewsonic.com/documents/white_papers/BYOD_whitepaper_hires_spc.pdf

http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRTcv%5DBuenas_practicas_dispositivos_moviles_0.pdf

http://www.ibm.com/developerworks/ssa/cloud/library/cl-mobilesecuritypolicy/

http://www.iso27000.es/sgsi.html

http://www.symantec.com/es/mx/products-solutions/solutions/detail.jsp?parent=mobile&child=5_pill

Imágen 1. Pilares clave para establecer una estrategia móvil. Elaboración de la autoracon información de Symantec.

[1] SGSI (Sistema de Gestión de la Seguridad de la Información), concepto central sobre el que se construye ISO 27001. La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

[2] http://technologyincontrol2.wordpress.com/2013/07/15/gestion-de-la-segur...

[3] VPN (Virtual Private Network): red privada construida dentro una red pública, utilizada para conectar de forma segura oficinas y usuarios remotos por medio de un acceso a Internet. A través de esta red se protegen los datos usando tecnologías de autenticación IPsec (Seguridad IP cifrada) o SSL (Secure Sockets Layer).

[4] VLAN: red de área local virtual, que agrupa un conjunto de equipos de forma lógica y no física, a partir de ciertos criterios.

[5] P2P (peer to peer): tecnología que hace referencia a un tipo de arquitectura de comunicación entre aplicaciones que permite a los usuarios comunicar y compartir información con otros usuarios.

[6] DLP (Data Loos Prevention): aplicación basada en contenido que detecta, supervisa y protege los datos confidenciales en donde se almacenan o se utilizan.

[7] IRM (Information Right Manager): tecnología que permite tener un control y auditoría sobre archivos, correo, a fin de otorgar permisos de lectura, modificación, acceso, eliminación, apertura e impresión de los mismos.

María del Rocío Sánchez Saavedra

Es Doctorante en Ciencias de la Administración y se desempeña como Profesor/Investigador en la Universidad del Valle de Atemajac, Plantel Zamora y Coordinadora de Redes y Telecomunicaciones de El Colegio de Michoacán, A.C.

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Revista .Seguridad Cultura de prevención para TI
No.21 / junio-julio 2014 ISSN: 1251478, 1251477