Seguridad informática y seguridad de la información

Calderón Arateco Laura Lorena
lauralcalderon@hotmail.com
Universidad Piloto de Colombia

***Resumen*— Cuando se habla de seguridad en el ámbito de la Tecnología de la Información y Comunicaciones a menudo se confunden los conceptos de seguridad de la información y seguridad informática. Y siendo ambos realmente importantes y similares, hay diferencias entre ellos.**

En este artículo hablaremos sobre los conceptos de seguridad de la información y seguridad informática y explicaremos los pilares sobre los que se basa la seguridad de la información.

También tendremos en cuenta los elementos vulnerables de un sistema informático, el concepto de amenaza, fuentes de amenazas y tipos, así como las políticas de seguridad que adoptan las organizaciones para asegurar sus sistemas o minimizar el impacto que éstas pudieran ocasionar.

***Abstract*—When we talk about security in the field of Information Technology and Communications often the concepts of information security and computer security are confused. And being both really important and similar, there are differences between them.**

In this article we will discuss the concepts of information security and information security and explain the pillars on which the security of the information is based.

We will also consider vulnerable components of a computer system, the concept of threat, sources and types of threats and security policies that take organizations to ensure their systems or to minimize the impact that they may cause.

***Índice de Términos*— seguridad informática, seguridad de la información, vulnerabilidad, amenazas, políticas de seguridad.**

I. INTRODUCCIÓN

Cuando hablamos de seguridad de la información estamos indicando que dicha información tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger.

Hasta la aparición y difusión del uso de los sistemas informáticos, toda la información de interés de una organización se guardaba en papel y se almacenaba en grandes cantidades de abultados archivadores. Datos de los clientes o proveedores de la organización, o de los empleados quedaban registrados en papel, con todos los problemas que luego acarreaba su almacenaje, transporte, acceso y procesamiento.

Los sistemas informáticos permiten la digitalización de todo este volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesamiento. Pero aparecen otros problemas ligados a esas facilidades. Si es más fácil transportar la información también hay más posibilidades de que desaparezca. Si es más fácil acceder a ella también es más fácil modificar su contenido, etc.

Desde la aparición de los grandes sistemas aislados hasta nuestros días, en los que el trabajo en red es lo habitual, los problemas derivados de la seguridad de la información han ido también cambiando, evolucionando, pero están ahí y las soluciones han tenido que ir adaptándose a los nuevos requerimientos técnicos. Aumenta la sofisticación en el ataque y ello aumenta la complejidad de la solución, pero la esencia es la misma.

La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de un sistema de información.

Existen también diferentes definiciones del término Seguridad de la Información. De ellas nos quedamos con la definición ofrecida por el estándar ISO/IEC 27001, que fue aprobado y publicado en octubre de 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC).

"La seguridad de la información consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, también pueden estar involucradas otras propiedades, como la autenticidad, responsabilidad, la confiabilidad y el no repudio."

II. SEGURIDAD DE LA INFORMACIÓN: MODELO PDCA

Dentro de la organización el tema de la seguridad de la información es un capítulo muy importante que requiere dedicarle tiempo y recursos. La organización debe plantearse un Sistema de Gestión de la Seguridad de la Información (SGSI).

El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer es identificar los 'activos de información' que deben ser protegidos y en qué grado.

Luego debe aplicarse el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad.

Un SGSI siempre cumple cuatro niveles repetitivos que comienzan por Planificar y terminan en Actuar, consiguiendo así mejorar la seguridad, como se identifica en la siguiente gráfica:

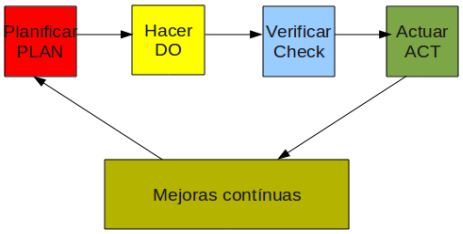

Figura No. 1 Plan PDCA. Tomado de: http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

PLANIFICAR (Plan): consiste en establecer el contexto, en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.

HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.

VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías internas.

ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

III. BASES DE LA SEGURIDAD INFORMÁTICA

Confiabilidad: Existe una frase que se ha hecho famosa dentro del mundo de la seguridad. Eugene Spafford, profesor de ciencias informáticas en la Universidad Purdue (Indiana, EEUU) y experto en seguridad de datos, dijo que "el único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él".

Definimos la confiabilidad como la probabilidad de que un sistema se comporte tal y como se espera de él.

En general, un sistema será seguro o confiable si podemos garantizar tres aspectos, como se ve en la siguiente gráfica:

Figura No. 2 Seguridad de la información. Tomado de: http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

Confidencialidad: En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.

En general, cualquier empresa pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos. Uno de los ejemplos más típicos es el de la inteligencia de un país. Además, es sabido que los logros más importantes en materia de seguridad siempre van ligados a temas estratégicos militares.

Un ejemplo típico de mecanismo que garantice la confidencialidad es la Criptografía, cuyo objetivo es cifrar o encriptar los datos para que resulten incomprensibles a aquellos usuarios que no disponen de los permisos suficientes.

Pero, incluso en esta circunstancia, existe un dato sensible que hay que proteger y es la clave de cifrado. Esta clave es necesaria para que el usuario adecuado pueda descifrar la información recibida y en función del tipo de mecanismo de cifrado utilizado, la clave puede/debe viajar por la red, pudiendo ser capturada mediante herramientas diseñadas para ello. Si se produce esta situación, la confidencialidad de la operación realizada (sea bancaria, administrativa o de cualquier tipo) queda comprometida.

Integridad: En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información.

La integridad hace referencia a:

- La integridad de los datos (el volumen de la información).

- La integridad del origen (la fuente de los datos, llamada autenticación).

Es importante hacer hincapié en la integridad del origen, ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.
A menudo ocurre que al hablar de integridad de la información no se da en estos dos aspectos.

Por ejemplo, cuando un periódico difunde una información cuya fuente no es correcta, podemos decir que se mantiene la integridad de la información ya que se difunde por medio impreso, pero sin embargo, al ser la fuente de esa información errónea no se está manteniendo la integridad del origen, ya que la fuente no es correcta.

Disponibilidad: En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

En términos de seguridad informática "un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados". Es decir, un sistema es disponible si permite no estar disponible.

Y un sistema 'no disponible' es tan malo como no tener sistema. No sirve.

Podemos decir que la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores. No tiene sentido conseguir la confidencialidad para un archivo si es a costa de que ni tan siquiera el usuario administrador pueda acceder a él, ya que se está negando la disponibilidad.

IV. MECANISMOS BÁSICOS DE SEGURIDAD

Autenticación: Verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.

Normalmente para entrar en el sistema informático se utiliza un nombre de usuario y una contraseña. Pero, cada vez más se están utilizando otras técnicas más seguras.

Es posible autenticarse de tres maneras:

1. Por lo que uno sabe (una contraseña).
2. Por lo que uno tiene (una tarjeta magnética).
3. Por lo que uno es (las huellas digitales).

La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. Pero la decisión de adoptar más de un modo de autenticación por parte de las empresas debe estar en relación al valor de la información a proteger.

La técnica más usual es la autenticación utilizando contraseñas. Este método será mejor o peor dependiendo de las características de la contraseña. En la medida que la contraseña sea más grande y compleja para ser adivinada, más difícil será burlar esta técnica.

Además, la contraseña debe ser confidencial. No puede ser conocida por nadie más que el usuario. Muchas veces sucede que los usuarios se prestan las contraseñas o las anotan en un papel pegado en el escritorio y que puede ser leído por cualquier otro usuario, comprometiendo a la empresa y al propio dueño, ya que la acción/es que se hagan con esa contraseña es/son responsabilidad del dueño.

Para que la contraseña sea difícil de adivinar debe tener un conjunto de caracteres amplio y variado (con minúsculas, mayúsculas, números y símbolos). El problema es que los usuarios difícilmente recuerdan contraseñas tan elaboradas y utilizan (utilizamos) palabras previsibles (el nombre, el apellido, el nombre de usuario, el grupo musical preferido,...), que facilitan la tarea a quién quiere entrar en el sistema sin autorización.

Autorización: Proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.

El mecanismo o el grado de autorización pueden variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización.

Dependiendo del recurso la autorización puede hacerse por medio de la firma en un formulario o mediante una contraseña, pero siempre es necesario que dicha autorización quede registrada para ser controlada posteriormente.

En el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea dando o denegando el acceso en lectura, modificación, creación o borrado de los datos.

Por otra parte, solo se debe dar autorización a acceder a un recurso a aquellos usuarios que lo necesiten para hacer su trabajo, y si no se le negará. Aunque también es posible dar autorizaciones transitorias o modificarlas a medida que las necesidades del usuario varíen.

Administración: establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema.
Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema.

La administración de la seguridad informática dentro de la organización es una tarea en continuo cambio y evolución ya que las tecnologías utilizadas cambian muy rápidamente y con ellas los riesgos.

Auditoría y registro: la Auditoría es continua vigilancia de los servicios en producción y para ello se recaba información y se analiza. Este proceso permite a los administradores verificar que las técnicas de autenticación y autorización utilizadas se realizan según lo establecido y se cumplen los objetivos fijados por la organización.

El Registro como el mecanismo por el cual cualquier intento de violar las reglas de seguridad establecidas queda almacenado en una base de eventos para luego analizarlo.

Pero auditar y registrar no tiene sentido sino van acompañados de un estudio posterior en el que se analice la información recabada.

Monitorear la información registrada o auditar se puede realizar mediante medios manuales o automáticos, y con una periodicidad que dependerá de lo crítica que sea la información protegida y del nivel de riesgo.

Mantenimiento de la integridad**:** conjunto de procedimientos establecidos para evitar o controlar que los archivos sufran cambios no autorizados y que la información enviada desde un punto llegue al destino inalterada. Dentro de las técnicas más utilizadas para mantener (o controlar) la integridad de los datos están: uso de antivirus, cifrado y funciones 'hash'.

V. VULNERABILIDADES DE UN SISTEMA INFORMÁTICO

En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en:

Hardware: elementos físicos del sistema informático, tales como procesadores, cableado de red, medios de almacenamiento (cabinas, discos, cintas, usb, DVDs,...).

Software: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.

Datos: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.

De ellos los más críticos son los datos, el hardware y el software. Es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software.

Definimos Vulnerabilidad como debilidad de cualquier tipo que compromete la seguridad del sistema informático.

Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

Diseño

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.

Implementación

- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.

Uso

- Mala configuración de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

Vulnerabilidad del día cero

- Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución “conocida”, pero se sabe cómo explotarla.

Vulnerabilidades conocidas

- Vulnerabilidad de condición de carrera (race condition).

Si varios procesos acceden al mismo tiempo a un recurso compartido puede producirse este tipo de vulnerabilidad. Es el caso típico de una variable, que cambia su estado y puede obtener de esta forma un valor no esperado.

- Vulnerabilidad de Cross Site Scripting (XSS).

Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBSript o JavaScript en páginas web vistas por el usuario. El phishing es una aplicación de esta vulnerabilidad. En el phishing la víctima cree que está accediendo a una URL (la ve en la barra de direcciones), pero en realidad está accediendo a otro sitio diferente. Si el usuario introduce sus credenciales en este sitio se las está enviando al atacante.

- Vulnerabilidad de denegación del servicio.

La denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red por el consumo del ancho de banda

de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

- Vulnerabilidad de ventanas engañosas (Windows Spoofing).

Las ventanas engañosas son las que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que el usuario de información. Hay otro tipo de ventanas que si las sigues obtienen datos del ordenador para luego realizar un ataque.

¿De qué queremos proteger el sistema informático?

Ya hemos hablado de los principales activos o elementos fundamentales del sistema informático que son vulnerables y ahora veremos a qué son vulnerables dichos elementos.

Entendemos la amenaza como el escenario en el que una acción o suceso, ya sea o no deliberado, compromete la seguridad de un elemento del sistema informático.

Cuando a un sistema informático se le detecta una vulnerabilidad y existe una amenaza asociada a dicha vulnerabilidad, puede ocurrir que el suceso o evento se produzca y nuestro sistema estará en riesgo.

Si el evento se produce y el riesgo que era probable ahora es real, el sistema informático sufrirá daños que habrá que valorar cualitativa y cuantitativamente, y esto se llama 'impacto'.

Integrando estos conceptos podemos decir que "un evento producido en el sistema informático que constituye una amenaza, asociada a una vulnerabilidad del sistema, produce un impacto sobre él".

Si queremos eliminar las vulnerabilidades del sistema informático o queremos disminuir el impacto que puedan producir sobre él, hemos de proteger el sistema mediante una serie de medidas que podemos llamar defensas o salvaguardas.

VI. AMENAZAS

De forma general podemos agrupar las amenazas en: amenazas físicas y amenazas lógicas.

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por: las personas, programas específicos, catástrofes naturales.

Amenazas provocadas por personas

La mayor parte de los ataques a los sistemas informáticos son provocados, intencionadamente o no, por las personas.

En general lo que se busca es conseguir un nivel de privilegio en el sistema que les permita realizar acciones sobre el sistema no autorizadas.

Podemos clasificar las personas 'atacantes' en dos grupos:

- Activos: su objetivo es hacer daño de alguna forma. Eliminar información, modificar o sustraerla para su provecho.

- Pasivos: su objetivo es curiosear en el sistema.

Tipos de personas que pueden constituir una amenaza para el sistema informático:

- Personal de la propia organización.
- Ex-empleados.
- Curiosos.
- Crackers.
- Terroristas.
- Intrusos remunerados.

Podemos tener otros criterios de agrupación de las amenazas, como son:

Origen de las amenazas

Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión, etc...

Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc...

Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc...

Intencionalidad de las amenazas

Accidentes: averías del hardware y fallos del software, incendio, inundación, etc...

Errores: errores de utilización, de explotación, de ejecución de procedimientos, etc...

Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etc...

VII. POLÍTICAS DE SEGURIDAD

Lo primero que debemos de hacer es un análisis de las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran.

A partir de este análisis habrá que diseñar una política de seguridad en la que se establezcan las responsabilidades y

reglas a seguir para evitar esas amenazas o minimizar los efectos si se llegan a producir.

La política de seguridad se implementa mediante una serie de mecanismos de seguridad que constituyen las herramientas para la protección del sistema. Estos mecanismos normalmente se apoyan en normativas que cubren áreas más específicas.

Los mecanismos de seguridad se dividen en tres grupos:

Prevención: Evitan desviaciones respecto a la política de seguridad. Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

Detección: Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema. Ejemplo: la herramienta DLP para la seguridad de los archivos.

Recuperación: Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento. Ejemplo: las copias de seguridad.

Dentro del grupo de mecanismos de prevención tenemos:

Mecanismos de identificación e autenticación: Permiten identificar de forma única 'entidades' del sistema. El proceso siguiente es la autenticación, es decir, comprobar que la entidad es quien dice ser.

En concreto los sistemas de identificación y autenticación de los usuarios son los mecanismos más utilizados.

Mecanismos de control de acceso: Los objetos del sistema deben estar protegidos mediante mecanismos de control de acceso que establecen los tipos de acceso al objeto por parte de cualquier entidad del sistema.

Mecanismos de separación: Si el sistema dispone de diferentes niveles de seguridad se deben implementar mecanismos que permitan separar los objetos dentro de cada nivel.

Los mecanismos de separación, en función de cómo separan los objetos, se dividen en los grupos siguientes: separación física, temporal, lógica, criptográfica y fragmentación.

Mecanismos de seguridad en las comunicaciones: La protección de la información (integridad y privacidad) cuando viaja por la red es especialmente importante. Clásicamente se utilizan protocolos seguros, tipo SSH o Kerberos, que cifran el tráfico por la red.

El objetivo de la Política de Seguridad de Información de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad.

La empresa debe disponer de un documento formalmente elaborado sobre el tema y que debe ser divulgado entre todos los empleados.

No es necesario un gran nivel de detalle, pero tampoco ha de quedar como una declaración de intenciones. Lo más importante para que estas surtan efecto es lograr la concienciación, entendimiento y compromiso de todos los involucrados.

Las políticas deben contener claramente las prácticas que serán adoptadas por la compañía. Y estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente.

Las políticas deben:

- Definir qué es seguridad de la información, cuáles son sus objetivos principales y su importancia dentro de la organización.
- Mostrar el compromiso de sus altos cargos con la misma.
- Definir la filosofía respecto al acceso a los datos.
- Establecer responsabilidades inherentes al tema.
- Establecer la base para poder diseñar normas y procedimientos referidos a Organización de la seguridad.
- Clasificación y control de los datos.
- Seguridad de las personas.
- Seguridad física y ambiental.
- Plan de contingencia.
- Prevención y detección de virus.
- Administración de los computadores.

A partir de las políticas se podrá comenzar a desarrollar, primero las normas, y luego los procedimientos de seguridad que serán la guía para la realización de las actividades.

La política de seguridad comprende todas las reglas de seguridad que sigue una organización. Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

La seguridad informática de una compañía depende de que los empleados (usuarios) aprendan las reglas a través de sesiones de capacitación y de concienciación.

Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados.
- Un procedimiento para administrar las actualizaciones.
- Una estrategia de realización de copias de seguridad planificada adecuadamente.
- Un plan de recuperación luego de un incidente.
- Un sistema documentado actualizado.

Por lo tanto y como resumen, la política de seguridad es el documento de referencia que define los objetivos de seguridad y las medidas que deben implementarse para tener la certeza de alcanzar estos objetivos.

VIII. CONCLUSIONES

El principal impedimento para aumentar la seguridad en la información en las empresas es la persistente ausencia de una cultura en seguridad de la información; es necesario que los usuarios incorporen buenas prácticas para proteger el entorno de información, y prevenir aún más la posibilidad de formar parte del conjunto que engloba a las potenciales y eventuales víctimas de cualquiera de las amenazas, que constantemente buscan sacar provecho de las debilidades humanas.

Además se debe tener presente que también es necesario mantenerse informados en lo que respecta a los problemas de seguridad que suponen el uso de determinados medios de comunicación e interacción, entender cómo y por qué se gestan las diferentes maniobras delictivas y conocer cuáles son las herramientas que permiten hacer frente a una problemática que a nivel mundial no tiene en cuenta fronteras y afecta por igual a todos los usuarios.

Tanto los usuarios (sin importar el nivel de conocimiento) como las organizaciones, son cada vez más dependientes de Internet y de las tecnologías de información, lo que también los expone constantemente a diferentes amenazas, en las que se utilizan estas condiciones para cometer acciones delictivas con fines económicos.

No obstante, existen todavía empresas que carecen de orientación sobre los ajustes que deben realizar en su negocio para proteger adecuadamente sus sistemas de información o que desconocen la existencia de los mismos. En este sentido, debemos insistir en el conocimiento, difusión e implantación de cuantos medios sean necesarios para garantizar la seguridad informática y seguridad de la información.

REFERENCIAS

[1]http://windowsupdate.microsoft.com
[2]http://www.intendenciaatacama.gov.cl/filesapp/Manual%20debuenas%20practicas%20politicas%20de%20seguridad.pdf
[3]http://www.welivesecurity.com/wp-content/uploads/2014/01/buenas_practicas_seguridad_informatica.pdf
[4]http://repositorio.utp.edu.co/dspace/bitstream/11059/2514/1/0058A973.pdf
[5]http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=6

Laura Calderón nació en San Antonio (Tolima) en 1981. Recibió el título de Ingeniero de Sistemas de la Universidad Cooperativa de Colombia en el año 2004.

Actualmente, se desempeña como Administrador en herramientas de Seguridad de la Información, de la Dirección de Inteligencia y realiza estudios de Postgrado en Seguridad Informática en la Universidad Piloto de Colombia.