EL RIESGO Y LA FALTA DE POLITICAS DE SEGURIDAD INFORMÁTICA UNA AMENAZA EN LAS EMPRESAS CERTIFICADAS BASC

Daniel Felipe González Agudelo
Código: 0800397

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD
ADMINISTRACION DE LA SEGURIDAD Y SALUD OCUPACIONAL
BOGOTÁ
2014

EL RIESGO Y LA FALTA DE POLITICAS DE SEGURIDAD INFORMÁTICA UNA AMENAZA EN LAS EMPRESAS CERTIFICADAS BASC

Ensayo presentado como requisito para obtener el título de
¨ADMINISTRADOR EN SEGURIDAD Y SALUD OCUPACIONAL¨

Daniel Felipe González Agudelo
Ensayo opción de grado

Cr. ® Luis Alfredo Cabrera Albornoz
Profesor Tutor Ensayo

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD
ADMINISTRACION DE SEGURIDAD Y SALUD OCUPACIONAL
BOGOTÁ
2014

1. Resumen Inicial

El presente ensayo está enfocado en el numeral 7 de los estándares de seguridad de la norma BASC, el cual menciona la seguridad en las tecnologías de la información (protección con contraseñas, responsabilidad y protección a los sistemas y datos). El tema a desarrollar se enfoca en la problemática que conlleva no tener políticas, procedimientos y/o normas de seguridad informática en las empresas certificadas BASC. La protección de datos, documentos y control de acceso a la información es un tema que cada día toma más fuerza en las grandes compañías, debido a las diferentes especialidades de hackers y crackers que roban información vital.

Los elementos de la información son denominados los activos de una institución los cuales deben ser protegidos para evitar su perdida, modificación o el uso inadecuado de su contenido.

Generalmente se dividen en tres grupos:

- Datos e Información: Son los datos e informaciones en si mismo
- Sistemas e Infraestructura: Son los componentes donde se mantienen o guardan los datos e informaciones
- Personal: Son todos los individuos que manejan o tienen acceso a los datos e informaciones y son los activos más difíciles de proteger, porque son móviles, pueden cambiar su afiliación y son impredecibles.

No tener una política de seguridad de la información clara y definida, lleva inevitablemente al acceso no autorizado a una red informática o a los equipos que en ella se encuentran y puede ocasionar en la gran mayoría de los casos graves problemas. El principal riesgo es el robo de información sensible y confidencial, el cual puede ocasionar hasta el cierre de una compañía solida financieramente.

La pérdida o mal uso de información confidencial genera daños y repercusiones relacionados con la confidencialidad, integridad y disponibilidad de los archivos para las empresas y a su vez para el titular del documento. La seguridad informática se distingue por tener dos propósitos de seguridad, la Seguridad de la Información y la Protección de Datos, estos se diferencian debido a que los datos son valores numéricos que soportan la información mientras que la información es aquello que tiene un significado para nosotros. En ambos casos las medidas de protección aplicadas serán las mismas.

Palabras clave: Seguridad Informática, protección de datos, hackers, crackers, elementos de la información.

2. Introducción

Sin lugar a duda una de las herramientas más importante producida en el siglo XX ha sido el computador, este ha provocado cambios agigantados en la sociedad y más aún en el futuro. En la actualidad, el entorno está prácticamente controlado por las nuevas tecnologías, que a medida que transcurre el tiempo avanzan sin límites y en ocasiones son utilizadas incorrectamente provocando daños de grandes dimensiones.

La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo la aparición de nuevas amenazas para los sistemas de información. Hoy es imposible hablar de un sistema 100% seguro, debido a que esta configuración no existe. Por eso las empresas asumen riesgos como perder un negocio o arriesgarse a ser hackeadas.

El delito informático esta catalogado como una actividad criminal en los diferentes países, los cuales han tratado de tipificar estos delitos en robos, hurtos, fraudes, falsificaciones, perjuicios, estafas y sabotajes.

Con la constante evolución de las computadoras es fundamental saber que recursos necesitar para obtener seguridad en los sistemas de información.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

3. Desarrollo del Tema

Los trascendentales cambios operados en el mundo moderno, caracterizados por su constante desarrollo; La acelerada globalización de la economía, la acentuada dependencia que incorpora el alto volumen de información y los sistemas que la proveen; El aumento de la vulnerabilidad y el amplio espectro de amenazas, tales como las amenazas cibernéticas, la escala y los costos de las inversiones actuales y futuras en información y en sistemas de información; y el potencial que poseen las tecnologías para cambiar drásticamente las organizaciones y las practicas de negocio, crear nuevas oportunidades, diseñar nuevas estructuras tecnológicas que permiten que la información sea cada día mas circulante. Tales cambios hacen que cada día el riesgo inminente en las tecnologías nos lleven a pensar en la problemática sobre la seguridad informática o seguridad de tecnologías y especialmente en la falta de políticas, procedimientos y/o normas de seguridad informática en las empresas certificadas BASC.

Si pensamos en la seguridad informática o seguridad de tecnologías de la información como el área de la informática que se enfoca en la infraestructura computacional y todo lo relacionado con esta y especialmente la información contenida o circulante, vemos la seguridad informática como la disciplina que se encarga de diseñar las normas, procedimientos, métodos, y técnicas destinadas a conseguir un sistema de información seguro y confiable. Por ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas convirtiéndose por ejemplo en información privilegiada.

En cuanto a la seguridad informática, las computadoras y el internet son ahora una parte familiar de nuestras vidas. Quizá no la veamos a menudo pero ahí están; involucradas de alguna manera en la mayoría de nuestras actividades diarias, en los negocios de cualquier empresa, en las instituciones educativas, en las diferentes áreas del gobierno, sin el apoyo de estas herramientas ninguna de ellas sería capaz de manejar la impresionante cantidad de información que parece caracterizar nuestra sociedad. Pero también existe una problemática en ellas, la seguridad; para ello se han desarrollado firewalls o dispositivos de software que protegen la integridad de las mismas. Cada vez más personas necesitaran conocer el manejo de las computadoras así como las protecciones que día a día se van ofreciendo para garantizarnos la seguridad en el manejo de la información.

Los inconvenientes en cuestión de seguridad no son conocidos por todos los usuarios de la red y por ello no saben cómo protegerse de dicha vulnerabilidad que tienen cada vez que se conectan a esta red de trabajo.

Convendría hablar un poco de que se entiende por seguridad informática. En este ensayo se entenderá como la protección frente a ataques e intrusiones en recursos corporativos por parte de intrusos a los que no se permite acceso a dichos recursos. La seguridad siempre esta relativa al tipo de servicios que se requiere ofrecer a los usuarios autorizados, según se establece en la política de seguridad de la empresa.

La idea de este ensayo es que todas las personas y en especial las empresas certificadas BASC se interesen y aprendan a valorar lo importante que es la información tanto para las grandes, medianas y pequeñas empresas y se interesen por capacitar a sus empleados sobre sistemas de seguridad que alejen visitas de posibles hackers y establecer normas que minimicen los riesgos a la información o infraestructura informática.

Para Erb, Markus (2014) la seguridad informática está concebida para proteger los activos informáticos como:

- *La infraestructura computacional: Siendo esta la parte fundamental para el almacenamiento y gestión de la información, debe ser protegida por un área encargada de velar que los equipos funcionen adecuadamente y protegerlos en casos de fallas, robos, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.*

- *Los usuarios: Se les deben diseñar protocolos que permitan proteger la información que manejan, para que esta no se vuelva vulnerable y su vez sea capacitarlos sobre las posibles amenazas existentes no solo surgidas por la programación y el funcionamiento de un dispositivo de almacenamiento sino también por programas maliciosos que puedan ser instalados por alguna circunstancia y abran la posibilidad a virus informáticos o a un programa espía. Existen también errores de programación pues pueden ser usados como exploits por los crackers produciéndose así el robo de la información o la alteración del funcionamiento.*

Según el Computer Security Institute (CSI) de San Francisco; Aproximadamente entre el 60 y el 80% de los incidentes de red son causados desde dentro de la misma.

¨Existe una amenaza informática del futuro, pues si en algún momento el objetivo de los ataques fue cambiar las plataformas tecnológicas, ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los certificados que contienen la información digital. El área semántica que era reservada para los humanos se convirtió ahora en el núcleo de los ataques debido a la evolución de la web y las redes sociales¨. (Ramírez, E. & Aguilera, A. 2009)

Las amenazas informáticas del futuro ya no son con la inclusión de troyanos en los sistemas o software espías sino con el hecho de que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

La web 3.0 basada en conceptos como elaborar, compartir y significar está representando un desafío para los hacker que ya no utilizan las plataformas convencionales de ataque sino que optan por modificar los significados del contenido digital, provocando así la confusión lógica del usuario permitiendo de este modo la intrusión en los sistemas.

Creo conveniente definir las principales redes que se manejan a nivel mundial y que se relacionan con la seguridad informática. En primer lugar tenemos la WAN (World Area Network) es una gran red de computo de cobertura mundial y una de las más comunes en internet. En segundo lugar esta LAN (Local Area Network) que es una red mediana denominada local ya que está limitada a una pequeña área geográfica y normalmente es utilizada por empresas privadas, publicas, educativas etc. Estas dos redes llegan a interactuar utilizando un conjunto de protocolos de comunicación de datos llamado TCP/IP es de los protocolos más comunes, sus siglas significan Protocolo de control de transmisión y protocolo de internet. Estos permiten el enrutamiento de información de una maquina a otra, la entrega de correo electrónico y noticias e incluso conexión remota. Vale la pena conocerlos pues nos ayudan a minimizar los riesgos informáticos.

Es importante tener una política de seguridad informática bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la compañía. Si actualmente sus usuarios tienen acceso irrestricto a la red, puede ser difícil aplicar una política que limite ese acceso. También es importante tomar en cuenta la política de seguridad que dichas empresas certificadas BASC deben asumir para que no se disminuya la capacidad de la organización. Una política de red que impide que los usuarios cumplan efectivamente con sus tareas puede traer consecuencias indeseables. Los usuarios quizá encuentren la forma de eludir la política de seguridad, lo cual la vuelve inefectiva.

Una política de seguridad informática efectiva es algo que todos los usuarios y administradores de redes pueden aceptar y estar dispuestos a aplicar.

Cada empresa puede tener muchos sitios y cada uno contar con sus propias redes. Si la empresa es grande, es muy probable que los sitios tengan diferente administración de red con metas y objetivos diferentes. Si estos sitios no están conectados a través de una red interna, cada uno de ellos puede tener sus propias políticas de seguridad en la red, sin embargo, si los sitios están conectados mediante una red interna, la política de red debe abarcar todos los objetivos de los sitios interconectados.

Los componentes que podemos considerar en una red los menciona Cristian Borghello (2009)

Un sitio es cualquier parte de una empresa que posee computadoras y recursos relacionados con redes. Algunos no todos, de esos recursos son:

- *Estaciones de trabajo*
- *Computadoras host y servidores*
- *Dispositivos de interconexión*
- *Servidores de terminal*
- *Software para conexión de red y de aplicaciones*
- *Cables de red*
- *La información de archivos y bases de datos*

La política de seguridad de los sitios debe tomar en cuenta la protección de estos recursos. Debido a que el sitio está conectado a otras redes, la política de seguridad del sitio debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas

Definir una política de seguridad de red significa elaborar procedimientos y planes que salvaguarden los recursos de la red contra pedida y daños. Uno de los enfoques posible para elaborar dicha política propondrá examinar lo siguiente:

- Que recursos está usted tratando de proteger?
- De quienes necesita proteger los recursos?
- Que tan posibles son las amenazas?
- Que tan importante es el recurso?
- Qué medidas puede implementar para proteger sus bienes de forma económica y oportuna?
- Examinar periódicamente su política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red.

En general el costo de proteger las redes de una amenaza debe ser menor que el de recuperación en caso de que se viera afectado por una amenaza de seguridad si no se tiene el conocimiento suficiente de lo que se está protegiendo y de las fuentes de amenaza, puede ser difícil alcanzar un nivel aceptable de seguridad.

Es importante hacer que en el diseño de la política de seguridad participe la gente adecuada. Un aspecto importante de la política de seguridad es asegurar que todos conozcan su propia responsabilidad para mantenerla, es entendible que este conjunto de normas llamadas políticas se anticipen a todas la amenazas que existen, sin embargo, esta no puede asegurar que para cada tipo de proceso haya alguien que lo pueda manejar de manera consciente y responsable.

Los niveles de seguridad pueden ser variados dentro de las normas establecidas, por ejemplo: Cada usuario de la red debe ser responsable de sus accesos o contraseñas; por otra parte, los administradores de la red y del sistema son responsables de controlar y garantizar la seguridad general de la red.

Los riesgos deben clasificarse por nivel de importancia y gravedad de la perdida, no debe terminar en una situación en que sea más el gasto de asegurar que el propio valor de lo que estemos protegiendo. En el análisis del riego hay que determinar dos factores:

1. Estimación del riesgo en el momento de perder el recurso
2. Estimación de la importancia del recurso

Los recursos que se deben considerar al calcular las amenazas a la seguridad general son:

1. HARDWARE: Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadores personales, impresoras, unidades de disco externas, líneas de comunicación, servidores terminales, routers.
2. SOFTWARE: Programas fuente, programas objeto, programas de diagnostico, sistemas operativos, programas de comunicación.
3. DATOS: Durante la ejecución, almacenados en línea, archivados fuera de línea, respaldos, registros de auditoría, bases de datos.
4. PERSONAS: Usuarios, personas necesarias para operar dichos sistemas.
5. DOCUMENTACION: Sobre programas, hardware, sistemas, procedimientos administrativos.
6. SUMINISTROS: Papel, formularios, cintas, medios magnéticos.

El acceso a los recursos de la red debe estar permitido solo a usuarios autorizados, el préstamo de contraseñas y accesos debe estar constituido como una violación a las políticas de seguridad y debe ser sancionado drásticamente en caso de presentarse. El solo hecho de conceder acceso a usuarios no autorizados puede causar

daños irreparables por la cobertura negativa de los medios a la compañía que sea víctima de estas malas prácticas e intenciones dañinas.

Por lo anterior surgen las políticas de seguridad, como una herramienta organizacional que valoriza y concientiza a los trabajadores, clientes y proveedores sobre la importancia y la sensibilidad de la información y sobre los métodos para asegurar el buen uso de los recursos informáticos, manteniéndolos libres de peligros, daños y riesgos.

A continuación, encontramos los tres principios que debe cumplir todo sistema informático para garantizar la seguridad en general, llamado también CID.

CONFIDENCIALIDAD se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasores y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están físicamente y lógicamente interconectados.

INTEGRIDAD se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mimos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

DISPONIBILIDAD: se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben reforzar la permanencia del sistema, en condiciones de actividad adecuadas para que los usuarios accedan a los

datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromisos con el usuario, son prestar servicio permanente.

De esta forma las empresas certificadas BASC deben definir los elementos de análisis de riesgo a través de un proceso que les permita generar una política de seguridad en donde se identifique los dispositivos y la manera como se relacionan los cálculos realizados. Este análisis es fundamental para lograr una correcta administración del riesgo.

El reto es saber administrar y gestionar los recursos de dichas empresas con el fin de establecer políticas efectivas de seguridad informática, confiables y acordes a la legislación Nacional determinadas por el gobierno y amparadas por la norma Mundial.

Como planteamiento final cabe recordar que existen diversas especialidades dentro de los actores que ejecutan estos delitos informáticos, algunos de los más reconocidos según sus características son los hacker los cuales son personas interesadas en el funcionamiento de los sistemas operativos y les gusta husmear por todas partes para llegar a conocer el funcionamiento de un sistema informático, su nombre en ingles hace referencia a un delincuente silencioso, además tienen la capacidad de crear sus propios programas de software para entrar a los sistemas y toman su actividad como un reto intelectual pero no pretenden hacer daños e incluso se apoya en un código ético. Los hackers se caracterizan por ser verdaderos expertos en el uso de computadores y por lo general rechazan hacer un uso delictivo de sus conocimientos, aunque no tienen reparo en intentar acceder a cualquier máquina conectada a la red, o incluso penetrar a una intranet privada siempre con el declarado fin de investigar las defensas de estos sistemas y sus lados débiles.

En la mayoría de casos ellos dan a conocer a sus víctimas los huecos de seguridad encontrados e incluso sugieren cómo corregirlos, otros llegan a publicar sus hallazgos en revistas o páginas web de poder hacerlo. Los cracker son otra especialidad

pero estos son personas que se introducen en los sistemas con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas.

El cracker es aquel hacker fascinado por su capacidad de romper sistemas y software y que se dedica única y exclusivamente a crackear sistemas. Crack es sinónimo de rotura y como su nombre indica se dedican a romper las protecciones y otros elementos de seguridad de los programas comerciales, en su mayoría con el fin confeso de sacar provecho de los mismos del mercado negro. Sus acciones pueden ir desde la destrucción de información ya sea a través de virus u otros medios hasta el robo de datos y venta de ellos. Ejemplo de su actuar ilegal son los millones de CDs con software pirata que circulan por el mundo entero y de hecho muchas personas no llegan a sospechar que parte del software que tienen en sus equipos son craqueados.

Otra especialidad son los phreaker los cuales se especializan en telefonía, tienen conocimientos profundos de los sistemas de telefonía tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago ya que la telefonía celular las emplea habitualmente. Estos buscan burlar la protección de las redes públicas y corporativas de telefonías desde sistemas computacionales, con el declarado fin de poner a prueba conocimientos y habilidades para obviar la obligatoriedad del pago por servicio e incluso lucrarse con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de hacking a sus servidores. Los gurús son los maestros y enseñan a los futuros hackers, normalmente se trata de personas que tienen amplia experiencia sobre los sistemas informáticos y están allí para enseñar o sacar de cualquier duda al usuario. El gurú no está activo, pero absorbe conocimientos ya que sigue practicando, pero para conocimiento propio y solo enseña las técnicas más básicas. Por ultimo existe un especialista llamado Trashing el cual obtiene información secreta o privada que logra por la revisión no autorizada de la basura descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas.

El tema se enfoca en que las organizaciones no tienen una política o norma que permita tener un adecuado manejo en la seguridad y protección de datos, o mas delicado aun que el personal que labora en las organizaciones no atiende los requerimientos y capacitaciones enfocadas a la protección y control de acceso a los datos.

Acerca de este tema se realizo una investigación en Colombia, que muestra con datos estadísticos la situación de la seguridad de la información; Citamos a continuación los resultados presentados por Alejandro Hernández, Country Manager Colombia para el Info Security News en el año 2011:

Cerca de 700 profesionales de los diferentes sectores de la empresa colombiana, incluyendo empresa privada, sector gobierno, PYMES y empresas grandes, respondieron una encuesta generada para medir el nivel de seguridad de la información en ésta área.

Los resultados son alarmantes, ya que dejan claro que los empresarios, no existe conciencia de los pros y los contras que hay en el acceso a mejores tecnologías de la información y las comunicaciones.

- *81 % de las empresas nunca ha implementado una herramienta para gestión de riesgos.*
- *53% ha instalado antivirus en todas las tecnologías de su empresa incluyendo las móviles.*
- *40% No revisa el marco normativo de seguridad de la información implementando en la empresa*
- *52% no ha implementado en su empresa ningún estándar internacional de Infosec*

- *47% nunca hizo ningún test de seguridad de las redes (Ethical Hacking, Análisis De Vulnerabilidades y/o Pruebas De Penetración en su empresa)*
- *47% no cuenta con un Plan de Continuidad del Negocio que le permita seguir con las operaciones en caso de un evento no deseado.*

Después de analizar las encuestas se llegó a la conclusión de que la empresa colombiana no distingue entre seguridad informática y seguridad de la información, inclusive conoce poco la legislación colombiana en materia de TICS: Todo esto no permite lograr una concientización en materia de seguridad de los actores que intervienen en la empresa colombiana, incluyendo clientes y proveedores.

Factor que lleva a que no sean partícipes reales de buenas prácticas internacionales en materia de protección de la información.

A pesar de que hay empresas que se preocupan por la seguridad en éste ámbito, son muchas las empresas colombianas que carecen del conocimiento necesario respecto a este tema, lo que las hace vulnerables a robos o fraudes.

Las recomendaciones que propone ISEC INFORMATION SECURITY son la capacitación comenzando desde la alta gerencia, el establecimiento de políticas empresariales alineadas a la legislación existente dentro del país y fuera de éste, la concientización de todos los actores involucrados en la vida de cada empresa, y finalmente la toma de medidas para evitar delitos informáticos, producto de los avances tecnológicos.

Teniendo en cuenta la investigación anterior, toda compañía o empresa que aspire a ser certificada BASC debe contar con políticas de seguridad informática y como mínimo deben considerar los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.
- Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.
- Los recursos del sistema y la información manejada en el mismo ha de ser útil para alguna función.
- La información del sistema debe estar disponible tal y como se almacenó por un agente autorizado, esto se define como integridad.
- El sistema debe ser capaz de verificar la identidad de sus usuarios, y los usuarios del sistema, esto se define como autenticidad.
- La información sólo debe estar disponible para agentes autorizados, especialmente su propietario, esto se define como confidencialidad.
- Posesión: Los propietarios de un sistema deben ser capaces de controlarlo en todo momento; Perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.
- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.

- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.
- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

En Colombia se tiene el problema que no hay suficientes personas capacitadas para tratar el tema de la seguridad informática, sumado a que no existe la cultura de seguridad. Es por esto que es permitible realizar algunas sugerencias para aplicar la seguridad informática en las empresas certificadas BASC.

1. Usar contraseñas robustas, todas deben ser diferentes además de contener letras mayúsculas y minúsculas, números u otros caracteres. Esto aplica para cuentas de correo, claves de acceso a sistemas, programas y claves de cuentas bancarias.

2. Encripte información sensible, de esta manera aunque un hacker haya ingresado a su pc, será más difícil que vea su información.

3. Use conexiones de internet seguras. Cuando ingrese a páginas bancarias revise que contenga la siguiente estructura https:// en lugar de http://

4. Esté alerta en Facebook y redes sociales, evite hacer click en cualquier anuncio o aplicación que no conozca. Existen innumerables casos de personas que han contagiado sus computadoras con virus al hacerlo.

5. Cuidado al usar computadoras públicas muchos servicios de redes sociales permiten mantener activa la sesión, no olvide finalizarla antes de alejarse de esa computadora.

6. Actualice su software la mayoría de las amenazas prosperan debido a fallas en el software. Mantenerlo actualizado eleva significativamente su seguridad informática.

7. Respalde su información mantenga un back up de la información crítica.

8. Asegure sus redes algunos ataques a altos ejecutivos han iniciado en sus propios hogares. Mediante diversas técnicas es posible interceptar los datos que viajan en una red inalámbrica insegura. Se recomienda usar redes conocidas las cuales tengan claves de acceso.

9. Cuide su celular este contiene información que no debe caer en manos de extraños. Se recomienda desactivar el Bluetooth, wi-fi o infrarrojos, instálele un antivirus y manténgalo actualizado, active el acceso mediante pin y bloquee la tarjeta sim en caso de pérdida.

4. Conclusiones

Actualmente, las empresas modernas operan y centran gran parte de su actividad a través de la tecnología y el internet, necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades; en este sentido cobra especial importancia el hecho de que puedan contar con mecanismos y elementos fundamentales de las nuevas tecnologías de seguridad que implementen y gestionen de manera eficaz sus sistemas de información.

Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe proteger y asegurar para garantizar su integridad, confidencialidad, entre otros servicios de seguridad.

La sociedad de la información y nuevas tecnologías de comunicación plantean la necesidad de mantener la usabilidad y confidencialidad de la información que soportan los sistemas en las organizaciones; para ello es especialmente importante elegir e implementar los sistemas y métodos de seguridad más idóneos que protejan las redes y sistemas ante eventuales amenazas, ya sean presente o futuras.

Los aspectos de seguridad y control de la información deben ser una prioridad para las compañías, debido a que las amenazas pueden surgir tanto desde el exterior como desde el interior de la organización (virus, hackers, empleados, etc.). El plan de seguridad de la información de una organización debe tratar todas estas amenazas que con el uso de internet se ven amplificadas, debido a que los principales ataques a los sistemas y a la información provienen de la red. La alta gerencia debe decidir el tiempo, dinero y esfuerzo, que hay que invertir para desarrollar las políticas y controles de seguridad apropiados puesto que cada organización debe analizar sus necesidades específicas y determinar sus requisitos y limitaciones en cuanto a recursos y programación. Cada sistema informático, entorno y directiva organizativa es distinta, lo

que hace que cada estrategia de seguridad sea única, sin embargo los fundamentos de una buena seguridad siguen siendo los mismos.

La implementación de políticas de seguridad informática en una organización es una solución que no sólo busca proteger, preservar y administrar de una manera eficiente todo tipo de recursos con los que cuenta una organización, sino que también busca dar solución, prevenir, evitar, controlar y minimizar los daños de incidentes que afectan a la organización es por esto que preparar y capacitar al personal en temas asociados a la seguridad informática y cómo hacer frente a incidentes que se llegarán a presentar con el fin de responder de una manera adecuada es una de las principales metas de esta estrategia. Capacitar al personal de la compañía es primordial debido a que éste puede tomar un papel activo dentro de la organización de manera que aplique este conocimiento en las diversas actividades que realiza dentro y fuera de la organización con el propósito de proteger de una forma adecuada la información que se le confía, así como la propia.

5. Bibliografía

Borghello, Cristian. F. (2009). *Seguridad Informática: sus implicancias e implementación*. Según.Info: Tesis de Seguridad de la información. Recuperado de http://www.segu-info.com.ar/tesis/

Erb, Markus. (2014). *Seguridad de la Información y Protección de Datos.* Protegete.Wordpress.com: Gestión de Riesgo en la Seguridad Informática. Recuperado de http://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

Hernández, Alejandro. (2011). *Inseguridad de la información de la empresa colombiana.* Estadísticas. Info Security News. Recuperado de: http://www.infosecurityvip.com/newsletter/estadisticas_ago11.html

ISO (2005). *Gestión de la seguridad de la información.* Norma ISO / IEC 27001.

Mifsud, Elvira. (2012). *Introducción a la seguridad informática.* Ministerio de Educación, Cultura y Deporte (España): Observatorio Tecnológico. Recuperado de http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

ONU. (2000). *Prevención eficaz del delito: adaptación a las nuevas situaciones.* Recuperado de http://www.uncjin.org/Documents/congr10/10s.pdf

ONU. (2010). *Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético*. Recuperado de

https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf

Ramírez, E. & Aguilera, A. (2009). *Los delitos informáticos. Tratamiento internacional*. Edumet.net: Contribuciones a las Ciencias Sociales. Recuperado de http://www.eumed.net/rev/cccss/04/rbar2.htm

Rios, Julio. (2014). *Seguridad Informática, parte 2.* Monografias.com: Computación. Recuperado de http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

Stolk, Alejandra. (2013). *Técnicas de seguridad informática.* Venezuela: Editorial Eslared.