IMPORTANCIA DE IMPLEMENTAR EL SGSI EN UNA EMPRESA CERTIFICADA BASC

SHIRLEY ALEXANDRA SÀNCHEZ TORRES
Autor

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD
PROGRAMA DE ADMINISTRACIÓN DE LA SEGURIDAD Y SALUD OCUPACIONAL
BOGOTÀ, D.C
OCTUBRE, 2014

IMPORTANCIA DE IMPLEMENTAR EL SGSI EN UNA EMPRESA CERTIFICADA BASC

SHIRLEY ALEXANDRA SÀNCHEZ TORRES

Asesor:
LUIS ALFREDO CABRERA ALBORNOZ
Coronel (RA)

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD
PROGRAMA DE ADMINISTRACIÓN DE LA SEGURIDAD Y SALUD OCUPACIONAL
BOGOTÀ, D.C
OCTUBRE, 2014

Resumen

Los últimos desarrollos tecnológicos se han convertido en una herramienta de uso fundamental para todas las organizaciones dado que los procesos e información que se manejan han pasado de estar en medio físico a medio electrónico, es decir antiguamente la información se encontraba soportada de múltiples formas gráficas y debido a los avances tecnológicos se han venido incluyendo en forma digital , lo cual permite que su forma de acceder sea más fácil y se pueda hacer desde cualquier dispositivo digital que existe en la actualidad como los celulares, iPad, Tablets, PC entre otros, usando como canal de comunicación el Internet. Para una empresa certificada BASC, es fundamental la información que maneja como fechas, rutas, cantidad de materiales entre otras, las cuales son imprescindibles en el buen desarrollo del proceso de exportación, razón por lo cual cada vez son un objetivo para los delincuentes cibernéticos cuyo interés es obtener la información para fines malintencionados como robo, estafa, soborno, entre otros. Esto crea la necesidad de contar con un SGSI (Sistema de Gestión de Seguridad de Información), teniendo en cuenta las normas ISO 27001 e ISO/IEC 27005, que brindan parámetros para gestionar los riesgos y lograr un nivel de seguridad óptimo, es decir que se minimicen los riesgos de tener una pérdida o daño en la información del proceso de exportación.

Palabras Claves: Información, Seguridad de la información, Ataques, Intrusos, Gestión del Riesgo

Introducción

La información se puede considerar el segundo mayor activo de una empresa porque tiene un valor para la organización es decir, es una parte fundamental para el desarrollo normal de sus procesos lo que hace necesario que cualquier empresa sin importar si es pública o privada implemente un sistema de protección, para garantizar el normal funcionamiento e incluso la continuidad de su razón de ser.

Con la aparición de la tecnología el ser humano siempre busca hacer más fácil su vida, por lo que aprovecha las aplicaciones digitales para sustituir la información que anteriormente se plasmaba de múltiples formas escritas; es decir ahora la información se encuentra almacenada en sistemas informáticos, resaltando el hecho de que este sistema ha tomado importancia a nivel mundial, por lo que se ha incrementado la cantidad de dispositivos electrónicos y a la vez los usuarios que acceden a este sistema a través de las redes.

El ser humano ha adoptado las tecnologías como un elemento primordial para su desarrollo tanto a nivel personal como laboral, así como estas herramientas avanzan día a día, los delincuentes también se encuentran a la vanguardia identificando las vulnerabilidades existentes en los sistemas informáticos, para crear nuevas formas e ingresar al sistema y cumplir con sus fines delictivos.

Teniendo en cuenta que las organizaciones al usar las herramientas tecnológicas se han vuelto dependientes del sistema informático, se genera la necesidad que las empresas exportadoras certificadas BASC, implementen un SGSI (Sistema de Gestión de Seguridad de Información), lo cual permite mantener su integridad y seguridad, que a su vez se convierte en una ventaja competitiva, porque al implementar este sistema se aplica control para minimizar los riesgos de que los intrusos cibernéticos tengan acceso a esta y puedan arruinar el normal funcionamiento del proceso de exportación.

Importancia de implementar el SGSI en una empresa certificada BASC.

A través de la historia la información siempre ha estado presente en todos los aspectos de la vida y el ser humano le ha dado un valor subjetivo, por lo que actualmente se considerada el segundo mayor activo de una empresa porque es uno de los recursos fundamentales para el desarrollo normal de los procesos que manejen y los cuales son la razón de ser de la organización.

Se debe tener claro que la información en cierto modo es intangible y por esto es necesario contar con un soporte, entre las múltiples formas que existen se resalta que antiguamente la información se plasmaba en documentos y hoy en día por los avances en la tecnología, los procesos se están almacenando en sistemas informáticos los cuales se transmiten a través de las redes, siendo así como se empieza a hablar de sistematización.

Es indiscutible la importancia que tiene la información para una organización por lo que se puede tomar como referente la definición que da la ISO 27001/2013 *"La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegido adecuadamente"*, de acuerdo a lo anterior es necesario que las organizaciones tomen las medidas necesarias para mantener protegida la información y así mismo los sistemas en los que se encuentra soportada esta.

Es así como existe una relación entre la información y la informática, la primera es el activo primordial de los procesos de una empresa y la segunda es la encargada de procesar y almacenar la información en los equipos tecnológicos, tales como (discos, memorias, backups), por esta razón es importante que las empresas implementen un sistemas que les permita salvaguardar la información, creando controles efectivos que impidan que los delincuentes puedan acceder al sistema con intereses malintencionados como el robo de la información o ejecutar acciones delictivas que puedan afectar la continuidad del negocio.

Efectuando un análisis de lo descrito anteriormente se infiere que es primordial que una empresa implemente el SGSI (Sistema de Gestión de Seguridad de la Información) con el fin de gestionar los riesgos y así minimizar la materialización de estos, la NTC-ISO/IEC 27001 define la gestión de riesgos como " las actividades coordinadas para dirigir y controlar una organización en relación con el riesgo" y a la vez establece la Seguridad de Información como la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Teniendo claro estos conceptos se hace necesario resaltar que en las empresas existen personas autorizadas para acceder a la información y que según el Fondo de Tecnologías de la información y las Comunicaciones de la República de Colombia la información tiene una clasificación así:

Tabla 1: clasificación de seguridad

Información que requiere protección por razones de interés público o privacidad personal	
Sensitiva	El compromiso de la información podría dañar los intereses del Estado o poner en peligro la seguridad de los ciudadanos
En confianza	El compromiso de la información podría perjudicar el mantenimiento de la ley y el orden, impedir la conducta efectiva del Gobierno o afectar adversamente la privacidad de sus ciudadanos.
Pública no clasificada	El compromiso de la información afecta la imagen de la entidad.

Tomado de http://wikigel.softwareworks.com.co/Wordpress/wp-content/uploads/SeguridaddelaInformaci%C3%B3n2-0_Anexo7_Clasificacion-de-Activos.pdf

Referente a la tabla anterior es importante destacar que la clasificación que requiere protección por razones de interés público o privacidad personal hace referencia a la

información que de ser robada puede llegar a afectar a una entidad, empresa o a una persona. En el caso de una empresa certificada BASC la información que se considera sensitiva son las rutas que se utilizaran para la exportación pues de llegar a manos equivocadas esta información puede llegar a presentarse algún tipo de contaminación a la carga, razón por la cual se presentaría afectación a la imagen del país y de la empresa exportadora, de la misma forma la seguridad del personal que maneja esa carga.

La información que se puede considerar en confianza son las bases de datos de los clientes, proveedores, de los empleados y todos los asociados de negocio de la empresa exportadora, es por esta razón que existen Políticas de Privacidad de Datos Personales.

Por último la información pública no clasificada es cuando cierta información como los estados financieros o documentos que son públicos al elaborarse presentan datos erróneos afecta la imagen de la organización.

Es fundamental tener conocimiento de los tres requerimientos de la información para garantizar el cumplimiento de la seguridad, que de acuerdo a la ISO 27001 son:

- ***Confidencialidad:*** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados, un ejemplo es cuando un exempleado publica información propia de la organización.
- ***Integridad:*** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso, es cuando un intruso modifica o manipula la información.
- ***Disponibilidad*****:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Se debe tener en cuenta que el sistema informático cuenta con tres elementos principales los cuales se deben proteger (Gómez, 2011)

1. El hardware: son los componentes tangibles de un PC.
2. El software: son los sistemas operativos de red es decir la parte lógica del PC.
3. Los datos: son los usuarios y las contraseñas personales.

Con base en lo anterior es evidente que no basta solo con identificar las falencias del sistema informático, también se debe tener claro a quién o quienes les interesa la información de la empresa, pueden ser competidores, rivales, enemigos, trabajadores internos, delincuentes comunes, o simplemente individuos aficionados a acceder a la información de una empresa para verificar hasta donde el sistema es factible de ser vulnerado, en este caso existen varios tipos de intrusos cibernéticos como lo define Álvaro Gómez en la enciclopedia de la seguridad informática :

- ***Hackers:*** son personas que se dedican a estas tareas como pasatiempos y como reto técnico: entran a los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos de los entresijos de Internet, pero no pretenden provocar daño en estos sistemas.
- ***Crackers:*** son individuos con interés de atacar un sistema informático para obtener beneficios de forma ilegal o, simplemente para provocar algún daño a la organización propietaria del sistema, motivados por intereses económicos, políticos, religiosos etc.
- ***Sniffers:*** son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como Internet. (
- ***Spammers:*** son los responsables del envió de miles de mensajes de correo electrónico no solicitados a través de redes como internet, provocando el colapso de los servidores y la sobrecarga de los buzones de correo de los usuarios.
- ***Personal*** (se pasa por alto el hecho de la persona de la organización incluso a la persona ajeno a la estructura informática, puede comprometer la seguridad de los equipos).
- ***Ex-empleados*** (generalmente se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema del que conocen

perfectamente, pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aún trabajaran en la organización).

- ***Curiosos*** (son los atacantes juntos con los crackers los que más se dan en un sistema)
- ***Intrusos remunerados*** (se trata de personas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema que son pagados por una tercera parte generalmente para robar secretos o simplemente para dañar la imagen de la organización).

Al hacer el análisis de las amenazas en contra de la tecnología se encuentra que actualmente el más latente es el ataque informático, razón por la cual se hace necesario que las personas responsables del manejo de información dentro de una organización, tengan el suficiente conocimiento para evitar que estas se materialicen., es decir que tengan en cuenta que actualmente hay múltiples formas de acceder a la información a través de dispositivos como celulares, fax, impresoras, iPad, Tablets, entre otros, al igual que existen múltiples formas en las que cualquier persona puede robar, manipular o modificar la información, aprovechando los medios tecnológicos y el uso de la red.

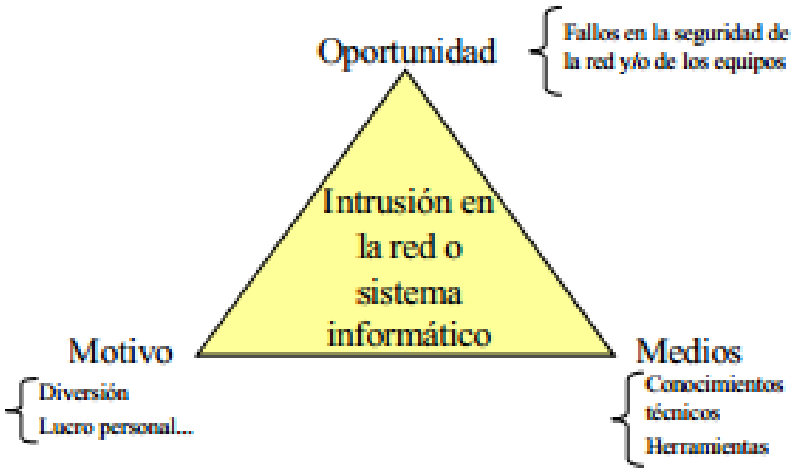
Las debilidades del sistema informático son aprovechadas por los delincuentes para causar daños o perdidas a una empresa, facilitando la ocurrencia de un ataque y dentro de las cuales podemos mencionar las siguientes:

- ***Interrupción:*** hace referencia a cuando un activo como la información se pierde, no está disponible, o no se puede utilizar (Gómez, 2011)
- ***Intercepción:*** es cuando alguna parte (persona, programa o sistema de cómputo) accede a la información sin ninguna autorización. (Gómez, 2011)
- ***Modificación:*** cuando una persona no autorizada accede y manipula indebidamente la información (Gómez, 2011)
- ***Generación:*** es cuando un individuo inserta o crea objetos falsos en un sistema computacional. (Gómez, 2011)

Teniendo claro los tipos de intrusos y las debilidades que tiene el sistema informático es preciso conocer que el **TRIANGULO DE LA INTRUSIÓN,** define de manera puntual, coherente y precisa la forma en que se interrumpe un sistema por parte de un delincuente, para que este se materialice en un sistema informático es necesario que se presente tres factores:

La oportunidad, que hace referencia a las vulnerabilidades que tiene el sistema informático, **El medio,** el cual se refiere a las herramientas y al conocimiento que tiene y usa el ciberdelincuente y el **Motivo,** es la razón que tiene el ciberdelincuente para ingresar a un sistema informático ajeno a su responsabilidad.

Imagen 1: Triangulo de la intrusión



Fuente: Gómez, 2011 *"enciclopedia de la seguridad informática"* pág. 196

El autor Álvaro Gómez Vietes en la "Enciclopedia de la Seguridad Informática" identifica tres tipos de riesgos que se encuentran en la seguridad de informática y son:

1. ***Natural:*** como por ejemplo los desastres naturales
2. ***Agentes externos:*** ataques.
3. ***Agentes internos***: en los que se encuentran exempleados y empleados de la organización

En este caso se analizaran los agentes externos que pueden llegar a vulnerar los sistemas informáticos para realizar sus actividades malintencionadas, es por esto que a continuación se mencionan algunos tipos de ataques que define el autor Vicente Aceituno Canal (2006):

- ***Espionaje:*** es el acceso ilegitimo a la información y su objetivo es revelar secretos.
- ***Suplantación:*** es cuando alguien simula ser otra persona, para esto se debe contar con sistemas de autenticación.
- ***Sabotaje:*** es un ataque destructivo cuyo objetivo es producir daño, para reducir esta amenaza se debe eliminar las oportunidades de acceso.
- ***Chantaje:*** es un ataque destructivo cuyo objetivo es producir daño y va acompañado de extorsión.

El ataque que más se presenta en el sistema informático es el ***código malicioso,*** entre los que se encuentra **EL MALWARE** el cual es un programa o software creado con un fin dañino, como infiltrarse a un sistema operativo sin el consentimiento del propietario, el malware tiene a siguiente clasificación:

Imagen 2 – Clasificación de malware

Tomado de https://edu.eset-la.com/default/std/myevents/7116#

En tabla anterior se hace una breve clasificación de los Malware existentes, entre los que se encuentran: ***el virus*** el cual infecta los archivos alterándolos y se propaga por sí solo, ***el gusano*** también tiene la capacidad de propagarse por sí solo, ***el troyano*** y ***spyware*** necesitan de la intervención del ser humano para propagarse, el ***Adware, Rogue*** y ***Ransomware*** aparte de propagarse por manipulación del ser humano tienen efectos visuales, y todos son programas maliciosos.

Una vez se tiene conocimiento sobre la tipología de malware existente es importante tener claro los aspectos o fases que según el autor Álvaro Gómez Vietes en su escrito "Enciclopedia de la Seguridad Informática" deben darse para la materialización de una Ataque:

1. ***Descubrimiento y exploración del sistema informático:*** Es cuando el intruso encuentra un objetivo y hace un análisis sobre el sistema que maneja este.
2. ***Búsqueda de vulnerabilidades en el sistema:*** el intruso hace análisis e identificación de las vulnerabilidades que el sistema tiene.
3. ***Explotación de las vulnerabilidades detectadas:*** se aprovecha de las vulnerabilidades encontradas.
4. ***Corrupción o compromiso del sistema:*** modificación de programas y ficheros del sistema para dejar instaladas determinadas puertas traseras o troyanos; creación de nuevas cuentas con privilegios administrativos que faciliten el posterior acceso del atacante al sistema afectado.
5. ***Eliminación de las pruebas que pueden revelar el ataque y el compromiso del sistema:*** eliminación o modificación de los registros de actividad del equipo ("logs"); modificación de los programas que se encargan de monitorizarla actividad del sistema.

Según los resultados de una encuesta realizada por Kaspersky Lab y la compañía analítica B2B International en el 2013 y publicada por Kaspersky Security Bulletin 2013 en http://www.viruslist.com/sp/analysis?pubid=207271238, el 91% de las empresas

encuestadas en todo el mundo fueron víctimas de por lo menos un ataque al año y el 9% de las compañías fueron víctimas de ataques selectivos.

Imagen 3- resultados encuesta Kaspersky Security Bulletin 2013

Tomado de: http://www.viruslist.com/sp/analysis?pubid=207271238

Como se observa en la imagen anterior se comprueba que actualmente los códigos maliciosos (explicados anteriormente), son las amenazas más latentes y a las que se les debe implementar controles.

Ante la situación anteriormente mencionada, la certificación BASC que es la alianza que promueve el comercio seguro, exige que las empresas interesadas en hacer parte del comercio internacional cumplan con unos estándares de seguridad, por esta razón es importante que una empresa certificada BASC establezca estrategias y controles que garanticen la seguridad de su información, se debe implementar el Sistema de Gestión de Seguridad de la Información, para mantener el nivel de seguridad de su

actividad comercial evitando pérdidas y robo de la información, incluyendo la protección del sistema informático contra los ataques explicados anteriormente.

El objetivo principal que tiene una empresa al hacer la implementación de un SGSI es identificar los riesgos para gestionar los controles pertinentes con el fin de mantener la confidencialidad, integridad y disponibilidad de la información. Para una empresa certificada BASC un punto de partida para hacer la implementación del SGSI es el ESTANDAR BASC Versión 3-2008 Adopción de Requisitos Mínimos de Seguridad C-TPAT Exportador, donde indica los criterios mínimos de seguridad que la empresa debe tener y entre ellos se encuentra la Seguridad en las Tecnologías de Información, estableciendo algunos parámetros como:

- Se debe establecer política y normas de tecnología de información.
- Hacer capacitaciones a todo el personal donde se les dé a conocer los procedimientos de seguridad.

Para implementar un SGSI es recomendable tener en cuenta los parámetros que brindan la ISO 27001 y la ISO 27005, en la que las dos normas establecen que para hacer la gestión de la seguridad de la información se debe realizar un proceso sistemático, documentado y conocido por toda la organización.

Se debe aclarar que el hecho que la empresa implemente el SGSI no garantiza la seguridad el 100%, pues esto es inalcanzable, lo que si garantiza es que se minimizan los riesgos y al mismo tiempo el impacto que tendría si el riesgo se materializará.

La norma ISO 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. (Gómez y Álvarez, 2012), con base en esta definición se deduce que al implementar este sistema la empresa tendrá conocimiento de cuál es su estado de seguridad, de poder tomar

medidas para mitigar los riesgos, también tienen la opción de controlar y evaluar si esas medidas fueron efectivas o no, esto conlleva al mejoramiento continuo.

Imagen 4. Ciclo PHVA

Tomado de: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

La norma ISO 27001 e ISO 27005 establecen que para gestionar el riesgo se debe aplicar el ciclo PHVA (Planear, Hacer, Verificar, Actuar), donde la empresa establece una Política de seguridad, en la que se determinan los procesos, procedimientos y normas que todos los miembros de la empresa deben cumplir para proteger la información que cada uno maneja y de la cual es responsable. Así mismo se debe tener claro que el SGSI debe contar con un seguimiento para verificar si las medidas que se han tomado para minimizar los riesgos han sido efectivas, por esta razón se deben hacer auditorias para así mantener y mejorar el SGSI.

En la etapa de Planear se establecen las políticas y su alcance teniendo en cuenta los medios que ayudaran al cumplimiento de las medidas de seguridad, en la segunda etapa Hacer, se pone en funcionamiento el SGSI, en la tercera fase de Verificar, se revisa que los controles que se implementaron hayan funcionado y así mismo se

identifica las falencias o errores que se presentaron y la última etapa es Actuar, donde se implementan acciones correctivas para mantener el SGSI.

Otro aspecto que se debe tener en cuenta en el momento en el que se va a implementar el SGSI es que existen unas medidas con las que se puede mitigar el riesgo y estas son:

- ***Evitar el riesgo:*** es cuando la organización no acepta este riesgo es decir se debe eliminar por completo la fuente del riesgo.
- ***Reducir o controlar el riesgo:*** cuando se han implementado medidas de control para el riesgo, con lo que se pretende mitigar el impacto del riesgo.
- ***Asumir el riesgo:*** la organización decide aceptar las consecuencias si se presenta el riesgo y por esto no aplica ninguna medida correctiva.
- ***Transferencia del riesgo:*** es cuando la organización transfiere el manejo y control de ese riesgo a otra organización que tiene la capacidad de asumirlo.

Por último es importante resaltar que la dirección en todo este proceso de la implementación del SGSI, es el principal organismo que tiene que estar comprometido el 100% con este proceso, porque debe supervisar, revisar y hacer todo lo que este a su alcance para mantener el sistema, claro está con la participación y colaboración de todos los empleados de la empresa.

CONCLUSIONES.

Una empresa que implemente el sistema de gestión de riesgos de la información, cumplirá con los estándares internacionales y certificara sus procesos de seguridad dado que identifico, gestiono y minimizo los riesgos que posee la seguridad de la información.

Implementar un SGSI no depende solo del cumplimiento de los parámetros brindados por la ISO 27001 e ISO 27005 sino es fundamental la participación de la alta dirección de la empresa, porque ellos son los principales interesados en que su proceso de exportación cumpla con las medidas de seguridad que exige el BASC para sus miembros.

La empresa certificada BASC que implemente el SGSI puede tener la certeza que sus clientes, proveedores y demás asociados de negocio, tomaran este hecho de forma seria y continuaran con la relación comercial de exportación, al saber que la empresa cumple con los estándares de seguridad en su proceso.

Es importante generar una cultura de seguridad en los miembros de la empresa, porque los cambios no siempre son aceptados con facilidad, esto con el fin de que el SGSI genere un alto nivel de seguridad en sus procesos.

De acuerdo a la investigación desarrollada se deduce que por más que se realice la implementación del SGSI no se puede garantizar el 100% de la seguridad, dado que el propósito del SGSI es gestionar los riesgos de la información, es decir que sean conocidos, gestionados y minimizados por la organización.

BIBLIOGRAFIA.

Compendio Sistema de Gestión de la Seguridad de la Información (SGSI), ICONTEC, "Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información (SGSI).Requisitos" Bogotá, Colombia.

Paloma, L (2012) *Delitos informáticos (en el ciberespacio): doctrina y análisis de casos reales.* Bogotá: Ediciones Jurídicas Andrés Morales.

Gómez, V, A (2011) *Enciclopedia de la Seguridad Informática*. México; alfaomega

Business Alliance for Secure Commerce (BASC) estándares BASC Versión 3-2008 Adopción de Requisitos Mínimos de Seguridad C-TPAT Exportador.

Norma BASC versión 4 de 2012

Cocho, J (2003) *Riesgo y seguridad de los sistemas Informáticos.* Valencia; editorial de la UVP

Gómez, L y Álvarez, A (2012) *Guía de aplicación de la norma UNE-ISO/IEC 27001 sobre la seguridad en sistemas de información para pymes.* España; AENOR

Aceituno, V, (2006) *Seguridad de le Información, México; Limusa.*

CIBERGRAFIA

Recuperado de: http://www.aircargopack.com/pdf/BASC_Exportador.pdf

Recuperado: http://www.ccit.org.co/files/SEGURIDAD%20INFORMATICA/Delitos_Informaticos.pdf

Recuperado: http://www.esetla.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

Recuperado: https://mail.google.com/mail/u/0/#search/historia/1480d45595fd3add?projector=1

Recuperado: http://seguridadinformaticasmr.wikispaces.com/TEMA+1+SEGURIDAD+IFORM%C3%81TICA, consultado en línea

Recuperado: http://www.virtual.unal.edu.co/cursos/economicas/2006838/html/cap08/cont03.html