SEGURIDAD INFORMÁTICA Y DE INFORMACIÓN

RUBEN DARIO CARVAJAL HERRERA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
CARTAGENA DE INDIAS
2013

SEGURIDAD INFORMÁTICA Y DE INFORMACIÓN

RUBEN DARIO CARVAJAL HERRERA

Director
Ing. Eduardo Gómez Vásquez

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
CARTAGENA DE INDIAS
2013

TABLA DE CONTENIDO

FIGURAS

MAPAS CONCEPTUALES

TABLAS

1 INTRODUCCIÓN

La implementación de la norma ISO 27001 depende de la capacidad económica de la empresa y el tipo de información. Como bien es cierto en Colombia en muchas empresas no se aplica esta norma completamente ya que es muy costosa y además muchas no se ven en la necesidad de hacerlo.

Por otro lado haciendo un breve definición de la norma se dice que, es un estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) fue aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

A esto se le suma un SGSI (sistema de gestión de seguridad de información) el cual está compuesto por una serie de políticas, reglas, protocolos entre otras cosas que ayudan a minimizar los riesgos de pérdida de información dentro de una empresa. En varias de las empresas donde he trabajado me encuentro con la sorpresa de que la seguridad de información está en un segundo plano y lo único que le interesa es una buena producción, y en el momento que se presenta un caso de pérdida de información pasan a corregir.

2 OBJETIVOS

2.1 Generales:

- ✓ Investigar y conocer la norma ISO 27001.
- ✓ Ver la norma ISO 27001 en Colombia.
- ✓ Mirar casos de pérdida de información en Colombia

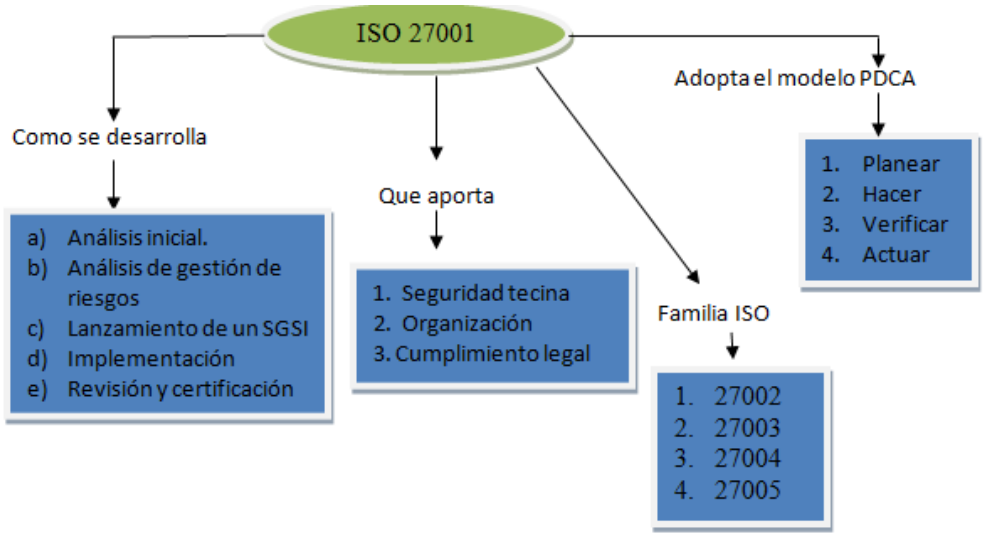
2.2 Específicos:

- ✓ Aprender algunos métodos y políticas para evitar perdida de información
- ✓ Ver cuales o como hacen las empresas en Colombia para evitar la pérdida de información
- ✓ Conocer un SGSI

3 NORMA ISO 27001

3.1 Definición

La ISO es la Organización Internacional de Normalización y se encarga de elaborar normas internacionales que el mercado requiere y necesita dando los lineamientos para que las organizaciones lleguen a sus clientes con productos y servicios de calidad. Las normas son de carácter voluntario, nadie obliga o vigila su cumplimiento, sin embargo su uso por millones de empresas facilita el entendimiento entre países y organizaciones y agregan un factor diferenciador a las organizaciones que se encuentran certificadas. Para asegurar competitividad y sobresalir en el mercado, una organización debe demostrar que sus servicios son gestionados de forma segura, eficiente y eficaz, esto se logra implementando dentro de la organización sistemas de gestión, que permitan un enfoque práctico y seguro de las actividades que se llevan a cabo en su interior.



Mapa Conceptual 1: ISO 27001

3.2 Características

ISO 27001 está alineada con otros sistemas de gestión, y apoya la implementación y funcionamiento estable e integrado con normas de gestión relacionadas.

Características de la ISO 27001:

- ✓ Armonización con normas de sistemas de gestión como ISO 9001 y ISO 14001.
- ✓ Énfasis y continuo proceso de mejora de su sistema de gestión de seguridad de la información.
- ✓ Aclaración de requisitos para la documentación y archivos.
- ✓ Valoración de riesgos y procesos de gestión utilizando un modelo de proceso Plan, Do, Check, Act –PDCA (Planificar, Realizar, Controlar, Actuar).

El objetivo principal de un Sistema de Gestión de Seguridad de la Información (SGSI) es que las distintas actividades relacionadas con la gestión de la seguridad de la información, como son la definición de objetivos, la planificación de actividades, la implantación de controles, el diagnóstico y la reacción ante incidencias y eventos se puedan definir, repetir, medir y optimizar, implantando por tanto un proceso de mejora continua y dotando así a las organizaciones del concepto de calidad a la Seguridad.

3.3 Historia

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

- ✓ 1979 Publicación BS 5750 - ahora ISO 9001
- ✓ 1992 Publicación BS 7750 - ahora ISO 14001
- ✓ 1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

3.4 Serie 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- ✓ ISO 27000: En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma está previsto que sea gratuita, a diferencia de las demás de la serie, que tendrán un coste.

- ✓ ISO 27001: Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas

empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en AENOR. Otros países donde también está publicada en español son, por ejemplo, Colombia, Venezuela y Argentina. El original en inglés y la traducción al francés pueden adquirirse en ISO.org.

- ✓ ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.

- ✓ ISO 27003: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2009. Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- ✓ ISO 27004: En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.

- ✓ ISO 27005: Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.

- ✓ ISO 27006: Publicada el 13 de Febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma

de acreditación por sí misma. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.

- ✓ ISO 27007: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoría de un SGSI.

- ✓ ISO 27011: En fase de desarrollo; su fecha prevista de publicación es finales de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

- ✓ ISO 27031: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

- ✓ ISO 27032: En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía relativa a la ciberseguridad.

- ✓ ISO 27033: En fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y remuneración de ISO 18028.

- ✓ ISO 27034: En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía de seguridad en aplicaciones.

- ✓ ISO 27799: Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos y imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida. El original en inglés o francés puede adquirirse en ISO.org.

3.5 Empresas Colombianas y norma iso 27001

Bueno esta me parece la parte más importante de este documento la cual contendrá casos reales de lo que realmente está haciendo o como esta y que piensan de esta norma en Colombia si bien es claro en la tabla siguiente en nuestro país solo tenemos 27 empresas certificadas.

ISO/IEC 27001 - Central / South America						
Year	2006	2007	2008	2009	2010	2011
Country	18	38	72	100	117	150
Argentina	1	1	6	4	8	24
Barbados				1	1	
Bolivia				1	1	3

Brazil	10	25	40	48	41	50
Chile	2	3	7	10	13	18
Colombia	3	8	11	14	23	27
Costa Rica			2	5	6	7
Cuba			1	1	2	
Dominican Republic				1	1	2
Ecuador				1	1	1
El Salvador					1	1
Guatemala					1	1
Guyana				1	1	
Honduras						1
Jamaica				1	1	
Panama					1	1
Peru	1	1	2	6	9	5
Puerto Rico			2	2	2	2
Uruguay	1		1	4	4	7

Tabla 1: lista de países en centro y sur América vs cantidad de empresas certificadas

En centro y sur América hasta el año 2011 solo teníamos 40 empresas certificadas como se muestra en la siguiente tabla esto es una cifra muy baja con respecto a la cantidad de empresas que existen. Pero como ya lo había mencionado antes la empresas solo entran a la norma escogen lo necesario y listo buscan protección mas no certificación. Es notable la diferencia que tenemos son el resto de continentes siendo África la de menor empresas certificadas hasta ese año esto se debe a que los empresarios no se preocupan tanto por ser certificados su preocupación es tener su información segura aplicando un poco de la norma quizás sin necesidad de crear un SGSI.

Overview						
Year	2006	2007	2008	2009	2010	2011
TOTAL	5797	7732	9246	12935	15626	17509
Africa	6	10	16	47	46	40
Central / South America	18	38	72	100	117	150
North America	79	112	212	322	329	433
Europe	1064	1432	2172	3563	4800	5446
East Asia and Pacific	4210	5550	5807	7394	8788	9664
Central and South Asia	383	519	839	1303	1328	1497
Middle East	37	71	128	206	218	279

Tabla 2: Lista de continentes y empresas certificadas

Name of the Organization	Country	Certificate Number	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
ComBanc S.A.	Colombia	IS 531192	ISO/IEC 27001:2005
Etek International Holding Corp.	Colombia	IS 84320	ISO/IEC 27001:2005
Financial Systems Company Ltda	Colombia	IND92101	ISO/IEC 27001:2005
Ricoh Colombia, S.A.	Colombia	IS 85241	ISO/IEC 27001:2005
SETECSA S.A	Colombia	IND102074	ISO/IEC 27001:2005
UNE EPM Telecomunicaciones. S.A E.S.P	Colombia	IND92122	ISO/IEC 27001:2005
UNISYS Global Outsourcing & Infrastructure Services (GOIS)/Maintenance	Colombia	IS 97104	ISO/IEC 27001:2005

Tabla 3: Empresas Colombianas certificadas

En la lista tenemos a UNE EPM Telecomunicaciones. S.A E.S.P la cual estuvo encargada de manejar la información de las elecciones de congresistas en el periodo de Alvaro Uribe Velez junto con el registrador nacional Carlos Ariel Sanchez, esto es una muestra de que no estamos 100% seguros aun estando certificados y más aun cuando no queremos que la norme se cumpla.

3.6 Como se aplica en Colombia

En las empresas donde he trabajado no he visto un SGSI bien formado, solo escogen de la norma lo necesario y cuando se presenta algún caso donde halla perdida de información entonces pasan a corregir. Dico telecomunicación una empresa encargada del diseño ingeniería y construcción de redes de telecomunicaciones aplica mucho este método que en algunos casos puede ocasionar perdida de mucho dinero, dicha empresa tiene sede en las principales ciudades de nuestro país y se comunican por medio de correo electrónico sin ningún tipo de seguridad tales como encriptar mensajes y una VPN para darle una mayor refugio a los mensajes que entre ciudades, no existen ningún tipo de políticas o

controles para proteger la información excepto el bloque de los puertos USB y contraseñas de usuario para los PC que no representan ningún tipo de seguridad.

Por otro lado ABOCOL tiene un poca mas de seguridad de la empresa anterior pero no la hace inmune a la perdida de información, en esta empresa note los router con lista de acceso lo cual impide que los usuarios revisen paginas indeseadas por la empresa las cuales infectan el pc y al igual que la anterior contiene los puertos USB bloqueados para cierto usuarios, corta fuegos y para solicitar documentación se requiere de cierto procedimiento entro otras.

Por último CBI colombiana empresa multinacional encargada de hacer la ampliación de Ecopetrol la cual maneja grandes cantidad de dinero aun no tiene un SGSI que garantice que su información no se pierda, aunque tiene muchas políticas, controles y procedimientos la cantidad de personal minimizan la seguridad de las misma. Por otro lado actúan después de presentarse el error muy poco previenen los ataques.
Ataques en Colombia

3.7 Ataque famosos en Colombia

La denuncia fue presentada ante la Fiscalía tres días después de las elecciones, luego de que el contratista para el proceso de preconteo de las elecciones, EPM-UNE Telecomunicaciones, contratara a la firma Adalid, certificada por la Unión Europea, para analizar cibercrímenes y evidencias digitales, para que revisara los factores que ocasionaron el colapso de la plataforma tecnológica. La conclusión, y así lo planteó el informe presentado: “la evidencia recolectada muestra claramente que el servicio de publicación de resultados el día 14 de marzo estuvo bajo ataque informático de magnitudes considerables más allá de previsiones razonables”.

En este ataque, Adalid encontró 14 direcciones I.P. con exagerado número de consultas al la plataforma informática —lo que generó el colapso—, direcciones que este diario investigó a quiénes pertenecían, encontrando la sorpresa de que el DAS había sido empleado para realizar maniobras en contra de una entidad cuyo jefe, el registrador Carlos Ariel Sánchez, había tenido claras desavenencias con miembros del gobierno del entonces presidente Álvaro Uribe Vélez. Pero las sorpresas no pararon ahí, otro de los puntos que se referencian como punto de emisión de estos ataques es el Ejército Nacional, pero investigando la dirección física del lugar desde donde se realizó la ofensiva, coincide con el Ministerio de Defensa Nacional Y el ataque que más daño hizo a la plataforma informativa de la Registraduría fue realizado desde la Policía Nacional, con más de 230.000 'hits' —consultas en la página web—, cifra que sobrepasa por amplio margen los límites normales de una consulta. Tan complejo resultó el ataque informático, que las estadísticas de la investigación muestran que hubo minutos en los que se realizaron más de 93.000 consultas, mucho más de lo que recibe un buscador como Google.

Este tipo de ataque se conoce como ping infinito y es muy fácil de hacer lo mismo que impedir pero las partes encargadas no lo quisieron y por tal razón hubo manipulación en el conteo de votos y las cifras hasta el momento no son creíbles pero igual se trabajaron con ellas y gobernaron nuestro país.

Haciendo una VPM entre las ciudades y manejando esa información por un medio único como un canal de televisión evitamos este tipo de riesgo pero no fue así.
Por otro lado tenemos que el problema de la alcaida de Bogotá

El 19 de abril de 2010, Martha Elena Díaz, entonces directora distrital de asuntos disciplinarios de la administración de Samuel Moreno, ordenó una indagación preliminar contra una administradora informática señalada de "presunta negligencia y omisión en el ejercicio de sus funciones". Dos años después, ya en la Alcaldía de Gustavo Petro, el asunto se convirtió en una pesquisa administrativa para establecer por qué dedica su

tiempo a consultar correos privados de distintas dependencias, incluyendo el despacho del alcalde.

Cuando se produjo el relevo en la Alcaldía y la Dirección Distrital de Asuntos Disciplinarios quedó a cargo del abogado Augusto Ocampo, después de rechazar un sinnúmero de pruebas requeridas por la funcionaria como parte de su defensa, reactivó el caso y encontró sorpresas que cambiaron el rumbo de la investigación. Con un estimado de 8.000 consultas en el sistema de informática de la Alcaldía, en áreas ajenas a su dependencia, se pretende establecer qué interés tenía en hacer esas averiguaciones.

Después de un cruce de correos entre la funcionaria y su jefe directo, en los cuales el segundo la conminó a cumplir con el reglamento y ella le reportó razones personales de su continua ausencia, el tema terminó en que Olga Orjuela le hizo saber a su superior que se estaba configurando un caso de acoso laboral y que ella no iba a permitir que se le siguieran vulnerando sus derechos como funcionaria, ciudadana y madre cabeza de familia. En adelante, según Fabio Sánchez, a cada reclamo recibió una desobligante respuesta y persistió en no cumplir su horario laboral.

La noticia es interesante debido a que realmente la persona implicada no se ve realmente como un hacker sino como alguien con los permisos suficientes para revisar los correos e información enviada y recibida por prácticamente todo el personal de la alcaldía. Otro dato interesante es que aun mencionando 8.000 accesos a las bases de datos en los últimos 6 meses, la cuestionada funcionaria lleva trabajando más de 20 años en la Alcaldía así que si hacemos cuentas de 16.000 consultas por 20 años la cifra es realmente astronómica.

Colombia lidera el ranking de inseguridad informática en América Latina Así lo dio a conocer la firma Kaspersky, según la cual el 39% de los usuarios fue atacado al menos una vez en lo corrido del año mientras navegaba por internet.

Los tres países pertenecen al grupo de más alto riesgo en la región en cuanto a seguridad informática se refiere. Según la compañía de seguridad informática, el 35% de los usuarios

de internet en la región son propensos a ser atacados por criminales cibernéticos mientras navegan, siendo República Dominicana, con el 30%, el de menor riesgo.

Pero este aumento tendría una explicación en la evolución tecnológica que los mercados latinoamericanos están presenciando.

“El uso del internet crece cada día más. Millones de personas guardan su dinero en cuentas bancarias y utilizan sus tarjetas de crédito para pagar por bienes y servicios al hacer compras en línea. Los delincuentes están al tanto de esto y es por eso es que la mayoría de sus ataques tienen como objetivo la información financiera”, señaló Dmitry Bestuzhev, director del Grupo de Análisis e Investigación de Kaspersky.

La firma también ha detectado que los criminales regionales han aprendido las tácticas empleadas por hackers de Europa del Este y están desarrollando amenazas cibernéticas nativas, en español y con objetivos segmentados. Asimismo, prácticas de los usuarios como la piratería, la visita a sitios pornográficos y la falta de conciencia a la hora de instalar antivirus genuinos se han convertido en un aliado clave para el delito.

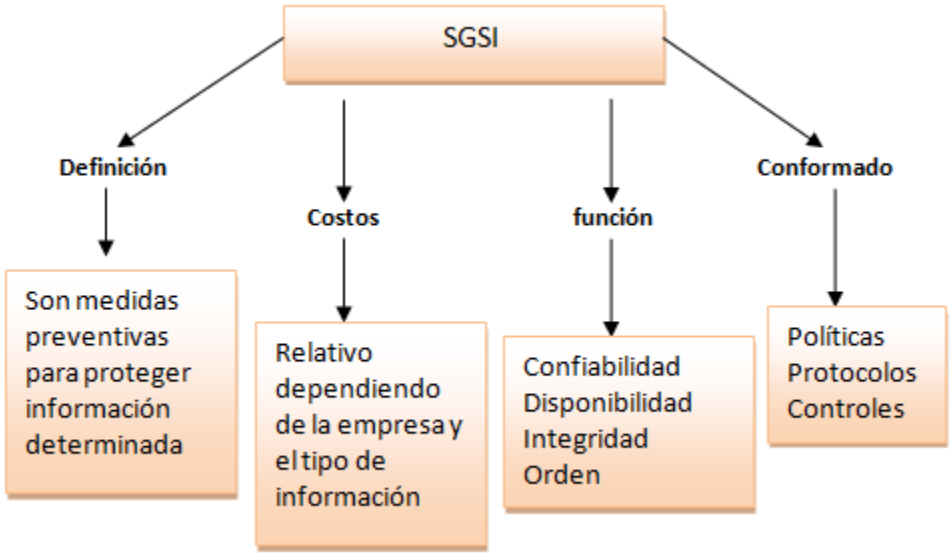
“Los dispositivos con plataforma Android serán probablemente los más atacados. Los países donde las tasas de penetración de Internet son altos, y los servicios de banca en línea son muy populares, atraen a los delincuentes que ponen sus tecnologías cada vez más sofisticadas a la prueba allí”, aseguró Bestuzhev.

Haciendo un zoom dentro de las políticas, controles y procedimientos mostrare mas detalles cada una de ellas y la forma de cómo se usan en empresas colombinas también aclaro que en Colombia más que todo lo hacen por tener su información segura mas no buscado una certificación y en alguno casos no se documentan simplemente el jefe da la arden de cumplir.

4 SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN (SGSI)

4.1 Definición

Es un conjunto de políticas de administración de la información basándose en el diseño, implantación y mantenimiento de procesos para gestionar eficientemente los activos de información minimizando a la vez los riesgos de seguridad de la información.



Mapa Conceptual 2: SGSI

La Seguridad de la Información se puede definir como la protección de la confidencialidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos de negocio de la organización. Estos activos se pueden definir de diversas formas (equipos, aplicaciones, personas que se utilizan para crear, gestionar, transmitir y destruir la información), que tiene un valor para la organización.

Hoy en día, se recogen, gestionan y transmiten multitud de datos a través de diferentes medios a mucha gente y todas las acciones relacionadas con ello pueden necesitar protección; por esta razón se debe implementar estrategias, controles y políticas que cubran la totalidad de los procesos inherentes al desarrollo corporativo; en materia de riesgo, vulnerabilidad, seguridad y continuidad siendo la información el activo más valioso de nuestro proceso.

4.2 Función

Entre las principales funciones y características de SGSI se tiene:

- ✓ Soporte a la gestión del estado de cumplimiento de controles, pudiendo controlar en todo momento el estado actual de conformidad.
- ✓ Posibilidad de gestionar diferentes marcos normativos de forma simultánea: ISO/IEC 27001, ISO/IEC 27002, RD 1720/2007, PCI DSS, ENS (RD 3/2010), etc.
- ✓ Definición de procedimientos de verificación personalizados.
- ✓ Mantenimiento de información histórica, con posibilidad de ver la mejora en el tiempo del estado de la seguridad.
- ✓ Definición y seguimiento de proyectos, agrupando controles y comprobando en cado momento el nivel de implantación.
- ✓ Gestión de indicadores de eficacia del SGSI.
- ✓ Registro de auditorías y seguimiento de las no conformidades y acciones correctivas.

4.3 Características

Un sistema de seguridad de información tiene como característica principal brindar:

- ✓ Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- ✓ Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- ✓ 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.

La gestión de la seguridad de la información es hoy en día una parte fundamental de las organizaciones, con independencia de su tamaño, sector o localización geográfica. Como norma, cuanto más grande es la organización, mayor es el reto de realizar una adecuada gestión de los riesgos potenciales existentes. Una inadecuada gestión puede resultar en la materialización de las amenazas potenciales, incurrir en incumplimientos que resulten en

sanciones o, peor aún, impactar en el desarrollo de la actividad de la organización, y en muchos casos, el coste de la reparación puede superar el costo percibido de la prevención.

El objetivo principal de un Sistema de Gestión de Seguridad de la Información (SGSI) es que las distintas actividades relacionadas con la gestión de la seguridad de la información, como son la definición de objetivos, la planificación de actividades, la implantación de controles, el diagnóstico y la reacción ante incidencias y eventos se puedan definir, repetir, medir y optimizar, implantando por tanto un proceso de mejora continua y dotando así a las organizaciones del concepto de calidad a la Seguridad.

4.4 Modelo PDCA

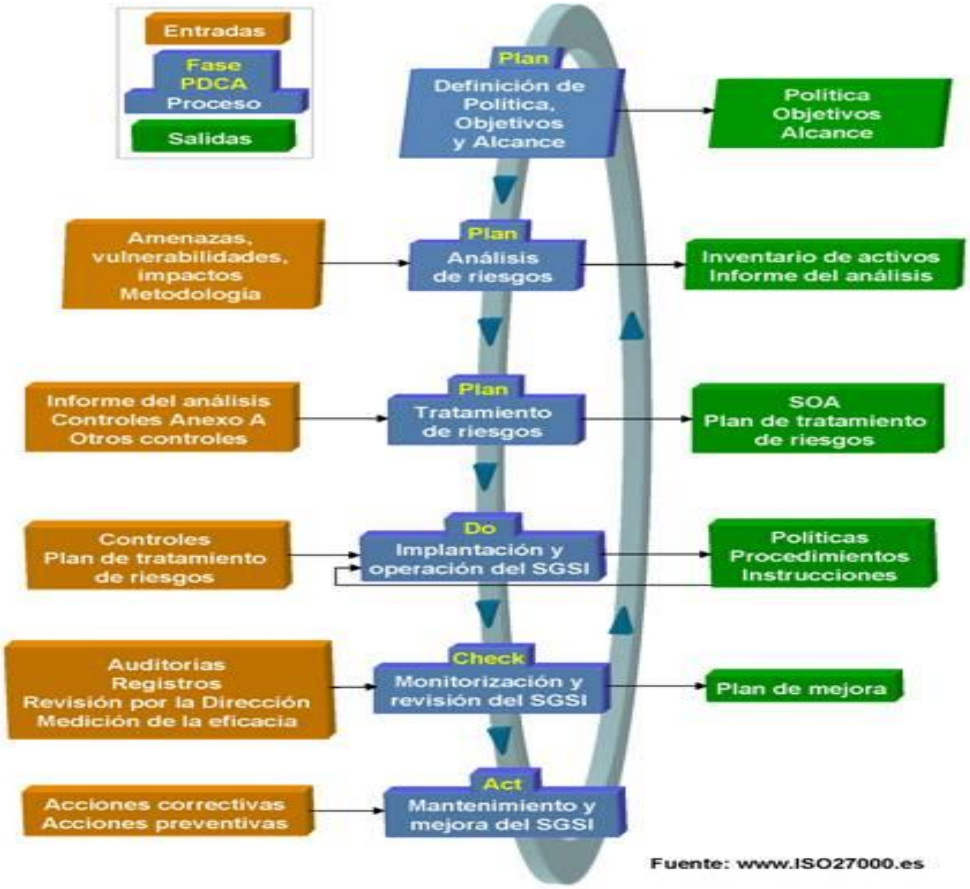


Figura 1: Modelo PDCA

Todos los Sistemas de Gestión de la Seguridad de la Información se basan en la necesidad de que la Seguridad de la Información esté en continua evolución y que, además, dicha evolución esté documentada y justificada. El modelo en el que se basa el SGSI es denominado Modelo PDCA ("Plan-Do-Check-Act") que se representa en el diagrama anterior

- Planificar

En esta primera fase se realiza un estudio de la situación de la Organización (desde el punto de vista de la seguridad), para estimar las medidas que se van a implantar en función de las necesidades detectadas. Hay que tener en cuenta que no toda la información de la que dispone la organización tiene el mismo valor, e igualmente, no toda la información está sometida a los mismos riesgos. Por ello un hito importante dentro de esta fase es la realización de un Análisis de Riesgos que ofrezca una valoración de los activos de información y las vulnerabilidades a las que están expuestos. Así mismo se hace necesario una Gestión para dichos riesgos de cara a reducirlos en la medida de lo posible.
El resultado de este Análisis y Gestión de Riesgos será establecer una serie de prioridades en las tareas a realizar para minimizar dichos riesgos. Puesto que los riesgos nunca van a desaparecer totalmente, es importante que la Dirección de la Organización asuma un riesgo residual, así como las medidas que se van a implantar para reducir al mínimo posible dicho riesgo residual.

- Ejecutar

En esta fase se lleva a cabo la implantación de los controles de seguridad escogidos en la fase anterior. En dicha implantación se instalarán dispositivos físicos (HW, SW, ...), pero también se creará o revisará la documentación necesaria (políticas, procedimientos, instrucciones y registros). Dentro de esta fase es muy importante dedicar un tiempo a la concienciación y formación del personal de la empresa de cara a que conozcan los controles implantados.

- Verificar

Es importante que la Organización disponga de mecanismos que le permitan evaluar la eficacia y éxito de los controles implantados. Es por esto que toman especial importancia

los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del SGSI.

- Actuar

En esta fase se llevarán a cabo las labores de mantenimiento del sistema así como las labores de mejora y de corrección si, tras la verificación, se ha detectado algún punto débil. Esta fase se suele llevar en paralelo con la verificación y se actúa al detectarse la deficiencia, no se suele esperar a tener la fase de verificación completada para comenzar con las tareas de mejora y corrección.

4.5 Costos

Hoy es imposible hablar de un sistema cien por cien seguros, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas.
La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios. “Si un Hacker quiere gastar cien mil dólares en equipos para descifrar una encriptación, lo puede hacer porque es imposible de controlarlo. Y en tratar de evitarlo se podrían gastar mucho dinero”.

Desde un punto de vista oficial, el desafío de responder la pregunta del valor de la información ha sido siempre difícil, y más difícil aún hacer estos costos justificables, siguiendo el principio que “si desea justificarlo, debe darle un valor”1

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones.

---

[1] STRASSMANN, Paul A. “El arte de presupuestar: como justificar los fondos para Seguridad Informática”. http://www.nextvision.com

Además, las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son reticentes a dedicar recursos a esta tarea. Por eso es importante entender que los esfuerzos invertidos en la seguridad son costeables.

Se debe tratar de valorar los costos en que se puede incurrir en el peor de los casos contrastando con el costo de las medidas de seguridad adoptadas. Se debe poner especial énfasis en esta etapa para no incurrir en el error de no considerar costos, muchas veces, ocultos y no obvios (costos derivados).

Una vez evaluados los riesgos y los costos en los que se está dispuesto a incurrir y decidido el nivel de seguridad a adoptar, podrá obtenerse un punto de equilibrio entres estas magnitudes:

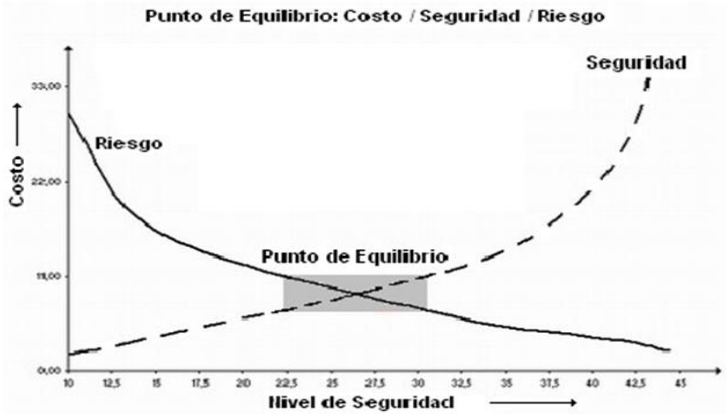


Figura 2: Punto de equilibrio Costos/seguridad

Como puede apreciarse los riesgos disminuyen al aumentar la seguridad (y los costos en los que incurre) pero como ya se sabe los costos tenderán al infinito sin lograr el 100% de seguridad y por supuesto nunca se logrará no correr algún tipo de riesgo. Lo importante es lograr conocer cuan seguro se estará conociendo los costos y los riesgos que se corren (Punto de Equilibrio).

4.6 Certificación

Sistemas de Gestión de la Seguridad de la Información Hasta final de 2007, al menos 7.732 certificados de ISO 27001 habían sido emitidos en 70 países, con un aumento de 1.935 certificados (+ 33%) respecto a 2006, cuando el total era 5.797 en 64 países

Una vez implantado el SGSI en la organización, y con un historial demostrable de al menos 3 meses, se puede pasar a la fase de auditoría y certificación, que se desarrolla de la siguiente forma:

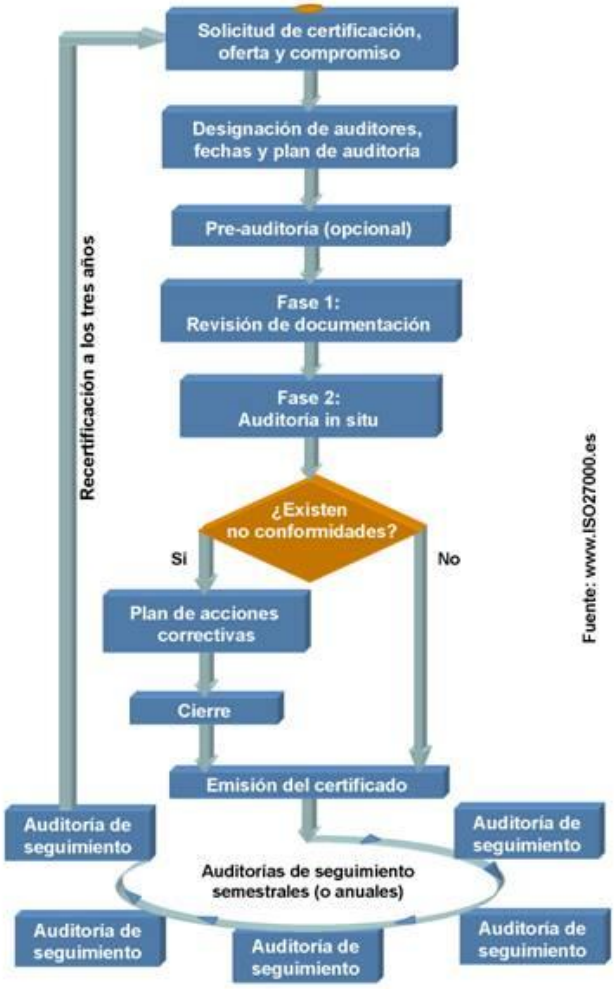


Figura 3: Diagrama de Flujo Proceso de certificación

- Solicitud de la auditoría por parte del interesado a la entidad de certificación y toma de datos por parte de la misma.

- Respuesta en forma de oferta por parte de la entidad certificadora.

- Compromiso.

- Designación de auditores, determinación de fechas y establecimiento conjunto del plan de auditoría.

- Pre-auditoría: opcionalmente, puede realizarse una auditoría previa que aporte información sobre la situación actual y oriente mejor sobre las posibilidades de superar la auditoría real.

- Fase 1 de la auditoría: no necesariamente tiene que ser in situ, puesto que se trata del análisis de la documentación por parte del Auditor Jefe (fundamentalmente centrada en el listado de la cláusula 4.3.1 del estándar ISO/IEC 27001) y la preparación del informe de la documentación básica del SGSI del cliente, destacando los posibles incumplimientos de la norma que se verificarán en la Fase 2. Este informe se envía junto al plan de auditoría al cliente. El periodo máximo entre la Fase 1 y Fase 2 puede ser de 6 meses con carácter general, aunque supeditado en cualquier caso a los procedimientos internos que cada entidad de certificación disponga para el desarrollo del proceso (conviene por tanto aclarar con la entidad de certificación previamente y antes de inciar el proceso).

- Fase 2 de la auditoría: es la fase de detalle de la auditoría, en la que se revisan in situ las políticas, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto. Se inicia con una reunión de apertura donde se revisa el objeto, alcance, el proceso, el personal, instalaciones y recursos necesarios, así como posibles cambios de última hora. Se realiza una revisión de las exclusiones según la Declaración de Aplicabilidad (documento SOA), de los hallazgos de la Fase

1, de la implantación de políticas, procedimientos y controles y de todos aquellos puntos que el auditor considere de interés. Finaliza con una reunión de cierre en la que se presenta el informe de auditoría.

- Certificación: en el caso de que se descubran durante la auditoría no conformidades (clasificadas como "mayores" y/o "menores"), la organización deberá presentar un Plan de Acciones Correctivas (1 PAC para cada desviación localizada) que incluya un análisis de las causas raíz que originaron la desviación. El auditor jefe debe revisar todos los PAC que la empresa envié, incluso verificar la implantación de las acciones correctivas en base al PAC en el caso de las "Mayores" y, una vez verificados los PAC y/o dicha implantación en el caso de las no conformidades mayores, el auditor podrá emitir un informe favorable de recomendación para la certificación a la comisión de certificación, que validará y emitirá el certificado correspondiente al alcance del SGSI de la organización que ha sido verificado en relación a los requisitos del estándar ISO 27001.

- Auditoría de seguimiento: semestral o, al menos, anualmente, debe realizarse una auditoría de mantenimiento; esta auditoría se centra, generalmente, en partes del sistema, dada su menor duración, y tiene como objetivo comprobar el uso del SGSI y fomentar y verificar la mejora continua.

- Auditoría de re-certificación: cada tres años, es necesario superar una auditoría de certificación formal completa como la descrita.

4.7 Software para el manejo de información

La disponibilidad del acceso a la Información se ha convertido en un requerimiento clave para el éxito y hasta supervivencia de las organizaciones. Cada día más, las empresas usan su Información como un medio para generar mayores ingresos, reducir costos y lograr ventajas competitivas. Sin embargo, el crecimiento explosivo en la cantidad de datos ha generado problemas graves relacionados con el manejo y administración de la

infraestructura tecnológica requerida para garantizar un acceso seguro y confiable a la información en el momento en que la misma sea solicitada por los usuarios. A continuación mostrare un software encargada de administrar información dentro de una empresa:

IDOCS

Es el motor de procesamiento central (administrador) de información a través de este podemos tener cualquier tipo de información de acuerdo a los privilegios de usuario y la información contenida en el.

Beneficios y Características:

- Ahorros relacionados con menos mano de obra y de los residuos de manejo de papel, documento de embarque, almacenamiento, distribución, franqueo / envío, fax, teléfono,
- Más rápido flujo de efectivo a través de más rápido (automatizado) de distribución de documentos
- Fiable y precisa agiliza la entrega de facturas, formularios, informes y otros documentos a las personas exactas que lo necesitan a través de correo electrónico, fax, impresión y / o archivo
- Opciones condicionales de gran alcance para los usuarios llamar de forma dinámica y automática diferentes rutinas de mapeo de datos, superposiciones, instrucciones de enrutamiento y conjuntos de formularios
- Fácil de usar menú de utilidades facilita la administración y configuración de productos

5 DOCUMENTACIÓN DE UN SGSI

Por otra parte se tiene que Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 está formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles.

Importancia

Lo importante de este conjunto de documentos que forman el marco normativo es, por un lado, documentar de forma clara y concreta las decisiones establecidas por la organización en materia de seguridad y, por otro, que sean utilizados por todas las personas de la organización para saber qué hacer en cada circunstancia en relación con la protección de la información.

La documentación debe incluir los registros de las decisiones de la dirección, asegurar que se puedan seguir los indicios de las decisiones de la dirección y las políticas, así como permitir que los resultados registrados sean reproducibles.

Una demostración clásica que suele solicitarse por los auditores es la realización del camino inverso, es decir, partiendo desde los controles seleccionados se observan los resultados del proceso de evaluación y tratamiento del riesgo hasta alcanzar la política del SGSI y los objetivos iníciales.

Existen varios tipos de documento o niveles de documentación que son:

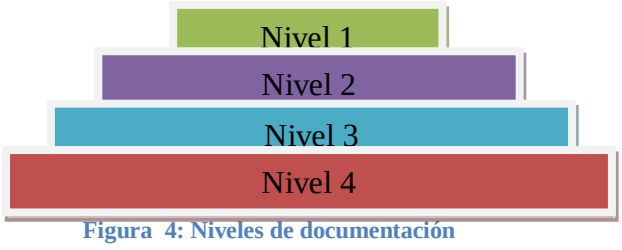


Figura 4: Niveles de documentación

5.1 Documentos de Nivel 1

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que

expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

5.2 Documentos de Nivel 2

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

5.3 Documentos de Nivel 3

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

5.4 Documentos de Nivel 4

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN ESPAÑOL" disponible en web http://www.iso27000.es/sgsi.html#section2c

Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.

Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados

Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

6 POLÍTICAS, PROCEDIMIENTOS Y CONTROLES DE SEGURIDAD.

Luego de haber pasado por la norma de manera fugaz hare un zoom el parte más visible de ella, la cual es fácil apreciar en el momento que se ingresa a una empresa que son las políticas, protocolos, controles y procedimientos para manipular la información.

6.1 Políticas

Una política de seguridad debe establecer las necesidades y requisitos de protección en el ámbito de la organización y es la guía o marco para la creación de otro tipo de documento más detallado que denominamos norma de seguridad. Formalmente describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos. Definen qué quiere la organización a muy alto nivel, de forma muy genérica, quedando como una declaración de intenciones sobre la seguridad de la Organización. A su vez, una política de seguridad puede apoyarse en documentos de menor rango que sirven para materializar en hechos tangibles y concretos los principios y objetivos de seguridad establecidos.

En la mayoría de los casos, los controles de seguridad son de lazo abierto, esto es, el resultado de su funcionamiento no es retroalimentado para mejorar el desempeño del control. Por ejemplo, el cortafuego es uno de los controles más comúnmente utilizados en las redes informáticas. Las reglas de un cortafuego generalmente son fijas, y ante un cambio en los requerimientos de tráfico en la red, se deben cambiar manualmente las reglas de filtraje. Una manera de convertir al cortafuego en un mecanismo de lazo cerrado sería acoplarlo a un detector de intrusiones de modo tal que ante la detección de un posible ataque las reglas del cortafuego se modifiquen automáticamente para bloquear el tráfico sospechoso.

Los protocolos de seguridad son un conjunto de reglas que gobiernan dentro de la transmisión de información.

A continuación mostrare ejemplo reales de políticas, protocolos y controles dentro de una empresa y aclaro nuevamente que todo este conjunto que forman un SGSI debe estar bien documentado también de ser creado, revisado y aprobado por diferentes personas para luego entrar en el proceso de certificación y tengo que aclara que las empresas en Colombia que no están certificadas por diferentes motivos de la alta gerencia solo implantan políticas, controles y procedimientos basados en la norma buscando un poco mas de seguridad pero sin pensar en una certificación.

Esta parte al igual que toda la norma requiere de un alcance y un objetivo para centralizar lo que se quiere lograr con ella. Si empezamos por las políticas tenemos lo siguiente:

6.2 Alcance

Todos los funcionarios, trabajadores de la empresa y en algunos casos clientes dependiendo de la razón social de la empresa ya sea un banco, fabrica entre otros. Todo depende de la forma como se maneje la información dentro de la misma

6.3 Objetivos

Establecer las pautas homogéneas que orienten y entreguen instrucciones sobre el accionar de los usuarios de estaciones de trabajo y distintos periféricos de empresa en el uso, manejo, distribución, modificación y manipulación de los elementos informáticos; ya sea hardware y software de propiedad de esta institución.

6.4 Ejemplos

1. Cada persona es responsable del equipo informático que le ha sido asignado, por tanto, procurará entregarle los cuidados considerados en el correcto uso de los equipos.

2. El equipamiento no debe ser abierto, desarmado, golpeado ni trasladado de lugar sin autorización, tampoco se utilizará para afirmar o sostener vajilla, utensilios, maceteros ni otros objetos que puedan producirle daños.

3. La configuración de cada equipo informático incluye un sistema operativo, una suite ofimática, programas antivirus y los sistemas de cada área. Software específico por departamento y persona, que serán detallados en anexo A del presente documento.

4. Toda instalación de hardware y software la debe realizar sólo el personal autorizado de la unidad de informática.

5. Se prohíbe cambiar la configuración instalada del sistema operativo WINDOWS de los equipos informáticos, tales como, de los controladores, drivers, etc.

6. Los trabajos de soporte a las estaciones de trabajo se realizarán en forma coordinada, a solicitud del usuario. Las actualizaciones en el caso que el software lo permita se realizarán de manera automatizada en línea, en la medida que se pueda realizar de esta manera.

7. Las solicitudes de instalación de estaciones de trabajo y periféricos serán visadas por la jefatura del departamento respectivo.

8. Se considerará falta grave utilizar en el computador personal archivos o programas relacionados a actividades de Hackeo, como escaneadores de puertos o capturadores de proxys.

9. Luego de haber visto algunas políticas apreciables en empresas colombianas pasamos a los procedimientos y controles que como lo mencione anteriormente

solo se pretende tener la información segura mas no una certificación unas se las excusas de la alta gerencia son los costos que esto genera y hasta el momento como esta funcionado las cosas no se presentan problemas por lo tanto dejemos eso así.

6.5 Procedimientos

Los procedimientos son la descripción detallada de la manera como se implanta una política. El procedimiento incluye todas las actividades requeridas, los roles y responsabilidades de las personas encargadas de llevarlos a cabo. Son lo que decir que hacer en cada momento.

- ✓ Una lista de procedimientos son los siguientes:
- ✓ Administración de cuentas de usuario.
- ✓ Manejo de Incidentes
- ✓ Manejo de Virus
- ✓ Administración de cuentas privilegiadas.
- ✓ Procedimiento de Control de Cambios.
- ✓ Procedimiento de Acceso al edificio.
- ✓ Procedimiento de acceso al centro de Cómputo.
- ✓ Procedimiento de respaldo

6.6 Controles

Son Intervenciones realizadas con el objeto de prevenir cualquier posible desvío respecto a lo que se pretende, Los controles son una combinación de medidas manuales y automatizadas que cuidan de la seguridad de los activos, la exactitud y fiabilidad de los registros contables y el cumplimiento operativo de las normas gerenciales

6.6.1 Controles Generales

Controles amplios que monitorean el funcionamiento eficaz de los procedimientos programados en todas las aéreas de aplicación.

6.6.2 Control de Implementación:

Audita el proceso de desarrollo de sistemas para asegurar que siga las pautas de calidad para el desarrollo, conversiones y pruebas.

- ✓ Control de Software: Monitorea el uso del software de sistemas y evita el acceso no autorizado a los programas de aplicación y al software de sistemas.
- ✓ Control de Hardware: Cuida que el equipo esté protegido físicamente contra incendios y extremos de temperatura y humedad. Debe garantizar la continuidad operativa ante desastres, implementando respaldos tanto de hardware como de datos.
- ✓ Control de Operaciones de Computación: Ejercido sobre la labor del centro de cómputos. Garantiza que los procedimientos programados se apliquen de forma congruente y correcta al almacenamiento y procesamiento de datos.
- ✓ Control de Seguridad de los datos: Garantiza que los archivos de datos de negocios no sufran accesos no autorizados, alteraciones o destrucción.
- ✓ Control Administrativo: Normas, reglas, procedimientos y disciplinas de control formalizados. Asegura que los controles generales y de aplicación de la organización se apliquen y cumplan debidamente.

6.6.3 Controles de Aplicación

Controles específicos y exclusivos de cada una de las aplicaciones computarizadas

- ✓ Control de Entrada: Verifica la exactitud e integridad de los datos cuando entran en el sistema. Son controles para evitar errores en las entradas, conversiones y/ó ediciones de datos. Es posible establecer totales de control.: Determina si los datos están completos y son exactos durante la actualización. Se pueden establecer totales de control de serie, el cotejo por computadora y verificaciones de edición.

- ✓ Control de Salida: Monitorea que los resultados del procesamiento sean correctos, estén completos y se distribuyan debidamente.

6.7 Empresas Colombianas y Seguridad de Información

Las empresas colombinas en su mayoría no aspiran a estar certificadas pero si quieren tener su información segura para ello emplean políticas de seguridad y así controlan el flujo de información en muy común llegar a una empresa e encontrar muchas restricciones que funciona de mucho como son las siguientes mencionadas

Lista de políticas de seguridad más comunes

1. No está permitido usar dispositivo de almacenamiento talos como menorías USB disco duro portátil. Al menos que sea autorizado por el gerente de la empresa sea por escrito o correo electrónico especificando las funciones y los alcances de dicho dispositivo y también deberá informar el personal de seguridad en el momento de su uso para habilitar los puertos de conexión.

2. Todo los puerto USB deben estar deshabilitados en caso tal se necesita alguno debe ser autorizado y bajo supervisión.

3. Si es necesario traer un computador personal este debe ser autorizado y no podrá tener acceso a intranet.

4. Cuando se reciba un mensaje de correo electrónico que hable de algo que desconoce (aunque lo haya mandado alguien conocido) conviene consultar su veracidad (por ejemplo a partir de buscadores de la web, tratando de consultar en el sitio web de la supuesta fuente de la información o en webs serias, fiables y especializadas en el tipo de información en cuestión.

5. El personal deberá renovar obligatoriamente cada dos meses sus contraseñas de acceso a correo y software de la empresa.

6. En caso de presentar una o más sedes estas estarán comunicadas atreves de un enlace VPN.

7. La empresa debe tener un cortafuego certificado.

8. Se bebe buscar actualizaciones mensuales del software de defensa.

9. Los servidores de la empresa debe estar un lugar seguro libre de humedad, altas temperaturas, su acceso de ser restringido y documentado.

10. Actualizar constantemente el sistema operativo y el software instalado, especialmente el navegador web. Los sistemas operativos y la mayoría de los programas utilizados tienen una función configurable de actualización (update) automática. Actívela.

11. Trabaje con una cuenta de usuario que no tenga privilegios de administrador. De esta forma evitará la posibilidad de instalación de muchos programas maliciosos.

12. No abrir mensajes de correo electrónico no solicitados o de procedencia desconocida. Elimínelos directamente sin revisarlos.

13. Tenga especial cuidado con las redes P2P (per to per). Es una de las más importantes fuentes de infección. Analice con su antivirus todo lo que se descarga.

14. Cuando se navegue por Internet, busque páginas de confianza, a ser posible, avalados por sellos o certificados de calidad, evitando contenidos dudosos. Su exigencia de calidad ayudará a lograr una Internet más segura
15. Se debe Utilizar siempre software legal.

16. Evitar las descargas de programas de lugares no seguros de Internet.

17. Si reciben mensajes que piden el reenvío a sus conocidos, informando de noticias llamativas o apelando a motivos filantrópicos, desconfíe por sistema. Muchos de ellos buscan captar direcciones de correo electrónico para prospectivas comerciales, y son un engaño (hoax). Desconfíe de los mensajes de correo procedentes de supuestas entidades bancarias. Confirme vía telefónica, en su sucursal bancaria, cualquier petición que reciba de datos de banca electrónica.

18. No deben facilitarse datos personales ni códigos PIN de acceso a nadie que nos llame por teléfono.

19. No deben guardarse claves importantes en archivos de texto en el ordenador.

20. No deben utilizarse PINs triviales ni claves fáciles de descubrir. Una buena clave alternará letras y números sin formar palabras.

21. Usar preferiblemente redes no inalámbricas.

22. Si es posible visite páginas de seguridad informática para mantenerse al tanto de las últimas amenazas pues estas están en constante evolución.

23. Debe tener una lista de control de acceso (ACL) en los router para garantizar que los usuarios no visiten paginas indebidas que pongan en riesgo la información de la empresa

24. Utilizar métodos de encriptación. Requieren dos Claves, una Privada (única y personal, solo conocida por su dueño) y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir.

25. Se debe hacer un manteniendo del sistema y ser revisado con regularidad.

26. Este documente tiene que ser revisado y aprobado por el personal competente de la empresa.

27. Capacitar al personal constantemente (es de mucha importancia)

28. Se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados. La implantación de controles específicos podría ser delegada por el propietario convenientemente. No obstante, el propietario permanece como responsable de la adecuada protección de los activos.

29. La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.

Se requieren ciertas precauciones para prevenir y detectar la introducción de código malicioso y códigos móviles no autorizados. El software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, gusanos de la red, caballos de troya y bombas lógicas. Los usuarios deberían conocer los peligros que puede ocasionar el software malicioso o no autor izado y los administradores deberían introducir controles y medidas especiales para detectar o evitar su introducción.

La gestión de la seguridad de las redes, las cuales pueden cruzar las fronteras de la organización, exige la atención a los flujos de datos, implicaciones legales, monitoreo y la

protección. Podrían ser necesarios controles adicionales con el fin de proteger la información sensible que pasa por las redes públicas.

La aplicación estas reglas garantizan un flujo de información más segura y es garantizado que si no se usan los ataques será mayores también tengo que decir que jamás estaremos 100% seguros aun certificados pero si lograr disminuir los niveles de riesgos.

6.8 Encuestas

A continuación mostrare una serie de encuestas realizadas en el año 2012 acerca de la seguridad de información en Colombia las cuales fueron hechas por ACIS (asociación colombiana de ingenieros de sistemas)

La encuesta nacional de seguridad informática conducida por ACIS para el año 2013, a través de Internet, contó con la participación de 162 encuestados de nuestro país, quienes han decidido responder a este llamado para observar la realidad de nuestro país que, año tras año, lo que nos muestra es un instrumento claro con el cual podemos conocer cómo las organizaciones perciben la seguridad de la información, además de servir como instrumento referente en Colombia y Latinoamérica frente a un panorama que vela por llamar la atención de todos los sectores interesados en estos asuntos

Con base en las respuestas obtenidas, los tres sectores más representativos de la industria para este año están distribuidos entre educación, con un 19.75%, seguida de los servicios financieros que mantienen la tendencia de participación en la encuesta, representada en 18.52%. Y, en tercer lugar, figura el sector Gobierno, con una participación del 12.96%.

Estos tres sectores de gran importancia muestran la forma en cómo la seguridad de la información penetra en los sectores empresariales. A nivel mundial vemos cómo los Gobiernos se preocupan más por el ciberespacio, al que algunos denominan la nueva frontera de las guerras venideras. De otro lado, el sector educativo ve con preocupación la seguridad, teniendo en cuenta los repetidos ataques a sus infraestructuras, originados por

los débiles diseños que exigen mejorar los esquemas. Por su parte, los sectores financieros se ven enfrentados a cumplir con una serie de controles para cumplir con ese competido negocio, considerando la globalización de las economías y la normatividad nacional e internacional.

Más del 50% de los encuestados dice al menos haber realizado una evaluación de seguridad en su organización, tendencia que se mantiene como una práctica adecuada para velar por el estado de salud de los ambientes sobre los cuales se prestan los servicios de las empresas. Llama la atención este 2013, que el porcentaje más alto 39,51% manifiesta haber realizado una prueba de seguridad en el año, hecho positivo que muestra la preocupación por tales asuntos dentro de las organizaciones.

Los mecanismos más usados en la realidad nacional son los antivirus con un 94,44%, como primer mecanismo de protección en las organizaciones. En segundo lugar los firewall, con el 90%; y, en tercer lugar, las contraseñas, con un 82%. Es importante ver cómo estos mecanismos estándar en la protección, siguen siendo validos, pese a las situaciones a las que se ven enfrentados, que nos muestran un panorama retador, en donde es necesario entender que no son suficientes para proteger la información.

7 TÉCNICAS HACKING

Por otro lado en el momento de diseñar un SGSI o implementar políticas, controles y procedimientos para un flujo de información, es bueno mirar o saber técnicas que las personas usan para robar información para ello enuncio algunas que son las siguientes:

1. Ataque criptográfico Padding Oracle: el primer puesto lo ocupa un ataque que puede hacer peligrar incluso algunas transacciones bancarias. Si los datos cifrados de la cookie cambian, la forma en que el framework ASP.NET maneja los resultados en la aplicación puede darnos información de cómo descifrar el tráfico. Con repetidos cambios, un hacker puede deducir los posibles bytes que pueden eliminarse de la clave de encriptación hasta facilitar así su obtención. Los desarrolladores del hack, Juliano Rizzo y Thai Duong, han creado unaherramienta para ejecutar esta técnica.

2. Evercookie: creado por Samy Kamkar, se trata de una API de JavaScript que produce cookies para los navegadores que son "extremadamente persistentes". Afecta al estándar HTML5, es muy difícil de eliminar y puede poner a disposición de un atacante información privada de los usuarios.

3. Hacking de autocompletar: creado por Jeremiah Grossman, es un técnica que se aprovecha de la función autocompletar de un formulario web, pudiendo forzar al navegador a rellenar los datos personales obteniendo los datos almacenados del ordenador de la víctima y sin interacción del usuario.

4. Atacando HTTPS con inyección en caché: inyectando librerías JavaScript maliciosas en el caché del navegador, los atacantes pueden comprometer sitios web protegidos con SSL. Esta técnica funciona hasta que el caché es limpiado. Sus autores son Elie Bursztein, Baptiste Gourdin y Dan Boneh.

5. Anulación de la protección CSRF con ClickJacking y parámetros HTTP contaminados: Lavakumar Kuppan combinaba estas dos técnicas para saltar las protecciones CSRF y engañar a los usuarios para que revelen los IDs de sus cuentas. Usándolo, un atacante podría resetear la contraseña de la víctima y obtener acceso a su cuenta.

6. XSS universal en IE8: su exploit puede eludir la protección cross-site scripting de Internet Explorer 8 y permitir que las páginas web sean procesadas de una forma potencialmente maliciosa.

7. HTTP POST DoS: ideado por Wong Onn Chee y Tom Brennan, consiste en enviar primero cabeceras HTTP POST al servidor para dar a conocer los datos que están siendo enviados, y luego transmitir los datos de una forma muy lenta consumiendo los recursos del servidor. Cuando se envían varios simultáneamente, los servidores pueden ser desbordados.

8. JavaSnoop: consiste en un agente Java instalado en la máquina objetivo que se comunica con la herramienta JavaSnoop. El objetivo es testear aplicaciones en búsqueda de fallos de seguridad y, dependiendo se su uso, puede actuar como una herramienta de seguridad o de hacking. Su autor es Arshan Dabirsiagh.

9. Hack CSS del historial en Firefox sin JavaScript para Intranet Port Scanning: Robert "RSnake" Hansen desarrolló una idea para que los CSS puedan ser utilizados para grabar los historiales de navegación. La información obtenida podría ser utilizada posteriormente para realizar ataques de phishing.

10. DNS Rebinding con Applets de Java: creado por Stefano Di Paola, mediante applets de Java es posible redireccionar el navegador hacia sitios web controlados por el atacante, forzando al navegador a saltarse su caché DNS.

8 CONCLUSIONES

1. La Información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización aunque no se valorado para algunas empresas.

2. Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

3. Se debe estudiar con mucho cuidado lo que significan los virus. Y conocer los diferentes tipos como ser: caballo de troya, gusano, trampilla, bomba de tiempo, bomba lógica y los recientes macro virus.

4. El que tiene la información tiene el poder. Pero en un entorno altamente competitivo, en medio de una economía llena de altibajos y cambios radicales en el mercado, tener la información no es suficiente. Las organizaciones de hoy, públicas y privadas, deben también analizarla, interpretarla y compartirla para poder tomar decisiones estratégicas oportunamente y ganar una ventaja competitiva

9 BIBLIOGRAFÍA

1. Garcia-moran, jean paul / fernandez hansen, yago /martinez sanchez, ruben / ochoa martin, angel / ramos. Hacking y seguridad en internet. Edicion 2011.

2. Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN ESPAÑOL" disponible en web http://www.iso27000.es/sgsi.html#section2c

3. STRASSMANN, Paul A. "El arte de presupuestar: como justificar los fondos para Seguridad Informática". http://www.nextvision.com

4. ICONTEC INTERNATIONAL. EL COMPENDIO DE TESIS Y OTROS TRABAJOS DE GRADO. {En línea}. {Consultado junio 2009}. Disponible en: http://www.ICONTEC.org/BancoConocimiento/C/compendio_de_tesis_y_otros_trabajos_de_grado/compendio_de_tesis_y_otros_trabajos_de_grado.asp?CodIdioma=ESP

5. Purificación Aguilera. Introducción a la seguridad informática. Seguridad informática. Primera edición. Madrid-España. Pag 07-12

Paginas

http://www.cpciba.org.ar/archivos/adjuntos/seguridad.pdf

http://www.sunai.gob.ve/images/stories/PDF/Ponencias/EF/3_Daniel_sandoval.pdf

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

http://www.iso27001standard.com/es/que-es-la-norma-iso-27001

http://www.colconectada.com/normas-icontec/

http://es.wikipedia.org/wiki/Sistema_de_Gesti%C3%B3n_de_la_Seguridad_de_la_Informaci%C3%B3n

http://www.acis.org.co/