REVISIÓN DE LAS NORMAS DE SEGURIDAD EN LAS REDES Y TELECOMUNICACIONES

RESEARCH ABOUT SECURITY IN NETWORKS AND TELECOMMUNICATIONS

ALEJANDRO BETANCUR LOPEZ[1]
ELIZABETH ESCOBAR SERNA[2]
…

Resumen: La infraestructura de una empresa está compuesta por la parte lógica y física, en cada una de estas fases se encuentra integrada la información, ésta debe estar protegida para cualquier intruso que desee vulnerar y hacer algún tipo de daño. Con este aspecto, se genera la idea de la revisión de las normas de seguridad en las tecnologías de la información y la comunicación, con el propósito de informar que estándares son aplicados en lo lógico y en lo físico para las áreas que conformar la infraestructura en una compañía, bridando así seguridad en la protección de la información, y de esta forma hacer que las empresas tomen conciencia aplicando los estándares de seguridad informáticos.

Palabras claves: *Amenaza, información, normas, seguridad, telecomunicaciones.*

Abstract: The infrastructure is composed by business logic and physical part, in each of these parts is integrated information, it must be protected from any intruders who want to violate and do some damage. With this aspect, the idea of reviewing the safety standards in the information technology and communication, in order to report that standards are applied in the logical thing is generated and in physics areas that form the infrastructure a company as well offer security protection information and that company are aware of the standards applying information security.

Key words: *Threat information, standards, security, telecommunications.*

[1] C.V.: **Alejandro Betancur López**: Aspirante al título de Ingeniero en Sistemas de la Institución Universitaria de Envigado. Trabajo de Grado realizado Diplomado de profundización en interventoría de contratos en las TIC (tecnologías de la información y la comunicación) 2014.

[2] C.V.: **Elizabeth Escobar Serna**: Aspirante al título de Ingeniero en Sistemas de la Institución Universitaria de Envigado. Trabajo de Grado realizado Diplomado de profundización en interventoría de contratos en las TIC (tecnologías de la información y la comunicación) 2014.

1. INTRODUCCIÓN

Cada día la tecnología crece a pasos agigantados, esto hace que a nivel mundial las grandes compañías deban mitigar las fallas en su infraestructura para brindar seguridad a sus datos e información. Debido a esta evolución los riesgos se presentan en diferentes formas o niveles. Los niveles de seguridad en las empresas varían dependiendo del tipo de información que maneja, si sus datos son muy delicados e importantes, mitigar fallas en la seguridad toma mayor importancia, y más aún cuando se implementa una cultura de seguridad informática en todos los empleados de la empresa, hace darle un valor especial a la protección en la información.

Las compañías evolucionan y la necesidad de estructurar o mejorar procesos para evitar perder información deben ser más ingeniosos, esto incluye enfrentarse con los riesgos ambientales como los son tormentas eléctricas, terremotos, inundaciones e incendios; para ello, mejorar o reestructurar un proceso evita perdida en la información, van de la mano con los diferentes estándares internacionales que existen para estos tipo de problemas.

Es importante tener presentes las normas y estándares de seguridad en las áreas donde están involucradas las tecnologías de la información y la comunicación e infraestructura. Una forma fácil para aprenderlas es por medio de un diagrama en el cual se informe cuáles son las principales normas, deseando así que se genere una disminución en las fallas de seguridad en los sistemas, en las tecnologías de la información y la comunicación.

2. OBJETIVOS

Objetivo general

- Revisar normas y estándares de seguridad a nivel informático e infraestructura.

Objetivos específicos

- Indicar las diferentes áreas que componen redes y telecomunicaciones.
- Enunciar las diferentes normas de seguridad que se manejan en las áreas de informática e infraestructura.

3. PLANTEAMIENTO (FORMULACIÓN DEL PROBLEMA)

La información representa grandes valores económicos, las grandes empresas invierten cifras astronómicas de dinero para mantener seguros sus datos. Existen muchas formas de mantener segura la información, aplicando normas y estándares de seguridad informática, tener backups de la información físicos y en la nube; y de esta forma evitar daños catastróficos.

En las organizaciones no siempre hay cumplimiento en las normas y políticas de seguridad informática, el no cumplimiento de la norma hace que se presenten fisuras tanto en la infraestructura como a nivel de usuario.

4. JUSTIFICACIÓN

Cada empresa debe de tener su propia política de seguridad basada en las normas y estándares establecidos en el medio, estas deben ir ligadas y trabajar en conjunto para cubrir todos los niveles y darle una estabilidad a nivel informática a la empresa.

Esta tarea no solo depende de las entidades o de las áreas encargadas en la seguridad de redes y telecomunicaciones, sino también de la cultura implementada en los usuarios.

Para implementar un esquema de seguridad informática y de infraestructura es necesario generar un diagrama de tipo informativo sobre las normas y estándares de seguridad informática, diseñando

estrategias en las cuales se motive al usuario a aplicarlas su ámbito laboral como en la actividad diaria.

5. METODOLOGÍA

La metodología que se implementara en el proyecto se basa en:

Enfoque: Cuantitativo

Método: Este proyecto se desarrollara bajo una metodología cuantitativa, puesto que recoge la información de algunas normas existentes a nivel de las TIC (tecnología de la información y la comunicación), informando en un diagrama las diferentes áreas y su respectiva norma para la prevención de las amenazas en la red.

Tipo de proyecto: El tipo de trabajo es descriptivo debido a que interpreta la información obtenida de algunas normas existentes a nivel de las TIC (tecnología de la información y la comunicación) sobre las falencias y amenazas en la información.

El diseño metodológico se basa en la revisión de las normas de seguridad en la red y en las telecomunicaciones, políticas de seguridad existentes en la actualidad, no solamente en Colombia, sino también normas Internacionales aplicadas también en nuestro país.

6. PRIMERAS ENTIDADES DE SEGURIDAD PARA LA TECNOLOGÍA DE LA INFORMACIÓN Y LA COMUNICACIÓN.

Hace 113 años, nace la primera entidad, creadora de la normalización en todo el mundo, llamado BSI (British Stand Ards Institution), este es un grupo británico comprometido en la divulgación de las normas más importante existente en aquel tiempo. En el mismo período nace la norma BS 5750 que en la actualidad la conocemos como la ISO 9001[1].

En el año 1995, se registra la norma BS 7799 de BSI, esta pretende facilitar a cualquier compañía británicas, un conjunto de buenas prácticas para la gestión de la seguridad en la información [2].

Con este nuevo estándar de buenas prácticas, se crea un certificado donde es legalizada esta norma (BS 779). En los dos años siguientes, por ley se generan las obligaciones de un sistema de seguridad de la información esto es SGSI. Finalizando los años 90 se adoptó lo nuevo en la parte de seguridad, la filosofía de ISO.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, en el mismo periodo que se examinó y renovó ISO17799. En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información [3].

Los aspectos de riesgos como la pérdida de información, desastres ambientales, fallas o la manipulación indebida de la información, provoca daños irremediables, generando grandes costos, tanto económicos como a nivel de información existiendo una alta probabilidad en la pérdida total de la misma.

Comúnmente, la infraestructura ha sido lo más importante para una empresa, es el corazón o motor donde se encuentra centralizada toda la información como los son: datos de usuarios, información del negocio, datos de los clientes entre otros; mantener una buena seguridad en este tipo de información para esta área de infraestructura, ya sea en la parte de hardware o software, es de vital importancia para esto existen estrategias de prevención en el riesgo de pérdida de la información.

Procesos de restricción donde indique evitar que un usuarios posea acceso total a la información en una empresa, como lo son los usuarios privilegiados analistas, administradores, que interviene en el acceso a toda la información de una compañía, por obligación la aplicación del acceso restringido debe ser también para este tipo de perfiles, dependiendo del estudio que se realice en una empresa y de los cargos que los usuarios manejen, se aplican los estándares en la protección de la información.

7. NORMAS BASICAS DE SEGURIDAD PARA LA TECNOLOGÍA DE LA INFORMACIÓN Y LA COMUNICACIÓN.

Tanto en lo lógico como en lo físico las amenazas de seguridad son frecuentes, presentan daños en la confidencialidad, la integridad y la disponibilidad de la información. Las normas básicas y estándares establecidos en el medio que se presentan en las TIC, buscan:

1. Evitar
2. Retrasar
3. Detectar
4. Defender

Estas normas y estándares ayudan a prevenir riesgos de la información, a nivel empresarial, debido a que son las grandes organizaciones las que manejan cantidades enormes de datos y de información.

El incumplimiento de normas y políticas de seguridad establecidas en una compañía con lleva a la generación de:

- Multas
- Suspensión o cierre de la compañía
- Sanciones por negligencia en el manejo de la información.
- Derecho penal.

Existen varias compañías a nivel nacional que se encargar de realizar auditorías, exigiendo la explicación y el por qué se usa cada aplicación y cada base de datos en la organización y cuales con los procedimientos para proteger los datos y la finalidad de los mismos. También verifican y controlan las medidas de análisis de una gestión de riesgo permanente.

En Colombia rigen leyes y normas de seguridad informática, en todo lo que respecta a la protección de los datos e información, ya sean en la parte física o lógica.

7.1 Entorno Físico

En el entorno físico se deben cumplir varios procedimientos de seguridad en la información, como por ejemplo la ubicación de los equipos de cómputo, instalaciones físicas de equipos o portátiles; estos deben de estar correctamente diseñados, la empresa debe verificar en conjunto con su analista de seguridad informática la implementación de los estándares en este tipo de diseños.

La empresa debe tener presente definir procesos o políticas de seguridad informática que produzca una efectividad en el entorno físico y en la infraestructura, esto con lleva a determinar los tiempos sin servicios por incidentes relacionados, número de incidentes ocasionados por fallos o vulnerabilidades en el sistema físico, frecuencia de la revisión y evaluación de los riesgos.

En las medidas de seguridad física se deben definir responsabilidades, procedimientos de supervisión e informes de resolución de incidentes. Un punto frágil para las empresas es la protección contra los factores ambientales y dispositivos electrónicos, a través de estándares y políticas de seguridad de la información, estos ayudan a que se mitiguen los riesgos de afectación ambiental.

Varios aspectos a considerar en el entorno físico son:

- ***Perímetro de seguridad:*** para proteger las áreas donde se almacenan soportes de información o procesamiento de datos.
- ***Controles físicos de entrada:*** para validar que solo ingrese personal autorizado y monitorear dichas entradas.
- ***Trabajo de áreas seguras:*** aplicar normas de trabajo seguro y su normatividad.
- ***Área de acceso público:*** zonas como cargue y descargue, allí se debe restringir ingresos.
- ***Protección de equipos:*** instalar equipos en zonas seguras y con sus respectivos controles físicos.
- ***Suministro eléctrico:*** Establecer medidas de protección contra los cortes de energía. Fallos en sistemas auxiliares.

- ***Seguridad del cableado:*** Proteger contra la interceptación y daño físico de la comunicación.

La Norma BS25999/ ISO 22301 Gestión de Continuidad de Negocio, ofrece prácticas y soluciones para la gestión de la continuidad de negocio, consiguiendo reducir los impactos ante una interrupción inesperada que afecte a la organización y ayudando a detectar las posibles contingencias que puedan parar la actividad de la empresa. [4].

La ISO/IEC 17799. En la parte física de la infraestructura en una empresa, aplica la versión de 2005 del estándar, incluye las varias secciones principales entre ellas esta Seguridad Física y Ambiental. Manifiesta en la responsabilidad por los activos tiene como objetivo: Mantener en buen estado los activos de la organización.

Para esta norma se tiene amparados los siguientes ítems:

- Inventario de los activos
- Propiedad de los activos
- Uso aceptable de los activos

La norma en la seguridad física y ambiental menciona: Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia. [5].

Ampara los siguientes ítems:

- Perímetro de seguridad física
- Controles de ingreso físico
- Ubicación y protección del equipo
- Mantenimiento de equipo
- Seguridad del equipo fuera del local
- Retiro de propiedad

Éste estándar hace mención a los medios físicos en tránsito, esto quiere decir que los medios que contienen información debieran ser protegidos contra accesos no-autorizados, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización. [6].

La infraestructura en una empresa, es apoyada por los diferentes organismos internacionales, existe la organización TIA (Telecommunications Industry Association), esta desarrolla normas de cableado industrial en el área de telecomunicaciones. A continuación se hace mención de los estándares creados por la organización:

- ***ANSI/TIA/EIA-568-B:*** Cableado de Telecomunicaciones en Edificios Comerciales sobre cómo instalar el Cableado.
- ***ANSI/TIA/EIA-569-A:*** Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales sobre cómo en rutar el cableado.
- ***ANSI/TIA/EIA-570-A:*** Normas de Infraestructura Residencial de Telecomunicaciones.
- ***ANSI/TIA/EIA-607:*** Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.
- ***TIE/EIA 606:*** recoge las guías para la administración del sistema de cableado de telecomunicaciones.
- ***TSB 67:*** permite verificar si un sistema de cableado estructurado se construyó y está funcionando de acuerdo con las normas establecidas.
- ***TIA-942:*** Este estándar es aplicado en la parte de infraestructura, unifica criterios en el diseño de áreas de tecnología de la información y comunicaciones, esta norma tiene especificaciones para cableado estructurado, su propósito es de proveer una serie de recomendaciones para el diseño e instalación de un datacenter.
- ***ANSI/TIA/EIA-758:*** Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones [7].

IEEE (Instituto de Ingenieros Eléctricos y de Electrónica), tiene como norma la IEEE 802.3-2008: Este estándar aplica para la utilización de Cable coaxial, par trenzado, fibra óptica, para la capa física de Ethernet.

ISO/IEC 27011: Guía de gestión de seguridad de la información específica para telecomunicaciones, seguridad física y del entorno [8].

ISO 14119 esta norma está enfocada a la seguridad en el bloqueo de la puerta de acceso a los recintos que contengan equipos delicados de computo como lo son los data center y los armarios de cableado, aplica para acceso restringido de áreas no autorizadas, solo el ingreso debe ser por el personal que pertenezca al área de ingreso.

7.2 Entorno lógico

Cuando hablamos del entorno lógico en una empresa, esta constituye mecanismos y procedimientos, que permiten hacer seguimiento en el acceso a los activos de información lógicos, esto contienen controles de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a los sistemas de información de acuerdo a las necesidades y funciones del usuario, análisis de incidentes de seguridad lógica y enseñanzas asimiladas de los mismos, vigilancia de aplicaciones críticas, análisis forense, documentación sobre sistemas, software malicioso.

El entorno lógico participa en la ilustración de la política de seguridad informática a seguir por medio de normas y procedimientos que conserven la integridad, medio y confiabilidad de la información necesario para la misión de una compañía sin afectar la operatividad de los procesos.

En la seguridad lógica se tienen en cuenta aspectos relevantes, de los cuales se resaltan:

- Validación de los datos de entrada.
- Control del procesamiento interno.
- Integridad de los mensajes.
- Validación de los datos de salida.
- Política de uso de los controles criptográficos.
- Gestión de claves criptográficas.
- Control del software en operación

La información tiene un valor importante para el funcionamiento de una empresa y de esta depende toda una organización. Las normas ayudan a que las empresas tengan un tiempo prudente de durabilidad, y que en sus procesos de seguridad informático se basen en estándares existentes en el medio y tengan una forma sabia de utilizar correctamente las normas de seguridad para la información.

El modelo de seguridad CIA (Confidencialidad, Integridad, Disponibilidad), establece políticas de seguridad. Este modelo trabaja protegiendo la información en tres formas:

- ***La Confidencialidad***: vigilan el acceso no autorizado de usuario o terceros de una compañía.

- ***La Integridad:*** Evita que no sea alterada la información.

- ***La Disponibilidad***: Se refiere para la parte de acuerdo de negocios, llamado Acuerdos de nivel de servicio (SLAs) usados por proveedores.

Ley 1273 “De la Protección de la información y de los datos". Esta ley en conjunto con sus artículos recrea los siguientes aspectos:

-***Capítulo I:*** De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.
-***Capítulo II:*** De los atentados informáticos y otras infracciones [9].

En ITIL (biblioteca de infraestructura tecnología de información), existe un proceso aplicado en la parte de seguridad informática, y es gestión de Accesos, en este proceso al usuario se le brinda permisos necesarios para acceder a la información, los cuales son:

- ***Petición de acceso***: Es una instrucción para autorizar el acceso.
- **Verificación:** Comprobación de la identidad del usuario que requiere el acceso.
- ***Monitorización de seguridad:*** Permisos que dependen del cambio de estatus que le realicen al usuario, por ejemplo un despido, una jubilación, un cambio de contrato.
- ***Registro y monitorización de accesos:*** Los permisos deben ser correctamente otorgados,

no se deben de asignar accesos de más al usuario sin autorización de su jefe inmediato.

- ***Eliminación y restricción de derechos:*** Se debe de asegurar que un usuario después de un despido, una terminación de contrato, un traslado del usuario éste se debe de eliminar completamente dependiendo del caso o se restringe el perfil según su nuevo cargo.

ISO/IEC 27000 estándar de seguridad, marco de Gestión de la Seguridad de Información apta empresas grandes, pequeñas o medianas. Certificación del Sistema de Gestión de Servicios de TI (Tecnologías de la Información), aplica para empresas que requiere la certificación. Conjunto de métodos de gran importancia para brindar un servicio seguro.

Esta norma tiene como metodología la gestión de la seguridad clara y estructurada, reduce el riesgo de pérdida en la información, implementa a sus clientes que tenga acceso a la información a través medidas de seguridad.

UNE-ISO 27001, norma que define procesos en servicio de seguridad. La norma ISO 27001 sé ha diseñado para implementa la calidad, experiencias y preparaciones notables para realizar auditorías de sistemas de gestión de la seguridad de la información.

La gestión de la seguridad de la información cumple unos requisitos que permite a las compañías inspeccionar y vigilar los riesgos de seguridad de la información, las amenazas y los puntos débiles existentes.

Esta norma de seguridad para procesos establecidos e implementados, y que estén en funcionamiento en una empresa, registra un control, una revisión y un progreso en la importancia para las auditorias.

La ISO 20071 hace que una empresa sea certificada, pueda registrarse ante entidades legas, como una compañía segura para sus clientes.

Con la ISO 27001, la norma ISO 27002 proporciona más información sobre cómo implementar los controles de seguridad especificados que en la ISO 27001. Otras normas que también pueden resultar útiles son la ISO 27005, que describe los procedimientos de evaluación de riesgos con mayor profundidad, y la BS 25999-2, que proporciona una descripción detallada de la gestión de la continuidad del negocio [10].

ISO 27002 es un código de buenas prácticas, donde se recolecta un inventario de inspecciones de seguridad. Esta norma pretende minimizar riesgos revelados en investigación de una organización. Su objetivo es proporcionar una guía y soporte en la dirección de seguridad de la información en relación a los requisitos del negocio, las leyes y regulación relevantes de una organización. Esta norma trabaja sobre varios aspectos, los cuales se mencionan a los más importantes:

- Política de Seguridad de la Información.
- Gestión de Activos de Información.
- Seguridad de los Recursos Humanos.
- Seguridad Física y Ambiental.
- Gestión de las Comunicaciones y Operaciones.
- Control de Accesos.
- Gestión de Incidentes en la Seguridad de la Información.

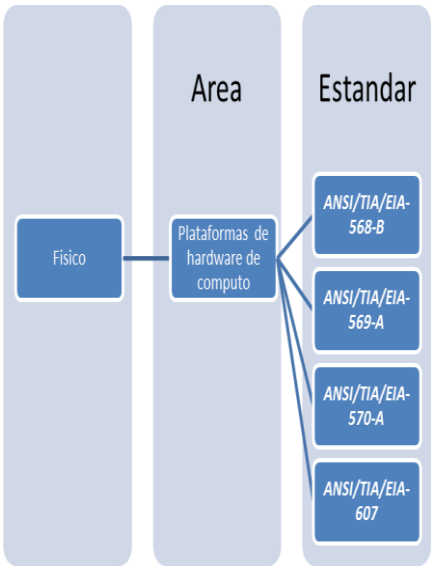
Ley 527 DE 1999 ampara la mensajería de datos, comercio electrónico, firma digital, entidad de certificación, intercambio electrónico de datos, sistemas de información. Cualquier tipo de violación a esta ley trae consecuencias altas [11].

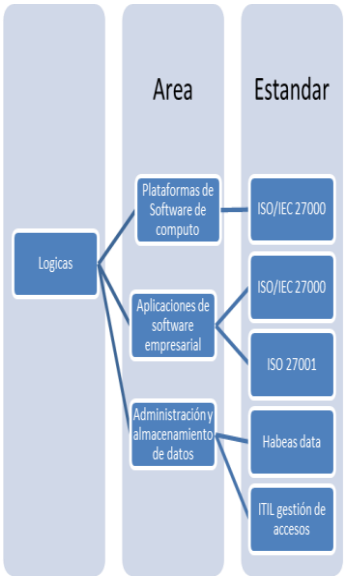
Unión Internacional de Telecomunicaciones (UIT), está catalogada como la más importante de las Naciones Unidas en todo lo que respecta a las Tecnologías de la Información y las Comunicaciones. Esta entidad se delega como la pionera de la regulación, la normativización y el progreso de las telecomunicaciones a nivel mundial, también trata la parte del espectro radioeléctrico y de las órbitas de los satélites. La norma más utiliza en la parte lógica es la:

- ***UIT-T X.1600*****:** éste estándar es aplicado para el marco de seguridad en la computación en la nube, describe las amenazas de seguridad

en el entorno de computación en la nube, proporciona referencia de implementación y seguridad en la información nivel de sistemas.

12. DIAGRAMA DE AREAS INFORMÁTICA E INFRAESTRUCTURA APLICANDO NORMAS DE SEGURIDAD.





CONCLUSIONES Y RECOMENDACIONES

- Se concluye que el movimiento de las normas de seguridad en las TIC dominan todos los datos a nivel mundial. En la actualidad el internet es una herramienta utilizada en todo el mundo, la cual permite acceder de forma más fácil a la información. Con los datos protegidos, los espías tendrán más dificultad para quebrantar los datos salvaguardados, y la información cada vez más es restringida con accesos autorizados, esta prevención se hace por medio del cumplimiento de la política de seguridad y esta es responsabilidad de todos.

- Se recomienda a las diferentes áreas que manejan tecnología, telecomunicaciones, que estén involucrada en la red de una compañía ya sea grande mediana o pequeña, profundizar más en la aplicación de las normas, leyes de seguridad, teniendo en cuenta que las normas evolucionan, y estas son aplicadas dependiendo del tipo de información que una compañía maneja.

REFERENCIAS

[1] Gómez, F., Tejero M., Vilar J.F., "Cómo hacer el Manual de Calidad la Nueva ISO 9001:2000", FC Editorial, España, 2005.

[2]Bon, J. "ISO/IEC 20000 Guía de Bolsillo", Itsm Library, 2006, noviembre.

[3] Díaz, G., "Procesos y herramientas para la seguridad de redes", Uned, Madrid, 2014 marzo.

[4] Gomez, A., "Seguridad Informática: Básico", Starbook, 2010.

[5] Miranda, L., "Norma ISO 17799", UTH, San Pedro Sula, 2012, diciembre.

[6] Cano, J, "Computación Forense", Alfaomega Grupo Editor S.A de C.V, México, 2009.

[7] Huidobro, J.M, "Redes de datos y convergencia IP", Creaciones Copyriht, 2007, marzo.

[8] Areitio, J., "Seguridad de la información, redes, informática y sistemas de información", Paraninfo, España, 2008.
[9] Suarez, S.R., “Comisión de conductas punibles en la internet en Colombia”, U de Nueva Granada, 2012.
[10] Atehortua, F., "sistema de gestión integral, una sola gestión, un solo equipo", U de A, Medellín, 2008, junio.
[11] Santofimio, J., “Procedimientos administrativos y tecnología”, U. Externado de Colombia, Bogotá, 2011.