ISO/IEC 27001:2013 – SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Zaida Milena Alvarez Isaza.
zaidam83@hotmail.com
Universidad Piloto de Colombia

Abstract— A Management System Information Security is a standard that allows the maintenance of the information security and data for both clients and suppliers, through the implementation of the ISO 2700 standard: 2013, This demonstrates that the information is integrated. Additionally, it strengthens the ethics of employees in order to improve the confidentiality of data in all areas within a company, reducing the risk of fraud and / or information requested.

Key words— Management, Standard, ISO, Integrity, Confidentiality, and Fraud.

Resumen— Un Sistema de Gestión de Seguridad de la Información es una norma que permite mantener la seguridad de la información y de los datos tanto del cliente como de los proveedores, por medio de la aplicación de la norma ISO 2700:2013: De esta manera es posible afirmar que la información se integra y que al mismo tiempo se fortalece la ética de los empleados. Una ética empresarial fortalecida permitirá aumentar el nivel de confidencialidad de los datos en todos los ámbitos dentro de una compañía, educiendo el posible riesgo de fraude y/o la pérdida de información.

Palabras clave—Gestión, Norma, ISO, Integridad, Confidencialidad, Fraude.

I. INTRODUCCIÓN

ISO/IEC-27001:3013 (Information Technology – Security Techniques – Information Security Management Systems – Requirements) fue aprobado y publicado en 2005 por la International Organization for Standardization y por la International Electrotechnical Commission, especificando los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) [1].

La norma ISO/IEC-27001 fue creada basándose en el ciclo de Deming, ciclo de mejora continua o ciclo PDCA, ciclo correspondiente a las iniciales de Planear (Plan), Hacer (Do), Verificar (Check) y Actuar (Act). A partir de lo anterior surge el Sistema de Gestión de la Seguridad de la Información (SGSI) o lo que es lo mismo en inglés: Information Security Management System [1].

Antes de proseguir, y para garantizar una mayor claridad sobre el concepto de un Sistema de Seguridad de la Información es necesario establecer las siguientes definiciones:

- Confidencialidad: Limitar el nivel de visibilidad de la visibilidad de la información a únicamente que tengan acceso a ésta.
- Integridad: La información podrá ser modificada solamente por aquellos con derecho a cambiarla.
- Disponibilidad. La información deberá estar disponible en el momento en que los usuarios autorizados requieran acceder a ella.

De acuerdo con las definiciones anteriores se puede asegurar que la seguridad de la información es el logro, gestión y el mantenimiento delos conceptos anteriores, de manera que estos se constituyen como sus como características elementales [2].

Adicionalmente a estas definiciones descritas, es necesario incluir la definición de una nueva característica denominada - no repudio – la cual también se debe tener en cuenta en la seguridad de la

información, debido a que asegura que un cambio a la información no sea negado (o repudiado) por quien realizó dicho cambio [2].

Por lo tanto, es permitir que las tres características claves de un sistema de Seguridad (CIA (Confidentiality, Integrity y Availability)) de la información, formen un vínculo entre procesos, gente y tecnología [2].

II. ESTADO DEL ARTE

La ISO/IEC 27001:2013 es la norma donde se contienen los requisitos para implementar y mejorar un Sistema de Gestión de Seguridad; tiene sus orígenes en una publicación del Departamento de Comercio e Industria (DTI), documento desarrollado origen en 1995 dentro de la norma BS7799-1 [3], que establecía un código de mejores prácticas para la administración de la seguridad de la información. Si bien ésta contenía algunas recomendaciones para la administración de la seguridad de la información, no definía realmente certificación alguna ni los mecanismos para lograrla. Con el paso del tiempo esta norma fue evolucionando, como se muestra a continuación [4].

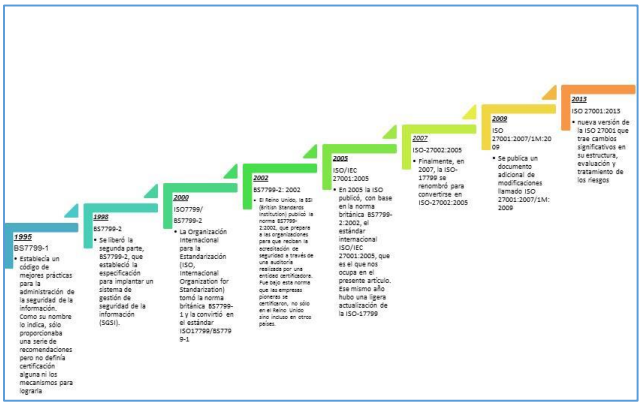

Ilustración 1 Origen y actualización de ISO/IEC 27001:2013. Imagen del autor.

A continuación, se describe la evolución de la norma ISO/IEC 27001:2013 a través de los últimos 20 años:

- ***1995***. BS7799-1: Contenía un código de mejores prácticas para el gobierno de la seguridad de la información. Sólo aportaba un conjunto de recomendaciones, pero no se hacía referencia a certificación alguna, ni los mecanismos para lograrla [4]. Ver **Ilustración 1.**
- ***1998***. BS7799-2: Contenía la descripción para establecer un Sistema de Gestión de seguridad de la Información (SGSI) [4]. Ver **Ilustración 1.**
- ***2000***. ISO7799/BS7799-2: La Organización Internacional para la Estandarización – ISO, tomó la norma británica BS7799-1 y la convirtió en el estándar ISO17799/BS7799-1[4]. Ver **Ilustración 1.**
- ***2002***. BS7799-2: 2002: Ésta versión de la norma prepara a las organizaciones para recibir la acreditación de seguridad a través de una auditoría realizada por una entidad certificadora. Se le atribuye a esta norma la certificación de las primeras compañías certificada en seguridad [4]. Ver **Ilustración 1.**
- ***2005***. IS O/IEC 27001:2005: En 2005 la ISO publicó el estándar internacional ISO/IEC 27001:2005, tema principal del presente artículo. Ver **Ilustración 1.**
- ***2007***. ISO-27002:2005: Finalmente, en 2007, la ISO-17799 se renombró para convertirse en ISO-27002:2005 [4]. Ver **Ilustración 1.**
- ***2009***. ISO 27001:2007/1M: 2009: Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M: 2009 [4]. Ver **Ilustración 1.**
- ***2013***. ISO 27001:2013: Nueva versión de la ISO 27001 que trae cambios significativos en su estructura, evaluación y tratamiento de los riesgos [4]. Ver **Ilustración 1.**

Actualmente, la norma es aplicable como ya se ha mencionado anteriormente, con el objetivo de proteger la información, teniendo en cuenta que cada vez más se presentan diferentes formas de incidentes relativos a la seguridad de la información.

En el mundo se han presentado diversas noticias relacionadas con incidentes de seguridad. A continuación, se mencionan algunos ejemplos:

- ***Hackean la botnet que distribuye locky para mostrar un mensaje de advertencia.***

Éste ataque consiste en el hackeo de la *botnet* que distribuye Locky, publicando un mensaje de advertencia a los usuarios y buscar así la generar conciencia sobre estas amenazas; se realiza la

descarga de un archivo comprimido que en su interior poseía un ejecutable que causó llegada de la amenaza y el posterior cifrado de la información almacenada en el equipo afectado. Tras este hackeo, el usuario continúa realizando la descarga de un archivo comprimido, pero en esta ocasión el código JavaScript realiza la apertura de una ventana del navegador para informar al usuario que no es recomendable realizar la ejecución de archivos descargados de páginas desconocidas o correos electrónicos enviados por un remitente desconocido. (Noticia publicada en mayo 19, 2016) [5].

- ***Un hacker encuentra un fallo que permitía a cualquiera robar 25.000 millones de un banco.***

Éste ataque, básicamente se realizaba debido al error que se encontraba en la aplicación en vista de que ésta no contaba con un *Certificate Pinning* (o cadena de certificado), de manera que podía ocurrir un ataque de man-in-the-middle, es decir que podía acceder a la información que se intercambia entre el usuario y el servidor sin que ninguna de las partes lo detectara. De esta manera, con certificados fraudulentos basados en SSL, se podía acceder a toda la información sin encriptar. (Noticia publicada en mayo 18, 2016) [6].

- ***Un ataque informático compromete la seguridad de millones de dispositivos ubiquiti.***

Éste ataque es posible debido a una vulnerabilidad conocida desde hace más de un año por medio de la cual cualquier usuario no autorizado podía acceder sin necesidad de credenciales a los equipos con versiones anteriores a estas que se mencionan a continuación:

- Airmax con firmware AiorOS. 5.6.4(XM/XW) y Legacy 4.0.4 (XS).
- AirFiber con firmware AF24/AF24HD 2.2.1 o 3.2.
- AirFiber con firmware AF5X 3.0.2.1+.

Para aprovecharse de estas vulnerabilidades los piratas informáticos crearon un virus que aprovechaba el fallo de seguridad en los módulos PHP y LightHttpd, instalándose así en los sistemas remotamente y controlándolos desde su posición de origen. Una vez que el virus se instala en el sistema empieza a buscar otras IPs de otros dispositivos y puede seguir infectando a otros usuarios vulnerables.

Una vez pasadas 18 horas desde la infección, el virus se activa, resetea los valores de fábrica de los equipos y obliga a sus dueños a desplazarse hasta ellos y volver a configurarlos nuevamente desde cero. (Noticia publicada en mayo 16, 2016) [7].

- ***Vulnerabilidad detectada hace seis años aún afecta a usuarios de sistemas SAP.***

Ésta vulnerabilidad se halla en Invoker Servlet, es una funcionalidad de sistemas SAP y afecta todos los elementos ejecutados en las plataformas SAP Java, o al menos las siguientes:

- SAP Enterprise Resource Planning (ERP).
- SAP Product Life-cycle Management (PLM).
- SAP Customer Relationship Management (CRM).
- SAP Supply Chain Management (SCM).
- SAP Supplier Relationship Management (SRM).
- SAP Enterprise Portal (EP).
- SAP Process Integration (PI).
- SAP Exchange Infrastructure (XI).
- SAP Solution Manager (SolMan).
- SAP NetWeaver Business Warehouse (BW).
- SAP Business Intelligence (BI).
- SAP NetWeaver Mobile Infrastructure (MI).
- SAP NetWeaver Development Infrastructure (NWDI).
- SAP Central Process Scheduling (CPS).
- SAP NetWeaver Composition Environment (CE).
- SAP NetWeaver Enterprise Search.
- SAP NetWeaver Identity Management (IdM).
- SAP Governance, Risk & Control 5.x (GRC).

Dicha vulnerabilidad ha permitido a los intrusos obtener acceso como administrador a los sistemas SAP por medio de Internet. Para ello se requiere únicamente la dirección IP del sistema SAP, y un

navegador al igual que un código de ataque. (Noticia publicada en mayo 14, 2016) [8].

A continuación, se mencionan algunas empresas certificadas ISO 27001:2015:

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 Support Services (MSS)	Colombia	IS 97104	ISO/IEC 27001:2005

Tabla 1 Empresas certificadas en Colombia [9].

En Colombia existen muchas entidades certificadoras; sin embargo, estas entidades deben estar acreditadas. Un tercero, conocido como organismo de acreditación, comprueba la competencia de estas entidades de mediante evaluaciones independientes e imparciales [9].

III. ISO/IEC 27001:2013

La norma está dividida en dos partes importantes; en la primera parte encontramos 10 puntos descritos a continuación:

1. *Objeto y campo de aplicación*: Detalla su finalidad y uso dentro de una organización.
2. *Referencias normativas.*
3. *Términos y definiciones*: Se basan en la norma ISO/IEC 27000.
4. *Contexto de la organización*: Busca determinar las necesidades y expectativas dentro y fuera de la organización que afecten directa o indirectamente al Sistema de Gestión de la Seguridad de la Información. Adicionalmente es necesario determinar el alcance.
5. *Liderazgo*: La importancia de la alta dirección y su compromiso con el sistema de gestión, estableciendo políticas, asegurando la integración de los requisitos del sistema de seguridad en los procesos de la organización, así como los recursos necesarios para su implementación y operatividad.
6. *Planificación*: Se deben valorar, analizar y evaluar los riesgos de seguridad de acuerdo a los criterios de aceptación de riesgos, así como establecer el tratamiento a los riesgos de seguridad de la información.
7. *Soporte***:** Se debe establecer la importancia de los recursos de la compañía, la concientización por parte de los stakeholders, las comunicaciones y de igual forma la información documentada.
8. *Operación*: Se establece la planificación y control de la operación.
9. *Evaluación de desempeño*: Se debe ejecutar un seguimiento, medición, análisis y evaluación del sistema de gestión de la información.
10. *Mejora*: Se debe ejecutar un seguimiento, medición, análisis y evaluación del sistema de gestión de la información.

Posteriormente a estos 10 puntos se encuentra el anexo A, el cual constituye la segunda parte de la norma en el que se establecen los objetivos de control y los controles de referencia [1]. Existen varios cambios con respecto a la versión 2005 en ésta versión 2013. Entre ellos se destacan:

- Desaparece la sección "Enfoque a Procesos" dando mayor flexibilidad para la elección de metodologías de trabajo para el análisis de riesgos y mejoras.
- Cambia su estructura conforme al anexo SL común al resto de estándares de la ISO.
- Pasa de 102 requisitos a 130.
- Se realizan cambios considerables en los controles establecidos en el Anexo A, incrementando el número de dominios a 14 y disminuyendo el número de controles a 114.

- Inclusión de un nuevo dominio sobre "Relaciones con el Proveedor" por las crecientes relaciones entre empresa y proveedor en la nube.
- Se parte del análisis de riesgos para determinar los controles necesarios y compararlos con el Anexo A, en lugar de identificar primero los activos, las amenazas y sus vulnerabilidades [1].

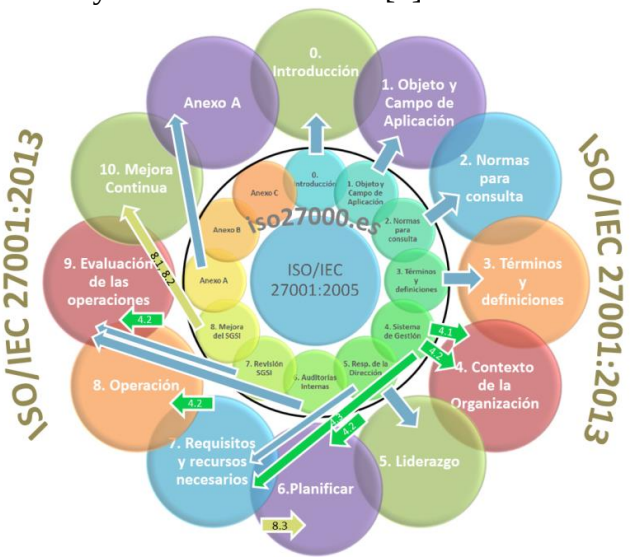

Ilustración 2 Diferencias fundamentales entre las dos versiones a modo de orientación. [4].

De igual forma dentro de esta nueva versión se han introducido los siguientes nuevos conceptos:

Concepto nuevo/actualizado	Explicación
Contexto de la organización	El ambiente en el que la organización opera
Problemas, riesgos y oportunidades	Reemplaza acciones preventivas
Partes interesadas	Reemplaza accionistas (stakeholders)
Liderazgo	Requerimientos específicos para la alta dirección
Comunicación	Hay requerimientos específicos tanto para comunicaciones internas como externas
Objetivos de seguridad de la información	Los objetivos de seguridad de la información ahora se establecen como funcio-nes relevantes y niveles
Evaluación de riesgos	La identificación de activos, amenazas y vulnerabilidades ya no es un pre requi-sito para la identificación de riesgos de seguridad de la información
Propietario de riesgo	Reemplaza propietario de los activos
Plan de tratamiento de riesgos	La efectividad del plan de tratamiento de riesgos es ahora considerado como más importante que la efectividad de los controles
Controles	Los controles ahora son determinados durante el proceso de tratamiento de riesgos, en lugar de ser seleccionados del Anexo A
Información documentada	Reemplaza documentos y registros
Evaluación del desempeño	Cubre las mediciones del SGSI y de la efectividad del plan de tratamiento de riesgos
Mejora continua	Se pueden utilizar metodologías distintas a Planear-Hacer-Verificar-Actuar (PDCA por sus siglas en inglés)

Tabla 2 Conceptos nuevos en la norma ISO – tabla tomada del siguiente sitio. [10].

Para entender con mayor calidad, pueden detallarse a continuación en cada una de las etapas los cambios presentados por esta versión de la norma:

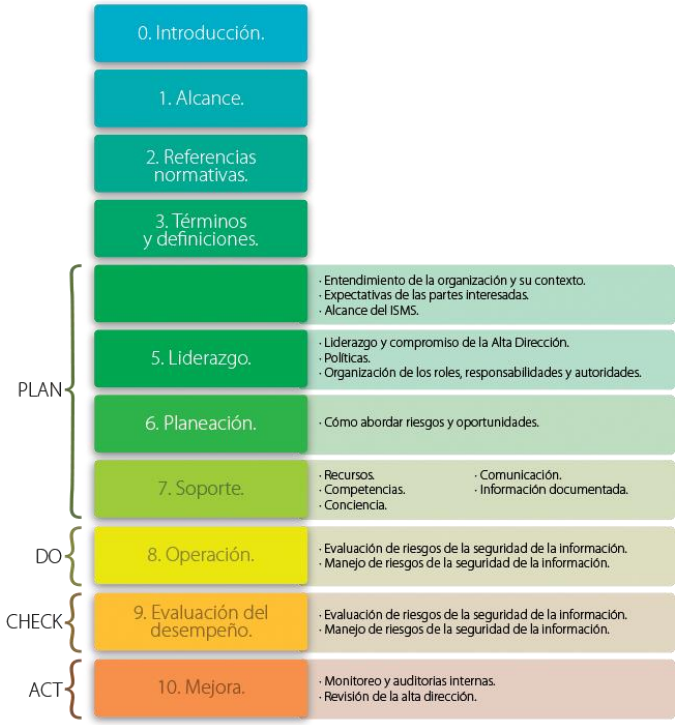

Ilustración 3Estructura del estándar ISO/IEC 27001:2013 [11].

El número de anexos también se modificó cambió en esta versión, aumentando el número de dominios de anexos de 11 a 14, permitiendo la inclusión de algunos controles con una mejor organización [11].

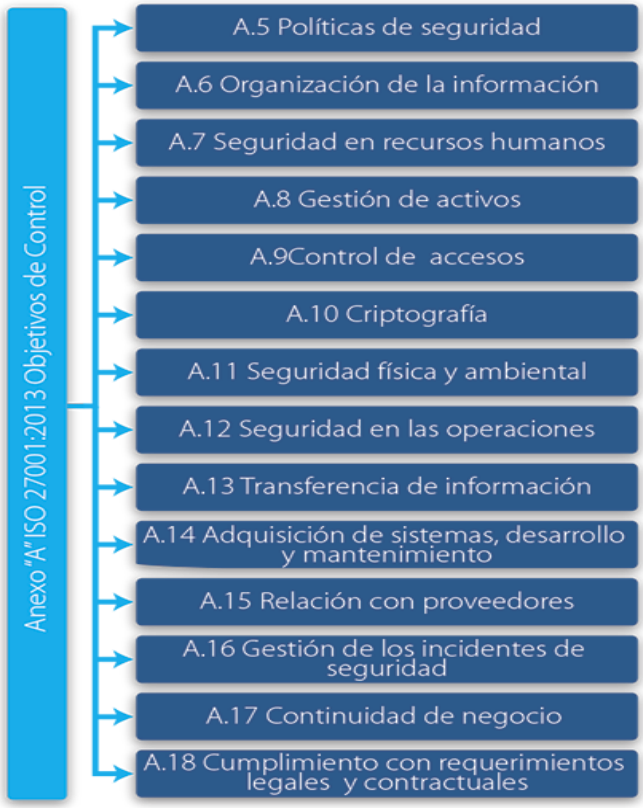

Ilustración 4 4 Dominios Anexo "A" de ISO 27001:2013 [11].

En consecuencia, se eliminan controles que no se incluyen en la nueva versión, los cuales se relacionan a continuación:

Control	Descripción
A.6.1.1	Comité de gestión para la seguridad de la información
A.6.1.2	Coordinación de seguridad de la información
A.6.1.4	Procesos de autorización para instalaciones para procesamiento de información
A.6.2.1	Identificación de riesgos relacionados con agentes externos
A.6.2.2	Direccionamiento de seguridad al tratar con clientes
A.10.2.1	Entrega del servicio
A.10.7.4	Seguridad del sistema de documentos
A.10.8.5	Sistema de información de negocios
A.10.10.2	Seguimiento al uso de sistema
A.10.10.5	Falla en el registro
A.11.4.2	Autenticación de usuarios para conexiones externas
A.11.4.3	Identificación de equipos
A.11.4.4	Puerto remoto de diagnóstico y configuración de protección
A.11.4.6	Control para la conexión de redes
A.11.6.2	Aislamiento del sistema sensible
A.12.2.1	Validación de datos de entrada
A.12.2.2	Control de procesamiento interno
A.12.2.3	Integridad de mensaje
A.12.2.4	Validación de datos de salida
A.12.5.4	Filtración de la información
A.15.1.5	Prevención del uso indebido de las instalaciones para el procesamiento de información
A.15.3.2	Protección de las herramientas de auditoría de sistemas de información

Tabla 3 Lista de controles que ya no forman parte del estándar [11].

Así como fueron eliminados algunos controles en la nueva normatividad, también es posible identificar algunos nuevos, y que también se presentan en este artículo:

Control	Descripción
A.6.1.4	Seguridad de la información en la gestión de proyectos
A.12.6.2	Restricciones en la instalación de software
A.14.2.1	Política de desarrollo de seguridad
A.14.2.5	Desarrollo de procedimientos para el sistema
A.14.2.6	Desarrollo de un entorno seguro
A.14.2.8	Sistema de prueba de seguridad
A.15.1.1	Información de seguridad para las relaciones de proveedores
A.15.1.3	Cadena de suministro ICT
A.16.1.4	Evaluación y decisión de los eventos de seguridad de la información
A.16.1.5	Respuesta a incidentes de seguridad de la información
A.17.1.2	Implementación de la continuidad de la seguridad de la información
A.17.2.1	Disponibilidad de las instalaciones para procesamiento de información.

Tabla 4 Nuevos controles propuestos [11].

IV. IMPLEMENTACIÓN.

En la implementación de la norma, es recomendable que las empresas sigan los siguientes pasos, de tal manera que puedan concluir con este proceso satisfactoriamente.

A continuación, se mencionan algunos pasos que se sugieren seguir para su implementación [3]:

- Obtener el apoyo de la dirección.
- Utilizar una metodología para gestión de proyectos.
- Definir el alcance del SGSI.
- Redactar una política de alto nivel sobre seguridad de la información.
- Definir la metodología de evaluación de riesgos.
- Realizar la evaluación y el tratamiento de riesgos.
- Redactar la Declaración de aplicabilidad.
- Redactar el Plan de tratamiento de riesgos.
- Definir la forma de medir la efectividad de sus controles y de su SGSI.
- Implementar todos los controles y procedimientos necesarios.
- Implementar programas de capacitación y concienciación.
- Realizar todas las operaciones diarias establecidas en la documentación de su SGSI.
- Monitorear y medir su SGSI.
- Realizar la auditoría interna.
- Implementar medidas correctivas.

V. DOCUMENTACIÓN REQUERIDA PARA UNA IMPLEMENTACIÓN DE LA NORMA

Para obtener la certificación de la norma en una empresa es necesario confeccionar la siguiente documentación:

- Alcance del SGSI.
- Objetivos y política de seguridad de la información.
- Metodología de evaluación y tratamiento de riesgos.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Informe de evaluación de riesgos.
- Definición de roles y responsabilidades de seguridad.
- Inventario de activos.
- Uso aceptable de los activos.
- Política de control de acceso.
- Procedimientos operativos para gestión de TI.
- Principios de ingeniería para sistema seguro.
- Política de seguridad para proveedores.
- Procedimiento para gestión de incidentes.
- Procedimientos para continuidad del negocio
- Requisitos legales, normativos y contractuales.

Adicionalmente, existe también un listado documentación que debe tener la empresa obligatoriamente:

- Registros de capacitación, habilidades, experiencia y calificaciones.
- Monitoreo y resultados de medición.
- Programa de auditoría interna.
- Resultados de auditorías internas.
- Resultados de la revisión por parte de la dirección.
- Resultados de medidas correctivas.
- Registros sobre actividades de los usuarios, excepciones y eventos de seguridad.

VI. CONCLUSIONES

La información en las empresas es considerada como uno de sus activos más valiosos, teniendo en cuenta

que en ella se pueden encontrarse datos confidenciales de proveedores, clientes, e incluso de la empresa misma. Por tal motivo ésta se ha convertido en el objetivo principal para los delincuentes cibernéticos. Para contrarrestar esta situación la norma ISO 27001:2013 se ha convertido en un escudo protector para proteger la información.

Es recomendable implementar los controles establecidos en la norma, de acuerdo a lo que sea conveniente en cada una de las empresas que se acogen a su implementación. Actualmente son muchas las empresas que ya tienen implementados los controles que brindan seguridad y confianza tanto a la empresa en el préstamo de sus servicios como a los proveedores y clientes.

Es vital tener en cuenta que para una empresa es muy importante la implementación de la norma para la seguridad de la información. Teniendo en cuenta que actualmente están surgiendo nuevas leyes y normativas contractuales relacionadas con la seguridad de la información, esta noma proporciona la metodología perfecta para ello.

Del mismo modo las empresas obtienen una ventaja comercial. Si la empresa obtiene una certificación de la norma y sus competidores no lo hacen, es probable que se produzca valor para los clientes, ya que la empresa se hace más confiable debido a que le interesa mantener segura su información.

También se genera menos costo teniendo en cuenta que la filosofía principal de la norma, es evitar que se produzcan incidentes de seguridad.

Adicionalmente, las empresas tienden a ser más organizadas puesto que la implementación de la norma ayuda a que en el crecimiento de las empresas s, los empleados definan procesos y procedimientos de la mejor manera, reduciendo sus tiempos de definición en comparación a cuando ésta no se implementa [3].

VII. REFERENCIAS

[1] Josepth Wayne «ISO/IEC 27001» Revisión del 16:04 14 mar 2016 - [En línea]. Available: https://es.wikipedia.org/wiki/ISO/IEC_27001 [Último acceso: 21 Junio 2016].

[2] Revisión del 22:37 15 jul 2016 «Seguridad de la información» [En línea]. Available: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3 [Último acceso: 21 Junio 2016].

[3] The ISO 27001 & ISO 22301 Blog | 27001Academy « ¿Qué es norma ISO 27001? » [En línea]. Available: http://advisera.com/27001academy/es/que-es-iso-27001/ [Último acceso: 21 Junio 2016].

[4] ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información «El portal de ISO 27001 en Español» Revisión del 23/08/2016 [En línea]. Available: http://www.iso27000.es/iso27000.html [Último acceso: 22 Junio 2016].

[5] Hackean la botnet que distribuye Locky para mostrar un mensaje de advertencia – Noticias de Hacking «Noticias de Hacking» Revisión del 19/05/2016 [En línea]. Available: https://noticiasdeseguridadinformatica.wordpress.com/2016/05/19/hackean-la-botnet-que-distribuye-locky-para-mostrar-un-mensaje-de-advertencia/ [Último acceso: 22 Junio 2016].

[6] Un hacker encuentra un fallo que permitía a cualquiera robar 25.000 millones de un banco Revisión del 23/08/2016 [En línea]. Available: http://www.adslzone.net/2016/05/18/un-hacker-encuentra-un-fallo-que-permitia-a-cualquiera-robar-25-000-millones-de-un-banco/ [Último acceso: 22 Junio 2016].

[7] Un ataque informático compromete la seguridad de millones de dispositivos Ubiquiti. Revisión del 16/05/2016 [En línea]. Available: http://www.redeszone.net/2016/05/16/ataque-informatico-compromete-la-seguridad-millones-dispositivos-ubiquiti/ [Último acceso: 22 Junio 2016].

[8] Vulnerabilidad afecta usuarios de SAP «Vulnerabilidad detectada hace seis años aún afecta a usuarios de sistemas SAP» Revisión del 23/08/2016 [En línea]. Available:

http://www.enhacke.com/2016/05/13/vulnerabilidad-afecta-sitemas-sap/. [Último acceso: 22 Junio 2016].

[9] Proceso Certificación 27001: EMPRESAS CERTIFICADAS DE COLOMBIA «EMPRESAS CERTIFICADAS DE COLOMBIA» Revisión del 23/08/2016 [En línea]. Available: http://certificacion27001.blogspot.com.co/2010/09/empresas-certificadas-de-colombia.html [Último acceso: 17 Agosto 2016].

[10] Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013 «El nuevo estándar internacional para los sistemas de gestión de seguridad de la información» Revisión del 23/08/2016 [En línea]. Available: http://docplayer.es/1146243-Pasando-de-iso-iec-27001-2005-a-iso-iec-27001-2013.html[Último acceso: 17 Agosto 2016].

[11] ISO-27001:2013 ¿Qué hay de nuevo? | Magazcitum [En línea]. Available: http://www.magazcitum.com.mx/?p=2397#.V7xiL_IUXIU [Último acceso: 17 Agosto 2016].

Autor:
Ingeniero de Sistemas graduado de la Corporación Universitaria Rafael Núñez en el año 2008 y con certificación COBIT 4. Cuenta con una amplia experiencia en auditorias, consultorías, revisoría fiscal enfocada en la seguridad informática, aplicada en entornos organizacionales, en diversos sectores de la industria colombiana.