ESTANDARES INTERNACIONALES PARA EL CONTROL

EN LAS ISO

ISBN: 978-9942-14-163-7
Título: Estandares Internacionales para el Control en las ISO

Autores: Quintana Sánchez, Armando Miguel
Quintanilla Romero, Marco Antonio
Ojeda Escobar, Jorge Aníbal
Trujillo Calero, Geoconda Elizabeth

Editorial: Quintanilla Romero, Marco Antonio

Materia: Administración de formas generales de control
Publicado: 2016-03-10
NºEdición: 2
Idioma: Español

www.uceinvestigar.com

ISBN 978-9942-14-163-7
9 789942 141637

ESTÁNDARES INTERNACIONALES PARA EL CONTROL EN LAS ISO

ÍNDICE

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

PRÓLOGO

En el presente trabajo de investigación, titulado "Normas ISO para aseguramiento de la Información en las Organizaciones" se realizó un investigación sobre todas las normas ISO que permiten a las Organizaciones asegurar la información, ya que ésta es su principal activo. Las normas son un modelo, un patrón, ejemplo o criterio a seguir.

Una norma es una fórmula que tiene valor de regla y tiene por finalidad definir las características que debe poseer un objeto y los productos que han de tener una compatibilidad para ser usados a nivel internacional.

El trabajo realizado se divide en cuatro capítulos que permiten tener una visión clara sobre las normas ISO, las mismas que son normas de estándares internacionales que deben aplicarse para el aseguramiento de la información, se describe origen, posicionamiento, y luego se hizo un resumen de las consideraciones clave del mismo.

En el Capítulo I se plantea el tema y su problemática, los objetivos de la investigación y su justificación.

En el Capítulo II se habla de los antecedentes de las Normas ISO y el marco teórico que nos redacta cada una de las normas, como son: NORMA ISO 15408 sobre Tecnologías de Seguridad, NORMAS ISO 17799 sobre Políticas de Seguridad, NORMAS ISO 20000 sobre Gestión de Servicios de las TIC, NORMA ISO 27001 sobre Norma Auditable (Requisitos para un Sistema de Gestión de la Seguridad de la Información), NORMA ISO 27002, NORMA ISO 38500 Gobierno de TI.

En el Capítulo III se plasma las conclusiones y recomendaciones del presente trabajo de Investigación.

Y para concluir en el Capítulo IV se incluye un glosario de términos, anexo de gráficos y la bibliografía.

1. INTRODUCCIÓN

Normas ISO para aseguramiento de la Información en las Organizaciones.

La seguridad en las tecnologías de la información y comunicaciones (TICs), se hace tan indispensable como su funcionalidad misma. Preservar la disponibilidad, integridad y confidencialidad, de sus datos y operaciones, es un reto que se hace cada día más complejo, por su misma evolución y los riesgos que cada día se vuelven más sofisticados, al estar cada vez los usuarios mejor conectados y menos controlados.

Actualmente existen diferentes estándares, modelos, sistemas de gestión y buenas prácticas que promueven la seguridad de la información en las compañías y tecnologías, dentro del más relevante es el estándar ISO/IEC 15408 Common Criteria, el cual es un acuerdo internacional entre diferentes organizaciones de todo el mundo para que con base al cumplimiento de funciones y niveles de evaluación, se garantice diseño, desarrollo y puesta en producción con medidas de seguridad adecuadas para el mercado, entidades vigilantes y la comunidad en general.

La seguridad en los componentes de las tecnologías de la información (Seguridad Informática), es una de las necesidades que junto con las funcionales es fundamental, debido a que un fallo en ella genera un impacto directo en contra del objetivo por el cual fueron concebidos los componentes.
Para la seguridad de las tecnologías de la información existen los siguientes estándares y buenas prácticas:

- ISO 27001
- Cobit
- Magerit
- ITIL
- ISO/IEC 15408 Common Criteria

La complejidad de las medidas requeridas para el aseguramiento de los sistemas de información, se hace mayor cada día, obligando a todos los interesados, a facilitar el desarrollo de esquemas, que tengan en cuenta el carácter globalizado de las Tecnologías de la Información por la conectividad y disponibilidad necesaria y los problemas de delitos informáticos que son cada día más críticos.

Hoy en día las Tecnologías de la Información y Comunicación (TIC), están presentes en todos los aspectos de nuestra vida diaria, teniendo impactos significativos en la vida social, económica y cultural de la sociedad, es así que la expansión de las TIC ha contribuido a modificar de manera

irreversible la vida de los países y la experiencia de las personas, alternado las coordenadas de tiempo y espacio que ordenan la vida en la sociedad, conformando una nueva forma de organización social en redes.

El desarrollo de la tecnología ha sido a lo largo de la historia de la humanidad el factor modernizador por excelencia, no solo de los sectores productivos, sino de la sociedad y por supuesto, la empresa como relación de comunicación, mediación y ganancias financieras; es por ello que se vale de los medios técnicos y tecnológicos disponibles para lograr sus objetivos de negocio.

Es quizá en las Pymes en donde se encuentran menores, pero crecientes esfuerzos por tecnificarse, pues a pesar de que cuentan con presupuestos limitados para desarrollo e implementación de TI, por lo menos se adhieren a este mundo cambiante gracias a la masificación de las tecnologías.

Bajo este contexto, es necesario que las pequeñas y medianas empresas de nuestro país y de todo el mundo opten por analizar nuevas alternativas de tecnología de seguridad en su información, implementen estándares internacionales, asignen recursos suficientes para TI, creen planes de aseguramiento para una correcta administración de TI, cambien sus formas de producción apoyados en la tecnologías, entre otras opciones, con el único fin de estar a la vanguardia de los tiempos y siempre en constante competitividad con el resto del mundo.

Las empresas en su gran mayoría manejan normas de seguridad, que aunque bastante obsoletas; sirven de fundamentos para el establecimiento de bases que permitan un desarrollo de negocio siempre creciente, enmarcado en un mundo industrializado digitalmente que cada vez más, se apoya en el Gobierno TI, para complementar su estrategia corporativa y de esta manera maximizar sus ingresos y tener un mejor control de sus procesos y costos.

“Pensamos que, en un futuro cercano, todos los departamentos de tecnología deberán tener implantadas buenas prácticas que cubran las diferentes áreas de gobierno y gestión, para lo cual deberán centrar sus esfuerzos en definir, medir y analizar los procesos relacionados con las TI y en su mejora continua.” (Fernandez & Piattini, 2012)

Actualmente la tendencia de la gran mayoría de las empresas dedicadas o relacionadas con las tecnologías de información, es enfocar sus procesos a transacciones y operaciones de manera más innovadora a través de una red, al hablar de innovación nos referimos a un sentido más amplio de la misma que abarca todos los conceptos empresariales: estrategias, procesos,

productos, servicios, etc.[1] En el 2015 las tendencias tecnológicas han sido englobadas en tres temas principales: la fusión de los mundos reales y virtuales, el advenimiento de la inteligencia en todas partes, y el impacto de las TI en el desarrollo del negocio digital. Con la evolución constante de las TI es indispensable contar con la llamada seguridad informática, para a través de mecanismo de seguridad aplacar los riesgos y amenazas existentes, salvaguardando así la infraestructura computacional y todo lo relacionado con esta, así como también la información que contenga. Las amenazas pueden ser ocasionadas por usuarios, programas maliciosos, errores de programación, intrusos, siniestros, personal técnico interno, fallos electrónicos, catastros naturales; mientras que el riesgo comprende el análisis propiamente dicho de vulnerabilidades y amenazas.[2]

Al ser un tema tan transcendental en la actualidad existen Estándares Internacionales normados y publicados por las organizaciones ISO, estas normas proporcionan lineamientos mecanismos de seguridad que proporcionan modelos, patrones a seguir, concluyendo en que los resultados conseguidos al aplicarlas son los ideales y que deberían ser implementados por todas las organizaciones relacionadas a las tecnologías de la información.

Uno de los inconvenientes de las empresas es la falta de importancia a la seguridad de información, al no tener mecanismos que ayuden a salvaguardarla hace que el activo más importante de la organización el cual es la información se vuelva vulnerable, a cualquier riesgo o amenaza, lo que puede ocasionar que las pérdidas por la falta de seguridad pueden ser tremendamente costosas, tanto en materia económica como en cuanto a prestigio lo que ocasionaría un decremento en el nivel de ventas, problemas legales, daños a empleados de la organización o a terceros, etc.

De acuerdo a la importancia de la seguridad en las tecnologías de la información citadas, se evidencia que el estudio y aplicación de las Normas Internacionales certificables, es un beneficio invalorable para las organizaciones. Por ello se justifica que el estudio de las Normas Internacionales alineadas a las TI son necesarias para cualquier organización relacionadas a aspectos de TI.

[1] http://www.monografias.com/trabajos23/organizaciones-innovadoras/organizaciones-innovadoras.shtml
[2] http://www.ticbeat.com/tecnologias/10-tendencias-tecnologicas-marcaran-2015/

2. ANTECEDENTES

La ISO (International Standarization Organization) es la entidad internacional encargada de favorecer la normalización en el mundo. Con sede en Ginebra, es una federación de organismos nacionales, éstos, a su vez, son oficinas de normalización que actúan de delegadas en cada país, como por ejemplo: AENOR en España, AFNOR en Francia, DIN en Alemania, etc. con comités técnicos que llevan a término las normas. Se creó para dar más eficacia a las normas nacionales.

ISO es el acrónimo de International Organization for Standardization. Aunque si se observan las iniciales para el acrónimo, el nombre debería ser IOS, los fundadores decidieron que fuera ISO, derivado del griego "isos", que significa "igual". Por lo tanto, en cualquier país o en cualquier idioma, el nombre de la institución es ISO, y no cambia de acuerdo a la traducción de "International Organization for Standardization" que corresponda a cada idioma. .

Respecto al origen de la organización ISO, oficialmente comenzó sus operaciones el 23 de febrero de 1947 en Geneva, Suiza. Nació con el objetivo de "facilitar la coordinación internacional y la unificación de los estándares industriales."

El gran éxito obtenido desde la primera edición de las normas en 1987, unido a que los protocolos de ISO requieren que todas las normas sean revisadas al menos cada cinco años para determinar si deben mantenerse, revisarse o anularse.

El proceso de revisión es responsabilidad del Comité Técnico ISO/TC 176, y se ha llevado a cabo sobre la base del consenso entre expertos en calidad de países miembros de ISO. Para la revisión del "año 2000", el TC 176 ha adoptado un enfoque de gestión de proyecto para hacer frente a la complejidad de esta tarea. Los objetivos y las especificaciones iniciales del proyecto fueron establecidos después de haber llevado a cabo una amplia encuesta a los usuarios para determinar sus necesidades y expectativas en cuanto a las nuevas revisiones.

Para el proceso de revisión el Comité Técnico 176 de ISO, adoptó un proceso de revisión, conocido como Visión 2000 que tiene como objetivos primordiales:

- Proporcionar una estructura común basada en el modelo de procesos
- Incrementar la compatibilidad con las normas de Sistemas de Gestión Medioambiental (ISO 14000)
- Proporcionar un alcance reducido de los requisitos de la Norma ISO 9001
- Incluir requisitos para la mejora continua

- Adecuación para organizaciones de cualquier tamaño y sector
- Relación amigable usuario / cliente
- Fácil transición para organizaciones ya certificadas

Por lo tanto, los principios que están guiando el proceso de revisión son, entre otros:

- Aplicación a todos los sectores de productos y servicios y a todo tipo de organizaciones.
- Sencillez de uso, lenguaje claro, facilitar su traducción y hacerlas más comprensibles.
- Aptitud para conectar los Sistemas de Gestión de la Calidad con los procesos de la organización.
- Gran orientación hacia la mejora continua y la satisfacción del cliente.
- Compatibilidad con otros sistemas de gestión tales como ISO 14000 para la Gestión Medioambiental.

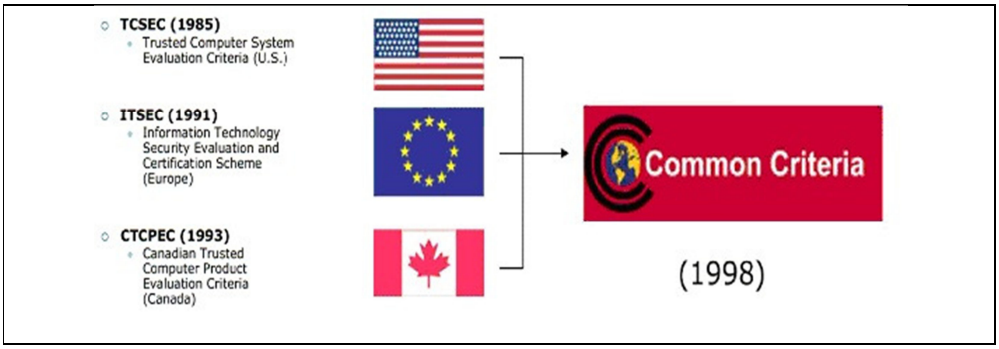
La revisión se hace por la necesidad de suministrar una base consistente y de identificar las necesidades primarias y los intereses de las organizaciones en sectores específicos, tales como aerospacial, automoción, productos sanitarios, telecomunicaciones y otros.

Esta familia adoptó el esquema de numeración utilizando las series del número 27000 en secuencia, por lo que a partir de julio de 2007, las nuevas ediciones del ISO/IEC 17799 se encuentran bajo el esquema de numeración con el nombre ISO/IEC 27002.

Cada día crece más la preocupación sobre la seguridad de la información contenida en los dispositivos hardware y sistemas de IT. Los usuarios finales de TI carecen de los conocimientos, la experiencia o los recursos necesarios para poder determinar o juzgar si sus dispositivos o sistemas le ofrecen el nivel de confianza adecuado.

Los “Common Criteria” (ISO/IEC 15408) son el resultado de la unificación de las diferentes normativas internacionales confluyendo en un estándar único y común reconocido a nivel mundial como se muestra en el siguiente gráfico.

Gráfico No. 1 Normativa Internacional



La serie ISO/IEC 20000 - Service Management normalizada y publicada por las organizaciones ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) el 14 de diciembre de 2005, es el estándar reconocido internacionalmente en gestión de servicios de TI (Tecnologías de la Información). La serie 20000 proviene de la adopción de la serie BS 15000 desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

ISO/IEC 20000 está basada y reemplaza a la BS 15000, la norma reconocida internacionalmente como una British Standard (BS), y que está disponible en dos partes: una especificación auditable y un código de buenas prácticas.

Razones del sistema de certificación ISO

En si las razones principales para implementar un sistema ISO son:

- Exigencias del mercado (en muchos casos no se puede vender sin ellas).
- Mejora la competitividad de la empresa (frente a competidores que no la poseen).
- Mejora la eficiencia interna de la empresa (la organización funciona mejor).
- Mejora la eficiencia de los proveedores (asegura suministros y servicios en tiempo y forma).
- Mejora la imagen de la organización frente a sus clientes, la comunidad y a su propio personal.

2.1. PRINCIPALES ISO

2.1.1. NORMA ISO 15408. TECNOLOGÍAS DE SEGURIDAD

2.1.1.1. IMPORTANCIA DE LA ISO 15408

En los años 90 surgió la necesidad de conocer qué requisitos de seguridad debería tener un software, hardware o firmware. A través de la combinación de los criterios aplicados en Inglaterra, Estados Unidos y Canadá, la International Organization for Standardization (ISO) constituyó y adoptó los Criterios Comunes de Evaluación de Seguridad para Tecnologías de la Información.

Los Criterios Comunes (CC) son la combinación de:

- TCSEC (del inglés Trusted Computer System Evaluation Criteria), conocido como "Libro Naranja" y utilizados por el Departamento de Defensa de EE.UU.

- ITSEC (del inglés Information Technology Security Evaluation Criteria) conocido como "Libro Blanco" y utilizados en Europa

- CTCPEC (del inglés Canadian Trusted Computer Product Evaluation Criteria) utilizados en Canadá.

Los Criterios Comunes (ISO/IEC 15408) son el resultado de la unificación de las diferentes normativas internacionales, desarrollando un estándar único y común reconocido a nivel mundial.

La norma ISO/IEC 15408 (Evaluation criteria for IT security) proporciona criterios para especificar medidas de seguridad y requisitos de seguridad de los productos y sistemas de tecnologías de la información, facilitando una expresión precisa de los mismos, así como los criterios para evaluar su seguridad.

Esta norma permite la comparación entre los resultados de las evaluaciones de seguridad independientes, a través de un conjunto común de requisitos para la funcionalidad de seguridad de los productos de TI y de las medidas de aseguramiento aplicadas a estos productos.

El objetivo es establecer los requisitos de seguridad que debe cumplir un determinado producto.

Los desarrolladores de productos o sistemas de tecnologías de información (fabricantes) pueden ajustar sus diseños y explicar lo que ofrecen.

Los usuarios pueden conocer el nivel de confianza y seguridad que los productos de TI y sistemas le ofrecen. Pueden expresar cuáles son sus necesidades.

Los evaluadores de seguridad, que juzgan y certifican en qué medida se ajusta una especificación de un producto o sistema IT a los requisitos de seguridad deseados, es decir, puede evaluar y certificar lo que asegura.

2.1.1.2. BASES DE LOS CRITERIOS COMUNES

1. **Perfiles de Protección (Protection Profiles - PP)**: Es un conjunto de requisitos de seguridad independientes de cualquier tipo de implementación para una categoría de Objetivos de Evaluación que cumplen una serie de necesidades específicas para el consumidor.

2. **Objetivos de Seguridad (Security Targets - ST):** Son un conjunto de requisitos de seguridad para una implementación concreta que sirve como base para la evaluación de un determinado TOE. Un ST puede hacer referencia a un PP. Un ST es la base para el acuerdo entre todas las partes acerca de la seguridad que ofrece un TOE. Al igual que en el PP, los requisitos de seguridad en un ST deben incluir un EAL de la parte 3 de la norma.

3. **Objetivos de Evaluación (Target of Evaluation - TOE):** Son productos de tecnologías de la información o sistemas y su documentación asociada en términos de guías de administración y usuario que son objeto de evaluación. Posibles ejemplos de TOEs pueden ser una aplicación, una aplicación en conjunción con un sistema operativo, un sistema operativo en conjunción con una estación de trabajo, entre otros.

4. **Niveles de Evaluación de Seguridad (Evaluation Assurance Levels - EAL):** Es un conjunto de requisitos de seguridad que conjuntamente proporcionan un nivel de confianza concreto.

2.1.1.3. ORGANIZACIÓN DE LA NORMA 15408

La norma ISO 15408 se divide en tres partes:

1. Introducción y modelo general

2. Requisitos funcionales de seguridad
3. Requisitos de garantía de seguridad

Introducción y modelo general

Define los conceptos y principios generales de la evaluación de seguridad TI y proporcionada un modelo de evaluación.

Los usuarios pueden especificar sus necesidades de seguridad, es decir, especificar qué funcionalidad debe tener los productos para cubrir esas necesidades, lo cual se concreta en los documentos Perfiles de Protección.

Componentes funcionales de seguridad

Establece el catálogo de requisitos funcionales de seguridad que sirven de plantillas para definir las funcionalidades de seguridad de un producto.

Los fabricantes e integradores pueden implementar y declarar los atributos de seguridad de sus productos, es decir, indicar qué hace cada producto, lo que se concreta en un documento llamado Declaración de Seguridad.

Requisitos de garantía de seguridad

Establece el catálogo de requisitos de garantía de seguridad que debe cumplir la documentación, el producto a evaluar, el entorno de desarrollo y otras partes implicadas en la seguridad del producto.

La tercera parte de los Criterios Comunes también define el criterio de evaluación de los Perfiles de Protección (PP), declaraciones de seguridad (ST) y otras evidencias de evaluación. Además se presentan siete paquetes de garantía predefinidos, los cuales son llamados niveles de garantía de evaluación (EAL).

A medida que se incrementa el nivel de garantía de evaluación (EAL), la inversión por parte del laboratorio en tiempo, recursos y exigencia, también aumentan.

2.1.1.4. NIVELES DE EVALUACIÓN DE SEGURIDAD

Los niveles de evaluación de seguridad representan una escala creciente que balancea el nivel de seguridad obtenido con el costo y viabilidad de adquisición de ese nivel de seguridad.

El nivel de esfuerzo necesario para pasar de un nivel a otro se basa en un incremento de:

- **Alcance:** El esfuerzo es mayor porque existen más componentes del producto a analizar.
- **Profundidad:** El esfuerzo es mayor porque aumenta el nivel de detalle de la implementación y el diseño.
- **Rigor:** El esfuerzo es mayor porque se aplica una forma más estructurada y formal.

Los niveles de seguridad son:

1. **EAL1:** Proporciona un nivel básico de seguridad mediante el análisis de la especificación funcional y de interfaces así como de las guías de documentación con el objetivo de entender el comportamiento en materia de seguridad.

2. **EAL2:** Proporciona un aumento significativo en seguridad con respecto al nivel anterior requiriendo el testeo por parte del desarrollador, un análisis de vulnerabilidad y unas pruebas independientes basadas en especificaciones del TOE más detalladas.

3. **EAL3:** Se incrementan las capacidades de seguridad solicitando una cobertura de pruebas más completas sobre las funciones de seguridad y mecanismos y/o procedimientos que proporcionen confianza de que el TOE no ha sido manipulado durante su desarrollo.

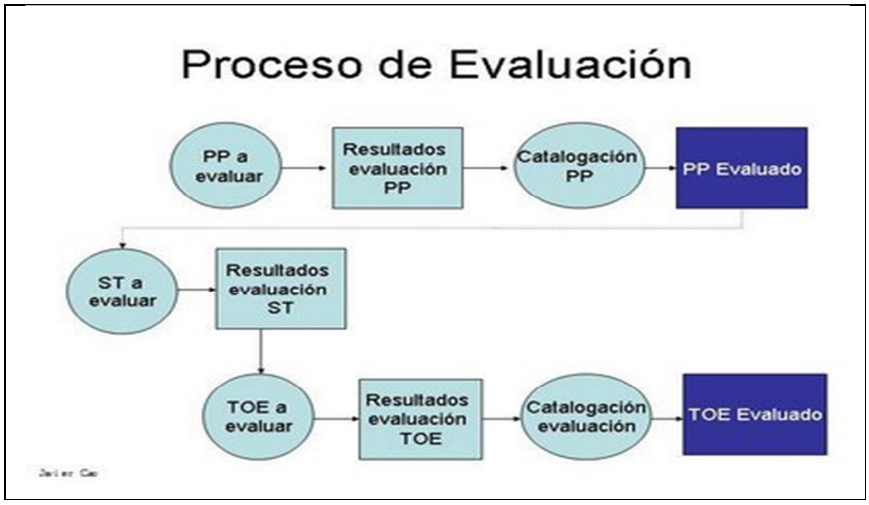
4. **EAL4:** Con respecto al nivel anterior, se requiere más descripción del diseño, un subconjunto de implementación, y mecanismos o procedimientos mejorados que provean confianza de que el producto no ha sido alterado durante su desarrollo o entrega.

5. **EAL5:** Se requieren descripciones semi-formales, la implementación completa y una arquitectura más estructurada y análisis de comunicaciones cifradas.

6. **EAL6:** Se requiere un análisis más exhaustivo, una representación estructurada de la implementación, una arquitectura más estructurada, un análisis de vulnerabilidades más exhaustivo, identificación cifrada, gestión de la configuración mejorada y más controles en el entorno de desarrollo.

7. **EAL7:** Se incrementa aún más la exhaustividad del análisis usando una representación o correspondencia formal

Gráfico No. 2: Proceso de Evaluación



2.1.2. NORMAS ISO 17799. POLITICAS DE SEGURIDAD

2.1.2.1. LOS ORÍGENES DE ISO 17799

Durante más de un siglo, el Instituto Británico de Normas Técnicas (BSI) y la Organización Internacional de Normas Técnicas (ISO) han brindado parámetros globales a las normas técnicas de operación, fabricación y desempeño. Solo faltaba que BSI e ISO propusieran una norma técnica para la seguridad de la información.

Finalmente en 1995, el BSI publicó la primera norma técnica de seguridad, BS 7799, la cual fue redactada con el fin de abarcar los asuntos de seguridad.

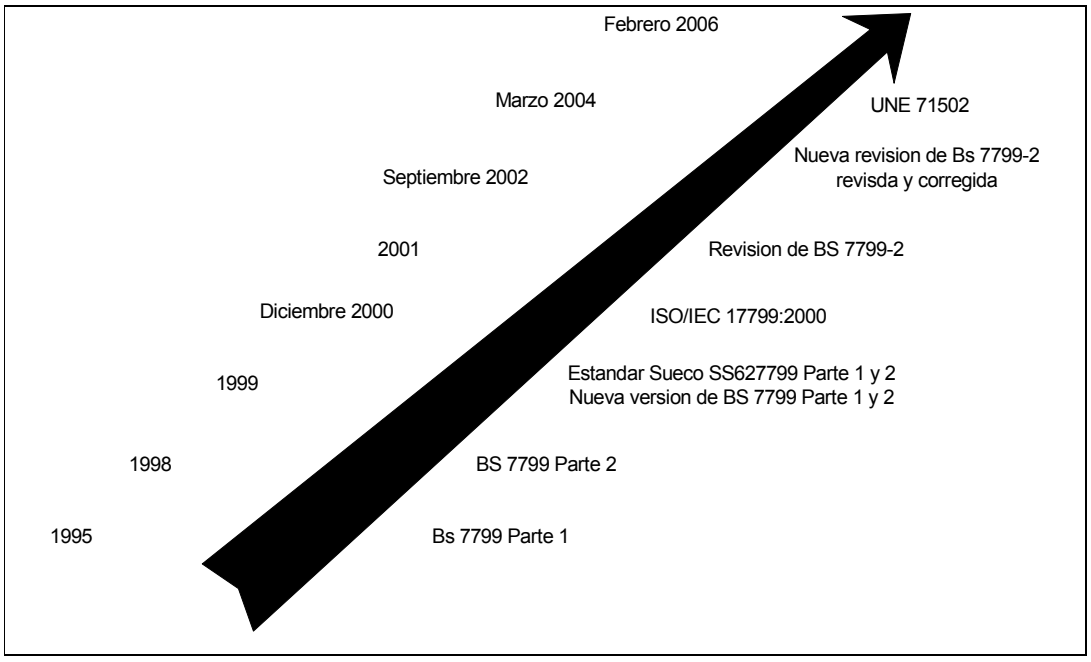
Después de 1995, problemas como el Y2K (año 2000 o efecto 2000) y la Unidad Monetaria Europea (EMU por su sigla en inglés) prevalecieron sobre otros. Para empeorar las cosas, la norma BS 7799 se consideraba inflexible y no tuvo gran acogida. No se presentó la norma técnica en un momento oportuno y los problemas de seguridad no despertaron mucho interés en ese entonces. La escasa implantación de accesos a Internet entre la población tampoco mejoraba esta situación.

Cuatro años después en mayo de 1999, el BSI intentó de nuevo publicar su segunda versión de la norma BS 7799, la que fue una revisión más amplia de la primera publicación.

Esta edición sufrió muchas mejoras y perfeccionamientos desde la versión de 1995. En este momento la ISO se percató de estos cambios y comenzó a trabajar en la revisión de la norma técnica BS 7799. En diciembre de 2000, la Organización Internacional de Normas Técnicas (ISO) adoptó y publicó la primera parte de su norma BS 7799 bajo el nombre de ISO 17799.

Alrededor de la misma época, se adoptó un medio formal de acreditación y certificación para cumplir con la norma técnica. Los problemas Y2K y EMU y otros similares se habían solucionado o reducido en 2000 y la calidad total de la norma técnica había mejorado considerablemente. La adopción por parte de ISO de los criterios de la norma técnica BS 7799 recibió gran aceptación por parte del sector internacional y fue en este momento en el que el grupo de normas técnicas de seguridad tuvo amplio reconocimiento.

Gráfico No. 3: Evolución de la Norma ISO 17799



2.1.2.2. DEFINICIÓN DE ISO 17799

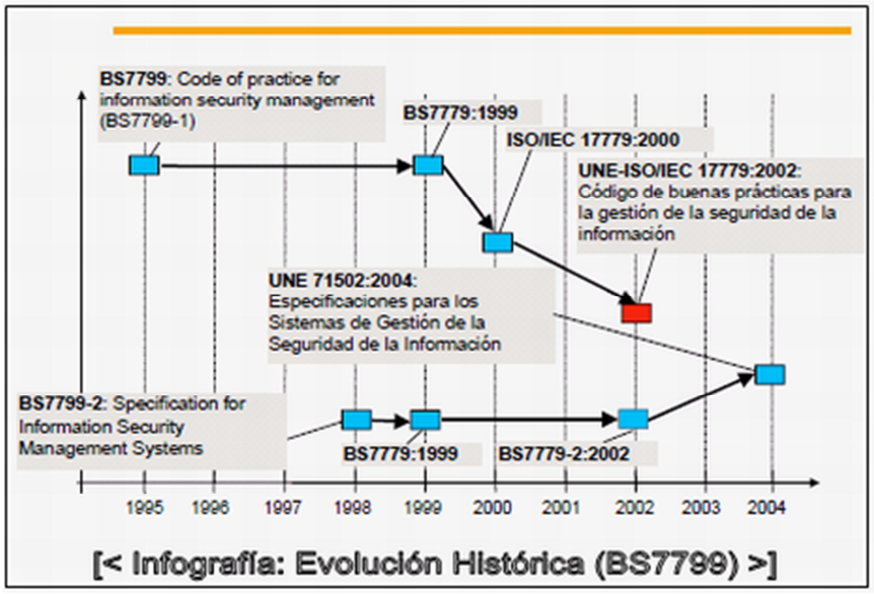
ISO 17799 al definirse como una guía protocolar (conjunto de normas a llevar a cabo) en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios:

- Confidencialidad: asegurar que, únicamente, personal autorizado tenga acceso a la información.

- Integridad: garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas; preservando exactitud y completitud de la misma y de los métodos de su procesamiento.
- Disponibilidad: cerciorar que los usuarios autorizados tendrán acceso a la información cuando la requieran y sus medios asociados.

Tales premisas en la protección de los activos de información constituyen las pautas básicas (deseables) en cualquier organización, sean instituciones de gobierno, educativas, de investigación o (meramente) pertenencias hogareñas; no obstante, dependiendo de la naturaleza y metas de las estructuras organizacionales, éstas mostrarán especial énfasis en algún dominio o área del estándar ISO 17799.

Gráfico No. 4 Evolución Histórica de la ISO



Como ha de saber, es "misión imposible" conseguir el 100% de Seguridad en cualquier aspecto de La Vida. Por lo tanto, el objetivo de la seguridad en los datos es (acéptese el juego de palabras) para asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una eventualidad, así como optimizar la inversión en tecnologías afines y prosperar en las novedosas oportunidades que nos brindará el porvenir del tiempo.

Como todo buen estándar, el ISO 17799 da la pauta en la definición sobre cuáles metodologías, políticas o criterios técnicos pueden ser aplicados en el régimen de manejo de la seguridad de la información.

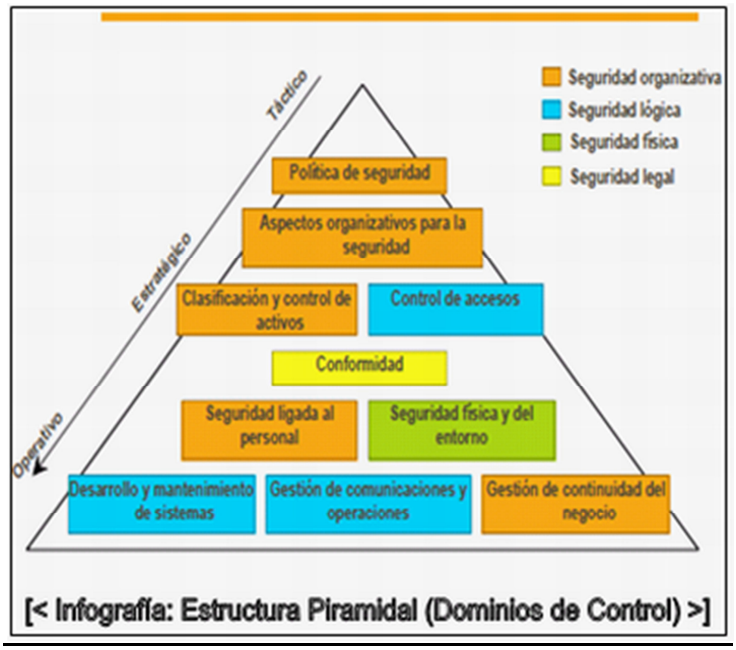
- **Confidencialidad:** Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
- **Integridad:** Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

La toma de decisiones sobre un marco de referencia de seguridad basado en ella proporciona beneficios a toda organización que lo implemente. Ya sea en su totalidad o en la parcialidad de sus postulaciones estipuladas.

2.1.2.3. ESTRUCTURA DE LA NORMA ISO 17799

Su elaboración y práctica integra mecanismos de control primordiales, que le permiten a las organizaciones demostrar que cuenta con el estado de la seguridad de la información pertinente; situación que resulta muy importante en aquellos convenios o contratos con terceros que establecen como requisito contractual la Declaración BS7799 u otras disposiciones de perfil similar que se acentúan mucho en "los tiempos que corren".

Gráfico No. 5 Estructura Piramidal



Así, la norma discute la necesidad de contar con cortafuegos, pero no profundiza sobre los tres tipos de cortafuegos y cómo se utilizan, lo que conlleva a que algunos detractores de la norma digan que ISO 17799 es muy general y que tiene una estructura muy imprecisa y sin valor real.

La flexibilidad e imprecisión de ISO 17799 es intencional por cuanto es difícil contar con una norma que funcione en una variedad de entornos de tecnología de la información y que sea capaz de desarrollarse con el cambiante mundo de la tecnología. ISO 17799 simplemente ofrece un conjunto de reglas a un sector donde no existían.

La Norma ISO/IEC 17799 establece diez dominios de control que cubren (casi) por completo la Gestión de la Seguridad de la Información:

1) Políticas de seguridad: el estándar define como obligatorias las políticas de seguridades documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.

2) Aspectos organizativos: establece el marco formal de seguridad que debe integrar una organización.

3) Clasificación y control de activos: el análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

4) Seguridad ligada al personal: contrario a lo que uno se puede imaginar, no se orienta a la seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información. Su objetivo es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, o sea, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.

5) Seguridad física y del entorno: identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

6) Gestión de comunicaciones y operaciones: integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el

control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.

7) Control de accesos: habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

8) Desarrollo y mantenimiento de sistemas: la organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.

9) Gestión de continuidad del negocio: el sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.

10) Cumplimiento o conformidad de la legislación: la organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

De estos diez dominios nombrados se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de inspecciones) y 127 o más controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo). Ambos, se encuentran destinados a dotar y esparcir Seguridad a la Información en el "ambiente digital", a través de numerosas auditorías, consultorías y/o paradigmas.

Cada una de las áreas constituye una serie de observaciones que serán seleccionadas dependiendo de las derivaciones obtenidas en los análisis de riesgos, conjuntamente, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle.

Por eso, es aplicable a toda organización, independientemente, de su tamaño o sector de negocio; siendo un argumento fuerte y dinámico para los detractores de la norma y un "conjunto de instrumentos" flexibles a cualquier solución de seguridad concreta: recomendaciones neutrales con respecto a la IT.

Pero… “Siempre hay un Pero” (así dice el lema), y es el consiguiente: como la ISO 17799 se forma de un compilado protocolar de normas y/o reglas fundadas en las Políticas de Seguridad, y éstas son erigidas y colocadas por el Ser Humano, no son inmunes a fallas o errores (infalibilidad absoluta) y con el tiempo deben ir siendo depuradas para acercarse lo más que se pueda (y un poco más) a un “monstruo desconocido”, aunque muy escuchado, que es llamado: Perfección.

Tal sentencia puede ser corroborada en el mismo alegato sobre el cual se excusan potenciales (factibles y/o aleatorios) inconvenientes de su puesta en práctica:

“No todos los alineamientos y controles de este código de práctica resultarán aplicables. Más aún, es probable que deban agregarse controles que no están incluidos en este documento. Ante esta situación puede resultar útil retener referencias cruzadas que faciliten la realización de pruebas de cumplimiento por parte de auditores y socios”

Esto da por sentado su propiedad de mutabilidad, actualización y adaptabilidad según las determinaciones organizacionales de las que dispongamos, sin embargo, presiento (y se que me acompañarán en tales laudos) que algo en ella podría innovarse y ser mejor.
Para ello tendría en cuenta las siguientes peticiones:

Interacción y transposición de procedimientos (métodos, normas, y/o reglas): que la disposición física del centro de cómputos, terminales o servidores no se contraponga con la norma IRAM que regula el recorrido físico dentro de las oficinas. Es indispensable la interacción con un profesional en Organización y Métodos, Analista o Ing. en Sistemas con vasta experiencia. Prestar mucha atención al implementar controles (para no estar debilitados o desordenados por “cosas” de otros lados).

Tendencias a las nuevas tecnologías: tener presente en el flujo de datos la permeabilidad o apropiación de los mismos a través de la tecnología VoIP (Voice over IP – Voz sobre IP), unidades de almacenamiento secundarias transportables (Pendrives, Cámaras, Celulares, Etc.) y mensajeros instantáneos (usados para el Chat).

Reclutamiento de personal (empleados): es una de las claves del éxito de una organización, el atraer e incorporar a gente apropiada para desempeñarse en la implementación de estas normas. El agente de RRHH tiene que tener vastos conocimientos técnicos, comprobar las habilidades y referencias que estén en el CV del potencial postulante.

Adaptación inteligente al medio: contar con el Software (recursos lógicos) y el Hardware (recursos físicos) convenientes para no perder la calidad de los servicios y/o bienes ofrecidos como producto.

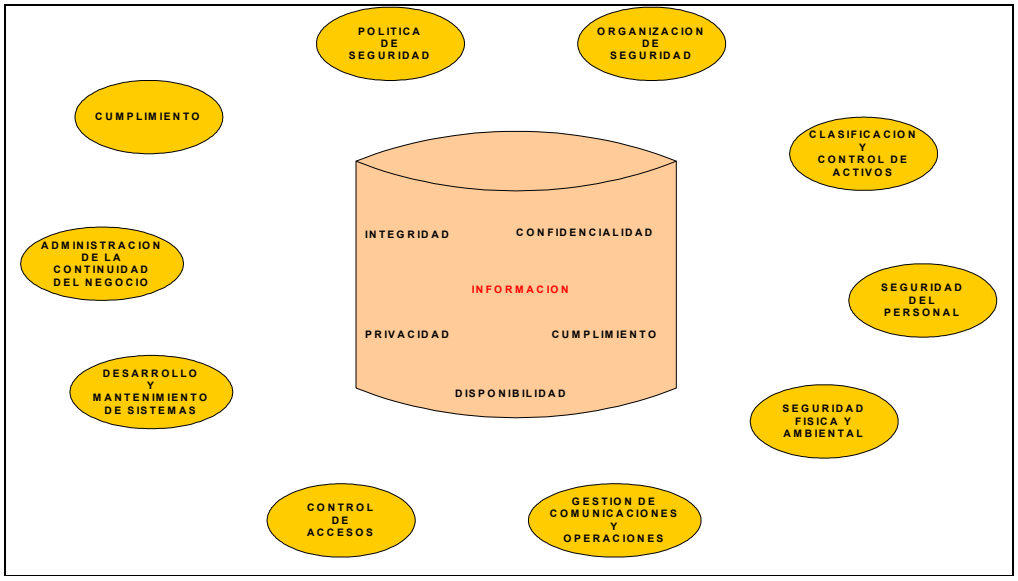
Invertir en capacitación conveniente y acertada en los trabajadores: tratar de entusiasmar e incentivar al usuario para que se faculte de mayores y mejores mañas (artilugios) al momento de operar en su cargo. De esta manera, se suprimirá (en enormes cantidades) la negligencia y las falencias a causa de ésta, teniendo secuelas de menor magnitud a la hora de resolver un problema.

Vigilancia en otros cuidados diversos a tener vigentes: monitorizaciones, seguimientos e investigación de los campos a los cuales subyace la materia u oficio contratado.

Para darnos el gusto con la "frutilla del postre o la cereza del helado (o ambas)", ha de estar al tanto que La Norma ISO/IEC 17799 no posee ningún tipo de certificación. Ya que sólo son recomendaciones y no es necesario aplicar la totalidad de sus controles, sino adaptarlos a la organización para no hacer algo tedioso e inútil, como así tampoco.

La estructura de la normatividad de gestión en seguridad de sistemas de información, norma ISO 17799, queda especificada en diez dominios, que incluyen: política de seguridad, organización de la seguridad, control y clasificación de los recursos de información, seguridad de personal, seguridad física y ambiental, manejo de las comunicaciones y las operaciones, control de acceso, desarrollo y mantenimiento de los sistemas, manejo de la continuidad de la empresa, así como el cumplimiento.

Gráfico No. 6: Estructura de la norma ISO 17799



Estos diez dominios se organizan de acuerdo al siguiente gráfico:

- **Seguridad Lógica:** Confidencialidad, integridad y disponibilidad del software y datos de un sistema de seguridad.
- **Seguridad Organizativa:** Relativa a la prevención, detección y corrección de riesgos.
- **Seguridad Física:** protección de elementos físicos de las instalaciones: servidores, Pcs, etc.
- **Seguridad Legal:** cumplimiento de la legislación vigente.

De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

2.1.2.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Su objetivo principal es dirigir y dar soporte a la gestión de la seguridad de la información. La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información.

La política se constituye en la base de todo el sistema de seguridad de la información. La alta dirección debe apoyar visiblemente la seguridad de la información en la compañía.

La política de seguridad de la información debe ser documentada para ayudar a proyectar las metas de seguridad de la información de una organización. Debe estar claramente redactada y comprensible para sus lectores. La política ayuda a la administración, con el manejo de la seguridad de la información a través de la organización.

Tabla No. 1: Política de Seguridad de la Información

Documentación de la política de seguridad de la información	• Definición de la seguridad de la información, objetivos, alcance e importancia. • Declaración del apoyo a nivel gerencial • Breve explicación de las políticas, normas y requisitos de cumplimiento • Definición de las responsabilidades generales y especificas • Referencia a documentos de respaldo o procedimientos más detallados
Revisión y Evaluación	• La política debe tener un propietario responsable de la revisión y mantenimiento • Garantizar su actualización frente a cambios que alteren la base de riesgos • Programar revisiones periódicas de: • Eficacia de la política o Costo e impacto de los controles (no debe superar lo que se protege) • Efectos de los cambios en la tecnología (impactos en la seguridad)

2.1.2.5. ORGANIZACIÓN DE LA SEGURIDAD

Gestionan la seguridad de la información dentro de la organización. Mantienen la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros. Mantienen también la seguridad de la información cuando la responsabilidad de su tratamiento se ha exteriorizado o a otra organización.

Debe diseñarse una estructura organizativa dentro de la compañía que defina las responsabilidades que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de cualquier forma. Dicha estructura debe poseer un enfoque multidisciplinar: los problemas de seguridad no son exclusivamente técnicos. Delimita cómo la alta gerencia puede dirigir la implementación de seguridad de la información dentro de una organización.

Proporciona un foro o política para revisar y aprobar las políticas de seguridad y asignar los roles de seguridad.

Tabla No. 2: Organización de la Seguridad

Infraestructura de seguridad de la información	• Foro gerencial sobre seguridad de la información • Coordinación de la seguridad de la información • Asignación de responsabilidades en materia de seguridad de la información • Proceso de autorización para instalaciones de procesamiento de información • Asesoramiento especializado en materia de seguridad de la información • Cooperación entre organizaciones • Revisión independiente de la seguridad de la información (Auditoría Externa)
Seguridad frente al acceso por parte de terceros	• Identificación de riesgos del acceso de terceras partes • Requerimientos de seguridad en contratos con terceros
Tercerización	• Requerimientos de seguridad en contratos de Tercerización

2.1.2.6. CLASIFICACIÓN Y CONTROL DE ACTIVOS (CLASIFICACIÓN DE HARDWARE Y SOFTWARE)

Mantener una protección adecuada sobre los activos de la organización. Asegurar un nivel de protección adecuado a los activos de información. Debe definirse una **clasificación** de los activos relacionados con los sistemas de información, manteniendo un **inventario** actualizado que registre estos datos, y proporcionando a cada activo el nivel de **protección** adecuado a su criticidad en la organización, administrar los activos físicos e intelectuales que son importantes para mantener las protecciones apropiadas, determinar la responsabilidad de quien es dueño y de que activo de la organización.

Tabla No. 3: Clasificación y control de activos

Responsabilidad por rendición de cuentas de los activos	• Inventario de activos (medios removibles, clasificación de los activos, clasificación de la información)
Clasificación de la Información	• Pautas de clasificación • Rotulado y manejo de la información

2.1.2.7. SEGURIDAD DEL PERSONAL

Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios. Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo. Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos. Las implicaciones del **factor humano** en la seguridad de la información son muy elevadas. Todo el personal, tanto **interno** como **externo** a la organización, debe conocer tanto las líneas generales de la política de seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la seguridad global.

Debe haber diferentes relaciones con los sistemas de información: operador, administrador, guardia de seguridad, personal de servicios, etc., y procesos de **notificación de incidencias** claros, ágiles y conocidos por todos.

La evaluación y asignación de las responsabilidades de seguridad de los empleados permite una administración de recursos humanos más efectiva (recurso humano de tecnología). Las responsabilidades de la seguridad deben ser determinadas durante el reclutamiento de todo el personal y durante toda la propiedad del empleado en la compañía.

Tabla No. 4: Seguridad del personal

Seguridad de la definición de puestos de trabajo y la asignación de recursos	• Inclusión de la seguridad en las responsabilidades de los puestos de trabajo • Selección y política de seguridad • Acuerdos de confidencialidad • Términos y condiciones de empleo
Capacitación del usuario	• Formación y capacitación en materia de seguridad de la información, incluir un sistema de capacitación cuando suceda un cambio. Los usuarios externos también deben estar capacitados (transacciones en línea)
Respuesta a incidentes y anomalías en materia de seguridad	• Comunicación de incidentes relativos a la seguridad • Comunicación de debilidades en materia de seguridad • Comunicación de anomalías del software • Aprender de los incidentes • Proceso disciplinario

2.1.2.8. SEGURIDAD FÍSICA Y AMBIENTAL

Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización. Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización. Prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información. Las áreas de trabajo de la organización y sus activos deben ser clasificadas y **protegidas** en función de su criticidad, siempre de una **forma adecuada** y frente a cualquier **riesgo factible** de índole física (robo, inundación, incendio...)

Asegurar las áreas físicas y los ambientes de trabajo dentro de la organización contribuyente, significativamente a la administración de seguridad de la información. Cualquier persona que se relaciona con su establecimiento físico, así sean los empleados, proveedores o clientes tienen un papel enorme en determinar la protección de seguridad organizacional.

Tabla No. 5: Seguridad física y ambiental

Áreas seguras	• Perímetro de seguridad física • Controles de acceso físico • Protección de oficinas, recintos e instalaciones • Desarrollo de tareas en áreas protegidas • Aislamiento de las áreas de entrega y carga
Seguridad del Equipamiento	• Ubicación y protección del equipamiento • Suministros de energía • Seguridad del cableado • Mantenimiento de equipos • Seguridad del equipamiento fuera del ámbito de la organización • Baja segura o reutilización de equipamiento (destrucción física de equipos)
Controles generales	• Políticas de escritorios y pantallas limpias • Retiro de bienes (llevar controles cuando alguien retira un bien)

2.1.2.9. GESTIÓN DE COMUNICACIÓN Y OPERACIONES

Asegurar la operación correcta y segura de los recursos de tratamiento de información. Minimizar el riesgo de fallos en los sistemas. Proteger la integridad del software y de la información. Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación. Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo. Evitar daños a los activos e interrupciones de actividades de la organización.

Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones. Se debe garantizar la seguridad de las **comunicaciones** y de la **operación** de los sistemas críticos para el negocio. Transmitir claramente las instrucciones de seguridad a los empleados ayuda a administrar las operaciones diarias de los recursos de procesamiento de información.

Tabla No. 6: Gestión de Comunicación y operaciones

Procedimientos y Responsabilidades	• Documentación de los procedimientos operativos • Control de cambios en las operaciones • Procedimientos de manejo de incidentes • Separación de funciones • Separación entre instalaciones de desarrollo e instalaciones operativas • Administración de instalaciones externas
Planificación y aprobación de sistemas (decidir si la aplicación cumple con los requisitos para pasar a producción**)**	• Planificación de la capacidad • Aprobación del sistema
Protección contra software malicioso	• Controles sobre software malicioso (virus, gusanos, spyware, spam)
Mantenimiento	• Respaldo de la información • Registro de actividades del personal operativo • Registro de fallas
Administración de la red	• Controles de redes (no hay problema en redes LAN ,WAN, protección y seguridad es del proveedor de comunicación)
Administración y seguridad de los medios de almacenamiento	• Administración de medios informáticos removibles • Eliminación de medios informáticos • Procedimientos de manejo de la información • Seguridad de la documentación del sistema
Intercambios de información y software	• Acuerdos de intercambio de información y software • Seguridad de los medios de tránsito • Seguridad del comercio electrónico • Seguridad del correo electrónico • Seguridad de los sistemas electrónicos de oficina • Sistemas de acceso público • Otras formas de intercambio de información

2.1.2.10. CONTROL DE ACCESOS

Controlar los accesos a la información, evitar accesos no autorizados a los sistemas de información, evitar el acceso de usuarios no autorizados, proteger los servicios en red. Evitar accesos no autorizados a ordenadores, el acceso no autorizado a la información contenida en los sistemas. Detectar actividades no autorizadas. Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y tele-trabajo.

Se deben establecer los **controles de acceso adecuados** para proteger los sistemas de información críticos para el negocio, a diferentes niveles: sistema operativo, aplicaciones, redes, etc. Administrar los niveles de acceso de todos los empleados ayuda a controlar la seguridad de la información en una organización. Controlar niveles de acceso a la red puede llegar a ser un factor crítico de éxito cuando se protegen los sistemas de documentación o información en la red.

Tabla No. 7: Control de accesos

Requerimientos de negocio para el control de accesos	• Requerimientos políticos y de negocio • Reglas de control de accesos
Administración de accesos de usuarios	• Registro de usuarios • Administración de privilegios • Administración de contraseñas de usuario • Revisión de derechos de derechos de acceso de usuario
Responsabilidades del usuario	• Uso de contraseñas • Equipos desatendidos en áreas de usuarios
Control de acceso a la red	• Política de utilización de los servicios de red • Camino forzado (no permitir a los usuarios que manipulen las líneas de comando) • Autentificación de usuarios para conexiones externas • Autentificación de nodos • Protección de los puertos (ports) de diagnóstico remoto • Subdivisión de redes • Control de conexión a la red • Control de ruteo de red • Seguridad de los servicios de red

Control de acceso al sistema operativo	• Identificación automática de terminales • Procedimientos de conexión de terminales • Identificación y autentificación de los usuarios • Sistemas de administración de contraseñas • Uso de utilitarios del sistema • Alarmas silenciosas para la protección de los usuarios • Desconexión de terminales por tiempo muerto (cortar la sesión si la estación esta inactiva por algún tiempo) • Limitación del tiempo de conexión
Control de acceso a las aplicaciones	• Restricción del acceso a la información • Aislamiento de sistemas sensibles
Monitoreo del acceso y uso de los sistemas	• Registro de eventos • Monitoreo del uso de los sistemas • Sincronización de relojes
Computación móvil y trabajo remoto	• Computación Móvil (usuarios externos) • Trabajo remoto (conexiones con otras redes por medio del proveedor de comunicación)

2.1.2.11. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones. Proteger la confidencialidad, autenticidad e integridad de la información. Asegurar que los proyectos de Tecnología de la Información y las actividades complementarias son llevadas a cabo de una forma segura.

Mantener la seguridad del software y la información de la aplicación del sistema. Debe contemplarse la seguridad de la información en todas las etapas del ciclo de vida del software en una organización: especificación de requisitos, desarrollo, explotación, mantenimiento.

La administración de la seguridad es imperativa en el desarrollo, mantenimiento y operación exitosa de un sistema de información, es obligatoria, exigente y una necesidad.

Tabla No. 8: Desarrollo y mantenimiento de sistemas

Requerimientos de seguridad de los sistemas	• Análisis y especificaciones de los requerimientos de seguridad • Las normas deben especificar los procedimientos de control
Seguridad en los sistemas de aplicación	• Validación de los datos de entrada • Controles de procesamiento interno, áreas de riesgo, controles y verificaciones (para detectar corrupción) • Autentificación de mensajes • Validación de los datos de salida
Controles criptográficos	• Política de utilización de controles criptográficos (definir cuando y en base a que) • Cifrado • Firmas digitales • Servicios de no repudio • Administración de Claves protección de claves criptográficas, normas, procedimientos y métodos
Seguridad de los archivos del sistema	• Control del software operativo • Protección de los datos de prueba del sistema • Control de acceso a las bibliotecas de programa fuente (ninguna persona del área de tecnología tiene acceso a el área de producción)
Seguridad de los procesos de desarrollo y soporte	• Procedimientos de control de cambios • Revisión técnica de los cambios en el sistema operativo • Restricción del cambio en los paquetes de software • Canales ocultos y código troyano (adquirir aplicaciones solo a proveedores acreditados) • Desarrollo externo de software

2.1.2.12. ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente grandes fallos o desastres. Todas las situaciones que puedan provocar la **interrupción** de las actividades del negocio deben ser **prevenidas** y **contrarrestadas** mediante los planes de

contingencia adecuados. Los **planes de contingencia** deben ser probados y revisados periódicamente. Se deben definir **equipos de recuperación** ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre.

Aspectos de la administración de la continuidad del negocio:

- Proceso de administración de la continuidad de los negocios: plan de recuperación de desastres del área tecnológica y productiva
- Continuidad del negocio y análisis del impacto, orientado al negocio
- Elaboración e implementación de planes de continuidad de los negocios
- Marco para la planificación de la continuidad de los negocios
- Prueba, mantenimiento y reevaluación de los planes de continuidad de los negocios.

2.1.2.13. CUMPLIMIENTO

Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad. Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma. Maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas.

El uso de asesores legales se está volviendo más importante para asegurar la observancia de una organización con las obligaciones contractuales, leyes y requisitos con las obligaciones contractuales, leyes y requisitos de seguridad.

Tabla No. 9: Cumplimiento

Cumplimiento de requisitos legales	• Identificación de la legislación aplicable • Derechos de propiedad intelectual (*DPI*) • Protección de los registros de la organización • Protección de datos y privacidad de la información personal • Prevención del uso inadecuado de los recursos de procesamiento de información • Regulación de controles para el uso de criptografía • Recolección de evidencia

Revisión de la política de seguridad y la compatibilidad técnica	• Cumplimiento de la política de seguridad • Verificación de la compatibilidad técnica
Consideraciones de auditoría de sistemas	• Controles de auditoría de sistemas • Protección de las herramientas de auditoría de sistemas

2.1.2.14. APLICACIÓN DE LA NORMA ISO 17799

a) AUDITORÍA

Un trabajo de auditoría ISO 17799 consiste en la valoración del nivel de adecuación, implantación y gestión de cada control de la norma en la organización. Valora la seguridad desde 4 puntos de vista:

- Seguridad lógica.
- Seguridad física.
- Seguridad organizativa.
- Seguridad legal.

Se trata de una referencia de la seguridad de la información estándar y aceptada internacionalmente. Una vez conocemos el estado actual de la seguridad de la información en la organización, podemos planificar correctamente su mejora o su mantenimiento. Una auditoría ISO 17799 proporciona información precisa acerca del nivel de cumplimiento de la norma a diferentes niveles: global, por dominios, por objetivos y por controles.

b) CONSULTORÍA

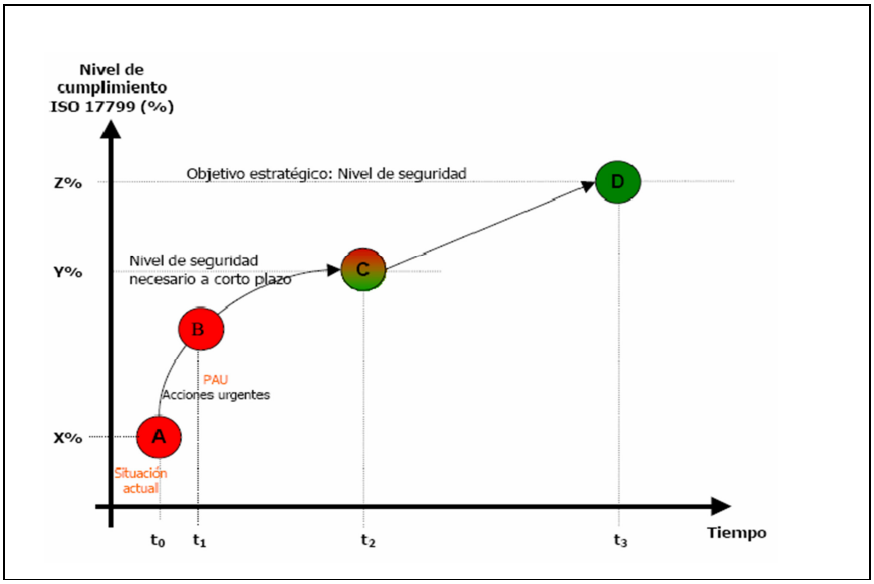
Conociendo el nivel de cumplimiento actual, es posible determinar el nivel mínimo aceptable y el nivel objetivo en la organización:

- **Nivel mínimo aceptable.** Estado con las mínimas garantías de seguridad necesarias para trabajar con la información corporativa.
- **Nivel objetivo.** Estado de seguridad de referencia para la organización, con un alto grado de cumplimiento ISO 17799.

A partir del nivel mínimo aceptable y el nivel objetivo, podemos definir un plan de trabajo para alcanzar ambos a partir del estado actual.

- Nivel **mínimo aceptable**. Implantación de los controles **técnicos** más **urgentes**, a muy **corto plazo**.
- Nivel **objetivo**. Se desarrolla en el tiempo dentro del **Plan Director de Seguridad** corporativo, y es el paso previo a la **certificación UNE 71502**.

Gráfico No. 7: Ejemplo de consultaría en base al cumplimiento y el tiempo



c) IMPLANTACIÓN

ISO 17799 no es una norma tecnológica. Ha sido redactada de forma flexible e independiente de cualquier solución de seguridad específica.

Proporciona buenas prácticas neutrales con respecto a la tecnología y a las soluciones disponibles en el mercado.

Estas características posibilitan su implantación en todo tipo de organizaciones, sin importar su tamaño o sector de negocio, pero al mismo tiempo son un argumento para los detractores de la norma. ¿Cómo traducir especificaciones de alto nivel a soluciones concretas, para poder implantar ISO 17799? Con un trabajo de consultoría, interna o externa.

✓ FASE PREVIA

- Elaboración de un estudio con los justificativos de la función de seguridad de la información

- Presentar el estudio a la Dirección, Gerencia, o Comité
- Obtener la aprobación para la creación de la función de seguridad de la información

✓ **FASE PRELIMINAR**

- Seleccionar y entrenar a los miembros del equipo
- Conducir el análisis de riesgos
  - Identificación
  - Valoración
  - Clasificación
  - Exposición
- Identificar todos los posibles perpetradores
- Elaborar un esquema de administración del riesgo
- Conducir un diagnóstico de la situación actual en seguridad de la información frente a las especificaciones de la norma ISO 17799
- Definir los objetivos y responsabilidades de la unidad de seguridad de la información
- Elaborar el plan de trabajo para 1 año como mínimo, esperado 2 años, ideal 3 años
- Identificar – definir roles y responsabilidades de involucrados
  - Auspiciantes
  - Autorizadores (nivel gerencial)
  - Usuarios
  - IT (Tecnología de la Información)
  - Auditores
  - Terceros

✓ **FASE DE ASENTAMIENTO**

- Elaborar, aprobar y difundir la Política General de Seguridad de la Información
- Asegurar el compromiso y apoyo de la alta gerencia (apoyo económico)

✓ **FASE DE DESARROLLO**

- Definir el manual de seguridad de la información

- Desarrollar esquema de propietarios de datos, perfiles, aplicaciones y transacciones
- Levantar inventario de recursos de información
- Conducir el proceso de clasificación de la información
- Definir el programa de difusión y concienciación del personal interno y externo
- Redactar las políticas y procedimientos de seguridad crítico
- Elaborar en paralelo el plan de continuidad del negocio

✓ **FASE DE IMPLANTACIÓNÓN**

- Implantar el esquema de propietarios de datos, perfiles y transacciones
- Aprobar, difundir e implantar las políticas y procedimientos de seguridad críticos
- Implantar las normas de clasificación de la información
- Seleccionar e implantar controles para reducir riesgos
- Definir con Recursos Humanos un esquema de premios y castigos
- Conducir procesos de entrenamiento y concienciación a usuarios internos y externos

✓ **FASE DE EVALUACIÓNÓN**

- Conducir un nuevo estudio de diagnóstico de seguridad de la información con relación a la norma de seguridad de la información ISO 17799.
- Incorporar las mejoras necesarias para conformarse a la norma.

2.1.2.15. VENTAJAS

La adopción de la norma ISO 17799 proporciona diferentes ventajas a cualquier organización:

- Aumento de la **seguridad efectiva** de los sistemas de información.
- Correcta **planificación** y gestión de la seguridad.
- Garantías de **continuidad del negocio**.
- Alianzas comerciales y e-commerce más seguras.
- **Mejora continua** a través del proceso de auditoría interna.
- Incremento de los niveles de **confianza** de nuestros clientes y *partners*.
- Aumento del **valor comercial** y mejora de la **imagen** de la organización.
- Auditorias de seguridad más **precisas** y **fiables.**
- **Mejora continua** a través del proceso de auditoría interna.

- Incremento de los niveles de **confianza** de nuestros clientes y *partners*.
- Aumento del **valor comercial** y mejora de la **imagen** de la organización.
- Auditorias de seguridad más **precisas** y **fiables.**
- Menor **Responsabilidad Civil**.

2.1.3. NORMAS ISO 20000. GESTIÓN DE SERVICIOS DE LA TIC (Tecnología de la Información y Comunicación)

2.1.3.1. ORIGEN

La norma ISO 20000 fue creada por la International Organization for Standardization (ISO) y es la norma utilizada para la certificación. Ha reemplazado a la norma BS 15000 y proporciona una norma internacionalmente reconocida de sistema de gestión de servicios de TI. La ISO 20000 utiliza un enfoque exhaustivo de la gestión de servicios de TI y define un conjunto de procesos necesarios para ofrecer un servicio efectivo. Recoge desde procesos básicos relacionados con la gestión de la configuración y la gestión del cambio hasta procesos que recogen la gestión de incidentes y problemas. La norma adopta un enfoque de proceso para el establecimiento, la implementación, operación, monitorización, revisión, mantenimiento, y mejora del sistema de gestión de servicios de TI.[3]

2.1.3.2. DEFINICIÓN

La norma ISO 20000 es una norma internacional para la Gestión de Servicios TI, la cual se concentra en la gestión de problemas de tecnología de la información mediante el uso de un planteamiento de servicio de asistencia. Esta norma describe un conjunto integrado de procesos y un enfoque de gestión para la provisión efectiva de servicios de TI a clientes internos y externos, promoviendo una cultura de mejora interna.[4]

[3] http://www.dnvba.com/es/Certificacion/Sistemas-de-Gestion/Seguridad-de-la-Informacion/Pages/ISO-20000%E2%80%93Certificacion-del-Sistema-de-Gestion-de-Servicios-de-TI-Tecnologias-de-la-Informacion.aspx

[4] Definición http://es.slideshare.net/hperez-ti/iso-20000-18944295

2.1.3.3. OBJETIVO

Mantener y mejorar la calidad de la gestión de servicios de la organización TI, y este aspecto se convierte en uno de los ejes fundamentales tanto para la realización de las auditorias de seguimiento anual, como en las de renovación del certificado, que se realiza cada 3 años.

2.1.3.4. ESTRUCTURA DE LA NORMA ISO 20000

La norma ISO/IEC 20000 está formada por partes publicadas bajo el mismo título "Tecnología de la información. Gestión del servicio":

- **Parte 1: Especificaciones**

  La norma ISO 20000-1 es la especificación formal y define los requisitos que tiene que cumplir una organización para proporcionar servicios gestionados de una calidad aceptable a los clientes. Su alcance incluye:

  - Requisitos para un sistema de gestión
  - Planificación e implantación de la gestión del servicio
  - Planificación e implantación de servicios nuevos o modificados
  - Proceso de provisión del servicio
  - Procesos de relación
  - Procesos de resolución
  - Procesos de control
  - Procesos de entrega
  - Relación completa de procesos de la norma ISO 20000

- **Parte 2: Código de buenas prácticas**

  Código de procedimiento y describe los mejores procedimientos para procesos de gestión de servicios dentro del ámbito de la norma ISO 20000-1. El Código de procedimiento resulta especialmente útil para organizaciones que se preparan para someterse a una auditoría según la norma ISO 20000-1 o para planificar mejoras del servicio.

- **Parte 3: Guía sobre la definición del alcance y la aplicabilidad de la norma ISO / IEC 20000-1**

  ISO/IEC TR 20000-3:2009 proporciona orientación sobre la definición del alcance, la aplicabilidad y la demostración de la conformidad de los proveedores de servicios orientados a satisfacer los requisitos de la norma ISO / IEC 20000-1, así como los proveedores de servicios que están planeando mejoras en el servicio con la intención de utilizar la norma ISO/IEC 20000 como un objetivo de negocio.

  También puede ayudar a los proveedores de servicios que están considerando utilizar la norma ISO/IEC 20000-1 para la aplicación de un sistema de gestión de servicios (SMS) y que necesitan asesoramiento específico sobre si la norma ISO/IEC 20000-1 se aplica a sus circunstancias y la forma de definir el alcance de su SMS.

  La norma ISO/IEC 20000 se encuentra actualmente bajo un proceso de revisión para alinearse mejor con ITSM y con otros estándares ISO. Es por esto, por lo que tras la reciente publicación de la norma ISO/IEC 20000-3, se están desarrollando dos nuevas partes:

- **Parte 4: Modelo de Procesos de Referencia (PRM) de gestión de servicios**

  Este modelo establece las bases del modelo de madurez y el marco de evaluación.

- **Parte 5: Ejemplar del Plan de Implementación para la norma ISO/IEC 20000-1**

  Especifica los requerisitos para el proveedor de servicios para planificar, establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SMS. Los requisitos incluyen el diseño, la transición, la entrega y la mejora de los servicios para cumplir con los requisitos de servicio acordados.

Gráfico No. 8: Esquema de Procesos de Control

Fuente de Información: http://www.normas-iso.com/iso-20000

2.1.3.5. IMPLANTAR LA NORMA ISO 20000

La norma ISO 20000 no es un proyecto que se instala y se consigue el objetivo deseado, realmente la norma ISO 20000 se centra en una gestión de los servicios orientada al negocio y basada en una estrategia de mejora continua, por lo que su adopción es más un cambio cultural y de las formas de trabajar que un proyecto con un inicio y un fin.

Si la organización decide adoptar como referencia la norma ISO 20000, podrá beneficiarse para conseguir de forma clara y guiada una gestión del servicio de alta calidad, independientemente de que finalmente decidan no solicitar formalmente la certificación. Los principales pasos para realizar una exitosa adopción de la norma ISO 20000 se centran en conocer la documentación, analizar la situación actual, planear la mejora del servicio y realizar un seguimiento y mejora continua.

2.1.3.6. PASOS PARA IMPLANTAR LA NORMA ISO 20000

1.- ANALISIS

Evaluar la situación actual de la gestión de los servicios TI con el fin de identificar los puntos fuertes y débiles de la organización y ayudar a determinar las áreas de mejora y alcance de aplicación de la norma, así como el estado de la cultura de servicios TI en la organización. Esto junto con el punto 2 debe prepararnos para establecer la estrategia y política en la que nos basaremos para implementar la norma en la empresa.

2.- FORMACIÓN Y SENSIBILIZACIÓN

Debemos realizar una acción de conocimiento y comprensión de la norma ISO 20000 (ISO 20000-1 e ISO 20000-2) para los miembros de la empresa relacionados con los servicios TI.

3.- PLANIFICACIÓN DE LAS MEJORAS

Después de evaluar aquellos puntos fuertes y débiles de nuestra organización podremos diseñar y desarrollar un plan de mejora para implantar de forma eficiente la estrategia establecida.

4.- SEGUIMIENTO DE LAS MEJORAS

El proceso de implantación de la Norma ISO-20000 es un proceso dinámico en el que se debe adoptar un proceso iterativo de mejora continua. Esto significa que el análisis de la situación, no debe incluir todas aquellas posibles mejoras que necesita nuestro sistema, sino que instaurado un sistema de mejoras incrementales, establecemos un plan que define cuales son las acciones a llevar a cabo que son más necesarias y posibles de implementar, y así en sucesivas revisiones podremos ir incorporando sucesivas mejoras e ir midiendo la eficacia de las medidas adoptadas para establecer medidas tanto correctivas como preventivas.

La organización debe implantar las áreas de mejora identificadas en al análisis de la situación inicial de forma incremental, midiendo sus progresos respecto a la norma, y utilizando para lograrlo, los elementos de referencia del mercado más adecuados: ITIL, COBIT, las buenas prácticas ya utilizadas en la organización, etc.

2.1.3.7. CERTIFICACIÓN DE LA NORMA ISO 20000

La certificación según los requisitos de una norma es el resultado satisfactorio de una evaluación realizada por una tercera parte independiente. Es la prueba para los clientes de que se satisfacen las exigencias de ciertas normas nacionales o internacionales, se trate de la certificación de un sistema de gestión, de un producto o de un proyecto. El proceso de certificación difiere según se trate de la certificación de sistemas de gestión o de productos.[5]

La certificación no debería ser un fin en sí misma, sino más bien un medio que permita al proveedor de servicios TI gestionar sus servicios mediante procesos de acuerdo a la norma ISO

[5] http://www.dnvba.com/es/Certificacion/Pages/El-camino-hacia-la-certificacion.aspx

20000, acreditando la calidad en la prestación de sus servicios, alineada con el negocio y aplicando criterios de eficiencia. A continuación se detalla el proceso que se llevan a cabo para la certificación en la norma ISO 20000:

Una vez que el proveedor de servicios TI ha implementado la gestión del servicio TI (SGSTI) según la norma y ha decidido certificar la conformidad de este sistema de gestión con la norma ISO/IEC 20000-1:2005, y por lo tanto su forma de diaria trabajo, es necesario cubrir una serie de actividades. Para iniciar este proceso se necesitan dos actores: el solicitante (empresa u organización que aspira a conseguir la certificación conforme a la norma ISO 20000) y la entidad de certificación (empresa u organización que tras el proceso de auditoría y evaluación respecto a la norma, concede o deniega la certificación).

Estos dos actores deben cubrir una serie de actividades, que a continuación se plasman, en donde la primera etapa es la certificación inicial y, a partir de este punto, no finaliza nunca.

2.1.3.8. PASOS PARA LA CERTIFICACIÓN

A continuación encontrará 10 pasos generales que conducen a la certificación:[6]

1. Conseguir la norma

Conseguir la norma y leerla para familiarizarse con los requisitos. Determinar después si tiene sentido que la empresa obtenga la certificación bajo esta norma.

2. Revisar la bibliografía

Existe gran cantidad de información publicada que ayuda a entender la norma y a saber cómo implantarla correctamente.

3. Formar un equipo y definir su estrategia

La adopción de un sistema de gestión debe ser una decisión estratégica que implique a toda la organización. Es esencial que la Dirección de la empresa esté involucrada en el proceso de certificación ya que en sus manos está el decidir la estrategia de negocio que un sistema de gestión

[6] http://www.dnvba.com/es/Certificacion/Pages/El-camino-hacia-la-certificacion.aspx

eficiente deberá sostener. Además usted necesitará de un equipo dedicado a desarrollar e implantar el sistema de gestión.

4. Determinar las necesidades de formación

Los miembros del equipo responsable de implantar y mantener el sistema de gestión deben conocer todos los detalles de la norma aplicable. Existe una amplia gama de cursos, talleres y seminarios destinados a satisfacer esas necesidades. DNV GL ofrece numerosos cursos de formación en todo el mundo. Contacte con su oficina local de DNV GL Business Assurance para más información.

5. Valorar la colaboración de un consultor

Los consultores independientes pueden ayudar a definir una estrategia de implantación que sea factible, realista y económica.

6. Elaborar un manual del sistema de gestión

Un manual del sistema de gestión debe describir las políticas y las operaciones de la empresa. A través del manual, se ofrecerá una descripción exacta de la organización y la mejor práctica adoptada para satisfacer las expectativas de los clientes de forma consecuente.

7. Elaborar procedimientos

Los procedimientos describen los procesos de la organización y la práctica apropiada para lograr el éxito en el objetivo de estos procesos. Los procedimientos deben responder a las siguientes preguntas sobre cada uno de los procesos:

- por qué
- quién
- cuándo
- dónde
- qué
- cómo

8. Implantar el sistema de gestión

La comunicación y la formación son dos factores clave para una correcta implantación de la norma. Durante la fase de implantación, la empresa estará trabajando según los procedimientos desarrollados para documentar y demostrar la eficacia del sistema de gestión.

9. Considerar la posibilidad de una preauditoría

Existe la posibilidad de optar por una evaluación preliminar de la implementación del sistema de gestión por parte de un organismo de certificación. Su propósito es detectar áreas de no-conformidad y permitir corregir esas áreas antes de comenzar el proceso de certificación. Decir que un área presenta una no-conformidad, significa que cierta parte del sistema de gestión no cumple con los requisitos de la norma.

10. Seleccione la entidad de certificación

El vínculo con la entidad de certificación se mantendrá durante años en tanto que la certificación requiere de un mantenimiento periódico. Para contar con un sistema de gestión eficiente es esencial contemplar un modelo de mejora contínua. DNV GL le ayudará a extraer el máximo valor de su proceso de certificación, evaluando para ello los puntos fuertes y las oportunidades de mejora. Esto significa para la Dirección un mayor conocimiento sobre la capacidad que tiene la organización para lograr sus objetivos estratégicos. En estos tiempos competitivos, es imprescindible escoger una entidad de certificación con una reputación intachable.

2.1.3.9. VENTAJAS

ISO / IEC 20000:2011 mejora la entrega de sus productos y servicios mediante la mejora de la fiabilidad y la calidad de los servicios de TI. ISO 20000 ayuda también a mejorar la planificación, gestión, prestación y la mejora continua de los servicios de TI y alinea las TI con las necesidades de su negocio y necesidades de los clientes.

ISO / IEC 20000, le permite alcanzar una serie de objetivos de los que se informará a lo largo de la jornada que BSI organiza el 15 de febrero. De este modo sabrá cómo ISO 20000:

- ✓ Proporciona una base para acordar niveles de servicio y la capacidad de medir la gestión del servicio.

- ✓ Demuestra que se tienen los controles adecuados y procedimientos para entregar, de forma constante servicios de TI a un coste efectivo.
- ✓ Permite que su sistema de TI esté más impulsado por un enfoque de negocio más que por la tecnología.
- ✓ Ofrece la posibilidad de seleccionar y gestionar los proveedores de servicios externos con mayor eficacia.
- ✓ Ofrece la certificación como elemento diferenciador y la posibilidad de ganar nuevos negocios.
- ✓ Está alineada con con ITIL (IT Infrastructure Library), versión 3.

2.1.4. NORMA ISO 27001. NORMA AUDITABLE: REQUISITOS PARA UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

2.1.4.1. NORMA ISO 27001

El proyecto nace con la aprobación de un artículo en el New Work Item (NWI) el 19 de mayo 2009.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Tabla No. 10: Diferencias ISO 27001-2005 y la ISO 27001-2013

1.Introducción	**1.Introducción**
2. Objeto	2. Objeto
3.Referencias Normativas	3.Referencias Normativas
4. Sistema de Gestión de la Seguridad de la Información **4.1.General** **4.2.SGSI** **4.2.1.Establecer** **4.2.2.Implementar y operar** **4.2.3.Monitorear y Revisar** **4.2.4.Mantener y Mejorar** **4.3.Documentar**	4.Contesto de la Organización 5.Liderazgo 6.Planificación
5.Responsabilidad de la Dirección	7.Soporte
6.Auditoría Interna	8.Operación
7.Revisión de la Dirección	9.Evaluación del desempeño
8.Mejora	10.Mejora

ELABORACIÓN: Autor

2.1.4.2. Documentación

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.

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.

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.

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.

• **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.

Control de la documentación Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

2.1.4.3. IMPLANTAR NORMA ISO 27001

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.[7]

- **Plan (planificar):** establecer el SGSI.
- **Do (hacer):** implementar y utilizar el SGSI.
- **Check (verificar):** monitorizar y revisar el SGSI.
- **Act (actuar):** mantener y mejorar el SGSI.

Plan*:* Establecer el SGSI

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una política de seguridad
- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).
- Identificar los riesgos
- Analizar y evaluar los riesgos
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos
- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.
- Definir una declaración de aplicabilidad.

Do*:* Implementar y utilizar el SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

[7] Sistema de Gestión de Seguridad de la Información (SGSI), www.ISO27000.es, 2007

- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Check*:* Monitorizar y revisar el SGSI

La organización deberá:

• Ejecutar procedimientos de monitorización y revisión para:

- Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
- Identificar brechas e incidentes de seguridad;
- Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
- Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
- Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior, requerimientos legales, obligaciones contractuales, etc.

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.

- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Act*:* Mantener y mejorar el SGSI

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases.

2.1.4.4. IMPORTANCIA DE LA NORMA ISO 27001

Cuando la información posee una importancia fundamental para el funcionamiento e incluso se vuelve vital para una organización. Disponer de la certificación ISO 27001 le ayudara a gestionar y a proteger su información.

La norma ISO 27001 es la única norma internacional auditable que define los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales. Esta norma ayuda a proteger los activos de información y otorga confianza a los clientes, proveedores y socios de negocios; la misma se adopta en un enfoque por procesos para establecer, realizar, revisar y mejorar un SGSI.

> *"La piedra angular del Sistema de Gestión ISO 27001 es el análisis y gestión de los riesgos basado en los procesos de negocio y servicios de TI"* (FERNÁNDEZ, 2012)

ISO 27001 se adecua a cualquier tipo de empresa (no importa su tamaño, ni a que funciones se dedica, ni en que parte del mundo se encuentre) si su objetivo es proteger su información más crítica. Esta norma es muy eficaz para empresas que gestionan o manipulan la información de otros, por ejemplo, empresas de subcontratación de TI. Puede utilizarse para garantizar a los clientes que su información está protegida.

Dichas empresas al certificarse en la norma ISO 27001 obtienen las siguientes ventajas:

- Proporciona una ventaja competitiva al demostrar a los clientes que la seguridad de su información es primordial.
- Garantiza el cumplimiento y el respeto de las leyes y normativas que se aplican en el país de origen.
- Demuestra la garantía de independencia de los controles internos y cumplimiento de los requisitos del negocio y la continuidad de las actividades del mismo.
- Garantiza la identificación, evaluación, administración y control de los riesgos de la organización.
- Demuestra el compromiso que adopta la alta dirección de la empresa con la seguridad de la información.
- Las evaluaciones periódicas supervisan el continuo rendimiento y mejoras en la seguridad de la información.

Hasta la fecha existen unas 7,279 empresas certificadas en la norma ISO 27001 a nivel mundial, a continuación la tabla de la International Register of ISMS Certificates de la cantidad de empresas por países.

Tabla No. 11: Number of Certificates Per Country

Japan	3840	Slovenia	18	Macau	3
India	526	Netherlands	15	Qatar	3
China	497	Philippines	15	Albania	2
UK	471	Iran	14	Argentina	2
Taiwan	420	Pakistan	14	Belgium	2
Germany	170	Vietnam	14	Bosnia Herzegovina	2
Korea	106	Iceland	13	Cyprus	2
Czech Republic	101	Indonesia	13	Isle of Man	2
USA	100	Saudi Arabia	13	Kazakhstan	2
Spain	73	Colombia	11	Luxembourg	2
Hungary	68	Kuwait	11	Macedonia	2
Italy	67	Norway	10	Malta	2
Poland	58	Portugal	10	Ukraine	2
Malaysia	55	Russian Federation	10	Mauritius	2
Ireland	41	Sweden	9	Armenia	1
Thailand	40	Bahrain	8	Bangladesh	1
Austria	38	Canada	8	Belarus	1
Romania	35	Croatia	7	Denmark	1
Hong Kong	32	Switzerland	7	Ecuador	1
Greece	30	Egypt	5	Jersey	1
Australia	29	Oman	5	Kyrgyzstan	1
Singapore	29	Peru	5	Lebanon	1
France	25	South Africa	5	Moldova	1
Mexico	24	Sri Lanka	5	New Zealand	1

Turkey	24	Dominican Republic	4	Sudan	1
Brazil	23	Lithuania	4	Uruguay	1
Slovakia	23	Morocco	4	Yemen	1
UAE	20	Chile	3		
Bulgaria	18	Gibraltar	3	**Total**	**7279**

Fuente http://iso27001certificates.com/

Como podemos observar en la tabla el país con más empresas certificadas es Japón, mientras que Republica Dominicana sólo cuenta con 4 empresas certificadas hasta el momento entre las que podemos mencionar Unipago y el Nap del Caribe dichas empresas se encarga de manipular información crítica de terceros.

Al parecer la implementación de esta norma es muy costosa y demanda de muchos recursos tanto humano como económico.

Ventajas

- Facilita la integración de los sistemas de gestión, debido a que es una estructura de alto nivel, donde los términos y definiciones ayudan a implementar.
- Todas las definiciones vienen del estándar ISO 2700 y las inconsistencias se han removido.
- Los riesgos en la seguridad de la información en su conjunto deben ser abordados.
- Los documentos requerimientos están claramente establecidos, hace referencias al tamaño y complejidad.
- Menciona que las acciones preventivas no van.

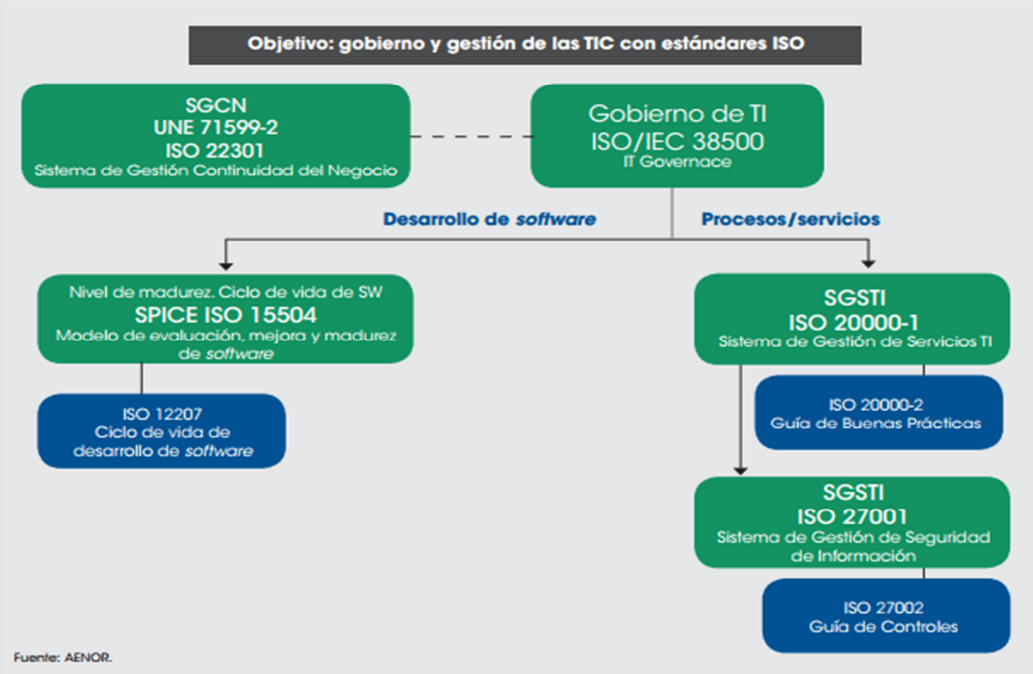
Desventajas

- Es una abstracción y es un nivel alto, no es tan detallado.
- Los requisitos son un tanto más difícil para interpretar, debido a los nuevos conceptos.
- No se menciona el enfoque PDCA.
- No se menciona las políticas del SGSI.
- No hay una descripción detallada de la identificación del riesgo

Modelo de gobierno y gestión para las TIC

La norma ISO 27001 tiene relación con otras normas que conforman el modelo de gobierno y gestión de las TIC, basado en estándares aceptados mundialmente (ver figura 4).

Gráfico No. 9: Ejemplo Modelos de Gobierno y Gestión de las TIC



2.1.5. NORMA ISO 27001. *TECNOLOGÍA DE LA PRÁCTICAS PARA LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN*

2.1.5.1. IMPORTANCIA DE LA NORMA ISO 27002

"La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegido adecuadamente" (NSTISSI No. 4009, January 2000)

La información es un activo que representa un gran valor dentro de la organización, por lo tanto requiere una protección adecuada ya sea por diferentes medios o técnicas de seguridades implantadas. Para estos hay que tomar muy en cuenta el creciente ambiente interconectado de negocios es por esto que la información está expuesta a un mayor rango de amenazas y vulnerabilidades (Romo Villafuerte & Valarezo Constante, 2012)

"Seguridad de los Sistemas de Información consiste en la protección de los sistemas de información respecto al acceso no autorizado o modificación de la información en el almacenamiento, proceso y tránsito y contra la denegación de servicio para los usuarios" (Romero) Las empresas se encuentran expuestas a riesgos físicos como incendios, inundaciones, terremotos o terrorismos que al explotar una amenaza pueden afectar la disponibilidad de nuestra información y recursos, por tal razón se debe realizar una evaluación de riesgos de forma periódica estableciendo un punto de equilibrio en relación de costo –beneficio.

Muchas empresas le restan valor o importancia al aspecto de seguridad, las pérdidas por la falta de seguridad pueden ser tremendamente caras, tanto en materia económica como en cuanto a prestigio, nivel de ventas, problemas legales, daños a empleados de la organización o a terceros (por ejemplo si se divulgara información confidencial luego de un ataque a un sistema) (Montoya.)

Gráfico No. 10 Especificación ISO 27000

La norma ISO/IEC 27002:2005 es una herramienta sencilla que permite establecer políticas, y controles bajo el objetivo de disminuir los riesgos que tienen los activos de la organización. En primer lugar, obtenemos una reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. Con lo que se reducen las amenazas hasta alcanzar un nivel asumible para la organización (Romo Villafuerte & Valarezo Constante, 2012)

2.1.5.2. ALCANCE

Este Estándar Internacional va orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo.

Gráfico No. 11 Análisis FODA de la ISO 27002 (Romo Villafuerte & Valarezo Constante, 2012)

FORTALEZAS	OPORTUNIDADES	DEBILIDADES	AMENZAS
Es un estándar adoptado en Ecuador como NTE ISO/IEC 27002:2009	Es una norma internacional y por eso se la puede aplicar para cualquier institución.	En los objetivos de control no se contempla la trazabilidad.	Es una norma conceptual, no se tienen las herramientas puntuales para su implementación.
Cada control tiene su guía de implementación para una fácil visión	Para la implementación de los controles no se requiere revisar los 133 controles, solo los que aplique a la organización	No es una guía madura para el análisis de riesgos.	Esta norma no es certificable.
Fácil adaptación para cada organización.			
Guía para mejorar la seguridad de la información.			

2.1.5.3. TÉRMINOS Y DEFINICIONES

Amenaza: Causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.

Análisis de riesgo: Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

Control: Medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida.

Criptografía: Arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.

Electrotecnia: Ciencia que estudia las aplicaciones técnicas de la electricidad.

Evaluación del riesgo: Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.

Evento de seguridad de la información: Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Incidente de seguridad de la información: Incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

Lineamiento: Descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas.

Medios de procesamiento de la información: Sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

Métrica: Metodología de planificación, desarrollo y mantenimiento de sistemas de información.

Política: Intención y dirección general expresada formalmente por la gerencia.

Riesgo: Combinación de la probabilidad de un evento y su ocurrencia.

Seguridad de la información: Preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-reputación y confiabilidad.

Tercera persona: Persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

2.1.5.4. ESTRUCTURA DE ESTE ESTÁNDAR

Este Estándar contiene un número de categorías de seguridad principales, entre las cuales se tienen once cláusulas:

a) Política de seguridad.
b) Aspectos organizativos de la seguridad de la información.
c) Gestión de activos.
d) Seguridad ligada a los recursos humanos.
e) Seguridad física y ambiental.
f) Gestión de comunicaciones y operaciones.
g) Control de acceso.
h) Adquisición, desarrollo y mantenimiento de los sistemas de información.
i) Gestión de incidentes en la seguridad de la información.
j) Gestión de la continuidad del negocio.
k) Cumplimiento.

Política de seguridad: deben haber políticas organizacionales claras y bien definidas que regulen el trabajo que se estará realizando en materia de seguridad de la información.

Aspectos organizativos de la seguridad de la información: cómo se trabajará en la seguridad de la información organizativamente, tanto de manera interna (empleados o personal de la organización) como de forma externa o con respecto a terceros (clientes, proveedores, etc.)

Gestión de activos: se debe tener un completo y actualizado inventario de los activos, su clasificación, quiénes son responsables por los activos, etc.

Seguridad ligada a los recursos humanos: especificar las responsabilidades del personal o recursos humanos de una organización, así como los límites que cada uno de ellos tiene con respecto al acceso y manipulación de la información.

Seguridad física y ambiental: consiste en tener una infraestructura física (instalaciones) y ambiental (temperaturas adecuadas, condiciones ideales de operación ideales) adecuadas de modo que no pongan en riesgo la seguridad de la información.

Gestión de comunicaciones y operaciones: asegurar la operación correcta de cada uno de los procesos, incluyendo las comunicaciones y operaciones que se dan en la organización.

Esto también incluye la separación entre los ambientes de desarrollo, de prueba y de operación, para evitar problemas operacionales.

Control de acceso: deben existir medidas adecuadas que controlen el acceso a determinada información, únicamente a las personas que están autorizadas para hacerlo, utilizando autenticaciones, contraseñas, y métodos seguros para controlar el acceso a la información.

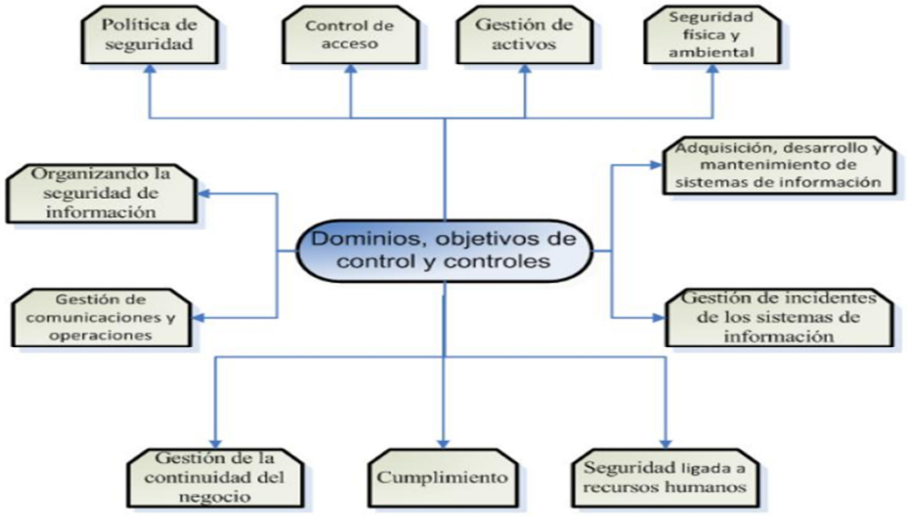
Adquisición, desarrollo y mantenimiento de los sistemas de información: consiste en tomar medidas adecuadas para adquirir nuevos sistemas (no aceptar sistemas que no cumplan con los requisitos de calidad adecuados), haciendo también un eficiente desarrollo y mantenimiento de los sistemas.

Gestión de incidentes en la seguridad de la información: los incidentes se pueden dar tarde o temprano, y la organización debe contar con registros y bitácoras para identificar a los causantes y responsables de los incidentes, recopilar evidencias, aprender de los errores para no volverlos a cometer.

Gestión de la continuidad del negocio: se deben tener planes y medidas para hacerle frente a los incidentes, de modo que el negocio pueda continuar en marcha gracias a medidas alternativas para que un incidente no detenga las operaciones por tiempos prolongados, que no se pierda información, que no se estanquen o detengan las ventas o negocios.

Cumplimiento: debe darse el debido cumplimiento a los requisitos legales, como derechos de propiedad intelectual, derecho a la confidencialidad de cierta información, control de auditorías.

Gráfico No. 12 Dominios de Control ISO 27002 - 2005



2.1.5.5. EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD

Se deben identificar, cuantificar y priorizar los riesgos de seguridad. Posterior a ello se debe dar un tratamiento a cada uno de los riesgos, aplicando medidas adecuadas de control para reducir la probabilidad de que ocurran consecuencias negativas al no tener una buena seguridad.

La reducción de riesgos no puede ser un proceso arbitrario y regido por la voluntad de los dueños o administradores de la empresa, sino que además de seguir medidas adecuadas y eficientes, se deben tener en cuenta los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales, objetivos organizacionales, bienestar de clientes y trabajadores, costos de implementación y operación (pues existen medidas de seguridad de gran calidad pero excesivamente caras, tanto que es más cara la seguridad que la propia ganancia de una empresa, afectando la rentabilidad).

Se debe saber que ningún conjunto de controles puede lograr la seguridad completa, pero que sí es posible reducir al máximo los riesgos que amenacen con afectar la seguridad en una organización.

2.1.5.6. POLÍTICA DE SEGURIDAD

El objetivo de esta norma es proporcionar a la gerencia la dirección y soporte para la seguridad de la información, en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes. Esto por supuesto debe ser creado de forma particular por cada organización. Se debe

redactar un "Documento de la política de seguridad de la información." Este documento debe ser primeramente aprobado por la gerencia y luego publicado y comunicado a todos los empleados y las partes externas relevantes.

El Documento de la Política de Seguridad de la Información debe contar con un claro lineamiento de implementación, y debe contener partes tales como una definición de seguridad de la información, sus objetivos y alcances generales, importancia, intención de la gerencia en cuanto al tema de seguridad de la información, estructuras de evaluación y gestión de riesgos, explicación de las políticas o principios de la organización, definición de las responsabilidades individuales en cuanto a la seguridad, etc.

Se debe tener especial cuidado respecto a la confidencialidad de este documento, pues si se distribuye fuera de la organización, no debería divulgar información confidencial que afecte de alguna manera a la organización o a personas específicas (por ejemplo que afecte la intimidad de alguien al divulgar sus datos personales, etc.)

Las políticas de seguridad de la información no pueden quedar estáticas para siempre, sino que por el contrario, tienen que ser continuamente revisadas y actualizadas para que se mantengan en condiciones favorables y en concordancia con los cambios tecnológicos o cualquier tipo de cambio que se dé. Por ejemplo, si aparece un nuevo virus o nuevas tecnologías que representen riesgos, las políticas de seguridad podrían cambiar o ser mejoradas de acuerdo a las necesidades actuales. Un caso práctico sería el aparecimiento de las memorias USB. Antiguamente esa tecnología no existía, entonces no se esperaba que existieran robos de información a través de puertos USB. Ahora las memorias USB son de uso global y por lo tanto, las políticas de seguridad deberían considerar bloquear puertos USB o algo por el estilo, para no permitir que se extraiga información de esa manera de forma ilícita o por personas no autorizadas.

Otro problema sería tener excelentes políticas de seguridad, pero que no sean implementadas correctamente o que simplemente se queden a nivel teórico y que no se apliquen. En la vida real se suelen dar casos donde las leyes están muy bien redactadas, pero que no se cumplen. Sucede en muchos países, que la legislación puede estar estructurada muy bien, pero que no se respeta. Igualmente podría darse que se tengan excelentes políticas, pero que no se cumplan o que no se sepan implementar correctamente. Por lo tanto, se requieren lineamientos de implementación adecuados.

2.1.5.7. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La organización de la seguridad de la información se puede dar de dos formas: organización interna y organización con respecto a terceros.

En cuanto a la organización interna, se tiene como objetivo manejar la seguridad de la información dentro de la organización.

Se requiere un compromiso por parte de la gerencia para apoyar activamente la seguridad dentro de la organización. La gerencia debe invertir en seguridad, y no verlo como un aspecto que no tiene relevancia. Algunas veces la seguridad requiere inversión económica, y parte del compromiso de la gerencia implica tener un presupuesto especial para seguridad, por supuesto de una forma razonable que no afecte la rentabilidad de la empresa. Por ejemplo, implementar un método carísimo de seguridad podría ser de gran beneficio, pero representar un costo demasiado elevado.

Es fundamental también asignar responsabilidades, se deben asignar claramente responsabilidades para que cuando se den los problemas, cada quien responda por sus actos y por lo que estaba bajo su cargo. La asignación de responsabilidades no solamente tiene que ser verbal, sino que escrita y en muchas ocasiones, incluso bajo un contrato legal.

Deben existir acuerdos de confidencialidad, se debe tener en cuenta mantener los contactos apropiados con las autoridades relevantes, por ejemplo con la policía, departamento de bomberos, etc.

La organización en materia de seguridad de la información debe también considerarse respecto a terceros, el objetivo de esto es mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos. Para ello se debe comenzar por la identificación de los riesgos relacionados con los grupos externos. Se debe estudiar cómo a raíz de procesos comerciales que involucran a grupos externos se les puede estar otorgando acceso que afecte la seguridad. Esto se puede dar tanto con clientes o con proveedores. Se debe tener especial cuidado respecto a los contratos que se hagan con terceros, para no afectar la seguridad de la información.

2.1.5.8. GESTIÓN DE ACTIVOS

Se deben asignar responsabilidades por cada uno de los activos de la organización, así como poseer un inventario actualizado de todos los activos que se tienen, a quien/quienes les pertenecen, el uso

que se les debe dar, y la clasificación de todos los activos. Para esto el departamento de contabilidad tendrá que hacer un buen trabajo en cuanto a esta clasificación y desglose de activos, y el departamento de leyes de la empresa también tendrá que ser muy metódico en estos procesos, ya que los activos son todos los bienes y recursos que posee una empresa, incluyendo bienes muebles e inmuebles, dinero, etc.

2.1.5.9. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

El objetivo de esto es asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados, reduciendo el riesgo de robo, fraude y mal uso de los medios. Es necesario definir claramente los roles y responsabilidades de cada empleado. Todo esto no debe ser simplemente mediante acuerdos verbales, sino que se debe plasmar en el contrato de trabajo. También deben existir capacitaciones periódicas para concientizar y proporcionar formación y procesos disciplinarios relacionados a la seguridad y responsabilidad de los recursos humanos en este ámbito.

También se deben especificar las responsabilidades cuando se da el cese del empleo o cambio de puesto de trabajo, para que la persona no se vaya simplemente y deje a la organización afectada de alguna manera en materia de seguridad.

2.1.5.10. SEGURIDAD FÍSICA Y AMBIENTAL

La seguridad física y ambiental se divide en áreas seguras y seguridad de los equipos. Respecto a las áreas seguras, se refiere a un perímetro de seguridad física que cuente con barreras o límites tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas, y medidas de esa naturaleza para proteger las áreas que contienen información y medios de procesamiento de información.

Se debe contar con controles físicos de entrada, tales como puertas con llave, etc. Además de eso, es necesario considerar la seguridad física con respecto a amenazas externas y de origen ambiental, como incendios (para los cuales deben haber extintores adecuados y en los lugares convenientes), terremotos, huracanes, inundaciones, atentados terroristas, etc. Deben también haber áreas de acceso público de carga y descarga, parqueos, áreas de visita, entre otros. Si hay gradas, deben ser seguras y con las medidas respectivas como antideslizantes y barras de apoyo sobre la pared para sujetarse.

En cuanto a la seguridad ambiental, se debe controlar la temperatura adecuada para los equipos, seguridad del cableado, mantenimiento de equipos, etc. Para todo esto se requerirá de los servicios de técnicos o ingenieros especializados en el cuidado y mantenimiento de cada uno de los equipos, así como en la inmediata reparación de los mismos cuando sea necesario.

La ubicación de los equipos también debe ser adecuada y de tal manera que evite riesgos. Por ejemplo si algún equipo se debe estar trasladando con frecuencia, quizá sea mejor dejarlo en la primera planta, en vez de dejarlo en la última planta de un edificio, pues el traslado podría aumentar los riesgos de que se caiga y dañe, especialmente si no se cuenta con un ascensor. Se debe igualmente verificar y controlar el tiempo de vida útil de los equipos para que trabajen en condiciones óptimas.

2.1.5.11. GESTIÓN DE COMUNICACIONES Y OPERACIONES

El objetivo de esto es asegurar la operación correcta y segura de los medios de procesamiento de la información.

En primer lugar, es necesario que los procedimientos de operación estén bien documentados, pues no basta con tener las ideas en la mente de los administradores, sino que se deben plasmar en documentos que por supuesto estén autorizados por la gerencia.

Otro aspecto fundamental es la gestión de cambios. Un cambio relevante no se debe hacer jamás sin documentarlo, además de la necesidad de hacerlo bajo la autorización pertinente y luego de un estudio y análisis de los beneficios que traerá dicho cambio.

Se debe tener cuidado que nadie pueda tener acceso, modificar o utilizar los activos sin autorización o detección. Para ello debe haber una bitácora de accesos, con las respectivas horas y tiempos de acceso, etc.

Es completamente necesario tener un nivel de separación entre los ambientes de desarrollo, de prueba y de operación, para evitar problemas operacionales.

Si la organización se dedica a vender servicios, debe implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.

A la hora de aceptar un nuevo sistema, se debe tener especial cuidado, verificando primeramente las capacidades y contando con evaluadores capacitados para determinar la calidad o falta de calidad de un sistema nuevo a implementar. Se tienen que establecer criterios de aceptación de los sistemas de información, actualizaciones o versiones nuevas, y se deben realizar pruebas adecuadas a los sistemas durante su desarrollo y antes de su aceptación.

La protección contra el código malicioso y descargable debe servir para proteger la integridad del software y la integración con los sistemas y tecnologías con que ya se cuenta. Se deben también tener controles de detección, prevención y recuperación para proteger contra códigos maliciosos, por ejemplo antivirus actualizados y respaldos de información. De hecho, los respaldos de información son vitales y deben realizarse con una frecuencia razonable, pues de lo contrario, pueden existir pérdidas de información de gran impacto negativo.

En cuanto a las redes, es necesario asegurar la protección de la información que se transmite y la protección de la infraestructura de soporte. Los servicios de red tienen que ser igualmente seguros, especialmente considerando cómo la tendencia de los últimos años se encamina cada vez más a basar todas las tecnologías de la información a ambientes en red para transmitir y compartir la información efectivamente. Los sistemas tienen que estar muy bien documentados, detalle a detalle, incluyendo por supuesto la arquitectura de red con la que se cuenta.

Se tienen que establecer políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación. Además de las medidas directas para proteger el adecuado intercambio de información, se le debe recordar al personal el tomar las precauciones adecuadas, como no revelar información confidencial al realizar una llamada telefónica para evitar ser escuchado o interceptado por personas alrededor suyo, intervención de teléfonos, personas en el otro lado de la línea (en el lado del receptor), etc. Igualmente para los mensajes electrónicos se deben tomar medidas adecuadas, para evitar así cualquier tipo de problema que afecte la seguridad de la información.

Cuando se haga uso del comercio electrónico, debe haber una eficiente protección cuando se pasa a través de redes públicas, para protegerse de la actividad fraudulenta, divulgación no autorizada, modificación, entro otros.

Debe haber un continuo monitoreo para detectar actividades de procesamiento de información no autorizadas. Las auditorías son también necesarias.

Las fallas deben ser inmediatamente corregidas, pero también registradas y analizadas para que sirvan en la toma de decisiones y para realizar acciones necesarias.

Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados con una fuente que proporcione la hora exacta acordada, todo acceso a la información debe ser controlado.

2.1.5.12. CONTROL DE ACCESO

En primer lugar, se debe contar con una política de control de acceso. Todo acceso no autorizado debe ser evitado y se deben minimizar al máximo las probabilidades de que eso suceda. Todo esto se controla mediante registro de usuarios, gestión de privilegios, autenticación mediante usuarios y contraseñas.

Aparte de la autenticación correspondiente, los usuarios deben asegurar que el equipo desatendido tenga la protección apropiada, como por ejemplo la activación automática de un protector de pantalla después de cierto tiempo de inactividad, el cual permanezca impidiendo el acceso hasta que se introduzca una contraseña conocida por quien estaba autorizado para utilizar la máquina desatendida.

Son necesarios controles de acceso a la red, al sistema operativo, a las aplicaciones y a la información. Para todo esto deben existir registros y bitácoras de acceso.

Deben también existir políticas que contemplen adecuadamente aspectos de comunicación móvil, redes inalámbricas, control de acceso a ordenadores portátiles, y teletrabajo, en caso que los empleados de la empresa ejecuten su trabajo fuera de las instalaciones de la organización.

2.1.5.13. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Contemplar aspectos de seguridad es requerido al adquirir equipos y sistemas, o al desarrollarlos. No solamente se debe considerar la calidad y el precio, sino que la seguridad que ofrecen.

Debe existir una validación adecuada de los datos de entrada y de salida, controlando el procesamiento interno en las aplicaciones, y la integridad de los mensajes.

La gestión de claves debe ser tal que ofrezca soporte al uso de técnicas criptográficas en la organización, utilizando técnicas seguras.

Garantizar la seguridad de los archivos del sistema es fundamental, por lo que se debe controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos de tecnologías de información y las actividades de soporte se deben realizar de manera segura.

Deben establecerse procedimientos para el control de la instalación del software en los sistemas operacionales. Con esto por ejemplo se evita el riesgo de realizar instalaciones ilegales o sin las respectivas licencias.

Se debe restringir el acceso al código fuente para evitar robos, alteraciones, o la aplicación de ingeniería inversa por parte de personas no autorizadas, o para evitar en general cualquier tipo de daño a la propiedad de código fuente con que se cuente.

La seguridad en los procesos de desarrollo y soporte debe considerar procedimientos de control de cambios, revisiones técnicas de aplicaciones tras efectuar cambios en el sistema operativo y también restricciones a los cambios en los paquetes de software. No se tiene que permitir la fuga ni la filtración de información no requerida.

Contar con un control de las vulnerabilidades técnicas ayudará a tratar los riesgos de una mejor manera.

2.1.5.14. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

La comunicación es fundamental en todo proceso. Por lo tanto, se debe trabajar con reportes de los eventos y debilidades de la seguridad de la información, asegurando una comunicación tal que permita que se realice una acción correctiva oportuna, llevando la información a través de los canales gerenciales apropiados lo más rápidamente posible. De la misma manera se debe contar con reportes de las debilidades en la seguridad, requiriendo que todos los empleados, contratistas y terceros de los sistemas y servicios de información tomen nota de y reporten cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios.

Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información es elemental.

Aprender de los errores es sabio, se deben establecer mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información, siempre con la idea de no volver a cometer los errores que ya se cometieron, y mejor aún, aprender de los errores que ya otros cometieron.

A la hora de recolectar evidencia, cuando una acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (ya sea civil o criminal); se debe recolectar, mantener y presentar evidencia para cumplir con las reglas de evidencia establecidas en la(s) jurisdicción(es) relevante(s).

2.1.5.15. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Las consecuencias de los desastres, fallas en la seguridad, pérdida del servicio y la disponibilidad del servicio debieran estar sujetas a un análisis del impacto comercial. Se deben desarrollar e implementar planes para la continuidad del negocio para asegurar la reanudación oportuna de las operaciones esenciales. La seguridad de la información debiera ser una parte integral del proceso general de continuidad del negocio, y otros procesos gerenciales dentro de la organización.

Se debe contar con planes de continuidad del negocio que incluyan la seguridad de la información. Estos planes no deben ser estáticos, sino que deben ser actualizados y ser sometidos a pruebas, mantenimiento y reevaluación.

Junto a la gestión de riesgos, debe aparecer la identificación de eventos que pueden causar interrupciones a los procesos comerciales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información. Por supuesto se requieren planes alternativos y de acción ante tales eventos, asegurando siempre la protección e integridad de la información y tratando de poner el negocio en su estado de operación normal a la mayor brevedad posible.

2.1.5.16. CUMPLIMIENTO

Es una prioridad el buen cumplimiento de los requisitos legales para evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad. La identificación de la legislación aplicable debe estar bien definida.

Se deben definir explícitamente, documentar y actualizar todos los requerimientos legales para cada sistema de información y para la organización en general.

Es necesario implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso del material con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentado.

El cumplimiento de los requisitos legales se aplica también a la protección de los documentos de la organización, protección de datos y privacidad de la información personal, prevención del uso indebido de los recursos de tratamiento de la información, y a regulaciones de los controles criptográficos.

Los sistemas de información deben estar bajo monitoreo y deben chequearse regularmente para ver y garantizar el cumplimiento de los estándares de implementación de la seguridad.

En cuanto a las auditorías de los sistemas de información, se tiene que maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información. Durante las auditorías de los sistemas de información deben existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría. También se requiere protección para salvaguardar la integridad y evitar el mal uso de las herramientas de auditoría.

Las actividades y requerimientos de auditoría que involucran chequeos de los sistemas operacionales deben ser planeados y acordados cuidadosamente para minimizar el riesgo de interrupciones en los procesos comerciales.

2.1.6. NORMA ISO 38500 GOBIERNO CORPORATIVO DE LAS TECNOLOGIAS DE INFORMACIÓN

2.1.6.1. ORIGEN

La ISO 38500 nace como un instrumento para el asesoramiento de los ejecutivos responsables del funcionamiento de las organizaciones, respecto del papel que deben jugar en el gerenciamiento y uso de las TI.

Esta norma se generó a partir de la norma australiana AS8015 del 2005 por la cual se controlaba el uso actual y futuro de las TIC, siendo uno de sus principales objetivos el de dirigir y evaluar los planes para que el uso de las TIC apoyen a la organización además de monitorear constantemente su uso para lograr los planes establecidos, lo cual incluye el establecimiento de estrategias y políticas relacionadas dentro de una organización.

2.1.6.2. ALCANCE Y APLICACIÓN

Esta norma proporciona principios de guía para los directores de las organizaciones sobre el uso eficaz, eficiente y aceptable de las TI en sus organizaciones y es aplicable al gobierno de los procesos de gestión y a las decisiones relacionadas con los servicios de información y comunicación, los cuales pueden ser controlados por especialistas de TI de la organización, por proveedores externos del servicio o por unidades de negocio dentro de la organización.

Las directrices expuestas en la norma son aplicables para una gran cantidad de organizaciones, cualquiera que sea su tamaño u objeto de negocio, incluso independientemente del nivel de extensión del uso de TI.

2.1.6.3. OBJETIVOS DE LA NORMA

El objetivo de la norma es fomentar el uso eficaz, eficiente y aceptable de las tecnologías de información en todas las organizaciones a través de las siguientes acciones:

- Asegurar del cumplimiento de la norma a las partes involucradas, además de generar confianza en el Gobierno Corporativo que tiene la organización sobre TI.

- Informar y orientar a los directores sobre el gobierno del uso de TI en las organizaciones

- Brindar una base para la evaluación objetiva del Gobierno Corporativo de TI.

2.1.6.4. BENEFICIOS DE USAR LA NORMA

2.1.6.4.1. Generales

- El establecimiento de principios para el uso eficiente, efectivo y aceptable de las TI.

- Asegurase de que sus organizaciones siguen dichos principios ayudará a los directores en el equilibrio de riesgos y fomentará las oportunidades que nacen del uso de las TI.

- Se establece un modelo de gobernanza de TI.

- Mitiga los riesgos de que los directores cumplan con sus obligaciones pues brinda un modelo apropiado el cual exige que se preste la debida atención a fin de aplicar apropiadamente estos principios.

2.1.6.4.2. Conformidad de la Organización

- Una apropiada gobernanza corporativa de Ti puede ayudar a los directores en asegurar la conformidad con las obligaciones (normativas, legales, leyes comunes, contractuales) sobre el uso de TI.

- Sistemas Inadecuados de TI pueden exponer a los directores al riesgo de no conformidad con la legislación. (Por ejemplo un director puede ser calificado como responsable de un inadecuado sistema contable que produzca impuestos que no han sido pagados)

- Procesos relacionados a TI pueden incorporar riesgos específicos que deben abordarse apropiadamente, por ejemplo un director puede ser responsable de infracciones dentro de:

  - Normas de seguridad,
  - Leyes de privacidad,
  - Spam,
  - Prácticas de Comercio,
  - Derechos de propiedad intelectual y licenciamiento,
  - Requisitos del mantenimiento de registros,
  - Legislación y reglamentación ambiental,
  - Leyes de salud y seguridad,
  - Controles de accesos,
  - Estándares de responsabilidad social

- Los directores que usan y aplican estas guías usualmente cumplen con sus obligaciones.

2.1.6.4.3. Rendimiento de la Organización

- Un gobierno corporativo apropiado de TI ayuda a los directores a asegurar que el uso de TI contribuye positivamente al rendimiento de la organización a través de:

  - Una apropiada implementación y operación de los activos de TI

- Responsabilidades claras y resultados la provisión y uso de TI en el logro de objetivos de la organización.
- Continuidad y sostenibilidad del negocio.
- Alineación de TI con las necesidades de negocio.
- Asignación eficiente de recursos.
- Innovación de servicios, mercados y negocios.
- Reducción de costos organizacionales y,
- Beneficios reales de cada inversión de TI.

2.1.6.5. MARCO PARA UNA BUENA GOBERNANZA CORPORATIVA DE TI

2.1.6.5.1. Principios

En esta sección se establece seis principios para una buena gobernanza corporativa de TI los cuales son aplicables a la mayoría de organizaciones.

- **Responsabilidad**

  Los Individuos dentro de la organización entienden y aceptan sus responsabilidades en la relación de oferta y demanda de TI, inclusive aquellos que tienen autoridad para ordenar ciertas acciones también la tienen para llevar acabo las mismas.

- **Estrategia**

  La estrategia de negocios de una organización tiene cuenta el presente y futuro de las capacidades de TI, sus planes estratégicos satisfacen las necesidades actuales y en curso de la estrategia de negocio de la organización.

- **Adquisición**

  Las adquisiciones de TI son realizadas por razones válidas, en base de apropiado análisis, en donde se determine de manera transparente cada decisión tomada. Debe existir un apropiado balance entre beneficios, oportunidades, costos y riesgos, tanto para el corto y largo plazo.

- **Rendimiento**

  Las TI deben ser aptas para el soporte de la organización en la prestación de servicios, niveles y calidad de servicio, necesarios satisfacer los requerimientos de negocio actuales y futuros.

- **Conformidad**

  TI debe cumplir con todas las regulaciones y leyes. Las políticas y prácticas deben estar definidas, implementadas y siendo cumplidas.

- **Comportamiento Humano**

  Las políticas, prácticas y decisiones de TI deben demostrar respecto por el comportamiento humano incluyendo las necesidades actuales y en evolución de todas las personas en el proceso.

2.1.6.5.2. Modelo

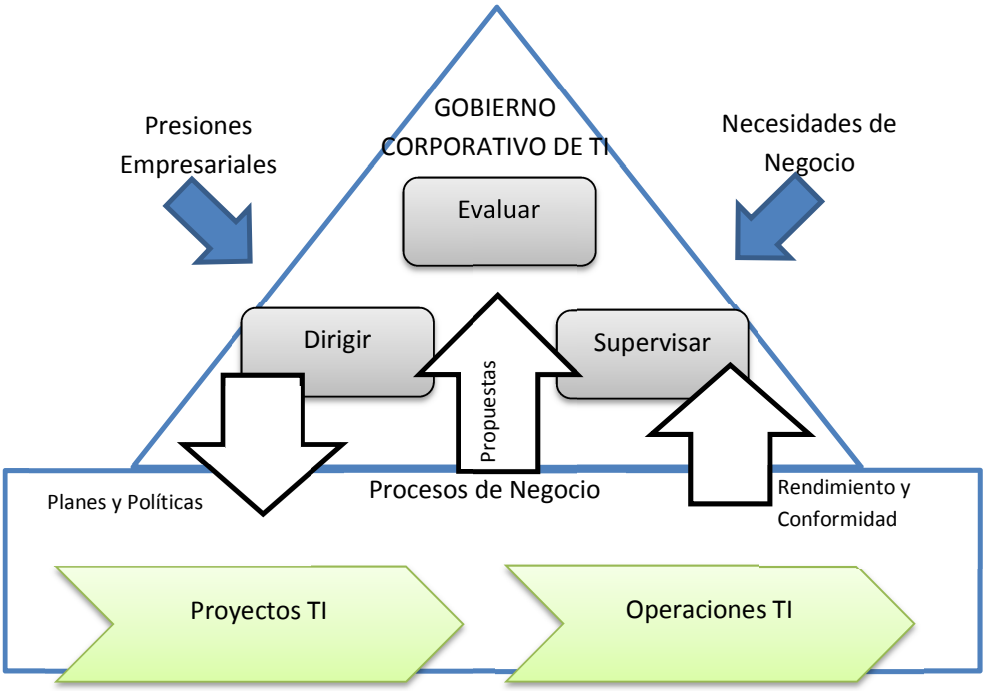
Los directores deben gobernar TI a través de 3 tareas principales:

a) Evaluar el uso corriente y futuro de TI.

b) Dirigir la preparación y ejecución de planes y políticas directas para asegurar que el uso de las TI cumple con los objetivos de negocio.

c) Supervisar el cumplimiento de las políticas y monitorear el desempeño respecto de los planes.

Gráfico No. 13 Gobierno Corporativo de TI



Evaluar

Los directores deben examinar y hacer juicios acerca del uso actual y futuro de TI, Incluyendo estrategias, propuestas y acuerdos de suministros (ya sea interno, externo o ambos)

Al evaluar el uso de las TI, los directores deben considerar las presiones internas y externas actuando sobre el negocio, tales como cambios tecnológicos, económicos, tendencias sociales e influencias políticas.

Los directivos deben realizar evaluaciones continuas con cada cambio de estas presiones.
También deben tomar en cuenta tanto las actuales y futuras necesidades de negocio, los actuales y futuras objetivos organizacionales que se deban alcanzar, tal como el mantenimiento de ventajas competitivas, así como los objetivos específicos de las estrategias y propuestas que se están evaluando.

Dirigir

Los directores deben asegurar que la puesta en marcha de los proyectos se planifica y gestiona adecuadamente, teniendo en cuenta los impactos de negocio y prácticas operacionales, así como los sistemas e infraestructura de TI existentes.

Los directivos deben fomentar una cultura de buena gobernanza de TI en sus organizaciones al exigir a sus administradores información oportuna, que cumpla con la dirección y que sea conforme a los 6 principios de buena gobernanza.

Supervisar

Los directores deben monitorear, a través de sistemas apropiados de medición, el rendimiento de TI. Se deben convencer de que el rendimiento está conforme a lo planificado, en particular con respecto a los objetivos de negocio.

Adicionalmente se debe asegurar que TI es conforme con las obligaciones externas y las prácticas internas de trabajo.

2.1.6.6. GUÍA PARA EL GOBIERNO CORPORATIVO DE TI

2.1.6.6.1. General

Las siguientes secciones proporcionan una guía para una buena gobernanza de TI, así como las prácticas requeridas para implementar estos principios.

Las prácticas descritas no son exhaustivas pero proveen un punto de inicio para discutir sobre las responsabilidades de los directores en el Gobierno de TI. Es decir las prácticas descritas sugieren guías para la gobernanza de TI.

Es responsabilidad de cada organización, de manera individual, identificar las acciones específicas requeridas para implementar estos principios, dando la debida consideración a la naturaleza de la organización, y un análisis apropiado de los riesgos y oportunidades del uso de TI.

Como una base de ilustración, las prácticas descritas son aplicables para la mayoría de organizaciones (grandes o pequeñas), la mayor parte del tiempo. Cualquier variación debería ser considerada.

2.1.6.6.2. Principio 1: Responsabilidad

Evaluar

Los directores deben evaluar las opciones para asignar las responsabilidades respecto del uso presente y futuro del uso de TI. En la evaluación de las opciones, los directores deben tratar de asegurar el uso y entrega efectiva, eficiente y aceptable de TI en apoyo de los objetivos actuales y futuros del negocio.

Los directores deben evaluar la competencia de los que recibieron la responsabilidad de tomar las decisiones relativas a TI. Generalmente, estas personas deben ser gerentes de negocios que también son responsables de los objetivos de negocio de la organización y rendimiento, con la asistencia de especialistas de TI que entienden los valores empresariales y procesos.

Dirigir

Los directores deben ordenar que los planes se lleven a cabo de acuerdo con la responsabilidad de TI asignada. Los directores deben pedir que reciban la información que necesitan para cumplir con sus responsabilidades y rendir cuentas.

Monitorear

Los directores deben vigilar que los mecanismos de gobernanza de TI adecuada son establecida. Directores deben vigilar que los que recibieron la responsabilidad reconoce y comprender sus responsabilidades.

Los directores deben monitorear el desempeño de los que recibieron la responsabilidad en el gobierno de TI (por ejemplo, aquellas personas que integran los comités de dirección o que presentan propuestas a los directores).

2.1.6.6.3. Principio 2: Estrategia

Evaluar

Los directores deben evaluar la evolución de TI y procesos de negocio para asegurar que proporcionará apoyo a las necesidades futuras del negocio.

Al considerar los planes y políticas, los directores de TI deben evaluar las actividades y asegurarse de que se alinean con los objetivos de la organización en circunstancias cambiantes, tomar en consideración las mejores prácticas y satisfacer los requerimientos de otras partes interesadas.

Los directores deben garantizar que el uso de TI está sujeto a una apropiada evaluación del riesgo, como se describe en las normas internacionales y nacionales pertinentes.

Dirigir

Los directores deben dirigir la preparación y el uso de los planes y políticas que aseguren que la organización se beneficia de los desarrollos de TI.

Los directores también deben alentar la presentación de propuestas para usos innovadores de TI que le permitan a la organización, responder ante nuevas oportunidades o desafíos, emprender nuevos negocios o mejorar procesos.

Monitorear

Los directores deben monitorear el progreso de las propuestas de TI aprobadas, para asegurar que se están logrando los objetivos en los plazos establecidos y con los recursos asignados.

Los directores deben supervisar el uso de las TI para asegurarse de que están obteniendo los beneficios previstos.

2.1.6.6.4. Principio 3: Adquisición

Evaluar

Los directores deben evaluar las opciones para proporcionar herramientas de TI, a fin de darse cuenta sobre las propuestas aprobadas, el equilibrio de riesgos y relación calidad-precio de las inversiones propuestas.

Dirigir

Los directores deben ordenar que los activos de TI (sistemas e infraestructura) se adquieran de una manera apropiada, incluyendo la preparación de la documentación adecuada, garantizando al mismo tiempo que se proporcionan capacidades requeridas.

Los directores deben controlar que los contratos de compra (tanto internos como externos) apoyen las necesidades del negocio de la organización.

Monitorear

Los directores deben monitorear las inversiones en TI, para asegurar que proporcionan las capacidades requeridas.

Los directores deben monitorear el grado en que su organización y proveedores mantienen la comprensión mutua de la intención de la organización en la adquisición de TI.

2.1.6.6.5. Principio 4: Rendimiento

Evaluar

Los directores deben evaluar los medios propuestos por los administradores para asegurar que apoyarán los procesos de negocio con la capacidad y competencia requerida. Estas propuestas deben abordar el mantenimiento normal del negocio y el tratamiento del riesgo asociado con el uso de las TI.

Los directores deben evaluar los riesgos en la operación continua del negocio derivados de las actividades de TI.

Los directores deben evaluar los riesgos para la integridad de la información y la protección de los activos de TI, incluida la propiedad intelectual asociada y memoria organizacional.

Los directores deben evaluar las opciones para asegurar decisiones eficaces y oportunas sobreuso de TI en apoyo de los objetivos de negocio.

Los directores deben evaluar regularmente la eficacia y el rendimiento del sistema de organización que interviene en la Gobernabilidad de TI.

Dirigir

Los directores deben garantizar la asignación de recursos suficientes para que cumpla con las necesidades de la organización, de acuerdo con las prioridades acordadas y las limitaciones presupuestarias.

Los directores deben orientar a los responsables a fin de garantizar que TI soporta el negocio, cuando es requerido por razones de negocios, con datos correctos y actualizados que se protegen de la pérdida o mal uso.

Monitorear

Los directores deben monitorear en qué medida TI, es compatible con el negocio.

Los directores deben monitorear el grado en que la asignación de recursos y presupuestos se priorizan de acuerdo con los objetivos de negocio.

Los directores deben monitorear el grado en que las políticas, como la exactitud de los datos y el uso eficiente de TI, se siguen correctamente.

2.1.6.6.6. Principio 5: Conformidad

Evaluar

Los directores deben evaluar regularmente el grado en que satisface las obligaciones (regulatorias, legales, leyes comunes, contratos), políticas internas, normas y directrices profesionales.

Los directores deben evaluar periódicamente el cumplimiento interno de la organización de su sistema de gobernanza de la TI.

Dirigir

Los directores deben dirigir a los responsables de establecer mecanismos regulares y rutinarios para asegurar que el uso de las TI cumple con las obligaciones pertinentes (regulatorias, legales, leyes comunes, contratos), normas y directrices.

Los directores deben ordenar que las políticas se establezcan y se aplican para permitir que la organización cumpla con sus obligaciones internas en el uso de las TI.

Los directores deben ordenar que el personal de TI, sigan las directrices pertinentes para la conducta profesional y el desarrollo.

Los directores deben dirigir que todas las acciones relacionadas con TI sean éticas.

Monitorear

Los directores de TI deben vigilar el cumplimiento y la conformidad a través de la presentación de informes y auditorías apropiadas, asegurando que las revisiones sean oportunas, integrales y adecuadas para la evaluación del grado de satisfacción de la empresa.

Los directores deben monitorear las actividades de TI, incluyendo la eliminación de los activos y datos, para asegurar que el medio ambiente, la privacidad, la gestión estratégica del conocimiento, la preservación de la memoria de la organización y otras obligaciones pertinentes se cumplen.

2.1.6.6.7. Principio 6: Comportamiento Humano

Evaluar

Los directores deben evaluar las actividades de TI para asegurar que los comportamientos humanos son identificados y considerados adecuadamente.

Dirigir

Los directores deben dirigir las actividades de TI a fin de que sean consistentes con el comportamiento humano identificado.

Los directores deben ordenar que los riesgos, oportunidades, problemas y preocupaciones puedan ser identificados y reportados por cualquier persona en cualquier momento. Estos riesgos deben gestionarse de acuerdo con las políticas y procedimientos publicados y escalados a los que toman las decisiones pertinentes.

Monitorear

Los directores deben monitorear las actividades de TI para asegurar que los comportamientos humanos identificados siguen siendo pertinentes y se da adecuada atención a los mismos.

Los directores deben monitorear las prácticas de trabajo para asegurarse de que son compatibles con el uso adecuado de las TI.

3. CONCLUSIONES

- El uso de la tecnología en las empresas hoy en día es fundamental para lograr estabilidad y seguridad en la información es importante que las organizaciones empiecen a evaluar el impacto potencial de la norma y decidir si deberían solicitar la certificación ya que los sistemas de información son de gran utilidad para cualquier empresa, al contar con lineamientos de estandarización ISO 20000 ayuda a proporcionar servicios a sus clientes con un nivel aceptable de calidad, además ayuda al mejoramiento de la eficacia, fiabilidad, y consistencia de sus servicios de TI los cuales impactan directamente a los costos de la organización.

- Existe un gran reto en la gestión de la seguridad de la información con la ISO 27001:2013 y los conceptos que se debe reforzar son: Partes interesadas, Liderazgo, Sensibilización, Comunicación, Capacidades, Propietario del riesgo, Activos, Gestión de Riesgos y Oportunidades, entre otros.

- Las empresas que han realizado el esfuerzo de implementar la ISO 27001:2005, deben tomar estrategias para alinear su implementación a la ISO 27001:2013.

- Algunos podrían considerar que apegarse a este tipo de estándares es en cierta forma costosa y complicada, pero en realidad resulta mucho más caros sufrir las consecuencias que suele traer la falta de seguridad en un importante sistema de información.

- El hecho de cumplir a cabalidad con el Estándar Internacional ISO/IEC 27002 no garantiza al 100% que no se tendrán problemas de seguridad, pues la seguridad al 100% no existe. Lo que sí se logra es minimizar al máximo las probabilidades de sufrir impactos negativos y pérdidas originados por la falta de seguridad.

- La adopción de la norma ISO 17799 presenta múltiples ventajas para la organización, entre ellas el primer paso para una certificación ISO 27001, pero ni la adopción de la norma ISO 17799, ni la certificación garantizan la inmunidad de la organización frente a problemas de seguridad.

- Hay que hacer análisis periódicos de los Riesgos y monitorear continuamente la situación.

- La seguridad no es un tema de un día ni un tema exclusivo del departamento de TI. Hay que prepararse para entender la norma y avanzar en el seguimiento de las recomendaciones establecidas

- Este documento proporciona una idea bastante clara de cómo se debe trabajar en materia de seguridad de tecnologías de información al apegarse a un Estándar Internacional (y por lo tanto mundialmente aceptado y conocido) como lo es el ISO/IEC 27002.

- Muchos de los aspectos resaltados por este Estándar son aspectos generales que muchas organizaciones los toman en cuenta aún sin tener el certificado ISO/IEC 27002; sin embargo existen muchas deficiencias en la gran mayoría de organizaciones en materia de seguridad.

- Algunos podrían considerar que apegarse a este tipo de estándares es en cierta forma costosa y complicada, pero en realidad resulta mucho más caros sufrir las consecuencias que suele traer la falta de seguridad en un importante sistema de información.

- El hecho de cumplir a cabalidad con el Estándar Internacional ISO/IEC 27002 no garantiza al 100% que no se tendrán problemas de seguridad, pues la seguridad al 100% no existe. Lo que sí se logra es minimizar al máximo las probabilidades de sufrir impactos negativos y pérdidas originados por la falta de seguridad.

- Este documento proporciona una idea bastante clara de cómo se debe trabajar en materia de seguridad de tecnologías de información al apegarse a un Estándar Internacional (y por lo tanto mundialmente aceptado y conocido) como lo es el ISO/IEC 27002.

3.1. RECOMENDACIONES

- Se recomienda implementar el Estándar Internacional ISO/IEC 27002 a la mayor brevedad posible en todas las empresas, o de no ser posible (por aspectos económicos, de infraestructura, etc.), por lo menos estudiar el documento oficial de este Estándar y estar conocedores de todos los elementos que se pueden implementar y de cómo esto podría beneficiar y minimizar la posibilidad de problemas por falta de seguridad.

- Tener claro, como ya se dijo, que la seguridad al 100% no existe pero que sí se puede maximizar la seguridad y minimizar los riesgos por falta de seguridad.

- De ser posible, se debería considerar adquirir la certificación de este Estándar Internacional, pues esto representa un gran activo no sólo por los beneficios que de por sí trae el tener excelentes mecanismos de seguridad, sino también por el prestigio de contar con certificaciones internacionales de calidad.

- Se recomienda también tener un equipo de analistas que evalúen las condiciones particulares de una organización, pues cada caso es único, y lo que a uno le funcionó, a otro podría no funcionarle debido a los aspectos particulares de cada empresa. Por esa razón, se debe estudiar cada caso en concreto, aunque nunca está de más aprender de los errores o del éxito de otros.

- Considerar adquirir la certificación de este Estándar Internacional, pues esto representa un gran activo no sólo por los beneficios que de por sí trae el tener excelentes mecanismos de seguridad, sino también por el prestigio de contar con certificaciones internacionales de calidad.

- Tener un equipo de analistas que evalúen las condiciones particulares de una organización, pues cada caso es único, y lo que a uno le funcionó, a otro podría no funcionarle debido a los aspectos particulares de cada empresa. Por esa razón, se debe estudiar cada caso en concreto, aunque nunca está de más aprender de los errores o del éxito de otros.

4. GLOSARIO DE TÉRMINOS

- **Activo:** cualquier cosa que tenga valor para la organización.

- **Aceptable:** Cumplir con las expectativas de las partes interesadas que son capaces de ser mostradas como razonables o merecidas

- **Administración:** El sistema de controles y procesos requerido para alcanzar los objetivos estratégicos establecidos por el órgano rector de la organización. La administración está sujeta a la orientación política y de control establecidos a través de la gestión empresarial.

- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** consiste en tomar medidas adecuadas para adquirir nuevos sistemas (no aceptar sistemas que no cumplan con los requisitos de calidad adecuados), haciendo también un eficiente desarrollo y mantenimiento de los sistemas.

- **Amenaza:** una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.

- **Análisis de riesgo:** uso sistemático de la información para identificar las fuentes y calcular el riesgo.

- **Aspectos organizativos de la seguridad de la información:** cómo se trabajará en la seguridad de la información organizativamente, tanto de manera interna (empleados o personal de la organización) como de forma externa o con respecto a terceros (clientes, proveedores, etc.)

- **Control:** medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida.

- **Control de acceso:** deben existir medidas adecuadas que controlen el acceso a determinada información, únicamente a las personas que están autorizadas para hacerlo, utilizando autenticaciones, contraseñas, y métodos seguros para controlar el acceso a la información.

- **Criptografía:** es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.

- **Competente:** Tener la combinación de conocimientos, habilidades formales e informales, la formación, la experiencia y los atributos de comportamiento necesarios para realizar una tarea o función.

- **Comportamiento Humano:** La comprensión de las interacciones entre los seres humanos y otros elementos de un sistema con la intención de garantizar el bienestar y el rendimiento de los sistemas. El comportamiento humano incluye la cultura, las necesidades y aspiraciones de las personas como individuos y como grupos.

- **Confidencialidad:** La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados. (ISO/IEC 13335-1:2004)

- **Cumplimiento:** debe darse el debido cumplimiento a los requisitos legales, como derechos de propiedad intelectual, derecho a la confidencialidad de cierta información, control de auditorías, etc.

- **Director:** Miembro del máximo órgano de gobierno de una organización. Incluye propietarios, miembros de la junta, socios, directivos o similares, y los funcionarios autorizados por la legislación o regulación.

- **Disponibilidad:** La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada. (ISO/IEC 13335-1:2004)
- **Electrotecnia:** es ciencia que estudia las aplicaciones técnicas de la electricidad.

- **El uso de TI:** La planificación, diseño, desarrollo, implementación, operación, administración yaplicación de TI para satisfacer las necesidades de la empresa. Incluye tanto la demanda y la oferta, los servicios de TI por las unidades internas de negocio, unidades especializadas de TI o proveedores externos y los servicios públicos (como los que proporcionan el software como servicios).

- **Evaluación del riesgo**: proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.

- **Evaluación de los riesgos de de seguridad:** se deben identificar, cuantificar y priorizar los riesgos.

- **Evento de seguridad de la información:** Ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

- **Gestión de comunicaciones y operaciones:** asegurar la operación correcta de cada uno de los procesos, incluyendo las comunicaciones y operaciones que se dan en la organización. Esto también incluye la separación entre los ambientes de desarrollo, de prueba y de operación, para evitar problemas operacionales.

- **Gestión de incidentes en la seguridad de la información:** los incidentes se pueden dar tarde o temprano, y la organización debe contar con registros y bitácoras para identificar a los causantes y responsables de los incidentes, recopilar evidencias, aprender de los errores para no volverlos a cometer, etc.

- **Gestión de la continuidad del negocio:** se deben tener planes y medidas para hacerle frente a los incidentes, de modo que el negocio pueda continuar en marcha gracias a medidas alternativas para que un incidente no detenga las operaciones por tiempos prolongados, que no se pierda información, que no se estanquen o detengan las ventas o negocios, etc.

- **Gobierno Corporativo:** El sistema por el cual las organizaciones son dirigidas y controladas.

- **Incidente de seguridad de la información:** un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

- **IEC:** International Electrotechnical Commission.

- **ISO:** International Organization for Standardization.
- **Lineamiento: descripción;** que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas.

- **Medios de procesamiento de la información:** cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

- **Métrica:** es una metodología de planificación, desarrollo y mantenimiento de sistemas de información.

- **Política:** intención y dirección general expresada formalmente por la gerencia.

- **Política de seguridad:** deben haber políticas organizacionales claras y bien definidas que regulen el trabajo, que se estará realizando en materia de seguridad de la información.

- **Profundidad:** El esfuerzo es mayor porque aumenta el nivel de detalle de la implementación y el diseño.

- **Rigor:** El esfuerzo es mayor porque se aplica una forma más estructurada y formal.

- **Riesgo:** combinación de la probabilidad de un evento y su ocurrencia.

- **Riesgo residual:** El riesgo remanente después del tratamiento del riesgo. (ISO/IEC Guía 73:2002)

- **Seguridad de la información:** preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-reputación y confiabilidad.

- **Seguridad ligada a los recursos humanos:** especificar las responsabilidades del personal o recursos humanos de una organización, así como los límites que cada uno de ellos tiene con respecto al acceso y manipulación de la información.

- **Seguridad física y ambiental:** consiste en tener una infraestructura física (instalaciones) y ambiental (temperaturas adecuadas, condiciones ideales de operación ideales) adecuadas de modo que no pongan en riesgo la seguridad de la información.

- **Tercera persona:** persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión.

- **Tratamiento del riesgo:** proceso de selección e implementación de medidas para modificar el riesgo.

- **Tecnología de la Información (IT):** Recursos necesarios para adquirir, procesar, almacenar y difundir información. Esta término también incluye "Tecnología de la Comunicación (TC)" y el término compuesto "Tecnología de Información y Comunicación (TIC)".

- **Vulnerabilidad:** la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

- **Contingencias:** Posibilidad de que una cosa suceda o no suceda. Cosa que puede suceder o no suceder.

.

- **Riesgo:** Posibilidad de que ocurra un peligro. Cada uno de los diferentes daños que cubre un seguro: el seguro no nos cubre el riesgo de inundación.

- **Derivaciones:** Hecho o acontecimiento que sigue o resulta de otro: las derivaciones de una enfermedad. consecuencia. Procedimiento para formar palabras nuevas a partir de otra ya existente, mediante la adición, supresión o intercambio de un afijo o morfema derivativo: la palabra "descansar´´ está formada por derivación.

  Separación de una parte de un todo para dirigirla a otra parte: han hecho una derivación para llevar el agua del río a la acequia.

- **Infalibilidad absoluta:** Calidad de infalible. Aserción hecha en tono de seguridad.

BIBLIOGRAFÍA

- Chamorro López, José Alejandro. “Modelo para la evaluación en seguridad informática a productos software, basado en el estándar ISO/IEC 15408 Common Criteria”. 2011

- Entrevista realizada a : Alfonso Ramírez, Director General de VMWARE para España por Ángel González, publicado: 11 de Mayo de 2007

- www.uoc.edu/rusc por: Ángel H. Facundo (consultor Unesco). publicado: Noviembre de 2004

- http://seguridad-de-la-informacion.blogspot.com/2009/04/iso-15408-y-el-dni-e-pp-para-el.html

- http://www.slideshare.net/dianadplc/importancia-del-tecnologa-e-informatica

- Basalla, G. (1991), La evolución de la tecnología. Barcelona: Editorial Critica.

- De Gortari, E. (1979), Indagación crítica de la ciencia y la tecnología. Buenos Aires: Editorial Grijalbo.

- FERNÁNDEZ, C. M. (2012). La norma ISO 27001 del Sistema de Gestión de la Garantía de la Seguridad de la Información. Seguridad y Salud, 5.

- Martínez, E., Albornoz, M. (eds.) (1998), Indicadores de ciencia y tecnología: estado del arte y perspectivas. Caracas: Editorial Nueva Sociedad.
- Montoya., J. (s.f.). Recuperado el 25 de JULIO de 2015, de http://jaimemontoya.com/systemsproductiontechniques/isoiec27002a.php

- NSTISSI No. 4009. (January 2000). National Information Systems Security (INFOSEC) Glossary,.

- Estándares básicos de competencias en ciencias naturales y ciencias sociales. Serie Guías No. 7. Bogotá.

- Romero, I. V. (s.f.). Auditorias de Sistemas.

- Romo Villafuerte, D., & Valarezo Constante, J. (2012). ANÁLISIS E IMPLEMENTACIÓN DE LA NORMA ISO 27002 PARA EL DEPARTAMENTO DE SISTEMAS DE LA UNIVERSIDAD. Guayaquil: Universidad Salesiana.

- www.itcio.es/virtualizacion/entrevistas/1004346010102/90-servidores-empresas-solo-utilizado-al-6-7.1.html

- www.enriquedans.com/2008/04/la-tecnologia-se-vuelve-verde-articulo-en-capital
- http://www.eduteka.org/
- http://cnets.iste.org/
- http://learndev.org
- http://www.iteaconnect.org/
- http://www.somece.org.mx/
- ISO/IEC 15408 Common Criteria (II) http://auditoriasi.blogspot.com/2010/01/isoiec-15408-common-criteria-ii.html
- ISO/IEC 15408-1:2009 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341
- ISO/IEC 38500:2008 Corporate governance of informationtechnology.
- Freely Available Standards http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
- Publications http://www.commoncriteriaportal.org/cc/
- Criterios de Evaluación de la Seguridad de TI https://prezi.com/l_9hp_kkll56/isoiec-15408-evaluation-criteria-for-itsecurity/
- http://unicda-ti.blogspot.com/2011/08/importancia-de-la-norma-iso-27001.html
- ISO/IEC 17799:2005, Documentación– International standard book numbering (ISBN) International Organization for Standarization. About ISO. Extraído el 1 de octubre, 2008, de http://www.iso.org/iso/about.htm
- International Organization for Standarization. Discover ISO. Extraído el 1 de octubre, 2008, de http://www.iso.org/iso/about/discover-iso_isos-name.htm

- IEC. IEC History. Extraído el 1 de octubre, 2008, de http://www.iec.ch/about/history/
- Wikipedia. Electrotecnia. Extraído el 1 de octubre, 2008, de http://es.wikipedia.org/wiki/Electrotecnia
- Wikipedia. International Electrotechnical Commission. Extraído el 1 de octubre, 2008, de http://en.wikipedia.org/wiki/International_Electrotechnical_Commission
- Wikipedia. IEC JTC1. Extraído el 1 de octubre, 2008, de http://en.wikipedia.org/wiki/ISO/IEC_JTC1
- Wikipedia. Métrica. Extraído el 1 de octubre, 2008, de http://es.wikipedia.org/wiki/M%C3%89TRICA
- Wikipedia. Criptografía. Extraído el 1 de octubre, 2008, de http://es.wikipedia.org/wiki/Criptograf%C3%ADa
- http://www.monografias.com/trabajos67/estandar-internacional/estandar-internacional2.shtml#ixzz2bienFP7b
- http://peritoit.com/2012/07/23/norma-isoiec-15408-common-criteria/
- Hector Gonzales. Extraído el 7 de octubre , 2014, http://www.eumed.net/ce/2010a/hdgr.htm
- DNV.GL. http://www.dnvba.com/es/Certificacion/Pages/
- Slideshare, http://es.slideshare.net/hperez-ti/iso-20000-18944295
- https://es.wikipedia.org/.../Organización_Internacional_de_Normalización.
- https://es.wikipedia.org/wiki/ISO/IEC_20000
- www.bvindecopi.gob.pe/normas/isoiec17799.pdf
- www.shutdown.es/ISO17799.pdf.