ISBN 978-9942-8679-3-3

UNIVERSIDAD TECNICA DE BABAHOYO

# METODOLOGÍA PARA ANÁLISIS DE RIESGO DE INFORMACIÓN APOYADO EN ISO 27005

**Autores:**
**Mejía Viteri, José T.**
**Gonzáles Valero, María I.**
**España León, Ángel R.**

**Metodología para análisis de riesgo de información apoyado en ISO 27005.**

**Autores:**

**José Teodoro Mejía Viteri**
**María Isabel Gonzáles Valero**
**Ángel Rafael España León**

## Indice

# INTRODUCCIÓN.

Hoy en día la informática es la columna vertebral de las empresas públicas y privadas, es tan crítico tener un departamento de Tecnologías de la Información y comunicación, que provea servicios, tales como páginas web, control en los accesos a la información, y software que funcionan a nivel LAN y WAN, esto lleva a que se deba asegurar la disponibilidad y la seguridad de la misma, tanto así que el bien más cotizado por las empresas es la información, hoy en día se escucha mucho que los hackers se apropian de la información de los clientes de las empresas, solicitando cuantiosas cantidades de dinero por esta, y se hace necesario poseer una infraestructura que cumpla con los más altos estándares en cuanto a seguridad, integridad y confidencialidad.

El aprovechamiento ilícito de las vulnerabilidades en la seguridad de los sistemas y ataques informáticos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de conocimientos en informática, han dado lugar a la generación de conductas ilícitas susceptibles de ser sancionadas por el derecho penal a aquellas personas que hacen el uso indebido de cualquier medio informático, los delitos informáticos pueden alterar, afectar, destruir, dañar o perjudicar a los, sistemas, procesos, infraestructura tecnológica e información en general, afectada por métodos que comprometen la confidencialidad, integridad y disponibilidad de la información de las personas, empresas y/u organizaciones.

La importancia que se deben plantear las empresas al momento de implementar medidas de seguridad sobre accesos y hurto de información debe enfocarse a través de normativas que apoyen la implementación de controles .Hoy en día el activo más valioso de una empresa es la información, por lo

tanto en el texto hace mucho énfasis a la implementación de las normas ISO 27001 para que las empresas tengan cierto grado de confidencialidad y controles de acceso.

Las políticas de seguridad informática fijan los mecanismos y procedimientos que debe adoptar el departamento de Tecnologías de toda Institución para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse "a medida" para así recoger las características propias de cada departamento. No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se debe proteger y el porqué de ello, por lo que pueden tomarse como una forma de comunicación entre los operadores y los directores. De acuerdo con lo anterior, el aplicar una auditoria de seguridad informática requiere un alto compromiso de los principales directivos de la empresa, explotar las destrezas, habilidades y experiencia técnica de los usuarios; detectar fallas, debilidades, y revisiones periódicas que permitan actualizar dichas políticas en función del dinámico ambiente que rodea las organizaciones modernas.

En el artículo científico del magister Carlos Manuel Fernández Sánchez docente de la Universidad Alcalá de Henares Madrid titulado La norma ISO 27001 del sistema de Gestión de la Garantía de Confidencialidad y garantía de la seguridad de la Información indica que la norma ISO 27001 tiene relación con otras normas que conforman el modelo de gobierno y gestión de las Tecnologías de la Información y Comunicación (TIC) desarrollado por AENOR, basado en estándares aceptados mundialmente." Se puede decir que, gracias a este modelo, el Centro de Proceso de Datos y el resto de la

organización comienzan hablar el mismo lenguaje y a interconectarse de manera más natural y eficiente", (Fernández Carlos, 2013).

Es por todos los peligros y razones detallados es que la contraloría general del estado para los organismo del sector público acopla a un marco de trabajo de procesos de tecnología que aseguren la transparencia y el control; crea las Normas de Control Interno donde existe una sección dedicada a las Tecnologías de la Información, que contiene controles a los accesos indebidos, procesos, proyectos y planes que se deben ejecutar para dar cumplimiento a la norma sin embargo en la sección de Mantenimiento y Control de Infraestructura Tecnológica hace referencia y establece la importancia del análisis de riesgo, para no comprometer la integridad, confidencialidad y disponibilidad en producción de los servicios proporcionados por tecnologías, sin embargo no existe una metodología o estructura para su realización.

Por lo tanto el libro desarrolla una metodología basada en ISO 27005 que ayude al cálculo de este riesgo en la infraestructura tecnológica que se vuelve imperante, y de esta manera contribuir a la gestión de la seguridad de la información y de los servicios, además de ayudar a la correcta aplicación de Controles que ayuden al cumplimiento de las Normas de control interno.

**Capitulo 1**

# Introducción a la Seguridad de la Información.

**1.1 Proceso de gestión Administrativa en Informática.**

**1.2 Importancia de la información.**

**1.3 Seguridad de la Información.**

**1. 4 Política de Seguridad.**

**1.5 Sistema de gestión de la seguridad.**

**1.6 Normas.**

## 1.1 Proceso de gestión Administrativa en Informática.

"La administración es el proceso de planear, organizar, dirigir y controlar el uso de los recursos para lograr los objetivos organizacionales" (Chiavenato Idalberto, 2004).

Tomando en cuenta esta definición los procesos de gestión Administrativa han evolucionado desde que se introdujo el equipo de cómputo a las empresas, esto genero un cambio en el manejo de la información, cambios que se produjeron en toda la estructura administrativa, y llevo a estructurar software para la automatización de los procesos en las diferentes áreas de las empresas generando grandes cantidades de información que ayuda a la gerencia en la toma de decisiones.

Pero al mismo tiempo surgió la necesidad de crear un área que administre, gestione esta información, y brinde asesoría sobre tecnología que se debe adquirir para mejorar estos procesos, llevando a los directivos a ver la información como un medio de ejercer el control y mejorar la gestión empresarial, estando en equipos de cómputos lleva a la necesidad que esta información no sea sustraída, sea confiable, integra y que esté disponible 24 horas al día y 7 días de la semana, dando origen a los sistemas de gestión de la seguridad de la información, que está sustentada en normas y manuales que ayudan a la administración, gestión y asegurarla cuando se traslade de un a lugar a otro.

### Datos.

"Los datos de nuestra empresa son exclusivamente suyos. Si desaparecen, la empresa no puede funcionar con normalidad. Si llegan a manos de la

competencia, la estrategia empresarial y el futuro de la compañía están en riesgo" (Roa José, 2013).

Las empresas necesitan organizar y asegurar la información, con la nueva tendencia de cero papeles, todos los documentos se encuentran informatizados, y son puestos en circulación al interior como al exterior de la empresa, es así que las empresas deben invertir en las infraestructuras tecnológicas para mantener niveles de seguridad elevados y evitar el daño por software malicioso, y no tenerla solamente almacenada en los equipos que la generan si no en lugares remotos, dando origen al almacenamiento distribuido que permite disponer al usuario de la información en diferentes equipos que brinda un nivel de seguridad elevado porque la información no se encuentra en un solo lugar evitando la perdida por daños físicos del hardware.

La importancia del cifrado de la información al momento de ser trasladada a través de la red LAN y la WAN, es de vital importancia para evitar modificaciones y hurto de la información por esto antes de poner los sitios web en funcionamiento especialmente los que llevan transacciones en línea de debe activar el protocolo seguro de transferencia de hipertexto (HTTPS), este permite cifrar utilizando TLS y SSL proporcionando un canal cifrado más apropiado para el viaje de información a través de la web.

### 1.2 Importancia de la información.

La información es un vehículo de transmisión de conocimiento, ha constituido un factor esencial en el avance de la sociedad." El desarrollo en todas las disciplinas se caracteriza, entre otros factores, por una aceleración en la recopilación, almacenamiento, procesamiento y transmisión de información, lo

que ha generado diversos efectos al constituir un elemento estratégico para el desarrollo integral de la sociedad" (Ileana R. Sánchez Alfonso, 2013).Para lograr este objetivo se requiere de un personal capacitado y comprometido con la importancia del desarrollo de la información de todo tipo que surge de las instituciones sean están públicas o privadas y del beneficio que esta información puede generar para la comunidad nacional como internacional.

**Seguridad.**

"En el mundo de la seguridad de la información e informática, es habitual manejar una terminología específica (activos, vulnerabilidades, amenazas, ataques, riesgos, impacto, desastre, contingencias, etc.) " (Gascó Gema, 2011).

Y se define las siguientes terminologías que a continuación se detallan:

**Activos**.

Se define como cualquier bien sea este informático o no, el cual permite a las instituciones públicas y privadas alcanzar sus objetivos amparados en sus Planes Operativos Anuales (POA), en el caso de las públicas , y de los planes de fortalecimiento en el caso de las privadas, es decir todo que requiere ser asegurado contra algún percance, tanto así que estas optan por adquirir seguros que permitan proteger los bienes contra las amenazas más comunes, por ejemplo de activos podemos mencionar hardware, software, personas, muebles y oficinas etc.

Por lo tanto se concluye que la seguridad informática tiene por objeto la identificación de los bienes informáticos que necesitan ser asegurados, analiza las principales amenazas para establecer los mecanismos necesarios para

protegerlos, desde el punto de vista de la informática podemos establecer los siguientes activos:

**Información:** Todo elemento almacenado en cualquier medio de soporte de información que sea de la empresa por ejemplo. Cd, DVD, discos rígidos etc. y esta puede ser manuales de usuario reglamentos, normas.

**Software:** Son programas de los equipos como office y sistemas operativos aplicaciones que se hayan adquirido por la empresa o software libre necesario, para la automatización de los procesos en las empresas.

**Físicos:** En cualquier infraestructura tecnológica existe un data center donde se encuentra la columna vertebral de nuestra infraestructura tecnológica, y los elementos que se consideran activos físicos serían los Swich, router, servidores, armarios y demás elementos.

**Personal de la organización** Toda persona que utilice la estructura tecnológica y de comunicación para el manejo de la información.

**Vulnerabilidades.**

Se considera vulnerabilidad a cualquier debilidad que se pueda presentar en la infraestructura tecnológica que lleve a un mal funcionamiento de esta. Estas debilidades también son conocidas como agujeros de seguridad, que por lo general son ocasionados por fallas en la programación de algún software adquirido por la empresa a fallos que tienen los sistemas operativos y no son actualizados. Un ejemplo de estos fallos es no utilizar firewall, no tener soporte de energía lo que llevaría que los servidores se apaguen, también no tener algún software antivirus, etc.

**Amenazas.**

Es cualquier actividad que atente con el funcionamiento de nuestra infraestructura tecnológica. "Aunque hay amenazas que afectan a los sistemas de forma involuntaria, por ejemplo, un desastre natural, en la mayoría de casos es necesaria una intención de producir daño. Las amenazas se suelen dividir en pasivas y activas" (Ileana R. Sánchez Alfonso, 2013).

**1.3 Seguridad de la Información.**

En el año 1992, el Consejo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), adoptó una importante recomendación relativa a las líneas directrices para la seguridad de los sistemas de información, en la que encontramos que: "La seguridad de los sistemas de información tiene por objetivo proteger los intereses de los que cuentan con sistemas de información contra los perjuicios imputables a defectos de DISPONIBILIDAD, de CONFIDENCIALIDAD y de INTEGRIDAD" (Fernández Carlos y Piattini Mario,2012).

El valor que hoy en día las empresas dan a la información es fundamental, que en la web encontramos artículos y noticias de como la fuga de información puede significar la banca rota de una empresa.

**Integridad.**

"La integridad es un principio básico de la seguridad informática que consiste en garantizar que la información solo pueda ser alterada por las personas autorizadas o usuarios legítimos, independientemente de si esa modificación se produce de forma intencionada o no" (Ramada Davis, Onrubia Ramón, 2011).

La opinión de Ramada Davis hace referencia a que la integridad busca mantener los datos sin modificaciones no autorizadas. La vulneración de la integridad tiene distinto significado según se produzca en un equipo o en una red informática:

**Equipo de Cómputo**. Esta violación se produce cuando un usuario no legítimo modifica la información del sistema.

**Redes Informáticas**. Existe violación de la integridad cuando una persona de la red se hace pasar por intermediario de la misma esto quiere decir que se pone en medio de los equipos que tienen una comunicación entre sí (ataques man-in-the-middle ).

**Confidencialidad.**

La confidencialidad es otro de los principios básicos de la seguridad informática que debe garantizar que la información sea extraída e interpretada solo por el usuario de destino.

"Un sistema de confidencialidad tiene éxito cuando un usuario externo no puede extraer información de una transmisión de información que hayan realizado dos o más interlocutores en un sistema de información". (Romero García, 2012).

La vulneración de la confidencialidad también afecta de forma diferente a equipos de cómputo y redes informáticas.

**Equipo de cómputo**.

Es cuando se consigue las contraseñas para iniciar sesión en un equipo y existen accesos a sus recursos. Un ejemplo sería la obtención de las claves de acceso.

**Redes Informáticas**.

Se vulnera la confidencialidad de una red cuando un atacante accede a los mensajes que circulan por ella sin tener autorización para ello.

**Disponibilidad.**

El tercer pilar básico de un sistema seguro, se da cuando los usuarios pueden acceder a la información en el momento adecuado por los usuarios que la requieren. La violación de la disponibilidad también se da de forma distinta en equipos y redes:

**Equipos informáticos**.

Se vulnera la disponibilidad de un equipo cuando los usuarios que tienen acceso a él no pueden utilizarlo. Por ejemplo, podría ser un virus que ha paralizado el sistema.

**Redes de comunicaciones**.

" Se produce un ataque contra la disponibilidad cuando se consigue que un recurso deje de estar disponible para otros usuarios que acceden a él a través de la red", (Ramada Davis, Onrubia Ramón, 2011).

"Para lograr niveles de confidencialidad, integridad y disponibilidad que la organización necesita la serie de normas ISO/IEC 27000, en UNE-ISO/IEC 27002:2009 añade que la seguridad puede abarcar además otras propiedades

como la autenticidad, la responsabilidad, la fiabilidad y el no repudio", (Ramón Jorge, 2011).

Existen diversos tipos de protección de la información que a continuación se detallan.

**Seguridad Lógica.**

Se encarga de proteger la parte lógica de un sistema informático (datos, aplicaciones y sistemas operativos). Uno de los medio más utilizados es la criptografía la cual es muy utilizada al momento de que la información fluye a través de la red.

**Seguridad Activa.**

Son medidas preventivas que se encargan de detectar y evitar cualquier incidente en los sistemas informáticos antes de que se produzca .Por ejemplo, utilización de contraseñas.

**Seguridad Pasiva.**

Son las medidas correctoras y comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad .Por ejemplo, las copias de seguridad.

**1. 4 Política de Seguridad.**

"Una política de seguridad constituye informar a los usuarios, trabajadores y personal de dirección, de los requisitos obligatorios para proteger los la información de la organización, debe especificar también los mecanismos a través de los cuales estos requisitos puedan ser conocidos", (Díaz Gabriel, 2014).

También se utiliza como base para auditar las infraestructuras tecnológicas, dando así lugar a la utilización de herramientas para auditar las empresas en cuanto a su funcionamiento y medidas contra algún tipo de amenaza o vulnerabilidad. Estas herramientas dan las pautas frente a las políticas de seguridad que puede y como debe utilizarse y que información puede viajar a través de la red.

**Aspectos físicos de la política de seguridad**.

"Cualquier política de seguridad debe tener en cuenta una serie de procedimientos relacionados con la seguridad física, tanto en el aspecto del control de acceso físico a equipos, como tener planes de contingencia y emergencia, de recuperación frente a desastres", (Díaz Gabriel, 2014).

Es importante mencionar que las empresas se preocupan mucho más del aseguramiento lógico de la información dejando a un lado la protección de la infraestructura física donde se encuentran alojados los equipos, siendo más fácil para un atacante sacar una copia de archivos de los servidores por la facilidad de acceso a lugar, también la seguridad contra los desastres naturales, como incendios, terremotos, disturbios etc.

**Aspectos lógicos de la política de seguridad**

Abarca las normas y procedimientos y se puede separar en normas básicas o fundamentales, como:

- Política de uso aceptable.
- Política de acceso remoto.
- Política de protección de la información.
- Política de seguridad perimetral,

- Política de protección anti-virus.
- Política de contraseñas.

### 1.5 Sistema de gestión de la seguridad.

En el ámbito de la empresa, la gestión supone la articulación y operación de los recursos necesarios para lograr los objetivos empresariales o de negocio previstos.

"Implantar un sistema de gestión, debe tenerse claro que se pretende, adónde se quiere llegar; es decir, los objetivos previstos. La naturaleza de estos objetivos será lo que identifique el sistema de gestión, en el caso de seguridad de la información". (Fernández Carlos, 2012).

La definición de un Sistema de Gestión de Seguridad de la Información (SGSI) según la Norma UNE-ISO/IEC 27001 , es: "parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información"(Álvarez Ana, Gómez Luis, 2012).

Aquí se define como dejar de trabajar de manera intuitiva es decir a comenzar a tomar el control de toda la infraestructura tecnológica y la información que se genera en toda la organización, además que nos permitirá conocer mejor nuestra empresa, en todos los ámbitos cómo funciona y que medidas implementar para que la situación mejore, considerando la ayuda de las normas internacionales para aseguramiento de la información.

### 1.6 Normas.

Son documentos aprobados por un organismo reconocido que establece normas y criterios para uso de las organizaciones .Establece las actividades para

cumplir condiciones mínimas que debe poseer un producto o servicio para que sirva para lo que fue destinado.

**Normalización.**

Es la actividad que tiene por objeto establecer, ante problemas reales o potenciales, disposiciones destinadas a usos comunes repetidos, con el fin de obtener un nivel de ordenamiento óptimo, en un contexto dado, que puede ser tecnológico, político o económico, (http://www.iram.org.ar,2012).

**Capitulo 2**

# Normativas para la seguridad de la Información.

**2.1 ITIL** (*Information Technology Infrastructure Library*).

**2.2 COBIT** (***Control Objectives for Information and related Technology*).**

**2.3 ISO** *(Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional).*

**2.4 ISO y la gestión de la seguridad.**

**2.5 Análisis de riesgos según ISO 27005 en la seguridad de la información**.

**2.6 Interrogantes para definir el valor del activo en cuanto confidencialidad integridad y disponibilidad.**

**2.7 Evaluación detallada de los riesgos en la seguridad de la Información.**

**2.8 Leyes y reglamentos de la legislación ecuatoriana sobre seguridad de la información.**

**2.9 Amenazas que está expuesta la información.**

**2.10 Plan de seguridad informática.**

## 2.11 Consideraciones ISO 27001 para el desarrollo del plan de seguridad informática.

### Normas de seguridad de la información.

Las normas de seguridad que más influyen en las empresas en el Ecuador son:

### 2.1 ITIL (Information Technology Infrastructure Library).

Es un conjunto de buenas prácticas destinadas a mejorar la gestión y provisión de servicios TI .Su objetivo es evitar los problemas asociados a los mismos y en caso de que estos ocurran ofrecer como actuar para que estos sean solucionados con el menor impacto y a la mayor brevedad posible. (Osiatisis, 2011).

ITIL se basa en su idea del ciclo de vida del servicio de Tecnología de la información (TI) .Muy brevemente, un servicio TI debe planificarse (fase de estrategia), diseñarse (fase de diseño), implementarse (fase de transición), operarse y mantenerse (fase de operación) y debe estar sujeto siempre al ciclo Plan Do Check Act (PDCA) (fase de mejora continua).

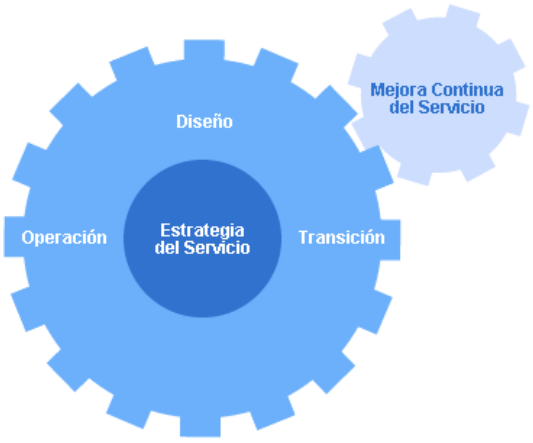


Gráfico 2.1 Ciclo de vida de ITIL

Fuente: Tomado de http://itilv3.osiatis.es

"ITIL es una aproximación muy sofisticada de todas las tareas a realizar para ofrecer y controlar servicios TI, pero en este caso teniendo en cuenta muchos más procesos, que cubren temas muy diversos" (HELAT.A, 2003). Para hacerse una idea basta la enumeración de algunos de los procesos más significativos:

- Gestión Financiera del servicio.
- Gestión de relaciones con el negocio.
- Gestión de niveles de servicio.
- Gestión del catálogo de servicios.
- Gestión del portfolio de servicios.
- Gestión de proveedores.
- Gestión de la disponibilidad.
- Gestión de la capacidad.
- Gestión de la seguridad
- Gestión de la continuidad.
- Gestión de los activos del servicio y de la configuración.
- Gestión de la entrega del servicio y su despliegue.
- Gestión del conocimiento del servicio.
- Gestión del cambio.
- Gestión de incidencias.
- Gestión de problemas en el servicio.
- Gestión de eventos.
- Gestión de accesos.

- Gestión de la mejora continua.

Todos los procesos de ITIL posee un sin número de actividades que utilizan datos de entrada y crean resultados de salida siempre alineados con los objetivos de los procesos. Los objetivos se fijan de manera cuantitativa y tienen asociados una serie de métricas que permiten implementar un ciclo PDCA continuo.

Es importante establecer que para llevar acabo cada proceso se necesita una serie de recursos y capacidades organizadas en funciones y son:

**Centro de servicio al usuario**. El cual se preocupa de garantizar que la continuidad, disponibilidad y calidad del servicio del usuario.

**Gestión Técnica.** La cual aporta las habilidades y los recursos necesarios para dar soporte a la fase de operación del servicio.

**Gestión de Aplicaciones.** Esta es responsable como su nombre lo indica de las aplicaciones que forman parte de la operación del servicio.

**Gestión de operaciones TI.** Es la unidad responsable del mantenimiento y la gestión continua de la infraestructura tecnológica TI.

Existen dos procesos ITIL especialmente significativos:

**El proceso de gestión de la seguridad.**

Este es responsable de las políticas de seguridad de los servicios que se encuentran en ejecución o que se vaya a implementar en la infraestructura TI y también de toda política de seguridad de la empresa.

ITIL hace mucho uso de la terminología y de los detalles de la norma ISO/IEC 27001, haciendo mucha referencia a la importancia de implantar un SGSI. Este proceso aparece en la fase de diseño del servicio.

**El proceso de Gestión de los accesos.**

"Es importante señalar que una organización no puede certificarse en ITIL, por no ser estándar sino un conjunto de buenas prácticas. Existen certificaciones individuales de mayor a menor nivel, permiten alcanzar una certificación de ITIL fundamentos, a Experto de ITIL "(Bernard.P, 2011).

ITIL se encuentra relacionado con algunas normas de Gestión de servicios TI como el estándar ISO/IEC 20000, que permite certificar un servicio como que cumple todo un conjunto de buenas prácticas de implementación de gestión de servicios, que van como en el caso de ITIL mucho más allá de la gestión de la seguridad. Como en el caso ya analizado de ISO/IEC 27001 e ISO/IEC 20000, que es solicitado por muchas empresas las cuales deben certificarse para poder entrar en la competencia de proveer servicios TI, en el país existen muy pocas compañías que poseen esta certificación.

## 2.2 COBIT (Control Objectives for Information and related Technology).

Es un marco de Gobierno de las tecnologías de la información donde se encuentran las mejores prácticas para las empresas, dirigidas al control y la supervisión, proporciona una serie de herramientas para los gerentes, pueden conectar los requerimientos de control con aspectos técnicos y de riesgo.

Como historia referencial de COBIT se puede decir que la primera versión apareció en 1996, la segunda en 1998 la tercera en el 2000 y la cuarta en 2005 y la 5 apareció en 2012.

COBIT se puede aplicar a toda la empresa a los sistemas de información, estaciones de trabajo computadores personales administradas por un conjunto de procesos que permiten la generación de información que ayuda a la empresa alcanzar sus objetivos propuestos.

La misión de COBIT es:

Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores Usuarios: La Gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control Los Usuarios Finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente. Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido. Los Responsables de TI: para identificar los controles que requieren en sus áreas (Rojas Soledad, 2009).

COBIT puede ser utilizado por algún responsable de un proceso del negocio que genere información y todos aquellos que tengan responsabilidades en los procesos TI en las empresas.

**Cobit y la gestión de la seguridad**.

"El principal valor de Cobit 5 es la gran diversidad de modelos y estándares a nivel global, resultado del trabajo de un gran grupo de practicantes de diversas regiones geográficas, quienes analizan y desarrollan en general estándares específicos para seguridad". (Salomón Rico, 2014).

COBIT se divide en tres niveles.

**Dominios** .Es la agrupación de procesos corresponden a una responsabilidad organizacional.

**Procesos.** Es una serie de actividades con delimitación o cortes de control.

**Actividades.** Acciones para obtener los resultados que siempre son medibles.

**Enfoque de Gobierno.**"El enfoque de gobierno extremo-a-extremo que es la base de COBIT 5 está representado en la figura, muestra los componentes clave de un sistema de gobierno Además del objetivo de gobierno, los otros elementos principales del enfoque de gobierno incluye catalizadores, alcance y roles, actividades y relaciones" (ISACA, 2012).

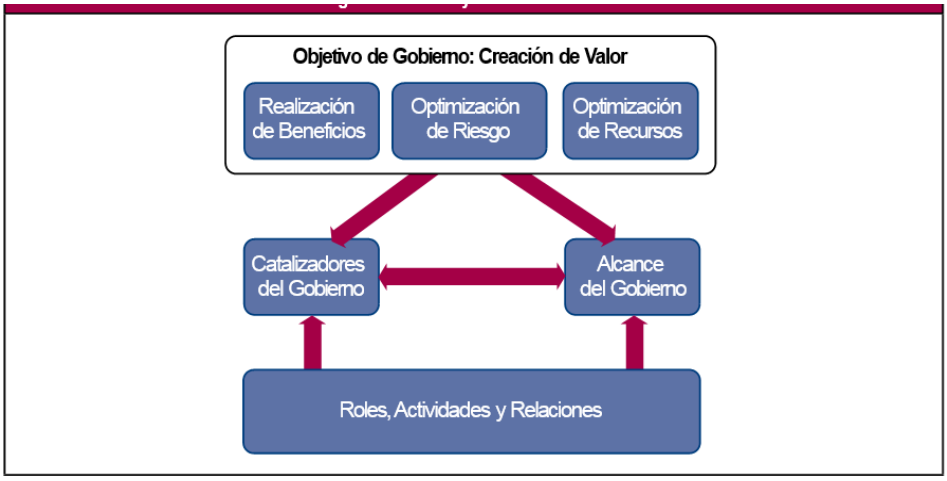


Gráfico 2.2 Gobierno y gestión de COBIT 5

Fuente: ISACA, Un marco de Negocio para el Gobierno y gestión de TI de la empresa

COBIT está diseñado para controlar y aplicar las buenas prácticas a nivel de todos los procesos de TI. Utiliza los Objetivos de Control de ISACA, mejorados con estándares específicos de tipo técnico, profesional, normativo e

industrial existentes y emergentes. Los objetivos de control están desarrollados para su aplicación en los sistemas de información en la empresa. Estos objetivos de control tienen en cuenta lo siguiente:

- Adecuación a los estándares y normativas legislativas y de hecho existentes que se aplican en el marco global, así como en los objetivos de control individuales.
- Revisión crítica de las diferentes actividades y tareas bajo los dominios de control y posibilitando la especificación de indicadores de prestaciones importantes (normas, reglas, etc.)
- Establecimiento de unas directrices y fundamentos para proporcionar investigación consistente sobre los temas de auditoría y control de TI.

## 2.3 ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional).

Es un sistema especializado para la normalización a nivel mundial. Los organismos que son miembros de ISO o IEC participan en el desarrollo de las normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo.

La Norma UNE-ISO/IEC 27002 establece las directrices y principios generales para el comienzo, la implementación, el mantenimiento y la mejora de la gestión de la seguridad de la información en una organización. Es un catálogo de buenas prácticas, obtenido a partir de la experiencia y colaboración de numerosos participantes, los cuales han alcanzado un consenso acerca de

los objetivos comúnmente aceptados para la gestión de la seguridad de la información (Gómez Luis, 2012).

A continuación se muestra en la gráfica a nivel macro lo que se debe establecer en las empresas para cumplir con las normas ISO 27000.


Gráfico 2.3 Estructura de ISO.

Fuente: ISO, Documentación oficial

**Establecimiento del SGSI**.

Para cumplir todos estos requerimientos la organización debe buscar los medios necesarios de acuerdo a su realidad y así mismo los recursos disponibles, además debe recopilarse mucha información sobre la organización como por ejemplo a que se dedica la organización, cuales son las necesidades de seguridad de acuerdo a su actividad, ámbito en el cual opera y los aspectos legales que regulan su actividad, estos requisitos en muchos casos no se encuentran definidos. La norma establece una serie de requisitos, que se detallan a continuación véase en la Grafico 1.4

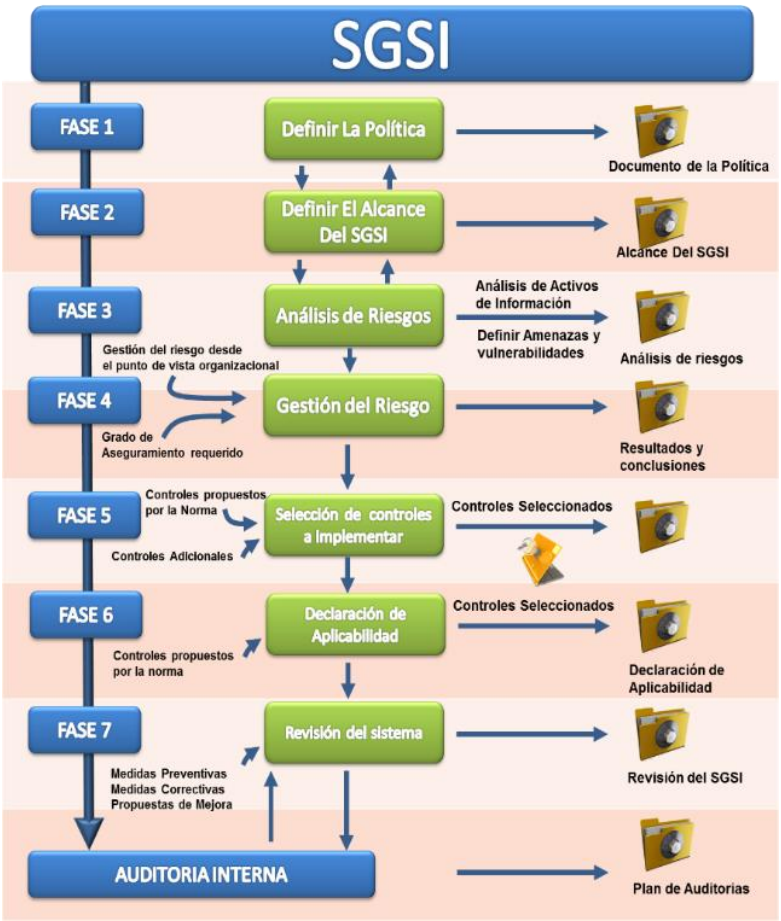


Gráfico 2.4 Sistema de Gestión de la seguridad informática

Fuente: http://www.normas-iso.com/iso-27001.

En las empresas no se debe comprometer recursos difíciles de conseguir, ya que estas saben todo lo que quieren asegurar, pero a su vez no tienen mecanismos para documentarlo y expresarlo.

"Hay que concretar esas necesidades que se perciben para poder comenzar el diseño del SGSI. Hay que ser realista con los recursos disponibles en cada momento y dimensionar el proyecto de acuerdo con las prioridades del negocio" (OECD, 2002).

### 2.4 ISO y la gestión de la seguridad.

ISO 27001 propone la seguridad de toda la información incluso si esta información es tratada en reuniones o si es información tratada del propio conocimiento y de experiencia de las personas de la empresa.

ISO hace mucho énfasis a la seguridad que existen normas para las diferentes etapas de la gestión de la seguridad de la información.

A continuación se detalla las normas ISO más importantes sobre la gestión de la seguridad de la información.

**ISO/IEC 27000**.Es un vocabulario estándar para el SGSI.

**ISO/IEC 27001.** Es la certificación para las organizaciones. Especifica los requisitos para la implantación del SGSI. La más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.

**ISO/IEC 27002.**Es un código de buenas prácticas para la gestión de seguridad de la información.

**ISO/IEC 27003.**Son directrices para la implementación de un SGSI.

**ISO/IEC 27004.**Son métricas para la gestión de seguridad de la información**.**

**ISO/IEC 27005.**Trata la gestión de riesgos en seguridad de la información.

**ISO/IEC 27006:2007.**Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información.

**ISO/IEC 27007.**Es una guía para auditar al SGSI.

**ISO/IEC 27799:2008.** Es una guía para implementar ISO/IEC 27002 en la industria de la salud**.**

**ISO/IEC 27035:2011.**Técnicas de Seguridad – Gestión de Incidentes de Seguridad: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

## 2.5 Análisis de riesgos según ISO 27005 en la seguridad de la información.

El procesos de aseguramiento de la información es un proceso que para establecer medidas en una empresa sea esta pública o privada se convierte en práctica engorrosa por lo que es necesario realizar un análisis de riesgo lo cual facilita este proceso.

Este análisis de riesgo es crucial en el desarrollo y operación de un plan de seguridad de la informática. El modelo de seguridad está basado en una identificación de sus activos todas las dependencias jerárquicas de estas, y las amenazas que pueden afectarlos, luego se realiza una estimación de impactos y se obtiene el riesgo de la organización.

El diagnostico de análisis de riesgo de la empresa es válido solo para ese momento y para darle seguimiento a las políticas, porque con el tiempo se van

adquiriendo nuevos activos por tanto existen nuevas amenazas que pueden afectarlos, es por esto que la empresa debe realizar continuamente un nuevo análisis de riesgo para mitigarlos y tener su información asegurada.

**Metodología para la estimación del riesgo.**

El análisis de riegos puede realizarse con diferentes grados de detalle depende de la criticidad de los activos involucrados, los tipos de vulnerabilidades presentes para cada uno de los activos, las amenazas detectadas por el departamento de tecnologías y otros incidentes ocurridos anteriormente.

El análisis de riesgo puede realizarse de manera cuantitativa, cualitativa y una mescla de ambas la selección depende del entorno de la empresa.

**Metodología cualitativa.**

Esta metodología es muy utilizada por su proceso dinámico e intuitivo se basa en una escala de atributos cualitativos y describen las consecuencias, por ejemplo alta, media baja. Una de las desventajas de esta metodología es subjetividad dentro de la escala establecida.

En el desarrollo de esta metodología se toman en cuenta cuatro parámetros principales: amenazas, vulnerabilidades que siempre están presentes en una red o sistema de información, el impacto asociado a una amenaza si ésta llegara a materializarse y las medidas o controles preventivos o correctivos.

**Metodología cuantitativa.**

"Implica realizar una recolección de datos, cálculos complejos, técnicas de modelamiento, etc. Se utiliza una escala con valores numéricos, a diferencia de la anterior que utilizaba una escala descriptiva, tanto para la evaluación de

probabilidades de ocurrencia como para sus consecuencias basándose en datos provenientes de varias fuentes" (ISO 27005, 2008).

El éxito de esta metodología depende de la exactitud de los valores cuantitativos que tienen los activos. Utiliza dos parámetros para la estimación del riesgo, la probabilidad de que el evento ocurra y una estimación del costo o las pérdidas en caso de que el evento sea positivo.

Una estimación cuantitativa del riesgo puede realizarse después de haber realizado una estimación cualitativa, sin embargo, cada tipo de metodología puede ser ejecutada por separado o combinarse y ser ejecutadas de forma simultánea.

## 2.6 Interrogantes para definir el valor del activo en cuanto confidencialidad integridad y disponibilidad.

"Los interrogantes a resolver con estos criterios de evaluación son: ¿Qué daño causaría a la Organización, el que la Información fuese conocida por quien no debe?, ¿Qué perjuicio causaría que el activo valorado estuviera dañado o suministrara información corrupta?, ¿Qué perjuicio causaría el no tener o poder usar el activo valorado?., ¿Qué niveles de Autenticidad y trazabilidad son requeridos para el manejo adecuado de la información?", (ISO 27005, 2008).

Los valores de los activos de los cuales dependen otros activos se pueden modificar de la siguiente manera:

- Si los valores de los activos dependientes (por ejemplo los datos) son menores o iguales al valor del activo considerado (por ejemplo el software), su valor permanece igual.
- Si los valores de los activos dependientes (por ejemplo, los datos)

son mayores, entonces el valor del activo considerado (por ejemplo, el software) se deberían incrementar de acuerdo con:

- el grado de dependencias;
- los valores de los otros activos.

**Evaluación del impacto.**

Cualquier incidente de seguridad puede tener influencia en uno de los activos en una parte realmente el impacto se lo relaciona directamente con el grado de éxito que tenga el incidente, existe una diferencia importante entre el valor del activo y el impacto resultante de un incidente. Se considera que el impacto tiene un efecto inmediato (operacional) o un efecto futuro (en el negocio) que incluye consecuencias financieras y de mercado.

El impacto inmediato (operacional) es directo o indirecto.

**Impacto directo.**

a) El valor financiero del reemplazo del activo perdido (o parte de este activo).
b) El costo de adquisición, configuración e instalación del activo nuevo o de su copia de soporte.
c) El costo de las operaciones suspendidas debido al incidente hasta que se restaure el servicio prestado por el (los) activo (s).
d) El impacto tiene como resultado una brecha en la seguridad de la información. Indirecto:
e) Costos de la oportunidad (nuevos recursos financieros necesarios para reemplazar o reparar un activo se podrían haber utilizado en otra parte).

f) El costo de las operaciones interrumpidas.
g) El potencial de la mala utilización de la información obtenida a través de una brecha en la seguridad.
h) Incumplimiento de las obligaciones estatutarias o reglamentarias.
i) Incumplimiento del código ético de conducta.

## 2.7 Evaluación detallada de los riesgos en la seguridad de la Información.

"Se pueden evaluar de varias maneras, incluyendo el uso de medidas cuantitativas, por ejemplo monetarias, y cualitativas o una combinación de ambas. Para evaluar la probabilidad de ocurrencia de una amenaza, se debería establecer el marco temporal en el cual el activo tendrá valor o necesitará protección", (ISO 27005, 2008). La probabilidad de ocurrencia de una amenaza específica está afectada por los siguientes aspectos:

- Lo atractivo que sea el activo, o el impacto posible aplicable cuando se toma en consideración una amenaza humana deliberada.
- La facilidad de conversión en recompensa de la explotación una vulnerabilidad del activo, aplicable cuando se toma en consideración una amenaza humana deliberada.
- Las capacidades técnicas del agente amenazador, aplicable a amenazas humanas deliberadas.
- La susceptibilidad de la vulnerabilidad a la explotación, aplicable tanto a vulnerabilidades técnicas como no técnicas.

## 2.8 Leyes y reglamentos de la legislación ecuatoriana sobre seguridad de la información.

**Esquema gubernamental de seguridad de la información.**

La secretaria de la Administración pública considerando que las Tecnologías de la Información se han convertido en una prioridad para brindar un mejor servicio al usuario, se vio en la necesidad de gestionar de forma eficiente y eficaz la seguridad de toda esta información generada, en las entidades públicas, emitió los Acuerdos Ministeriales No. 804 y No. 837, de 29 de julio y 19 de agosto de 2011 respectivamente, mediante estos creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación.

La comisión para la seguridad Informática, realizo un levantamiento de información que dio como resultado un informe sobre la gestión de la seguridad de información en las instituciones públicas y llego a la conclusión de implementar Normas y procedimiento para la seguridad de la información y así incentivar una cultura dentro de las instituciones de gestión permanente de las mismas.

"El Esquema Gubernamental de la Seguridad de la Información (EGSI) establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública" (http://www.planificacion.gob.ec , 2013). No reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices.

**Normas de control interno de la contraloría general del estado**.

El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro delos objetivos institucionales y la protección de los recursos públicos. Constituyen componentes del control interno el ambiente de control,

la evaluación de riesgos, las actividades de control, los sistemas de información y comunicación y el seguimiento.

"El control interno está orientado a cumplir con el ordenamiento jurídico, técnico y administrativo, promover eficiencia y eficacia de las operaciones de la entidad y garantizar la confiabilidad y oportunidad de la información, y la adopción de medidas oportunas para corregir las deficiencias de control". (http://www.contraloria.gob.ec,2009).

Uno de los objetivos de estas normas es controlar la gestión del departamento de Tecnologías de la Información y Comunicación , que establece partir de las normas 410- 500-02 y su objetivo fundamental es Garantizar la confiabilidad, integridad y confidencialidad de la información.

Por tanto es factible proponer una metodología de análisis de Riesgo de la Información basado en la Norma ISO 27005 ; porque las Normas de Control Interno de la Contraloría solicitan en la norma 410-09 Mantenimiento y control de la infraestructura tecnológica en su literal 2 que a continuación se detalla : Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción, pero esta normas no establecen proceso o mecanismo para poder realizar este análisis de riesgo.

Antes de comenzar con el análisis de riesgo sobre una infraestructura tecnológica es necesario establecer algunas definiciones y conceptos que a continuación se detallan:

## 2.9 Amenazas que está expuesta la información.

Las amenazas son cualquier entidad que origine un tipo de evento que puede realizar daño en un sistema de información, aunque también existen amenazas que afectan a los sistemas de información de manera involuntaria por ejemplo algún tipo de desastres natural. Las amenazas pueden ser activas o pasivas de acuerdo al tipo de ataque que se puede realizar.

### Amenazas Pasivas.

También son conocidas como escuchas su objetivo es obtener información de una comunicación. Por ejemplo existe software que monitorea el tráfico de una red wifi.

### Amenazas Activas.

Estas tratan de realizar cambios en la información de un sistema, por ejemplo se encuentra la inserción de mensajes ilegítimos la clonación de certificados etc.

### Ataques que está expuesta la información.

"Es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él tomar el control del mismo. Trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema" (Roa José, 2013).

De hecho algunas metodologías distingue entre ataques y errores cada una con sus diferencias la primera siendo acciones intencionadas y la segunda de carácter fortuito.

La utilización de programas para conseguir acceso al servidor de forma ilegítima o la realización de ataques de denegación de servicio para colapsar el

servidor son algunos ataques que se pueden realizar donde se distinguen las siguientes acciones.

**Reconocimiento.** Consiste en obtener toda la información necesaria de la víctima, que puede ser una persona o una organización.

**Exploración.** Se trata de conseguir información sobre el sistema a atacar, como por ejemplo, direcciones IP, nombres de host, datos de autenticación, etc.

**Obtención de acceso**. A partir de la información descubierta en la fase anterior, se intenta explotar alguna vulnerabilidad detectada en la víctima para llevar a cabo el ataque.

**Mantener el acceso.** Después de acceder al sistema, se buscará la forma de implantar herramientas que permitan el acceso de nuevo al sistema en futuras ocasiones.

**Borrar las huellas**. Finalmente, se intentarán borrar las huellas que se hayan podido dejar durante la intrusión para evitar ser detectado. "En el mercado existen una gran variedad de herramientas de seguridad que permiten conseguir un nivel óptimo de seguridad, pero hay estrategias de ataque que hacen ineficaces a estas herramientas, como las orientadas a explotar las debilidades del factor humano"(Pérez Onrubia, 2011).

**Riesgo.**

"Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente" (Roa José, 2013).Es importante establecer el grado de interés de cada activo y

cuáles son sus principales características cuales están en peligro, es decir, analizar el sistema.

Las tareas de análisis y tratamiento de los riesgos no son un fin en sí mismas, sino que se encajan en la actividad continua de gestión de la seguridad. El análisis y evaluación del riesgo permite identificar las amenazas y las vulnerabilidades que están expuestas la información de la empresa, hay que tomar en cuenta los objetivos, estrategias y políticas de la organización y el tratamiento de los riegos permitan elaborar un plan de seguridad de la información, que implementado y operado, satisfaga en gran medida la necesidad de tratamiento de riesgo de cada una de los departamentos que generan la información de la empresa.

Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos. La implantación de las medidas de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con el sistema de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

"El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, controla todas las actividades. La fase de tratamiento estructura las acciones a realizar en materia de seguridad para anular las amenazas detectadas por el análisis" (Amutio Miguel, 2013).

**2.10 Plan de seguridad informática.**

"Es la expresión gráfica Sistema de Seguridad Informática diseñado y constituye el documento básico que establece los principios organizativos de

una Entidad y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático" (https://seguridadinformaticaufps.wikispaces.com, 2012).

El plan de seguridad debe garantizar.

- La Disponibilidad de los sistemas de información
- La Recuperación de los sistemas de información
- La Trazabilidad de los sistemas de información
- La Autenticidad de la información
- La Integridad de la Información
- El Acceso a la información
- La Confidencialidad de la información
- La Conservación de la información.

### 2.11 Consideraciones ISO 27001 para el desarrollo del plan de seguridad informática.

La norma ISO 27001 establece los lineamientos necesarios para establecer, implantar, mantener y mejorar un SGSI, para lo cual la empresa debe realizar una serie de pasos que a continuación se detalla.

- Definir el alcance y los límites del SGSI en términos de las características del negocio, la
- Organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance.
- Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología que:

a) Incluya un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información.
b) Tome en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual.
c) Esté alineada con el contexto de la gestión riesgo estratégico de la organización en el cual se dará el establecimiento y mantenimiento del SGSI.
d) Establezca el criterio con el que se evaluará el riesgo.
e) Haya sido aprobada por la gerencia.

- Definir el enfoque de valuación del riesgo de la organización.
- Identificar una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información comercial.
- Desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables
- La metodología de estimación del riesgo seleccionada debe asegurar que los cálculos del riesgo produzcan resultados comparables y reproducibles.
  a) Identificar los riesgos.
  b) Identificar los activos dentro del alcance del SGSI y los propietarios de estos activos.
  c) Identificar las amenazas para aquellos activos.
  d) Identificar las vulnerabilidades que podrían ser explotadas por las amenazas.
  e) Identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

f) Analizar y evaluar el riesgo.

g) Calcular el impacto comercial sobre la organización que podría resultar de una falla en la seguridad, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.

h) Calcular la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, y los impactos asociados con estos activos, y los controles implementados actualmente.

i) Calcular los niveles de riesgo.

j) Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido.

- Identificar y evaluar las opciones para el tratamiento de los riesgos
- Seleccionar objetivos de control y controles para el tratamiento de riesgos se deben seleccionar e implementar para cumplir con los requerimientos identificados por el proceso de tasación del riesgo y tratamiento del riesgo.
- Obtener la aprobación de la gerencia para los riesgos residuales propuestos.
- Obtener la autorización de la gerencia para implementar y operar el SGSI.
- Preparar un Enunciado de Aplicabilidad.
- Se debe preparar un Enunciado de Aplicabilidad que incluya lo siguiente:

a) los objetivos de control y los controles seleccionados y las razones para su selección

b) los objetivos de control y controles implementados actualmente.

c) La exclusión de cualquier objetivo de control y la justificación para su exclusión.

d) Uno de los puntos de partida para el desarrollo de un plan de seguridad es determinar el valor de los activos de la empresa, la fuente para determinar las posibles afectaciones a los activos de una organización esta establecidas por las normas ISO 27005.

**Capitulo3**

# Metodología de Análisis de Riesgo basado en ISO 27005

**3.1 Situación previa de la seguridad informática en el caso de estudio.**

**3.1 Definición del Alcance del análisis.(ampliar).**

**3.3 Valoración de Activos.**

**3.4 Cálculo de ocurrencias de las amenazas y facilidad de explotación.**

**3.5 Evaluación del Riesgo.**

**3.6 Cálculo de Riesgo sobre los Activos.**

**3.7 Tratamiento de Riesgo y toma de decisiones Gerencial.**

**3.8 Riesgo Residual.**

Para elaborar el esquema de análisis de riesgo fue necesario realizar una revisión de la normas ISO 27001 para realizar el análisis en su etapa inicial definiendo el alcance del análisis de Riesgo, esto ayuda en la segunda etapa para la definición de los activos, para pasar a la tercera etapa de valoración de los activos de acuerdo a su impacto en la integridad, confidencialidad y disponibilidad de la información y servicios, la cuarta etapa identifica las amenazas a las cuales están sometidos cada uno de los activos y las vulnerabilidades que pueden estar expuestos, la quinta etapa expone los valores a la probabilidad y las consecuencias de un riesgo, finalizando con la obtención del riesgo para cada uno de los activos fijados todo esto se obtiene tomando como referencia la Norma ISO 27005. A continuación, se detalla gráficamente la metodología planteada.

Gráfico 3.1 Esquema del Análisis de Riesgo.

Fuente: Elaborada por los autores.

| |
|---|
| INCUMPLIMIENTO DE LA LEGISLACIÓN O REGLAMENTACION |
| DETERIORO DE DESEMPEÑO DEL NEGOCIO |
| PERDIDA DEL NOMBRE /EFECTO NEGATIVO EN LA REPUTACIÓN |
| BRECHAS ASOCIADAS CON LA INFORMACIÓN PERSONAL |
| EFECTOS ADVERSOS EN EL CUMPLIMIENTO DE LA LEY |
| BRECHAS EN LA CONFIDENCIALIDAD |
| PERDIDA FINANCIERA |
| ALTERACION EN LAS ACTIVIDADES DEL NEGOCIO |
| HACER PELIGRAR SEGURIDAD AMBIENTAL |
| INTERRUCION DE SERVICIOS |
| INCAPACIDAD PARA PRESTAR EL SERVICIO |
| PERDIDA DE CONFIANZA DEL CLIENT |
| PERDIDA DE CREDIBILIAD EN EL SISTEMA DE INFORMACIÓN INTERNO |
| DAÑO EN LA REPUTACIÓN |
| ALTERACION DE LA OPERACIÓN INTERNA |
| ALTERACION EN LA PROPIA ORGANIZACIÓN |
| COSTO INTERNO ADICIONAL |
| ALTERACION EN LA OPERACIÓN DE UNA TERCERA |

| |
|---|
| PARTE |
| ALTERACIÓN DE LA TERCERAS PARTES QUE TIENE TRANSACCIONES CON LA ORGANIZACIÓN |
| DIVERSOS TIPOS DE AGRAVIOS |
| CONTRAVESIONES DE LEYES Y REGLAMENTOS |
| INCAPACIDAD PARA CUMPLIR LAS OBLIGACIONES LEGALES |
| INCUMPLIMIENTO DE CONTRATO |
| INCAPACIDAD PARA CUMPLIR LAS OBLIGACIONES CONTRACTUALES |
| PELIGRO AREA EL PERSONAL DE LA ORGANIZACIÓN |
| ATAQUE A LA VIDA PRIVADA DE LOS USUARIOS |
| PERDIDAS FINACIERA |
| COSTO FINANCIERO PARA EMERGENCIAS O REPARACIONES |
| EN TERMINOS DEL PERSONA |
| EN TERMINOS DEL EQUIPO |
| EN TERMINOS DE ESTUDIOS , INFORMES DE EXPERTOS |
| PERDIDAD DE MERCANCIAS /FONDOS /ACTIVOS |
| PREDIDA DE CLIENTES, PERDIDA DE PROVEEDORES |
| PROCESOS JUDICIALES Y CASTIGOS. |
| PERDIDA DE UNA VENTAJA COMPETITIVA |
| PERDIDA DE LIDERAZGO TECNOLOGICO / TECNICO |
| PERDIDA DE EFICACIA/CONFIANZA |

| |
|---|
| PERDIDA DE REPUTACIÓN TECNICA |
| DEBILIDAD EN LA CAPACIDAD DE NEGOCIACIÓN |
| CRISIS INDUSTRIAL |
| CRISIS DE GOBIERNO |
| DESPIDOS |
| DAÑOS MATERIALES |

**Tabla 3.1 :** Parametros parala valoración de los activos.

**Fuente:** ISO27005

### 3.1 Situación previa de la seguridad informática en el caso de estudio.

El departamento de tecnologías de la información es un área fundamental de la universidad donde se encuentran los dispositivos, software y toda la infraestructura tecnológica que hace posible brindar servicios a la comunidad universitaria, por esta razón se requiere que la información y la seguridad sea tratada de manera organizada, porque al momento de realizar el estudio no se tienen políticas de seguridad, y todas las actividades se siguen sin tener lineamientos para el aseguramiento de los activos.

A continuación, se detalla la aplicación del esquema del análisis de riesgo con varios activos de responsabilidad del departamento de TIC y que existe en todas las infraestructuras.

### 3.2 Definición del Alcance del análisis.

Esta incluido el departamento de tecnologías de la Información y todos los equipos de la parte administrativa de la Universidad Técnica de Babahoyo.

**Identificación de los activos.**

Según la norma ISO 27005 Tenemos:

**Activos Primarios.**

Son aquellos que implican procesos del negocio.

**Información.**

**Activos de Soporte** .Estos dependen los elementos primarios del alcance, y pueden ser Hardware, software, redes, personal, sitio, estructura de la organización.

Para el estudio de aplicación de análisis de riesgo, son tomados como base tres tipos de activos que existen y son muy comunes en las infraestructuras tecnológicas.

Para tener un criterio de cómo establecer cualitativamente la valoración de un activo ISO 27005 entrega una lista de parametros a tener en cuenta:

### 3.3 Valoración de Activos.

Es de vital importancia dentro de la fase de Análisis de Riesgo, se lo realiza con el objetivo de establecer el valor de afectación de estos activo en cuanto a la utilidad de los servicios y procesos de negocio de la empresa. La base para la valoración de los activos del departamento de TIC es el costo en que se incurre debido a la perdida de la confidencialidad, integridad y disponibilidad como resultado de un incidente. Esta valoración proporciona las dimensiones que tienen los elementos importantes para el valor del activo. Para este proceso se realiza una escala de valoración que se detalla en la **tabla 3.2.**

| PARAMETROS/VALORACION | | DEPENDENCIA | FUNCIONALIDAD | INTEGRIDAD, CONFIDENCIALIDAD Y |
|---|---|---|---|---|
| 1 | MUY BAJO | Ningún otro activo depende de este para la entrega de servicios | Activo con capacidades tecnológicas muy limitadas | La divulgación, modificación y no disponibilidad de su |
| 2 | BAJO | Pocos activos dependen de este para la entrega de servicios | Activo con capacidades tecnológicas limitadas | La divulgación, modificación y no disponibilidad de su |
| 3 | MEDIO | Una mínima cantidad de activos dependen de este para la entrega | Activo con capacidades tecnológicas avanzadas | La divulgación, modificación y no disponibilidad de su |
| 4 | ALTO | Un número considerable de activos dependen de | Activo con capacidades tecnológicas muy avanzadas. | La divulgación, modificación y no disponibilidad de su |
| 5 | CRITICO | Todos los activos dependen de éste para la entrega de servicios | Activo con capacidades tecnológicas de última generación | La divulgación, modificación y no disponibilidad de su |

**Tabla 3.2:** Escala de valoración de los activos

**Fuente:** Elaborada por los autores.

La tabla de la valoración de activos se la obtuvo en las reuniones de trabajo con los miembros del departamento de tecnologías realizando un análisis de la dependencia de entrega de servicios del activo, si del activo dependen otros, la funcionalidad en cuanto a las capacidades y la afectación del activo en caso de falla sobre la integridad de la confidencialidad y disponibilidad de los servicios. A continuación, se realizó la identificación de las funciones del activo y se le asigna un valor de acuerdo a la escala realizada de la pérdida de

confidencialidad, integridad y disponibilidad de las funciones que provee al suscitarse algún incidente. Este proceso se encuentra detallado en la **tabla 3**.

| ACTIVOS DE SOPORTE | Funciones | CONFIDENCIALIDAD | INTEGRIDAD | DISPONIBILIDAD | PROMEDIO |
|---|---|---|---|---|---|
| Servidor | **contiene la configuración de los software y servicios de la Universidad y tienen alojada base de datos** | **4** | **4** | **5** | **4** |
| Portátil | **permite acceder a los servicios y acceso a las redes** | **5** | **5** | **4** | **5** |
| Equipos de escritorio | **permite acceder a los servicios y acceso a las redes** | **5** | **5** | **4** | **5** |

**Tabla 3.3:** Valoración de los activos.

**Fuente:** Elaborada por los autores.

### 3.4 Cálculo de ocurrencias de las amenazas y facilidad de explotación.

Una vez realizada la valoración de los Activos del departamento de TIC a través de reuniones de trabajo, inspección física y revisión de documentos. A continuación, se realizó la identificación de las amenazas, vulnerabilidades que afectan a cada uno de los activos. "Una amenaza es una acción que trata de

aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él tomar el control del mismo. Trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema" (Roa, 2013).

El listado de ejemplos de vulnerabilidades con sus respectivas amenazas se encuentra en la norma ISO 27005 y un ejemplo detallado en la **tabla 4**.

| Tipos | Ejemplos de vulnerabilidades | Ejemplos de amenazas |
|---|---|---|
| Hardware | Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento. | Incumplimiento en el mantenimiento del sistema de información |
| | Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad | Destrucción del equipo o los medios. Polvo, corrosión, congelamiento |
| | Sensibilidad a la radiación electromagnética | Radiación electromagnética |
| | Falta de control de cambio con configuración eficiente | Error en el uso |
| | Susceptibilidad a las variaciones de tensión | Pérdida del suministro de energía |
| | Susceptibilidad a las variaciones de temperatura | Fenómenos meteorológicos |
| | Almacenamiento sin protección | Hurto de medios o documentos |
| | Falta de cuidado en la disposición final | Hurto de medios o documentos |
| | Copia no controlada | Hurto de medios o documentos |
| Software | Falta o insuficiencia de la prueba del software | Abuso de los derechos |
| | Defectos bien conocidos en el software | Abuso de los derechos |
| | Falta de "terminación de la sesión" cuando se abandona la estación de trabajo | Abuso de los derechos |

| | | |
|---|---|---|
| | Disposición o reutilización de los medios de almacenamiento sin borrado adecuado | Abuso de los derechos |
| | Falta de pruebas de auditoría | Abuso de los derechos |
| | Distribución errada de los derechos de acceso | Abuso de los derechos |
| | Software de distribución amplia | Corrupción de datos |
| | Utilización de los programas de aplicación a los datos errados en términos de tiempo | Corrupción de datos |
| | Interfase de usuario complicada | Error en el uso |
| | Falta de documentación | Error en el uso |
| | Configuración incorrecta de parámetros | Error en el uso |
| | Fechas incorrectas | Error en el uso |
| | Falta de mecanismos de identificación y autentificación, como la autentificación de usuario | Falsificación de derechos |
| Software | Tablas de contraseñas sin protección | Falsificación de derechos |
| | Gestión deficiente de las contraseñas | Falsificación de derechos |
| | Habilitación de servicios innecesarios | Procesamiento ilegal de datos |
| | Software nuevo o inmaduro | Mal funcionamiento del software |
| | Especificaciones incompletas o no claras para los desarrolladores | Mal funcionamiento del software |
| | Falta de control eficaz del cambio | Mal funcionamiento del software |
| | Descarga y uso no controlados de software | Manipulación con software |
| | Falta de copias de respaldo | Manipulación con software |
| | Falta de protección física de las puertas y ventanas de la edificación | Hurto de medios o documentos |
| | Falla en la producción de informes de gestión | Uso no autorizado del equipo |

| | | |
|---|---|---|
| Red | Falta de prueba del envío o la recepción de mensajes | Negación de acciones |
| | Líneas de comunicación sin protección | Escucha subrepticia |
| | Tráfico sensible sin protección | Escucha subrepticia |
| | Conexión deficiente de los cables. | Falla del equipo de telecomunicaciones |
| | Punto único de falla | Falla del equipo de telecomunicaciones |
| | Falta de identificación y autentificación de emisor y receptor | Falsificación de derechos |
| | Arquitectura insegura de la red | Espionaje remoto |
| | Transferencia de contraseñas autorizadas | Espionaje remoto |
| | Gestión inadecuada de la red (capacidad de recuperación del enrutamiento) | Saturación del sistema de información |
| | Conexiones de red pública sin protección | Uso no autorizado del equipo |
| Personal | Ausencia del personal | Incumplimiento en la disponibilidad del personal |
| | Procedimientos inadecuados de contratación | Destrucción de equipos o medios |
| | Entrenamiento insuficiente en seguridad | Error en el uso |
| | Uso incorrecto de software y hardware | Error en el uso |
| | Falta de conciencia acerca de la seguridad | Error en el uso |
| | Falta de mecanismos de monitoreo | Procesamiento ilegal de los datos |
| | Trabajo no supervisado del personal externo o de limpieza | Hurto de medios o documentos |
| | Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería | Uso no autorizado del equipo |
| Lugar | Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos | Destrucción de equipo o medios |

| | | |
|---|---|---|
| | Ubicación en un área susceptible de inundación | Inundación |
| | Red energética inestable | Pérdida del suministro de energía |
| | Falta de protección física de las puertas y ventanas de la edificación | Hurto de equipo |
| Organización | Falta de procedimiento formal para el registro y retiro del registro de usuario | Abuso de los derechos |
| | Falta de proceso formal para la revisión (supervisión) de los derechos de acceso | Abuso de los derechos |
| | Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes | Abuso de los derechos |
| | Falta de procedimiento de monitoreo de los recursos de procesamiento información | Abuso de los derechos |
| | Falta de auditorías (supervisiones) regulares | Abuso de los derechos |
| | Falta de procedimientos de identificación y evaluación de riesgos | Abuso de los derechos |
| | Falta de reportes sobre fallas incluidos en los registros de administradores y operador | Abuso de los derechos |
| | Respuesta inadecuada de mantenimiento del servicio | Incumplimiento en el mantenimiento del sistema de información |
| | Falta o insuficiencia en el acuerdo a nivel de servicio | Incumplimiento en el mantenimiento del sistema de información |
| | Falta de procedimiento de control de cambios | Incumplimiento en el mantenimiento del sistema de información |
| | Falta de procedimiento formal para el control de la documentación del SGSI | Corrupción de datos |

| | | |
|---|---|---|
| | Falta de procedimiento formal para la supervisión del registro del SGSI | Corrupción de datos |
| | Falta de procedimiento formal para la autorización de la información disponible al público | Datos provenientes de fuentes no confiables |
| | Falta de asignación adecuada de responsabilidades en la seguridad de la información | Negación de acciones |
| | Falta de planes de continuidad | Falla del equipo |
| | Falta de políticas sobre el uso del correo electrónico | Error en el uso |
| | Falta de procedimientos para la introducción del software en los sistemas operativos | Error en el uso |
| | Falta de registros en las bitácoras*(logs) de administrador y operario. | Error en el uso |
| | Falta de procedimientos para el manejo de información clasificada | Error en el uso |
| | Falta de responsabilidades en la seguridad de la información en la descripción de los cargos | Error en el uso |
| | Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados | Procesamiento ilegal de datos |
| | Falta de política formal sobre la utilización de computadores portátiles | Hurto de equipo |
| | Falta de control de los activos que se encuentran fuera de las instalaciones | Hurto de equipo |
| | Falta o insuficiencia de política sobre limpieza de escritorio y de pantalla | Hurto de medios o documentos |
| | Falta de autorización de los recursos de procesamiento de la información | Hurto de medios o documentos |
| | Falta de mecanismos de monitoreo establecidos para las brechas en la seguridad | Hurto de medios o documentos |
| | Falta de revisiones regulares por parte de la | Uso no autorizado del equipo |

| | | |
|---|---|---|
| | gerencia | |
| | Falta de procedimientos para la presentación de informes sobre las debilidades en la seguridad | Uso no autorizado del equipo |
| | Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales | Uso de software falso o copiado |

**Tabla 3.4:** Ejemplo de vulnerabilidades y amenazas**.**

**Fuente: ISO 27005**

En la **tabla 5** se socializó a través de reuniones de trabajo con los responsables de los activos una escala de valoración para las amenazas y probabilidad de ocurrencia de explotar vulnerabilidades con las bases especificadas en la norma ISO 27005.

| PARAMETROS/VALORACION | | DESCRIPCIÓN |
|---|---|---|
| **1** | BAJO | Amenazas cuya probabilidad de explotar vulnerabilidades es muy baja. |
| **2** | MEDIO | Amenazas que con poca frecuencia explotan vulnerabilidades. |
| **3** | ALTO | Amenazas que frecuentemente explotan vulnerabilidades. |

**Tabla 3.5:** Probabilidad que ocurra la amenaza

**Fuente: ISO 27005**

En la **Tabla 6** se muestra el resultado que se obtuvo a través de la observación y reuniones trabajo para obtener las amenazas y vulnerabilidades que influyen

en cada uno de los activos esto constituye la base para realizar el cálculo de la ocurrencia de la amenaza y la facilidad que puede ser explotada.

| ACTIVOS | AMENAZAS | VULNERABILIDAD | PROBABILIDAD OCURRA LA AMENZA | Facilidad de explotación |
|---|---|---|---|---|
| SERVIDOR | INCUMPLIMIENTO EN EL MANTENIMIENTO | MANTENIMIENTO INSUFICIENTE | ALTA | MEDIA |
| | ERROR DE USO | FALTA DE CONTROL DE CAMBIO EN LA CONFIGURACIÒN | ALTA | ALTA |
| | | FALTA DE DOCUMENTACIÓN | ALTA | ALTA |
| | ABUSO DE DERECHOS | FALTA DE TERMINACION DE LA SESIÓN | BAJA | MEDIA |
| | | DISPOSICION O REUTILIZACIÓN DE LOS | MEDIA | MEDIA |
| | | FALTA DE PRUEBAS DE AUDITORIA | ALTA | ALTA |
| | | | | |
| PORTATIL | INCUMPLIMIENTO EN EL MANTENIMIENTO | MANTENIMIENTO INSUFICIENTE | ALTA | ALTA |
| | HURTO DE MEDIOS O DOCUMENTOS | ALMACENAMIENTO SIN PROTECCIÓN | MEDIA | MEDIA |

| | | | | |
|---|---|---|---|---|
| EQUIPOS DE ESCRITORIO | INCUMPLIMIENTO EN EL MANTENIMIENTO | MANTENIMIENTO INSUFICIENTE | ALTA | ALTA |
| | HURTO DE MEDIOS O DOCUMENTOS | COPIA NO CONTROLADA | ALTA | ALTA |
| | | ALMACENAMIENTO SIN PROTECCIÓN | ALTA | ALTA |
| | ERROR DE USO | FALTA DE CONTROL DE CAMBIO EN LA CONFIGURACION | MEDIA | MEDIA |

**Tabla 3.6: Análisis de amenazas y vulnerabilidades que influyen en los activos.**

**Fuente:** Elaborada por los autores.

### 3.5 Evaluación del Riesgo.

"Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente" (Roa, 2013).

Esta evaluación del riesgo se la realizó por una combinación de los valores de los activos y los niveles de seguridad requeridos, para evitar que las amenazas exploten las vulnerabilidades.

**Estimación del riesgo.**En esta etapa se asignan valores a la probabilidad y a las consecuencias de un riesgo (ISO 27005, 2009). Esta escala se detalla en la **tabla 3.7.**

| Valores | Nivel de riego |
|---|---|

| | |
|---|---|
| 8 | ALTO |
| 6-7 | MEDIO ALTO |
| 4-5 | MEDIO |
| 2-3 | MEDIO BAJO |
| 0-1 | BAJO |

**Tabla 3.7:** Estimación del riesgo**.**

**Fuente:** Elaborada por los autores.

### 3.6 Cálculo de Riesgo sobre los Activos.

La siguiente actividad fue la determinación de cada tipo de amenaza, para cada agrupación de activos con los cuales se relaciona el tipo de amenaza, con el fin de habilitar la evaluación de los niveles de amenazas (probabilidad de ocurrencia) y niveles de vulnerabilidades (facilidad de explotación por parte de las amenazas para causar consecuencias adversas). Cada respuesta a un interrogante suscita un puntaje. Estos puntajes se acumulan a través de una base de conocimientos y se compara con los rangos (ISO 27005,2009). Esto identifica los niveles de amenaza en una escala de alto a bajo y los niveles de vulnerabilidad de manera similar, tal como se presenta en la **tabla 8**, diferenciando entre los tipos de consecuencias según sea pertinente.

| | **Probabilidad de ocurrencia – Amenaza** | **Baja** | | | **Media** | | | **Alta** | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Facilidad de explotación** | **Baja** | **Media** | **Alta** | **Baja** | **Media** | **Alta** | **Baja** | **Media** | **Alta** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **VALORACIÓN DEL ACTIVO** | **1** | **0** | **1** | **2** | **1** | **2** | **3** | **2** | **3** | **4** |
| | **2** | **1** | **2** | **3** | **2** | **3** | **4** | **3** | **4** | **5** |
| | **3** | **2** | **3** | **4** | **3** | **4** | **5** | **4** | **5** | **6** |
| | **4** | **3** | **4** | **5** | **4** | **5** | **6** | **5** | **6** | **7** |
| | **5** | **4** | **5** | **6** | **5** | **6** | **7** | **6** | **7** | **8** |

**Tabla 3.8:** Evaluación del Riesgo**.**

**Fuente: ISO 27005**

Los valores del activo, los niveles de amenaza y vulnerabilidad, pertinentes para cada tipo de consecuencias se contrastan en una matriz con el fin de identificar para cada combinación la medida pertinente de riesgo en una escala de 0 a 8. Los valores se ubican en la matriz de manera estructurada. En la **tabla 9** se muestra los activos, amenazas y la vulnerabilidad que presenta el activo su valoración la probabilidad de ocurrencia y facilidad de explotación.

| **ACTIVOS** | **AMENAZAS** | **VULNERABILIDAD** | **V/ACTIVO** | **PROBABILIDAD Q OCURRA** | **Facilidad de explotaci** | RIESGO |
|---|---|---|---|---|---|---|
| | | | | | | |
| SERVIDOR | INCUMPLIMIENTO EN EL MANTENIMIE | MANTENIMIENTO INSUFICIENTE | 5 | ALTA | MEDIA | 7 |
| | ERROR DE USO | FALTA DE CONTROL DE CAMBIO EN LA | 5 | ALTA | ALTA | 8 |
| | | FALTA DE DOCUMENTACIÓN | 5 | ALTA | ALTA | 8 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | ABUSO DE DERECHOS | FALTA DE TERMINACION DE LA SESIÓN | 5 | BAJA | MEDIA | 5 |
| | | DISPOSICION O REUTILIZACIÓN DE LOS | 5 | MEDIA | MEDIA | 6 |
| | | FALTA DE PRUEBAS DE AUDITORIA | 5 | ALTA | ALTA | 8 |
| | | | | | | |
| PORTATIL | INCUMPLIMIENTO EN EL MANTENIMIE | MANTENIMIENTO INSUFICIENTE | 5 | ALTA | ALTA | 8 |
| | HURTO DE MEDIOS O DOCUMENTOS | ALMACENAMIENTO SIN PROTECCIÓN | 5 | MEDIA | MEDIA | 6 |
| EQUIPOS DE ESCRITORIO | INCUMPLIMIENTO EN EL MANTENIMIE | MANTENIMIENTO | 5 | ALTA | ALTA | 8 |
| | HURTO DE MEDIOS O DOCUMENTOS | COPIA NO CONTROLADA | 5 | ALTA | ALTA | 8 |
| | | ALMACENAMIENTO SIN PROTECCIÓN | 5 | ALTA | ALTA | 8 |
| | ERROR DE USO | FALTA DE CONTROL DECAMBIO EN | 5 | MEDIA | MEDIA | 6 |

**Tabla 3.9: Valoración del Riesgo sobre los Activos.**

**Fuente:** Elaborada por los autores.

## 3.7 Tratamiento de Riesgo y toma de decisiones Gerencial.

| Valores | Nivel de riego | Descripción del riesgo y acciones |
|---|---|---|

| | | |
|---|---|---|
| 8 | ALTO | Requiere fuertes medidas correctivas. Planes de tratamiento implementados en corto tiempo, reportados y controlados con atención directa de alta dirección |
| 4-5 | MEDIO | Se requieren acciones correctivas controladas por grupos de manejo de incidentes en periodo de tiempo razonable |
| 0-1 | BAJO | El propietario del activo lo administra con procedimientos rutinarios o decide aceptar el riego |

**Tabla 3.10 Tratamiento del Riesgo**

**Fuente: elaborado por el autor**

Los criterios de aceptación de riesgo demandados por la universidad Técnica de Babahoyo y el departamento de tecnologías, establece que riesgos de niveles "Alto" y "Medio Alto" se consideran inaceptables y deben ser tratados de forma inmediata con los recursos necesarios requeridos. Así mismo, para los niveles "Medio" y "Bajo" se requiere de un registro en el cual la gerencia demuestre que se acepta el riesgo asociado a estos activos.

Este tratamiento del riesgo es detallado en la tabla que se muestra a continuación

Para el riesgo de los activos que va a ser reducido se aplicará los controles de la norma ISO 27002.

### 3.8 Riesgo Residual.

Se dejará un riesgo remanente debido que para las amenazas identificadas es evidente que no se pueden eliminar todas las vulnerabilidades.

El riesgo residual es aceptable para las diferentes amenazas identificadas y se dispone de un registro de aceptación de este riesgo remanente.

Para disminuir los riesgos que están establecido en el análisis como alto es necesario realizar el siguiente proceso

**1.- Seleccionar Objetivos de Control y Controles para el Tratamiento de Riesgos.**

A continuación se determina los controles que pueden ser implementados, una vez identificados los procesos de tratamiento del riesgo y haberlos evaluado, se debe decidir qué objetivos de control y controles se van a implementar .

**2.- Preparación de la declaración de aplicabilidad.**

La declaración de aplicabilidad debe incluir los objetivos de control y controles que serán aplicados y los que serán excluidos. La declaración de aplicabilidad da la oportunidad a la empresa que asegure y verifique que no ha omitido algún control ejemplo:

| CONTROL ISO 27002 | CONTROLES | APLICABILIDAD | |
|---|---|---|---|
| | | SI | NO |
| 5. POLÍTICA DE SEGURIDAD. | | | |
| | 5.1 Política de seguridad de la información. | | |

| | | | |
|---|---|---|---|
| | 5.1.1 Documento de política de seguridad de la información. | X | |
| | 5.1.2 Revisión de la política de seguridad de la información. | X | |
| 6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC. | | | |
| | 6.1 Organización interna. | | |
| | 6.1.1 Compromiso de la Dirección con la seguridad de la información. | X | |
| | 6.1.2 Coordinación de la seguridad de la información. | X | |
| | 6.1.3 Asignación de responsabilidades relativas a la seg. de la información. | X | |
| | 6.1.4 Proceso de autorización de recursos para el tratamiento de la información | | X |
| | 6.1.5 Acuerdos de confidencialidad. | X | |
| | 6.1.6 Contacto con las autoridades. | X | |
| | 6.1.7 Contacto con grupos de especial interés. | X | |
| | 6.1.8 Revisión independiente de la seguridad de la información. | X | |
| | 6.2 Terceros. | | X |
| | 6.2.1 Identificación de los riesgos derivados del acceso de terceros. | | X |
| | 6.2.2 Tratamiento de la seguridad en la relación con los clientes. | | X |
| | 6.2.3 Tratamiento de la seguridad en contratos con terceros. | | X |
| 7. GESTIÓN DE ACTIVOS. | | | |

| | | | |
|---|---|---|---|
| | 7.1 Responsabilidad sobre los activos. | | |
| | 7.1.1 Inventario de activos. | X | |
| | 7.1.2 Propiedad de los activos. | X | |
| | 7.1.3 Uso aceptable de los activos. | X | |
| | 7.2 Clasificación de la información. | | |
| | 7.2.1 Directrices de clasificación. | X | |
| | 7.2.2 Etiquetado y manipulado de la información. | X | |
| 8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS. | | | |
| | 8.1 Antes del empleo. | | X |
| | 8.1.1 Funciones y responsabilidades. | | X |
| | 8.1.2 Investigación de antecedentes. | | X |
| | 8.1.3 Términos y condiciones de contratación. | | X |
| | 8.2 Durante el empleo. | | X |
| | 8.2.1 Responsabilidades de la Dirección. | | X |
| | 8.2.2 Concienciación, formación y capacitación en seg. de la informac. | | X |
| | 8.2.3 Proceso disciplinario. | | X |
| | 8.3 Cese del empleo o cambio de puesto de trabajo. | | X |
| | 8.3.1 Responsabilidad del cese o cambio. | | X |
| | 8.3.2 Devolución de activos. | | X |

| | | | |
|---|---|---|---|
| | 8.3.3 Retirada de los derechos de acceso. | | X |
| 9. SEGURIDAD FÍSICA Y DEL ENTORNO. | | | |
| | 9.1 Áreas seguras. | | X |
| | 9.1.1 Perímetro de seguridad física. | | X |
| | 9.1.2 Controles físicos de entrada. | | X |
| | 9.1.3 Seguridad de oficinas, despachos e instalaciones. | | X |
| | 9.1.4 Protección contra las amenazas externas y de origen ambiental. | | X |
| | 9.1.5 Trabajo en áreas seguras. | | X |
| | 9.1.6 Áreas de acceso público y de carga y descarga. | | |
| | **9.2 Seguridad de los equipos.** | | |
| | 9.2.1 Emplazamiento y protección de equipos. | X | |
| | 9.2.2 Instalaciones de suministro. | | X |
| | 9.2.3 Seguridad del cableado. | | X |
| | 9.2.4 Mantenimiento de los equipos. | X | |
| | 9.2.5 Seguridad de los equipos fuera de las instalaciones. | | X |
| | 9.2.6 Reutilización o retirada segura de equipos. | | X |
| | 9.2.7 Retirada de materiales propiedad de la empresa. | | X |
| 10. GESTIÓN DE COMUNICACIONES Y | | | |
| | **10.1 Responsabilidades y** | | |

| | | | |
|---|---|---|---|
| OPERACIONES. | **procedimientos de operación.** | | |
| | 10.1.1 Documentación de los procedimientos de operación. | | X |
| | 10.1.2 Gestión de cambios. | X | |
| | 10.1.3 Segregación de tareas. | | X |
| | 10.1.4 Separación de los recursos de desarrollo, prueba y operación. | | X |
| | 10.2 Gestión de la provisión de servicios por terceros. | | X |
| | 10.2.1 Provisión de servicios. | | X |
| | 10.2.2 Supervisión y revisión de los servicios prestados por terceros. | | X |
| | 10.2.3 Gestión del cambio en los servicios prestados por terceros. | | X |
| | 10.3 Planificación y aceptación del sistema. | | X |
| | 10.3.1 Gestión de capacidades. | | X |
| | 10.3.2 Aceptación del sistema. | | X |
| | **10.4 Protección contra el código malicioso y descargable.** | | |
| | 10.4.1 Controles contra el código malicioso. | | X |
| | 10.4.2 Controles contra el código descargado en el cliente. | | X |
| | **10.5 Copias de seguridad.** | | |
| | 10.5.1 Copias de seguridad de la información. | X | |
| | **10.6 Gestión de la seguridad de las redes.** | | |

| | | | |
|---|---|---|---|
| | 10.6.1 Controles de red. | X | |
| | 10.6.2 Seguridad de los servicios de red. | X | |
| | **10.7 Manipulación de los soportes.** | | |
| | 10.7.1 Gestión de soportes extraíbles. | X | |
| | 10.7.2 Retirada de soportes. | X | |
| | 10.7.3 Procedimientos de manipulación de la información. | X | |
| | 10.7.4 Seguridad de la documentación del sistema. | X | |
| | **10.8 Intercambio de información.** | | |
| | 10.8.1 Políticas y procedimientos de intercambio de información. | | X |
| | 10.8.2 Acuerdos de intercambio. | | X |
| | 10.8.3 Soportes físicos en tránsito. | | X |
| | 10.8.4 Mensajería electrónica. | | X |
| | 10.8.5 Sistemas de información empresariales. | | X |
| | **10.9 Servicios de comercio electrónico.** | | |
| | 10.9.1 Comercio electrónico. | | |
| | 10.9.2 Transacciones en línea. | | |
| | 10.9.3 Información públicamente disponible. | | |
| | **10.10 Supervisión.** | | |
| | 10.10.1 Registros de auditoría. | X | |

| | | | |
|---|---|---|---|
| | 10.10.2 Supervisión del uso del sistema. | X | |
| | 10.10.3 Protección de la información de los registros. | | X |
| | 10.10.4 Registros de administración y operación. | | X |
| | 10.10.5 Registro de fallos. | X | |
| | 10.10.6 Sincronización del reloj. | | X |
| 11. CONTROL DE ACCESO. | | | |
| | **11.1 Requisitos de negocio para el control de acceso.** | | |
| | 11.1.1 Política de control de acceso. | X | |
| | **11.2 Gestión de acceso de usuario.** | | |
| | 11.2.1 Registro de usuario. | X | |
| | 11.2.2 Gestión de privilegios. | X | |
| | 11.2.3 Gestión de contraseñas de usuario. | X | |
| | 11.2.4 Revisión de los derechos de acceso de usuario. | | X |
| | **11.3 Responsabilidades de usuario.** | | |
| | 11.3.1 Uso de contraseñas. | X | |
| | 11.3.2 Equipo de usuario desatendido. | X | |
| | 11.3.3 Política de puesto de trabajo despejado y pantalla limpia. | X | |
| | **11.4 Control de acceso a la red.** | | |

| | | | |
|---|---|---|---|
| | 11.4.1 Política de uso de los servicios en red. | | X |
| | 11.4.2 Autenticación de usuario para conexiones externas. | | X |
| | 11.4.3 Identificación de los equipos en las redes. | X | |
| | 11.4.4 Protección de los puertos de diagnóstico y configuración remotos. | X | |
| | 11.4.5 Segregación de las redes. | X | |
| | 11.4.6 Control de la conexión a la red. | X | |
| | 11.4.7 Control de encaminamiento (routing) de red. | X | |
| | **11.5 Control de acceso al sistema operativo.** | | |
| | 11.5.1 Procedimientos seguros de inicio de sesión. | X | |
| | 11.5.2 Identificación y autenticación de usuario. | X | |
| | 11.5.3 Sistema de gestión de contraseñas. | X | |
| | 11.5.4 Uso de los recursos del sistema. | X | |
| | 11.5.5 Desconexión automática de sesión. | X | |
| | 11.5.6 Limitación del tiempo de conexión. | X | |
| | 11.6 Control de acceso a las aplicaciones y a la información. | | X |
| | 11.6.1 Restricción del acceso a la información. | | X |

| | | | |
|---|---|---|---|
| | 11.6.2 Aislamiento de sistemas sensibles. | | X |
| | 11.7 Ordenadores portátiles y teletrabajo. | | X |
| | 11.7.1 Ordenadores portátiles y comunicaciones móviles. | | X |
| | 11.7.2 Teletrabajo. | | X |
| 12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFO. | | | |
| | **12.1 Requisitos de seguridad de los sistemas de información.** | | |
| | 12.1.1 Análisis y especificación de los requisitos de seguridad. | | X |
| | **12.2 Tratamiento correcto de las aplicaciones.** | | |
| | 12.2.1 Validación de los datos de entrada. | X | |
| | 12.2.2 Control del procesamiento interno. | X | |
| | 12.2.3 Integridad de los mensajes. | | |
| | 12.2.4 Validación de los datos de salida. | | |
| | **12.3 Controles criptográficos.** | | |
| | 12.3.1 Política de uso de los controles criptográficos. | | |
| | 12.3.2 Gestión de claves. | X | |
| | **12.4 Seguridad de los archivos de sistema.** | | |
| | 12.4.1 Control del software en explotación. | | X |

| | | | |
|---|---|---|---|
| | 12.4.2 Protección de los datos de prueba del sistema. | | X |
| | 12.4.3 Control de acceso al código fuente de los programas. | x | |
| | **12.5 Seguridad en los procesos de desarrollo y soporte.** | | |
| | 12.5.1 Procedimientos de control de cambios. | X | |
| | 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el | | X |
| | Sistema operativo. | | X |
| | 12.5.3 Restricciones a los cambios en los paquetes de software. | | X |
| | 12.5.4 Fugas de información. | | X |
| | 12.5.5 Externalización del desarrollo de software. | | X |
| | **12.6 Gestión de la vulnerabilidad técnica.** | | |
| | 12.6.1 Control de las vulnerabilidades técnicas. | | X |
| 13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. | | | |
| | **13.1 Notificación de eventos y puntos débiles de seguridad de la información** | | |
| | 13.1.1 Notificación de los eventos de seguridad de la información. | | x |
| | 13.1.2 Notificación de puntos débiles de seguridad. | | x |
| | **13.2 Gestión de incidentes y mejoras de seguridad de la información.** | | |

| | | | |
|---|---|---|---|
| | 13.2.1 Responsabilidades y procedimientos. | | x |
| | 13.2.2 Aprendizaje de los incidentes de seguridad de la información. | | x |
| | 13.2.3 Recopilación de evidencias. | | x |
| 14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. | | | |
| | **14.1 Aspectos de seguridad de la información en la gestión de la** | | |
| | Continuidad del negocio. | | x |
| | 14.1.1 Inclusión de la seguridad de la información en el proceso de | | x |
| | Gestión de la continuidad del negocio. | | x |
| | 14.1.2 Continuidad del negocio y evaluación de riesgos. | | x |
| | 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la | | x |
| | Seguridad de la información. | | x |
| | 14.1.4 Marco de referencia para la planificación de la cont. del negocio. | X | |
| | 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad. | | x |
| 15. CUMPLIMIENTO. | | | |
| | 15.1 Cumplimiento de los requisitos legales. | | X |
| | 15.1.1 Identificación de la legislación aplicable. | | X |

| | | | |
|---|---|---|---|
| | 15.1.2 Derechos de propiedad intelectual (DPI). | | X |
| | 15.1.3 Protección de los documentos de la organización. | X | |
| | 15.1.4 Protección de datos y privacidad de la información de carácter | | X |
| | Personal. | | x |
| | 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información | | x |
| | 15.1.6 Regulación de los controles criptográficos. | | x |
| | 15.2 Cumplimiento de las políticas y normas de seguridad y | | x |
| | Cumplimiento técnico. | | x |
| | 15.2.1 Cumplimiento de las políticas y normas de seguridad. | | x |
| | 15.2.2 Comprobación del cumplimiento técnico. | | x |
| | 15.3 Consideraciones sobre las auditorías de los sistemas de información. | | x |
| | 15.3.1 Controles de auditoría de los sistemas de información. | | x |
| | 15.3.2 Protección de las herramientas de auditoría de los sistemas de información. | | x |

**Tabla 3.11 : Aplicabilidad de Controles ISO 27002**

**Fuente: Elaborado por el autores.**

**BIBLIOGRAFÍA.**


- AMUTIO, A. (2013). MAGERIT versión 3.0 Metodología de Análisis y gestión de Riesgo de los Sistemas de Información: España. Ministerio de Hacienda y administración Pública.
- BERNARD, P. (2011): Foundations of ITIL®. Ed. Van Haren Publishing.
- CHIAVENATO I. (2004). Introducción a la Teoría General de la Administración, Interamericana: McGraw-Hill.
- DÍAZ, G., ALZÓRRIZ, I., & Castro, M. (2014).Procesos y Herramientas para la seguridad de redes. España: Publicaciones UNED.
- DÍAZ, G., ALZÓRRIZ, I., & Castro, M. (2014).Procesos y Herramientas para la seguridad de redes. España: Publicaciones UNED.
- ESCRIVÁ,G.,ROMERO,D.,&Ramada,D.(2011).SeguridadInformática. España:MacMillan Iberia S.A.
- FERNÁNDEZ, C., &PIATTINI, M. (2012).Modelo para el Gobierno de las TIC basado en las normas ISO. España: AENOR.

- GÓMEZ, L., & ÁLVAREZ A.(2012).guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes: España: AENOR.
- HELAT, A. (2003): Remembrance of Data Passed: A Study of Disk Sanization Practices: IEEE Security & Privacy: IEEE Computer Society.
- Information Systems Audit and Control Association. (2013).COBIT el Gobierno y la Gestión de las TI de la Empresa. Argentina.
- Instituto argentino de Normalización. (2010).Que es una norma. Recuperada de http://www.iram.org.ar/index.php?IDM=7.
- Organización para la Cooperación y el Desarrollo Económicos.2002.Lineamientos para la Seguridad de Sistemas de Información y Redes: "hacia una Cultura de Seguridad. Francia.
- ROA, J. (2013).Seguridad Informática. España: McGraw-Hill.
- ROJAS, S., E.(2009).Trabajo de auditoria normas ,E libro.
- Sitio Oficial de ipyme (2009).Plan de Empresa recuperado de http://planempresa.ipyme.org/
- Sitio Oficial de ITIL. (2012). El estándar ITIL. Recuperado http://www.itil-officialsite.com/.

- Sitio Oficial de la Contraloría general del estado de Ecuador. (2009).Normas de Control Interno recuperado http://www.contraloria.gob.ec/normatividad.asp.
- Sitio Oficial de Planificación del Ecuador. (2013).Esquema Gubernamental de la seguridad de la información. Recuperado de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%B3n.pdf.