Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Escuela Académico Profesional de Ingeniería de Sistemas

Análisis y administración de riesgos para prestadores de servicios de sistemas de valor añadido (SVA) tipo sistema de intermediación digital (SID) basados en controles ISO 27002 alineados a ITIL

TESINA

Para optar el Título Profesional de Ingeniera de Sistemas

AUTOR

Rosario Celeste CERDÁN OBREGÓN

ASESOR

Norberto OSORIO BELTRÁN

Lima, Perú

2010

Referencia bibliográfica

Cerdán, R. (2010). *Análisis y administración de riesgos para prestadores de servicios de sistemas de valor añadido (SVA) tipo sistema de intermediación digital (SID) basados en controles ISO 27002 alineados a ITIL.* Tesina para optar el título profesional de Ingeniera de Sistemas. Escuela Académico Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

AGRADECIMIENTO

Esta Tesina está dedicada a Dios por ser mi guía en mi desarrollo profesional y en la vida, a mi mejor amiga Carina Estrada que gracias a su orientación y apoyo pude elaborar este trabajo de investigación y al profesor Norberto Osorio Beltrán por su orientación para que éste trabajo cumpla con los objetivos establecidos.

DEDICATORIA

Este trabajo está dedicado a Dios y a mis Padres que gracias a ellos me enseñaron a ser mejo cada día.

Análisis y Administración de riesgos para Prestadores de Servicios de Sistemas de Valor Añadido (SVA) Tipo Sistema de Intermediación Digital (SID) basados en controles ISO 27002 alineados a ITIL

RESUMEN

En estos últimos tiempos han surgido tendencias como la revolución de las Tecnologías de información donde las empresas han expresado la necesidad de mejorar sus estándares competitivos a niveles internacionales. Esto significa que se han visto en la necesidad de adoptar mejores prácticas de gestión de tecnologías de información y mejora continua en los procesos, alineándolos a modelos de control para hacer frente a los riesgos asociados a los procesos de tecnologías de información que soportan los procesos de negocio de la Empresa. Sin embargo en la actualidad la mayoría de Empresas Peruanas se encuentran en un nivel primario de adopción de mejores prácticas y no cuentan con una guía que les permita implementarlas de manera adecuada sin generar un impacto nocivo para la Empresa. Por tal motivo el presente trabajo de investigación tiene como objetivo realizar una propuesta metodológica, que aporte a la Administración Pública, una herramienta que permita implementar de manera ordenada un modelo de administración de riesgos, mediante la identificación de los controles y riesgos asociados a los procesos de TI, categorización del nivel de riesgo, generación de planes de acción que permitan la continuidad de los proceso de TI y el desarrollo de indicadores de gestión para el monitoreo del correcto funcionamiento de los procesos, mejorando de esta manera los estándares de calidad en la Empresa.

Palabras Claves: “Riesgos”, “SVA”, “SID”, “ITIL”, “ISO 27002”

Risk Analysis and Management for Value Added Systems (VAS) Providers of Digital Intermediation Systems (DIS) type ISO 27002 controls-based aligned with ITIL

ABSTRACT

In recent times tendencies like the information Technologies have come up in which the companies have expressed their necessity to improve their competitive standards to international levels. This means that they require to adopt best practices for information technologies management and processes continual improvement, aligning them to control models to face the risks associated to the information technology process that support the business processes.

Nonetheless, nowadays the majority of Peruvian companies are in a primary stage of adoption of best practices and do not have a guide that allows them to implement them in a proper way without causing a negative effect on the company. That's the reason why this investigative work has the objective of creating a methodological proposal, which can provide to the Public Administration, a tool that allows to implement in an orderly fishing a risk management model, by identifying the controls and risks associated with the IT processes, risk level classification, action plan generation that allow the IT process continuity and the development of management metrics for the appropriate monitoring of processes functioning, improving in this way the quality standards of the company.

Keywords: "Risks", "VAS", "DIS", "ITIL", "ISO 27002"

ÍNDICE

LISTA DE GRÁFICOS Y FIGURAS

INDICE DE TABLAS

CAPITULO 1: INTRODUCCIÓN

En la actualidad el desarrollo de las Tecnologías de la Información se extiende sobre la administración pública, en particular con el proyecto de la planta de certificación digital que se está implementando en RENIEC y con el nuevo reglamento de la ley de firmas y certificados digitales los cuales impulsan el desarrollo de nuevos servicios de trámites documentarios en línea. Estos servicios permitirán a los ciudadanos realizar transacciones con la administración pública en línea sin tener q apersonarse al local de cada entidad, colaborando así con el desarrollo del gobierno y comercio electrónico y los proyectos de inclusión, estos servicios conocidos como Servicio de Valor Añadido de certificación digital (SVA) poseen características comunes en particular respecto del uso de los certificados y firmas digitales. Sin embargo como todo sistema en línea posee vulnerabilidades de seguridad de la información que deben ser identificadas a fin de garantizar la confiabilidad y credibilidad de estos servicios, en este sentido el presente trabajo de investigación pretende colaborar con los desarrollos de estos servicios identificando las vulnerabilidades , amenazas y riesgos comunes que estos sistemas pueden experimentar en base a metodologías reconocidas internacionalmente como el ISO 27005 y MAGERIT a fin de recomendar controles apropiados basados en estándares y buenas prácticas internacionales de Seguridad de la información como lo son el ISO 27002 e ITIL v3.

1.1. Antecedentes

1.1.1. Reconocimiento legal de los certificados y las firmas digitales

Los principales precedentes que impulsaron el desarrollo de los servicios de los Prestadores de Servicios de Valor Añadido (SVA), en particular de los Sistemas de Intermediación Digital (SID) son el reconocimiento legal de la utilización de las firmas y los certificados digitales mediante la Ley de Firmas y Certificados Digitales – Ley 27269 y la creación de las SVA mediante el Reglamento de la Ley de Firmas y Certificados Digitales – DECRETO SUPREMO N° 052-2008 - PCM creándose así el marco normativo nacional de la Infraestructura Oficial de Firma Electrónica en el Perú.

En la actualidad una firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita. En tal sentido, cuando la ley exija la firma de una persona, ese requisito se entenderá cumplido en relación con un documento electrónico si se utiliza una firma digital generada en el marco de la Infraestructura Oficial de la Firma Electrónica, es decir si se utiliza un certificado digital emitido por una Entidad de Registro y una Entidad de Certificación acreditadas ante la Autoridad Administrativa Competente (el INDECOPI) y que además, es realizada mediante un software acreditado.

Los documentos electrónicos firmados digitalmente dentro del marco de la Infraestructura Oficial de Firma Electrónica deberán ser admitidos como prueba en los procesos judiciales y/o procedimientos administrativos, siempre y cuando la firma digital haya sido realizada utilizando un certificado emitido por una Entidad de Certificación acreditada en cooperación con una Entidad de Registro o Verificación acreditada, salvo que se tratara de la misma entidad con ambas calidades y con la correspondiente acreditación para brindar ambos servicios, asimismo deberá haberse aplicado un software de firmas digitales acreditado ante la Autoridad Administrativa Competente. Esto incluye la posibilidad de que a voluntad de las partes pueda haberse utilizado un servicio de intermediación digital.

La firma digital generada en el marco de la Infraestructura Oficial de Firma Electrónica garantiza el no repudio del documento electrónico original. Esta garantía no se extiende a los documentos individuales que conforman un documento compuesto, a menos que cada documento individual sea firmado digitalmente.

1.1.2. Creación de las SVA en la Administración Pública

Mediante el artículo 4 del Reglamento de la Ley de Firmas y Certificados Digitales se estipuló que, a fin de lograr una correcta implementación de la prestación de servicios de gobierno electrónico a través del empleo de canales seguros y servicios que garanticen el no repudio para el intercambio seguro de datos, las Entidades de la Administración Pública debían elaborar un rediseño funcional para la simplificación de los procedimientos, trámites y servicios administrativos, debiéndose poner principal énfasis en los aspectos siguientes:

a) La creación y mantenimiento de archivos electrónicos para el almacenamiento y gestión de los documentos electrónicos generados durante los trámites y procedimientos públicos: recepción y envío de solicitudes, escritos y comunicaciones.

b) El establecimiento de convenios que hagan factible el intercambio electrónico seguro de información y documentos obtenidos de los ciudadanos, entre las entidades encargadas de su archivo y las entidades interesadas, con el propósito de suprimir su reiterada solicitud.

c) La protección del derecho a la intimidad y a la confidencialidad de las comunicaciones dentro de lo establecido para tales efectos por la Norma Marco sobre Privacidad.

d) El empleo de la dirección oficial de correo electrónico cuando dicho servicio sea implementado.

e) La puesta a disposición de los ciudadanos de sus servicios empleando firmas digitales, certificados digitales y canales seguros que se encuentren dentro del ámbito de la Infraestructura Oficial de Firma Electrónica, es decir, la creación de Sistemas de Valor Añadido del tipo Sistema de Intermediación Digital.

En cumplimiento de lo establecido en dicho artículo, las entidades de la Administración Pública que brinden el servicio de Sistema de Intermediación Digital deberán acreditarse ante la Autoridad Administrativa Competente como Prestador de Servicios de Valor Añadido para el Estado Peruano.

1.2. Definición del Problema

Las Entidades de la Administración Pública enfrentan constantes ataques internos y externos a la Seguridad de la Información, y puesto que cuentan con presupuestos limitados, es difícil determinar la prioridad con la que una vulnerabilidad de Seguridad debe ser atendida, por lo que se debe iniciar con un estudio de análisis de riesgos incluso desde las etapas de diseño de los Servicios de Valor Añadido (SVA), a fin de cubrir las vulnerabilidades primarias, sin embargo esto puede implicar también una inversión significativa.

Los Servicios de Valor Añadido (SVA) son servicios soportados en tecnologías de la información, en los que se produce un importante flujo de datos en doble dirección.

Son, por ejemplo, los trámites documentarios, las transferencias electrónicas de dinero o de documentos, la mensajería electrónica, los diversos servicios de acceso a bases de datos nacionales o internacionales, etc.

1.3. Objetivos

1.3.1. General

Identificar los riesgos comunes y determinar controles del ISO 27002 e ITIL v3, que puedan ser considerados desde las etapas de Diseño de los Servicios de Valor añadido (SVA) a fin de reducir las futuras pérdidas posibles.

1.3.2. Específicos

- Identificar un proceso modelo general para los Servicios de Valor Añadido (SVA).
- Identificar los Activos importantes del proceso.
- Identificar las Vulnerabilidades y Amenazas comunes.
- Evaluar los riesgos.
- Recomendar controles apropiados basados en el ISO 27002 e ITIL v3.

1.4. Justificación

En la actualidad las entidades de la Administración pública se encuentran obligadas por la regulación peruana a cumplir con la norma técnica peruana NTP/ISO-IEC 17799, la cual está basada en el estándar ISO 27002. Sin embargo, puesto que esta norma técnica solamente hace referencia a la implementación de controles, debe ser completada con un sistema de análisis de riesgo que permita priorizar los controles y determinar las áreas de la organización sobre las cuales deben implementarse, a fin de optimizar la inversión económica y garantizar que solamente se implementen aquellos controles cuya inversión sea menor que la pérdidas por vulnerabilidades de seguridad.

Por otro lado, según el nuevo Reglamento de la Ley de Firmas y Certificados Digitales – Ley 27269, todas las entidades del Estado están obligadas a la implementación de sistemas de trámite documentario utilizando firmas y

certificados digitales, llamados Sistemas de Intermediación Digital (SID), del tipo de Prestadores de servicios de valor añadido (SVA).

Todos los prestadores de servicios de valor añadido están obligados a participar en una evaluación de acreditación de parte del INDECOPI. Dicha evaluación consta de criterios basados en las características propias de los sistemas de la Infraestructura de la Clave Pública (PKI), y de seguridad de la información basados en los estándares ISO 27001:2005 e ISO 27002.

En este sentido, la presente investigación permitirá el análisis de riesgo basado en los estándares ISO 27001:2005 e ISO 27005:2008 de un modelo general de SID/SVA para las entidades de la Administración Pública, a fin de permitir recomendar los controles de seguridad que deben implementarse desde la formación de estos sistemas, estos controles estarán basados en el ISO 27002 e ITIL v3.

Por otro lado, con esta investigación se busca demostrar que se puede lograr una adecuada administración de los riesgos de tecnologías de información mediante la aplicación de distintas metodologías como el ISO 27001:2005, ISO 27002 e ISO 27005:2008 así como también ITIL v3, las cuales no son excluyentes sino que en convergencia crean una sinergia que brinda una mejor infraestructura a los procesos de negocio, ya que están basadas en las mejores prácticas internacionalmente aceptados.

Asimismo ésta investigación resalta y enriquece el conocimiento sobre cómo los indicadores orientados a controles y la evaluación de riesgos sobre procesos de TI pueden ser una herramienta útil para el desarrollo de planes de acción preventivos y toma de decisiones gerenciales relacionadas a la prestación de los servicios de TI a clientes externos.

El enfoque realizado en esta investigación será aplicado como una solución real para las Empresas de nuestro entorno, en la cual se permitirá garantizar el no repudio en las transacciones y facilitará el trámite documentario para los ciudadanos peruanos, colaborando con el proyecto de inclusión.

CAPITULO 2: MARCO TEÓRICO

En el presente Capítulo se desarrolla el Marco Conceptual de las Metodologías relacionadas, donde se detalla las principales definiciones de las metodologías y conceptos relacionados.

2. Marco Conceptual de las Metodologías Relacionadas

2.1. Firma Digital

Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su control, de manera que está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior, tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica.

Las firmas digitales son las generadas a partir de certificados digitales que son:

a) Emitidos conforme a lo dispuesto en el Reglamento de firmas y certificados digitales por entidades de certificación acreditadas ante la Autoridad Administrativa Competente.

b) Incorporados a la Infraestructura Oficial de Firma Electrónica bajo acuerdos de certificación cruzada, conforme Reglamento de la Ley de firmas y certificados digitales.

c) Reconocidos al amparo de acuerdos de reconocimiento mutuo suscritos por la Autoridad Administrativa Competente conforme al art.72 del Reglamento de la Ley de firmas y certificados digitales.

d) Emitidos por Entidades de Certificación extranjeras que hayan sido incorporados por reconocimiento a la Infraestructura Oficial de Firma Electrónica conforme al art.73 del Reglamento de la Ley de firmas y certificados digitales.

2.1.1. Características de la firma digital

Las características mínimas de la firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica son:

a) Se genera al cifrar el código de verificación de un documento electrónico, usando la clave privada del titular del certificado.

b) Es exclusiva del suscriptor y de cada documento electrónico firmado por éste.

c) Es susceptible de ser verificada usando la clave pública del suscriptor.

d) Su generación está bajo el control exclusivo del suscriptor.

e) Está añadida o incorporada al documento electrónico mismo de tal manera que es posible detectar si la firma digital o el documento electrónico fue alterado.

2.2. Certificado Digital

Para la obtención de un certificado digital, el solicitante deberá acreditar lo siguiente:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

2.3. La Infraestructura Oficial de Firma Electrónica (IOFE)

La Infraestructura Oficial de Firma Electrónica está constituida por:

a) El conjunto de firmas digitales, certificados digitales y documentos electrónicos generados bajo la Infraestructura Oficial de Firma Electrónica.

b) Las políticas y declaraciones de prácticas de los Prestadores de Servicios de Certificación Digital, basadas en estándares internacionales o compatibles con los internacionalmente vigentes, que aseguren la interoperabilidad entre dominios y las funciones exigidas, conforme a lo establecido por la Autoridad Administrativa Competente.

c) El software, el hardware y demás componentes adecuados para las prácticas de certificación y las condiciones de seguridad adicionales comprendidas en los estándares señalados en el literal b).

d) El sistema de gestión que permita el mantenimiento de las condiciones señaladas en los incisos anteriores, así como la seguridad, confidencialidad, transparencia y no discriminación en la prestación de sus servicios.

e) La Autoridad Administrativa Competente, así como los Prestadores de Servicios de Certificación Digital acreditados o reconocidos.

2.4. Gestión de servicios de TI

La Gestión de Servicio TI, ITSM por sus siglas en inglés IT Service Management, es una disciplina basada en procesos, enfocada en alinear los servicios de TI proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final. GSTI propone cambiar el paradigma de gestión de TI, por una colección de componentes enfocados en servicios de punta a cabo usando distintos marcos de trabajo con las "mejores prácticas", como por ejemplo la Information Technology Infrastructure Library (ITIL) o el eSCM (enabled Service Capability Model).

Los proveedores de los servicios de TI no pueden seguir manteniendo su enfoque en la tecnología y sus propias organizaciones, ahora tienen que considerar la calidad de los servicios que proveen y enfocarse en sus relaciones con los clientes.

Usualmente la gestión de servicios de TI involucra el uso de outsourcings, insourcings y servicios compartidos. Es extremadamente importante mantener

una base de conocimiento amplia dentro de la organización para que estas prácticas sean exitosas.

Los objetivos de una buena gestión de servicios TI han de ser:

- Proporcionar una adecuada gestión de la calidad.
- Aumentar la eficiencia.
- Alinear los procesos de negocio y la infraestructura TI.
- Reducir los riesgos asociados a los Servicios TI.
- Generar Negocio.

2.5. Alineación con los Objetivos del Negocio

Las organizaciones actuales hacen inversiones importantes en recursos de tecnología de información para apoyar los procesos de negocio. El valor significativo y relevante que el uso de la información tiene para las organizaciones, determina que todos los procesos relativos a la producción, administración y uso de servicios de Tecnologías de Información (TI) deben ser óptimamente gestionados y controlados para asegurar la calidad de la información, soporte del cumplimiento de los objetivos del negocio.

Los procesos de datos e información producto de las operaciones y procesos del negocio, requieren la aplicación de técnicas y medidas de control en el marco de un sistema de gestión que garantice la prestación de los servicios y la reducción de vulnerabilidad a amenazas generadoras de riesgo que pongan en peligro la estabilidad del sistema operacional, organizacional y del sistema macro del negocio. Todo lo anterior, justifica la necesidad de optimizar los recursos de TI en apoyo y alineación con los objetivos de negocio a través de procesos efectivos de "Gestión de servicio TI".

En las organizaciones existe una organización de TI que genera y provee los servicios de TI y un grupo de clientes internos (usuarios) y externos que demandan esos servicios y esperan su prestación oportuna y con calidad. Las relaciones y comunicaciones entre el proveedor de TI y los clientes de TI deben ser canalizadas a través de un sistema que garantice la optimación de los

procesos de entrega y soporte de servicios a través de la consolidación de Gestión de Servicio TI.

Las inversiones en la infraestructura de TI y en los activos de información de las organizaciones cada vez son más importantes, lo cual justifica la implantación de sistemas que aseguren el rendimiento de los procesos basados en servicios de TI para asegurar la reducción del costo total de propiedad (TCO) y un retorno de la inversión (ROI) razonable. Hasta ahora, solo algunas empresas de alto nivel y tamaño han asumido e incorporado a su cultura organizacional y planes de negocio, los procesos de Gestión de Servicio TI basada en las mejores prácticas de aceptación internacional.

Este nuevo paradigma basado en el servicio debe tener un acercamiento a las organizaciones de cualquier tamaño, las empresas deben adoptar y adaptar estas mejores prácticas bajo un enfoque de "Calidad de Servicio" y oportunidad para el cambio del negocio con la aplicación de estándares actualizados. Este paradigma se fundamenta en el mejoramiento continuo de la Cultura de Servicio TI.

Los productos y servicios de estos marcos de referencia están orientados a la implantación de sistemas consolidados de mejoramiento continuo en la gestión de servicio de tecnología de información en alineación con los objetivos del negocio, de punta a punta desde las fases diagnostica y de planificación hasta la implantación, monitoreo, supervisión y optimación. La tendencia de Gestión de Servicio TI se basa en la promoción y soporte de aplicación de las mejores prácticas, marcos referenciales y estándares de aceptación internacional, tales como ISO/IEC 20000, ITIL, ITSCMM, COBIT, ISO/IEC -17799 – 2700X y otras.

2.6. Gobierno de la Tecnología de Información

Esta disciplina se encuentra poco desarrollada, debido a que cuenta con pocos estándares y marcos de trabajo reconocidos.

El Gobierno TI es un conjunto de procedimientos, estructuras y comportamientos utilizados para lograr una mejor relación entre los actores implicados en el funcionamiento y la administración de los sistemas de información en una organización.

El Gobierno TI se basa en la conclusión de que las TI han llegado a ser la base del funcionamiento de las organizaciones actuales.

Esta constatación tiene varias consecuencias:

1. Las TI llegan a ser un “recurso” de alta importancia estratégica.
2. Las TI deben alinearse con el negocio para asegurar que lo sostienen de la mejor manera posible.
3. Los accionistas y terceras partes deben ser informados de la situación TI de las organizaciones.
4. Las TI deben ser gestionadas de manera racional y controlada.

El principal objetivo del Gobierno TI es trasladar las TI de un rol de apoyo (nivel táctico) a un rol de motor de la organización (nivel estratégico).

Si las TI son la base de todo el funcionamiento de una empresa y soportan sus procesos, es imposible no incluirlas en las decisiones estratégicas de la empresa.

Figura 2.6. Gobierno de la Tecnología de Información

2.7. ITIL v3

La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Information Technology Infrastructure Library), es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de Servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI. [Fuente: Wikipedia]

ITIL especifica un modelo sistemático que garantiza la calidad de los servicios de TI. Ofrece una descripción detallada de los procesos más importantes en una organización de TI, incluyendo listas de verificación para tareas, procedimientos y responsabilidades que pueden servir como base para adaptarse a las necesidades concretas de cada organización.

Al mismo tiempo, el amplio campo de aplicación de ITIL la convierte en una útil guía de referencia en muchas áreas, lo que puede servir a las organizaciones de TI para definir nuevos objetivos de mejora que llevan a su crecimiento y madurez.

Con el paso de los años, ITIL se ha convertido en mucho más que una serie de libros útiles sobre Gestión de Servicios de TI. El marco de trabajo para el desarrollo de “mejores prácticas” en la Gestión de Servicios de TI no deja de crecer por la contribución de asesores, formadores y suministradores de tecnologías o productos.

Al tratarse de un marco de trabajo de mejores prácticas para la Gestión de Servicios de TI, ITIL presenta, como cualquier marco de trabajo, ventajas y desventajas. Muchas de las aplicaciones de “Mejores Prácticas” sirven para evitar posibles problemas o para resolverlos en caso de que se produzcan. [Fuente: itSMF International]

2.7.1. El Objetivo de usar ITIL en la Gestión de Servicios

ITIL como metodología propone el establecimiento de estándares que nos ayuden en el control, operación y administración de los recursos. Plantea hacer una revisión y reestructuración de los procesos existentes en caso de que estos lo necesiten (si el nivel de eficiencia es bajo o que haya una forma más eficiente de hacer las cosas), lo que nos lleva a una mejora continua.

2.7.2. Ciclo de vida de Servicios

ITIL enfoca la gestión de servicios a partir del Ciclo de Vida de un servicio. El Ciclo de Vida de un servicio es un modelo de organización que ofrece información sobre:

- La forma en que está estructurada la gestión del Servicio.
- La forma en que distintos componentes del Ciclo de Vida están relacionada entre sí.
- El efecto en que los cambios en un componente tendrán sobre otros componentes y sobre todo el sistema del Ciclo de Vida.

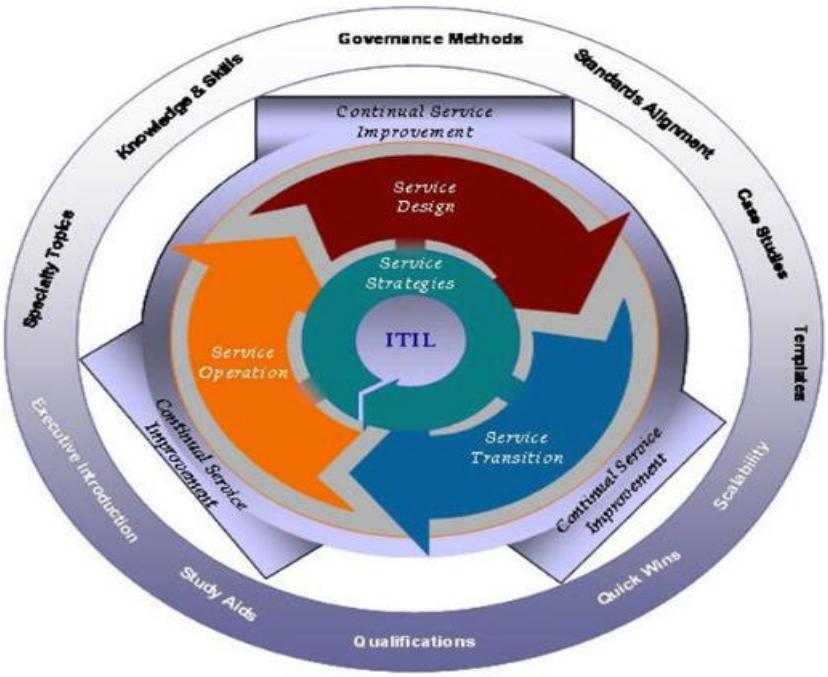


Figura 2.7.2. Ciclo de Vida de Servicio

El Ciclo de Vida del Servicio es una combinación de múltiples puntos de vista sobre la realidad de las organizaciones, lo que ofrece un mayor nivel de flexibilidad y control.

El padrón dominante en el Ciclo de Vida del Servicio es el paso desde la estrategia del Servicio al Diseño del Servicio, a la Transición del Servicio y a la Operación del Servicio hasta llegar a la Mejora Continua del Servicio y volver a la Estrategia del Servicio, y así sucesivamente. [Fuente: itSMF International]

2.8. Sistema de Gestión de la Seguridad de la Información – Según el estándar ISO 27001:2005

Un Sistema de Gestión de Seguridad de la Información (SGSI) puede entenderse como el establecimiento de un conjunto de procedimientos y tecnologías organizados sistemáticamente que permite determinar dentro de un negocio qué se debe proteger, por qué, contra qué y cómo se debe proteger, preservando la confidencialidad, integridad y disponibilidad de la información relevante para el negocio. El diseño y la implementación de un SGSI se encuentran influenciados por las necesidades, los objetivos, los requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la Organización.

El estándar ISO/IEC27001:2005 se ha desarrollado como modelo para el establecimiento, la implementación, la operación, el monitoreo, la revisión, el mantenimiento y la mejora de un SGSI para cualquier clase de negocio dentro de una organización.

Este estándar sigue el ciclo de Deming del Plan, Do, Check, Act. (ver Naturaleza de la norma ISO/IEC27001:2005), a través de las siguientes etapas:

2.8.1. Establecer el SGSI

1. Definir el alcance del SGSI, donde se definen los procesos, recursos, actividades y las instalaciones (definiendo la ubicación geográfica) que se deberán ser protegidas por el SGSI.

2. Establecer una política de seguridad aprobada por la alta dirección de la organización, a fin de establecer un fundamento normativo para proteger la seguridad de la información en la organización.

3. Establecer una metodología de análisis de riesgos

4. Establecer criterios propios de las necesidades del negocio para determinar los niveles de riesgo aceptable.

5. Identificar los activos importantes del negocio, sus vulnerabilidades y amenazas que pueden afectar la disponibilidad, integridad y confidencialidad de estos activos y su frecuencia.

6. Calcular el impacto sobre el negocio que puede ser causado por la materialización de una amenaza sobre un activo importante

7. Determinar el riesgo.

8. Determinar cómo gestionar el riesgo:

    - **Aceptar:** La autoridades competentes asumen formalmente las posibles consecuencias.

    - **Transferir:** Se transfiere el riesgo a un tercero, por ejemplo el uso de seguros.

    - **Rechazar:** Se evade la parte del negocio que causa el riesgo.

    - **Mitigar:** Se implementan controles para reducir el riesgo.

9. Identificar los objetivos de control y los controles que pueden ser utilizados para minimizar el riesgo en base al anexo A del ISO 27001:2005.

Estos controles son complementados con recomendaciones precisadas en el estándar ISO 27002.

10. Se calcula el riesgo residual y se logra la aceptación del mismo por la alta dirección.

11. Se elabora el documento de Declaración de Aplicabilidad donde se declara y sustenta formalmente que controles son aplicables a la organización y que serán implementados y verificados durante la auditoría para la obtención de la certificación internacional ISO 27001:2005.

2.8.2. Implementar el SGSI

1. Se establece un plan de tratamiento del riesgo: en función de los objetivos de control y los controles seccionados, se evalúan las alternativas para implementar dichos controles y se elabora un plan de implementación.

2. Se implementan las alternativas seleccionadas conforme al plan de tratamiento del riesgo.

3. Se establecen métricas para medir la efectividad de los controles seleccionados.

4. Se realizan procesos de concientización y entrenamiento.

2.8.3. Monitorear y revisar el SGSI

1. Se evalúa la efectividad de los controles implementados en base a las métricas establecidas.

2. Se realizan auditorías de acuerdo a la criticidad de los activos y a la efectividad de los controles.

3. Se evalúa el riesgo residual.

4. Se evalúan los reportes de incidentes ocurridos.

2.8.4. Mejora continua del SGSI

1. Se implementan medidas correctivas frente a los incidentes de seguridad ocurridos.

2. Se implementan medidas preventivas para reducir la posibilidad de que ocurran incidentes de seguridad.

El modelo está basado en un enfoque racional para su desempeño y su perfeccionamiento en el tiempo. En primera instancia, se exige que el modelo siga una serie de prerrequisitos para que se establezca, a través de la fase denominada “plan”. Una vez establecido el modelo se implementa y opera, siguiendo los lineamientos de la fase “do”. Luego que el modelo se ha implantado y está funcionando, se debe “monitorear y revisar” durante la fase “check”. Por último, con base en lo observado en la fase “Do”, se procede a “actuar” y tomar los correctivos y preventivos necesarios.

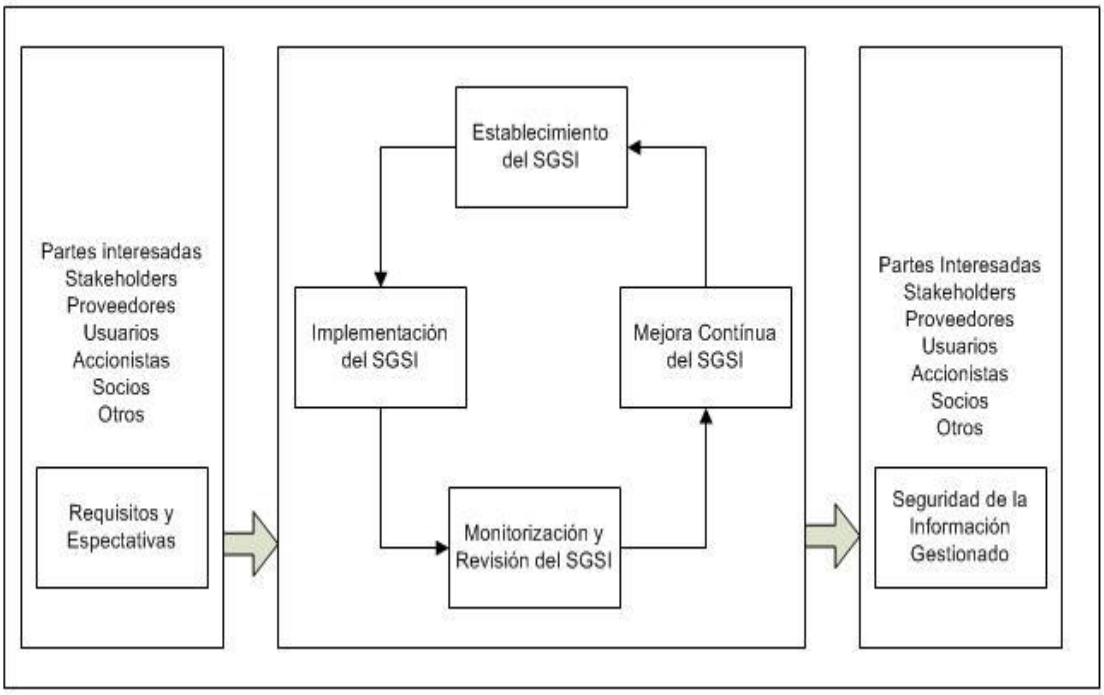


Figura 2.8.4. Naturaleza de la Norma ISO/IEC27001:2005

2.9. Controles del ISO 27001:2005

Las distintas cláusulas de la norma pueden clasificarse en globales y focales.

Las globales son aquellas genéricas que cubren todo el sistema y están orientadas a dar lineamiento genérico. Las focales son el grupo que dan pautas puntuales para instaurar ciertas exigencias.

Cuando se procede a iniciar un proyecto de implantación del modelo en la empresa, se debe empezar documentando las cláusulas globales y después se procede con las focales.

Ver ANEXO A

2.9.1. Documentación requerida del ISO 27001:2005

Los documentos del SGSI son los siguientes:

1. Los enunciados de la Política de Seguridad, los procedimientos y los objetivos de control.
2. El alcance del SGSI, los procedimientos y los controles que sostienen el SGSI.
3. El plan de tratamiento de riesgo.
4. Los procedimientos documentarios necesarios para la organización, a fin de asegurar la planeación, la operación y el control efectivo de sus procesos de seguridad de la información.
5. Los registros requeridos por el estándar.
6. Declaración de aplicabilidad.
7. El reporte de evaluación del riesgo.
8. La descripción de la metodología de evaluación del riesgo.

2.9.2. Enfoque a Procesos del ISO 27001:2005

El modelo ISO 27001:2005 está diseñado bajo una óptica de enfoque a procesos. El SGSI está conceptualizado para funcionar en cualquier tipo de organización, operando bajo el enfoque de procesos.

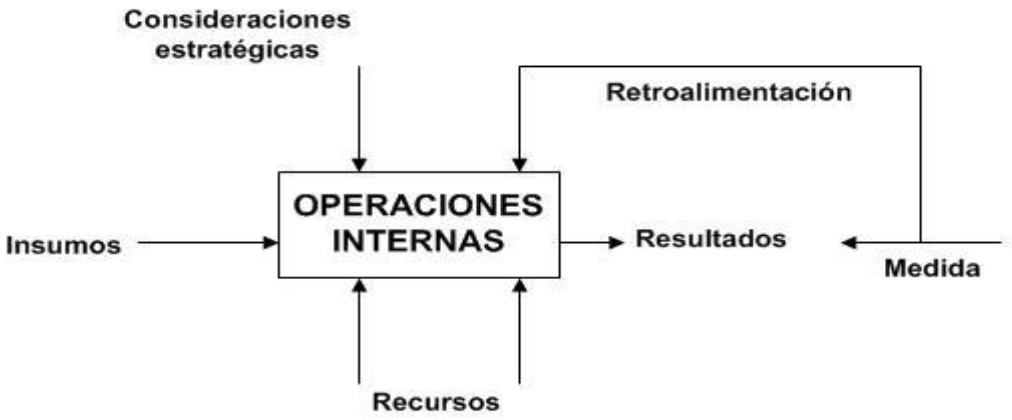


Figura 2.9.1. Enfoque a procesos del ISO 27001:2005

El modelo está concebido para que opere con base en insumos provenientes de stakeholders, clientes, proveedores, usuarios, accionistas, socios y otras partes interesadas.

Estos insumos a través de las operaciones internas del SGSI, proporcionan resultados concretos del desempeño del SGSI. La norma exige que el mecanismo de retroalimentación para controlar el desempeño del SGSI se establezca y se diseñe métrica para, por medio de indicadores, poder medir su desempeño.

El enfoque a procesos del SGSI también contempla los recursos que deben ser provistos para que las operaciones internas funcionen adecuadamente.

El modelo ISO 27001:2005, en su óptica de procesos, también permite que cada organización influencie el desempeño del modelo a través de consideraciones estratégicas, tales como objetivos y políticas particulares de la firma.

2.10. ISO 27002

ISO 27002 es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la estandarización de la Organización Internacional y por la Comisión electrotécnica Internacional en el año 2000, con el título de Tecnología Internacional - Técnicas de Seguridad - Código de buenas prácticas para la gestión de información de seguridad. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995.

La ISO 27002 también llamada ISO/IEC 17799:2000, es de uso obligatorio en todas las instituciones públicas desde agosto de 2004, estandarizando de esta forma los diversos proyectos y metodologías en este campo, respondiendo a la necesidad de seguridad por el uso intensivo de internet y redes de datos institucionales. La supervisión de su cumplimiento está a cargo de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI.

La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2005 del estándar incluye las siguientes once secciones principales:

1. Política de seguridad.
2. Aspectos organizativos para la seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.

8. Desarrollo y mantenimiento de sistemas.
9. Gestión de incidentes de seguridad de la información.
10. Gestión de continuidad de negocio.
11. Conformidad.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades. Cada cláusula corresponde a los controles enlistados en el anexo A del estándar ISO 27001: 2005.

2.11. Servicio de Valor Añadido (SVA)

Los Servicios de Valor Añadido son aquellos que utilizando como soporte servicios portadores o finales de difusión, añaden algunas características o facilidad al Servicio que les sirve de base. Estos servicios se presentan en régimen de competencia.

La explotación de los Servicios de Valor añadido podrá ser realizada por cualquier persona natural o jurídica, observando las regulaciones contenidas en la ley y sus reglamentos. Para la prestación de estos servicios no se requiere autorización previa; sin embargo, las empresas prestadoras se inscribirán en un registro pertinente.

Según el Reglamento de la Ley de Firmas y Certificados Digitales del DECRETO SUPREMO N° 052-2008-PCM los Prestadores de Servicios de Valor añadido tienen las siguientes funciones:

a) Participar en la transmisión o envío de documentos electrónicos firmados digitalmente, siempre que el usuario lo haya solicitado expresamente.

b) Certificar los documentos electrónicos con fecha y hora cierta (Sellado de Tiempo) o en el almacenamiento de tales documentos, aplicando medios que garanticen la integridad y no repudio de los datos de origen y recepción (Sistema de Intermediación Digital).

c) Generar certificados de autenticación a los usuarios que lo soliciten. Dichos certificados serán utilizados sólo en caso que se requiera la autenticación del usuario para el control de acceso a domicilios electrónicos correspondientes a los servicios vinculados a notificaciones electrónicas. Su uso fuera del servicio, en aplicaciones ajenas al Prestador de Servicios de Valor Añadido que lo emitió, no gozará del amparo de la Infraestructura Oficial de Firma Electrónica.

Dependiendo de las modalidades del Prestador de Servicio de Valor Añadido pueden adoptar cualquiera de las modalidades siguientes:

a) Prestador de Servicios de Valor Añadido con firma digital del usuario final. En este caso, se requiere en determinada etapa del servicio de valor añadido la firma digital del usuario final en el documento.

b) Prestador de Servicios de Valor Añadido sin firma digital del usuario final. En ninguna parte del servicio de valor añadido se requiere la firma digital del usuario final.

En cualquiera de los casos, el Prestador de Servicios de Valor Añadido puede contar con los servicios de un notario o fedatario con diploma de idoneidad técnica registrado ante su correspondiente colegio o asociación profesional, de conformidad con lo establecido en el Decreto Legislativo Nº 681, para los casos de prestación de servicios al amparo de lo señalado en el artículo 35 inciso a) del presente Reglamento.

De las modalidades del Prestador de Servicios de Valor Añadido con firma digital del usuario final. Los Prestadores de Servicios de Valor Añadido que realizan procedimientos con firma digital del usuario final, podrán a su vez adoptar dos modalidades:

a) Sistema de Intermediación Digital cuyo procedimiento concluye con una microforma o microarchivo.

b) Sistema de Intermediación Digital cuyo procedimiento no concluye en microforma o microarchivo.

En la modalidad de Sistema de Intermediación Digital cuyo procedimiento concluye con una microforma o microarchivo y se requiera de una formalidad para la conservación de documentos electrónicos firmados digitalmente, se deberá respetar para tales efectos lo establecido en el artículo 5 del presente Reglamento.

De la modalidad del Prestador de Servicios de Valor Añadido sin firma digital del usuario final. El Prestador de Servicios de Valor Añadido sin firma digital del usuario final se refiere al sistema de Sellado de Tiempo, el cual permite consignar la fecha y hora cierta de la existencia de un documento electrónico.

2.11.1. Las Obligaciones de los SVA

Los Prestadores de Servicios de Valor Añadido (SVA) tienen las siguientes obligaciones:

a) Cumplir con los requerimientos de la Autoridad Administrativa Competente respecto de la Política de Valor Añadido, Declaración de Prácticas de Servicios de Valor Añadido, Política de Seguridad, Política y Plan de Privacidad. Estos documentos deberán ser aprobados por la Autoridad Administrativa Competente dentro del procedimiento de acreditación.

b) Informar a los usuarios de todas las condiciones para la prestación de sus servicios.

c) Mantener la confidencialidad de la información relativa a los usuarios de los servicios, limitando su empleo a las necesidades propias del servicio de valor añadido prestado, salvo orden judicial o pedido del usuario utilizando medios que garanticen el no repudio, debiendo respetar para tales efectos los lineamientos establecidos en la Norma Marco sobre Privacidad.

d) Tener operativo software, hardware y demás componentes adecuados para la prestación de servicios de valor añadido y las condiciones de seguridad adicionales basadas en estándares internacionales o compatibles a los internacionalmente vigentes que aseguren la

interoperabilidad y las condiciones exigidas por la Autoridad Administrativa Competente.

e) Cumplir los términos bajo los cuales obtuvo la acreditación, así como los requerimientos adicionales que establezca la Autoridad Administrativa Competente conforme a lo establecido en el presente Reglamento.

f) Cumplir con las disposiciones de la Autoridad Administrativa Competente a que se refiere el artículo 38 del presente Reglamento.

g) Brindar todas las facilidades al personal autorizado por la Autoridad Administrativa Competente para efectos de supervisión y auditoría.

a) Estas obligaciones podrán ser precisadas por la Autoridad Administrativa Competente, a excepción de las que señale expresamente la Ley.

2.11.2. Responsabilidad por riesgos

Para operar en el marco de la Infraestructura Oficial de Firma Electrónica y afrontar los riesgos que puedan surgir como resultado de sus actividades de valor añadido, los Prestadores de Servicios de Valor Añadido acreditados, de acuerdo a los niveles de seguridad establecidos, deberán cumplir con:

a) Nivel de seguridad Medio: mantener vigente la contratación de seguros o garantías bancarias.

b) Nivel de seguridad Medio Alto: acreditar una certificación internacional, según:

- Sistema de Intermediación Digital cuyo procedimiento concluye con una microforma o microarchivo: certificación de acuerdo al Decreto Legislativo Nº 681.

- Sistema de Intermediación Digital cuyo procedimiento no concluye con una microforma o microarchivo: certificación internacional de calidad para la provisión de sus servicios, de acuerdo a lo establecido por la Autoridad Administrativa Competente.

- Sistema de Sellado de Tiempo: certificación internacional de calidad para la provisión de sus servicios, de acuerdo a lo establecido por la Autoridad Administrativa Competente.

La Autoridad Administrativa Competente establecerá la cuantía mínima de las pólizas de seguros o garantías bancarias, las certificaciones de calidad internacional, así como las medidas tecnológicas correspondientes a cada nivel de seguridad.

Asimismo, la Autoridad Administrativa Competente determinará los criterios para evaluar el cumplimiento de este requisito.

2.12. Sistema de Intermediación Digital (SID)

Un Sistema de Intermediación Digital (SID) es un sistema Web que permite la realización de procesos automatizados de trámite documentario, empleando certificados digitales para realizar autenticaciones y firma digitales que garanticen el no repudio de las transacciones electrónicas realizadas.

El Sistema de Intermediación Digital (SID) comprende los siguientes componentes principales:

- Firma Digital.
- Solicitante.
- Funcionario.
- Servidor Principal.
- Servidor de Domicilios Electrónicos.
- Servidor de Transacciones.
- Servidor de Base de Datos.
- Bitácora digital.

2.13. Gestión de Procesos

Según la ISO 9000 define el proceso como un conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

Los Procesos han existido desde siempre ya que es la forma más natural de organizar el trabajo; otra cosa bien distinta es que los tuviéramos identificados para orientar a ellos la acción. Para ello y en primer lugar, hemos de:

- Determinar sus límites para, en función de su nivel, asignar responsabilidades.
- Identificar sus elementos y factores para determinar sus interacciones y hacer posible su gestión.

2.13.1. Límites de un Proceso

No existe una interacción homogénea sobre los límites de los procesos, ya que varía mucho con el tamaño de la Empresa. Lo realmente importante es adoptar un determinado criterio y mantenerlo a lo largo del tiempo.

Parece lógico que:

a) Los límites del Proceso determinen una unidad adecuada para gestionarlo, en sus diferentes niveles de responsabilidad.
b) Estén fuera del “departamento” para poder interactuar con el resto de Procesos (Proveedores y Clientes).
c) El límite inferior sea n producto con valor.

Teniendo en el punto de vista la tradicional organización por departamentos, en cuanto a su alcance, existirían tres tipos de Procesos:

- Unipersonales.
- Funcionales o intradepartamentales.
- Interfuncionales o interdepartamentales.

2.13.2. Elementos de un Proceso

Todo proceso tiene tres elementos:

a) Un Input (entrada principal)

Producto con unas características objetivas que responda al estándar o criterio de aceptación definido: la factura del suministrador con los datos necesarios.

El Input es un “Producto” que provienen de un suministrador (externo o interno); es la salida de otro proceso (precedente en la cadena de valor) o de un “proceso del proveedor” o “del cliente”.

La existencia del Input es lo que justifica la ejecución sistemática del proceso.

Se adjunta un cuadro con la secuencia de procesos que componen el Proceso del Negocio de una Empresa de fabricación bajo pedido; compruebe el lector como el output de un proceso es el Input del siguiente.

b) El Proceso, la secuencia de actividades propiamente dicha.

Unos factores, medios y recursos con determinados requisitos para ejecutarlo siempre bien a la primera: una persona con la competencia y autoridad necesarias para asentar el compromiso de pago, hardware y software para procesar las facturas, un método de trabajo (procedimientos), un impreso e información sobre qué procesar y cómo (calidad) y cuando entregar el output al siguiente subproceso del proceso administrativo.

Algunos de estos factores del proceso son entradas laterales, es decir, input necesarios o convenientes para la ejecución del proceso, pero cuya existencia no lo desencadena. Son también productos que provienen de otros procesos con los que interactúan.

Un sistema de control conocido con indicadores de funcionamiento del proceso y medidas de resultados del producto del proceso y del nivel de satisfacción del usuario (interno muchas veces).

c) Un output (Salida)

Producto con la calidad exigida por el estándar del proceso: el impreso diario con el registro de facturas recibidas, importe, vencimiento, etc.

La salida es un “producto” que va destinado a un usuario o cliente (externo o interno); el output final de los procesos de la cadena de valor es el input o una entrada para un “proceso del cliente”.

El producto del proceso (salida) ha de tener un valor intrínseco, medible o evaluable, para su cliente o usuario.

En el ejemplo del cuadro, el input del Proceso de Negocio (columna central) serán unas necesidades del cliente y el output puede ser la entrega del producto, la recepción del mismo o la satisfacción percibida al incorporar el producto a un proceso del cliente (percepción de satisfacción de auténtica necesidad).

En la plantilla adjunta, se puede generar alternativas de output en los procesos indicados; la evaluación y selección de la alternativa ha de hacerse con criterios de valor. Normalmente hay dos:

1) Output como “producto tangible”.

2) Output en términos de eficacia del proceso, valor, satisfacción.

Así pues, el input y output, proveedor y cliente, definen los límites de todo proceso que han de ser claros y conocidos para poder asignar la responsabilidad funcional.

LIMITES DE UN PROCESO: ALTERNATIVAS

ENTRADA/INPUT	PROCESO	SALIDA/OUTPUT
	COMERCIAL	
	DETERMINACIÓN Y REVISIÓN DE REQUISITOS	
	DISEÑO DEL PRODUCTO	
	COMPRAS	
	PRODUCCIÓN	
	LOGÍSTICA	

Tabla 2.13.2.1. Límites de un Proceso

LIMITES DE UN PROCESO: ALTERNATIVAS

ENTRADA/INPUT	PROCESO	SALIDA/OUTPUT
Necesidad (Competencias, fecha y coste)	INCORPORACIÓN DE PERSONAL	• Persona con el perfil requerido, el día previsto y al coste estimado. • Persona integrada; pasado un cierto tiempo su cliente interno ha podido "percibir el valor".
	FORMACIÓN	
	COMUNICACIÓN INTERNA	
	MEDICIÓN DE LA SATISFACCIÓN DEL CLIENTE	
	AUDITORÍA INTERNA	
	SEGUIMIENTO Y MEDICIÓN DE LOS PROCESOS	
	MEJORA CONTINUA	
	ENTREGA AL CLIENTE ("Proceso del Negocio")	

Tabla 2.13.2.2. Límites de un Proceso

2.13.3. Factores de un Proceso

- Persona.
  Un responsable y los miembros del equipo de procesos, todas ellas con el conocimiento, habilidades y actitudes (competencias) adecuados. La contratación, integración y desarrollo de las personas la proporciona el proceso de Gestión de personal.

- Materiales.
  Materias primas o semielaboradas, información (muy importante especialmente en los procesos de servicio) con las características adecuadas para su uso. Los materiales suelen ser proporcionados por el proceso de "Compras".

- Recursos Físicos.
  Instalaciones, maquinarias, utillajes, hardware, software que han de estar siempre en adecuadas condiciones de uso. Aquí nos referimos al proceso de Gestión de Proveedores de bienes de inversión y al proceso de Mantenimiento de la Infraestructura.

- Métodos/Planificación del proceso.
  Método de trabajo, procedimientos, hoja de proceso, gama, instrucciones de trabajo, etc. Es la descripción de la forma de utilizar los recursos, quién hace qué, cuándo y ocasionalmente el cómo.

Se incluye el método para la medición y el seguimiento del:

- Funcionamiento del proceso (medición o evaluación).
- Producto del proceso (medida de cumplimiento).
- La satisfacción del cliente (medida de satisfacción).

Un proceso está bajo control cuando su resultado es estable y predecible, lo que equivale a dominar los factores del proceso, supuestamente la conformidad del input. En caso de un funcionamiento incorrecto, poder saber cuál es el factor que lo ha originado es de capital importancia para orientar la acción de mejora (gestión de calidad).

LIMITES, ELEMENTOS Y FACTORES DE UN PROCESO

<table>
<tr><td colspan="2">ENTRADA/INPUT</td><td rowspan="2"></td><td colspan="2">SALIDA/OUTPUT</td></tr>
<tr><td>PRODUCTO</td><td>PROVEEDOR</td><td>PROCESO</td><td>PRODUCTO</td><td>CLIENTE (*)</td></tr>
<tr><td>CARACTERÍSTICAS OBJETIVAS (Requisitos QSP)

CRITERIOS DE EVALUACIÓN</td><td></td><td>PERSONAS
• Responsable del proceso.
• Miembros del equipo.

MATERIALES
• Materias primas.
• Información.

RECURSOS FÍSICOS
• Maquinaria y utillaje.
• Hardware y software.

METODOS DE:
• Operación
• Medición/Evaluación:
Funcionamiento del proceso.
Producto.
Satisfacción del cliente.
CAUSAS</td><td>CARACTERÍSTICAS OBJETIVAS (Requisitos QSP)

CRITERIOS DE EVALUACIÓN

EFECTOS</td><td>SATISFACCIÓN</td></tr>
<tr><td colspan="2">MEDIDAS DE</td><td>Eficiencia y Eficacia</td><td colspan="2"></td></tr>
</table>

Tabla 2.13.2.3. Límites, elementos y factores de un Proceso

(*) Proveedor y Cliente pueden ser varios, internos o externos.

2.13.4. Mapa de Procesos

No hay una aceptación unánime sobre la clasificación de los procesos ni sobre la forma de mostrar la empresa vista como un conjunto de procesos.

La representación gráfica de la empresa facilita la comunicación; la más clásica es el organigrama que permite comunicar la estructura departamental así como mostrar las relaciones de dependencia jerárquicas.

Cada gráfico sirve para una cosa; el organigrama representa la jerarquía pero no refleja los procesos de empresa ni sus interacciones. Al contrario, en el “mapa de procesos” no se ven las relaciones de dependencia jerárquica.

Los grafismos utilizados para hacer los mapas pasan determinados “mensajes”, por lo que vale la pena diseñarlos como herramientas de comunicación; para ello han de ser fáciles de explicar y de comprender y tener una cierta estabilidad en el tiempo.

Afortunadamente la forma de elaborar los mapas no está normalizada; utilicemos la creatividad para hacer “nuestro mapa de procesos”, el que mejor refleje la realidad de nuestra empresa, aquel con el que todos se sientan identificados.

2.13.5. Tipos de procesos

Al no existir normalización ni práctica generalmente aceptada al respecto se va a distinguir a los procesos por su misión, donde se propondrá la siguiente clasificación:

- Procesos Operativos.
- Procesos de Apoyo.
- Procesos de Gestión.
- Procesos de Dirección.

2.13.5.1. Procesos Operativos

Combinan y transforman recursos para obtener el producto o proporcionar el servicio conforme a los requisitos del cliente, aportando en consecuencia un alto valor añadido. Las actividades en ellos incluidas y que no cumplan esta condición, es muy probable que se hagan de manera más eficiente como parte de un proceso de otro tipo.

Estos procesos son también los principales responsables de conseguir los objetivos de la empresa.

2.13.5.2. Procesos de Apoyo

Proporcionan las personas y los recursos físicos necesarios por el resto de procesos y conforme a los requisitos de sus clientes internos.

Aquí incluiríamos:

a) El proceso de Gestión de los recursos humanos (terminología ISO 9001).

Denominado de “Gestión e integración de las personas”. Se dice que una persona está integrada cuando se comporta y toma decisiones coherentes con el escenario (interno y externo). Incluiríamos los procesos de:

- Selección y contratación.
- Promoción interna.
- Integración.
- Comunicación interna.
- Desarrollo de las personas (formación).
- Evaluación de las personas.

Son muchas las empresas que ubican aquí “prevención de riesgos laborales”. Otras pioneras están incorporando la “Gestión del Conocimiento” como proceso de desarrollo de la capacidad de las personas para resolver problemas (generación, difusión y uso del conocimiento).

b) El proceso de Aprovisionamiento en bienes de inversión, maquinarias, utillajes, hardware y software y el proceso de Mantenimiento de la Infraestructura, incluyendo lo que se suele denominar como Servicios Generales.

c) El proceso de Gestión de Proveedores (de materiales). Nosotros operativos preferimos contemplarlo como un proceso de apoyo y con esta denominación; subyace el hecho de que los proveedores son un valiosísimo recurso externo que hay que gestionar e integrar en la empresa.

d) La elaboración y revisión del sistema de Gestión de la Calidad así como los procesos operativos tienen una secuencia y un producto final claros, los procesos de este grupo hemos de verlos como transversales en la medida que proporcionen recursos en diferentes fases del “Proceso de negocio”.

2.13.5.3. Procesos de Gestión

Mediante actividades de evaluación, control, seguimiento y medición aseguran el funcionamiento controlado del resto de procesos, además de proporcionarlos la información que necesitan para tomar decisiones (mejor preventivas que correctoras) y elaborar planes de mejora eficaces.

Como una manifestación de su enfoque a procesos, podrían exigir prioridades a los procesos operativos y que orienten sus esfuerzos a objetivos.

Estos procesos funcionan recogiendo datos del resto de los procesos y procesándolos para convertirlos en información de valor para sus clientes internos; información comprensible, fiable, precisa, oportuna, puntual y, sobre todo, accesible y aplicable para la toma de decisiones.

Estamos hablando de:

- El proceso de Gestión económica, que a su vez se dividirá en varios procesos de alcance específicos.
- El proceso de Gestión de Calidad/ medio ambiente.

Hablando con más rigor, éste proceso sería un sistema de procesos con un conjunto de responsabilidades de ejecución de las diferentes actividades y de cada proceso a establecer en cada empresa:

- Los procesos de control de documentos y control de los registros.
- El proceso de medición de la satisfacción del cliente.
- El de auditoría interna.
- Los procesos de seguimiento y medición del producto y de los procesos.
- Con ellos conectados estarían los procesos de análisis de datos y de mejora.

2.13.5.4. Procesos de Dirección

Los concebimos con carácter transversal a todo el resto de procesos de empresa.

- El proceso de “formulación, comunicación, seguimiento y revisión de la estrategia”.
- “Determinación, despliegue, seguimiento y evaluación de objetivos”. ISO 9001.
- “Comunicación interna”, aunque su ejecución corresponda a personal.
- “Revisión de resultados por Dirección”. Retroalimenta a la determinación de objetivos.

En algunas ocasiones las empresas caen en el eufemismo de “adaptarse al enfoque a procesos simplemente cambiando el título del procedimiento o reemplazando departamento por proceso”, para evitarlo, y dar un sentido finalista, vale la pena vincular la gestión por Procesos con la estrategia de la empresa.

2.14. Definiciones Teóricas Metodológicas

Activo: Cualquier cosa que tenga valor para la organización. [ISO/IEC 13335-1:2004]

Actividad [Activity]: algo que tiene valor para la organización. [ISO/IEC 13335-1:2004]

Administración de riesgos: Actividades coordinadas para dirigir y controlar las medidas necesarias para la observación del riesgo dentro de la Organización.

Alcance [Range]: El límite, o grado, al que un Procedimiento de Proceso, Certificación, Contrato, etc. se aplica. Por ejemplo, el Alcance de la Gestión de Cambio pueden incluir todos los Servicios TI Vivos y relatar Elementos de Configuración, el Alcance de un Certificado ISO/IEC 20000 puede incluir todos los Servicios de TI implementados desde un centro de datos en cuestión.

Amenazas [Threats]: la potencial causa de un incidente no deseado, que puede resultar en daño a un sistema u organización (factor externo). Es cualquier cosa que pueda aprovechar un Vulnerabilidad, cualquier causa potencial de un Incidente puede ser considerada una Amenaza. Este término es comúnmente usado en la Gestión de la Información de Seguridad y la

Gestión de Continuidad del Servicio de TI, pero también aplica a otras áreas tales como Gestión de la Disponibilidad y Problemas.

Análisis de Riesgo: Un sistemático de la información para identificar fuentes y estimar riesgos.

Aplicación [Application]: Programa que provee Funciones requeridas por un Servicio TI. Cada Aplicación podría ser parte de más de un Servicio TI. Una Aplicación se puede ejecutar en uno o más Servidores o Clientes.

Arquitectura de TI: Un marco integrado para evolucionar o dar mantenimiento a la TI existente y adquirir nueva TI para alcanzar las metas estratégicas y de negocio de la empresa.

Arquitectura Empresarial: Mapa de rutas tecnológicas orientada al negocio para el logro de las metas y objetivos de negocio.

Autenticación [Authentication]: El acto de verificar la identidad de un usuario y su elegibilidad para acceder a la información computarizada. La autenticación está diseñada para proteger contra conexiones de acceso fraudulentas.

Acreditación: Es el acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, el Reglamento y las disposiciones dictadas por ella, faculta a las entidades solicitantes reguladas en el presente Reglamento a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.

Archivo: Es el conjunto organizado de documentos producidos o recibidos por una entidad en el ejercicio de las funciones propias de su fin, y que están destinados al servicio.

Archivo Electrónico: Es el conjunto de registros que guardan relación. También es la organización de dichos registros.

Autenticación: Es el proceso técnico que permite determinar la identidad de la persona que firma digitalmente, en función del documento electrónico firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.

Autoridad Administrativa Competente (AAC): Es el organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el presente Reglamento o aquellas que requiera en el transcurso de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI.

Buenas Prácticas [Best Practices]: Actividades o Procesos que se han usado con éxito por más de una Organización. ITIL es un ejemplo de Buenas Prácticas.

Canal seguro: Es el conducto virtual o físicamente independiente a través del cual se pueden transferir datos garantizando una transmisión confidencial y confiable, protegiéndolos de ser interceptados o manipulados por terceros.

Calidad: Característica de un producto, Servicio o Proceso para proporcionar su propio valor. Por ejemplo, un Componente hardware puede ser considerado de alta Calidad si rinde según lo esperado y proporciona la Fiabilidad requerida.

Cambios [Change]: Adición, modificación o eliminación de algo que podría afectar a los Servicios de TI. El Alcance debería incluir todos los Servicios de TI, Elementos de Configuración, Procesos, Documentación etc.

Certificado Digital: Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de claves con una persona natural o jurídica confirmando su identidad. El ciclo de vida de un certificado digital podría comprender:

Confidencialidad (Confidentiality): Propiedad que la información no esté disponible o pueda ser descubierta por usuarios no autorizados, entidades o procesos.

Continuidad: Prevenir, mitigar y recuperarse de una interrupción. Los términos planear la reanudación del negocio, planear la recuperación después de un desastre y planear contingencias, también se pueden usar en este contexto; todos se concentran en los aspectos de recuperación de la continuidad.

Control: Las políticas, procedimientos, practicas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados.

Código de verificación o resumen (hash): Es la secuencia de bits de longitud fija obtenida como resultado de procesar un documento electrónico con un algoritmo, de tal manera que:

(1) El documento electrónico produzca siempre el mismo código de verificación (resumen) cada vez que se le aplique dicho algoritmo.

(2) Sea improbable a través de medios técnicos, que el documento electrónico pueda ser derivado o reconstruido a partir del código de verificación (resumen) producido por el algoritmo.

(3) Sea improbable por medios técnicos, se pueda encontrar dos documentos electrónicos que produzcan el mismo código de verificación (resumen) al usar el mismo algoritmo.

Clave privada: Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital.

Clave pública: Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma digital puesta en dicho documento. La clave pública puede ser conocida por cualquier persona.

Cliente [Customer]: Alguien que compra bienes o Servicios. El Cliente de un Proveedor de Servicios TI es la persona o grupo que define y acuerda el Objetivo de Nivel de Servicio. El término Cliente –customer- es también informalmente usado para Usuario, por ejemplo: "Esta es una Organización focalizada en el Usuario".

Depósito de Certificados: Es el sistema de almacenamiento y recuperación de certificados, así como de la información relativa a éstos, disponible por medios telemáticos.

Destinatario: Es la persona designada por el iniciador para recibir un documento electrónico, siempre y cuando no actúe a título de intermediario.

Dirección de correo electrónico: Es el conjunto de palabras que identifican a una persona que puede enviar y recibir correo. Cada dirección es única y pertenece siempre a la misma persona.

Dirección oficial de correo electrónico: Es la dirección de correo electrónico del ciudadano, reconocido por el Gobierno Peruano para la realización confiable y segura de las notificaciones electrónicas personales requeridas en los procesos públicos.

Esta dirección recibirá los mensajes de correo electrónico que sirvan para informar al usuario acerca de cada notificación o acuse de recibo que haya sido remitida a cualquiera de sus domicilios electrónicos. A diferencia del domicilio electrónico, esta dirección centraliza todas las comunicaciones que sirven para informar al usuario que se ha realizado una actualización de los documentos almacenados en sus domicilios electrónicos. Su lectura es de uso obligatorio.

Disponibilidad (Availability): Propiedad de ser accesible y usable bajo demanda por una entidad autorizada.

Documento: Es cualquier escrito público o privado, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos, y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho, o una actividad humana o su resultado.

Los documentos pueden ser archivados a través de medios electrónicos, ópticos o cualquier otro similar.

Documento electrónico: Es la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos.

Documento oficial de identidad: Es el documento oficial que sirve para acreditar la identidad de una persona natural, que puede ser:

a) Documento Nacional de Identidad (DNI);

b) Carné de extranjería actualizado, para las personas naturales extranjeras domiciliadas en el país; o,

c) Pasaporte, si se trata de personas naturales extranjeras no residentes.

Domicilio electrónico: Está conformado por la dirección electrónica que constituye la residencia habitual de una persona dentro de un Sistema de Intermediación Digital, para la tramitación confiable y segura de las notificaciones, acuses de recibo y demás documentos requeridos en sus procedimientos. En el caso de una persona jurídica el domicilio electrónico se asocia a sus integrantes.

Para estos efectos, se empleará el domicilio electrónico como equivalente funcional del domicilio habitual de las personas naturales o jurídicas.

En este domicilio se almacenarán los documentos y expedientes electrónicos correspondientes a los procedimientos y trámites realizados en el respectivo Sistema de Intermediación Digital. El acceso a este domicilio se realiza empleando un certificado digital de autenticación.

Entidad de Certificación: Es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Empresa: Un grupo de individuos que trabajan juntos para un fin común, por lo general dentro del contexto de una forma organizacional, como una corporación agencia pública, entidad de caridad o fondo.

Estándar: Una práctica de negocio o producto tecnológico que es una práctica aceptada, avalada por la empresa o por el equipo gerencial de TI. Los estándares se pueden implantar para dar soporte a una política o a un proceso, o como respuesta a una necesidad operativa. Así como las políticas, los estándares deben incluir una descripción de la forma en que se detectará el incumplimiento.

Evaluación de riesgos: Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado significativo del riesgo.

Disponibilidad: Propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada. [ISO/IEC 13335-1:2004]

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

Gobierno Electrónico: Es el uso de las Tecnologías de Información y Comunicación para redefinir la relación del gobierno con los ciudadanos y la industria, mejorar la gestión y los servicios, garantizar la transparencia y la participación, y facilitar el acceso seguro a la información pública, apoyando la integración y el desarrollo de los distintos sectores.

Infraestructura Oficial de Firma Electrónica: Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de:

1) La integridad de los documentos electrónicos;

2) La identidad de su autor, lo que es regulado conforme a Ley.

El sistema incluye la generación de firmas digitales, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Certificación para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

Integridad: Es la característica que indica que un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

Interoperabilidad: Según el OASIS Forum Group la interoperabilidad puede definirse en tres áreas:

- Interoperabilidad a nivel de componentes: consiste en la interacción entre sistemas que soportan o consumen directamente servicios relacionados con PKI.

- Interoperabilidad a nivel de aplicación: consiste en la compatibilidad entre aplicaciones que se comunican entre sí.

- Interoperabilidad entre dominios o infraestructuras PKI: consiste en la interacción de distintos sistemas de certificación PKI (dominios, infraestructuras), estableciendo relaciones de confianza que permiten el reconocimiento indistinto de los certificados digitales por parte de los terceros que confían.

Ley: Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.

Incidente de Seguridad: uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazas a la Seguridad de la Información.

ISO 17799: Código de Prácticas para la administración de la Seguridad de la Información de la Organización Internacional para la Estandarización (ISO).

ISO 9001:2000: Código de práctica para la administración de la calidad de la

Organización internacional para la Estandarización (ISO). El ISO 9001:2000 especifica los requisitos para un sistema de administración de calidad para cualquier organización que necesite demostrar su habilidad para ofrecer productos de manera consistente que satisfagan al cliente, a los requisitos regulatorios aplicables y que desee aumentar la satisfacción del cliente.

Incidente: Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de la calidad de ese servicio (alineado a ITIL).

Medios electrónicos: Son los sistemas informáticos o computacionales a través de los cuales se puede generar, procesar, transmitir y archivar de documentos electrónicos.

Medios electrónicos seguros: Son los medios electrónicos que emplean firmas y certificados digitales emitidos por Prestadores de Servicios de

Certificación Digital acreditados, donde el intercambio de información se realiza a través de canales seguros.

Madurez: Indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar las metas y objetivos deseados.

Marco de control: Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.

Niveles de seguridad: Son los diversos niveles de garantía que ofrecen las variedades de firmas digitales, cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma digital para enviar o recibir documentos electrónicos.

No repudio: Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación acreditada en cooperación de una Entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil.

En el ámbito del artículo 2 de la Ley de Firmas y Certificados Digitales, el no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).

Notificación electrónica personal: En virtud del principio de equivalencia funcional, la notificación electrónica personal de los actos administrativos se realizará en el domicilio electrónico o en la dirección oficial de correo electrónico de las personas por cualquier medio electrónico, siempre que permita confirmar la recepción, integridad, fecha y hora en que se produce. Si la notificación fuera recibida en día u hora inhábil, ésta surtirá efectos al primer día hábil siguiente a dicha recepción.

Par de claves: En un sistema de criptografía asimétrica comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.

Organización: La manera en que una empresa está estructurada.

Política: Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos gerenciales de la empresa. Además del contenido de la política, esta debe describir las consecuencias de la falta de cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera en que se verificará y medirá el cumplimiento de la política.

Prestador de Servicios de Certificación: Es toda entidad pública o privada que indistintamente brinda servicios en la modalidad de Entidad de Certificación, Entidad de Registro o Verificación o Prestador de Servicios de Valor Añadido.

Prestador de Servicios de Valor Añadido: Es la entidad pública o privada que brinda servicios que incluyen la firma digital y el uso de los certificados digitales. El presente Reglamento presenta dos modalidades:

a. Prestadores de Servicio de Valor Añadido que realizan procedimientos sin firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido, como Sellado de Tiempo que no requieren en ninguna etapa de la firma digital del usuario final en documento alguno.

b. Prestadores de Servicio de Valor Añadido que realizan procedimientos con firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido como el sistema de intermediación electrónico, en donde se requiere en determinada etapa de operación del procedimiento la firma digital por parte del usuario final en algún tipo de documento.

Prestador de Servicios de Valor Añadido para el Estado Peruano: Es la Entidad pública que brinda servicios de valor añadido, con el fin de permitir la realización de las transacciones públicas de los ciudadanos a través de medios electrónicos que garantizan la integridad y el no repudio de la información (Sistema de Intermediación Digital) y/o registran la fecha y hora cierta (Sello de Tiempo).

Problema: Causa subyacente desconocida de uno o más incidentes.

Procedimiento: Una descripción de una manera particular de lograr algo; una forma establecida de hacer las cosas; una serie de pasos que se siguen en un orden regular definido, garantizando un enfoque consistente y repetitivo hacia las actividades.

Recursos (Asset): Cualquier cosa que tenga valor para la organización.

Registro: En términos informáticos, es un conjunto de datos relacionados entre sí, que constituyen una unidad de información en una base de datos.

Reglamento: El presente documento, denominado Reglamento de la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.

Riesgo (risk): Un posible evento que podría causar daños o pérdidas, a afectar la habilidad de alcanzar objetivos. Un Riesgo es medido por la probabilidad de una Amenaza, la Vulnerabilidad del Activo a esa Amenaza, y por el Impacto que tendría en caso que ocurriera.

Riesgo Residual: el riesgo remanente luego de aplicar un control.

Seguridad de la información [Information Security]: Preservación de la confidencialidad, integridad y disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividades, no repudio y confiabilidad pueden ser también consideradas.

Servicio [Service]: Un medio de entregar Valor a los Clientes facilitando Resultados que los Clientes quieren lograr sin la propiedad de Costes y Riesgos específicos.

Servicio de Valor Añadido: Son los servicios complementarios de la firma digital brindados dentro o fuera de la Infraestructura Oficial de Firma Electrónica que permiten grabar, almacenar, conservar cualquier información remitida por medios electrónicos que certifican los datos de envío y recepción, su fecha y hora, el no repudio en origen y de recepción. El servicio de intermediación electrónico dentro de la Infraestructura Oficial de Firma Electrónica es brindado por persona natural o jurídica acreditada ante la Autoridad Administrativa Competente.

Sistema de Gestión de Seguridad de la Información (SGSI) [Information Security Management System]: Parte del sistema de gestión global, basado en un enfoque de riesgos del negocio, para establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar la seguridad de la información.

Sistema de Intermediación Digital: Es el sistema WEB que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma digital, autenticación y canales seguros.

Sistema de Intermediación Electrónico: Es el sistema WEB que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma electrónica, autenticación y canales seguros.

Sistema WEB (“World Wide Web”): Sistema de documentos electrónicos enlazados y accesibles a través de Internet. Mediante un navegador Web, un usuario visualiza páginas Web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces.

Suscriptor: Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el

representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

Tercero que confía o tercer usuario: Se refiere a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.

Vulnerabilidad [Vulnerability]: una debilidad en un activo, grupo de activos o controles de seguridad que lo protegen, que puede ser aprovechada por una o más amenazas para concretarse (factor interno).

CAPITULO 3: ESTADO DE ARTE

El desarrollo del Sistema de análisis y Evaluación de Riesgos se puede considerar en estado de evolución, donde aún no se han establecido de manera clara las características necesarias para una buena implementación, sin embargo, existen diversas Empresas Internacionales quienes ven la importancia de la Gestión de Riesgos.

Como parte de la presente investigación se analizaron metodologías diferentes para implementar el sistema de análisis y evaluación de riesgos que formará parte de la solución propuesta:

- Gestión de Riesgos en la Actualidad
- Criterio para la Gestión de Riesgo según MAGERIT
- Criterio para la Gestión de Riesgo según ISO/IEC 27005:2008
- Metodología Propuesta

3.1. Gestión de Riesgos en la Actualidad

Existe una diversidad de empresas a nivel Internacional y Nacional que han expresado su preocupación por la Administración de Riesgos de la TI, optando por desarrollar diferentes tipos de conceptos básicos y estudios de implementación de mejores prácticas relacionadas al Servicio de Análisis y evaluación de Riesgos. Dichos estudios son vistos a continuación *[tesina Propuesta metodológica para la administración de riesgos de TI basados en controles SOX alineados a ITIL y COBIT]*:

3.1.1. Estadísticas actuales:

Según estudios realizados por Ernst & Young a nivel Global en el año 2007, encuestó a 1300 organizaciones en 50 países, en representación de 23 Industrias, donde participaron Gerentes de Informática, Gerentes de Seguridad de la Información y otros ejecutivos de TI, se presentan una serie de estadísticas que sustentan la situación actual de las Empresas:

Algunos puntos desplegados relacionados con dichas investigaciones son:

• Según las respuestas de las organizaciones encuestadas más del 80% reconoce haber integrado, parcial o totalmente, sus funciones de seguridad de información con las operaciones de gestión de riesgo, en comparación con el 40%, en 2005, y el 43%, en 2006.

Gráfico 3.1.1. Integración de SI en la Gestión de Riesgos

El 64% de las organizaciones se orientan a la mejora en Seguridad de información por Cumplimientos regulatorios, el 80% de éste porcentaje opina que cumplir con las normas obligatorias han mejorado sus sistemas de seguridad de la información, pero también la gestión de riesgos en general. También es importante mencionar que el 58% y el 45% de las Organizaciones encuestadas consideran que la privacidad de la información y alcanzar los objetivos del negocio son motivos también importantes para la mejora en las prácticas de Seguridad de Información.

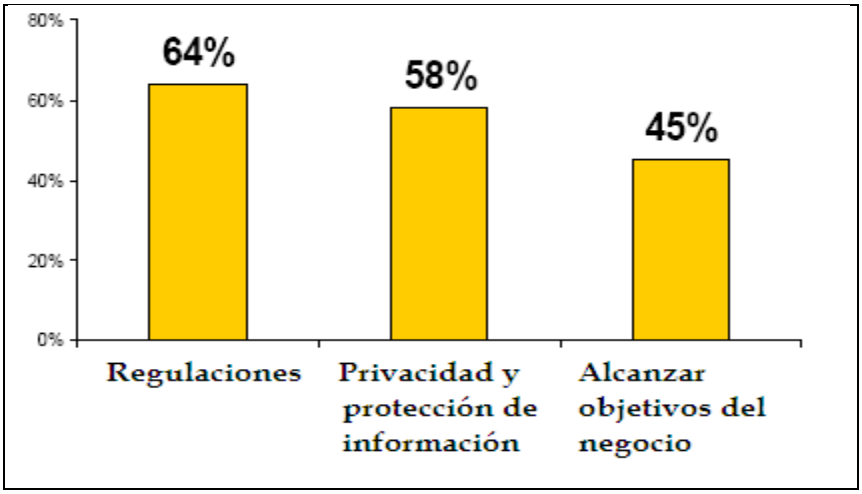


Gráfico 3.12. Motivos para la Mejora de las prácticas en la Seguridad de la información

Entre el 42% y 27% consideran un nivel alto de importancia de la Seguridad de información en la Mejora de Eficiencias operativas y de Tecnologías de Información en las Organizaciones

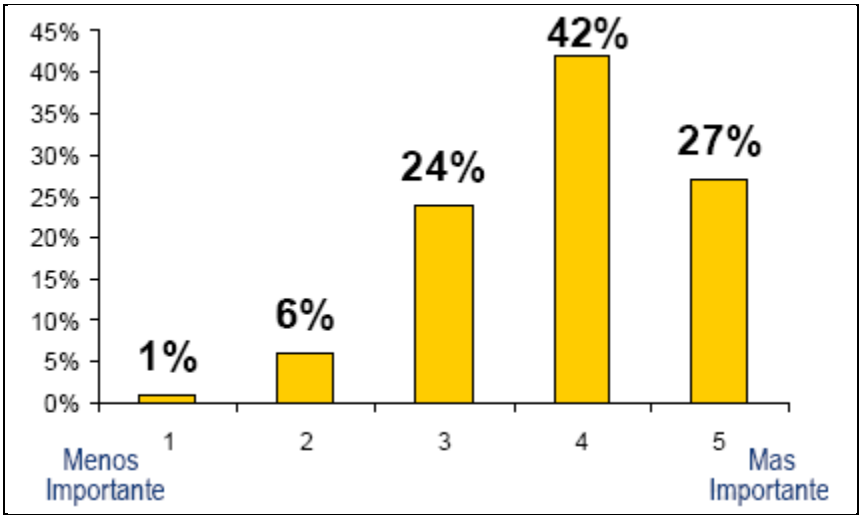


Gráfico 3.1.3. Niveles de Importancia de la Seguridad de la Información en las Organizaciones

Actualmente las organizaciones están demandando mayor atención en la seguridad de su información en los servicios que reciben de proveedores o terceros; por tanto el control interno de la empresa se extiende a los terceros a través de la gestión de la seguridad de información. El 78% de las organizaciones requiere que sus terceros cumplan con las políticas, procedimientos y estándares de la empresa. Este porcentaje se ha incrementado en 12% en relación al 2006.

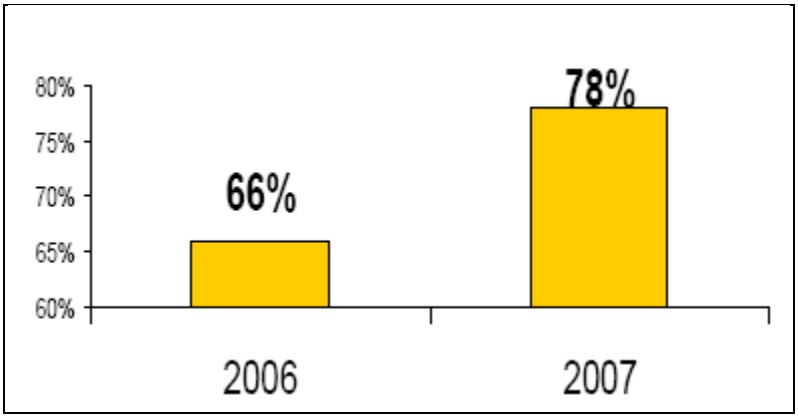


Gráfico 3.1.4. Preocupación de las Organizaciones para que terceros adopten prácticas de Seguridad de la Información

Adicionalmente se cuenta con un Estudio comparativo realizado en Empresas a nivel América sobre temas relacionados con la Gestión de Riesgos de TI:

• Se observa que en Perú y Venezuela la integración del área de Seguridad de Información con el Área de Sistemas en las Empresas es casi total, constituyendo un 93% y 100% respectivamente. Lo cual representa la preocupación de los Altos Directivos en la Gestión de los Riesgos de TI, debido a que no existe un área independiente que se encargue de identificar, gestionar y monitorear los riesgos asociados a los procesos, el establecimiento de controles que mitiguen los riesgos y el desarrollo de indicadores de gestión que permita a la Alta Gerencia tomar decisiones basadas en la tecnología que cuentan; limitando así su funcionamiento a las actividades diarias del Área de Tecnología de Información.

	Perú	Argentina	Brasil	Venezuela	Méjico	EEUU	Canadá
Sí	93%	88%	85%	100%	85%	87%	84%
No	7%	12%	15%	0%	15%	13%	16%

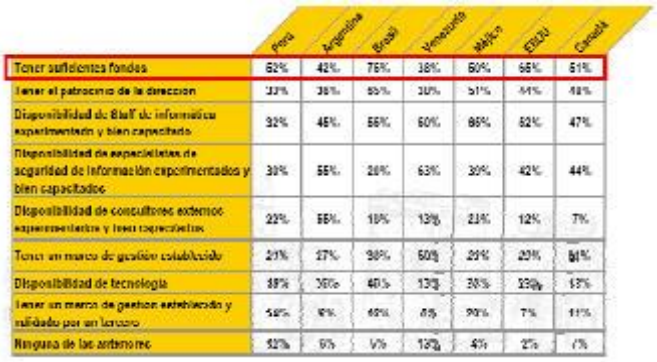
Gráfico 3.1.5. Área de Seguridad de Información en las Empresas

La mayoría de las Empresas en la mayoría de los países de América consideran la Seguridad de Información parte integrada de la Gestión de Riesgos de la Empresa, lo cual permite incluir los riesgos de Tecnologías de Información en la Gestión Global de Riesgos que mantiene la misma, debido a que los riesgos de TI pueden afectar los riesgos en los procesos de negocio.

	Perú	Argentina	Brasil	Venezuela	Méjico	EEUU	Canadá
Totalmente integrada	21%	31%	44%	38%	26%	27%	30%
Parcialmente integrada	66%	38%	44%	38%	44%	54%	49%
Sin integración	13%	31%	13%	25%	30%	19%	22%

Gráfico 3.1.6. Niveles de Interpretación de la seguridad de la Información con la Gestión de Riesgos en la Empresa

Como se muestra en la figura 3.7, existen diversas limitaciones para llevar a cabo Proyectos de Seguridad de Información en las Empresas, pero en lo que todas las Empresas coinciden es la disponibilidad de fondos de la Organización. Por tal motivo es necesario buscar mayor compromiso de parte de las Gerencias para que inviertan en seguridad de información desde una perspectiva de negocio, considerando ventajas de posicionamiento de la Empresa en el mercado por el uso de mejores prácticas asociadas a ésta y establecer iniciativas para el mantenimiento del cumplimiento regulatorio.



	Perú	Argentina	Brasil	Venezuela	México	EEUU	Canadá
Tener suficientes fondos	62%	42%	75%	38%	60%	66%	61%
Tener el patrocinio de la dirección	33%	38%	55%	38%	51%	44%	48%
Disponibilidad de Staff de informática experimentado y bien capacitado	32%	45%	55%	50%	66%	62%	47%
Disponibilidad de especialistas de seguridad de información experimentados y bien capacitados	30%	55%	20%	63%	30%	42%	44%
Disponibilidad de consultores externos experimentados y bien capacitados	22%	55%	10%	13%	21%	12%	7%
Tener un marco de gestión establecido	21%	27%	30%	50%	21%	20%	9%
Disponibilidad de tecnología	18%	36%	40%	13%	36%	23%	13%
Tener un marco de gestión establecido y validado por un tercero	16%	9%	10%	0%	30%	7%	11%
Ninguna de las anteriores	12%	9%	5%	13%	4%	2%	7%

Gráfico 3.1.7. Principales Limitaciones para llevar a cabo proyectos de Seguridad de Información en las Empresas

El mayor porcentaje de encargados de la evaluación de seguridad de información en la Empresa está dado por Auditoría Externa, constituyendo un eje fundamental para la entrega de observaciones y recomendaciones a implementar en las Empresas. Sin embargo es recomendable que a nivel interno también exista un porcentaje equilibrado correspondiente a la evaluación de seguridad de información en la Empresa, de tal manera que sea responsabilidad de la misma, controlar el funcionamiento de los procesos de negocio.

	Perú	Argentina	Brasil	Venezuela	México	EEUU	Canadá
Auditoría Externa	74%	75%	70%	50%	71%	64%	82%
Auditoría Interna	57%	64%	50%	63%	57%	80%	82%
Evaluación de control interno	57%	45%	80%	13%	46%	74%	76%
Evaluación independiente de terceros (ej.: SAS 70)	5%	27%	20%	13%	21%	52%	42%
Otros	12%	9%	5%	13%	8%	7%	7%

Gráfico 3.1.8. Responsable de la Evaluación de Seguridad de Información en la Empresa

A manera de conclusión podemos decir que en promedio más del 50% de Empresas de América se preocupan por el desarrollo de un proceso de evaluación de riesgos. Sin embargo cabe mencionar que la administración de riesgos en el Perú se hace de manera informal o en algunas ocasiones no se toma en cuenta metodologías externas que sustenten el desarrollo del proceso de evaluación.

	Perú	Argentina	Brasil	Venezuela	Méjico	EEUU	Canadá
Sí	66%	45%	70%	71%	52%	57%	53%
No	34%	55%	30%	29%	48%	43%	47%

Gráfico 3.1.9. Desarrollo de una Evaluación formal de Riesgos

En el Perú, la Gestión de Riesgos es importante en las Empresas de diversos sectores. Según las investigaciones realizadas, las Empresas del Perú se preocupan por el desarrollo de un proceso de Sistema de Análisis y evaluación de riesgos. Sin embargo, muchas veces éste proceso no se da de la mejor manera o con la guía correcta de un especialista en implementación de programas de Gestión de Riesgos, basándose en estándares internacionales o en buenas prácticas que ayuden a dirigir un Plan de Gestión de Riesgos del área de TI al Plan de Riesgos integral en la Empresa.

3.2. Criterios para la gestión de riesgos según MAGERIT

MAGERIT cuyo significado es Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, es una metodología española que establece criterios generales para la Gestión de Riesgos de Seguridad de la Información y ha sido creada como respuesta a la percepción de que la Administración española donde depende de forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.

MAGERIT define conceptos y catálogos de amenazas y tipo de activos que sirven de complemento a los criterios establecidos en el estándar ISO 27005:2008 y que son utilizados en la presente investigación para el desarrollo del análisis de riesgos del modelo general de proceso de la SVA tipo Sistema de Intermediación Digital (SID).

3.2.1. Objetivos de MAGERIT

MAGERIT persigue los siguientes objetivos:

1. Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.

2. Ofrecer un método sistemático para analizar tales riesgos.

3. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Aquí se muestra una explicación detallada de la elaboración de los Requerimientos de Seguridad basados en los criterios según MAGERIT, que se aplicarán para los Servicios de Valor Añadido (SVA).

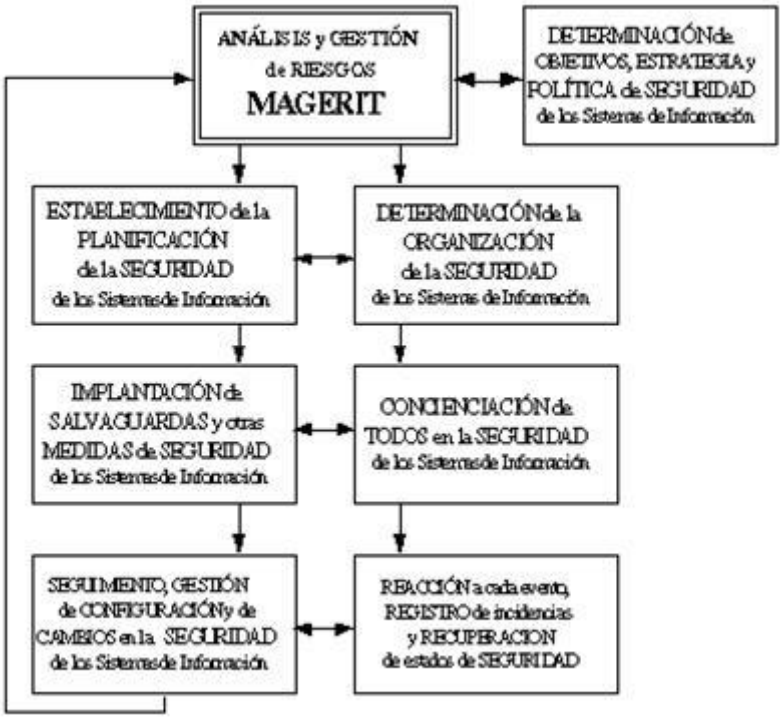


Tabla 3.2.1. Análisis y Gestión de Riesgos MAGERIT

Para la elaboración del Análisis de Riesgos del presente trabajo de Investigación se realizaron criterios según la metodología establecida por MAGERIT.

3.2.2. Requerimientos de seguridad

3.2.2.1. Disponibilidad

Aseguramiento de que los usuarios autorizados tienen acceso cuando requieran de la información y de sus activos asociados.

¿Qué importancia tendría que el activo no estuviera disponible?

Un activo debe recibir un gran valor desde el punto de vista de disponibilidad cuando: las consecuencias en el negocio, en caso una amenaza afectara a su disponibilidad, pudieran ser graves.

A menudo la disponibilidad requiere un tratamiento por escalones pues el coste de la indisponibilidad aumenta de forma no lineal con la duración de la

interrupción, desde breves interrupciones sin importancia, pasando por interrupciones que causan daños considerables y llegando a interrupciones que no admiten recuperación.

3.2.2.2. Integridad de los datos

Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

¿Qué importancia tendría que los datos fueran modificados fuera de control?

Los datos deben recibir una alta valoración desde el punto de vista de integridad cuando: su alteración, voluntaria o intencionada, pudiera causar graves daños a la organización.

3.2.2.3. Confidencialidad de los datos

Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

Los datos deben recibir una alta valoración desde el punto de vista de confidencialidad cuando su revelación pudiera causar graves daños a la organización.

3.2.2.4. Autenticidad de los usuarios del servicio

Aseguramiento de la identidad u origen.

¿Qué importancia tendría que quien accede al servicio no se realmente quien se cree?

La falta de controles que permitan asegurar la autenticidad de los usuarios de un servicio genera la oportunidad de fraude o uso no autorizado de un servicio. En este sentido un servicio debe recibir una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para la organización.

3.2.2.5. No repudio

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

¿Qué importancia tendría que no quedara constancia del acceso a los datos?

Abriría las puertas al fraude, incapacitaría a la Organización para perseguir delitos y podría suponer el incumplimiento de obligaciones legales.

La importancia de la Gestión de Riesgos deriva de que es la herramienta que nos va a permitir identificar las amenazas a las que se encuentran expuestos dichos activos, estimar la frecuencia de materialización de tales amenazas y valorar el impacto que supondría en nuestra Organización esa materialización.

3.2.3. Catálogo de Amenazas

3.2.3.1. Desastres Naturales

Fuego:
Incendios: Posibilidad de que el fuego acabe con recursos del sistema.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Redes de comunicaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Medios de almacenamiento	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Equipamiento auxiliar	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Instalaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

Daños por agua:

Inundaciones: Posibilidad de que el agua acabe con recursos del sistema.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Redes de comunicaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Medios de almacenamiento	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Equipamiento auxiliar	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Instalaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

Desastres naturales

Incidentes que se producen sin intervención humana: rayos, tormentas eléctricas, terremotos, ciclones, avalanchas, sismos, etc.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Redes de comunicaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Medios de almacenamiento	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Equipamiento auxiliar	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Instalaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

3.2.3.2. De Origen Industrial

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

Fuego

Incendio: Posibilidad de que el fuego acabe con recursos del sistema.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Redes de comunicaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Medios de almacenamiento	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Equipamiento auxiliar	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Instalaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

Daños por agua

Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Redes de comunicaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Medios de almacenamiento	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Equipamiento auxiliar	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Instalaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

Desastres industriales

Desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Redes de comunicaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Medios de almacenamiento	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Equipamiento auxiliar	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Instalaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

Contaminación mecánica

Vibraciones, polvo, suciedad, etc.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Redes de comunicaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Medios de almacenamiento	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Equipamiento auxiliar	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Instalaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

Contaminación electromagnética

Interferencias de radio, campos magnéticos, luz ultravioleta, etc.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

Redes de comunicaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Medios de almacenamiento	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Equipamiento auxiliar	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Instalaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

Avería de origen físico o lógico

Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Redes de comunicaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Medios de almacenamiento	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Equipamiento auxiliar	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Aplicaciones de software	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

Corte del suministro eléctrico

Cese de la alimentación de potencia.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	disponibilidad
Redes de comunicaciones	disponibilidad
Medios de almacenamiento	disponibilidad
Equipamiento auxiliar	disponibilidad

Condiciones inadecuadas de temperatura y/o humedad

Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Redes de comunicaciones	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Medios de almacenamiento	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos
Equipamiento auxiliar	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

Fallo de servicios de comunicaciones

Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.

Tipos de activos afectados	Principios de seguridad afectados
Redes de comunicaciones	disponibilidad

Interrupción de otros servicios y suministros esenciales

Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante, etc.

Tipos de activos afectados	Principios de seguridad afectados
Equipamiento auxiliar	disponibilidad

Degradación de los soportes de almacenamiento de la información

Como consecuencia del paso del tiempo.

Tipos de activos afectados	Principios de seguridad afectados
Medios de almacenamiento	Disponibilidad, trazabilidad de los servicios, trazabilidad de los datos

Emanaciones electromagnéticas

Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos (hardware)	confidencialidad
Redes de comunicaciones	confidencialidad

3.2.3.3. Errores y Fallos no intencionados

Errores de los usuarios

Equivocaciones de las personas cuando usan los servicios, datos, etc.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Integridad, disponibilidad
Datos	Integridad, disponibilidad
Aplicaciones de software	Integridad, disponibilidad

Errores del administrador

Equivocaciones de personas con responsabilidades de instalación y operación.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Datos	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Aplicaciones de software	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Equipos informáticos	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Redes de comunicaciones	Integridad, disponibilidad,

	autenticidad del servicio, autenticidad de datos confidencialidad

Errores de monitorización (log)

Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Trazabilidad del servicio Trazabilidad de los datos
Datos	Trazabilidad del servicio Trazabilidad de los datos
Aplicaciones de software	Trazabilidad del servicio Trazabilidad de los datos

Errores de configuración

Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Datos	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Aplicaciones de software	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos Confidencialidad
Equipos informáticos	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Redes de comunicaciones	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad

Deficiencias en la organización

Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.

Tipos de activos afectados	Principios de seguridad afectados
Aplicaciones	Disponibilidad

Difusión de software dañino

Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

Tipos de activos afectados	Principios de seguridad afectados
Aplicaciones de software	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos Confidencialidad Trazabilidad de datos, trazabilidad de servicio

Errores de [re-]encaminamiento

Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Autenticidad del servicio, autenticidad de datos Confidencialidad Integridad
Aplicaciones de software	Autenticidad del servicio, autenticidad de datos Confidencialidad Integridad
Redes de comunicaciones	Autenticidad del servicio, autenticidad de datos Confidencialidad Integridad

Errores de secuencia

Alteración accidental del orden de los mensajes transmitidos.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Integridad
Aplicaciones de software	Integridad
Redes de comunicaciones	Integridad

Escapes de información

La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Confidencialidad
Aplicaciones de software	Confidencialidad
Redes de comunicaciones	Confidencialidad

Alteración de la información

Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Integridad

Introducción de información incorrecta

Inserción accidental de información incorrecta. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Integridad

Degradación de la información

Degradación accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Integridad

Destrucción de información

Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Disponibilidad

Divulgación de información

Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Confidencial

Vulnerabilidades de los programas (software)

Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.

Tipos de activos afectados	Principios de seguridad afectados
Aplicaciones de software	Integridad Disponibilidad Confidencial

Errores de mantenimiento / actualización de programas (software)

Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

Tipos de activos afectados	Principios de seguridad afectados
Aplicaciones de software	Integridad Disponibilidad

Errores de mantenimiento / actualización de equipos (hardware)

Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos de hardware	Disponibilidad

Caída del sistema por agotamiento de recursos

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Disponibilidad
Equipos informáticos	Disponibilidad
Redes de comunicaciones	Disponibilidad

Indisponibilidad del personal

Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, etc.

Tipos de activos afectados	Principios de seguridad afectados
Personal interno	Disponibilidad

3.2.3.4. Ataques Intencionados

Manipulación de la configuración

Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Autenticidad del servicio, autenticidad de datos Confidencialidad Integridad Disponibilidad Trazabilidad del servicio Trazabilidad de datos
Datos	Autenticidad del servicio, autenticidad de datos Confidencialidad

	Integridad Disponibilidad Trazabilidad del servicio Trazabilidad de datos
Aplicaciones de software	Autenticidad del servicio, autenticidad de datos Confidencialidad Integridad Disponibilidad Trazabilidad del servicio Trazabilidad de datos
Equipos informáticos	Autenticidad del servicio, autenticidad de datos Confidencialidad Integridad Disponibilidad Trazabilidad del servicio Trazabilidad de datos
Redes de comunicaciones	Autenticidad del servicio, autenticidad de datos Confidencialidad Integridad Disponibilidad Trazabilidad del servicio Trazabilidad de datos

Suplantación de la identidad del usuario

Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Autenticidad del servicio, autenticidad de datos Confidencialidad Integridad
Aplicaciones de software	Autenticidad del servicio, autenticidad de datos Confidencialidad Integridad
Redes de comunicaciones	Autenticidad del servicio, autenticidad de datos Confidencialidad Integridad

Abuso de privilegios de acceso

Cuando un usuario, operador o administrador abusa de su nivel de privilegios para realizar tareas que no son de su competencia.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Datos	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Aplicaciones de software	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Equipos informáticos	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Redes de comunicaciones	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad

Uso no previsto

Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Disponibilidad
Aplicaciones de software	Disponibilidad
Equipos informáticos	Disponibilidad
Redes de comunicaciones	Disponibilidad
Medios de almacenamiento	Disponibilidad
Equipamiento auxiliar	Disponibilidad
Instalaciones	Disponibilidad

Difusión de software dañino

Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad
Aplicaciones de software	Integridad, disponibilidad, autenticidad del servicio, autenticidad de datos confidencialidad

[Re-] encaminamiento de mensajes

Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información adonde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Integridad, autenticidad del servicio, autenticidad de datos, trazabilidad del servicio, confidencialidad

Alteración de secuencia

Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Integridad

Acceso no autorizado

El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

Tipos de activos afectados	Principios de seguridad afectados

Servicios	Confidencialidad, integridad, autenticidad del servicio
Datos	Confidencialidad, integridad
Aplicaciones de software	Confidencialidad, integridad
Equipos informáticos	Confidencialidad, integridad
Redes de comunicaciones	Confidencialidad, integridad
Medios de almacenamiento	Confidencialidad, integridad
Equipamiento auxiliar	Confidencialidad, integridad
Instalaciones	Confidencialidad, integridad

Análisis de tráfico

El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.

Tipos de activos afectados	Principios de seguridad afectados
Redes de comunicaciones	Confidencialidad

Repudio

Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.

Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación.

Repudio de recepción: negación de haber recibido un mensaje o comunicación.

Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Trazabilidad del servicio

Interceptación de información (escucha)

El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Confidencialidad
Aplicaciones de software	Confidencialidad
Equipos informáticos	Confidencialidad
Redes de comunicaciones	Confidencialidad

Modificación de la información

Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Integridad

Introducción de falsa información

Inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Integridad

Corrupción de la información

Degradación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Integridad

Destrucción la información

Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.

Tipos de activos afectados	Principios de seguridad afectados
Datos	Integridad

Divulgación de información

Tipos de activos afectados	Principios de seguridad afectados
Datos	Confidencialidad

Manipulación de programas

Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

Tipos de activos afectados	Principios de seguridad afectados
Aplicaciones de software	Confidencialidad, integridad, autenticidad del servicio, autenticidad de datos, trazabilidad del servicio, trazabilidad de los datos

Denegación de servicio

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

Tipos de activos afectados	Principios de seguridad afectados
Servicios	Disponibilidad
Equipos informáticos	Disponibilidad
Redes de comunicaciones	Disponibilidad

Robo

La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos	Disponibilidad, confidencialidad de datos
Redes de comunicaciones	Disponibilidad, confidencialidad de datos
Medios de almacenamiento	Disponibilidad, confidencialidad de datos
Equipamiento auxiliar	Disponibilidad

Ataque destructivo

Vandalismo, terrorismo, acción militar, etc.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos	Disponibilidad
Redes de comunicaciones	Disponibilidad
Medios de almacenamiento	Disponibilidad
Equipamiento auxiliar	Disponibilidad
Instalaciones	Disponibilidad

Ocupación enemiga

Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.

Tipos de activos afectados	Principios de seguridad afectados
Equipos informáticos	Disponibilidad, confidencialidad

Redes de comunicaciones	Disponibilidad, confidencialidad
Medios de almacenamiento	Disponibilidad, confidencialidad
Equipamiento auxiliar	Disponibilidad, confidencialidad
Instalaciones	Disponibilidad, confidencialidad

Indisponibilidad del personal

Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc.

Tipos de activos afectados	Principios de seguridad afectados
Personal interno	Disponibilidad

Extorsión

Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.

Tipos de activos afectados	Principios de seguridad afectados
Personal interno	Integridad, autenticidad del servicio, autenticidad de datos, trazabilidad del servicio, trazabilidad de datos, confidencialidad

Ingeniería social

Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

Tipos de activos afectados	Principios de seguridad afectados
Personal interno	Integridad, autenticidad del servicio, autenticidad de datos, trazabilidad del servicio, trazabilidad de datos, confidencialidad

3.2.4. Tipos de activos

1. [S] **Servicios**: los servicios pueden aparecer bien como servicios finales (prestados por la Organización a terceros), bien como servicios instrumentales (donde tanto los usuarios como los medios son propios), bien como servicios contratados (a otra organización que los proporciona con sus propios medios).

[anon] anónimo (sin requerir identificación del usuario)
[pub] al público en general (sin relación contractual)
[ext] a usuarios externos (bajo una relación contractual)
[int] interno (usuarios y medios de la propia organización)
[cont] contratado a terceros (se presta con medios ajenos)
[www] world wide web
[telnet] acceso remoto a cuenta local
[email] correo electrónico
[file] almacenamiento de archivos
[ftp] transferencia de archivos
[edi] intercambio electrónico de datos
[dir] servicio de directorio
[idm] gestión de identidades
[ipm] gestión de privilegios
[pki] PKI - infraestructura de clave pública

2. [D] **Datos/Información**: elementos de información que, de individuales o agrupados, representan el conocimiento que se tiene de algo. Los datos son el principal activo que permite a una organización prestar sus servicios. Se encuentran almacenados en equipos o soportes de información (normalmente agrupado en forma de bases de datos) o son transferidos de un lugar a otro por los medios de transmisión de datos.

[vr] datos esenciales para la supervivencia de la Organización
[com] datos de interés comercial
[adm] datos de interés para la administración pública
[int] datos de gestión interna
[voice] voz
[multimedia] multimedia
[source] código fuente
[exe] código ejecutable

[conf] datos de configuración
[log] registro de actividad (log)
[test] datos de prueba
[per] datos de carácter personal
[label] datos clasificados
[S] secreto
[R] reservado
[C] confidencial
[DL] difusión limitada
[SC] sin clasificar

3. [SW]**Aplicaciones de software**: las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. No preocupa en este apartado el denominado "código fuente" o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.

[prp] desarrollo propio (in house)
[sub] desarrollo a medida (subcontratado)
[std] estándar (off the shelf)
[browser] navegador web
[www] servidor de presentación
[app] servidor de aplicaciones
[email_client] cliente de correo electrónico
[file] servidor de ficheros
[dbms] sistema de gestión de bases de datos
[tm] monitor transaccional
[office] ofimática
[av] anti virus
[os] sistema operativo
[ts] servidor de terminales
[backup] sistema de backup

4. [HW]**Equipos informáticos**: bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, sirviendo como almacenamientos temporales o permanentes de los datos,

soportes de ejecución de las aplicaciones de software, del procesamiento o la transmisión de datos.

[pc]	computadores personales
[mobile]	computadores móviles
[pda]	agendas electrónicas
[easy]	fácilmente reemplazables
[data]	que almacena datos
[peripheral]	periféricos
[print]	medios de impresión
[scan]	escáneres
[crypto]	dispositivos criptográficos
[network]	soportes de la red
[modem]	módems
[hub]	concentradores
[switch]	conmutadores
[router]	encaminadores
[bridge]	pasarelas
[firewall]	cortafuegos
[wap]	punto de acceso wireless
[pabx]	centralita telefónica

5. [COM]**Redes de comunicaciones**: medios de transporte que llevan datos de un sitio a otro, incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.

[PSTN]	red telefónica
[ISDN]	rdsi (red digital)
[X25]	X25 (red de datos)
[ADSL]	ADSL
[pp]	punto a punto
[radio]	red inalámbrica
[sat]	por satélite
[LAN]	red local
[MAN]	red metropolitana
[Internet]	Internet
[vpn]	red privada virtual

6. [ALM]**Medios de almacenamiento**: dispositivos físicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo.

[electronic] electrónicos
[disk] discos
[san] almacenamiento en red
[disquette] disquetes
[cd] CD-ROM
[usb] dispositivos USB
[dvd] DVD
[tape] cinta magnética
[mc] tarjetas de memoria
[ic] tarjetas inteligentes
[non_electronic] no electrónicos
[printed] material impreso
[tape] cinta de papel
[film] microfilm
[cards] tarjetas perforadas

7. [AUX]**Equipamiento auxiliar**: equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

[power] fuentes de alimentación
[ups] sistemas de alimentación ininterrumpida
[gen] generadores eléctricos
[ac] equipos de climatización
[cabling] cableado
[robot] robots
[supply] suministros esenciales
[destroy] equipos de destrucción de soportes de información
[furniture] mobiliario: armarios, etc
[safe] cajas fuertes

8. [L]**Instalaciones**: lugares donde se hospedan los activos de información y comunicaciones.

[site] emplazamiento

[building] edificio

[local] local

[mobile] plataformas móviles

[car] vehículo terrestre: coche, camión, etc.

[plane] vehículo aéreo: avión, etc.

[ship] vehículo marítimo: buque, lancha, etc.

[shelter] contenedores

[channel] canalización

9. [P] **Personal**: personas relacionadas con los sistemas de información.

[ue] usuarios externos

[ui] usuarios internos

[op] operadores

[adm] administradores de sistemas

[com] administradores de comunicaciones

[dba] administradores de BBDD

[des] desarrolladores

[sub] subcontratas

[prov] proveedores

3.3. Análisis y Gestión de Riesgos según el estándar ISO 27005:2008

ISO 27005:2008 “derogó” las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000, y proporciona desde su publicación en Junio del año 2008, un conjunto de directrices para la correcta realización de un Análisis de Riesgos.

El estándar ISO 27005:27008 fue creado para complementar los lineamientos generales definidos en el estándar ISO 27001:2005, en particular respecto del proceso de Gestión del Riesgo. Este estándar define la Gestión de Riesgos de la Seguridad de la Información como un enfoque sistemático necesario para identificar las necesidades organizacionales respecto de los requerimientos de seguridad de la información y crear un efectivo Sistema de Gestión de la Seguridad de la Información (SGSI). Este enfoque debería estar ajustado al contexto de la organización y en particular debería estar alineado a la Gestión de Riesgos de todas las empresas.

Gráfico 3.3. ISO 27005:2008 – Gestión de Riesgos

La gestión del riesgo permite analizar qué puede pasar y las posibles consecuencias que pueden ocurrir, antes de decidir qué debería hacerse y el cuándo, de modo que los esfuerzos de seguridad, en particular los controles que se implementen, sean direccionados en una manera efectiva y oportuna

de modo que sean implementados solamente dónde y cuándo sean necesarios, a fin de reducir los riesgos a un nivel aceptable.

La gestión de riesgos de la seguridad de la información debería ser un proceso continuo. Este proceso debería primero establecer el contexto, luego evaluar los riesgos y tratarlos mediante un plan de tratamiento del riesgo acorde recomendaciones y decisiones tomadas.

La efectividad del tratamiento del riesgo depende de los resultados del análisis del riesgo. Es posible que el tratamiento adoptado no logre obtener inmediatamente un nivel de riesgo residual aceptable. En tal caso, es necesario repetir el análisis del riesgo cambiando los parámetros que rigen el contexto, en un proceso cíclico de mejora continua.

ISO 27005:2008 no proporciona una metodología concreta de Análisis de Riesgos, sino que describe el proceso recomendado de análisis incluyendo las fases que lo conforman:

- Establecimiento del contexto
- Evaluación del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitorización y revisión del riesgo

La siguiente tabla resume las actividades relevantes de la gestión de riesgos de la seguridad de la información, los cuales serán descritos con mayor profundidad en las siguientes secciones:

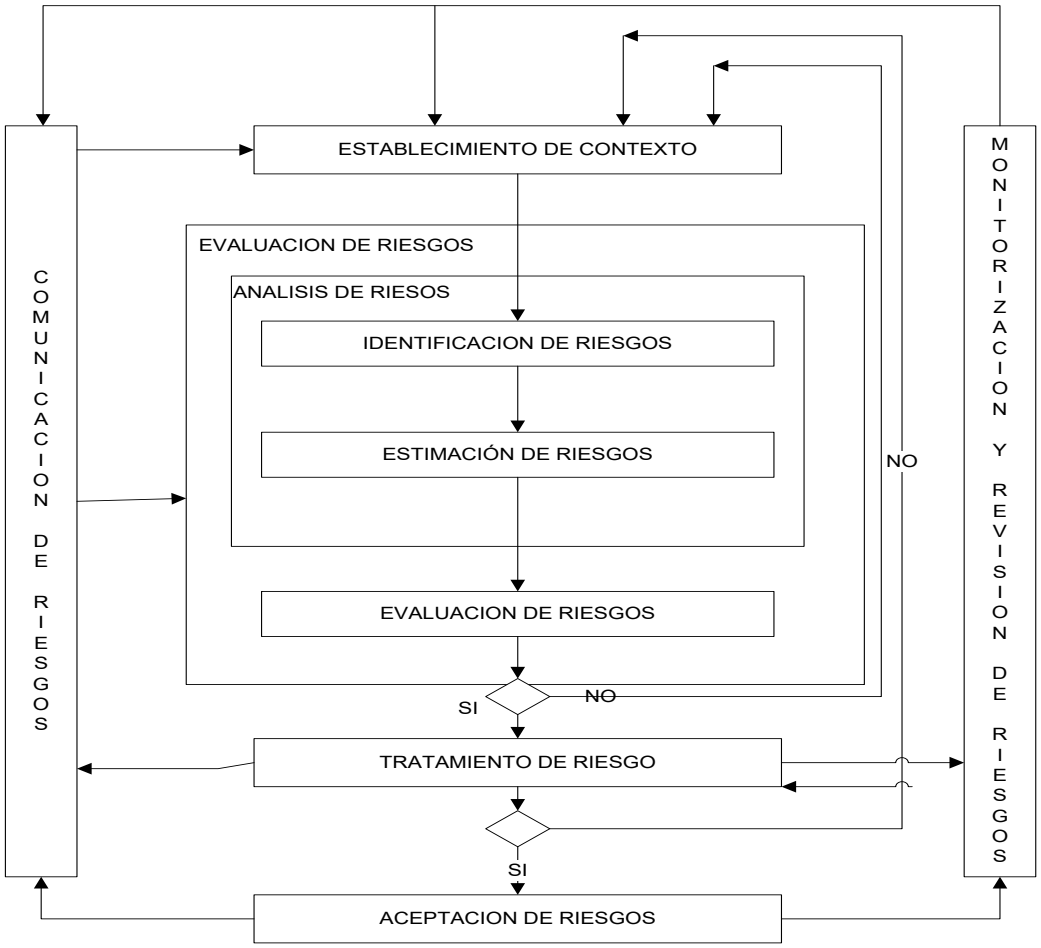


Tabla 3.3. Proceso de Análisis de Riesgo ISO 27005:2008

Los puntos que se utilizarán en éste trabajo de investigación se mencionan a continuación:

3.3.1. Establecimiento del contexto:

3.3.1.1. Criterios de evaluación del riesgo

Los criterios de evaluación de riesgo deben ser desarrollados para evaluar los riesgos de la seguridad de la información considerando lo siguiente:

- El valor estratégico de los procesos de información del negocio
- La criticidad de los activos de información involucrados
- Requerimientos legales y regulatorios, y obligaciones contractuales

- Importancia de la disponibilidad, confidencialidad e integridad operacional y del negocio.

- Expectativas percepciones de los interesados (stakeholeders), y consecuencias negativas contra la imagen y la reputación.

Adicionalmente, los criterios de riesgo aceptable deben ser usados para priorizar el tratamiento del riesgo.

3.3.1.2. Criterios de evaluación de impacto

Los criterios de impacto deberían ser desarrollados y especificados en términos de estimar el daño o costo que un evento de seguridad pueda causar sobre la organización, considerando lo siguiente:

- Nivel de clasificación de los activos de información impactados

- Brechas en la seguridad de la información (Por ejemplo, pérdida de la confidencialidad, integridad y disponibilidad)

- Operaciones relacionadas (internas o con terceras partes)

- Pérdidas de valor comercial y financiero

- Interrupción de planes y metas

- Daños en la reputación

- Incumplimiento de los requerimientos legales, regulatorios y contractuales.

3.3.1.3. Criterios de aceptación del riesgo

Los criterios de aceptación del riesgo deberían ser desarrollados y especificados. Y deben depender frecuentemente de las políticas, metas, objetivos e intereses de los stakeholders.

Cada organización debería definir sus propias escalas para establecer los niveles de riesgo aceptable. Para su desarrollo se debe considerar lo siguiente:

- Los criterios de aceptación de riesgos pueden incluir múltiples objetivos, con un deseado nivel de riesgo, pero con la provisión del gerente general para aceptar los riesgos que superen este nivel bajo determinadas circunstancias.

- Los criterios de aceptación del riesgo puede ser expresado como una tasa de estimación para estimar el riesgo.

- Se pueden aplicar diferentes criterios de aceptación del riesgo para diferentes clases de riesgo

- Los criterios de aceptación del riesgo pueden incluir requerimientos para futuros tratamientos.

3.3.2. Evaluación de riesgos

3.3.2.1. El enfoque y las fronteras

El enfoque de los procesos de gestión de la seguridad de la información deben ser definidos para asegurar que todos los activos relevantes son tomados en cuenta en la evaluación.

3.3.2.2. Organización para la gestión de riesgos de la información

Los siguientes son los principales roles y responsabilidades de la organización:

- El desarrollo de los procesos de gestión de la seguridad de la información debe ser ajustado a la organización.

- Identificación y análisis de los stakeholders.

- Definición de roles y responsabilidades de todas las partes internas y externas a la organización.

- Establecimiento de las relaciones requeridas entre la organización y los stakeholders, tal como las interfaces a las funciones de gestión de riesgos de alto nivel de la

organización tal como interfaces a otros proyectos o actividades relevantes.

3.3.3. Evaluación de riesgos de seguridad de la información:

3.3.3.1. Identificación de activos

Un activo es cualquier cosa que genere valor para la organización y que por lo cual requiere de protección. La identificación de activos debe ser realizada a un nivel de detalle provea suficiente información para la evaluación de riesgos.

3.3.3.2. Identificación de amenazas

Una amenaza tiene el potencial de dañar los activos como la información, procesos y sistemas y demás organizaciones.

3.3.3.3. Identificación de controles existentes

La identificación de controles existentes debería ser hecha para impedir trabajos o costos adicionales.

3.3.3.4. Identificación de vulnerabilidades

Las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o a la organización debería ser identificado.

3.3.3.5. Identificación de consecuencias

Las consecuencias que la pérdida de confidencialidad, integridad y disponibilidad deben tener sobre los activos deberían ser identificadas. Una consecuencia puede ser la pérdida de efectividad, condiciones operativas adversas, pérdidas comerciales, reputación, daño, etc.

3.3.3.6. Evaluación de consecuencias

El impacto en el negocio de la organización que puede resultar de posibles o actuales incidentes deberían ser direccionados, tomando en cuenta las consecuencias de una brecha de la seguridad de la información como la pérdida de confidencialidad, integridad o disponibilidad de los activos.

3.3.3.7. Evaluación de la probabilidad de un incidente

Después de identificar los escenarios de los incidentes, es necesaria la evaluación de la probabilidad de cada e impacto ocurrido, usando técnicas de estimación cualitativas y cuantitativas. Estas estimaciones deberían tomar en cuenta de cuan frecuentemente ocurren las amenazas y cuan fácilmente las vulnerabilidades pueden ser explotadas, considerando:

- Experiencia y estadísticas aplicables para estimar la probabilidad de que la amenaza ocurra.
- Para fuentes de amenazas deliberadas: la motivación y capacidades, las cuales cambiarán en el tiempo, y recursos disponibles para los posibles atacantes, tal como la percepción de del valor o atractivo del activo y para el posible atacante y de las vulnerabilidades que pueden ser explotadas.
- Para fuentes de amenazas accidentales: factores geográficos (por ejemplo, proximidad

3.3.4. Estimación del riesgo

El ***riesgo*** es una función de la estimación del impacto que una amenaza puede ocasionar en el negocio y de la estimación de la probabilidad con la que dicha amenaza puede actuar. El riesgo permite estimar las pérdidas probables que puede experimentar el negocio.

3.4. Propuesta Metodológica

Esta investigación pretende realizar un análisis de riesgos basado en una metodología internacional sobre un proceso cuyo modelo general es un Prestador de Servicios de Valor Añadido (SVA) tipo Sistema de Intermediación Digital (SID), que permita identificar los riesgos claves y comunes, a fin de determinar los controles necesarios y sus prioridades desde la etapa de formación de las SVAs de la Administración Pública.

Se establecen pautas y criterios del Estándar ISO 27005:2008 para elaborar un adecuado análisis de riesgos y también se propone los controles del ISO 27002 e ITIL v3 conforme a los resultados del análisis.

En éste trabajo de Investigación se consideran los principios de seguridad establecidos por MAGERIT, con el fin de lograr un completo entendimiento de los requerimientos de los Activos de los Servicios de Valor Añadido (SVA).

Se explicará de manera detallada en el Capítulo 4.

CAPITULO 4: APLICACIÓN DE LA PROPUESTA METODOLOGICA

Como proceso modelo de evaluación se adoptará un proceso que comprenderá las fases generales que deberán implementarse en los servicios de solicitud de trámite documentario en línea como parte de los SID que se establecerán en la Administración Pública. En el modelo se han considerado las siguientes tres fases:

1˚ fase: Ingreso de Solicitud de Trámite Documentario.

2˚ fase: Firma del Funcionario.

3˚ fase: Verificación del estado del Trámite del solicitante.

A continuación se presenta el mapa del proceso modelo expresado en tres fases:

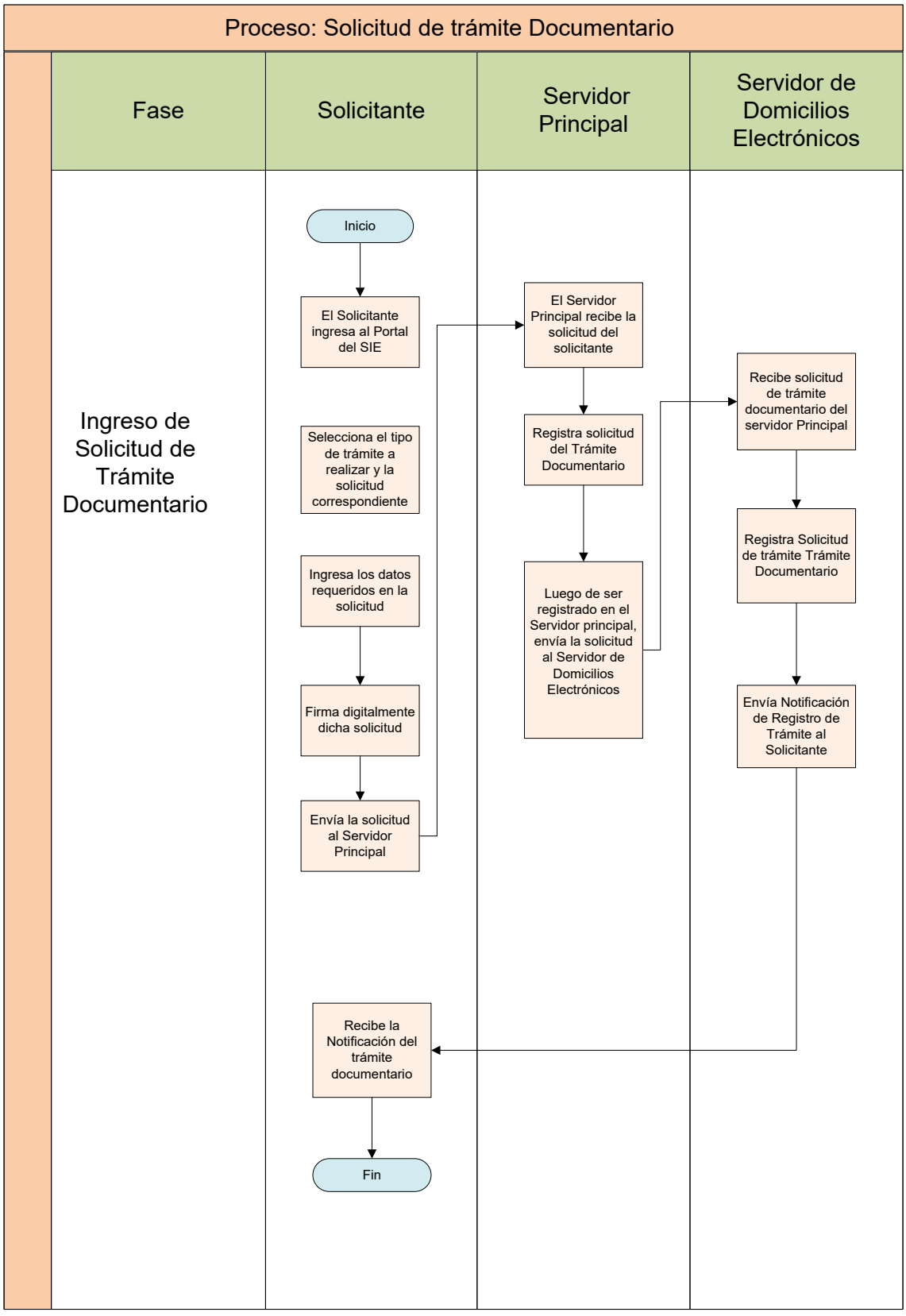


Tabla 4.1.a. Fase 1: Ingreso de Solicitud de Trámite Documentario [Elaboración propia]

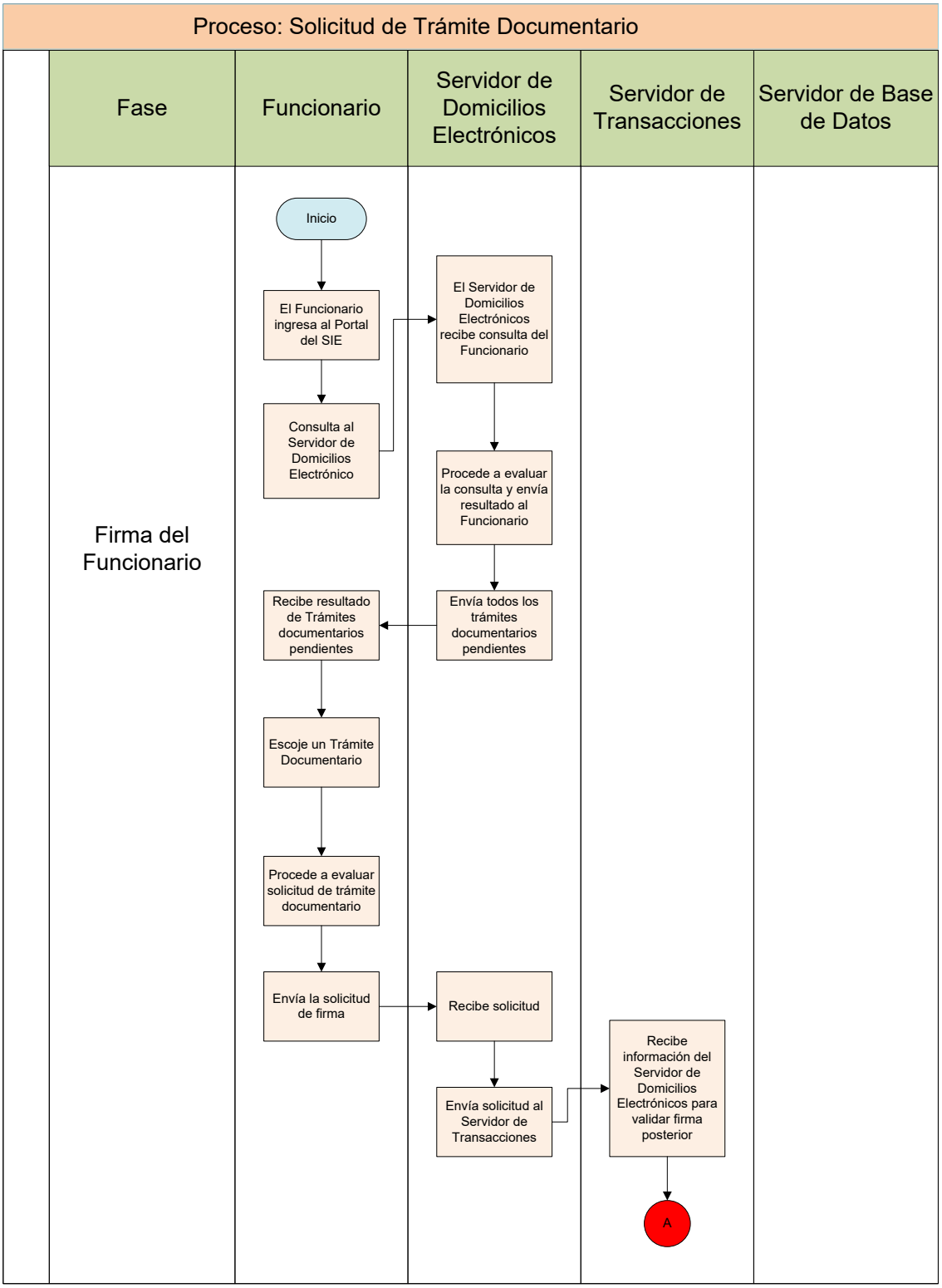


Tabla 4.2.b. Fase 2: Firma del Funcionario [Elaboración propia]

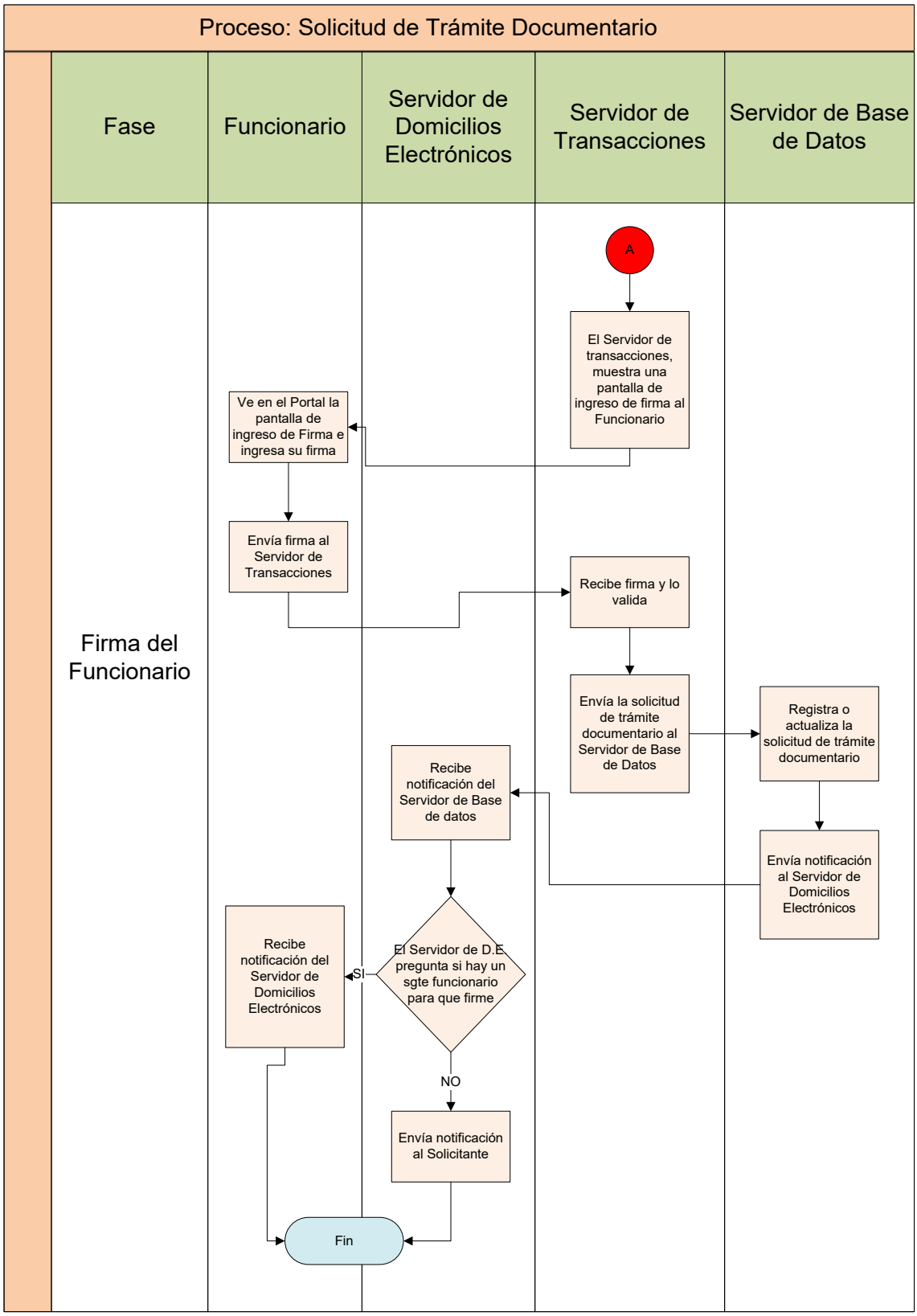


Tabla 4.3.c. Fase 2: Firma del Funcionario [Elaboración propia]

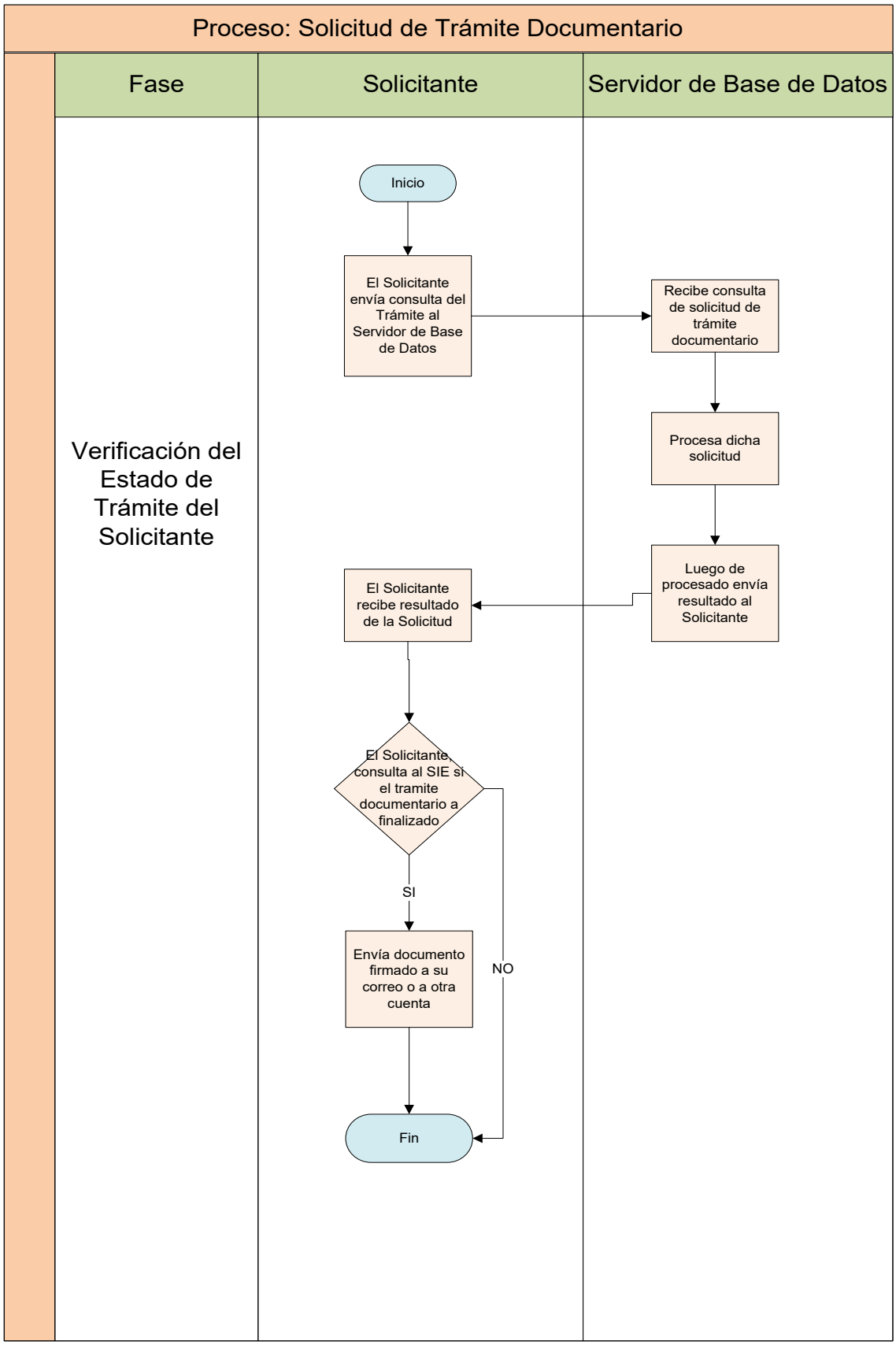


Tabla 4.4.d. Fase 3: Verificación del estado del Trámite del solicitante [Elaboración propia]

4.1. Análisis de Riesgos para los Servicios de Valor Añadido (SVA)

La Gestión del Riesgo es la base para crear un efectivo Sistema de Gestión de la Seguridad de la Información que permita determinar los procesos críticos de un negocio y en particular los activos críticos que deben ser protegidos, contra qué deben ser protegidos y de una manera eficiente y oportuna. La gestión de riesgos implica el análisis del riesgo latente y el tratamiento del riesgo, en un proceso de mejora continua. En este sentido, la presente investigación sigue las pautas y criterios del estándar ISO 27005:2008 para realizar un análisis del riesgo y proponer los controles del ISO 27002 e ITIL v3 conforme a los resultados del análisis.

Para realizar el proceso de análisis de riesgo se ha implementado una herramienta basada en Excel, que permite definir el contexto del negocio estableciendo los criterios de impacto, frecuencia y riesgo aceptable. La herramienta refleja los criterios del estándar ISO 27005:2008, para definir los criterios de impacto, frecuencia y los niveles de riesgo aceptable, e identificar las vulnerabilidades y amenazas. Y puesto los criterios de la gestión de riesgos deben ser alineados a las necesidades de cada organización, la herramienta ha sido ajustada para reflejar las necesidades del proceso modelo de trámite documentario del SID.

Siguiendo el enfoque de procesos del estándar ISO 27001:2005 y el ISO 27005:2008, se siguieron los siguientes pasos:

a. Se establecieron los criterios para valorar los activos en función del impacto que la pérdida de confidencialidad, disponibilidad o integridad puede causar sobre el negocio de la organización:

NIVELES DE IMPACTO QUE EL DAÑO DE UN ACTIVO PUEDE CAUSAR SOBRE LOS SERVICIOS DE VALOR AÑADIDO (SVA)					
Operacional	*Imágen institucional*	*Obligaciones legales o regulatorias*	*Económicas*	*Impacto*	
Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones	Constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros	Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación	Sería de enorme interés para la competencia, de muy elevado valor comercial para terceros, sería causa de muy significativas ganancias o ventajas para individuos u organizaciones. Causa de pérdidas económicas excepcionalmente elevadas	**Alto**	**3**
Probablemente cause una interrupción temporal de las actividades propias de la Organización con cierto impacto en otras organizaciones	Constituye un incumplimiento de las obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros	Probablemente sea causa de incumplimiento de una regulación	Sería de cierto interés para la competencia, de cierto valor comercial para terceros, sería causa ganancias o ventajas moderadas para individuos u organizaciones. Causa de pérdidas económicas moderadas	**Medio**	**2**
No podría causar la interrupción de actividades propias de la Organización	Sería causa de inconveniencias mínimas a las partes afectadas	No sería causa de incumplimiento de ninguna regulación	Supondría pérdidas económicas insignificantes	**Bajo**	**1**

Tabla 4.1.1. Niveles de Impacto que el Daño de un Activo puede causar sobre los Servicios de Valor Añadido (SVA)

b. Se establecieron los criterios para determinar la frecuencia o probabilidad con la que una amenaza deliberada o accidental puede materializarse:

CRITERIOS PARA DETERMINAR LA FRECUENCIA DE UNA AMENAZA SOBRE LOS ACTIVOS DE LOS SERVICIOS DE VALOR AÑADIDO (SVA)						
FRECUENCIA		**CRITERIOS**				
¿Cada cuánto se puede materializar una amenaza?		**¿El activo es atractivo para atacantes internos o externos?**		**¿Es difícil materializar la amenaza?**		**¿Existen controles eficaces?**
Muy frecuente	Puede ocurrir a diario	Si	**Y**	Muy Fácil	**Y**	No
Frecuente	Puede ocurrir mensualmente	Si	**Y**	Fácil	**Y**	No
Normal	Puede ocurrir una vez al año	Si	**Y**	Difícil	**Y**	No
Poco frecuente	Puede ocurrir cada varios años	No	**O**	Muy difícil	**O**	Si

Tabla 4.1.2. Criterios para determinar la Frecuencia o Probabilidad con la que una Amenaza deliberada o accidental puede materializarse

c. Se establecieron los criterios de riesgo aceptable en función de garantizar un nivel apropiado de calidad en los servicios brindados por la SVA a los ciudadanos, asegurando la continuidad, integridad y autenticidad de sus operaciones, se establecieron los siguientes criterios que permitirán definir los niveles aceptables de riesgo.

El riesgo es aceptable cuando:

- Siendo el activo valioso para garantizar la continuidad, integridad, autenticidad y buen rendimiento del negocio (Impacto *Alto*), la frecuencia o probabilidad de que la amenaza en cuestión se materialice no es poco frecuente.

- Siendo el activo valioso moderadamente para garantizar la continuidad, integridad, autenticidad y buen rendimiento del negocio (Impacto *Medio*), la pérdida acumulada debido a la frecuencia con la que la amenaza en cuestión puede materializarse es normal de

modo que puede ser asumida por la organización sin causar pérdidas significativas

- Siendo el activo poco valioso para garantizar la continuidad, integridad, autenticidad y buen rendimiento del negocio (Impacto *Bajo*), la pérdida acumulada debido a la frecuencia con la que la amenaza en cuestión puede materializarse puede ser afrontada por la organización sin causar perjuicio en la continuidad de las operaciones ni en el nivel de rendimiento esperado.

A fin de priorizar la utilización de los esfuerzos económicos, de personal y tiempo para resolver los incidentes de seguridad en las SVA, según los criterios expuestos en los párrafos anteriores se consideran como aceptables de riesgo los niveles medio, bajo y muy bajo. Por lo que no se propondrán controles.

RIESGO		***FRECUENCIA***			
		Poca frecuencia	**Frecuencia Normal**	**Frecuente**	**Muy Frecuente**
IMPACTO	**Alto**	Muy bajo	**Alto**	**Muy alto**	**Muy alto**
	Medio	Muy bajo	**Medio**	**Alto**	**Muy alto**
	Bajo	Muy bajo	Bajo	**Medio**	**Alto**
	Muy Bajo	Muy bajo	Muy bajo	Bajo	**Medio**

Tabla 4.1.3. Niveles de Riesgos según la Frecuencia

d. Identificación de los activos de mayor importancia que sostienen el proceso modelo de trámite documentario. A continuación se muestra una imagen de la herramienta desarrollada

SELECCIÓN DE ACTIVOS IMPORTANTES DE LOS SERVICIOS DE VALOR AÑADIDO (SVA)		
MISIÓN: La SVA, en particular el SID tiene como misión brindar servicios de trámite documentario con los ciudadanos peruanos garantizando el no repudio de las transacciones. Para eso utiliza herramientas de software de firma y autenticación digital ,mediante los cuales los ciudadanos pueden utilizar sus certficados digitales para realizar transacciones en línea no repudiables. La SVA debe garantizar la autenticidad, integridad, confiabilidad y disponibilidad de sus activos a fin de brindar un nivel óptimo de calidad a sus clientes.		
SERVICIOS IMPORTANTES: Brindar servicio de trámite documentario en línea a los ciudadanos peruanos en todo el país, garantizando el no repudio de las transacciones documentarias.		
N°	**¿Cualés son los activos más importantes que sostienen el negocio de la SVA?**	**¿Por qué es importante?**
1	Solicitud firmada digitalmente del trámite documentario	Sirve de evidencia ante un proceso judicial, de que el servicio es auténtico y por lo tanto no repudiable
3	Acceso a Internet del Sistema	Permite publicar el Sistema web
4	Acceso a Internet del Funcionario	Permite las comunicaciones vía Web con el Solicitante, tambien permite conocer al Funcionario el estado de la solicitud del trámite documentario
5	Suministro de energía eléctrica (Funcionario)	Permite al Funcionario recibir la solicitud y realizar las autorizaciones correspondientes
	Suministro de energía eléctrica (Centro de datos)	Sostiene todas las operaciones del SIE, en particular los servicos de solicitud de trámite documentario.
6	Computadores del Funcionario	Permite realizar las actividades de los servicios brindados por el SIE
7	Funcionario	Realiza las operaciones de consulta, elección de trámite, envío de notificación y envío de solicitud firmada al solicitante
8	Direccción de correo electrónico del Solicitante	Permite la recepción de la notificación enviada por el Funcionario
9	Correo Electrónico del Funcionario	Permite la comunicación con el Solicitante
10	Documentos de gestión en formato electrónico	Permiten al ciudadano recibir documentos de la administración pública en formato electrónico con la misma validez que los documentos de papel
11	Administrador de la red y encargado de soporte	Controla las configuraciones necesarias en los sistemas informáticos
12	Acceso al Servidor Principal	Permite el registro de los trámites documentarios así como tambien la interacción con el Servidor de Domicilios Electrónicos
13	Acceso al Servidor de Domicilios Electrónicos	Permite la interacción con el Servidor Principal y con el Servidor de transacciones. Recibe las consultas del funcionario, envía notificación de registro de trámite así como tambien verifica si hay un siguiente funcionario para firmar digitalmente
14	Acceso al Servidor de Transacciones	Recibe información del servidor de Domicilios Electrónicos para validar la firma posterior
15	Acceso al servidor de Base de Datos	Registra y Actualiza los trámites documentarios enviados del Servidor de Transacciones
16	Interconexión de Servidores	Permite la comunicación con el Funcionario dependiendo del tipo de Servidor
17	Infraestructura física	Permite proteger los activos de información contra vandalismo y robo
18	Sistema web para las solicitudes de la administración pública	Permite el registro y autorización para los trámites documentarios
19	Software de firma digital del funcionario	Permite validar la firma del Funcionario

Tabla 4.1.4. Identificación de Activos

e. Se identificó la importancia de cada activo respecto del negocio de la organización, en caso de pérdida de confidencialidad, disponibilidad, integridad, autenticidad del servicio y no repudio. En este caso se consideraron los principios de seguridad establecidos por MAGERIT a fin de lograr un mayor entendimiento de los requerimientos de seguridad de los activos de la SVA.

Tabla 4.1.5. Evaluación de los Requerimientos de seguridad de los SVA

f. Se identificaron las amenazas, vulnerabilidades y controles existentes en los procedimientos de la SVA

g. En función del valor que el activo pueda tener para un posible atacante, la facilidad del ataque y la efectividad de los controles existentes se determinó la frecuencia.

h. En función de la importancia del activo y de la frecuencia, mediante la herramienta, se calculó el riesgo. Identificando los niveles de riesgo aceptables.

i. Tomando como referencia los controles propuestos en el estándar ISO 27002 se han recomendado objetivos de control y controles para los niveles de riesgo alto y muy alto.

Tabla 4.1.6. Caracterización de Amenazas de los Activos importante de los Servicios de Valor Añadido (SVA)

4.2. Controles basados en la fase de Operación del Servicio según ITIL v3

A fin de complementar controles respecto de la gestión de incidencias y mantenimiento del SGSI según el estándar ISO 27001:2005 se propone la implementación de los procesos de control de la fase de Operación del Servicio según ITIL v3. Los siguientes son algunos ejemplos de Servicios de Valor Añadido (SVA) para el negocio de la Organización al implementar un sistema de gestión de eventos e incidentes:

La gestión de eventos proporciona mecanismos para la rápida detección de incidencias.

La gestión de eventos permite la monitorización por excepción de ciertos tipos de actividades automatizadas

Detectar excepciones o cambios de estado.

Ofrece una base para operaciones automatizadas, lo que aumenta la eficacia y libera costosos recursos humanos pata dedicarlos a trabajos más innovadores.

4.2.1. Gestión de Eventos en los Servicios de Valor Añadido (SVA)

Un evento es un suceso detectable que tiene importancia para la gestión de la infraestructura TI, entrega y evaluación del impacto de una posible desviación en los Servicios de Valor Añadido (SVA).

El proceso de Gestión de Eventos en las SVA es responsable de la gestión de eventos a lo largo de su ciclo de vida, siendo una de las principales actividades de las operaciones TI. Para garantizar la eficacia de la Operación del Servicio, toda entidad pública debe ser consciente del estado de su infraestructura y poder así detectar desviaciones respecto a la operación normal prevista.

Las actividades del proceso de Gestión de Eventos son:

1. Aparición de eventos
2. Informes de eventos
3. Detección de eventos
4. Filtrado de eventos
5. Clasificación de eventos
6. Correlación de eventos
7. Disparador
8. Opciones de respuesta
9. Revirones de acciones
10. Cierre del evento

El factor crítico de éxito más relevante en las SVAs, para la Gestión de Eventos es no poder conseguir los fondos suficientes.

A continuación se presenta una propuesta para la implementación de un sistema de gestión de eventos para los sistemas de la SVA como complemento a los controles del ISO 27001:2005 propuestos en las secciones anteriores.

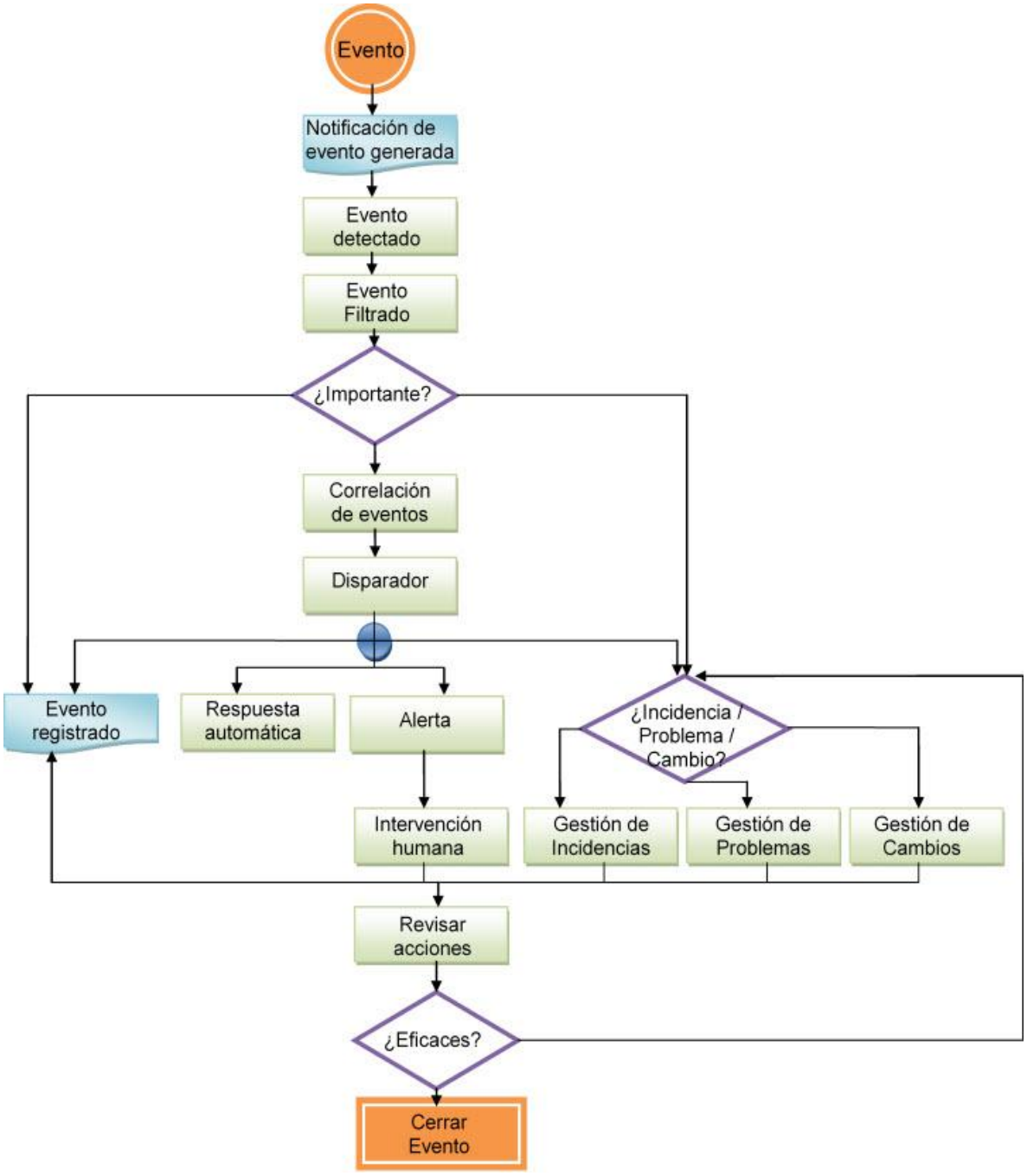


Tabla.4.2. Propuesta para la implementación de un sistema de gestión de eventos para los sistemas de la SVA

4.2.2. Gestión de Incidencias en los Servicios de Valor Añadido (SVA)

Una incidencia en los Servicios de Valor Añadido (SVA), es una interrupción no planificada o una reducción de la calidad de un servicio de TI.

El proceso de Gestión de Incidencias en las SVAs cubre todo tipo de incidencias, ya sean fallos, consultadas planteadas por usuarios o por el propio personal técnico, incluso aquéllas detectadas de forma automática por herramientas de monitorización de eventos.

Actividades de Gestión de Incidencias en los Servicios de Valor Añadido (SVA):

1. Identificación
2. Registro
3. Clasificación
4. Priorización
5. Diagnóstico (inicial)
6. Escalado
7. Investigación y diagnóstico
8. Resolución y recuperación
9. Cierre

El factor crítico de éxito más relevante en las SVAs, para la Gestión de Incidencias es tener los objetivos claramente definidos.

A continuación se presenta una propuesta para la implementación de un sistema de gestión de incidencias para los sistemas de la SVA como complemento a los controles del ISO 27001:2005 propuestos en las secciones anteriores.

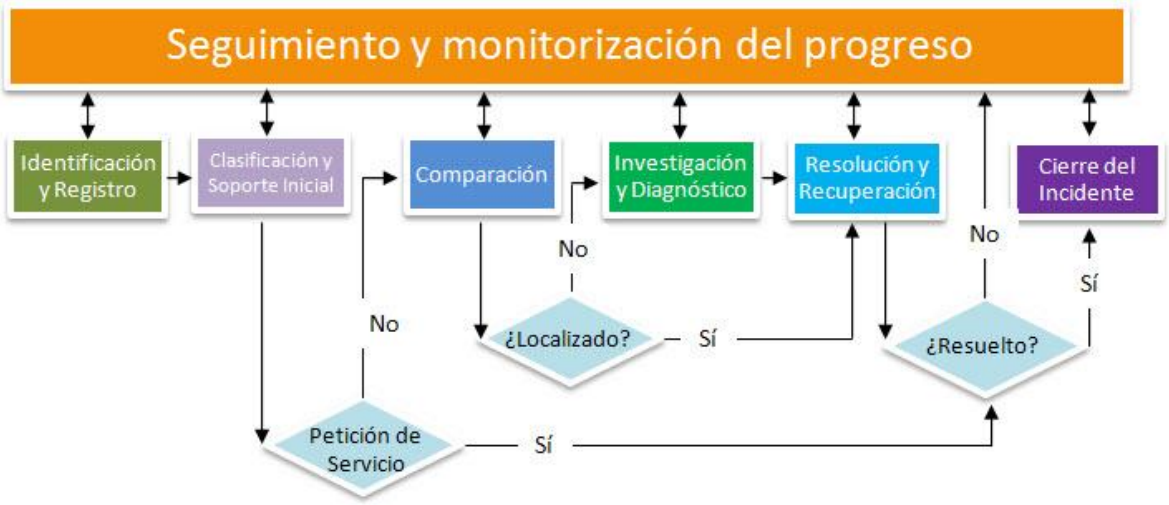


Tabla.4.3. Propuesta para la implementación de un sistema de gestión de incidencias para los sistemas de la SVA

ESPECIFICACIÓN DIFERENCIAL UTILIZADA EN EL PRESENTE TRABAJO DE INVESTIGACIÓN

(Detalle diferencial de las normas: ISO 27001, ISO 27002 e ISO 27005)

ESPECIFICACIÓN DIFERENCIAL UTILIZADAS EN EL PRESENTE TRABAJO DE INVESTIGACIÓN		
ISO 27001	**ISO 27002**	**ISO 27005**
Es certificable	No es certificable	No es certificable
Es una especificación	Código de Buenas Prácticas	Diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos en los Servicios de Valor Añadido (SVA)	Guía para, en distintos ámbitos, conocer qué se puede hacer para mejorar la seguridad de la información en los Servicios de Valor Añadido (SVA).	Proporciona directrices para la gestión de riesgos en la seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información en los Servicios de Valor Añadido (SVA), en soporte del proceso de gestión de riesgos de la norma ISO 27001
Enumera los objetivos de control y controles que desarrolla la ISO 27002, como se muestra en la Tabla Caracterización de Amenazas de los Activos importante de los Servicios de Valor Añadido (SVA)	Describe los objetivos de control y controles recomendables, detallados en la Tabla Caracterización de Amenazas de los Activos importante de los Servicios de Valor Añadido (SVA)	Apoya los conceptos generales especificados en la ISO 27001
Lo que importa en la ISO 27001 es que los riesgos se analicen y se gestionen, que la seguridad se planifique, se implemente y, sobre todo, se revise y se corrija y mejore. Siendo éste el objetivo primordial para los Servicios de Valor Añadido (SVA) en las entidades públicas	Es una guía para conocer qué se puede hacer para mejorar la seguridad de la información. Expone, en distintos campos, una serie de apartados a tratar en relación a la seguridad, Los objetivos de seguridad a perseguir, una serie de consideraciones (controles) a tener en cuenta para cada objetivo y un conjunto de “sugerencias”	El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO 27001 e ISO 27002 es importante para un completo entendimiento de la norma ISO 27005, que es aplicable a todo tipo de organizaciones (por ejemplo: entidades públicas, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar

	para cada uno de esos controles. Detallados en la Tabla Caracterización de Amenazas de los Activos importante de los Servicios de Valor Añadido (SVA)	los riesgos que puedan comprometer la organización de la seguridad de la información, en particular las entidades públicas
En el Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002, para que sean seleccionados por las organizaciones (entidades públicas) en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.	Es la única norma que no sólo cubre la problemática de la seguridad TI, sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de una organización en cuanto a la seguridad de la información que maneja. Este concepto marca la diferencia con el de seguridad informática que, en la práctica, se vino convirtiendo en equivalente de seguridad de sistemas TI, mientras que la norma considera también los riesgos organizacionales, operacionales y físicos de una empresa u entidad pública, con todo lo que esto implica.	Este estándar define la Gestión de Riesgos de la Seguridad de la Información como un enfoque sistemático necesario para identificar las necesidades organizacionales respecto de los requerimientos de seguridad de la información y crear un efectivo Sistema de Gestión de la Seguridad de la Información (SGSI)

Tabla. Especificación diferencial utilizada en el presente trabajo de investigación

CAPITIULO 5: CONCLUSIONES

Como resultado de la presente investigación, se concluye lo siguiente:

1. Los sistemas SVA del tipo SID pueden ser expresados siguiendo los criterios de las metodologías de gestión por procesos permitiendo identificar fácilmente las etapas críticas y los activos más relevantes de dichos procesos.

2. Los SVA del tipo SID pese a contar con tecnologías que garantizan el no repudio requieren ser complementados con un sistema de gestión de la seguridad de la información que permita identificar de manera eficiente y oportuna las vulnerabilidades de cada SVA.

3. El proceso de análisis y evaluación de riesgo es la base fundamental para establecer un Sistema de Gestión de la Seguridad de la Información, permitiendo priorizar los esfuerzos económicos, personal y tiempo para cubrir los requerimientos de seguridad de la información.

4. Los procesos y funciones de ITIL v3 se complementan con los controles del ISO 27001:2005 para lograr una mejor gestión de la seguridad de la información.

ANEXO A

OBJETIVOS DE CONTROL Y CONTROLES DEL ESTÁNDAR ISO 27001:2005

	OBJETIVOS DE CONTROL		CONTROLES		
A.5	Política de seguridad				
A.5.1	Política de seguridad de la información	Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes			
			A.5.1.1	Documentar la política de seguridad de la información	La gerencia debe aprobar un documento de política, publicarlo y comunicarlo a todos los empleados y partes externas relevantes
			A.5.1.2	Revisión de la política de seguridad de la información	La política de seguridad de la información debe ser revisada a intervalos planificados o cuando ocurren cambios significativos a fin de garantizar su idoneidad, adecuación y efectividad
A.6	Organización de la seguridad de la información				
A.6.1	Organización interna	Manejar la seguridad de la información dentro de la organización			
			A.6.1.1	Compromiso de la gerencia con la seguridad de la información	La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita, y reconocimiento de las responsabilidades de la seguridad de la información
			A.6.1.2	Coordinación de la seguridad de la información	Las actividades de la seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con funciones y roles relevantes

		A.6.1.3	Asignación de responsabilidades de la seguridad de la información	Todas las responsabilidades de la seguridad de la información deben ser claramente definidas
		A.6.1.4	Proceso de autorización para los medios de procesamiento de la información	Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
		A.6.1.5	Acuerdos de confidencialidad	Se deben identificar y revisar con regularidad los requerimientos de confidencialidad o los acuerdos de no divulgación que reflejen las necesidades de la organización para la protección de información
		A.6.1.6	Contacto con autoridades	Se deben mantener apropiados contactos con las autoridades relevantes
		A.6.1.7	Contacto con grupos de interés especial	Se deben mantener apropiados contactos con grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales
		A.6.1.8	Revisión independiente de la seguridad de la información	Se debe revisar de manera independiente en intervalos planificados o cuando ocurran cambios significativos en la implementación de la seguridad, el enfoque de la organización para gestionar la seguridad de la información y su implementación (P. Ej. objetivos de control, controles, políticas, procesos, y procedimientos para la seguridad de la información)
A.6.2	Partes externas	Mantener la seguridad de la información de la organización y los medios de procesamiento de la información que son procesados,		

		accesados, comunicados a, o gestionados por partes externas			
			A.6.2.1	Identificación de riesgos relacionados con terceras partes	Los riesgos de la seguridad de la información de la organización y sus medios de procesamiento, que forman parte de los procesos del negocio en los cuales participan terceras partes deben ser identificados y se deben identificar controles apropiados antes de otorgar el acceso
			A.6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes	Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o a activos de la organización
			A.6.2.3	Tratamiento de la seguridad en contratos con terceras partes	Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras partes a la información o los medios de procesamiento de la información de la organización, agregación de productos o servicios a los medios de procesamiento de la información deben abarcar requerimientos de seguridad relevantes
A.7	Gestión de activos				
A.7.1	Responsabilidad por los activos	Lograr y mantener la protección apropiada de los activos organizacionales			
			A.7.1.1	Inventarios de activos	Todos los deben ser claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes
			A.7.1.2	Propiedad de los activos	Toda la información y los activos asociados con los medios de procesamiento de información deben ser propiedad de una parte asignada de la organización

			A.7.1.3	Uso aceptable de activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos asociados con los medios de procesamiento de la información
A.7.2	Clasificación de información	Asegurar que la información recibe un apropiado nivel de protección			
			A.7.2.1	Lineamientos de clasificación	La información debe ser clasificada en términos de su valor, requerimientos legales, sensibilidad y criticidad para la organización
			A.7.2.2	Etiquetado y manejo de la información	Se debe desarrollar e implementar un apropiado conjuntos de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización
A.8	Seguridad de los recursos humanos				
A.8.1	Antes del empleo	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y sean adecuados para los roles para los cuales se les considera y reducir el riesgo de robo, fraude o mal uso de los medios			
			A.8.1.1	Roles y responsabilidades	Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización
			A.8.1.2	Selección	Se deben llevar a cabo revisiones de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros usuarios en concordancia con las leyes, regulaciones y ética relevantes, y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a ser accesada, y los riesgos percibidos

			A.8.1.3	Términos y condiciones de empleo	Como parte de la obligación contractual, los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización respecto de la seguridad de la información
A.8.2	Durante el empleo	Asegurar que todos los empleados, contratistas y terceras partes sean concientizados acerca de las amenazas e inquietudes sobre la seguridad de la información, sus responsabilidades y obligaciones, y sean equipados para soportar la política de seguridad de la organización en el curso de su trabajo normal, y reducir los riesgos de error humano			
			A.8.2.1	Gestión de responsabilidades	La gerencia debe requerir a los empleados, contratistas y terceros aplicar la seguridad en concordancia con las políticas y procedimientos establecidos de la organización
			A.8.2.2	Concientización, educación y entrenamiento de seguridad de la información	Todos los empleados de la organización y, si fuera relevante, contratistas y terceros deben recibir entrenamiento apropiado y actualizaciones regulares sobre las políticas y procedimientos organizacionales, como sea relevante para cumplir su función
			A.8.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad
A.8.3	Terminación o cambio de empleo	Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada			
			A.8.3.1	Responsabilidades de terminación	Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambo de empleo
			A.8.3.2	Retorno de activos	Todos los empleados, contratistas y terceros deben retornar todos los activos de la organización que se encuentran en su posesión al terminar su empleo, contrato o acuerdo

			A.8.3.3	Remoción de derechos de acceso	Todos los derechos de acceso de los empleados contratistas y terceros, a la información y a los medios de procesamiento de la información deben ser removidos al terminar su empleo, contrato o acuerdo, o ser ajustados al cambio
A.9	Seguridad física y ambiental				
A.9.1	Áreas seguras	Prevenir accesos físicos no autorizados, daños e interferencia al local y a la información de la organización			
			A.9.1.1	Perímetro de seguridad física	Se deben usar perímetros de seguridad (barreras como paredes, puertas controladas por tarjetas o módulos de recepción) para proteger las áreas que contienen información y los medios de información
			A.9.1.2	Controles de entrada físicos	Las áreas seguras deben ser protegidas por controles de entrada apropiados para asegurar que solo el personal autorizado tiene autorizado el acceso
			A.9.1.3	Seguridad de oficinas, habitaciones y medios	Se debe diseñar y aplicar seguridad física para oficinas, habitaciones y medios
			A.9.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra daños causados por fuego, inundaciones, terremoto, explosión, disturbios civiles y otras formas de desastres naturales o causados por el hombre
			A.9.1.5	Trabajo en zonas seguras	Se debe diseñar y aplicar protección y lineamientos para el trabajo en zonas seguras

			A.9.1.6	Áreas de acceso público, entrega y carga	Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado
A.9.2	Seguridad del equipo	Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización			
			A.9.2.1	Ubicación y protección del equipo	El equipo debe estar ubicado o protegido para reducir el riesgo de amenazas y peligros ambientales, y oportunidades de acceso no autorizado
			A.9.2.2	Servicios públicos	El equipo debe ser protegido de fallas en la alimentación energética, y otras interrupciones causadas por fallas en los servicios públicos
			A.9.2.3	Seguridad en el cableado	El cableado de la energía y las telecomunicaciones que llevan datos o sostienen los servicios de información deben ser protegidos de la intercepción o daño
			A.9.2.4	Mantenimiento del equipo	El equipo debe ser correctamente mantenido para asegurar su continua disponibilidad e integridad
			A.9.2.5	Seguridad del equipo fuera del local	Se debe aplicar seguridad al equipo que se encuentra fuera del local tomando en cuenta los diferentes riesgos de de trabajar fuera del local de la organización

			A.9.2.6	Eliminación o reúso seguro del equipo	Todos los artículos del equipo que contienen medios de almacenamiento deben ser revisados para asegurar que cualquier dato sensible y software licenciado ha sido removido o sobre-escrito de forma segura antes de su eliminación
			A.9.2.7	Traslado de propiedad	Los equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización
A.10	Gestión de las comunicaciones y operaciones				
A.10.1	Procedimientos y responsabilidades operacionales	Asegurar la operación correcta y segura de los medios de procesamiento de la información			
			A.10.1.1	Documentación de los procedimientos de operación	Los procedimientos operacionales deben ser documentados, mantenidos y puestos a disposición de todos los usuarios que los necesiten
			A.10.1.2	Gestión de cambios	Se deben controlar los cambios realizados a los medios de información
			A.10.1.3	Segregación de deberes	Los deberes y áreas de seguridad deben ser segregadas para reducir las oportunidades de modificación no autorizada o no intencionales o mal uso de los activos de la organización
			A.10.1.4	Separación de los medios de desarrollo y operacionales	Los medios de desarrollo, prueba y de operación deberán ser separados para reducir los riesgos de accesos o cambios no autorizados al sistema operacional
A.10.2	Gestión de la entrega del servicio de terceros	Implementar y mantener el nivel apropiado de seguridad de la información y entrega de servicio conforme a los acuerdos de entregas de servicios de terceros			

			A.10.2.1		Se debe asegurar que los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega del servicio son implementados, operados y mantenidos por la tercera parte
			A.10.2.2	Monitoreo y revisión de los servicios de terceros	Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados, y deben realizarse auditorías con regularidad
			A.10.2.3	Manejar los cambios en los servicios de terceros	Se deben gestionar los cambios en la provisión de servicios, incluyendo mantenimiento y mejora de las políticas, procedimientos y controles existentes, tomando en cuenta la criticidad de los sistemas y procesos del negocio involucrados y la re-evaluación de riesgos
A.10.3	Planificación y aceptación del sistema	Minimizar el riesgo de fallas en los sistemas			
			A.10.3.1	Gestión de capacidad	El uso de los recursos debe ser monitoreado, sincronizado, y se deben realizar proyecciones de los futuros requerimientos de capacidad para asegurar el desempeño requerido del sistema
			A.10.3.2	Aceptación del sistema	Se deben establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones y deben realizarse pruebas de idoneidad de los sistemas durante su desarrollo y antes de ser aceptados
A.10.4	Protección contra software malicioso y código móvil	Proteger la integridad del software y de la información			

			A.10.4.1	Controles contra software malicioso	Se deben implementar controles de protección para la detección, prevención y recuperación contra software malicioso y se deben implementar procedimientos apropiados de concientización
			A.10.4.2	Controles contra código móvil	Si fuere autorizado el uso de código móvil, la configuración debe asegurar que el código móvil autorizado opera conforme a una política de seguridad claramente definida y debe prevenirse la ejecución de código móvil no autorizado
A.10.5	Respaldo	Mantener la integridad y disponibilidad de la información y de los medios de procesamiento de la información			
			A.10.5.1	Información de respaldo	Se deben tomar copias de respaldo de la información y software y deben ser probadas regularmente conforme a la política de respaldo
A.10.6	Gestión de la seguridad de redes	Asegurar la protección de la información en redes y la protección de la infraestructura de soporte			
			A.10.6.1	Controles de red	Las redes deben ser adecuadamente gestionadas y controladas, para ser protegidas contra amenazas y mantener la seguridad de los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito
			A.10.6.2	Seguridad de los servicios de red	Características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de redes deben ser identificados e incluidos en los acuerdos de servicios de cualquier red, tanto si los servicios fueran provistos dentro o fuera de la organización
A.10.7	Gestión de medios	Prevenir la publicación, modificación, remoción o destrucción no autorizada de activos, y la interrupción de las actividades del negocio			

			A.10.7.1	Gestión de medios removibles	Deben existir procedimientos establecidos para la gestión de medios removibles
			A.10.7.2	Eliminación de medios	Los medios deben ser eliminados utilizando procedimientos formales y de manera segura cuando ya no se les requiere
			A.10.7.3	Procedimientos de manejo de información	Procedimientos para el manejo y almacenamiento de la información deben ser establecidos para proteger esta información de publicación no autorizada o mal uso
			A.10.7.4	Seguridad de la documentación del sistema	La documentación del sistema debe ser protegida contra acceso no autorizado
A.10.8	Intercambio de información	Mantener la seguridad de la información y software intercambiado dentro de una organización y con alguna parte tercera			
			A.10.8.1	Políticas y procedimientos para el intercambio de información	Se deben establecer políticas, procedimientos y controles formales para el intercambio de información por medio del uso de todos los tipos de medios de comunicación
			A.10.8.2	Acuerdos de intercambio	Acuerdos deben ser establecidos para el intercambio de información y software entre la organización y terceros
			A.10.8.3	Medios físico en tránsito	Los medios que contienen información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante su transporte fuera de las fronteras físicas de la organización
			A.10.8.4	Mensajes electrónicos	La información envuelta en mensa en los mensajes electrónicos debe ser protegida apropiadamente

			A.10.8.5	Sistemas de información comercial	Políticas y procedimientos deben ser desarrollados e implementados para proteger la información asociada con la interconexión de los sistemas de información comercial
A.10.9	Servicios de comercio electrónico	Asegurar los servicios de comercio electrónico y su uso seguro			
			A.10.9.1	Comercio electrónico	Se debe proteger la información involucrada en el comercio electrónico que se transmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada
			A.10.9.2	Transacciones en línea	La información envuelta en transacciones en línea debe ser protegida para prevenir la transmisión incompleta, error de encaminamiento, alteración no autorizada del mensaje, publicación no autorizada, duplicación o repetición no autorizada del mensaje
			A.10.9.3	Información disponible públicamente	La integridad de la información que se encuentra públicamente disponible debe ser protegida contra modificaciones no autorizadas
A.10.10	Monitoreo	Detectar actividades no autorizadas de procesamiento de información			
			A.10.10.1	Registro de auditoría	Registros de auditoría de las actividades de los usuarios, excepciones y eventos de seguridad de la información deben ser producidos y guardados por un periodos acordado para asistir en futuras investigaciones y monitoreo de control de acceso

			A.10.10.2	Uso del sistema de monitoreo	Procedimientos para monitorear el uso de los medios de información debe ser establecida y los resultados de las actividades de monitoreo deben ser revisadas con regularidad
			A.10.10.3	Protección de la información del registro	Los medios de registro y la información de registro debe ser protegida contra manipulación y acceso no autorizado
			A.10.10.4	Registros del administrador y del operador	Las actividades del administrador y del operador del sistemas deben ser registrados
			A.10.10.5	Registro de fallas	Las fallas deben ser registradas, analizadas y deben tomarse apropiadas acciones
			A.10.10.6	Sincronización de relojes	Los relojes de todos los sistemas relevantes de procesamiento de información deben dentro de la organización o en el dominio de seguridad deben ser sincronizados con una fuente de tiempo exacta acordada
A.11	Control de acceso				
A.11.1	Requerimientos del negocio para el control de acceso	Controlar el acceso a la información			
			A.11.1	Política de control de acceso	Se debe establecer y documentar una política de control de acceso y debe ser revisada en base a los requerimientos comerciales y de seguridad sobre el acceso
A.11.2	Gestión de acceso del usuario	Asegurar el acceso de usuarios autorizados y prevenir los accesos no autorizados a los sistemas			
			A.11.2.1	Registro de usuario	Debe existir un procedimiento formal establecido para el registro y des-registro de usuarios para otorgar y revocar el acceso para todos los sistemas y servicios de información

			A.11.2.2	Gestión de privilegios	Se debe restringir y controlar la asignación y usos de privilegios
			A.11.2.3	Gestión de contraseñas de usuario	La asignación de contraseñas debe ser controlada a través de un proceso formal de gestión
			A.11.2.4	Revisión de los derechos de acceso	La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal
A.11.3	Responsabilidades del usuario	Prevenir el acceso de usuarios no autorizados y el compromiso o robo de la información y los medios de procesamiento de la información			
			A.11.3.1	Uso de contraseñas	Los usuarios deben ser requeridos a seguir buenas prácticas en la selección y uso de contraseñas
			A.11.3.2	Equipo de usuario desatendido	Los usuarios se deben asegurar que los equipos desatendidos tengan la apropiada protección
			A.11.3.3	Política de pantalla y escritorio limpios	Una política de escritorio limpio para documentos y medios de almacenamiento removibles y una política de pantalla limpia para los medios de procesamiento de la información deben ser adoptadas
A.11.4	Control de acceso a redes	Prevenir el acceso no autorizado a los servicios en red			
			A.11.4.1	Política sobre el uso de servicios de red	Los usuarios deben ser sólo provistos del acceso a los servicios a los que han sido específicamente autorizados para usar
			A.11.4.2	Autenticación de usuarios para conexiones externas	Métodos de autenticación apropiados deben ser usados para controlar el acceso por usuarios remotos
			A.11.4.3	Identificación del equipo en red	Identificación automática de equipos debe ser considerada como un medio para autenticar las conexiones desde ubicaciones

					y equipos específicos
			A.11.4.4	Protección del puerto de diagnóstico y configuración remotos	Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración
			A.11.4.5	Segregación en redes	Los grupos de servicios de información, usuarios, y sistemas de información deberán ser segregados en redes
			A.11.4.6	Control de conexión de redes	Para redes compartidas, especialmente aquellas que se extienden a través de los límites de la organización, la capacidad de usuarios para conectarse a la red debe ser restringida, en concordancia con la política de control de acceso y los requerimientos de las aplicaciones comerciales
			A.11.4.7	Control de enrutamiento en redes	Controles de enrutamiento en redes deben ser implementados en redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales
A.11.5	Control de acceso al sistema de operación	Prevenir el acceso no autorizado al sistema de operación			
			A.11.5.1	Procedimientos de registro seguro	Se debe controlar el acceso a los servicios operativos mediante un procedimiento de registro seguro
			A.11.5.2	Identificación y autenticación del usuario	Todos los usuarios deben tener un único identificador (ID de usuario) para uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario

			A.11.5.3	Sistema de gestión de claves	Los sistemas para la gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las claves
			A.11.5.4	Uso de utilidades del sistema	EL uso de programas utilitarios que pueden ser capaces de sobre-escribir en el sistema y en las aplicaciones de control deben ser restringidas y estrictamente controladas
			A.11.5.5	Sesión inactiva	Las sesiones inactivas deben cerrarse después de un periodo definido de inactividad
			A.11.5.6	Limitación del tiempo de conexión	Restricciones en los tiempos de conexión deben ser usados para proveer seguridad adicional para aplicaciones de alto riesgo
A.11.6	Control de acceso a las aplicaciones y a la información	Prevenir el acceso no autorizado a la información manejada por los sistemas de aplicación			
			A.11.6.1	Restricciones de acceso a la información	Se debe restringir el acceso de los usuarios y a la información y al sistema de aplicación en concordancia con la política de control de acceso
			A.11.6.2	Aislamiento del sistema sensible	Los sistemas sensibles deben tener un sistema de cómputo dedicado (aislado)
A.11.7	Computación móvil y tele-trabajo	Asegurar la seguridad de la información cuando se utilizan sistemas de computación móviles y medios de tele-trabajo			
			A.11.7.1	Computación y comunicaciones móviles	Se debe establecer una política formal y apropiadas medidas deben ser adoptadas para proteger contra riesgos contra computación y comunicaciones móviles
			A.11.7.2	Tele-trabajo	Una política, planes y procedimientos operacionales deben ser desarrollados e implementados para las actividades de tele-trabajo
A.12	Adquisición, desarrollo y mantenimiento de los sistemas de información				

A.12.1	Requerimientos de seguridad de seguridad de la información	Asegurar que la seguridad es una parte integral de los sistemas de información			
			A.12.1.1	Análisis y especificaciones de los requerimientos de seguridad	Las declaraciones de los requerimientos comerciales o mejoras para los sistemas de información existentes deben especificar los controles de seguridad
A.12.2	Procesamiento correcto en aplicaciones	Prevenir errores, pérdida, modificaciones no autorizadas o mal uso de información en aplicaciones			
			A.12.2.1	Validación de datos de entrada	Los datos de entrada para aplicaciones deben ser validadas para asegurar que son correctos y apropiados
			A.12.2.2	Control de procesamiento interno	Controles de validación deber ser incorporados dentro de aplicaciones para detectar cualquier corrupción de información causadas por errores de procesamiento o actos deliberados
			A.12.2.3	Integridad del mensaje	Requerimientos para asegurar la autenticidad y proteger la integridad del mensaje en aplicaciones debe ser identificada y apropiados controles deben ser identificados e implementados
			A.12.2.4	Validación de datos de salida	Los datos de salida de una aplicación deben ser validados para asegurar que el procesamiento de la información almacenada es correcta y apropiada para las circunstancias
A.12.3	Controles criptográficos	Proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos			
			A.12.3.1	Política para el uso de controles criptográficos	Una política en el uso de controles criptográficos para la protección de información debe ser desarrollada e implementada

			A.12.3.2	Gestión de claves	Se debe establecer la gestión de claves para soportar el uso de técnicas criptográficas de la organización
A.12.4	Seguridad de los archivos del sistema	Asegurar la seguridad de los archivos del sistema			
			A.12.4.1	Control de software operacional	Deben existir procedimientos establecidos para controlar la instalación de software en sistemas operacionales
			A.12.4.2	Protección de los datos de prueba del sistema	Los datos de prueba deben ser seleccionados cuidadosamente y protegidos y controlados
			A.12.4.3	Control de acceso al código fuente del programa	El acceso al código fuente de los programas debe ser protegido
A.12.5	Seguridad en los procesos de desarrollo y soporte	Mantener la seguridad del software e información del sistema de aplicación			
			A.12.5.1	Procedimientos de control de cambios	La implementación de cambios debe ser controlada por medio del uso de procedimientos formales de cambios
			A.12.5.2	Revisión técnica de aplicaciones después de cambios en el sistema operativo	Cuando los sistemas operativos son cambiados, las aplicaciones críticas del negocio deben ser revisadas y probadas para asegurar que no existe un impacto adverso en las operaciones organizacionales y en la seguridad
			A.12.5.3	Restricciones en cambios para los paquetes de software	Se deben rechazar las modificaciones a los paquetes de software, se debe limitar a cambios específicos y todos los cambios deben ser estrictamente controlados
			A.12.5.4	Filtración de información	La oportunidades para la fuga de información deben ser prevenidas

			A.12.5.5	Desarrollo de software por externos (outsourcing)	El desarrollo externo de software debe ser supervisado y monitorizado por la organización
A.12.6	Gestión de vulnerabilidad técnica	Reducir riesgos resultantes de explotación de vulnerabilidades técnicas publicadas			
			A.12.6.1	Vulnerabilidades técnicas de los controles	Se debe obtener información oportuna sobre vulnerabilidades técnicas de sistemas de información en uso, se debe evaluar la exposición de la organización a ales vulnerabilidades y se deben tomar las medidas apropiadas para tratar el riesgo asociado
A.13	Gestión de incidentes de la seguridad de la información				
A.13.1	Reporte de eventos y debilidades de seguridad de la información	Asegurar que los eventos de seguridad de la información y debilidades asociadas con los sistemas de información son comunicados en una manera que permita que las acciones correctivas sean realizadas oportunamente			
			A.13.1.1	Reporte de eventos de seguridad de la información	Los eventos de la seguridad de la información deben ser reportados a través de los canales gerenciales apropiados tan pronto como sea posible
			A.13.1.2	Reporte de debilidades de seguridad	Todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información deben ser requeridos para tomar nota y reportar cualquier debilidad de seguridad observada o sospechada en los sistemas o servicios
A.13.2	Gestión de incidentes y mejoras de la seguridad de la información	Asegurar que un consistente y efectivo enfoque es aplicado para gestionar los incidentes de seguridad de la información			
			A.13.2.1	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos gerenciales para asegurar una rápida, efectiva, y ordenada respuesta a los incidentes de seguridad de la información

			A.13.2.2	Aprendiendo de los incidentes de seguridad de la información	Deben existir mecanismos establecidos para cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información
			A.13.2.3	Recolección de evidencia	seguimiento contra una persona u organización después de un incidente de seguridad involucra una acción legal (civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la jurisdicción relevante
A.14	Gestión de la continuidad del negocio				
A.14.1	Aspecto de la seguridad de la información de la gestión de la continuidad del negocio	Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas importantes de los sistemas de información o desastres y asegurar su reanudación oportuna			
			A.14.1.1	Incluyendo la seguridad de la información en el proceso de gestión de la continuidad del negocio	Un proceso de gestión debe ser desarrollado y mantenido para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización
			A.14.1.2	Continuidad del negocio y evaluación del riesgo	Los eventos que pueden causar interrupciones a los procesos del negocio deben ser identificados, junto con la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información

			A.14.1.3	Desarrollo e implementación de los planes de continuidad incluyendo la seguridad de la información	Los planes deben ser desarrollados e implementados para mantener o restaurar las operaciones y asegurar la disponibilidad de información en el nivel requerido y en las escalas de tiempo requeridas después de la después de la interrupción o falla en los procesos críticos del negocio
			A.14.1.4	Marco referencial para la planificación de la continuidad del negocio	Se debe mantener un solo marco referencial de planes de continuidad del negocio para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de las pruebas de mantenimiento
			A.14.1.5	Prueba, mantenimiento y re-evaluación de los planes de continuidad	Los planes de continuidad del negocio deben ser probados y actualizados regularmente para asegurar que se encuentren actualizados y sean efectivos
A.15	Cumplimiento				
A.15.1	Cumplimiento con requerimientos legales	Evitar la violación de cualquier ley, regulación u obligaciones contractuales, y cualquier requerimiento de seguridad			
			A.15.1.1	Identificación de legislación aplicable	Todos los estatutos, regulaciones y requerimientos contractuales relevantes y el enfoque de la organización para atender estos requerimientos deben ser explícitamente definidos, documentados y mantenidos actualizados para cada sistema de información y la organización

			A.15.1.2	Derechos de propiedad intelectual	Procedimientos apropiados deben ser implementados para asegurar el cumplimiento con requerimientos legislativos, regulatorios y contractuales en el uso de material respecto de cual puede existir derechos de propiedad intelectual o en el uso de productos de software propietario
			A.15.1.3	Protección de registros organizacionales	Los registros importantes deben ser protegidos de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, regulatorios, contractuales y del negocio
			A.15.1.4	Protección de datos y privacidad de información personal	Protección de datos y privacidad deben ser asegurados como es requerido en la legislación y regulación relevante, y si fuera aplicable, en las cláusulas contractuales
			A.15.1.5	Prevención del mal uso los medios de procesamiento de la información	Los usuarios deben ser impedidos de usar los medios de procesamientos de información para propósitos no autorizados
			A.15.1.6	Regulación de controles criptográficos	Los controles criptográficos deben ser usados en cumplimiento con todos los acuerdos, leyes y regulaciones relevantes
A.15.2	Cumplimiento de las políticas y cumplimiento técnico	Asegurar el cumplimiento de los sistemas con políticas y estándares organizacionales			
			A.15.2.1	Conformidad con políticas y estándares de seguridad	Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad son realizados correctamente para lograr el cumplimiento de las políticas y estándares de seguridad

			A.15.2.2	Revisión del cumplimiento técnico	Los sistemas de información deben ser regularmente revisados para cumplir con los estándares de implementación de la seguridad
A.15.3	Consideraciones de la auditoría de los sistemas de información	Maximizar la efectividad de y minimizar la interferencia al/del proceso de auditoría de los sistemas de información			
			A.15.3.1	Controles de auditoría de los sistemas de información	Los requerimientos de auditoría y actividades que involucran la revisión de los sistemas operacionales debe ser planificada cuidadosamente para minimizar el riesgo de interrupciones a los procesos del negocio
			A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información	El acceso a las herramientas de los sistemas de auditoría deben ser protegidos para prevenir cualquier posible mal uso o compromiso

REFERENCIAS BIBLIOGRÁFICAS

Reglamento de la Ley de Firmas y Certificados Digitales – DECRETO SUPREMO N° 052-2008 – PCM

Bon, J. Van, M. Pieper y A. Van der Venn (Eds.) (2006). Fundamentos de la gestión de Servicios de TI basados en ITIL. Zaltbommel: Van Haren Publishing para itSMF. v3,2008, pp.10-11,15-18.

Cambridge Advanced Learner`s Dictionary. Gestión de Infraestructura ICT. (2002)

Gestión de Seguridad (1999). OGC. Londres: TSO.
Gestión de aplicaciones. (2002). OGC. Londres: TSO.

[ISO03] Orientación sobre el concepto y uso del "Enfoque basado en procesos" para los sistemas de gestión Documento: ISO/TC 176/SC 2/N 544R2 - Diciembre 2003
© ISO 2003 -Normas ISO 9000

Diseño de un SGSI – ISO 27001:2005 Alberto G. Alexander

Documento Autorizado ISO/IEC/POCOSA/1992 INDECOPI ISO 27005

REFERENCIAS WEB

[WEB01]
[Wikipedia01] Web, Gestión de Servicio de TI,
http://es.wikipedia.org/wiki/Gesti%C3%B3n_de_Servicio_TI

[WEB02]
http://en.wikipedia.org/wiki/Big_Four_auditors
Big Four Auditors and Consulting Companies