# Propuesta de un Sistema de Gestión de la Seguridad de la Información para organizaciones en Costa Rica

Guillermo Roldán López, Leonardo Hernández Núñez y Julio Cordoba Retana

Escuela de Ingeniería,
Universidad Latinoamericana de Ciencia y Tecnología,
ULACIT, Urbanización Tournón, 10235-1000
San José, Costa Rica
groldanl953@ulacit.ed.cr,lhernandezn138@ulacit.ed.cr
http://www.ulacit.ac.cr

**Resumen** Hoy con la globalización, se genera gran cantidad de datos que deben almacenarse de manera segura. Las organizaciones en Costa Rica no escapan a esa situación. Estos informes pueden contener datos básicos hasta confidenciales y primordial para las empresas.
Para gestionar la seguridad de la información existen normas como la ISO 27000 que da pautas para mantener la referencia de manera que incluya los tres pilares básicos del saber: confidencialidad, integridad y disponibilidad.
Mediante el uso de la norma ISO 27000 y el marco de Referencia COBIT 5, se desarrolló una guía de políticas básicas necesarias que debe seguir toda en el país para resguardar su información.

**Palabras Clave:** SGSI, COBIT, ISO 27000, Información

## 1. Introducción

La tecnología ha innovado nuevos descubrimientos, herramientas y facilidades para los usuarios; las empresas experimentan con instrumentos tecnológicos que mejoran procesos, tareas, servicios; que agilizan el trabajo y las tareas diarias, y aumentan sus ingresos, en relación con la inversión que los implementan.

Como toda herramienta nueva, la tecnología tiene sus vulnerabilidades, tal es el caso de las organizaciones que pueden llegar a tener en una memoria extraíble toda su información, lo que puede provocar pérdidas millonarias e incluso la bancarrota. Además, no hay que olvidar a todas las empresas o personas que se dedican a quebrantar las leyes, como es el caso de los piratas informáticos, quienes buscan portillos para violentar la seguridad de las empresas.

En Costa Rica, muchas organizaciones e instituciones no cuentan con un manual de políticas de seguridad definido; en algunos casos se tienen políticas dispersas, no bien definidas o delimitadas, que no abarcan todos los contextos. los departamentos de tecnologías de información han sido vistos como un gasto y no una inversión, y eso provoca pérdida de datos de terminales, duplicidad de memorias, alteración no permitida, robos e información incorrecta en los sistemas.

Con la implementación de una política de seguridad de la información se puede controlar la seguridad de las terminales y sistemas, porque todo se encuentra correctamente asegurado y respaldado. Para tratar de reducir estos riesgos, toda empresa u organización debe contar con un Sistema de Gestión de Seguridad de la Información (SGSI) basado en alguna norma técnica.

El presente proyecto tiene como fin desarrollar una propuesta de gestión de seguridad de la información para organizaciones en Costa Rica que contenga las políticas necesarias para mantener segura, confiable y disponible la información de una organización, explica los beneficios de desarrollar e implementar el sistema y, por último, utiliza como referencia la norma ISO 27000 y COBIT 5, que trabajando en conjunto se complementan y vuelvan más completo y eficiente el SGSI para una organización.

## 2. Marco Teórico

Las políticas de seguridad son un plan de acción o conjunto de reglas con las que una empresa hace frente a los riesgos de seguridad ante los que se ve vulnerable, para brindar cierto nivel de seguridad a la misma, que es lo se busca con la implementación, seguridad de la información, lo cual asegura la integridad de los datos, así como, los activos de Hardware y Software(Audit y Association, 2012).

Toda empresa debe salvaguardar la información, pues es todo aquello que la constituye, desde el conocimiento de su recurso humano y sus sistemas de expertos, como resultado de interacción con el entorno o percepciones sensibles del mismo .Todos estos datos constituyen un conjunto organizado, que forma la unidad base de todo el manifiesto.

Un negocio debe confrontar los avances innovadores y los cambios constantes de la tecnología, por lo que debe trazar un plan de políticas de seguridad de la información, las cuales mantendrá actualizadas, así como su infraestructura; para lograr estar a la vanguardia de la operación. El no evitar las vulnerabilidades en la organización es un riesgo,ya que podría ser víctimas de ataques de cibernautas o piratas informáticos que intentan burlar estas defensas, para robar

o alterar la información.

La constitución o implementación de SGSI [1] mantendría firme un plan de políticas, para esto el marco de gestión COBIT 5 presenta una guía de mejores prácticas, dirigidas al control y supervisión de tecnología de la información (TI). Para la investigación se utilizó dicho marco,que específica los procesos:

- Gestionar la Seguridad. [2]
- Gestionar los Servicios de Seguridad.[3]

Estas políticas deben ser realizadas, en primera instancia, acorde a las necesidades de la empresa y las mismas deben revisarse, por parte de la gerencia de TI, cada año, junto con la unidad de seguridad de TI, y la de gestión de riesgo (COBIT).

Las definiciones de la seguridad informática y la seguridad de la información, son confundidas con frecuencia, en primera instancia, por su paronimia, pero sobre todo,porque en el desarrollo y la evolución de la tecnología tienden hacia el modelo de digitalizar y manejar todo tipo de información mediante un sistema informático. No obstante, aunque están destinados para vivir y trabajar en armonía conjuntamente, cada uno tiene objetivos y actividades de seguridad diferentes.

La seguridad de la información es el nivel superior a la seguridad informática, ya que esta es la encargada de dictar las directrices y los planes estratégicos,los cuales aseguran la información e incluyen desde el análisis de riesgos, normativas y los objetivos de la organización. Ver Figura 1.

La seguridad informática está encargada de las implementaciones técnicas de la protección de la información, el despliegue de las diferentes tecnologías, como por ejemplo: antivirus, firewall, detección de intrusos, detección de anomalías, eventos, incidentes, entre otros elementos, que en conjunto con las prácticas de gobierno de la información establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando un activo de la organización se encuentra en algún riesgo; es decir,cómo aplicar las políticas y planes desarrollados en la seguridad de la información.Ver Figura 1. En resumen, se puede definir a la seguridad de la información como la línea estratégica de la seguridad , mientras que la seguridad informática es la táctica y operativo de la seguridad.

**COBIT 5**

[1] Sistema de Gestión de la Seguridad de la Información
[2] APO - Alinear Planificar y Organizar
[3] DSS - Distribuir, Servicio y Soporten

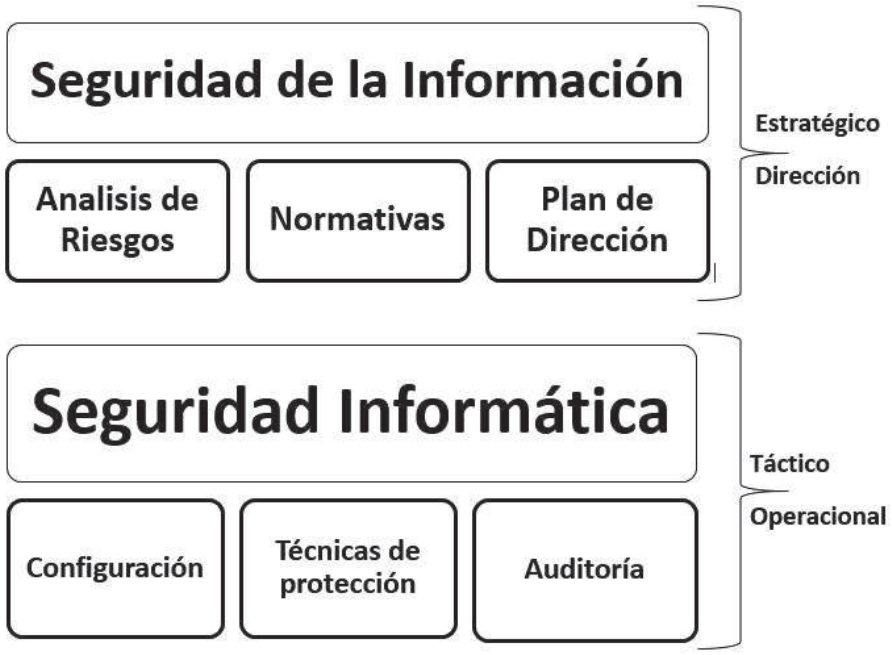


**Figura 1.** Diferencia entre Seguridad Informática y Seguridad de la Información

En esta actualización del COBIT, se publica ÇOBIT 5 para la seguridad de la información"; su principal enfoque, es ofrecer a los interesados una guía práctica para cubrir las necesidades de la empresa, en todos sus niveles,y reducir sus perfiles de riesgo, por medio de una adecuada administración de la seguridad de la información(Audit y Association, 2012). Cabe destacar que este marco de referencia es el único para el gobierno y administración de la TI empresarial.

Gestionar la Seguridad:
Definir, operar y supervisar un sistema para la gestión de la seguridad de la información. Las prácticas de gestión son establecer y mantener un SGSI, definir un plan de tratamiento del riesgo de la seguridad de la información, supervisar y revisar el SGSI.

Gestionar los Servicios de Seguridad

El objetivo principal de este proceso es proteger la información de la empresa en un nivel de riesgo de seguridad de la información aceptable. Dar roles de seguridad y privilegios para el acceso a la información,y supervisarlos.

Las prácticas para gestionar los servicios de la seguridad son: proteger contra software malicioso, urdir la seguridad de la red y conexiones, administrar la seguridad del usuario final, tramitar la identidad de los usuarios,agenciar el acceso a los activos físicos, manipular documentación sensible y por ultimo, supervisar la infraestructura para detectar eventos relacionados con la seguridad.

**Norma ISO/IEC 27000**

Es un grupo de estándares desarrollados por ISO[4] e IEC[5], los cuales brindan un marco de mejores prácticas para ser desarrolladas, implementadas y mantener las especificaciones para la gestión de la seguridad de la información(ISO, 2013); estas normas pueden ser aplicadas a cualquier organización, que pretenda tener una gestión de su SGSI adecuada, algunas de ellas aún se encuentran en preparación.Su primer versión fue la ISO/IEC 27000, publicada el 1 de mayo 2009, revisada 1 de Diciembre 2012 y una tercera edición 14 enero 2014. La norma proporciona las definiciones de la serie de normas 27000, además se publicó la ISO/IEC 27001 el 15 de octubre 2005, revisada en 25 de septiembre 2013, esta es la norma principal de la serie, contiene los requisitos del SGSI y es certificable.

La gerencia de una organización debe de tomar a la SGSI como herramienta de primera instancia para dirigir y controlar la seguridad de la información, la ISO/IEC 27001 es una buena opción, ya que, cubre muchas de las áreas para desarrollar un buen SGSI.

Fundamentos de ISO/IEC 27001

El principal fundamento de la Norma ISO/IEC 27001 es la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en el análisis, evaluación y tratamiento de riesgos, con el fin de lograr reducir las posibles amenazas a niveles asumibles por la empresa; hay que tener en cuenta que la seguridad absoluta no existe, por lo que la SGSI, pretende disminuir los riesgos, no eliminarlos.

Es lógico que cualquier negocio deseé mantener una SGSI actualizada y mejorar constantemente, eso se logra al aplicar el modelo PDCA[6](Deming y Medina, 1989), el cual se aplica para todos los procesos de la SGSI,que va a tomar como entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas,así obtendrá como resultado, la seguridad de la Información gestionada.

[4] ISO: Organización Internacional de Normalización
[5] IEC: Comisión Electrotécnica Internacional
[6] Planificar- Ejecución - Verificar - Mejora

El círculo de Deming[7](Deming y Medina, 1989), como también es conocido por el nombre de círculo PDCA o espiral continua, es plantada como una estrategia continua para mejorar la calidad basada en 4 pasos, el modelo PDCA que corresponde a sus siglas en inglés: Plan, Do, Check, Act, y se traducen como: planificación, ejecución, seguimiento y mejora. Este es un ciclo continuo,que permite mejorar del SGSI.


**Figura 2.** Ciclo PDCA.

La planificación: Pretende establecer las políticas, objetivos para la gestión de riesgo y mejorar la seguridad de la información, por lo que se debe identificar qué se va a mejorar, recopilar los datos de los procesos regenerados , analizarlos y con base en eso, establecer los objetivos desarrollados, detallar los resultados logrados y definir qué procedimientos se necesitaron para conseguir estos fines.

La ejecución: Es donde se da la gestión de la SGSI, pone en ejecución los política, controles, procesos y procedimientos, elaborados en la etapa de planifi-

[7] Edwards Deming

cación, siempre en la medida, bajo un entorno de prueba, para así verificar sus resultados antes de llegar a la implementación final.

La verificación: Revisará los resultados emitidos en la etapa de planificación,y comprobará si las medidas adoptadas dan el resultado esperado.

La mejora: Se lleva a cabo para eliminar cualquier riesgo antes que aparezca, con el objetivo de mejorar la SGSI, lo cual definirá la actitud que se debe de implementar o tomar una vez realizados los tres primeros pasos y según lo ocurrido.

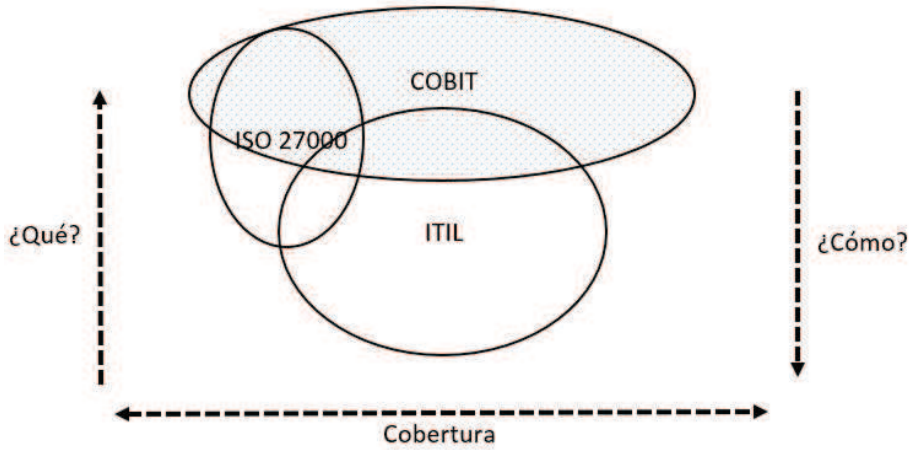


**Figura 3.** Relación COBIT-ISO 27000

En la Figura 3 se muestra la relación que tiene la Norma ISO 27000, con el marco de referencia COBIT 5, e ITIL v3. COBIT 5 e ISO 27000 se enfocan en la implementación de una SGSI; bien estructurada, ISO 27000 tiene como fortaleza principal la implementación de los controles de seguridad, por lo que su cobertura se ve reducida a sólo este aspecto de la SGSI, como se aprecia en el cuadro con respecto a COBIT 5 e ITIL v3, por lo contrario COBIT tiene una cobertura mayor, ya que su enfoque va más allá de la seguridad,y tiene como respaldo, los controles y métricas de la seguridad de la información, y no es tan fuerte en el aspecto de seguridad, por lo que el aplicar de COBIT 5 junto con ISO/IEC 27000, resultan buen complemento, al implementar la SGSI en una organización.

Por la parte de ITIL v3 tiene su fortaleza en los procesos, a través del conjunto de buenas prácticas que lo conforman, con el fin de ofrece un mejor servicio de forma continua que ofrece la organización y , pero tiene la gran limitante que es el desarrollo de sistemas y la seguridad. Al combinar COBIT 5 con ITIL v3, se logra es un aseguramiento en el cumplimiento de los objetivos del negocio y el

regulativo, que de lo contrario representaría un gran riesgo para la organización. Ambos están diseñados en un ciclo de vida de las aplicaciones sistemáticas y servicios de TI, junto con ISO 27000 contemplan el aplicar el ciclo de Deming o Ciclo de mejora continua a la SGSI, que buscan implementar. Al integrar el ISO/IEC 27000 se estará manteniendo la seguridad de la información, de acuerdo con los estándares relevantes de la materia.

En cuanto a la forma que cada uno de ellos interactúa para el "qué hacer" y "cómo hacerlo", se puede leer de la parte superior hacia la parte inferior del mismo, inicia diciendo "qué hacer" para la implementación de la seguridad de la información pasando a un "cómo hacerlo". Iniciando con COBIT 5, que el indica "qué se debe de hacer", lo mismo para ISO/IEC 27000, en el momento que se involucra a ITIL v3, este comienza guiar la pauta hacia un "cómo se debe hacer".

## 3. SGSI - Sistema de Gestión de Seguridad de la Información

Para definir qué controles deben implementarse, se realizó una comparación entre el marco de referencia COBIT y la Norma ISO 27000; se tomó de cada uno los controles y se compararon para tomar las fortalezas de ambos para formar una propuesta más completa, ver en la tabla Tabla 1.

**Tabla 1.** Comparación Controles COBIT 5 e ISO/IEC 27000

| **COBIT 5** | **Norma ISO/IEC 27000** |
|---|---|
| Establecer un SGSI,Supervisar y revisar el SGSI | Establecer un SGSI,Supervisar y revisar el SGSI |
| Proteger contra software malicioso | Proteger contra Software Malicioso |
| Gestionar la seguridad de la red y conexiones | Seguridad en comunicaciones<br>Gestión de criptografía |
| Gestionar la seguridad de los puestos de usuarios final | Seguridad física y ambiental |
| Gestionar la identidad del usuarios y acceso lógico | Control de acceso a datos<br>Organización de la seguridad de la información |
| Gestionar el acceso físico a los activos de TI | |
| Gestionar documentos sensibles y dispositivos de salida | Gestión de Activos |
| Supervisar la infraestructura para detectar eventos relacionados con la seguridad | Información de gestión de incidentes de seguridad |
| | Gestión de operaciones |
| | Sistemas de adquisición, desarrollo y mantenimiento |

**Establecer un SGSI**

La implementación de un SGSI es una decisión estratégica y primordial por todos los beneficios que tiene, es de suma importancia que esta decisión sea completamente apoyada por la dirección superior ya que la implementación involucra toda la organización.

EL diseño del SGSI dependerá, en gran medida, de los objetivos y las necesidades de la organización, esto definirá el alcance de la implantación. El sistema no solamente cubre la organización completa, también se puede diseñar para abarcar áreas o procesos definidos que se requieran controlar, pero lo ideal es desarrollar un sistema integral que cubra todos los riesgos que pueda tener la organización.

El tiempo para desarrollar e implementar un SGSI varía dependiendo del tamaño la organización y el estado actual de la seguridad que tengan en la que se quiere implementar, pero el tiempo estimado es de 6 meses a 1 año, con el agravante que al acercarse al año exista la posibilidad que quede obsoleto al final de ese tiempo y requiere otro proceso de revisión y actualización.

Para poder implantar correctamente un SGSI, la organización debe contar con una estructura definida, así como los recursos necesarios para poder llevar a cabo la implementación correcta del SGSI. La utilización del modelo PDCA es básico para la buena ejecución de cualquier sistema de gestión de la información; ya al finalizar el ciclo con la evaluación, vuelve a iniciar el proceso con las mejoras o correcciones encontradas.

Para un SGSI todo el sistema debe estar completamente documentado, por lo que se utilizan cuatro tipos de documentación, que se representan en la estructura piramidal en la figura 4.

En la cúspide de la pirámide se encuentran las **políticas** , estas son la base de las políticas de seguridad, indican las líneas generales para alcanzar los objetivos de la organización, pero no entran en detalles técnicos, dicho régimen debe ser bien conocido por toda la empresa.

En el segundo nivel se encuentran los **procedimientos**, estos entran a un nivel de detalle más técnicos y se define cómo alcanzar los objetivos expuestos por las políticas, también estos procedimientos deben ser conocidos y entendidos por aquellos que realicen sus funciones.

En el tercer nivel están las **instrucciones** que constituyen los procedimientos, estas instrucciones describen en detalle lo que se debe realizar para la ejecución de los procedimientos.

Para finalizar, en el último nivel se encuentran los **registros**, estos son la evidencia efectiva del cumplimiento del sistema y sus requisitos, deben incluir


**Figura 4.** Pirámide Documentos.

indicadores y métricas de seguridad que permitan la consecución de los objetivos de la seguridad.

**Proteger contra software malicioso**

Protege contra el ataque de software malicioso,por ejemplo a virus, gusanos, ataques informáticos.Para protegerlo implementa, mantiene medidas preventivas y correctivas.

Tanto en COBIT como en ISO 27000, especifica que se debe implementar estas medidas para proteger la información de la organización. COBIT determina con más detalle las actividades que se deben ejecutar, por ejemplo; divulgación de las políticas de seguridad, instalar herramientas de protección, mantener actualizado el software, filtrar todo el tráfico entrante y saliente en la red, revisar continuamente las amenazas y crear controles para regular los accesos a Internet y correos electrónicos.

Al final de este control se debe tener una política de prevención de software malicioso y evaluaciones periódicas de amenazas potenciales.

Como se presenta en el documento "Una Propuesta de Seguridad en la Información: Caso Systematics de México S.A." (BUGARINO HERNANDEZ, 2008), se analiza los riesgos sobre las diferentes posibles brechas que tiene la compañía Systematic y hace una propuesta de política de seguridad para minimizar los riesgos, crea acciones preventivas para evitar algunos virus, tipos y análisis de diferentes antivirus para su elección e instalación, software anti troyanos, software anti espías y por último, recomendaciones de cómo usar el correo electrónico

para evitar el correo basura y estafas.

**Seguridad en la red, conexiones y comunicaciones**

Para gestionar la seguridad de la red y las conexiones, se debe usar una guía de clasificación de información y la política de seguridad en la conectividad; adicionalmente se usa el análisis de riesgos para establecer los controles necesarios.

Es importante implementar controles adecuados que protejan la información de posibles riesgos e integridad de los sistemas y aplicaciones de la red. Se deben de especificar los acuerdos tomados de nivel servicio de las redes, las características de seguridad, los niveles de servicio y requisitos de gestión. Las redes se deben de segregar y crear grupos de usuarios, servicios y sistemas de información; este control también especifica que es necesario establecer políticas y procedimientos para la transferencia de información, así como los acuerdos sobre la transferencia. Se debe gestionar el control de acceso a la información y red de la organización mediante claves y credenciales para hacer uso de esos recursos, además se debe implementar mecanismos de filtrado, como por ejemplo: cortafuegos, detección de instrucciones y políticas de control sobre el tráfico entrante y saliente de la red.

Asimismo, se debe implementar criptografía, esta es la aplicación de técnicas para el cifrado de la información; esto abarca desde documentos, bases de datos o claves de accesos, todo aquello que se quiera guardar de forma secreta o confidencial y se requiera de aplicar un proceso cifrado para ser codificado, ya sea para su consumo o almacenado, su aplicación depende de su categoría, como se puede ver en la tabla 2.

Es de suma importancia realizar pruebas periódicas de intrusiones y de las políticas de seguridad, para analizar su rendimiento o determinar si tiene posibles riesgo que se deban de atender.

Un ejemplo de estos controles son los de la Universidad Francisco de Paula Santander Ocaña (ARRIETA SANCHEZ, SANGUINO REYES, y LOBO SÁNCHEZ, 2015), donde implementaron un cortafuegos, en cada una de sus redes, con el fin de protegerlas contra accesos no autorizados desde el Internet, hacia los interiores de sus redes.

La universidad también tiene estipulado en su política de Seguridad de la Información, aspectos como las reglas de acceso a los servicios de red, dando autorizaciones específicas para sus usuarios.

**Seguridad física y ambiental**

Este control corresponde a la seguridad física de la organización y establece métodos que aseguren la protección de los lugares que sean de acceso restringi-

**Tabla 2.** Categorización de la información

| Categoría | **Descripción** | Ejemplos |
|---|---|---|
| Público, sin clasificación | La información no es confidencial y puede ser pública sin ningún tipo de consecuencias para la organización. | • Descargas de ejemplo de software de la empresa que está a la venta<br>• Los informes financieros requeridos por las autoridades reguladoras |
| Propietaria | La información se limita el acceso interno mediante previa aprobación y protegido del acceso externo. | • Las contraseñas e información sobre los procedimientos de seguridad de la empresa<br>• Procedimientos operativos estándar utilizados en todas las partes del negocio de la organización |
| Datos confidenciales de clientes | La información recibida de los clientes en cualquier forma para el procesamiento de la producción de la empresa | • Medios digitales de clientes<br>• Transmisiones electrónicas de los clientes<br>• Información sobre el producto generado para el cliente por la compañía |
| Datos confidenciales de la organización | La información recopilada y utilizada por la organización en el desarrollo de su negocio para emplear emplear personal que registran, atienden cliente y manejar todos los aspectos de las finanzas corporativas. | • Los datos contables e informes financieros internos<br>• Los datos de negocio del cliente confidenciales y contratos confidenciales<br>• Acuerdos de no divulgación con clientes y vendedores<br>• Planes de negocio de la organización |

do, evita las tentativas de introducción no permitidas, así como del daño de los equipo que se están pretendiendo proteger dentro de ese perímetro.

En cuanto a este aspecto, sólo la norma ISO 27000 hace referencia,y especifica que su principal objetivo es evitar el acceso físico no autorizado, prevenir el daño o interferencia con la información. Todo medio de información o proceso de esta, se debe ubicar en áreas seguras y con acceso controlado,además establecer perímetros de seguridad por medio de barreras físicas (paredes, puertas con accesos controlado),y definir cada una de estas áreas. Los accesos a cada uno de estos ambientes deben ser controlados por medio de revisiones físicas (tarjetas de acceso o ingreso biométrico), lo que permitirá el ingreso sólo del personal autorizado a esas áreas. También a este control le corresponde el aseguramiento del cableado, ya sea, el de energía o el de información, protegiéndose del daño o intercepción.

Se debe contar con monitoreo de las condiciones ambientales tales como: temperatura y humedad, que puedan afectar la operación de los equipos. Además se requiere contar con un procedimiento a seguir, en caso de que el riesgo se materialice. La instalación de protecciones eléctricas contra rayos, sobre voltajes o faltantes de fluido eléctrico, son primordiales en la protección de los equipos.

En el documento desarrollado para la Universidad Francisco de Paula Santander Ocaña (ARRIETA SANCHEZ y cols., 2015), referente a la implementación de políticas de seguridad de la información, con respecto a ítem Áreas Seguras, demostró que se necesita hacer un esfuerzo para proveer a la Universidad de un lugar físico, adecuado para su cuarto de servidores y de mayor seguridad , dado que actualmente se encuentra en un lugar reducido, el cual es asegurado por una llave.

De igual manera salió a relucir la poca vigilancia, por medio de cámaras o algún otro dispositivo, para el área de recepción de activos y el área administrativa de la División de Sistemas.

**Control de acceso a la información**

Para este control se tiene como propósito llevar un control de los accesos a los datos, por medio de un sistema de restricciones y excepciones, como base de todo sistema de seguridad, con el fin de garantizar el acceso de la información al personal autorizado; para lograr este cometido, es imprescindible implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información (bases de datos, servicios de información), cada uno de estos debidamente documentados, comunicados y controlados, verificando que se realicen y se cumplan.

Se debe gestionar que todos los usuarios tengan credenciales correctas con sus derechos establecidos, de qué áreas tienen permiso de accesar . Estos perfiles deben estar basados en la definición de roles y responsabilidades que se realiza en el proceso de planificación, además, deben estar coordinados con cada unidad del negocio, para la administración de los derechos de accesos , cambios y revisiones de la gestión de todas las cuentas y privilegios relacionados. Es de suma importancia mantener un registro de auditoria de los accesos, a la información altamente sensible.

Con los usuarios se debe de establecer procedimientos formales, con el fin de controlar la asignación de permisos de acceso a los sistemas de información, estos procedimientos deben de cumplir con todo el ciclo de vida del accesos de los usuarios, esto incluye el momento del registro al sistema, hasta la dada de baja, cuando ya no se requiera el acceso.

Todo usuario debe de tener conciencia de sus responsabilidades, en particular el uso de su contraseña, por medio de políticas que especifiquen mantener los escritorios monitores o espacios de acceso común libre de cualquier información sensible a los accesos del usuario, con el fin de reducir las entradas no autorizadas. Se debe de establecer las responsabilidades de seguridad, definiendo y documentando las relativas a seguridad de la información, en la descripción de los puestos.

Los accesos a sistemas y aplicaciones, deben ser controlados y protegidos físicamente, al igual que los anteriores es necesario establecer procedimientos operativos para la protección de los documentos del sistema y medios informáticos y asegurar el tránsito de la información electrónica por medio del cifrado de datos.

En cuanto a la organización de la seguridad, ISO 27000 expone dos tipos de organizaciones: la interna y la externa.

La interna tiene como objetivo principal el manejo de la información dentro de la empresa,y establecer un marco de referencia gerencial para iniciar y controlar la implementación de la seguridad de la información. Por parte de la gerencia se debe dar una aprobación a las políticas de seguridad de la información, asignar roles de seguridad, coordinar y revisar la implementación de las políticas, en toda la organización. También la gerencia debe mostrar compromiso, apoyando activamente la seguridad por medio de una directiva clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información.

La organización de la seguridad externa, busca mantener la seguridad y procesamiento de la información que es manejada por grupos externos. Dicta que la seguridad y procedimientos, no deben ser reducidos por la introducción de productos y servicios, se debe controlar cualquier ingreso a la información al existir la necesidad de trabajar con grupos externos, los cuales requieren de acceso a la misma. Es necesario realizar una evaluación de riesgo para determinar las implicaciones de seguridad y los requerimientos de control.

El El documento de Políticas de Seguridad de la Información que se ha desarrollado para la Universidad Francisco de Paula Santander Ocaña (ARRIETA SANCHEZ y cols., 2015), contempla de buena forma las reglas de control de acceso y los derechos para cada usuario o grupos de usuarios de los sistemas de información, estableciendo las responsabilidades de cada unos de los usuarios, en lo que se refiere al tratamiento de la información y todos aquellos que se requiera el uso de accesos.

Además el artículo “Diseño de un plan estratégico de tecnologías de información para la universidad Francisco de Paula Santander de Caña”(ARRIETA SANCHEZ y cols., 2015) evidencia que bajo este proceso se ha creado procedimientos documentados, aprobados, controlados e implementados, que detallan la manera como se deben llevar a cabo las actividades propias del procedimiento.

**Acceso físico a activos de TI**

Se debe gestionar todos los activos, desarrollarse el inventario, tener todas las propiedades de los activos, un manual del uso aceptable, gestionar el uso de

medios extraíbles, un manual de disposiciones de los medios de comunicación, etiquetado de activos y por último, una gestión de activos de información con su clasificación y etiquetado.

Además se requiere implementar procedimientos para conceder o limitar el acceso a los activos, que puede ser desde computadoras, hasta acceso a edificios. Es importantes gestionar todas las peticiones y concesiones; en todo momento debe tenerse actualizado los perfiles de acceso para limitar los riesgos o brechas de seguridad.

Restringir el acceso a ubicaciones sensibles de TI, estableciendo parámetros de acceso y restricciones de acceso como vallas, muros u otros dispositivos de seguridad.

En el artículo "Identificación de los controles de seguridad física del centro de datos de la Universidad Autónoma de Occidente" (Montes Santacruz y cols., 2014) , habla de la importancia de implementar este grupo de controles en la institución, todo el artículo se refiere al implementación de controles de seguridad física utilizando diferentes normas, entre ellas la ISO /IEC 27001: 2013 y la ISO /IEC 27002: 2013, desarrollando todo un documento de que se debe de implementar. El documento concluye con que se debe de dar una mejora documentación, procedimientos, políticas de la institución.

**Gestión de Activos y Documentos Sensibles**

La gestión de documentos es el manejo adecuado de los documentos de la organización, en cualquiera que sea el formato de sistematización que está empleé;Además, es importante tener presente que un documento es un contenedor de información, aquello que es posible organizar, ya sea de forma física o digital. La gestión de documentos permite a la empresa implementar un adecuado manejo de su documentación sensible, aplicando la tecnología y procedimientos que permitan la gestión.

COBIT 5 habla de la gestión de documentos, como el establecer salvaguardas físicos apropiados para los documentos, ya sean físicos o digitales de la empresa, asignándole privilegios de acceso a los usuarios, según el principio de menor privilegio, con el fin de equilibrar los riesgos, además de llevar un inventario de los documentos, así como la destrucción y desecho de los mismos.

En el artículo "Diseño de un plan estratégico de tecnologías de información para la universidad Francisco de Paula Santander Ocaña" (ARRIETA SANCHEZ y cols., 2015) se aplica el proceso de la gestión de activos, lo que le brinda a la universidad un buen manejo de sus activos, manteniéndolos en un inventario actualizado y debidamente identificados. También ellos cuentan con el manejo de entrega de activos, así como, dado de baja de los mismos, y tiene como res-

ponsable al jefe de la División de Sistemas.

Por otro lado se destaca que se cuenta con un grupo de reglas de uso aceptable de los activos, dentro del plan de políticas de seguridad de la información de la universidad, estos no son de dominio público, es decir existe el desconocimiento de dichas reglas por la comunidad de la universidad.

**Gestión de incidentes de seguridad**

La gestión de incidentes tiene con finalidad crear controles de detección y corrección, para reducir los incidentes desfavorables que se presenten y puedan afectar a la SGSI; también busca crear una base de datos de conocimiento, de la cual se obtenga información de los incidentes que se han presentado, saber cómo enfrentarlos y posibles soluciones, además de como reportar las nueva afectaciones que se presentan.

COBIT e ISO 27000 hablan de cómo aplicar este control de forma adecuada para garantizar a la SGSI una buena supervisión de su infraestructura. COBIT detalla el uso de herramientas de monitoreo que permitan la vigilancia de la red ante estos ataques, especifica que cada uno de los eventos deben de ser monitoreados e identificados según su nivel de seguridad, y almacenarse por un tiempo definido con el fin de que sirva de información para futuras investigaciones, y a su vez, para ser revisadas regularmente para la detección de incidentes potenciales.

Los procedimientos para la gestión de incidentes deben ser comunicados a todo el personal de la empresa. De suceder uno de los eventos, la información de la misma debe ser recolectada,esto por si acaso, en un momento posterior se requiera alguna evidencia y el aseguramiento de los requisitos legales.

Como se mencionó en el artículo “Diseño del plan de gestión de seguridades de la información para CEPSA S.A ” (Rosero Proaño, 2015), ninguna empresa está exenta de incidentes de seguridad. Los resultados, según este artículo, muestra que los incidentes provocados por virus y malware son de un 72,73 % y 54,55 % ,respectivamente, estos son generados por la falta de cultura en la seguridad de la información, de igual forma, no hay que desinteresarse por los demás incidentes que puede afectar a una organización, de ahí la importancia que se implementen los controles de la gestión de percances, dentro de un plan se seguridad de la información.

**Gestión de Operaciones**

Para ISO 27000 la gestión de operaciones tiene como fin principal, garantizar la operación correcta y segura de los medios de procesamiento de la información,y establezca responsabilidades, procedimientos para la gestión y operación

de estos e incluya el desarrollo de los procedimientos adecuados.

La norma dice que los procedimientos operacionales se deben documentar y mantener al alcance de todos los usuarios que lo necesiten, para que en el momento que requieran ser consultados, estén a la mano. Los documentos de los procesos operacionales deben ser preparados para actividades tales como: procedimientos para encender y apagar computadoras, copias de seguridad, mantenimiento del equipo, manejo de medios, cuarto de cómputo, manejo del correo y seguridad.

La gestión del cambio debe estar sujeta a un estricto control gerencial, verificando los cambios de sistemas de procesamiento de la información, sistemas operacionales y software de aplicación. Para asegurar el control satisfactorio del cambio, se debe asignar responsabilidades y procedimientos gerenciales, dado que el control inadecuado es una de las principales fallas y vulnerabilidades en los sistemas o en la seguridad.

Los ambientes de desarrollo, pruebas y operacionales deben de ser ambientes totalmente separados, con el fin de reducir el riesgo de accesos no autorizados o que los cambios en los sistemas operacionales afectan ambientes que no deben verse involucrados en el cambio; los niveles de separación entre ellos deben ser claramente identificados, implementando los controles adecuados.

Como lo menciona el artículo "Diseño de un plan estratégico de tecnologías de información para la universidad Francisco de Paula Santander Ocaña" (ARRIETA SANCHEZ y cols., 2015) se cuenta con procedimientos documentados para las actividades del sistema, estos procedimientos son controlados por la Oficina de Calidad de la universidad.

**Adquisición, Desarrollo y Mantenimientos**

El sistema de adquisiciones busca garantizar la seguridad de la parte integral de los sistemas de información, estos incluyen sistemas operativos, infraestructuras, aplicaciones de negocio y estándar o de uso generalizado, aplicaciones desarrolladas por los usuarios y servicios. Antes de realizar un desarrollo y/o implementación de los sistemas de información, se debe haber identificado y consensuado los requisitos de seguridad a aplicar, cada uno de estos requisitos debe ser recolectado en la fase de elaboración de requisitos del proyecto, justificados, aceptados y documentados en el proceso completo para el sistema de información.

Como se menciona anteriormente, el objetivo del control es la seguridad de la información y para lograr ese cometido es necesario implementar la seguridad de las aplicaciones del sistema, con el fin de evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones, diseñando los controles apropiados para cada una ellas, inclusive aquellas que hayan sido

desarrolladas por el usuario,y asegurar así, el procesamiento correcto de la información.

También es importante proteger la integridad de la información, así como su autenticidad y confidencialidad, por lo que se deben de implementar controles criptográficos, que hacen referencia a la gestión de la criptografía mencionada anteriormente, la cual especifica qué políticas criptográficas se deben de aplicar a la información, así como la gestión de claves y técnicas de encriptación.

En el artículo(ARRIETA SANCHEZ y cols., 2015) se hace referencia, que la universidad, con respecto a su desarrollo de aplicaciones, no tiene tareas asignadas a los diferentes usuarios, por cada etapa del proceso. Con lo que respecta a la realización de pruebas de los requerimientos operacionales de los sistemas que se adquieren o de sus actualizaciones, tampoco posee un documento procedimental que hable de cómo se debe de realizar dichas pruebas. Como recomendaciones dadas por la autora del documento,es la segregación de las tareas en cada una de las fases de desarrollo de aplicaciones, como el documentar las actividades de cada fase, definir los controles para especificar los requerimientos para el desarrollo y pruebas de las adquisiciones.

## 4. Conclusiones y Recomendaciones

En conclusión, la norma ISO 27000 detalla más los controles que COBIT 5, con respecto a la creación e implementación de un sistema de gestión de seguridad de la información, ya que está formado por más dominios con procesos bien definidos y claramente establecidos.

Además, la norma ISO 27002 y COBIT 5 proporciona los elementos necesarios para desarrollar una planificación de seguridad de la información, no sólo por ser fácilmente ajustable para la mejor práctica del negocio, sino también de la estrategia de la organización que permite un marco de la seguridad de la información, para entender los requisitos de seguridad de TI y, en el diseño de las políticas y procedimientos, implementación y operación de los controles, los cuales gestionan los riesgos y son de un valor agregado, que protege la información como un activo fundamental en una organización.

Como recomendación, se debe contar con una política de seguridad bien definida, ya que es el pilar para cualquier SGSI, como se explicó en el artículo :"La norma ISO 27000 y COBIT 5", marcan una pauta de cómo crear una SGSI robusta, ambas se complementan, una a la otra; en donde COBIT 5, detalla qué se debe hacer y el grupo de normas ISO 27000, indica cómo hacerlo. Así se tiene en cuenta que toda organización que deseé contar una, debe crear una política de seguridad. Con un SGSI, correctamente implementado se puede lograr una certificación en ISO 27001, con ellas se brindará un gran valor agregado al ne-

gocio, el cual será sinónimo de seguridad y confiabilidad, en cuando al manejo de su información interna y externa.

## Referencias

ARRIETA SANCHEZ, M. A., SANGUINO REYES, M. R., y LOBO SÁNCHEZ, C. L. (2015). *Diseño de un plan estratégico de tecnologías de información para la universidad francisco de paula santander ocaña* (Tesis Doctoral no publicada). pages 11, 13, 14, 15, 17, 18

Audit, I. S., y Association, C. (2012). *Cobit 5: A business framework for the governance and management of enterprise it*. ISACA. pages 2, 4

BUGARINO HERNANDEZ, F. (2008). *Una propuesta de seguridad en la informacion: Caso systematics de mexico, sa* (Tesis Doctoral no publicada). pages 10

Deming, W. E., y Medina, J. N. (1989). *Calidad, productividad y competitividad: la salida de la crisis*. Ediciones Díaz de Santos. pages 5, 6

ISO, I. (2013). *Iso/iec 27001:2013 information technology – security techniques – specification for an information security management system*. pages 5

Montes Santacruz, K. R., y cols. (2014). Identificación de los controles de seguridad física del centro de datos de la universidad autónoma de occidente. pages 15

Rosero Proaño, P. V. (2015). *Diseño del plan de gestión de seguridades de la información para cepsa sa* (Tesis Doctoral no publicada). Quito: EPN, 2015. pages 16