# INTRODUCCIÓN AL RIESGO Y GESTIÓN DE SEGURIDAD. PARTE II

AUTOR: LUIS RAMÍREZ LORÍA

MARZO: 2021

San Marcos

# Tabla de contenido

## Introducción

En la actualidad la administración y la gestión de la información dentro de una organización o empresa, requiere el establecimiento de procesos de control y gestión de la seguridad, debido a que, en con el auge de la revolución digital cada empresa debe estar preparada para el resguardo y adecuada gestión de sus activos de información, base fundamental de muchos de sus procesos productivos, así como de la relación con clientes, proveedores, acreedores, organismos oficiales, reguladores y demás actores en el ambiente empresarial donde se desempeñe, donde la comunicación y digitalización establecen una base fundamental de interconexión de personas y empresas, reduciendo brechas o barreras geográficas e incursionando muchas organizaciones en la globalización de la economía, pero a su vez, insertando una nueva condición, la necesidad de gestionar riesgos asociados a la información, infraestructura y procesos automatizados que los soportan.

Las empresas que están inmersas en estos procesos de incursión en negocios digitales, cuyos procesos se encuentran automatizados o que tienen una consolidación de sus tecnologías de información deben modificar sus acciones de administración y gestión de riesgos productivos para incorporar y asignar recursos a la gestión de riesgos asociados a la información, sistemas informáticos, recursos de infraestructura y comunicaciones.

En esta lectura abordaremos las recomendaciones y mejores prácticas asociadas a los modelos de gestión de seguridad, el modelo base de seguridad informática, sus alcances, objetivos, políticas y su cumplimiento, así como condiciones requeridas para su mantenimiento, establecimiento de roles y responsabilidades de seguridad de la información, entre otros.

## Modelos de gestión de seguridad

La gestión de seguridad, como se analizó en la lectura anterior, busca la protección de los activos de la organización, sean estos los recursos humanos, infraestructura y en este abordaje, la información de la empresa, en la actualidad la mayor parte de este información es almacenada y estructurada de forma digital y está contenida en los sistemas, infraestructura, bases de datos, directorios, sharepoint, directorios en la nube y en los computadores, lo cual genera un abanico de posibilidades sobre las cuales debe prestarse atención y tomar control desde el modelo de gestión de seguridad, para esto debe establecerse cuál es el ciclo de vida de la información, no solo su uso comercial o hacia el cliente, deben analizarse funciones relacionadas con su captura, procesamiento e incluso su destrucción.

## Conceptos importantes

En estos análisis debe considerarse el activo “información”, pero también la infraestructura, equipos de almacenamiento, redes de comunicaciones, instalaciones físicas, centros de impresión, de publicidad y personas relacionadas.

Como se analizó en la lectura anterior, algunas propiedades o características importantes de la **información** importantes de retomar son:

- **Confidencialidad**: La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.
- **Integridad**: La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.
- **Disponibilidad**: La información debe estar siempre accesible para aquellos que estén autorizados.

Sobre el activo de información caben las **amenazas**, que pueden ser de muy diversa naturaleza u origen, tales como:

- **Origen natural:** En nuestro país existen factores usuales como lluvias, inundaciones, terremotos, rayería, incendios, huracanes, entre otros, que pueden afectar la infraestructura donde reside.
- **Fallos en Sistemas Informáticos y Comunicación:** Fallos, incidencias o errores en los sistemas, interrupciones por fallos de hardware, cortes en la comunicación, fallos de fibra o conectividad, entre otros.

- **Error humano:** errores accidentales o deliberados de las personas, acceso no autorizados tanto en funciones de sistema como a nivel de infraestructura, sistemas operativos o centros de datos, sustracción de datos, uso incorrecto de derechos de autor o de acceso, fallas de disponibilidad, uso indebido de licencias, información comprometida por robo de equipos a funcionarios, revelación de secretos corporativos, espionaje y otros,

Aunado a las amenazas deben tomarse en consideración las **vulnerabilidades** que son propias del entorno de los sistemas de información y que dependen de su naturaleza, por lo cual están intrínsecas a los activos de información, pueden relacionarse con el hardware, software, redes, personal, edifico, infraestructuras y dinámicas de la organización, por ejemplo:

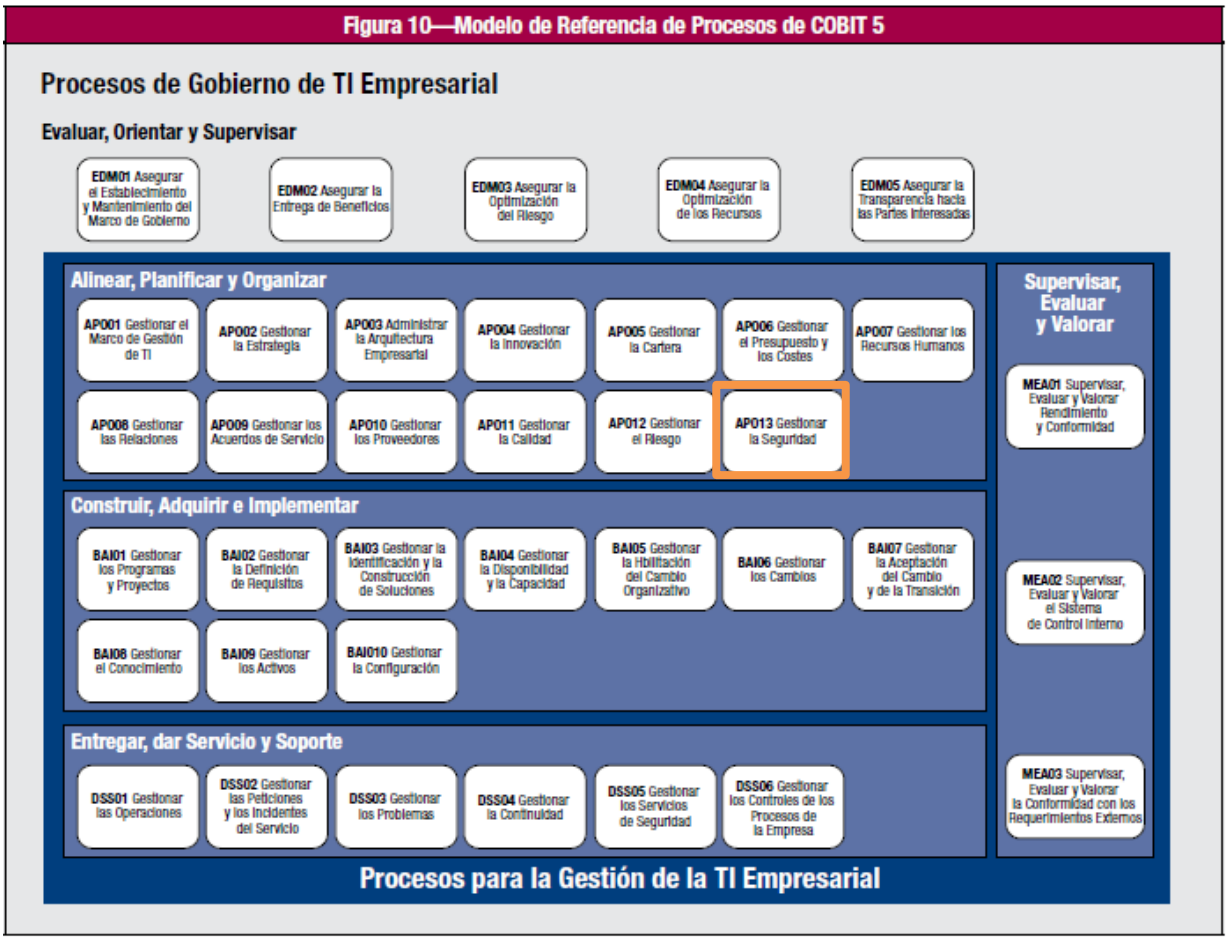
- El equipo informático y la posible variación de temperaturas, humedad, sistemas de supresión de incendios y otros.
- Las vulnerabilidades de los sistemas operativos por su estructura, actualización, configuración, accesibilidad, protección o mantenimiento.
- La localización de los equipos y centros de datos, en lo particular en el país existe una identificación de sitios con mayor susceptibilidad a desastres naturales, inundaciones, terremotos, rayería, etc.
- Aplicaciones y sistemas de información acorde con su diseño, pueden generar vulnerabilidades si no se tratan adecuadamente, incluyendo sus esquemas de almacenamiento de información.
- Personal responsable de los activos de información, el cual requiere una formación suficiente en lo relacionado a riesgos informáticos, y esto según su nivel, rol y responsabilidad en la organización.

Adicionalmente en la lectura anterior abordamos conceptos como los **virus informáticos**, los **ciberataques**, el inadecuado **uso de la información**, las políticas o **protocolos**, todos estos son factores sobre los cuales las organizaciones deben establecer o reforzar los mecanismos de control y gestión de seguridad de las tecnologías de información.

## Modelo de Gestión de Seguridad según COBIT5

Para ISACA, una empresa puede organizar sus procesos como estime conveniente siempre y cuando los objetivos básicos de gobierno y de gestión de las tecnologías de información y comunicación sean cubiertas, un buen modelo de gobierno debe procurar evaluar, orientan y supervisar cada acción asociada a los recursos TIC, en cuanto a temas de seguridad, a nivel del Modelo de Referencia de COBIT 5 las recomendaciones y mejores

prácticas sobre Gestión de Seguridad se ubican en el dominio APO, Alinear, Planificar y Organizar, el cual puede verificarse con mayor detalle en la siguiente figura sobre el Modelo de Referencia:




Modelo de Referencia de Procesos COBIT 5. Fuente: (ISACA®, 2012)

## APO13 Gestionar la Seguridad

Acorde con ISACA, este proceso busca *"mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa."* (ISACA®, 2012), por lo cual su declaración u objetivo es definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

La implementación de este proceso busca las siguientes Metas de TI:

- Cumplir y brindar soporte de TI al negocio, sobre leyes y regulaciones externas.
- Administrar los riesgos de negocio relacionados con las TIC gestionadas.

- Demostrar con transparencia costes, beneficios y gestión de riesgo de las TI.
- Administrar la seguridad de la información, infraestructura de procesamiento y aplicaciones.
- Garantizar la disponibilidad de información útil y relevante para la toma de decisiones.

Por su parte las metas del proceso son:

1. Mantener el sistema para la gestión de la seguridad de la información de forma efectiva acorde a los requerimientos de seguridad de la información definidos por la empresa.
2. Establecer, aceptar y comunicar el plan de seguridad de la información.
3. Implementar las soluciones de seguridad de la información y garantizar su operación cotidiana y consistente en toda la organización.

La siguiente figura resume el proceso, metas y métricas.

| **EDM04 Asegurar la Optimización de Recursos** | **Área: Gobierno**<br>**Dominio: Evaluar, Orientar y Supervisar** |
|---|---|
| **Descripción del Proceso**<br>Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo. | |
| **Declaración del Propósito del Proceso**<br>Asegurar que las necesidades de recursos de la empresa son cubiertas de un modo óptimo, que el coste TI es optimizado y que con ello se incrementa la probabilidad de la obtención de beneficios y la preparación para cambios futuros. | |
| **El proceso apoya la consecución de un conjunto de principales metas TI:** | |
| **Meta TI** | **Métricas Relacionadas** |
| 09 Agilidad de las TI | • Nivel de satisfacción de los ejecutivos de la empresa con la capacidad de respuesta de TI a nuevos requerimientos<br>• Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas<br>• Tiempo medio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada |
| 11 Optimización de los activos, recursos y capacidades de las TI | • Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes<br>• Tendencia de los resultados de las evaluaciones<br>• Niveles de satisfacción de los ejecutivos de negocio y TI con los costes y capacidades TI |
| 16 Personal del negocio y de las TI competente y motivado | • Porcentaje del personal cuyas habilidades TI son suficientes para las competencias requeridas para su función<br>• Porcentaje del personal satisfecho con su función TI<br>• Número de horas de aprendizaje/prácticas por trabajador |
| **Metas y Métricas del Proceso** | |
| **Meta del Proceso** | **Métricas Relacionadas** |
| 1. Las necesidades de recursos de la empresa son cubiertos con capacidades óptimas. | • Nivel de realimentación de las partes interesadas sobre la optimización de los recursos<br>• Serie de beneficios (p.ej., ahorro de costes) que se logran a través de la utilización óptima de los recursos<br>• Número de desviaciones del plan de recursos y las estrategias de arquitectura empresarial |
| 2. Los recursos se asignan para satisfacer mejor las prioridades de la empresa dentro del presupuesto y restricciones. | • Número de desviaciones (y excepciones) de los principios de gestión de recursos<br>• Porcentaje de proyectos con asignación de recursos adecuados |
| 3. El uso óptimo de los recursos se logra a lo largo de su completo ciclo de vida económico. | • Porcentaje de reutilización de componentes de la arquitectura<br>• Porcentaje de proyectos y programas con un estado de riesgo medio o alto debido a la problemas en la gestión de recursos<br>• Número de metas de rendimiento de la gestión de recursos alcanzadas |

Fuente: (ISACA®, 2012)

Este proceso se compone de tres prácticas, las cuales se mencionan y resumen a continuación:

### *APO13.01 Establecer y mantener un SGSI.*

Acorde con el COBIT 5, esta práctica de Gobierno busca: *"Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa."* (ISACA®, 2012)

Su cumplimiento implica desarrollar las siguientes actividades:

1. Definir alcance y límites del SGSI según las características de la empresa, localización, activos, tecnología, giro de negocio y exclusiones.
2. Definir el SGSI según las características definidas por el negocio, alcance y límites.
3. Alinear el SGSI con el enfoque de gestión de seguridad general de la empresa.
4. Obtener autorización de la alta administración para implementar/operar el SGSI.
5. Preparar y mantener la declaración de aplicabilidad del SGSI.
6. Definir y comunicar roles y responsabilidades de la gestión de seguridad de la información.
7. Comunicar el enfoque del SGSI.

### *APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.*

Acorde con el COBIT 5, esta práctica de Gobierno busca: *"Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio."* (ISACA®, 2012)

Su cumplimiento implica desarrollar las siguientes actividades:

1. Definir y mantener el plan de tratamiento de riesgos de seguridad de la información, alineado a objetivos estratégicos, arquitectura de la empresa, incluyendo prácticas

de gestión, soluciones de seguridad y los recursos, responsabilidades, prioridades respectivas para la gestión de riesgos identificados en seguridad de información.

2. Definir y mantener un inventario de componentes implementados para gestión de riesgos de seguridad de la información (parte de la arquitectura informática).
3. Desarrollar propuestas de implementación del plan de tratamiento de riesgos de seguridad de la información, con casos de negocio que incluyan financiamiento, roles y responsabilidades.
4. Brindar información para diseñar y desarrollar las prácticas de gestión y soluciones según el plan de tratamiento de riesgos de seguridad de información.
5. Definir la forma de medir la efectividad de las prácticas de gestión y especificar la forma de uso de las mediciones para evaluar efectividad y que los resultados sean reproducibles y comparables.
6. Recomendar programas de formación y concientización en materia.
7. Integrar planificación, diseño, implementación y supervisión de los procedimientos de seguridad de la información con otros controles para asegurar la prevención y detección temprana de eventos de seguridad y la respuesta a incidentes de seguridad.

### *APO13.03 Supervisar y revisar el SGSI.*

Acorde con el COBIT 5, esta práctica de Gobierno busca: *"Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua."* (ISACA®, 2012)

Su cumplimiento implica desarrollar las siguientes actividades:

1. Revisar periódicamente el SGSI, políticas, objetivos y prácticas. Considerando resultados de auditorías, incidentes, resultados de mediciones de efectividad, sugerencias y realimentación de los interesados.
2. Auditar internamente el SGIS a intervalos definidos.
3. Revisar el SGSI periódicamente por la Dirección (TI/Negocio) para asegurar que su alcance se mantiene adecuado e identificar mejoras al proceso.
4. Proporcionar datos e información para mantenimiento de planes de seguridad, considerando incidencias de actividades de supervisión y revisión periódica.
5. Registrar acciones y eventos que pueden impactar la efectividad y desempeño del SGSI.

## Alcance del SGSI

**AL REDACTAR LA DOCUMENTACIÓN DE SU SGSI, NO TIENE QUE USAR TÉRMINOS EXACTOS. SIN EMBARGO, DEFINIR LOS TÉRMINOS UTILIZADOS PUEDE ESCLARECER SU SIGNIFICADO E INTENCIÓN. PUEDE SER ÚTIL PROPORCIONAR UN GLOSARIO JUNTO A LA DOCUMENTACIÓN DE SU SISTEMA. (NQA., 2018)**

Acorde con las mejores prácticas y recomendaciones de la ISO/IEC 27001, el Sistema de Gestión de Seguridad de la Información debe cubrir en su alcance:

- Los límites del sitio físico o sitios incluidos (o no incluidos)
- Los límites de las redes físicas y lógicas incluidas (o no incluidas)
- Los grupos de empleados internos y externos incluidos (o no incluidos);
- Los procesos, actividades o servicios internos y externos incluidos (o no incluidos); y
- Interfaces clave en los límites del alcance.

Inicialmente un factor clave es el establecimiento de los recursos prioritarios sobre los cuales el SGSI debe actuar, aquellas condiciones de mayor relevancia para la organización deben incorporarse en el alcance lo cual debe definirse con las partes interesadas. Por ejemplo:

- Las operaciones realizadas en el área de TI
- El soporte y gestión de sistemas, correo electrónico y accesos.
- Los equipos, sistemas, datos e infraestructura del centro de datos

Esta documentación debe resguardarse en un sitio (documento, bitácora, mapa) con toda la información recopilada y en análisis, para tener documentación del contexto establecido por la organización durante la formulación del SGSI. Deben resguardarse aspectos tales como:

- Actas con los representantes e involucrados de negocio y niveles gerenciales.
- Actas de reuniones, planes de negocio.
- Identificación de problemas internos, externos, partes interesadas, necesidades y expectativas de negocio.
- Análisis FODA, estudio PESTLE o evaluación de riesgo empresarial de alto nivel.

## Objetivos del SGSI

En relación con los objetivos las mejores prácticas y recomendaciones de la ISO/IEC 27005, señala que el Sistema de Gestión de Seguridad de la Información debe incluir, según (NQA., 2018):

1. Proporcionar aviso para la identificación sistemática de riesgos (revisión de activos, grupos de activos, procesos, tipos de información), verificando la presencia de amenazas y vulnerabilidades comunes y registrando los controles que actualmente tiene implementados para administrarlos.
2. Proporcionar un marco para evaluar la probabilidad de que el riesgo ocurra de manera persistente (una vez al mes, una vez al año).
3. Proporcionar un marco para evaluar las consecuencias de cada riesgo que ocurra de manera consistente (por ejemplo, pérdidas de capital monetario).
4. Proporcionar un marco para calificar o categorizar cada riesgo identificado (por ejemplo, alto/medio/bajo), teniendo en cuenta su evaluación de probabilidad y las consecuencias.
5. Establecer criterios documentados que especifiquen, para cada categoría de riesgo, qué tipo de acción debe tomarse y el nivel o prioridad que se le asigna.

## Cumplimiento de la política

Para asegurar el cumplimiento de las políticas, procedimientos y procesos asociados al SGSI una organización puede acudir a la gestión de la auditoría interna a efecto de garantizar el cumplimiento de los requisitos de la norma, para lo cual la norma ISO/IEC 27001 recomienda establecer las siguientes acciones:

- Planificación de la auditoría:
    - Establecer un calendario de trabajo acorde a la escala y complejidad de las operaciones, puede ser mensual o anual.
    - Realizar una evaluación asociada a la normativa, cumplimiento y establecer los modelos de desempeño por cumplir (durante la ejecución) para ser evaluados.
- Mentalidad basada en riesgos:
    - Las auditorías o evaluaciones de cumplimiento de las políticas deben considerar el riesgo del proceso y de la seguridad de la información, entre

mayor riesgo potencial del fallo o de sus consecuencias la evaluación de cumplimiento debe realizarse con mayor frecuencia.

- Auditoría externa:
    - Dependiendo del marco de gestión, políticas, normativas e incluso los entes reguladores de la industria donde se desempeña la organización es necesario recurrir a auditores externos para que evalúen las políticas de gestión de seguridad de la información, el desempeño de los controles y brinden las recomendaciones para asegurar su función.
- Auditorías para certificación.
    - Si la organización se ha acoplado a normas como la ISO/IEC 27000, una certificación garantiza la evaluación regular de controles, el establecimiento de recomendaciones de mejora, la credibilidad del sistema, la reducción de riesgos o de incertidumbre de su evaluación, y el cumplimiento de las expectativas de los interesados.

Un adecuado proceso de evaluación de cumplimiento de las políticas requiere cumplir con:

- La definición del alcance y criterios de evaluación
- El establecimiento de un plan de acción sobre el estudio
- Definición del requerimiento del informe de auditoría
- Establecimiento del enfoque de procesos para garantizar la asignación de tiempo y habilidades requeridas por los auditores

NAQ nos señala que: *"Los resultados consistentes y predecibles se logran de manera más efectiva y eficiente cuando las actividades se entienden y gestionan como procesos interrelacionados que funcionan como un sistema coherente"* (NQA., 2018)

Adicionalmente otra alternativa para garantizar el cumplimiento es mediante la incorporación de mecanismos de control interno, para lo cual la organización requiere establecer mecanismos para la designación de responsables del proceso de gestión y del proceso de control interno, y adicionalmente establecer formalmente los procesos de entrenamiento para su preparación adecuada tanto para operacionalizar como para controlar.

## Mantenimiento del documento

Un Sistema de Gestión de Seguridad de la Información debe contener un conjunto de normas y mejores prácticas interrelacionado y coherente con las definiciones de negocio, su normativa y su estrategia, de forma que facilite y respalde el diseño, implementación y mantenimiento de los controles de riesgos asociados a dicha gestión de seguridad de la información.

Los procesos documentados que forman parte del SGSI suelen ser una combinación de procesos comerciales, de negocio, centrales y existentes, tales como compras, diseño de productos, capacitación, reclutamiento, mantenimiento de equipos, prestación de servicios, y procesos de gestión del SGSI tales como el mantenimiento y mejora de la seguridad, algunos de ellos procesos estándares de TI tales como la gestión de cambios, el respaldo de información, control de accesos, gestión de incidentes y problemas, clasificación de la información, entre otros. Todos estos requieren el establecimiento de proceso de revisión, adecuación y mejora, con el correspondiente mantenimiento y actualización de la documentación de respaldo.

Uno de los elementos fundamentales, señalado en normas como COBIT e ISO/IEC 27000 es la participación activa de las Gerencias de Negocio y la Gerencia de TI, quienes deben incluir en su base de elementos prioritarios la implementación y el mantenimiento efectivo de un SGSI y su documentación.

Para lo anterior NQA en su guía para la implantación de la norma ISO-27001 nos brinda las siguientes características de la información que debe ser documentada para utilizarla durante la implementación y mantenimiento del SGSI, señalando que para ser utilizada esta información debe:

- *"Ser precisa.*
- *Ser comprensible para las personas que la usan regularmente u ocasionalmente.*
- *Apoyar en el cumplimiento de los requisitos legales, administrar los riesgos y alcanzar los objetivos.*

- *Para que su información documentada siempre satisfaga estos requisitos, necesitará contar con procesos para garantizar que:*
    - *La información documentada se revisa cuando lo requieren las personas apropiadas antes de que se divulgue a la circulación general.*
    - *El acceso a la información documentada se controla para que no pueda ser cambiado, corrompido, eliminado o accedido por individuos sin permiso.*
    - *La información se elimina de forma segura o se devuelve a su propietario cuando existe el requisito de hacerlo.*
    - *Puede realizar un seguimiento de los cambios en la información para garantizar que el proceso esté bajo control.*
- *La fuente de su información documentada puede ser interna o externa, por lo que sus procesos de control deben administrar la información documentada de ambas fuentes."* (NQA., 2018)

Dentro de las recomendaciones que se brindan a las organizaciones para un buen control de documentos están la siguientes:

- La documentación y su actualización deben estar a cargo de una única persona o de un grupo reducido, responsable de garantizar que los documentos nuevos / modificados se revisen antes de su emisión, se almacenen en la ubicación correcta, se retiren de la circulación cuando se reemplacen y se mantenga un registro de cambios.
- Se recomienda utilizar un sistema de gestión de documentos electrónicos que implemente controles y flujos de trabajo automáticos, incluyendo respaldo, control de versiones, generación de informes de auditoría de los documentos, su gestión y cambios
- Establecer un respaldo de datos electrónicos y procesos de archivado y almacenamiento de archivos impresos.
- Establecer una gestión de conocimiento para garantizar el conocimiento de los empleados sobre el control de documentos, el mantenimiento de registros y los requisitos de acceso/retención de información.

## Roles y responsabilidades de seguridad de la información

Al igual que en la mayor parte de las normas de gestión de tecnologías de la información y comunicaciones, un aspecto fundamental para la implantación y gestión de un sistema de seguridad de la información es el establecimiento y control de los roles y responsabilidades de los involucrados en la seguridad de la información.

Según NQA: *"Para que las actividades de seguridad de la información formen parte de las actividades cotidianas para el personal de la organización, las responsabilidades que tienen deben definirse y comunicarse claramente. Aunque no hay ningún requisito en las normas (como la ISO/IEC 27001) respecto al nombramiento de un representante de Seguridad de la Información, puede ser útil para algunas organizaciones designar a uno para dirigir un equipo de seguridad de la información que coordine la capacitación, el control de los controles y la presentación de informes sobre el desempeño del SGSI a la gerencia. Este individuo puede ser el responsable de la protección de datos o servicios de TI. Sin embargo, para llevar a cabo su función de manera efectiva, lo ideal sería que fuese miembro de la gerencia y con conocimiento de la gestión de seguridad de la información."* (NQA., 2018)

## Conclusiones y recomendaciones

La implementación de un SGSI debe permitir a las organizaciones el establecimiento de políticas y normativas de seguridad de la información, lógicas, incrementales y principalmente alineadas con el entorno y capacidades de la organización, lo cual requiere un alineamiento estratégico y una gestión oportuna por parte de la organización, lo cual no puede ser solamente dirigido por los procesos o Gerencia de Tecnologías de la Información, sino que requiere el patrocinio, conocimiento e impulso gerencia de forma general, identificando la seguridad de la información como un factor estratégico e incluso como un factor crítico para asegurar el éxito de la empresa.

Implementar y mantener un SGSI requiere por lo tanto de un compromiso organizacional, por lo cual el entendimiento de su función y la adecuada acotación de su alcance y costes necesita un esfuerzo importante y suficientemente amplio como para cubrir la información crítica que necesita protección, pero no tan amplio como para carecer de recursos para implementarlo y mantenerlo, esto implica que debe asegurarse que las partes interesadas comprendan y apoyen su establecimiento.

El estudio concreto del análisis de riesgos informáticos y del establecimiento de un Sistema de Gestión de Seguridad de la Información, incorporan un conocimiento significativo y muy vigente para que los futuros profesionales en ingeniería informática brinden a sus organizaciones un mayor potencial y habiliten nuevas facultades requeridas para el aseguramiento de las capacidades y aporte de valor de las TI a las empresas, por lo cual es de alta relevancia su estudio e incorporación al currículo formativo.

Para ampliar los conceptos es importante que el estudiante amplíe los conocimientos mediante la lectura de los documentos adjuntos:

- Gestión de riesgos. Una guía de aproximación para el empresario.
- ISO 27001:2013 Guía de implantación para la seguridad de la información.

## Referencias bibliográficas


- Baca Urbina, G. (2016). *Introducción a la Seguridad Informática* (Primera ed.). México: Grupo Editorial Patria. Obtenido de https://elibro.net/es/ereader/usanmarcos/40458
- ISACA®. (2012). *Cobit 5. Procesos Catalizadores.* Estados Unidos: ISACA.
- LaRepublica.Net. (20 de 02 de 2020). *LaRepublica.net*. Obtenido de https://www.larepublica.net/noticia/costa-rica-registro-casi-32-millones-de-intentos-de-ciberataques-en-primeros-tres-meses
- Madrigal Chaves, W. (2019). *SUWA Universidad San Marcos, Repositorio.* Obtenido de http://repositorio.usam.ac.cr/xmlui/
- NQA. (01 de Enero de 2018). *ISO 27001:2013 Guía de implantación para la seguridad de la información.* Obtenido de https://www.nqa.com/certification/standards/iso-27001
- Real Academia Española. (12 de 12 de 2020). *Diccionario de la Lengua Española*. Obtenido de https://dle.rae.es/
- Red Global de Conocimientos en Auditoría y Control Interno. (01 de 01 de 2021). *www.Auditool.com*. Obtenido de https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque
- Romero Castro, M. I., Figueroa Moran, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alcoy - Alicante, España: Editorial Área de Innovación y Desarrollo,S.L. doi:http://dx.doi.org/10.17993/IngyTec.2018.46
- UNICEM. (22 de 12 de 2020). *El Modelo OSI*. Obtenido de http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

San Marcos

**www.usanmarcos.ac.cr**

San José, Costa Rica