Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000

Francisco Javier Valencia Duque

UNIVERSIDAD NACIONAL DE COLOMBIA · 1867 ·

Francisco Javier Valencia Duque

Ingeniero de sistemas de la Universidad Antonio Nariño y Administrador de empresas de la Universidad Nacional de Colombia; Especialista en diseño de sistemas de auditoría de la misma institución; Magíster en Administración de Tecnologías de Información y Comunicaciones del Instituto Tecnológico de Estudios Superiores de Monterrey; Ph. D. en Ingeniería, Industria y Organizaciones de la Universidad Nacional de Colombia.

Es profesor asociado del Departamento de Informática y Computación de la Universidad Nacional de Colombia; Coordinador de la Especialización en Auditoría de Sistemas de la misma universidad y director del grupo de investigación Teoría y Gestión de Tecnologías de Información. Es autor de diversas ponencias y artículos alrededor del gobierno, la gestión, el control, los riesgos y la auditoría TIC y coautor del libro *Técnicas y herramientas de auditoría asistidas por computador* (2016); autor del libro *Aseguramiento y auditoría de tecnologías información orientados a riesgos* (2018) y coautor del libro, *La auditoría continua, una propuesta para el control concomitante y preventivo* (2019).

Cuenta con las certificaciones internacionales CISA, CRISC, COBIT Foundations, Auditor Líder ISO/IEC 27001 e ITIL Foundations v.4.

Ciencias de Gestión

Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000

Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000

Francisco Javier Valencia Duque

UNIVERSIDAD NACIONAL DE COLOMBIA

Bogotá, D. C., 2021

© Universidad Nacional de Colombia - Sede Manizales
Facultad de Administración, Departamento de Informática y Computación
© Francisco Javier Valencia Duque

Primera edición, agosto de 2021
ISBN 978-958-794-601-7 (digital)

Colección Ciencias de Gestión

Edición
Editorial Universidad Nacional de Colombia
direditorial@unal.edu.co
www.editorial.unal.edu.co

Julián Naranjo Guevara
Coordinación editorial

Hernando Sierra
Corrección de estilo

Henry Ramírez Fajardo
Diseño de la colección

Olga Lucía Cardozo Herreño
Diagramación

Creative Commons Atribución-No Comercial-Sin obras derivadas 4.0 Internacional (CC BY-NC-ND 4.0)
https://creativecommons.org/licenses/by-nc-nd/4.0/

Editado en Bogotá D.C., Colombia.

Catalogación en la publicación Universidad Nacional de Colombia

Valencia Duque, Francisco Javier, 1968-
Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000 / Francisco Javier Valencia Duque. -- Primera edición. -- Bogotá : Editorial Universidad Nacional de Colombia ; Manizales : Universidad Nacional de Colombia. Facultad de Administración. Departamento de Informática y Computación, 2021.
1 PDF (189 páginas) : ilustraciones (principalmente a color), diagramas. -- (Colección Ciencias de Gestión).

Incluye referencias bibliográficas e índices temático y onomástico
ISBN 978-958-794-601-7 (e-book)

1. Administración de recursos de información -- Medidas de seguridad 2. Seguridad informática 3. Sistemas de información en administración 4. Sistemas de gestión de bases de datos -- Normas 5. Normas ISO/IEC serie 27000 6. Protección de datos -- Normas 7. Política de información -- Normas I. Título II. Serie

CDD-23 658.478 / 2021

Contenido

Lista de figuras 9
Lista de tablas 11
Presentación 13

Introducción a la seguridad de la información 17
Datos, información, conocimiento e inteligencia 18
Información y activos tecnológicos 20
Concepto de seguridad 28
Lenguaje de contexto de la seguridad de la información 30
Génesis de las amenazas de seguridad en tecnologías de información 34
Tríada de seguridad 37
Sistemas de gestión 41

Marcos de referencia de la seguridad de la información 43
Gobierno y gestión de la seguridad de la información 43
Estándares, marcos de referencia y guías profesionales de gestión de seguridad de la información 44
Certificaciones personales en materia de seguridad de la información 63

Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000 65
La serie ISO/IEC 27000 66
Principales normas de la familia ISO/IEC 27000 para la implementación de un SGSI 68

Propuesta metodológica para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000 77

Fase 1: obtener la aprobación de la dirección para iniciar el proyecto 80

Fase 2. Definir el alcance, los límites y la política del SGSI 85

Fase 3. Realizar el análisis de los requisitos de seguridad de la información 92

Fase 4. Realizar la valoración de riesgos y planificar el tratamiento de riesgos 97

Fase 5. Diseñar el SGSI 113

Aspectos complementarios que se deberían tener en cuenta al implementar un SGSI 117

Ciberseguridad y seguridad en la nube como temas emergentes de la seguridad de la información 121

Ciberseguridad 122

Cloud computing 128

Anexos 141

Referencias 177

Índice temático 183

Índice onomástico 185

Lista de figuras

Figura 1. Ciclo de la información 18
Figura 2. Pirámide informacional 19
Figura 3. Modelo de seguridad en profundidad de Microsoft 21
Figura 4. Arquitectura de seguridad extremo a extremo 22
Figura 5. *Framework* de seguridad de IBM 22
Figura 6. Modelo propuesto de capas tecnológicas 25
Figura 7. Elementos del lenguaje de seguridad 31
Figura 8. Representación genérica de la amenaza de intercepción entre recursos de información 35
Figura 9. Representación genérica de la amenaza de interrupción de recursos de información 36
Figura 10. Representación genérica de la amenaza de modificación de recursos de información 36
Figura 11. Representación genérica de la amenaza de generación de recursos de información 37
Figura 12. Tríada de seguridad de la información 38
Figura 13. Modelo PHVA aplicado a los procesos de un SGSI 42
Figura 14. Categorización de las guías de seguridad de la información 45
Figura 15. Seguridad de la información desde la perspectiva de ITIL 50
Figura 16. Familia de productos de Cobit 5.0 51
Figura 17. Ciclo de vida de seguridad de la información del NIST 55
Figura 18. Modelo BMIS 57
Figura 19. Certificaciones requeridas en seguridad de la información y relacionadas 63
Figura 20. Relaciones entre las diferentes normas de la familia ISO/IEC 27000 67
Figura 21. Principales normas para la implementación de un SGSI 68
Figura 22. Numerales de la norma en función del ciclo Deming 71
Figura 23. Evolución de la norma ISO de controles de seguridad de la información 72
Figura 24. Estructura por dominios de la norma ISO/IEC 27002 73

Figura 25. Estructura de gestión de riesgo propuesta en la ISO/IEC 27005 75
Figura 26. Fases para implementar un SGSI con base en la norma ISO/IEC 27003:2010 78
Figura 27. Ejemplo de plan de proyecto SGSI 83
Figura 28. Ejemplo de información mínima que debería tener una ficha de identificación de activos tecnológicos 94
Figura 29. Estructura general de desglose de activos de información 95
Figura 30. Ejemplos de escenarios de riesgo de tecnologías de información 106
Figura 31. Ejemplos de matrices de riesgos 111
Figura 32. Estructura general de documentación de un SGSI 116
Figura 33. Fases de la gestión de incidentes de seguridad de la información de acuerdo con la ISO/IEC 27035 119
Figura 34. Núcleo del marco de referencia para el mejoramiento de la ciberseguridad de infraestructuras críticas 124
Figura 35. Componentes estructurales del *cloud computing* 129
Figura 36. Capas tecnológicas y su evolución hacia *cloud computing* 134

Lista de tablas

Tabla 1. Clasificación de activos de acuerdo con Magerit 23
Tabla 2. Relación de amenazas genéricas con los objetivos de seguridad de la información 40
Tabla 3. Estándares y buenas prácticas de seguridad de la información utilizadas en Latinoamérica 45
Tabla 4. Certificaciones en la norma 27001 emitidas por la ISO a nivel mundial 47
Tabla 5. Normas de la familia ISO/IEC 27000 48
Tabla 6. Procesos de Cobit 5.0 relacionados directamente con la seguridad de la información 52
Tabla 7. Guías y estándares asociados a la gestión de seguridad de la información del NIST 56
Tabla 8. Preguntas asociadas a las diferentes arquitecturas del modelo SABSA 60
Tabla 9. Principales certificaciones asociados a la seguridad de la información y relacionadas 64
Tabla 10. Estructura de la Norma ISO/IEC 27001:2013 69
Tabla 11. Conceptos nuevos de la ISO/IEC 27001:2013 71
Tabla 12. Fases de implementación de un SGSI y su relación con los numerales de la ISO/IEC 27001:2013 79
Tabla 13. Requisitos de la ISO/IEC 27001 relacionados con la aprobación de la dirección 81
Tabla 14. Requisitos de la ISO/IEC 27001 relacionados con el alcance y la política 85
Tabla 15. Ejemplos de alcance del SGSI 86
Tabla 16. Ejemplo de políticas generales de SGSI 88
Tabla 17. Algunos roles asociados directamente a un SGSI 91
Tabla 18. Requisitos de la ISO/IEC 27001 relacionados con el análisis de requisitos de seguridad 92
Tabla 19. Propuesta de estructura de desglose de clasificación de activos del SGSI 96
Tabla 20. Requisitos de la ISO/IEC 27001 relacionados con la valoración y el tratamiento de riesgo 97

Tabla 21. Modelos de gestión de riesgos para la seguridad de la información 98
Tabla 22. Ejemplo de parámetros de probabilidad de ocurrencia 100
Tabla 23. Parámetros para medir el impacto de la tríada CIA, de acuerdo con el NIST 101
Tabla 24. Parámetros de impacto de un SGSI en el Gobierno argentino 102
Tabla 25. Ejemplo de criterios de aceptabilidad del riesgo 104
Tabla 26. Técnicas/metodologías para llevar a cabo un proceso de identificación de riesgos 105
Tabla 27. Ejemplos de amenazas comunes establecidos en la ISO/IEC 27005 107
Tabla 28. Requisitos de la ISO/IEC 27001 relacionados con el diseño del SGSI 113
Tabla 29. Resumen de la información documentada que debe tener un Sistema de Gestión de Seguridad de la Información basado en la ISO/IEC 27001:2013 114
Tabla 30. Plantilla de ejemplo de declaración de aplicabilidad 116
Tabla 31. Categorías de procesos del marco de referencia de ciberseguridad del NIST 124
Tabla 32. Veinte controles críticos del SANS y su relación con el marco de referencia de ciberseguridad del NIST 125
Tabla 33. Categorías de servicios de cloud *computing* asociados a sus capacidades 131
Tabla 34. Marcos de referencia relacionados con *cloud computing* 133
Tabla 35. Ontología de riesgos de *cloud computing* 136
Tabla 36. Dominios de controles *cloud* del Cloud Security Alliance 138

Presentación

La gestión de la seguridad de la información se ha convertido en un proceso fundamental en las organizaciones modernas, de modo que ha dejado de ser tan solo un tema del área de tecnologías de la información y las comunicaciones (TIC) para convertirse en una prioridad de la alta dirección (IBM, 2011), y justificado en el contexto organizacional, como mínimo, desde tres perspectivas: la importancia de la información como recurso vital para el cumplimiento de los objetivos, la respuesta a las diversas amenazas tecnológicas que ocurren en el día a día y el cumplimiento de las diferentes normas de protección de la información impuestas por los gobiernos.

En relación con la importancia de la información como recurso, esta se considera un activo crítico de la organización a través del cual no solo se toman decisiones, sino que además es un insumo fundamental para la operación diaria de la empresa y la transformación, incluso, de los modelos de negocio; de allí la necesidad e importancia de su adecuada protección.

Desde el punto de vista de las amenazas tecnológicas, en los últimos años se ha incrementado la cantidad y sofisticación de las amenazas a las que están expuestas las organizaciones, de modo que son múltiples los ataques a los sistemas de información y a las diferentes infraestructuras tecnológicas en el que se soporta su funcionamiento, dado que se ha intensificado de manera exponencial en periodos recientes y ha atacado compañías cuyo principal activo es la información. Casos como los ocurridos a Yahoo en 2014, con cerca de 3 000 000 000 de cuentas de usuarios comprometidas, o al gigante de ventas y subastas online, eBay, con el robo de información de cerca de 145 000 000 de usuarios en 2014, o la filtración de información sufrida por Uber en octubre de 2016, cuando se logró filtrar información de cerca de 600 000 conductores del servicio en Estados Unidos, o la reciente exposición de información privada de los perfiles de Facebook de más de 50 000 000 de usuarios sin su consentimiento, por parte de la firma Cambridge Analítica, ponen de manifiesto la importancia que representa la información como activo intangible para los diferentes tipos de organizaciones.

Por último, y no menos importante, el cumplimiento a las diferentes normas impuestas por los Gobiernos a los distintos sectores de la economía para proteger la información. En el caso particular de

Colombia, existen diversas normas aplicables tanto al sector público como privado, entre las que se destacan la obligatoriedad de los proveedores de la factura electrónica en Colombia de contar con una certificación en seguridad de la información bajo la norma ISO/IEC 27001 (Decreto 2242 del 2015, art. 12, numeral 3); los requerimientos del Consejo Nacional de Operación (CNO) en el sector energético para todas las empresas del sector eléctrico del país de incorporar modelos de ciberseguridad (Acuerdo 788 del 2015 del CNO); la Circular 052 de 2007 de la Superintendencia Financiera, en su numeral 3.1.2, en la que se establece la necesidad de gestionar de forma adecuada la seguridad de la información; el Decreto 1078 de 2015 en su título 9, asociado al gobierno en línea, en el que se exige a las entidades públicas implementar un modelo de seguridad y privacidad de la información; la norma de protección de datos personales y, en general, otras normas que obligan a las organizaciones a implementar mecanismos de seguridad de la información.

Todo lo anterior lleva a la necesidad de plantear propuestas que conciban la seguridad de la información con una visión holística y sistemática que permita implementar un adecuado sistema de gestión de la seguridad de la información a la luz de las mejores prácticas internacionales, que trascienda la instantaneidad de las medidas de control correctivas que se toman tradicionalmente en las organizaciones con el fin de responder a las amenazas que se presentan, pero, además, para que se convierta en una práctica común en la organización y, como tal, pueda ser medida y gestionada de forma permanente, si se tiene en cuenta que, por lo general, la seguridad de la información se inicia como un proyecto, pero termina como un proceso que se debe gestionar de forma permanente. Este es el objetivo del presente texto, con el cual se pretende aportar a la comunidad académica y profesional con una estructura conceptual y metodológica que articule teorías, normas, metodologías y prácticas que permitan implementar un sistema de gestión de seguridad de la información de acuerdo con el principal referente a nivel internacional: la familia de normas ISO/IEC 27000.

Para lograr el propósito previsto, se ha construido un documento compuesto de cinco capítulos. El primero orientado a presentar las bases de la seguridad de la información, como preámbulo al conocimiento detallado de las normas internacionales relacionadas, en el cual no solo se incorporan las bases conceptuales de la seguridad de la información, sino que también se plantean las diferencias que existen entre la seguridad de la información, la seguridad informática

y la ciberseguridad, y se realiza una serie de propuestas que hacen parte estructural de la implementación de un sistema de gestión de seguridad de la información (en adelante SGSI).

A partir de los conceptos, se desarrollan en el segundo capítulo los principales marcos de seguridad de la información existentes a nivel internacional, no obstante ser la familia de la norma ISO/IEC 27000 el principal referente en la materia, ratificado por la cantidad de certificaciones emitidas por la ISO.

Una descripción de las normas de seguridad de la información de la ISO/IEC 27000 se presenta en el tercer capítulo, con énfasis en cuatro de las principales normas que se utilizan en la implementación de un sistema de gestión de seguridad de la información y cuya metodología, basada en la ISO/IEC 27003, se desarrolla en el cuarto capítulo, con miras a aportar aspectos prácticos a partir de experiencias del autor y de otros autores. Sin embargo, no se pueden desconocer dentro de los aspectos de seguridad de la información dos temas omnipresentes en cualquier estrategia empresarial y que se encuentran asociados de forma directa a la seguridad de la información, como lo son la ciberseguridad y la seguridad en la *cloud computing*, temas que son objeto de análisis en el quinto capítulo.

Introducción a la seguridad de la información

Este primer capítulo presenta las bases de la seguridad de la información como preámbulo al conocimiento detallado de las normas internacionales relacionadas y a la metodología de implementación de un SGSI, lo que le permitirá al lector identificar y reconocer la importancia de la seguridad de la información en el entorno empresarial actual.

Las tecnologías de la información y las comunicaciones son recursos vitales para la productividad y competitividad de las organizaciones, sin embargo, como cualquier recurso, es vulnerable a múltiples amenazas que se pueden materializar en riesgos, con consecuencias en términos de pérdida de datos, interrupción de servicios, pérdidas financieras, daños a la reputación e, incluso, pérdidas humanas.

Amenazas tan comunes como, por ejemplo, los virus, los fallos de *software*, programas espía, troyanos, los robos de equipos y el *spam*, hasta aspectos tan sofisticados como las amenazas persistentes avanzadas (APT, por sus siglas en inglés para *advanced persistent threat*), o los ataques día cero (en inglés *zero-day attack*), requieren la implementación de controles que puedan ser gestionados a través de un adecuado enfoque de seguridad de la información.

La seguridad de la información es una disciplina asociada, tradicionalmente, a la gestión de tecnologías de la información

y las comunicaciones, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. La ISO/IEC 27000 la define como la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sin embargo, antes de realizar nuestra inmersión en el mundo de la seguridad de la información, es necesario y pertinente proporcionar las bases conceptuales sobre las que se construyen muchas de las estructuras que soportan esta disciplina. Para esto, a continuación, se plantean diversos conceptos que son indispensables en el propósito de comprender esta importante disciplina técnico-organizacional.

Datos, información, conocimiento e inteligencia

Tal como se puede observar en la figura 1, el ciclo de información de una empresa nace a partir de la generación y el procesamiento de los datos, los cuales se transforman en información y conocimiento (de modo que crean valor para la empresa), a través de lo cual se toman decisiones que permiten el funcionamiento de la organización en sus diferentes niveles (operativo, táctico y estratégico).

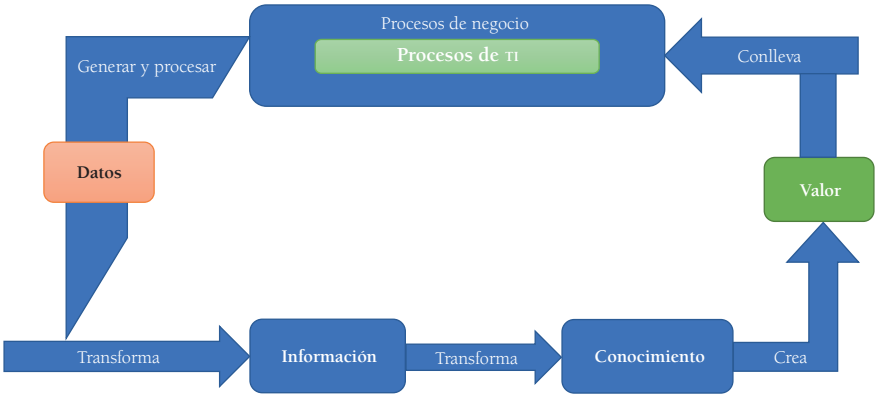

Figura 1. Ciclo de la información.
Fuente: elaboración propia a partir de ISACA (2012c).

Desde la perspectiva de la pirámide informacional, tal como se puede apreciar en la figura 2, el valor que genera conocimiento a la organización se denomina "inteligencia", de modo que existe una relación inversamente proporcional entre los datos y la inteligencia, al ser esta última más difícil de conseguir, debido a la complejidad que representa su obtención.

Tradicionalmente, se afirma que las organizaciones se encuentran inundadas por datos, los cuales, en ocasiones, no se aprovechan de forma adecuada como insumo para la generación de información que sirva de base para convertirla en conocimiento y, a partir de allí, incorporarla en sus diferentes estrategias organizacionales, para garantizar ciertos niveles de competitividad en el mercado.

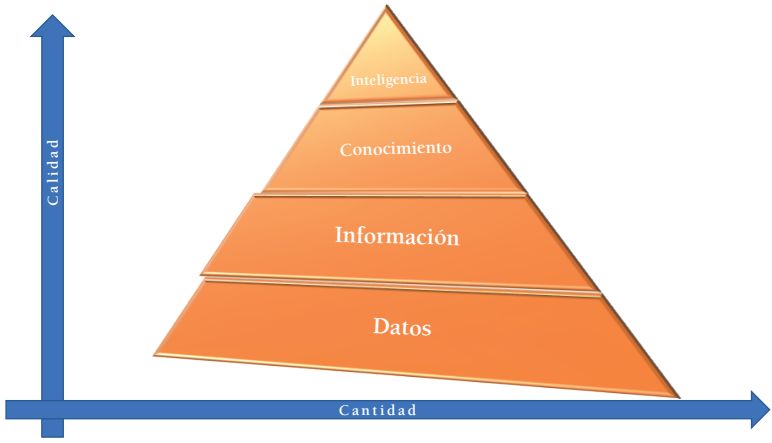

Figura 2. Pirámide informacional.
Fuente: elaboración propia a partir de Newton (2019).

Un dato es un elemento que carece de significado por sí solo. Sin embargo, se convierte en un elemento fundamental solo o en conjunto con otros datos, cuando lo situamos en un contexto, de forma tal que tiene significado en el tiempo y lugar indicado, convirtiéndose en información. Esta, una vez se analiza, discrimina, valida y sintetiza con la experiencia de la persona o las personas que la van a utilizar, se convierte en conocimiento, el cual, aprovechado de manera oportuna, permite tomar de decisiones para generar ventajas competitivas convirtiéndola así en inteligencia.

Si se provee un adecuado aseguramiento de las tecnologías de la información y las comunicaciones, como principal medio para la gestión de los

datos y la información, se sientan las bases que permitirán contar con organizaciones más inteligentes, desde la perspectiva de la pirámide informacional.

A partir de la importancia de los datos, la información, el conocimiento y la inteligencia en el ámbito organizacional, se han acuñado términos como, por ejemplo, *economía de los datos*, para referirse no solo a la importancia de estos dentro de la competitividad organizacional, sino a la forma en la que se pueden generar nuevos modelos de negocios a partir del uso de los datos y las diferentes tecnologías que existen a su alrededor.

Información y activos tecnológicos

La información es la base sobre la que se genera conocimiento para la toma de decisiones en los diferentes niveles de la organización. De allí que el objetivo de proveer niveles de aseguramiento de la información se considere un aspecto crítico de la vida organizacional tanto a nivel estratégico como táctico y operativo.

El proceso de gestión de la información puede ser llevado a cabo de forma manual o con el uso de las TIC, dado que es esta última la forma más generalizada para su tratamiento, lo que nos lleva a utilizar los diferentes activos tecnológicos para garantizar eficacia y eficiencia en el tratamiento de la información.

Las organizaciones cuentan con una gran cantidad y variedad de activos tecnológicos. Tratar de establecerlos y clasificarlos puede ser una tarea extensa, sobre todo, en aquellas grandes organizaciones, ya que es probable que existan *terabytes* de datos electrónicos, almacenes de documentos y miles de personas y dispositivos que hacen parte de los activos tecnológicos (Isaca, 2012e), lo cual requiere de esquemas conceptuales que proporcionen una visión holística de todos los activos tecnológicos de una organización. Entre las propuestas que existen con relación a este requerimiento, se encuentran diversos modelos; se destacan los propuestos por Microsoft, la Unión Internacional de Telecomunicaciones, IBM, la ISO/IEC 27005, Magerit y la norma UNE 71504:2008.

Modelo de clasificación de activos tecnológicos de Microsoft

Microsoft ha planteado un concepto denominado *seguridad en profundidad* o *defensa en profundidad*, tal como se puede apreciar en la figura 3, cuyo

principio se basa en una estrategia militar que tiene como objetivo demorar el avance del oponente al mantener múltiples capas de defensa y no solo una fuerte línea defensiva.

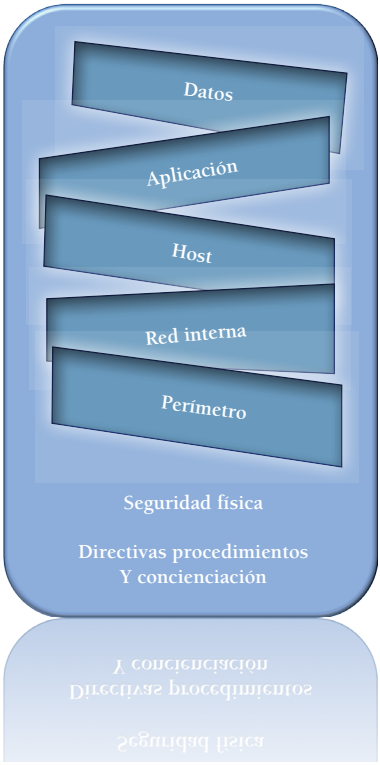

Figura 3. Modelo de seguridad en profundidad de Microsoft.
Fuente: Montenegro (2015).

Modelo de clasificación de activos tecnológicos de la Unión Internacional de Telecomunicaciones (ITU)

Por su parte, la ITU ha planteado un modelo denominado arquitectura de seguridad para sistemas de comunicaciones extremo a extremo, tal como se puede observar en la figura 4, desarrollado a través de la recomendación UIT-T X.805, en el cual se definen los elementos de seguridad generales de la arquitectura que son necesarios para garantizar la seguridad extremo a extremo.

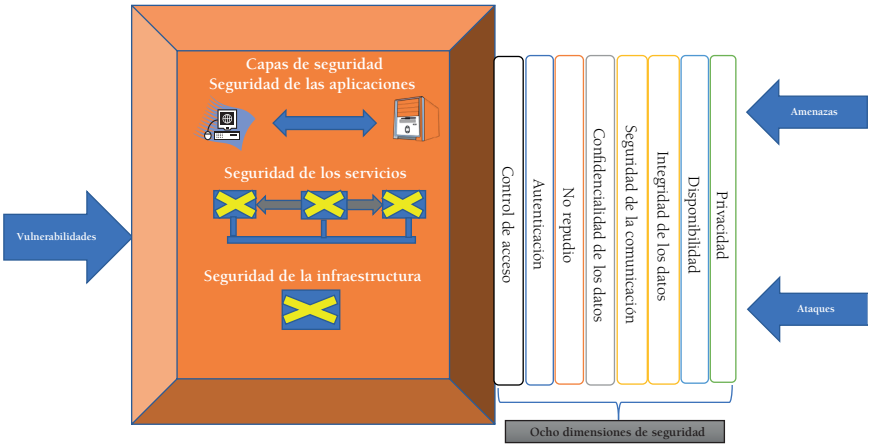

Figura 4. Arquitectura de seguridad extremo a extremo.
Fuente: elaboración propia a partir de ITU (2008).

Modelo de clasificación de activos tecnológicos de IBM

De igual forma, IBM ha establecido su propio *framework* de seguridad, a partir del cual ha planteado una estructura de activos tecnológicos, tal como se puede observar en la figura 5.

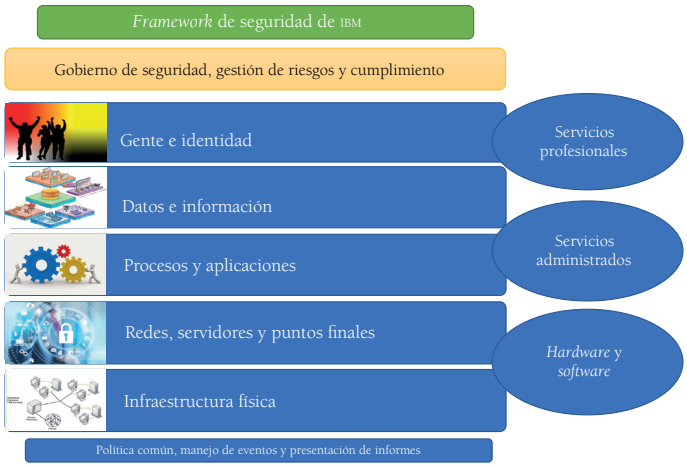

Figura 5. *Framework* de seguridad de IBM.
Fuente: elaboración propia a partir de Buecker, Borrett, Lorenz y Powers (2010).

Modelo de clasificación de activos tecnológicos de la norma ISO/IEC 27005

La norma ISO/IEC 27005 diferencia dos tipos de activos: activos primarios y activos de soporte. Los activos primarios son los procesos de negocio y de la información, mientras que los activos de soporte son aquellos de los cuales dependen los activos primarios y se clasifican en *hardware*, *software*, redes, personal, ubicación y estructura de la organización.

Modelo de clasificación de activos tecnológicos de Magerit

La metodología Magerit (metodología de análisis y gestión de riesgos de los sistemas de información) establece una clasificación basada en capas tecnológicas interdependientes, teniendo presente que existen dependencias entre activos, de modo que se forman árboles o grafos de dependencia en los que la seguridad de los activos que se encuentran más arriba en la estructura o superiores dependen de los activos ubicados más abajo o inferiores (Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica, 2012). Acorde con lo anterior, los activos propuestos por Magerit se clasifican en función del nivel de dependencia, tal como se puede observar en la tabla 1.

Tabla 1. Clasificación de activos de acuerdo con Magerit

Capa	Activos
Activos esenciales	Información que se maneja
	Servicios prestados
Servicios internos	Que estructuran ordenadamente el sistema de información
Equipamiento informático	Aplicaciones (*software*)
	Equipos informáticos (*hardware*)
	Comunicaciones
	Soportes de información (discos, cintas, entre otros)
El entorno	Activos que se precisan para garantizar las siguientes capas. Dentro de estos se encuentran equipamiento y suministro tales como energía y climatización, entre otros.

Continúa en la siguiente página ►

Capa	Activos
Servicios subcontratados a terceros	Servicios de tecnologías de información y comunicaciones tercerizados.
Instalaciones físicas	Instalaciones en las que se encuentran ubicados los diferentes elementos de TIC.
El personal	Usuarios, operadores, desarrolladores y administradores.

Fuente: estructurado a partir de Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica (2012).

Modelo de clasificación de activos tecnológicos de acuerdo con la norma UNE 71504:2008

De acuerdo con lo establecido en la cláusula 5.2.1. de la norma española UNE 71504:2008-*Metodología de análisis y gestión de riesgos para los sistemas de información*, las clasificaciones de los activos tecnológicos se pueden dividir en seis capas:

- Capa 1: servicios y procesos;
- Capa 2: información;
- Capa 3: equipamiento lógico (*software*);
- Capa 4: equipamiento físico (*hardware*, comunicaciones, etc.);
- Capa 5: instalaciones;
- Capa 6: personal.

Cuando el número de activos por cada capa es elevado se puede acudir a su agrupación por roles o funciones, considerando un solo activo como representante de todos los que son equivalentes a él en cuanto a riesgos se refiere (AENOR, 2008).

Propuesta de activos tecnológicos multinivel

A partir de la revisión de los modelos presentados se propone a continuación un modelo que denominaremos "seguridad multinivel", tal como se puede apreciar en la figura 6, teniendo en cuenta doce capas tecnológicas interdependientes y organizadas de forma tal que, en caso de falla de alguna de ellas, puede generar un efecto domino sobre las demás, lo que lleva a contemplar la seguridad integral con un aseguramiento de cada capa.

Es importante tener en cuenta que cada una de las doce capas tiene un nivel de dependencia de las capas inferiores y, en caso de verse amenazada alguna de las capas de las cuales dependen, podrían estar amenazadas las demás capas. De igual forma, es necesario denotar que el talento humano (personas) que se menciona en los diferentes modelos no se incorpora como una capa tecnológica, debido a que es un recurso transversal que está presente en todas las capas y sin el cual no funcionaría ningún modelo.

1	Procesos de negocio
2	Servicios de TI
3	Datos / información / conocimiento
4	Sistemas de información transaccionales
5	Sistemas de información soporte
6	Motores de bases de datos
7	Sistemas operativos
8	PC de escritorio e impresoras
9	Servidores (físicos, virtuales y en la nube)
10	Centro de redes y cableado
11	Centros de cómputo
12	Energía

Figura 6. Modelo propuesto de capas tecnológicas.
Fuente: Valencia Duque, Marulanda y López Trujillo (2015).

- *Procesos de negocio*. Los procesos de negocio son todas aquellas actividades desarrolladas por la organización para cumplir con sus objetivos. Tradicionalmente, estas se encuentran asociadas a diferentes categorías como, por ejemplo, procedimientos, los cuales en su conjunto conforman un proceso y, a su vez, en su conjunto, se denominan macroprocesos.

  Todas las organizaciones cuentan, por lo general, con un mapa de procesos, agrupados en estratégicos, misionales y de apoyo (o términos similares), los cuales reflejan la forma en la que opera la organización y el nivel de interrelación que existe entre cada uno de ellos. Algunos ejemplos de procesos son cartera, nómina, presupuesto y ventas.

- *Servicios de TI*. De acuerdo con la definición planteada por el marco de referencia ITIL (Information Technology Infrastructure Library), un servicio de TI es un medio por el cual se entrega valor a los clientes (usuarios) y se les facilita un resultado deseado sin la necesidad de que estos asuman los costos y los riesgos específicos (ITSMF International, 2007). Los servicios se construyen a partir de la combinación de la infraestructura tecnológica y los procesos de gestión y operación de las TIC.

  Algunos ejemplos de servicios son correo electrónico, servicio de *backups*, servicio de procesamiento de nómina, servicio de soporte y mantenimiento y servicio de capacitación.
- *Datos, información, conocimiento*. Se dio a conocer en apartados anteriores al referirnos a la pirámide informacional.
- *Sistemas de información transaccionales*. Son todos aquellos sistemas de información que utilizan la organización para automatizar sus procesos de negocio. Algunos ejemplos son: ERP (*enterprise resource planning*), CRM (*customer relation management*), sistemas de información de nómina y sistemas de información de ventas.
- *Sistemas de información de soporte*. Son todas aquellas herramientas de *software* que apoyan el negocio y la función de tecnologías de información para cumplir diferentes funciones operacionales. Se diferencian de los sistemas de información transaccionales en los que estas herramientas no soportan un proceso de negocio en especial. Dentro de esta categoría podemos encontrar herramientas ofimáticas, *software* antivirus, compiladores para desarrollo de *software*, herramientas RAD (*rapid application developer*), *software* utilitario para apoyar diferentes funciones de tecnologías de información.
- *Motores de bases de datos*. Equivale a lo que en el mercado se conoce como sistemas gestores de bases de datos (SGBD), o *database management system* (DBMS), los cuales permiten añadir, borrar, modificar, almacenar y analizar los datos que tiene una organización y que se gestionan tradicionalmente a través de sistemas de información. Entre los principales motores de bases de datos se encuentran Oracle, SQL Server, Postgresql y Mysql.
- *Sistemas operativos*. Es el programa que se encarga de administrar los servicios de *hardware* de un computador personal, de un servidor o de cualquier dispositivo que requiere de una interfaz entre los recursos de *hardware* y las diferentes funcionalidades de uno o

varios sistemas de información. Dentro de esta categoría existen diferentes tipologías de sistemas operativos, desde sistemas operativos para computadores o dispositivos personales de un solo usuario y monotarea, hasta sistemas operativos para servidores que atienden diferentes tareas y diferentes usuarios. Algunos ejemplos de sistemas operativos son Windows (en sus diferentes versiones), Android, OS2 de IBM, Unix y Linux.

- *PC de escritorio y periféricos*. En el caso de los computadores personales (PC) son los dispositivos que, tradicionalmente, tiene cualquier usuario en su escritorio y a través de los cuales pueden acceder a los diferentes sistemas de información de la organización, y que, por lo general, se encuentran acompañados de periféricos tales como impresoras, escáneres y discos externos, entre otros.
- *Servidores*. Los servidores son computadores dotados de ciertas características especiales (mayor capacidad de procesamiento, multitarea, mayores capacidades de almacenamiento, mayor capacidad en memoria) que se encuentran al servicio de otros dispositivos y, tradicionalmente, son dedicados a tareas especializadas, para lo cual toman nombres de acuerdo con la actividad asignada: servidor de aplicaciones, servidor de archivos, servidor de correo, servidor de impresoras y servidor de base de datos.

  Dentro de esta categoría se encuentran tres tipos genéricos de servidores: servidores físicos, servidores virtuales (una o varias particiones en un servidor para dedicarlo a prestar varios servicios) y servidores en la nube.
- *Centros de redes y cableado*. Comprende toda la infraestructura de red con la que cuenta una organización y se encuentra distribuida en sus diferentes dependencias. Dentro de esta categoría encontramos centros de cableado, equipos de red activos y pasivos, así como todo el tendido de red que interconectan los diferentes dispositivos que tiene la organización.
- *Centros de cómputo*. También llamado centro de procesamiento de datos, centro de datos o *data center*, es aquel sitio o sitios donde tradicionalmente las organizaciones concentran los dispositivos de cómputo más críticos a través de los cuales se centraliza el procesamiento y el almacenamiento de la información considerada más crítica para el negocio.

- *Sistemas de energía*. Son todos aquellos servicios y dispositivos que permiten que un dispositivo físico de procesamiento de información pueda operar, si se tiene en cuenta que casi en su totalidad hoy dependen de la energía eléctrica. Dentro de esta categoría también se encuentran los dispositivos que permiten generar energía alterna y su adecuado resguardo, como es el caso de los bancos de baterías y las UPS.

Esta capa tecnológica es una de las capas más importantes, por no decir la más importante de la infraestructura tecnológica de una organización, debido a que es la que permite a las demás cumplir su función.

Concepto de seguridad

Las organizaciones están sometidas de forma permanente a amenazas de diversa índole, ya sean de origen natural, tecnológico o social, que pueden afectar sus objetivos de negocio. La probabilidad de que estas amenazas se materialicen con sus respectivas consecuencias es lo que se denomina tradicionalmente "riesgo".

A fin de enfrentar los diferentes riesgos a los que está expuesta una organización se ha desarrollado el concepto de *seguridad*, definida como un proceso a través del cual las organizaciones buscan permanentemente contar con niveles aceptables de riesgo.

El nivel de aceptabilidad de riesgo es una variable relativa, definida por las mismas organizaciones, las cuales, ante la imposibilidad de eliminar los riesgos, deben plantear alternativas para realizar un manejo adecuado de ellos, bien sea al controlarlos, minimizarlos o modificarlos. Acorde con lo anterior, no existe seguridad absoluta.

La seguridad, en función de las TIC, es la capacidad de estas de resistir, con un determinado nivel de confianza, los accidentes o las acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, así como de los servicios que proveen o hacen accesible las tecnologías de la información y las comunicaciones (Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica, 2012).

La ISO/IEC 27000, al referirse a la seguridad de la información, la define como la preservación de la confidencialidad, integridad y disponibilidad de

la información, integrando adicionalmente otras propiedades tales como la autenticidad, la responsabilidad, el no repudio y la confiabilidad (ISO/IEC, 2018a). Estos términos se explican con mayor nivel de detalle más adelante.

Para llevar a cabo un adecuado proceso de seguridad de la información en una organización se requiere contar con un enfoque que permita proveer una visión sistémica que garantiza una mejora continua que sea medible, lo cual se puede lograr a través de un sistema de gestión, en el propósito de mantener niveles aceptables de riesgo y aportar al cumplimiento de los objetivos organizacionales.

Diferencias entre seguridad informática, seguridad de la información y ciberseguridad

La diferencia entre los términos *seguridad informática*, *seguridad de la información* y *ciberseguridad* se da en función del tipo de recursos sobre los que actúa. Mientras la primera se enfoca en la tecnología propiamente dicha, en las infraestructuras tecnológicas que sirven para la gestión de la información en una organización, la segunda se relaciona con la información, como activo estratégico de la organización, mientras que la ciberseguridad se enfoca en la información digital y en los sistemas interconectados que la procesan, almacenan y transmiten (Joyanes Aguilar, 2017).

El concepto de seguridad es el mismo, sin embargo, la seguridad informática actúa sobre todos los elementos técnicos que hacen parte de las TIC, mientras la seguridad de la información lo hace sobre uno de los recursos más importante para la toma de decisiones empresariales como lo es la información.

Hasta antes de que surgieran de forma masiva las TIC, el concepto que podría predominar era el de seguridad de la información. Sin embargo, con el advenimiento de las TIC y su nivel de dependencia por parte de las organizaciones, y más aún, su nivel de dependencia para un adecuado tratamiento de la información, se ha pasado de pensar tan solo en la seguridad informática como fin, a pensar en su correcta implementación como medio dirigido a obtener un adecuado sistema de gestión de seguridad de la información que permita garantizar niveles también adecuados de protección de la información empresarial como recurso vital para la toma de decisiones empresariales, además del diseño de estrategias competitivas que diferencien a una organización de otra.

Desde esta perspectiva, lo que persigue un sistema de gestión de seguridad de la información es proteger la información como recurso valioso de la organización, para lo cual debe proteger los diferentes medios a través de los que se genera, almacena, procesa, transmite, circula y transforma la información en un recurso útil para los negocios. Estos medios son las tecnologías de información y comunicaciones en su conjunto.

De acuerdo con Cano (2011), la seguridad informática o seguridad de TI es la función táctica y operacional de la seguridad que se encarga de las implementaciones técnicas de la protección de la información, de las tecnologías antivirus, las *firewalls*, los sistemas de detección de intrusos (IDS, por sus siglas en inglés) y el manejo de incidentes, mientras que la seguridad de la información es la disciplina en el arte y la ciencia de la protección, de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y los esquemas normativos que exigen niveles de aseguramiento de procesos y tecnologías con miras a elevar el nivel de confianza en la creación, el uso, el almacenamiento, la transmisión, la recuperación y la disposición final de la información.

▶ Lenguaje de contexto de la seguridad de la información

En general, un modelo es una simplificación de la realidad que permite interrelacionar una serie de características y representarlas mediante un lenguaje común, entendible para todos (Vargas y Parra, 2002). Ese lenguaje comprende términos y conceptos que deben ser claramente identificados a fin de entender el modelo que se quiere construir. En este caso en particular, existe una serie de términos que tradicionalmente se encuentran asociados a la seguridad de la información.

Entre los aspectos clave de la seguridad de la información, los procesos de gestión de riesgos son el eje central que integra y vuelve operativos los diferentes elementos que hacen parte de un modelo de seguridad, y como tal comparten muchos de sus conceptos. En este sentido, los modelos de gestión de riesgos son la base sobre la que se construye la seguridad de la información de una organización.

La figura 7 interrelaciona una serie de conceptos asociados a la seguridad de la información que permiten delimitar su lenguaje y ponerlo en contexto con aspectos organizacionales y técnicos. De allí que su interpretación se relaciona a continuación.

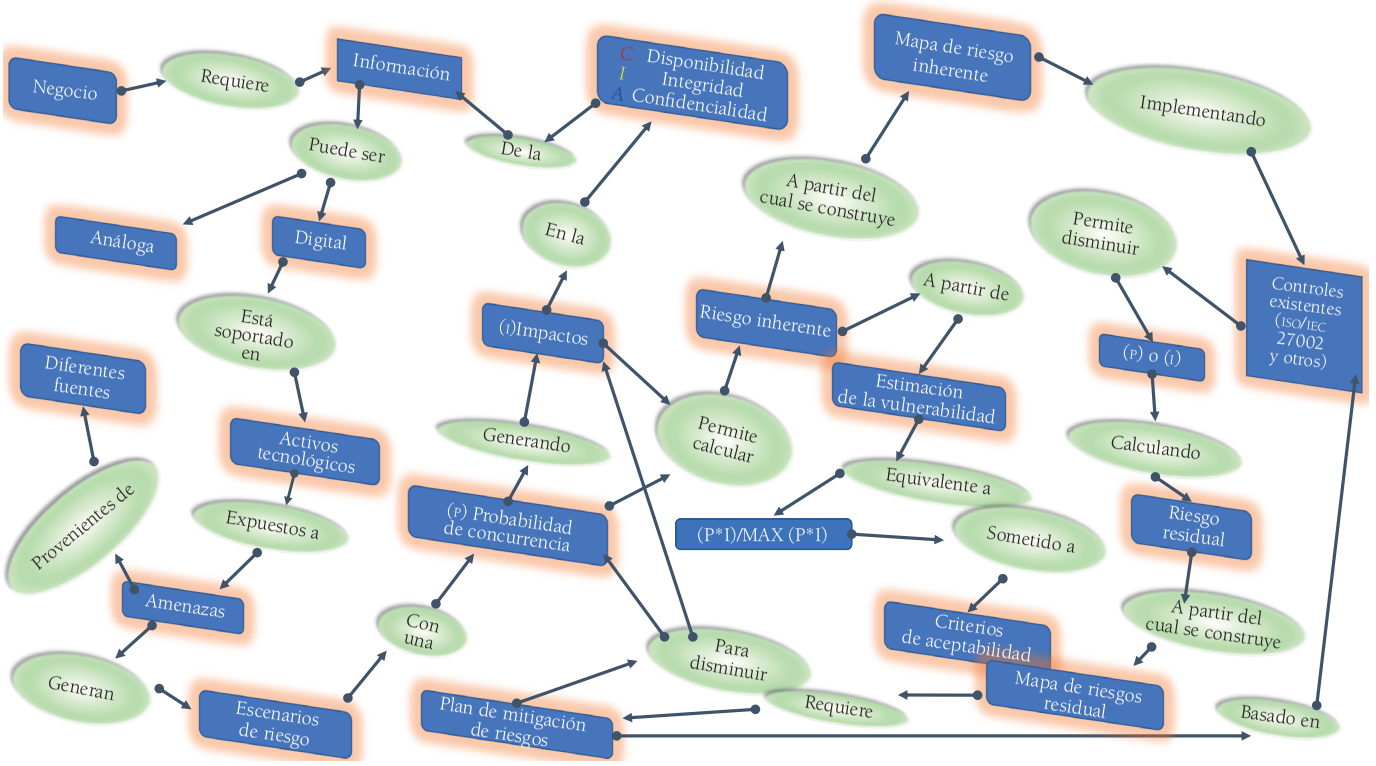

Figura 7. Elementos del lenguaje de seguridad.

Fuente: elaboración propia.

*Todo *negocio* requiere *información* para la toma de decisiones, la cual se puede presentar de forma *análoga* o *digital*, siendo esta última la más generalizada en el mundo de los negocios En tal sentido, la gestión de la información que requiere un negocio esta soportada en *activos tecnológicos*, los cuales se encuentran expuestos a diversas *amenazas*, definidas por lo general como eventos adversos que pueden afectar una organización y que provienen de *diferentes fuentes*. La exposición de un activo tecnológico a una amenaza configura lo que se denomina un *escenario de riesgo*, el cual es evaluado a través de dos variables, la *probabilidad de ocurrencia y el impacto que puede llegar a generar en principio en la confidencialidad, integridad y disponibilidad* de la información. Ambas variables permiten establecer el *riesgo inherente* cuya representación cuantitativa se construye a partir de la *estimación de la vulnerabilidad*, cuyo resultado se somete a los *criterios de aceptabilidad* de riesgos (apetito de riesgo) definido por la misma organización. Una vez calculado el riesgo inherente, se construye el *mapa de riesgos inherentes*, que es la forma tradicional como se representa el conjunto de riesgos de una organización para mostrar su criticidad (a través de colores). Un riesgo inherente es aquel riesgo que se calcula y evalúa sin tener en cuenta los *controles* existentes en la organización, los cuales requieren ser identificados en el marco de lo establecido en la norma ISO/IEC 27002, entre otras normas, para poder calcular el *riesgo residual*, equivalente al efecto que tienen los controles sobre la disminución de la probabilidad o el impacto y que permite construir el *mapa de riesgos residual*, que sirve de referente para elaborar un plan de mejoramiento denominado *Plan de mitigación de riesgos*, que tradicionalmente involucra diferentes estrategias para avanzar en la construcción de niveles aceptables de seguridad.

Lenguaje formal de un SGSI

El lenguaje formal de un sistema de gestión de seguridad de la información está contenido en la norma ISO/IEC 27000:2018, denominada *Tecnología de información-técnicas de seguridad-sistemas de gestión de seguridad de la información-marco general y vocabulario,* en la cual se delimitan los términos y las definiciones que se utilizan en las diferentes normas de la familia ISO/IEC 27000.

A continuación, se presentan los principales términos y definiciones contenidos en esta norma.

- Aceptación del riesgo: decisión informada para tomar un riesgo en particular.
- Análisis de riesgos: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- Confidencialidad: propiedad de que la información no esté disponible o revelada a personas, entidades o procesos no autorizados.
- Consecuencias (impacto): resultado de un evento que afecte los objetivos.
- Control: medida que modifica el riesgo.
- Criterios de riesgo: términos de referencia contra los que se evalúa la importancia del riesgo.
- Disponibilidad: propiedad de ser accesible y utilizable bajo la demanda de una entidad autorizada.
- Eventos de seguridad de la información: ocurrencia identificada de un sistema, servicio o red que indica un posible incumplimiento de la política de seguridad de la información, la falla de controles o una situación desconocida previamente que puede ser relevante para la seguridad.
- Evaluación de riesgos: proceso general de identificación del riesgo, análisis de riesgos y valoración del riesgo.
- Gobierno de seguridad de la información: sistema por el cual las actividades de seguridad de la información se dirigen y controlan.
- Identificación del riesgo: proceso de búsqueda, reconocimiento y descripción del riesgo.
- Integridad: propiedad de exactitud y completitud.
- Nivel de riesgo: magnitud de un riesgo, expresado en términos de la combinación de la consecuencia (impacto) y su probabilidad.
- Objetivo de control: declaración que describe lo que se quiere lograr como resultado de la implementación de controles.
- Política: intenciones y directrices de una organización expresadas formalmente por la alta dirección.
- Procesos: conjunto de actividades interrelacionadas e interactuantes, las cuales transforman elementos de entrada en resultados.
- Probabilidad: posibilidad de que algo suceda.

- Proyecto SGSI: actividades estructuras realizadas por una organización con el fin de implementar un SGSI.
- Requerimiento: necesidad o expectativa establecida, por lo general implícita u obligatoria.
- Riesgo: efecto de la incertidumbre sobre los objetivos.
- Riesgo residual: riesgo restante después del tratamiento del riesgo.
- Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.
- Sistema de gestión: conjunto de elementos interrelacionados e interactuantes de una organización dirigidos a establecer políticas y objetivos, así como los procesos para lograr dichos objetivos.
- Sistemas de información: aplicaciones, servicios, activos de tecnología de información u otros componentes de manejo de información.
- Tratamiento del riesgo: proceso para modificar el riesgo.
- Valoración de riesgos: proceso de comparación de los resultados de análisis de riesgos con los criterios de riesgo que permiten determinar si el riesgo y/o su magnitud es aceptable o tolerable.
- Vulnerabilidad: debilidad de un activo o de un control que puede ser explotado por uno o más amenazas.

Génesis de las amenazas de seguridad en tecnologías de información

Diversos autores clasifican de forma genérica los recursos tecnológicos en *hardware*, *software* y datos, mientras que las amenazas hacia estos recursos las asocian de forma genérica a los eventos relacionados con la intercepción, interrupción, modificación y fabricación.

Estos eventos son la génesis de muchas de las amenazas pasadas, presentes y futuras que afectan, en general, los recursos relacionados con la información.

- *Intercepción/interceptación*. Consiste en el acceso a los recursos tecnológicos por parte de personas, procesos o recursos tecnológicos no autorizados que usan privilegios no adquiridos. Tal como se puede observar en la figura 8, tanto el emisor como el receptor pueden ser recursos tecnológicos, lo que incluye a las personas; de igual forma, la intercepción se puede realizar con estos mismos recursos.

La intercepción está relacionada de manera directa con la confidencialidad de la información.

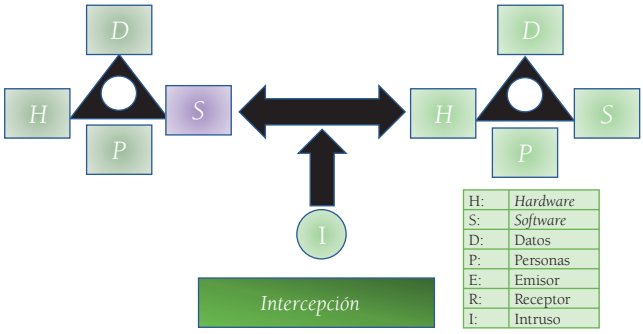

Figura 8. Representación genérica de la amenaza de intercepción entre recursos de información.
Fuente: elaboración propia.

Entre los ejemplos de este tipo de amenaza se encuentran la interceptación de datos, la interceptación de comunicaciones (escucha en líneas de comunicación [chuzadas]), y el robo de datos a través de su interceptación. El caso más sonado en Colombia de este tipo de amenaza es el caso Andrómeda.

- *Interrupción*. Consiste en que un recurso tecnológico se destruye, modifica o inutiliza total o parcialmente para interrumpir el cumplimiento de su objetivo, tal como se esquematiza en la figura 9. Es un ataque contra la disponibilidad de información. Ejemplos de este tipo de ataque son la destrucción de un elemento *hardware*, cortar una línea de comunicación, gusanos que se activan y transmiten a través de la red y tienen como finalidad su multiplicación hasta agotar la RAM o espacio en disco duro, dejando por fuera los recursos.
- *Modificación*. Este tipo de amenaza puede ser considerada una derivación de la interceptación, debido a que el intruso debe inicialmente tener acceso al recurso (interceptación) para proceder a modificarlo. No obstante, también se puede presentar por personas que no son considerados intrusos por tener autorización para acceder a los recursos y, a partir de su acceso, realizar modificaciones. Este tipo de amenaza afecta la integridad de los datos.

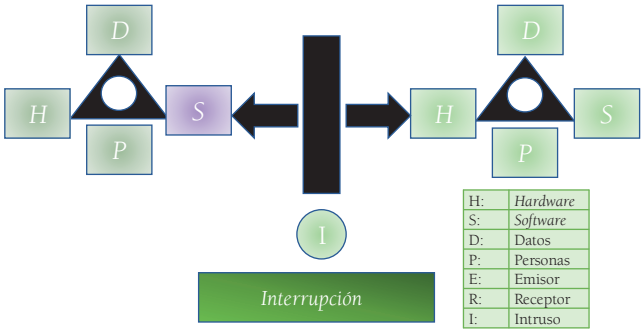

Figura 9. Representación genérica de la amenaza de interrupción de recursos de información.
Fuente: elaboración propia.

La figura 10 presenta un esquema genérico de modificación de recursos de información.

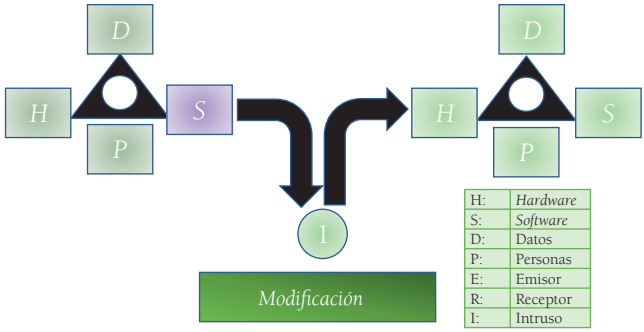

Figura 10. Representación genérica de la amenaza de modificación de recursos de información.
Fuente: elaboración propia.

Entre los ejemplos de este tipo de amenazas se encuentran los virus diseñados con el propósito de modificar o destruir datos, acceso a bases de datos para modificar registros o cambios no autorizados en el código fuente.

- *Generación*. Es un ataque contra la autenticidad y tiene que ver con la inserción de objetos no autorizados como parte de un recurso tecnológico, tal como se puede observar en la figura 11. Ejemplos de este tipo de amenazas son la introducción de mensajes falsos en

la red, añadir registros no autorizados en bases de datos y la incorporación de servidores falsos dentro del ambiente informático.

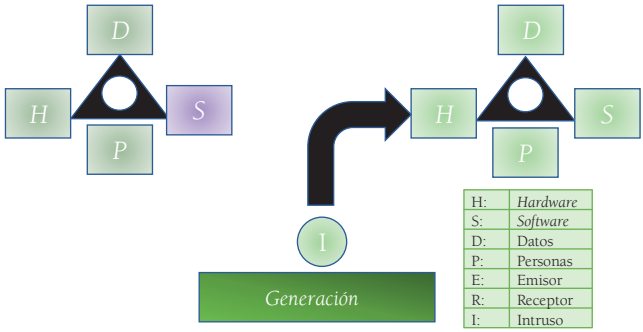

Figura 11. Representación genérica de la amenaza de generación de recursos de información.
Fuente: elaboración propia.

▶ Tríada de seguridad

Tradicionalmente, la seguridad de la información se asocia a la tríada confidencialidad, integridad y disponibilidad (conocida como CIA, sigla en inglés correspondiente a los términos *confidentiality*, *integrity* y *avalaible*), y, de acuerdo con la comunidad académica y profesional, son los objetivos a los que debe apuntar cualquier sistema de gestión de seguridad de la información (véase la figura 12).

Sin embargo, existen otros atributos complementarios de la seguridad de la información, tales como la autenticidad, la responsabilidad, el no repudio y la confiabilidad (ISO/IEC, 2014a).

Confidencialidad

La confidencialidad es un término asociado con el acceso y el uso de la información solo por parte de quienes se encuentran autorizados y tienen la necesidad de conocerla. En términos formales, de acuerdo con lo establecido en la norma ISO/IEC 27000, la confidencialidad es la propiedad que tiene la información de no estar disponible o revelada a individuos, entidades o procesos no autorizados.

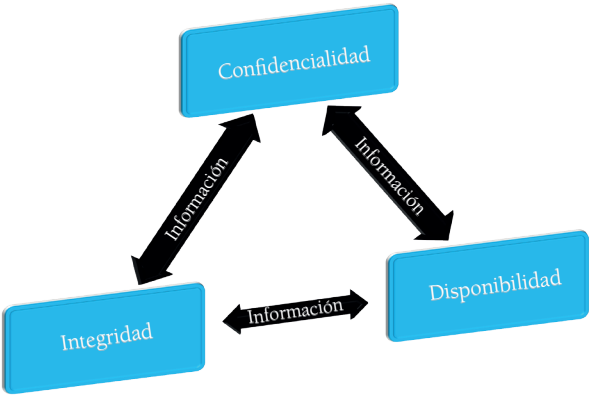

Figura 12. Tríada de seguridad de la información.
Fuente: Valencia Duque *et al.* (2015).

El concepto de *confidencialidad* es más cercano a la información que a los activos tecnológicos y persigue, fundamentalmente, que esta sea accesible únicamente a las personas, entidades o mecanismos autorizados.

La confidencialidad está asociada con secretos de diversa índole (personales, empresariales, militares). Algunos de ellos son técnicos, como, por ejemplo, la descripción de un método de fabricación (la fórmula de la Coca-Cola), otros son de índole comercial (una lista de nombres y direcciones de clientes que podría interesar a un competidor), e incluso militares, tales como planes de guerra o planes de incursión.

Entre los casos más sonados a nivel internacional que se encuentran relacionados con la confidencialidad se encuentra el caso de WikiLeaks, una plataforma digital para compartir documentos que se hizo famosa en julio de 2010 debido a los miles de documentos de carácter reservado que se difundieron por la web, lo que le provocó la antipatía del Gobierno de los Estados Unidos cuando se divulgaron más de 25 000 cables diplomáticos de sus embajadas en 274 países.

El caso más reciente en este ámbito es la extracción de información privada de los perfiles de Facebook de más de cincuenta millones de usuarios sin su consentimiento por parte de la firma Cambridge Analítica, lo que se convirtió en una de las filtraciones de información más grandes en la historia de las redes sociales (Rosenberg, Confessore y Cadwalladr, 2018).

Integridad

La integridad es un concepto que presenta diversas interpretaciones. En general, podría definirse como la propiedad de salvaguardar la exactitud e integridad de la información y de los activos tecnológicos ante su modificación o destrucción no autorizada.

De acuerdo con Cobit, la integridad está relacionada con la precisión y la completitud de la información, así como con su validez, de acuerdo con las expectativas y los valores del negocio.

La ISO/IEC 27000: 2018 define la integridad de la información como la propiedad de exactitud y completitud. Si la información está completa y libre de errores, es íntegra (Isaca, 2012c).

Uno de los ataques contra la integridad de la información es el caso del gusano Stuxnet, descubierto en 2010 y diseñado con la finalidad de dañar sistemas de control industriales y modificar su código a fin de permitir que los atacantes tomen el control. Este virus se hizo famoso por atacar una planta nuclear iraní.

Disponibilidad

Se refiera a que los usuarios autorizados tienen acceso a la información y a los activos tecnológicos cuando lo requieran. Para Cobit la disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento.

La ISO/IEC 27000:2018 define *disponibilidad* como la propiedad de ser accesible y utilizable a petición de una entidad autorizada. Entre las amenazas más cotidianas que afectan la disponibilidad de la información y/o de los activos tecnológicos se encuentra la denegación de servicio.

La disponibilidad de la información y/o de los activos tecnológicos asociados se puede presentar de forma cotidiana en diversas formas. Algunos ejemplos de estas son la salida de un sistema de información bancario de atención al cliente ante problemas de bases de datos; un servidor crítico fuera de línea ante un corte de energía; la imposibilidad de acceder a la información de un computador personal por problemas de *hardware*, por una falla del sistema operativo o por caídas de red.

Atributos complementarios relacionados con la seguridad de la información

Además de la tríada de seguridad, existen otros atributos que complementan los conceptos de seguridad y hacen parte del lenguaje de seguridad de la información. Entre estos se destacan:

- *Autenticidad*. Propiedad de la información por la cual se garantiza que una entidad es la que dice ser; busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar la suplantación de identidades.
- *No repudio*. Es la característica que permite garantizar la autoría de un mensaje y/o su envío, de forma tal que un emisor no niegue su autoría.

Relación de amenazas genéricas de seguridad con objetivos de seguridad de la información

Mediante la integración de los conceptos establecidos, en relación con las amenazas genéricas a la información y los objetivos de seguridad de la información, es posible relacionar ambos conceptos, tal como se puede apreciar en la tabla 2.

Tabla 2. Relación de amenazas genéricas con los objetivos de seguridad de la información

Amenazas generales	Objetivos de seguridad de la información			
	Confidencialidad	Integridad	Disponibilidad	Autenticidad
Intercepción o interceptación	▲			
Interrupción			▲	
Modificación		▲		
Generación				▲

Fuente: elaboración propia.

Sistemas de gestión

Con el fin de proteger la información y los recursos tecnológicos en los que se soporta, las empresas afrontan proyectos de seguridad mediante la protección de elementos aislados, de acuerdo con las necesidades del día a día de la operación del negocio, sin un enfoque sistémico, como un todo interrelacionado. Esto lleva no solo al incumplimiento de los objetivos previstos, sino también al rechazo generalizado de los sistemas de seguridad por parte de los empleados, quienes terminan por percibir la seguridad como un problema que entorpece la adecuada prestación de servicios.

Lo anterior llevó a la necesidad de concebir la seguridad como un sistema de gestión articulado a los demás sistemas de gestión con los que cuenta la organización, cuyo propósito es garantizar niveles aceptables de riesgo.

Un sistema de gestión, de acuerdo con lo establecido por la ISO/IEC 27000:2018 en el numeral 3.41, es un conjunto de elementos interrelacionados o interactuantes de una organización dirigido a establecer políticas, objetivos y procesos con el fin de cumplir con sus objetivos (ISO/IEC, 2018a). El término *sistema de gestión* proviene del inglés *management system*, lo cual representa un modo o forma de gestionar, o una manera formalizada de realizar las cosas (Morán Abad, Pérez Sánchez, Trujillo Gaona, Bathiely Fernández y González-Simancas, 2010).

Los sistemas de gestión en las organizaciones, por lo general, se encuentran basados en lo que se ha denominado ciclo Deming (en honor a su creador, Edward Deming), el cual se basa en el ciclo PDCA (*plan*, *do*, *check*, *act*) o su equivalencia en español PHVA (planear, hacer, verificar, actuar). Este es el ciclo en el que se fundamentan actualmente la mayoría de los sistemas de gestión promulgados por la ISO.

Si se tiene en cuenta que a nivel internacional la base de los procesos de seguridad de la información se ha desarrollado a partir de que lo se ha denominado sistema de gestión de seguridad de la información (en adelante SGSI), fundamentado en la familia de las normas ISO/IEC 27000, es importante, de manera inicial, dado su tratamiento de forma más extensa en el próximo capítulo, explicar el ciclo PHVA en el contexto de la seguridad de la información en los puntos que se enlistan a continuación, tal como se puede observar en la figura 13.

- *Planificar*. Esta fase es equivalente a establecer el SGSI a través del diseño de políticas objetivos, procesos y procedimientos de seguridad para gestionar el riesgo y obtener niveles aceptables de seguridad.

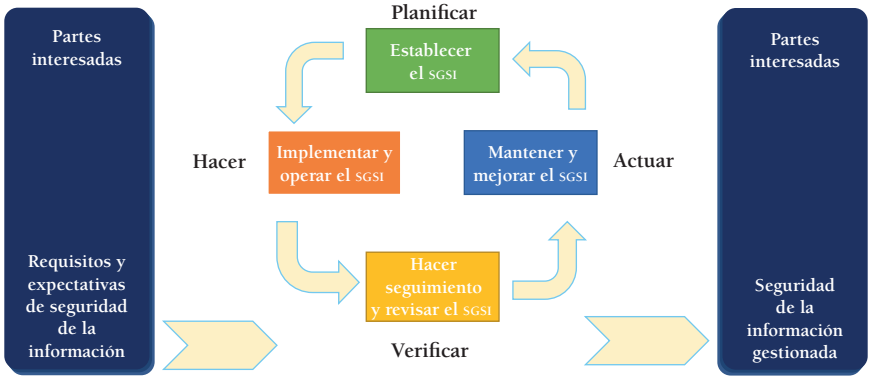

Figura 13. Modelo PHVA aplicado a los procesos de un SGSI.
Fuente: elaborado a partir de Icontec (2009a).

- *Hacer*. Esta fase conlleva la implementación y operación de las políticas, los controles, los procesos y los procedimientos del SGSI.
- *Verificar*. La verificación consiste en hacer seguimiento y revisar el nivel de cumplimiento de lo planeado (fase planear) frente a lo ejecutado (fase hacer), con el fin de garantizar el cumplimiento de los objetivos previstos por el SGSI.
- *Actuar*. Con el fin de mantener y mejorar constantemente el SGSI, esta fase supone el desarrollo de acciones correctivas y preventivas orientadas a lograr los resultados esperados por el SGSI.

Marcos de referencia de la seguridad de la información

La seguridad absoluta no existe y siempre se tendrá un antagonismo entre los riesgos y los controles, con los niveles de sofisticación que de manera incremental se presentarán entre ambos a través del tiempo. De allí que no existe un punto de llegada definitivo de la seguridad de la información. La búsqueda de niveles aceptables de riesgo es el reto de cualquier profesional dedicado a la seguridad, en general, y del oficial de seguridad de la información —en inglés, CISO o *chief information security officer*— en particular, o de cualquier profesional que ostente el desarrollo de tal actividad.

Acorde con lo anterior, el objetivo de la seguridad es un objetivo movible que se encuentra en constante cambio, lo que requiere no solo profesionales conocedores de las novedades que en materia de riesgos y controles existan, sino, fundamentalmente, de un adecuado sistema de gestión que permita un ciclo de mejoramiento continuo que pueda planearse, ejecutarse, evaluarse y corregirse con miras a lograr ese objetivo movible.

▸ Gobierno y gestión de la seguridad de la información

Los conceptos de *gobierno* y *gestión* están presentes en el ámbito empresarial y en el ámbito tecnológico, en lo que tiene que ver

con el gobierno de seguridad de la información, como parte integral del gobierno corporativo. Autores tales como Cano (2013, citando a Macmillan y Scholtz), definen el *gobierno de seguridad de la información* como todos aquellos procesos que aseguran las acciones requeridas para proteger los recursos de información de la organización, lo que demanda estrategias que permitan avanzar hacia los retos que esta afronta.

El gobierno de seguridad es responsabilidad tanto del consejo de dirección como de la dirección ejecutiva. De acuerdo con ISACA (2013), debe contemplar seis resultados básicos para un gobierno efectivo de seguridad de la información: alineación estratégica, gestión de riesgos, entrega de valor, gestión de recursos, medición del desempeño e integración.

En lo atinente a la gestión, entendida como la aplicación de la seguridad de la información en el día a día de la organización, existe una serie de marcos de referencia que proveen una guía para implementar procesos efectivos de seguridad de la información.

Estándares, marcos de referencia y guías profesionales de gestión de seguridad de la información

En el campo de la seguridad de la información, la comunidad académica, profesional y gubernamental ha generado múltiples estándares, *frameworks* y guías profesionales con el fin de abordar la forma como se debe llevar a cabo la seguridad de la información en una organización. Prislan, Lobrikar y Bernik (2017) establecen una categorización de las diferentes guías existentes, tal como se observa en la figura 14. No obstante, "la familia de normas ISO/IEC 27000 es la más reconocida y ampliamente aceptada" (Prislan *et al.*, 2017, p. 8), lo cual se demuestra en las diferentes encuestas que al respecto se han adelantado a nivel internacional, además del incremento exponencial que ha tenido la certificación en ISO/IEC 27001 por parte de las organizaciones a nivel mundial.
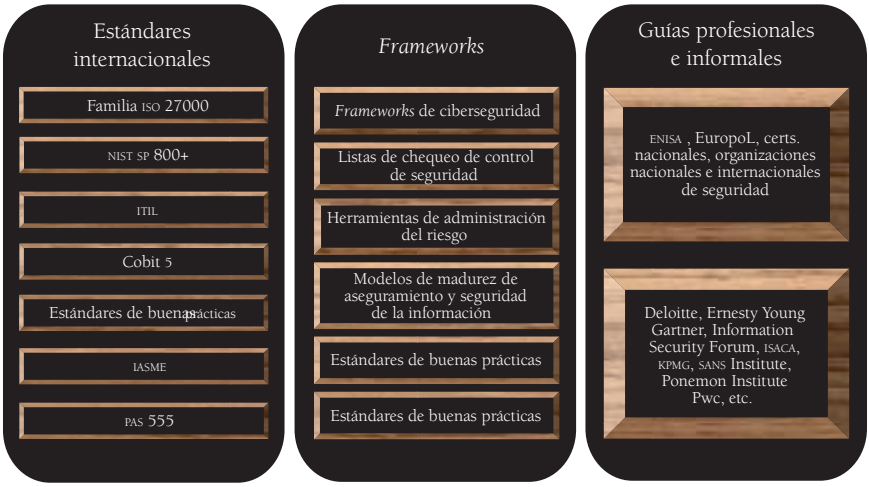
Figura 14. Categorización de las guías de seguridad de la información.
Fuente: elaboración propia a partir de Prislan *et al.* (2017).

Históricamente, de acuerdo con los resultados arrojados por la Encuesta Latinoamericana de Seguridad de la Información, en el periodo 2009-2018 los marcos de gestión de seguridad de la información más usados fueron, en su orden, la ISO/IEC 27001, ITIL, COBIT 4.1/5 y las guías del NIST, tal como se puede apreciar en la tabla 3.

Tabla 3. Estándares y buenas prácticas de seguridad de la información utilizadas en Latinoamérica

Estándares y buenas prácticas	2009	2010	2011	2012	2013	2014	2018
ISO/IEC 27001	45,80 %	27,367 %	28,88 %	55,83 %	58,33 %	63,33 %	58 %
ITIL	26,90 %	17,47 %	18,28 %	40,27 %	32,08 %	41,48 %	29 %
Cobit 4.1/5	23,40 %	14,88 %	15,62 %	31,11 %	31,25 %	19,63 %	28 %
Guías del NIST (National Institute of Standars and Technology) EE. UU.	12,30 %	8,09 %	7,49 %	12,50 %	12,92 %	14,81 %	15 %
No se consideran	37,70 %	10,19 %	14,80 %	21,38 %	28,75 %	20,00 %	-

Continúa en la siguiente página ►

Estándares y buenas prácticas	2009	2010	2011	2012	2013	2014	2018
OSSTM (Open Standard Security Testing Model)	7,50 %	3,23 %	4,38 %	6,38 %	5,00 %	-	4 %
Guías de la ENISA (European Network of Information Security Agency)	2,30 %	9,70 %	1,46 %	1,94 %	1,67 %	1,85 %	3 %
Common criterio	5,20 %	1,21 %	3,65 %	3,33 %	3,75 %	-	2 %
Magerit	5,20 %	3,23 %	2,74 %	7,22 %	4,58 %	4,81 %	-
Octave	2,30 %	1,29 %	2,19 %	2,22 %	2,50 %	1,11 %	-
ISM3-Information Security Management Maturiy Model	3,90 %	9,70 %	1,46 %	3,01 %	1,67 %	0,74 %	2 %
Otra; top 20 de fallas de seguridad del SANS, ISO 17799, BS 259999; NTC 5254, OWASP, ISSAF, PCI- DSS, MCIIEF SOX N-24360, SARO, Comunicación A4609, Propias Circular 052	7,10 %	2,91 %	-	6,94 %	9,17 %	-	16 %

Fuente: elaboración propia a partir de Cano, Saucedo y Chávez (2014) y Almanza (2019).

Las encuestas más recientes realizadas en Latinoamérica por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) posicionan la ISO 27001 e ITIL como los marcos de referencia más usados. Lo anterior lo confirma otro tipo de encuestas tales como las realizadas por CISCO (2017), en las que se destaca la ISO 27001 como el estándar más utilizado para la gestión de la seguridad de la información.

ISO/IEC 27001

La norma ISO/IEC 27001 es el principal referente de seguridad de la información a nivel internacional. Así lo demuestran no solo los resultados

arrojados por la encuesta latinoamericana de seguridad desde el 2009, sino también, a nivel internacional, el incremento sostenido que han tenido las certificaciones emitidas por la ISO en los diferentes países del mundo. Son los de Asia Oriental y del Pacífico los de mayor número de certificaciones en esta norma, tal como se puede observar en la tabla 4.

Tabla 4. Certificaciones en la norma 27001 emitidas por la ISO a nivel mundial

Año	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Total	5797	7732	9246	12935	15626	17355	19620	21604	23005	27536	33290	39501
África	6	10	16	47	46	40	64	99	79	129	224	301
Suramérica y Centroamérica	18	38	72	100	117	150	203	272	273	347	564	620
Norteamérica	79	112	212	322	329	435	552	712	814	1445	1469	2108
Europa	1064	1432	2172	3563	4800	5289	6379	7952	8663	10446	12532	14605
Asia Oriental y del Pacífico	4210	5550	5807	7394	8788	9665	10422	10116	10414	11994	14704	17562
Asia Central y del Sur	383	519	839	1303	1328	1497	1668	2002	2251	2569	2987	3382
Oriente Medio	37	71	128	206	218	279	332	451	511	606	810	923

Fuente: elaboración propia a partir de ISO (2019).

La norma ISO/IEC 27001:2013 ha sido elaborada con el fin de establecer los requisitos para el establecimiento, la implementación, el mantenimiento y la mejora continua de un sistema de gestión de seguridad de la información que permita preservar la confidencialidad, la integridad y la disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos (Icontec, 2013).

No obstante, la seguridad de la información no solo está basada en esta norma, sino en la familia de normas de seguridad de la información ISO/IEC 27000, la cual está compuesta por las normas que se referencian en la tabla 5.

Tabla 5. Normas de la familia ISO/IEC 27000

Norma	Descripción de la norma
ISO/IEC 27000	Sistema de gestión de seguridad de la información. Visión general y vocabulario.
ISO/IEC 27001	Sistema de gestión de seguridad de la información. Requerimientos.
ISO/IEC 27002	Código de práctica para controles de seguridad de la información.
ISO/IEC 27003	Guía para la implementación del sistema de gestión de seguridad de la información.
ISO/IEC 27004	Gestión de seguridad de la información. Monitoreo, medición, análisis y evaluación.
ISO/IEC 27005	Gestión del riesgo de seguridad de la información.
ISO/IEC 27006	Requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.
ISO/IEC 27007	Guía para la auditoría de sistemas de gestión de seguridad de la información.
ISO/IEC TR 27008	Guía para auditores sobre los controles de seguridad de la información.
ISO/IEC 27009	Requerimientos para la aplicación de la ISO/IEC 27001 en sectores específicos.
ISO/IEC 27010	Gestión de seguridad de la información para comunicaciones intersectoriales e interorganizacionales.
ISO/IEC 27011	Guía de gestión de seguridad de la información para organizaciones de telecomunicaciones basado en la ISO/IEC 27002.
ISO/IEC 27013	Guía para la implementación integrada de la ISO/IEC 27001 y la ISO/IEC 20000-1.
ISO/IEC 27014	Gobierno de seguridad de la información.
ISO/IEC TR 27015	Guía de gestión de seguridad de la información para servicios financieros.
ISO/IEC TR 27016	Gestión de seguridad de la información. Economía de las organizaciones.
ISO/IEC 27017	Código de prácticas para controles de seguridad de la información basado en la ISO/IEC 27002 para servicios *cloud*.
ISO/IEC 27018	Código de prácticas para la protección de la información de identificación personal (PII) en nubes públicas que actúan como procesadores PII.
ISO/IEC 27019	Controles de seguridad de la información para la industria de servicios energéticos.
ISO/IEC 27021	Requerimientos de competencia para profesionales de sistemas de gestión de seguridad de la información.
ISO/IEC 27799	Informática de salud-Gestión de seguridad de la información en salud utilizando ISO/IEC 27002.

Fuente: elaboración propia a partir ISO/IEC (2018a).

ITIL

La Biblioteca de Infraestructura de Tecnologías de Información (ITIL, por sus siglas en inglés para Information Technology Infrastructure Library) es una norma publicada por el Reino Unido con el fin de dar a conocer mejores prácticas para la gestión de servicios de tecnologías de información. La versión 3 está compuesta por cinco volúmenes, a través de los cuales se cubre el ciclo de vida de la gestión de servicios de tecnologías de información: estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio.

Como parte del ciclo de vida de diseño del servicio, se encuentra el proceso de gestión de seguridad de la información, cuyos principales objetivos se resumen en diseñar una política de seguridad en colaboración con clientes y proveedores correctamente alineada con las necesidades del negocio, asegurar el cumplimiento de los estándares de seguridad acordados y minimizar los riesgos de seguridad que amenazan la continuidad del servicio (Osiatis, 2015).

Para cumplir este proceso se sigue el flujo establecido en la figura 15. Esto se logra a través de un adecuado sistema de gestión de seguridad de la información que, de acuerdo con el ITSMF International (2007), representa la base para un desarrollo en términos de costo beneficio de un programa de seguridad de la información que soporte los objetivos del negocio, para lo cual se usan las cuatro P: personas, procesos, productos (lo que incluye la tecnología) y *partners*.

Como parte de los subprocesos que establece ITIL versión 3, en lo que tiene que ver con seguridad se encuentran la política y el plan de seguridad, la aplicación de las medidas de seguridad y la evaluación y el mantenimiento.

- *Políticas y plan de seguridad*. La política de seguridad permite establecer un marco general por medio del cual se articulen las diferentes fases de desarrollo de un sistema de gestión de seguridad. Esta debe estar alineada con un plan de seguridad que permita proteger los diferentes servicios de tecnología de información y, a su vez, pueda hacer parte de los acuerdos de niveles de servicio (SLA), de los acuerdos de nivel de operación (OLA) y de los contratos de soporte (UC).

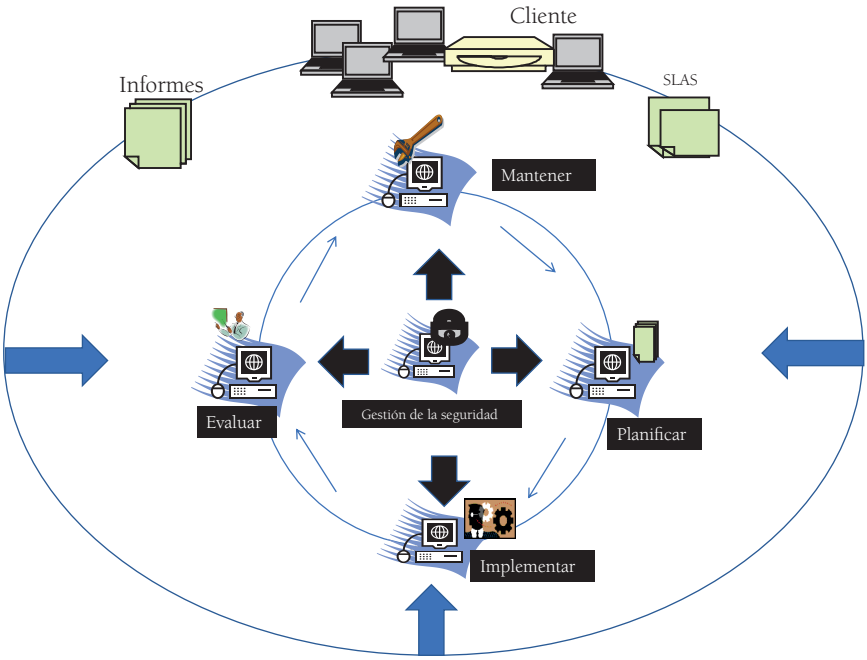

Figura 15. Seguridad de la información desde la perspectiva de ITIL.
Fuente: elaboración propia a partir de Osiatis (2015).

- *Aplicación de las medidas de seguridad*. Este subproceso implica, con base en la planeación, la aplicación de las diversas medidas de seguridad previstas, teniendo en cuenta que se asignen los recursos necesarios para tal fin, se genere la documentación de referencia pertinente, se instalen y mantengan las herramientas de *hardware* y *software* requeridas y se realice un monitoreo permanente de los servicios de tecnologías de información.
- *Evaluación y mantenimiento*. Es imprescindible evaluar el nivel de aplicación de las medidas de seguridad de acuerdo con los planes elaborados para tal fin, con el propósito de tomar las acciones requeridas con miras a garantizar los objetivos previstos de seguridad de la información. Estas evaluaciones incluyen el desarrollo de auditorías de seguridad internas y/o externas.

Cobit 5.0 para la seguridad de la información

La estructura de la versión 5.0 de Cobit presenta un renovado marco de referencia principal, el cual lo complementan guías habilitadoras y guías profesionales de orientación, tal como se puede observar en la figura 16.

Figura 16. Familia de productos de Cobit 5.0.
Fuente: elaboración propia a partir de Isaca (2012a).

La guía de Cobit 5 para la seguridad de la información presenta un enfoque integral y orientado al negocio para la gestión de la seguridad de la información y utiliza muchos de los componentes del modelo BMIS.

El marco principal de Cobit 5 presenta tres procesos relacionados directamente con la seguridad de la información: el proceso APO13 —administrar la seguridad—, el proceso DSS04 —administrar la continuidad— y el proceso DSS05 —administrar los servicios de seguridad—, los cuales proveen una guía básica sobre cómo definir, operar y monitorear un sistema para la administración de la seguridad (Isaca, 2012d). Una relación detallada de estos procesos se puede observar en la tabla 6.

Tabla 6. Procesos de Cobit 5.0 relacionados directamente con la seguridad de la información

APO13. Administrar la seguridad	
Descripción del proceso Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	**Propósito del proceso** Mantener el impacto y la ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.
Prácticas de gestión	
APO13.01 Establecer y mantener un SGSI Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, la tecnología y los procesos de negocio que esté alineado con los requerimientos de negocio y la gestión de seguridad en la empresa.	
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información 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.	
APO13.03 Supervisar y revisar el SGSI Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de la 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.	
DSS04. Gestionar la continuidad	
Descripción del proceso Establecer y mantener un plan dirigido a permitir al negocio y a las TI responder a incidentes e interrupciones de servicio con miras a la operación continua de los procesos críticos para el negocio y los servicios TI requeridos, así como mantener la disponibilidad de la información en un nivel aceptable para la empresa.	**Propósito del proceso** Continuar las operaciones críticas del negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.
Prácticas de gestión	
DSS04.01 Definir la política de continuidad de negocio, los objetivos y el alcance Definir la política y el alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.	

Continúa en la siguiente página ▶

DSS04.02 Mantener una estrategia de continuidad
Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.

DSS04.03 Desarrollar e implementar una respuesta
Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente, a fin de facilitar que la empresa continúe con sus actividades críticas.

DSS04.04 Ejercitar, probar y revisar el BCP
Probar los acuerdos de continuidad regularmente con el propósito de ejercitar los planes de recuperación con respecto a unos resultados predeterminados, a fin de permitir el desarrollo bien sea de soluciones innovadoras o bien para ayudar a verificar que el plan funcionará en el tiempo como se espera.

DSS04.05 Revisar, mantener y mejorar el plan de continuidad
La dirección debe realizar una revisión de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo con el proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja de forma continua los requerimientos actuales del negocio.

DSS04.06 Proporcionar formación en el plan de continuidad
Proporcionar a todas las partes implicadas —internas y externas— sesiones formativas regulares que contemplen los procedimientos, sus roles y sus responsabilidades en caso de disrupción.

DSS04.07 Gestionar acuerdos de respaldo
Mantener la disponibilidad de la información crítica del negocio.

DSS04.08 Ejecutar revisiones posreanudación
Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y los servicios luego de una disrupción.

DSS05. Gestionar servicios de seguridad

Descripción del proceso
Proteger la información de la empresa con el fin de mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y los privilegios de acceso a la información, así como realizar la supervisión de la seguridad.

Propósito del proceso
Minimizar el impacto en el negocio de las vulnerabilidades y los incidentes operativos de seguridad en la información.

Prácticas de gestión

DSS05.01 Proteger contra *software* malicioso (*malware*)
Implementar y mantener medidas efectivas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa, con la finalidad de proteger los sistemas de información y tecnología del *software* malicioso (por ejemplo, virus, gusanos, *software* espía —*spyware*— y correo basura).

Continúa en la siguiente página ▶

DSS05.02 Gestionar la seguridad de la red y las conexiones Utilizar medidas de seguridad y procedimientos de gestión relacionados con miras a proteger la información en todos los modos de conexión.
DSS05.03 Gestionar la seguridad de los puestos de usuario final Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y *software* móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.
DSS05.04 Gestionar la identidad del usuario y el acceso lógico Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.
DSS05.05 Gestionar el acceso físico a los activos de TI Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren a los locales, lo que incluye a empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.
DSS05.06 Gestionar documentos sensibles y dispositivos de salida Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (*token*) de seguridad.
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad Mediante herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

Fuente: Isaca (2012b).

NIST SP 800

El Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology-NIST) del departamento de comercio de los Estados Unidos ha desarrollado una serie de normas relacionadas con la gestión del riesgo de los sistemas de información federal, las cuales se clasifican en:

- normas de procesamiento de información federal (FIPS);
- publicaciones especiales (SP);
- informes interinstitucionales Nist (Nistir's);
- boletines de laboratorio de tecnología de información (DIT).

La mayoría de estas normas se encuentran articuladas al ciclo de vida de seguridad de la información, definido por el NIST, tal como se puede observar en la figura 17.

Figura 17. Ciclo de vida de seguridad de la información del NIST.
Fuente: elaboración propia a partir de NIST (2014a).

Cada una de estas fases de gestión de riesgos cuenta con normas y guías asociadas para dar cumplimiento a cada una de las fases que hacen parte del marco, tal como se puede observar en la tabla 7.

Tabla 7. Guías y estándares asociados a la gestión de seguridad de la información del NIST

Fase	Estándar	Descripción del estándar
1. Categorizar	Estándar FIPS-199	Estándares para categorizar la seguridad de la información y los sistemas de información federales.
	Guía SP 800-60	Guía para mapear los tipos de información y los sistemas de información dirigidos a categorizar la seguridad.
2. Seleccionar	Estándar FIPS-200	Requerimientos de seguridad mínimos para información y sistemas de información federales.
	Guía SP 800-53	Controles de seguridad recomendados para información y sistemas de información federales.
	Guía SP 800-18	Guía para el desarrollo de planes de seguridad orientados a tecnologías de información.
3. Implementar	Guía SP 800-53	Controles de seguridad recomendados para información y sistemas de información federales.
	Guía SP 800-53[a]	Guía para evaluar los controles de seguridad en sistemas de información federal.
	SP 800-70	*Checklist* de configuración de seguridad de la información para productos de TIC.
4. Evaluación	Guía SP 800-53[a]	Guía para evaluar los controles de seguridad en sistemas de información federal.
	Guía SP 800-115	Guía técnica para evaluar y probar la seguridad de la información.
5. Autorizar	Guía SP 800-37	Guía para aplicar el marco de gestión de riesgos a los sistemas de información federal.
6. Monitorear	Guía SP 800-37	Guía para aplicar el marco de gestión de riesgos a los sistemas de información federal.

Fuente: Valencia Duque (2018).

En particular, en lo que tiene que ver con los controles de tecnologías de información que proporciona la NIST, la guía SP 800-53 establece un catálogo de 240 controles de seguridad de la información, estructurado cada uno de ellos en cinco secciones: la sección de descripción del control, una sección de guía suplementaria, una sección de mejoras del control, una sección de referencias y una sección de asignación de prioridades y de línea base.

BMIS (Business Model for Information Security)

El modelo de negocio de seguridad de la información es un modelo originado en el Institute for Critical Information Infrastructure Protection de la Universidad de Southern California, de Estados Unidos, adoptado y difundido por ISACA. Como se puede apreciar en la figura 18, el modelo lo estructuran cuatro elementos unidos por seis interconexiones, los cuales interactúan de manera dinámica.

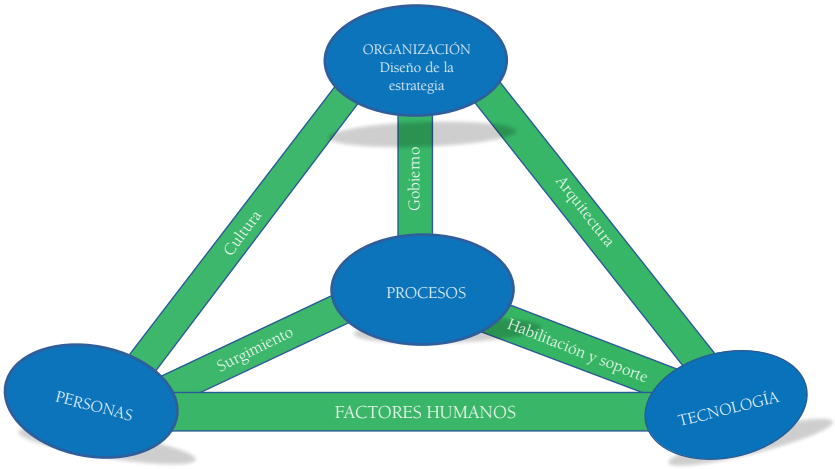

Figura 18. Modelo BMIS.
Fuente: elaborado a partir de ISACA (2013).

Los cuatro elementos que conforman la estructura principal del modelo son los siguientes.

1. *Diseño y estrategia de la organización*. A una organización la componen personas, procesos y activos que permanecen en constante interacción en busca del cumplimiento de una meta, en este caso, una meta de seguridad de la información. La estrategia de la empresa especifica las metas y los objetivos que espera alcanzar la organización, de manera que debe diseñarse de forma adecuada en conformidad con las personas y su cultura, la tecnología y su arquitectura y los procesos y su nivel de gobernabilidad.
2. *Personas*. Este elemento representa los recursos humanos y los aspectos de seguridad que los rodean, de modo que identifica roles y responsabilidades mientras define aspectos tales como estrate-

gias de reclutamiento y cuestiones relacionadas con el empleo, así como términos de contratación y relacionados con terceros.

3. *Procesos*. Representa el eje principal del modelo, dado que proporciona equilibrio a los demás componentes y a las diferentes interrelaciones. Comprende la parte operacional del diseño y la estrategia de la organización, para lo cual se realiza una definición de las tareas requeridas en el propósito de cumplir con las estrategias de seguridad. A través de los procesos se gestiona y controla el riesgo, con lo cual se cumplen los criterios de confidencialidad, integridad y disponibilidad de la información; deben cumplir, como mínimo, con las siguientes características: satisfacer los requerimientos del negocio, considerar situaciones emergentes y adaptarse a los cambios, estar documentados y ser comunicados y revisados periódicamente.
4. *Tecnología*. Este elemento lo conforman la infraestructura tecnológica como recurso estratégico de la organización y su relación dinámica con las personas a través de los factores humanos que influyen en su uso y operación, con los procesos como habilitadores y el respectivo soporte con la organización a través de su arquitectura.

Las interconexiones enlazan los elementos y ejercen una fuerza multidireccional que empuja y atrae a medida que las situaciones cambian; representan el componente dinámico del modelo. Estas se enlistan a continuación.

1. *Gobierno*. Esta interconexión se encarga de garantizar que se determinen los objetivos al brindar dirección y control estratégico a la organización, así como al articular su cumplimiento con los procesos definidos para tal fin.
2. *Cultura*. Representa un conjunto de conductas, convicciones, supuestos y actitudes requeridas para cumplir con los objetivos trazados por la organización en relación con la seguridad de la información.
3. *Habilitación y soporte*. Esta interconexión entre tecnología y proceso requiere la implementación de procesos prácticos y ágiles que permitan asegurar que las personas cumplan con las medidas, las políticas y los procedimientos técnicos de seguridad.

4. *Surgimiento*. Se refiere a los patrones que surgen en la vida de la empresa que parecen no tener una causa obvia y cuyos resultados parecen imposibles de predecir y controlar, lo que implica, en su relación entre personas y procesos, la introducción de posibles soluciones.
5. *Factores humanos*. Representa la interacción entre las personas y la tecnología; parte de la necesidad de que las personas entiendan cómo utilizar la tecnología, para que sea aceptada y puedan seguir políticas pertinentes ante problemas graves de seguridad.
6. *Arquitectura*. Una arquitectura robusta de información del negocio es esencial con el propósito de entender la necesidad de la seguridad y de diseñar su arquitectura.

Otros marcos de referencia de seguridad de la información

O-ISM3 (The Open Information Security Management Maturity Model)

El modelo abierto de madurez de gestión de seguridad de la información (en adelante O-ISM3), actualmente en su segunda versión, fue desarrollado por el consorcio Open Group y establece un modelo basado en la relación que existe entre procesos, capacidades y madurez (The Open Group, 2017).

Los procesos que hacen parte de un sistema de gestión de seguridad de la información bajo la óptica de este modelo se dividen en cuatro categorías: procesos genéricos, procesos estratégicos, procesos tácticos y procesos operacionales.

Las capacidades están relacionadas con la forma en la que se gestiona un proceso. Desde una perspectiva gerencial, cuanto mayor sea la capacidad, más prácticas administrativas serán aplicables y más sólido y transparente será el proceso. Algunos de los factores que ayudan a lograr niveles de capacidad más altos son: distribución adecuada de responsabilidades, recursos disponibles para el proceso, motivación, habilidades, responsabilidad y empoderamiento del personal.

Los niveles de madurez son combinaciones específicas de procesos O-ISM3 practicados a niveles de capacidad específicos. Existe una relación entre la cantidad de procesos, su capacidad y la madurez del SGSI. Cuantos más procesos y cuanto mayor sea la capacidad, mayor será la madurez.

Los niveles de madurez están diseñados para satisfacer las necesidades de las organizaciones con diferentes tamaños, recursos, amenazas, impactos (tanto financieros como no financieros), apetito del riesgo y sector económico.

SABSA framework

El marco de referencia Sherwood Applied Business Security Architecture (SABSA) es un método de arquitectura de seguridad empresarial desarrollado por el SABSA Institute (SABSA Institute, 2018), relacionado con el modelo de arquitectura empresarial TOGAF y definida por Sherwood, Clark y Lynas (2009) como una metodología para el desarrollo de la seguridad de la información empresarial y el aseguramiento de arquitecturas de información orientadas a riesgos, cuya principal característica es que su aplicación parte del análisis de los requerimientos de seguridad que tiene el negocio.

SABSA está compuesta por seis capas que reflejan los diferentes tipos de arquitectura con las que cuenta el modelo: arquitectura contextual, arquitectura conceptual, arquitectura lógica, arquitectura física, arquitectura de componentes y arquitectura de gestión del servicio (esta última es transversal a las demás capas). Dada la relación con el modelo TOGAF, para desarrollar cada una de las arquitecturas se formulan las mismas preguntas que contempla este modelo, las cuales son: qué (activos), por qué (motivaciones), cómo (procesos), quién (personas), dónde (localización) y cuándo (tiempo).

Una descripción de cada una de las preguntas por cada una de las arquitecturas que hacen parte del modelo se presenta en la tabla 8.

Tabla 8. Preguntas asociadas a las diferentes arquitecturas del modelo SABSA

Pregunta	Producto	Descripción
Arquitectura contextual		
Qué (activos)	Decisiones del negocio	Taxonomía de activos del negocio, incluyendo metas y objetivos.
Por qué (motivaciones)	Riesgos del negocio	Inventario de amenazas y oportunidades.
Cómo (procesos)	Procesos del negocio	Inventario de procesos operacionales.
Quién (personas)	Gobierno del negocio	Estructura organizacional y organización extendida.

Continúa en la siguiente página ▶

Pregunta	Producto	Descripción
Dónde (localización)	Geografía del negocio	Inventario de edificios, sitios, jurisdicciones, etc.
Cuándo (tiempo)	Tiempos de dependencia del negocio	Tiempos de dependencia de los objetivos del negocio
Arquitectura conceptual		
Qué (activos)	Conocimiento del negocio y estrategias de riesgo	Perfil de atributos del negocio.
Por qué (motivaciones)	Objetivos de administración del riesgo	Objetivos de habilitación y control; arquitectura política.
Cómo (procesos)	Estrategias para el aseguramiento del proceso	Mapeo de procesos; estrategias de TIC.
Quién (personas)	Roles y responsabilidades	Propietarios, custodios y usuarios; proveedores de servicio y clientes.
Dónde (localización)	Marco de trabajo del dominio	Marco de referencia y conceptos del dominio de seguridad.
Cuándo (tiempo)	Marco de referencia de tiempos del negocio	Marco de referencia del ciclo de vida de gestión del riesgo.
Arquitectura lógica		
Qué (activos)	Activos de información	Inventario de activos de información.
Por qué (motivaciones)	Políticas de gestión del riesgo	Políticas en el dominio.
Cómo (procesos)	Mapas de procesos y servicios	Flujos de información; transformaciones funcionales; arquitectura orientada a servicios.
Quién (personas)	Marco de entidades y confianza	Esquema de entidades; modelos de confianza; perfiles de privilegio.
Dónde (localización)	Mapas de dominio	Definiciones de dominio; asociaciones e interacciones entre dominios.
Cuándo (tiempo)	Horarios y calendarios	Tiempos de inicio, ciclos de vida y fechas límite.
Arquitectura física		
Qué (activos)	Activos de datos	Diccionario de datos e inventario de datos.
Por qué (motivaciones)	Prácticas de gestión del riesgo	Reglas y procedimientos de gestión del riesgo.

Continúa en la siguiente página ►

Pregunta	Producto	Descripción
Cómo (procesos)	Mecanismos en procesos	Aplicaciones, *middleware*, sistemas, mecanismos de seguridad.
Quién (personas)	Interfaces humanas	Interfaces de usuario para sistemas TIC; sistemas de control de acceso.
Dónde (localización)	Infraestructura TIC	Servidores; redes y capas tecnológicas.
Cuándo (tiempo)	Gestión de horarios.	Tiempos y secuencias de sesiones y procesos.
Arquitectura de componentes		
Qué (activos)	Componentes TIC	Productos TIC incluyendo repositorios de datos y dispositivos de procesamiento.
Por qué (motivaciones)	Herramientas y estándares de gestión del riesgo	Herramientas de análisis de riesgos; registros de riesgos; herramientas de monitoreo y reporte de riesgos.
Cómo (procesos)	Herramientas de procesos y estándares	Herramientas y protocolos para el desarrollo de procesos.
Quién (personas)	Herramientas de gestión de personal y estándares.	Identidades; descripción de trabajos; roles; funciones; acciones y listas de control de acceso.
Dónde (localización)	Herramientas de localización y estándares	Nodos, direcciones y otras localizaciones.
Cuándo (tiempo)	Tiempos de paso y herramientas de secuencia.	Gestión de horarios; relojes, tiempos e interrupciones.
Arquitectura de gestión de servicios		
Qué (activos)	Gestión de entrega de servicios	Aseguramiento de la continuidad y excelencia operacional.
Por qué (motivaciones)	Gestión del riesgo operacional.	Evaluación del riesgo; monitoreo y reporte del riesgo; tratamiento del riesgo.
Cómo (procesos)	Gestión de la entrega de procesos	Administración y soporte de sistemas, aplicaciones y servicios.
Quién (personas)	Gestión de personal	Gestión de cuentas; gestión de soporte a usuarios.
Dónde (localización)	Gestión del ambiente	Gestión de edificios, sitios, plataformas y redes.
Cuándo (tiempo)	Gestión de tiempos	Gestión de calendarios y tiempos.

Fuente: elaboración propia a partir de SABSA Institute (2018).

Certificaciones personales en materia de seguridad de la información

La seguridad de la información es una disciplina en la que se conjugan permanentemente los riesgos que afectan a una organización y los controles que ayudan a mitigarlos, pero son las personas las que integran ambos conceptos y los ponen al servicio de la organización. De esta forma desarrollan la función de seguridad de la información, lo que requiere una cualificación continua que le permita responder a los retos que día a día impone esta función. Si bien dicha cualificación se puede lograr al estar en permanente contacto con las fuentes de información relacionadas, es la obtención de una de las certificaciones existentes en el mercado la que determina el nivel de competencia del profesional de la seguridad de la información.

Actualmente existen más de cuarenta certificaciones relacionadas con el control y la seguridad de la información, lo que incluye una de las más recientes, como lo es la certificación propuesta por ISACA a través del programa Cybersecurity Nexus (CSX), denominada Cybersecurity Fundamentals Certificate. No obstante, las que tienen mayor demanda son, en su orden, CISSP, CISM, CISA y CRISC, tal como se ha presentado en una de las encuestas latinoamericanas de seguridad de la información.

De acuerdo con Martínez Contreras (2016), las certificaciones en seguridad de la información se pueden clasificar en cinco áreas: SGSI, *forensic*, redes, desarrollo, *hacking* y protección de datos, tal como se puede apreciar en la figura 19.

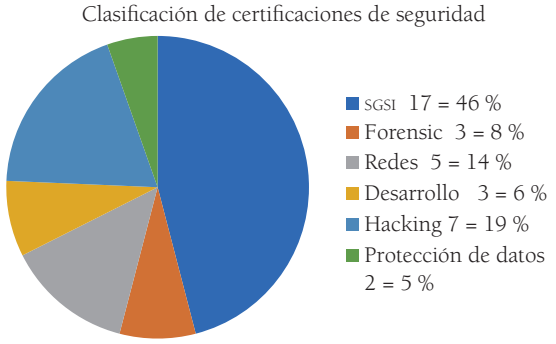

Figura 19. Certificaciones requeridas en seguridad de la información y relacionadas.
Fuente: Martínez Contreras (2016).

Una descripción de las principales certificaciones en materia de control y seguridad de la información se expone en la tabla 9.

Tabla 9. Principales certificaciones asociados a la seguridad de la información y relacionadas

Sigla	Certificación	Entidad que la otorga	Sitio web
CISSP	Certified Information Systems Security Professional	Information System Security Certification Consortium (ISC)[2]	www.isc2.org
CISM	Certified Information Security Manager	Information Systems Audit and Control Association (ISACA)	http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx
CEH	Certified Ethical Hacker	EC-Council	http://www.eccouncil.org/Certification/certified-ethical-hacker
CISA	Certified Information Systems Auditor	Information Systems Audit and Control Association (ISACA)	http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx
CRISC	Certified in Risk and Information Systems Control	Information Systems Audit and Control Association (ISACA)	http://www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Pages/default.aspx
CFE	Certified Fraud Examiner	Association of Certified Fraud Examiners (ACFE)	http://www.acfe.com/

Fuente: elaboración propia.

Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000

Luego de presentar una introducción a la seguridad de la información y los principales referentes que existen al respecto, es necesario abordar la forma en la que se puede materializar la implementación de un sistema de gestión de seguridad de la información a partir de las mejores prácticas establecidas a través de la familia de normas de la ISO/IEC 27000.

Para esto es necesario conocer la familia de normas ISO/IEC 27000, sus objetivos, la interrelación y las normas más representativas en el momento de abordar una implementación de este tipo que permita, a través de su adecuada combinación, un proceso entendible y coherente.

A partir del conocimiento de las diferentes normas que hacen parte de la familia de normas del SGSI, es necesario presentar un enfoque que permita también, a partir de la interrelación de las normas más representativas, sentar las bases sobre las cuales se puede desarrollar un proceso metodológico sólido; en este caso, tomando como referente las fases planteadas por la versión 2010 de la ISO/IEC 27003, las diferentes experiencias empresariales y la base bibliográfica disponible.

No obstante, es necesario iniciar con el concepto de sistema de gestión de seguridad de la información, de acuerdo con lo establecido en la ISO/IEC 27000:2018.

> Un sistema de gestión de seguridad de la información (SGSI) está compuesto de políticas, procedimientos, guías, recursos y actividades asociadas, gestionadas colectivamente por una organización, con el propósito de proteger sus activos de información. Un SGSI requiere de un enfoque sistémico para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para poder cumplir con sus objetivos. Está basado en una evaluación de riesgos y en los niveles de aceptación de riesgos de una organización diseñado para tratar y gestionar los riesgos de forma efectiva. Analizando los requerimientos para la protección de activos de información y aplicando apropiados controles para asegurar la protección de los activos de información, de acuerdo a lo requerido, contribuyendo a la implementación del SGSI. (ISO/IEC, 2018a, p. 11)

La serie ISO/IEC 27000

Las normas de la serie ISO/IEC 27000 las publica la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Estas normas contienen las mejores prácticas para la gestión de seguridad de la información en cualquier organización.

En el capítulo anterior se presentaron de forma general las normas relacionadas con la ISO/IEC 27000, por lo que a continuación se presentan de manera detallada, con miras a que una organización puede utilizar estas normas como marco de referencia de buenas prácticas y/o para la búsqueda de una certificación internacional.

En lo relacionado con la certificación internacional, es importante tener en cuenta que la norma certificable es la ISO/IEC 27001, así como las demás normas son complementarias al proceso y sirven de guía para su desarrollo.

Norma ISO/IEC 27000:2018

Esta norma, denominada formalmente *Tecnología de información-técnicas de seguridad-sistemas de gestión de seguridad de la información-marco general y vocabulario,* describe los fundamentos de un SGSI, el cual contiene los siguientes elementos:

- un marco general de la familia de estándares de un SGSI;
- una introducción a la gestión de seguridad de la información;

- términos y definiciones usados en los diferentes estándares de la familia SGSI.

Es importante destacar de esta norma los principales términos que se utilizan para la implementación de un SGSI, los cuales se requieren para evitar ambigüedades (términos descritos en el primer capítulo, sección "Lenguaje formal de un SGSI").

Relación entre las normas

La familia de estándares del sistema de gestión de seguridad de la información lo componen, aproximadamente, diecinueve normas principales, clasificadas en cuatro categorías, tal como se puede apreciar en la figura 20. Estas categorías son las siguientes:

- la norma que contiene el vocabulario, contenido en la ISO/IEC 27000;
- las normas de requerimientos, contenidos en la ISO/IEC 27001, la ISO/IEC 27006 y la ISO/IEC 27009;
- las normas guía desarrolladas a través de nueve normas: ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, TR 27008, ISO/IEC 27013, ISO/IEC 27014, TR 27016 e ISO/IEC 27021;
- y las normas para sectores específicos, contenidas en la ISO/IEC 27010, ISO/IEC 27011, ISO/IEC 27017, ISO/IEC 27018, e ISO 27019.

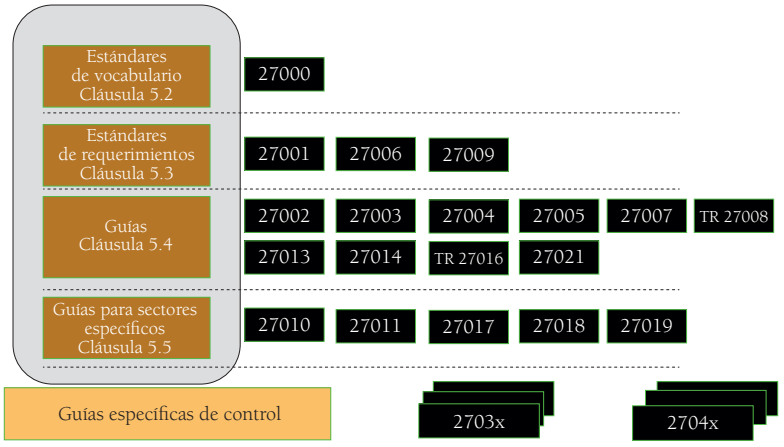

Figura 20. Relaciones entre las diferentes normas de la familia ISO/IEC 27000.
Fuente: elaboración propia a partir de ISO/IEC (2018b).

Principales normas de la familia ISO/IEC 27000 para la implementación de un SGSI

Uno de los requisitos para implementar un SGSI, bajo la perspectiva de los estándares internacionales, es conocer los estándares, su estructura y la relación que existe entre cada uno de ellos. De allí la necesidad de conocer las diferentes normas de la familia ISO/IEC 27000, su estructura y sus relaciones, para, posteriormente, estar en capacidad de plantear un esquema de implementación en el que sea posible articular cada una de ellas.

Si bien la familia de la serie ISO/IEC 27000 la componen cerca de diecinueve normas, las principales normas que sirven de referente para la implementación de un SGSI se enmarcan en cuatro de ellas, tal como se puede observar en la figura 21, las cuales se explican con cierto nivel de detalle a continuación.

Figura 21. Principales normas para la implementación de un SGSI.
Fuente: Valencia-Duque y Orozco Alzate (2017).

Norma ISO/IEC 27001:2013

Norma actualizada en 2013, denominada formalmente *Tecnología de información-técnicas de seguridad-sistemas de gestión de seguridad de la información-Requerimientos*, la cual específica los requerimientos para el establecimiento, la implementación, la operación, el monitoreo, la revisión, el mantenimiento y la mejora de un SGSI debidamente formalizado. El cumplimiento de los requerimientos de esta norma es lo que permite que una organización obtenga la certificación internacional ISO/IEC 27001.

Es importante conocer que cada país cuenta con una organización que adopta las diferentes normas ISO en su territorio y, por lo general, es idéntica en su contenido a la promulgada por la ISO Internacional. Para el caso colombiano, la entidad encargada de esta labor es el Instituto Colombiano de Normas Técnicas y Certificación (Icontec), la cual, el 11 de diciembre de 2013, adoptó de forma idéntica a la norma internacional esta norma ISO y que se denomina para Colombia como norma técnica NTC[1]- ISO/IEC 27001.

La norma NTC-ISO/IEC 27001:2013 es un documento de 34 páginas cuyos requisitos se encuentran concentrados en cerca de 12 de estas páginas, resumidos en la tabla 10, mientras que el resto del documento se concentra en el Anexo A relacionado con los objetivos de control y los controles de referencia.

Tabla 10. Estructura de la Norma ISO/IEC 27001:2013

1. Objetivo y campo de aplicación	
2. Referencias normativas	
3. Términos y definiciones	
4. Contexto de la organización	4.1 Conocimiento de la organización y de su contexto 4.2 Comprensión de las necesidades y expectativas de las partes interesadas 4.3 Determinación del alcance del sistema de gestión de seguridad de la información 4.4 Sistema de gestión de seguridad de la información
5. Liderazgo	5.1 Liderazgo y compromiso 5.2 Política 5.3 Roles, responsabilidades y autoridades en la organización
6. Planificación	6.1 Acciones para tratar riesgos y oportunidades 6.1.1 Generalidades 6.1.2 Valoración de riesgos de la seguridad de la información 6.1.3 Tratamiento de riesgos de seguridad de la información 6.2 Objetivos de seguridad de la información y planes para lograrlos

Continúa en la siguiente página ▶

1 Norma Técnica Colombiana.

7. Soporte	7.1 Recursos 7.2 Competencia 7.3 Toma de conciencia 7.4 Comunicación 7.5 Información documentada 7.5.1 Generalidades 7.5.2 Creación y actualización 7.5.3 Control de la información documentada
8. Operación	8.1 Planificación y control operacional 8.2 Valoración de riesgos de la seguridad de la información 8.3 Tratamiento de riesgos de la seguridad de la información
9. Evaluación del desempeño	9.1 Seguimiento, medición, análisis y evaluación 9.2 Auditoría interna 9.3 Revisión por la dirección
10. Mejora	10.1 No conformidades y acciones correctivas 10.2 Mejora continua
11. Anexo A. Objetivos de control y controles de referencia	Resumen de los objetivos de control y controles de la ISO/IEC 27002

Fuente: elaboración propia.

Si articulamos cada uno de los requisitos de la norma dentro del ciclo Deming o ciclo PHVA, tendremos una visión más cercana a una estructura para su implementación, tal como se puede apreciar en la figura 22.

Transición de la norma ISO/IEC 27001:2005 a la norma ISO/IEC 27001:2013

La norma ISO/IEC 27001:2013 es la primera revisión a la ISO/IEC 27001:2005, lo que, de acuerdo con diversos autores, no es un cambio estructural; tan solo se han ajustado algunos términos y elementos de la norma (BSI, 2013) en los que se han introducido nuevos conceptos, entre los que se destacan los establecidos en la tabla 11.

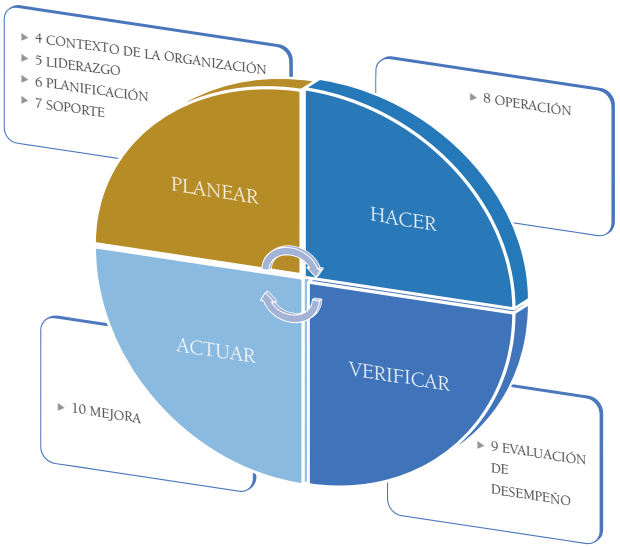

Figura 22. Numerales de la norma en función del ciclo Deming.
Fuente: elaboración propia.

Tabla 11. Conceptos nuevos de la ISO/IEC 27001:2013

Concepto nuevo o actualizado	Descripción
Contexto de la organización	El ambiente en el cual la organización opera.
Problemas, riesgos y oportunidades	Reemplaza acción preventiva.
Partes interesadas	Reemplaza *stakeholders*.
Liderazgo	Requerimientos específicos para la alta gerencia.
Comunicación	Existe un requerimiento específico para comunicaciones tanto internas como externas.
Objetivos de seguridad de la información	Los objetivos de seguridad de la información pueden establecerse en las funciones y niveles relevantes.
Evaluación de riesgos	La identificación de activos, amenazas y vulnerabilidades ya no es un requisito previo para la identificación de riesgos de seguridad de la información.
Propietario del riesgo	Reemplaza propietario de activos.

Continúa en la siguiente página ▶

Concepto nuevo o actualizado	Descripción
Plan de tratamiento de riesgos	La eficacia del plan de tratamiento de riesgos es ahora considerado más importante que la eficacia de los controles.
Controles	Los controles son ahora determinados durante el tratamiento de riesgos en lugar de ser seleccionado del Anexo A.
Información documentada	Reemplaza documentos y registros.
Evaluación de desempeño	Cubre la medición del SGSI y la eficacia del plan de tratamiento de riesgos.
Mejoramiento continuo	Se pueden usar otras metodologías diferentes al PHVA.

Fuente: BSI (2013).

Estos nuevos y actualizados elementos son importantes para aquellas organizaciones que ya cuentan con la certificación ISO/IEC 27001:2005, debido a que deben realizar un proceso de transición hacia la ISO/IEC 27001:2013.

ISO/IEC 27002: 2013

Esta norma surgió originalmente en el 2000 como ISO/IEC 17799, para, posteriormente, ser actualizada como ISO/IEC 27002:2005, y, a su vez, a la par de la actualización de la ISO/IEC 27001, ser actualizada en 2013 con cambios en cada una de ellas; básicamente, en la cantidad de controles y algunos aspectos de forma, tal como se observa en la figura 23.

Figura 23. Evolución de la norma ISO de controles de seguridad de la información.
Fuente: elaboración propia.

La ISO/IEC 27002:2013 se denomina formalmente como *Tecnología de información-técnicas de seguridad-código de prácticas para controles de*

seguridad de la información y ha sido diseñada, de acuerdo con ISO (2015), para utilizarse en organizaciones que intentan:

- seleccionar controles dentro de un proceso de implementación de un sistema de gestión de seguridad de la información basado en la ISO/IEC 27001;
- implementar controles de seguridad de la información comúnmente aceptados;
- desarrollar sus propias guías de gestión de seguridad de la información.

La estructura de los controles de seguridad de la información se encuentra conformada por 14 dominios, 35 objetivos de control y 114 controles, los cuales se encuentran divididos entre controles organizacionales, controles técnicos y controles normativos, tal como se puede apreciar en la figura 24.

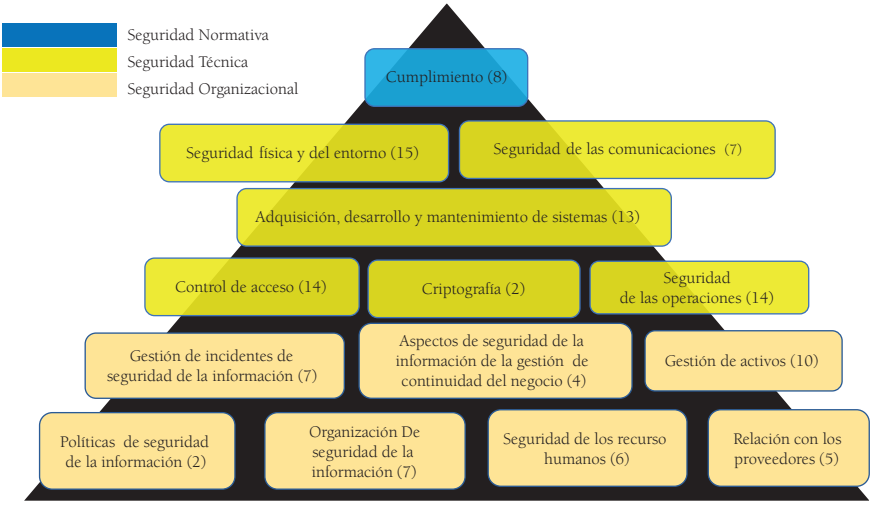

Figura 24. Estructura por dominios de la norma ISO/IEC 27002.
Fuente: Valencia Duque y Orozco Alzate (2017).

Si realizamos un análisis porcentual de los controles organizacionales, técnicos y normativos en función de su clasificación por dominios, se encuentra un 36 % de controles organizacionales, un 57 % de controles técnicos y un 7 % de controles normativos.

De igual forma, autores como Carter y Treu (2017) establecen una clasificación de los controles en función de la tríada confidencialidad, integridad y disponibilidad, mientras Shojaie, Federrath y Saberi (2014) los clasifican alrededor de la tipología de activos tecnológicos de una organización. Una combinación de ambas clasificaciones se puede observar en el Anexo 1.

Es necesario aclarar que los 114 controles propuestos como mejores prácticas en esta norma son un marco de clasificación para los controles específicos que se implementan en las organizaciones, así como su incorporación y posterior clasificación dependen de los riesgos identificados como parte del proceso de diseño del SGSI.

ISO/IEC 27003:2010

Esta norma denominada formalmente como *Tecnología de información-técnica de seguridad-guía de implementación de un sistema de gestión de seguridad de la información* tiene como objetivo servir de referencia para la especificación y diseño de un SGSI, desde su inicio hasta los planes de implementación.

Es importante aclarar que el enfoque de esta norma se ha actualizado y rediseñado en 2017. No obstante, se toma la guía originalmente propuesta por considerarla pertinente desde el punto de vista metodológico.

Esta norma se explica más adelante con mayor nivel de detalle, teniendo en cuenta que servirá de guía para explicar el método de implementación de un SGSI.

ISO/IEC 27005: 2008

Norma denominada formalmente *Tecnología de la información-técnicas de seguridad. Gestión del riesgo en la seguridad de la información* es la norma que proporciona directrices para la gestión del riesgo de la seguridad de la información, sin proporcionar metodologías específicas para tal fin.

La figura 25 presenta el esquema sugerido por la ISO/IEC 27005 para implementar el componente de gestión del riesgo como uno de los insumos esenciales para desarrollar un SGSI. Ahora, si bien existen múltiples marcos de referencia de gestión de riesgos, en su mayoría presentan los mismos elementos.

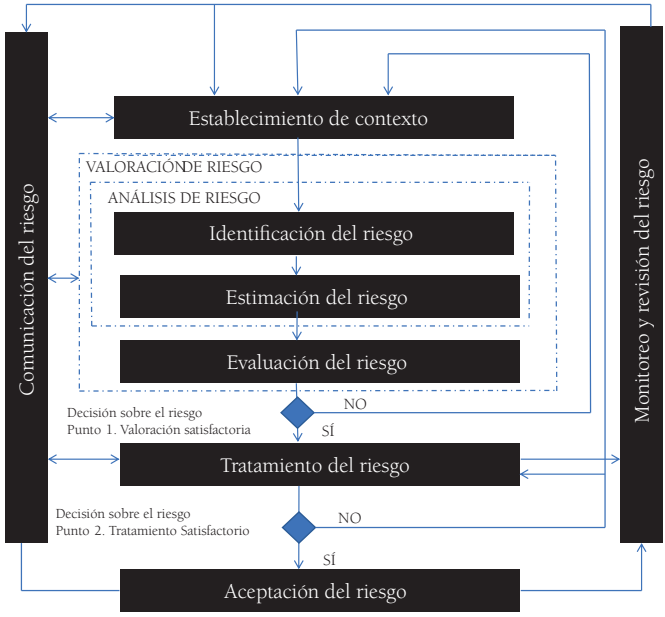

Figura 25. Estructura de gestión de riesgo propuesta en la ISO/IEC 27005.
Fuente: Icontec (2009b).

Propuesta metodológica para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000

Abordar la implementación de un sistema de gestión de seguridad de la información es una tarea prioritaria para aquellas organizaciones cuyo principal activo es la información, pues, ¿qué organizaciones no dependen hoy de este activo? Esto, además de disminuir la incertidumbre en la confidencialidad, integridad y disponibilidad de la información, trae ciertos beneficios, en caso de que su orientación no sea simplemente hacia implementar mejores prácticas, sino a obtener una certificación internacional. Entre estos beneficios, de acuerdo con Gómez Fernández y Fernández Rivero (2015), se encuentran:

- aportar un valor añadido de confianza en la protección de la información;
- asegurar una buena implementación del SGSI con base en las recomendaciones, las observaciones y la experiencia de los organismos de certificación;
- mejorar la imagen de la organización y diferenciarse de otras empresas del sector;

- cumplir con uno de los requerimientos que se exigen hoy de manera incremental en el mercado en el momento de contratar nuevos productos y/o servicios.

La literatura académica y profesional ha presentado diversas propuestas para llevar a cabo la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000. No obstante, la familia de normas cuenta con una norma específica que establece la metodología para llevar a cabo una adecuada implementación de un sistema de gestión de seguridad de la información.

El enfoque que se adoptará será la metodología propuesta por la ISO/IEC 27003:2010, denominada "Guía de implementación de un SGSI", y se combinará con la experiencia del autor y de diferentes referentes académicos.

Esta guía, tal como se puede apreciar en la figura 26, contempla cinco fases. Estas se detallan a continuación de manera que es posible comprender los pasos a desarrollar no solo desde el punto de vista conceptual, sino también metodológico, a partir de un proyecto que incorpore personas, tiempos y recursos, así como el respaldo de la alta dirección, como un requisito fundamental para cumplir los objetivos previstos.

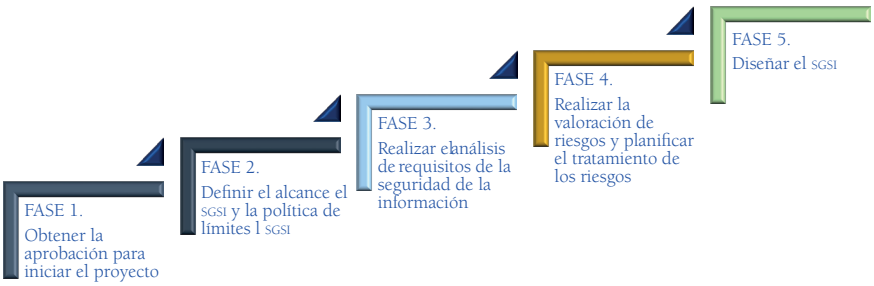

Figura 26. Fases para implementar un SGSI con base en la norma ISO/IEC 27003:2010.
Fuente: elaboración propia.

Estas cinco fases y sus diferentes etapas están alineadas con los requisitos de la norma ISO/IEC 27001, tal como se puede apreciar en la tabla 12. Su cumplimiento es obligatorio si se quiere aplicar las mejores prácticas y obtener la certificación a nivel internacional.

Tabla 12. Fases de implementación de un SGSI y su relación con los numerales de la ISO/IEC 27001:2013

Fases	Etapas	Numerales de la ISO/IEC 27001:2013 relacionadas
Obtener la aprobación de la dirección para iniciar el proyecto	Establecimiento de las prioridades de la organización para desarrollar un SGSI.	4.1 Conocimiento de la organización y de su contexto 4.2 Comprensión de las necesidades y expectativas de las partes interesadas
	Definir el alcance preliminar del SGSI.	
	Creación del plan del proyecto para ser aprobado por la dirección.	5.1 Liderazgo y compromiso 7.1 Recursos 7.4 Comunicación
Definir el alcance, los límites y la política del SGSI	Definir el alcance y los límites del SGSI.	4.3 Determinación del alcance del sistema de gestión de seguridad de la información
	Definir el alcance y los límites de las tecnologías de información y comunicaciones.	
	Definir el alcance y los límites físicos.	
	Integrar cada alcance y los límites para obtener el alcance y los límites del SGSI.	
	Desarrollar la política del SGSI y obtener la aprobación de la dirección.	5.1 Liderazgo y compromiso 5.2 Política 6.2 Objetivos de seguridad de la información y planes para lograrlos
	Definición de roles, responsabilidades del SGSI.	5.3. Roles, responsabilidades y autoridades en la organización 7.2. Competencia 7.3. Toma de conciencia
Realizar el análisis de los requisitos de seguridad de la información	Definir los requisitos de seguridad de la información para el proceso SGSI.	4.2. b) La organización debe determinar los requisitos de las partes interesadas pertinentes a la seguridad de la información
	Identificar los activos dentro del alcance del SGSI.	6.1.2 Valoración de riesgos de seguridad de la información
	Realizar una evaluación de la seguridad de la información.	

Continúa en la siguiente página ▶

Fases	Etapas	Numerales de la ISO/IEC 27001:2013 relacionadas
Realizar la valoración de riesgos y planificar el tratamiento de riesgos	Realizar la valoración de riesgos.	6.1.2 Valoración de riesgos de seguridad de la información
	Seleccionar los objetivos de control y los controles.	6.1.3 Tratamiento de riesgos de la seguridad de la información 6.2 Objetivos de seguridad de la información y planes para lograrlo
	Obtener la autorización de la dirección para implementar y operar el SGSI.	5.1 Liderazgo y compromiso
Diseñar el SGSI	Diseñar la seguridad de la información de la organización.	7.4 Comunicación 7.5 Información documentada 8.1 Planificación y control operacional 8.2 Valoración de riesgos de seguridad de la información 8.3 Tratamiento de riesgos de seguridad de la información 9.1 Seguimiento, medición, análisis y evaluación 9.2 Auditoría interna 9.3 Revisión por la dirección
	Diseñar la seguridad física y de las tecnologías de información y comunicaciones.	
	Diseñar la seguridad específica de un SGSI.	
	Producir el plan del proyecto final del SGSI.	

Fuente: elaboración propia.

A continuación, se explica en detalle cada una de estas fases, en busca de incorporar una serie de elementos prácticos que permitan poner en contexto de una forma más didáctica su implementación.

▶ Fase 1: obtener la aprobación de la dirección para iniciar el proyecto

Uno de los aspectos que se deben tener en cuenta y en ocasiones no es claro, es que un proyecto de SGSI no es solo del área de tecnologías de información, es un proyecto organizacional y como tal requiere la aprobación y el apoyo de la dirección a fin de avanzar en su adecuada implementación.

Tabla 13. Requisitos de la ISO/IEC 27001 relacionados con la aprobación de la dirección

Objetivo de la fase		
Obtener aprobación de la dirección para iniciar el proyecto SGSI mediante la definición de un caso de negocio y un plan de proyecto.		
Requisitos de la ISO/IEC 27001:2013 relacionados		
4.1 Conocimiento de la organización y de su contexto	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	
5.1 Liderazgo y compromiso	7.1 Recursos	7.4 Comunicación

Fuente: elaboración propia.

Esta fase tiene ese objetivo, de modo que para lograrlo se deben llevar a cabo las actividades que se describen a continuación.

Establecimiento de las prioridades de la organización para desarrollar un SGSI

Para llevar a cabo esta actividad, es necesario conocer a fondo las prioridades que tiene la organización para implementar un SGSI. En este sentido, se recomienda tener en cuenta los elementos que se enlistan a continuación.

- *Objetivos estratégicos de la organización*. Este elemento permitirá determinar la forma en la que un SGSI puede aportar a los diferentes objetivos de la organización y justificar aún más su necesidad como parte de la estrategia organizacional. Una vez identificados los objetivos estratégicos a los que podría aportar el SGSI, es posible establecer las líneas de negocio y los procesos involucrados que dependen de estos objetivos estratégicos.
- *Requisitos normativos o de terceros relacionados con la seguridad de la información*. Es necesario identificar los requerimientos normativos que tenga la entidad, o los requerimientos que en materia de información se tengan de terceros y requieran cumplir con criterios de confidencialidad, integridad y disponibilidad de la información. Estos requisitos son fundamentales en el propósito de complementar la necesidad de justificar un SGSI.
- *Sistemas de gestión existentes*. Con el fin de aprovechar la base instalada con la que cuenta la organización en relación con otras

normas de sistemas de gestión incorporadas en la organización, es necesario identificarlas si se tiene en cuenta que, por lo general, todas las normas de gestión basadas en las normas ISO cuenta con algunos elementos estructurales idénticos establecidos en el Anexo SL y, como tal, pueden ser compatibles con los requerimientos establecidos en la ISO/IEC 27001:2013.

Es importante que el SGSI sea parte de la estructura de gestión de la organización y se incorporé como parte de los procesos en aquellas actividades que requieren adecuados niveles de protección de la información.

Definir el alcance preliminar del SGSI

El punto de partida para desarrollar un SGSI es definir qué se quiere proteger y, con base en esto, se determina de manera preliminar el alcance que va a tener el sistema de gestión de seguridad de la información.

De acuerdo con lo establecido en la ISO/IEC 27003, el alcance preliminar de un SGSI incluye un resumen de los requisitos para la gestión de seguridad de la información establecidos por la dirección, así como de las obligaciones impuestas externamente a la organización.

Creación del plan del proyecto para ser aprobado por la dirección

Si bien la incorporación de un SGSI en la organización es una tarea permanente, el primer paso para impulsar su diseño y la implementación parte de la elaboración de un proyecto que permita definir con certeza los tiempos, los recursos y el personal requerido, utilizando para esto las diferentes herramientas de gestión de proyectos que existen en el mercado.

Al crear y administrar el proyecto de SGSI se recomienda utilizar herramientas y mejores prácticas de proyectos. Además, una vez elaborado, debería ser aprobado por el comité de seguimiento o por el comité de gerencia. De igual forma, se deben presentar por parte del director del proyecto informes de avance físico y financiero del proyecto, como una medida para monitorear permanentemente su ejecución. Un ejemplo de esquema de plan de proyecto se presenta en la figura 27.

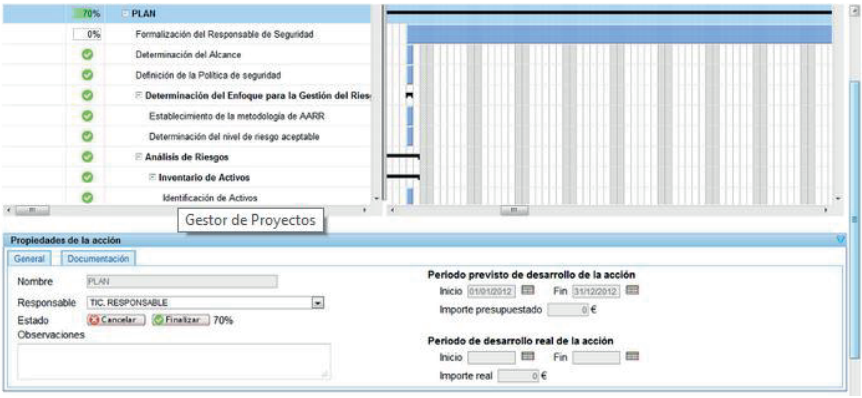

Figura 27. Ejemplo de plan de proyecto SGSI.
Fuente: Gesconsultor (2015).

Es importante tener en cuenta en la planificación el conocimiento que se puede tener de los otros sistemas de gestión implementados en la organización (ISO 9001, ISO 14000, etc.), debido a que los diferentes sistemas de gestión tienen aspectos comunes, en especial aquellos relacionados con la documentación y los registros, puesto que permitirían realizar una integración y minimizar así con esto los esfuerzos. De esta forma se requiere tan solo, en algunos casos, una ampliación de la documentación que existe para incorporar los aspectos específicos del SGSI. En este sentido, algunos autores recomiendan realizar un análisis de brecha del estado actual de los requisitos de la ISO/IEC 27001 y de los controles que existen a partir de la ISO/IEC 27002, como insumo fundamental para definir de forma apropiada la planificación del proyecto. No obstante, es importante tener en cuenta que, por lo general, muchas organizaciones incorporan controles asociados a la información y a los recursos tecnológicos sin una identificación previa de los riesgos, por lo que se deben tomar los resultados como insumos preliminares para establecer el nivel de esfuerzo requerido.

Se requiere que el líder del proyecto cuente con los recursos adecuados para abordarlo, que exista tiempo suficiente (incluso destinado a lo que salga mal) y todos comprendan los riesgos en el proyecto. Lo anterior implica gestionar el cambio que genera este nuevo proyecto y abandonar la "zona de comodidad" de muchos de los actores involucrados. Siempre existirán uno o dos que apoyan la idea de mejorar la seguridad de la información, pero, para la mayoría, será un proyecto que seguramente genera incomodidades, supone más trabajo o complica la forma en la que se llevan

a cabo muchas de las tareas cotidianas relacionadas con la gestión de la información y sus recursos tecnológicos (Calder, 2006).

Una vez formulado el proyecto para implementar el SGSI, es necesario —y muy importante—involucrar a la alta dirección de la organización, si se tiene en cuenta que es allí donde inicia el proyecto y, en últimas, se autoriza la implementación y operación del sistema de gestión de la seguridad de la información. Adicionalmente, es allí que se aprueba el presupuesto que permite llevar a cabo el plan de mitigación de riesgos resultante del análisis de estos y desarrollar realmente un proceso de mejoramiento continuo.

Es necesario que la dirección proporcione evidencias de su compromiso con los procesos y las actividades involucradas en el establecimiento, la implantación, la operación, el monitoreo, la evaluación, el mantenimiento y la mejora permanente del SGSI, de acuerdo con la cláusula 5 de la ISO 27001:2013. De esta manera, se establece la política de seguridad de la información al fijar los objetivos, asignar los papeles y las responsabilidades, la comunicación de la importancia de la gestión de seguridad de la información para el negocio, la provisión de recursos dirigidos al SGSI y la decisión sobre el nivel aceptable del riesgo.

Por último, es importante incorporar en la planeación dos elementos claves: un programa de gestión del cambio, como una buena práctica en la gestión de proyectos, así como un plan de comunicaciones que permita presentar de manera permanente el nivel de avance del proyecto y los compromisos requeridos por las diferentes instancias que están relacionadas con este.

Calder (2006) recomienda de manera particular tener en cuenta los aspectos que se enlistan a continuación relacionados con la comunicación.

- Comunicación, de arriba hacia abajo, de la visión que tiene la organización acerca de la seguridad de la información; es decir, por qué es necesario el SGSI, cuáles son las responsabilidades legales de la organización y cuáles son los beneficios esperados con su desarrollo.
- Sesiones informativas regulares para todo el personal acerca del progreso del proyecto.
- Establecer un mecanismo para garantizar que se consulte a personas o entidades estratégicas de la organización y que estos participen en el desarrollo de aspectos clave del SGSI.
- Establecer un mecanismo que permita obtener y brindar retroalimentación de manera regular por parte de las organizaciones o

personas que son terceras partes afectadas, de modo que su experiencia directa de cómo se implementó el sistema inicial pueda usarse en la evolución de la versión final.

- Incorporar comunicados permanentes a través de la intranet corporativa, en la que se publiquen reportes regulares de progreso e información detallada acerca de aspectos específicos del SGSI.

▶ Fase 2. Definir el alcance, los límites y la política del SGSI

Tabla 14. Requisitos de la ISO/IEC 27001 relacionados con el alcance y la política

Objetivo de la fase		
Definir el alcance y los límites detallados y desarrollar la política del SGSI, así como obtener el respaldo de la dirección.		
Requisitos de la ISO/IEC 27001:2013 relacionados		
4.3 Determinación del alcance del sistema de gestión de seguridad de la información	5.1 Liderazgo y compromiso	
5.2 Política	6.2 Objetivos de seguridad de la información y los planes para lograrlos	
5.3 Roles, responsabilidades y autoridades en la organización	7.2 Competencia	7.3 Toma de conciencia

Fuente: elaboración propia.

Esta fase contempla tres importantes elementos de un SGSI: la definición del alcance, la definición de la política y la aprobación por parte de la dirección, los cuales se explican a continuación.

Definición del alcance

La importancia que tiene el establecimiento de un adecuado alcance se fundamenta en que permite delimitar el proceso de gestión de riesgos y, por ende, pone el foco en todo el proceso de implementación del SGSI.

El alcance es el filtro inicial sobre el cual se determinarán los activos involucrados, las amenazas y los riesgos a contemplar, así como los controles requeridos. De allí que establecer el alcance es clave en el desarrollo del SGSI, pues no puede ser tan amplio como para que el proyecto sea inviable,

ni tan estrecho como para que el esfuerzo y la certificación (en caso de ser parte del proyecto) no tengan un valor real.

El alcance se debe determinar en función de la organización, con límites claros (definidos en términos de las características de la organización, su ubicación, sus activos y su tecnología), y al establecer aquellos aspectos que se excluyen, con su respectiva justificación.

Para establecer el alcance del SGSI, es posible establecer en función del negocio o en función de su ubicación en el caso de aquellas entidades que cuentan con varias sedes.

El alcance del SGSI puede ser un proceso, un conjunto de procesos, una sede, un servicio o un conjunto de servicios. Además, debe definirse de forma adecuada para evitar ambigüedades, teniendo presente que su definición no conlleve a un proyecto inalcanzable en términos de tiempo y recursos.

Se recomienda elaborar un diagrama de red que muestre cómo se interconectan los diferentes elementos que van a ser parte del SGSI, lo que incluye los procesos organizacionales, los servicios y/o productos involucrados, los elementos del mundo exterior con los que interactúan y los principales activos tecnológicos que se relacionan.

El producto final del alcance, por lo general, es un párrafo que resume lo que se protege en la organización y hace parte del documento de certificación entregado a aquellas entidades que logran cumplir con los requisitos exigidos.

Algunos ejemplos de alcance se presentan en la tabla 15.

Tabla 15. Ejemplos de alcance del SGSI

Entidad	Alcance SGSI	Entidad certificadora	URL de referencia
Isotools	Los sistemas de información que soportan los servicios de diseño, desarrollo y mantenimiento de aplicaciones informáticas. Alojamiento de aplicaciones informáticas. Diseño e implantación de formación en áreas de innovación y gestión empresarial, de acuerdo con la declaración de aplicabilidad en vigor.	AENOR	http://www.isotools.org/wp-content/uploads/2014/02/Certificado-SGSI_Astivia_.jpg

Continúa en la siguiente página ▶

Entidad	Alcance SGSI	Entidad certificadora	URL de referencia
Polar Technologies, S. L.	Prestación de servicios de *data center* (*housing* y *hosting*), los servicios de procesador multicanal de transacciones electrónicas, y el desarrollo de *software*.	Bureau Veritas	http://polartech.es/about/securitypolicy.htm
Libnova S. L.	Desarrollo de *software* y mantenimiento e instalación de *software* y *hardware*, de acuerdo con la declaración de aplicación versión 2 con fecha de 26 de julio de 2011.	Sgs	http://www.libnova.com/es/certificaciones.html#prettyPhoto/0/
Appser Data Engineering S. L.	Despliegue y administración de plataformas TIC avanzadas, de acuerdo con la declaración de aplicabilidad Rev. 03 de fecha 15 de julio de 2011.	Sgs	http://www.apser.es/blog/2013/01/17/nueva-certificacion-en-iso-27001-e-iso-20000/
Ecodese (Ecológica De Destrucción S. L.)	Recogida, transporte, custodia y destrucción de la información de clientes.	Bureau Veritas	http://www.ecodese.com/solvencia-garantia

Fuente: elaboración propia a partir de las fuentes referenciadas.

Definición de la política y objetivos de seguridad

De acuerdo con Díaz (2010), la política de seguridad refleja lo que la organización busca hacer con respecto a la seguridad de la información y los objetivos que pretende conseguir, con miras a los requisitos legales y reglamentarios aplicables, así como en conformidad con el compromiso de la dirección para conseguirlo.

Una política es una directriz que ayuda al cumplimiento de los objetivos, definida en función del alcance. Se encuentra contemplada como el primer control de la ISO/IEC 27002:2013, por la cual se establece, a través del control 5.1.1. —"Políticas para la seguridad de la información"— la necesidad de definir un conjunto de políticas para la seguridad de la información, aprobadas por la dirección, publicadas y comunicadas a los empleados y a las partes externas pertinentes.

Es importante tener en cuenta que la política general de seguridad de la información es una sola y, a partir de allí se pueden definir las diferentes políticas específicas en los diversos niveles, tales como la política de acceso, la política de uso de dispositivos móviles o la política de *backups*, entre otras.

La política del SGSI recoge y transmite el compromiso de la dirección a través de una declaración de intenciones de alto nivel que proporcione las bases para definir y delimitar responsabilidades dirigidas a las diversas actuaciones técnicas y organizativas que se requieran en el propósito de llevar a cabo la gestión de la seguridad de la información en la organización (Fernández Sánchez y Piattini, 2012).

Por último, es importante que la organización conozca y entienda la política de seguridad de la información como parte de las políticas organizacionales. Esto, si bien, como lo establecen Altamirano y Bayona (2017), su implementación es uno de los temas que más polémica puede generar debido a que, no obstante su existencia y que son incumplidas de forma constante por parte de las personas, son necesarias como directrices generales y particulares en los diferentes ámbitos de la seguridad de la información.

La tabla 16 presenta algunos ejemplos de políticas generales de seguridad de la información.

Tabla 16. Ejemplo de políticas generales de SGSI

Entidad	Política SGSI	URL De referencia
Isotools	Astivia adquiere con sus clientes la responsabilidad de ofrecer servicios con un nivel adecuado de confianza, con lo cual asegura el cumplimiento de la legislación vigente. Para alcanzar el citado nivel de confianza en el desarrollo de su actividad, la Dirección de Astivia es consciente de la importancia de aplicar una adecuada gestión de la seguridad de la información en sus tres dimensiones: confidencialidad, integridad y disponibilidad.	http://www.spiritsa.com.ar/SEGURIDAD.pdf
Sonda	La Dirección de Sonda Uruguay reconoce la importancia de identificar y proteger los activos de información de la organización, de manera que evita la destrucción, divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, estrategia, gestión y otros conceptos relacionados. En consecuencia, se compromete a desarrollar, implantar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información (SGSI) con el objetivo de asegurar la confidencialidad, disponibilidad e integridad de la información.	http://www.sonda.com/media/docs/PO-S-4.2.1-02-Politica-de-Seguridad-de-la-Informacion.pdf

Continúa en la siguiente página ▶

Entidad	Política SGSI	URL De referencia
Artesanías de Colombia	La información es el activo más preciado de las empresas y de las entidades, en general, por tanto, se deben tomar todas las precauciones necesarias, a fin de mantener y preservar información. En este propósito Artesanías de Colombia S. A. ha desarrollado y evolucionado su modelo de seguridad de la información soportado en tres pilares fundamentales: confidencialidad, integridad y disponibilidad. Asimismo, ha adoptando buenas prácticas en cuanto a la gestión y la administración de las tecnologías de la información.	http://artesaniasdecolombia.com.co/PortalAC/images/politica-seguridad-informacion-proteccion-datos-personales.pdf

Fuente: elaboración a partir de las fuentes referenciadas.

En cuanto a los objetivos de seguridad, es importante delimitar los dos tipos de objetivos que contempla un SGSI: los objetivos generales del sistema y los objetivos de control resultantes del proceso de análisis y valoración de riesgos.

Al menos en esta primera parte se deben definir los objetivos generales que busca la implementación del sistema de gestión de seguridad de la información, articulado con las políticas y dentro del alcance previsto.

Aprobación de la dirección

La seguridad de la información es un tema gerencial relacionado con la adecuada gobernabilidad de una organización. De allí la importancia de vender el proyecto como parte de la estrategia empresarial, no como un proyecto de TI. A partir de esto, la implementación de un SGSI dependerá por completo del apoyo real de la alta dirección de la organización; sin este apoyo no existe probabilidad de éxito del proyecto.

El apoyo brindado por la dirección debe ser real, no solo con palabras, pues esto se traduce en la asignación de los recursos financieros y humanos que requiere el proyecto, en proporcionar la atención necesaria a este cuando se requiera, en comunicar a la organización y, en particular, al comité de gerencia la importancia del proyecto, así como en delegar a una persona del nivel directivo para ser el representante de la gerencia ante el proyecto.

De igual forma, se recomienda conformar un comité de seguimiento liderado por el representante de la dirección que lleve a cabo reuniones periódicas para tomar decisiones estratégicas alrededor del proyecto.

Una de las formas de demostrar el apoyo de la dirección de manera inicial es la aprobación que da la dirección de las políticas y objetivos del SGSI dentro del alcance. De allí que el numeral 5.1., literal a), de la ISO/IEC 27001:2013, establece como parte del compromiso de la dirección el aseguramiento que esta hace del establecimiento de la política y los objetivos de la seguridad de la información, además de que estos sean compatibles con la dirección estratégica de la organización.

Definición de roles, responsabilidades del SGSI

En general, toda la organización debe ser responsable de la seguridad de la información, en cabeza de la alta dirección. No obstante, es necesario delimitar con claridad responsabilidades a través de la adecuada identificación de los roles que deben desempeñar como parte de todo el sistema de gestión.

El control 6.1.1. —"Roles y responsabilidades para la seguridad de la información"— de la ISO/IEC 27002:2013 establece la necesidad de definir y asignar todas las responsabilidades de seguridad de la información, las cuales deberían fijarse de acuerdo con las diversas políticas de seguridad de la información, mediante la identificación de responsabilidades para la protección de activos individuales y con el fin de llevar a cabo procesos de seguridad específicos. Es necesario que las personas que desempeñan los diversos roles asignados cuenten con la capacidad de cumplir con tales responsabilidades, para lo cual se les debe brindar oportunidades de mantenerse actualizados.

Algunos de los roles asociados a un sistema de gestión de seguridad de la información se presentan en la tabla 17. Sin embargo, tal como lo establecen Gómez Fernández y Fernández Rivero (2015), el marco organizacional para la gestión de la seguridad de la información depende de la organización interna y las jerarquías establecidas en la entidad, por lo que deberían contemplarse, como mínimo, un responsable de seguridad de la información y un comité de seguridad que resuelva asuntos interdisciplinarios y apruebe directrices y normas.

Tabla 17. Algunos roles asociados directamente a un SGSI

Rol	Descripción del rol
Comité directivo (alta dirección)	De acuerdo con lo establecido en el numeral 5.3. de la ISO/IEC 27001, la alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen. De igual forma, de acuerdo con el numeral 9.3, es responsable de revisar el sistema de gestión de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continua.
Representante de la gerencia ante el SGSI	Miembro delegado de la alta dirección, cuya responsabilidad es asegurarse de que el SGSI se implemente y mantenga, e informar a la alta dirección de forma permanente su estado.
Comité de seguridad de la información o equivalente	Responsable de la aprobación de las diversas directrices y normas asociadas a la seguridad de la información, así como de aprobar el plan de mitigación de riesgos del SGSI.
Oficial de seguridad de la información o equivalente	Por lo general, es el responsable de coordinar todas las actividades relacionadas con la gestión de la seguridad de la información.
Propietario de activos de información	De acuerdo con lo establecido en la ISO/IEC 27002:2013, en su numeral 8.1.2., todos los activos que hacen parte del inventario de la organización deben tener un propietario, quien deberá: asegurarse de que los activos este inventariados, asegurarse de su clasificación y adecuada protección, dar cumplimiento a las restricciones establecidas a través de las diferentes políticas de control de acceso definidas y asegurarse de su adecuado manejo cuando este se elimina o destruye.
Custodio de los activos de información	Rol delegado por el propietario de los activos de información para salvaguardar sus activos.
Usuarios de la información	Personas que utilizan la información y los activos tecnológicos en la entidad para la normal ejecución de sus procesos.
Auditores de SGSI	Responsables de llevar a cabo auditorías internas a intervalos planificados con miras a proporcionar información acerca del estado actual del sistema de gestión de seguridad de la información.

Fuente: elaboración propia.

Fase 3. Realizar el análisis de los requisitos de seguridad de la información

Tabla 18. Requisitos de la ISO/IEC 27001 relacionados con el análisis de requisitos de seguridad

Objetivo de la fase	
Definir los requisitos más importantes que debe sustentar el SGSI e identificar los activos de información.	
Requisitos de la ISO/IEC 27001:2013 relacionados	
4.2. b) La organización debe determinar los requisitos de las partes interesadas pertinentes a la seguridad de la información	6.1.2 Valoración de riesgos de seguridad de la información

Definir los requisitos de seguridad de la información para el proceso SGSI

De acuerdo con lo establecido en la ISO/IEC 27003:2010 para determinar los requisitos de seguridad de la información se deben tener en cuenta cinco elementos:

- identificación preliminar de los activos de información importantes y la protección de la seguridad de la información actual.
- identificación de las visiones de la organización y la determinación de sus efectos sobre los futuros requisitos de procesamiento de información;
- el análisis de las formas actuales de procesamiento de información, las aplicaciones de sistemas, las redes de comunicación, la ubicación de las actividades y los recursos de TI;
- la identificación de todos los requisitos esenciales (requisitos legales y reglamentarios, obligaciones contractuales, requisitos de la organización, normas de la industria, acuerdos con clientes y proveedores, condiciones de pólizas de seguros, y demás requisitos propios de la organización);
- identificación del nivel de toma de conciencia sobre seguridad de la información y, a partir de este, obtener los requisitos de formación y educación de la organización.

Estos requisitos son los que justifican la necesidad de contar con un sistema de gestión de seguridad de la información en la organización.

Identificar los activos dentro del alcance del SGSI

Los activos en el contexto del SGSI, según la ISO/IEC 13335-1:2004 —*Tecnología de información -técnicas de seguridad-gestión de seguridad de tecnologías de información y comunicaciones-parte 1: conceptos y modelos de para la gestión de la seguridad de tecnologías de información y comunicaciones*—, son cualquier cosa que tiene valor para la organización. En general, un activo es cualquier información, proceso o sistema relacionado con el tratamiento de esta que tenga *valor* para la organización.

Tal como se presenta en capítulos previos de este texto, existen diversas clasificaciones de los activos tecnológicos. Así, por ejemplo, la ISO/IEC 27005 diferencia dos tipos de activos: activos primarios y activos de soporte. Los activos primarios son los procesos de negocio y la información, mientras que los activos de soporte son aquellos de los cuales dependen los activos primarios y se clasifican en: *hardware*, *software*, redes, personal, ubicación y estructura de la organización.

Por su parte, Magerit establece una clasificación basada en capas tecnológicas interdependientes, en conformidad con que existen dependencias entre activos que forman árboles o grafos de dependencia en los que la seguridad de los activos que se encuentran más arriba en la estructura o superiores dependen de los activos más abajo o inferiores (Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica, 2012).

Además de identificar y clasificar los activos según sus requerimientos de seguridad (y su criticidad para el negocio), se debe identificar quién es el propietario (o dueño) de ese activo, quien será el responsable por su seguridad, de modo que puede delegar actividades o poder sobre la gestión de controles sobre este, pero no podrá transferir (ni delegar) la responsabilidad.

Es importante una vez realizado el inventario de los activos llevar a cabo su clasificación, para efectos de estar en capacidad de tipificar los activos de información con los que cuenta una organización y establecer, en función de su clasificación, controles similares para todos los activos que hacen parte de la respectiva clasificación (esto es, control de acceso para los activos que hacen parte de la clasificación de sistemas de información).

El control 8.1.1. —"Inventario de activos"— de la ISO/IEC 27002:2013 establece la necesidad de elaborar y mantener un inventario de la información, los activos asociados a la información y las instalaciones de procesamiento de la información. De igual forma, a través del control 8.1.2. —"Propiedad de los activos"— establece la importancia de establecer su propietario y como parte de dicho inventario, llevar a cabo una clasificación de cada uno de ellos, de acuerdo con lo establecido en el control 8.2.1. —"Clasificación de la información"—.

Un ejemplo de la información mínima que debería contener una ficha de identificación de activos tecnológicos se presenta en la figura 28.

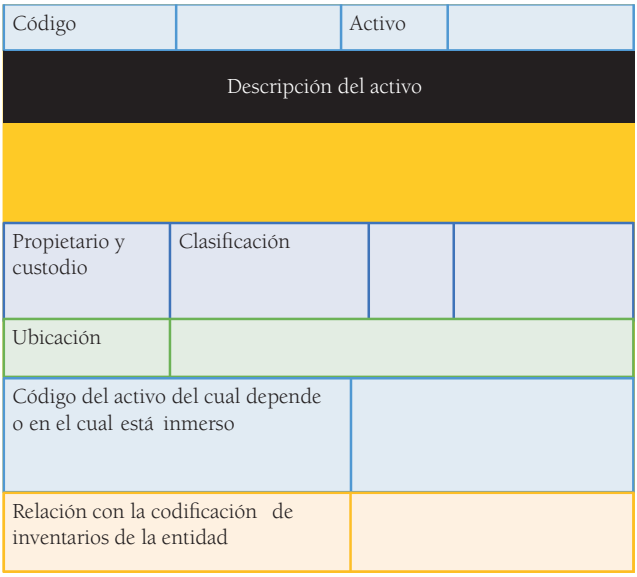

Figura 28. Ejemplo de información mínima que debería tener una ficha de identificación de activos tecnológicos.

Fuente: elaboración propia.

Clasificación y determinación del nivel de importancia de los activos tecnológicos

Es necesario establecer la importancia que representa para la organización cada uno de los activos tecnológicos con los que cuenta, si se tiene presente que cada activo representa un nivel de importancia diferente. Este nivel de

importancia puede medirse en función del valor con el que se adquirió, o en función del nivel de dependencia de los activos que lo preceden, de acuerdo con el nivel de importancia para el negocio o, incluso, algunos autores establecen su importancia en relación con la tríada confidencialidad, integridad o disponibilidad.

Una propuesta para tal fin es adoptar un enfoque *top-down* dirigido a la identificación de activos tecnológicos a partir del proceso organizacional y haciendo uso del concepto de dependencia entre activos. El enfoque *top-down* estará representado tal como se puede apreciar en la figura 29, en la cual se observan dos grandes categorías de activos: los activos primarios y los activos de soporte.

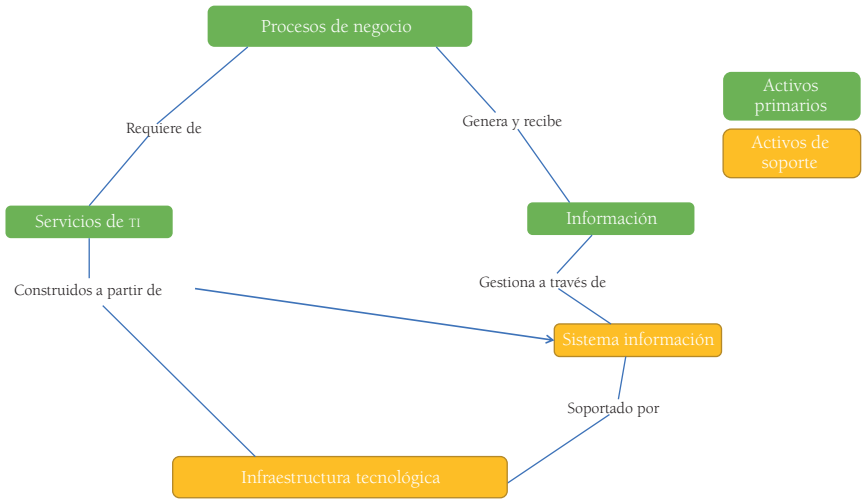

Figura 29. Estructura general de desglose de activos de información.
Fuente: elaboración propia.

En función de lo anterior, el principio sobre el que se deberá construir el inventario de activos que hacen parte del alcance del SGSI a implementar será el principio de dependencia. Para esto se debe tener en cuenta los niveles a los que pertenecen las diferentes categorías de activos, de acuerdo con la clasificación propuesta en la tabla 16 explicada en el primer capítulo de este libro.

Tabla 19. Propuesta de estructura de desglose de clasificación de activos del SGSI

Nivel	Representación	Activos dentro del alcance del SGSI	Descripción
0	[P]	Procesos de negocio	Procesos críticos de negocio que se encuentra dentro del alcance del SGSI.
1	[S]	Servicios	Servicios de tecnologías de información y comunicaciones.
1	[I]	Información del proceso	Categorías de información que hacen parte del proceso.
2	[sit]	Sistemas de información transaccional	Sistemas que automatizan la información de procesos de negocio.
2	[SIA]	Sistemas de información de apoyo	Sistemas de información que no están en relación directa con los procesos de negocio pero que apoyan diversos procesos tecnológicos. (p. ej., antivirus, compiladores, etc.).
3	[BD]	Bases de datos	Sistemas gestores de bases de datos que soportan los diferentes sistemas de información de la empresa.
4	[SO]	Sistemas operativos	Sistemas operativos cliente y servidor sobre los cuales reposan los sistemas de información transaccional, de apoyo y los respectivos sistemas gestores de bases de datos.
5	[PC]	Computador personal y periféricos	Los computadores de escritorio y periféricos que utilizan los usuarios.
6	[S]	Servidor	Equipos especializados físicos o virtuales que permiten diversas operaciones informáticas en la organización y sobre los cuales se desarrollan funciones especializadas (p. ej., procesamiento, almacenamiento, impresión, correo, etc.).
7	[IR]	Infraestructura de red	Dispositivos activos y pasivos que conforman la red de la organización.
8	[DC]	Data center	Los diferentes centros de cómputo que tiene la organización.
9	[E]	Sistemas de energía	Los diferentes componentes de energía que permiten el funcionamiento de los diferentes componentes de cómputo.

Fuente: elaboración propia.

Realizar una evaluación de la seguridad de la información

Antes de abordar de manera directa un proceso de implementación de un sistema de gestión de seguridad de la información, se recomienda llevar a cabo un diagnóstico del estado actual de la seguridad de la información con el fin de establecer las brechas existentes con los requerimientos de la ISO/IEC 27001, incluido su anexo.

Lo anterior permite determinar el nivel de esfuerzo requerido en su implementación, si se tiene en cuenta que, por lo general, muchas organizaciones que van a iniciar este tipo de proyectos, frente a la obtención de la certificación internacional, pues cuentan con otros sistemas de gestión certificados, lo que les permite tener avances en algunos requerimientos de la norma, además de la cultura de la gestión basada en ISO.

▶ Fase 4. Realizar la valoración de riesgos y planificar el tratamiento de riesgos

Tabla 20. Requisitos de la ISO/IEC 27001 relacionados con la valoración y el tratamiento de riesgo

Objetivo de la fase	
Definir la metodología para valorar los riesgos, identificar, analizar y evaluar los riesgos de seguridad de la información para seleccionar las opciones de tratamiento de riesgos, los objetivos de control y los controles.	
Requisitos de LA ISO/IEC 27001:2013 relacionados	
5.1 Liderazgo y compromiso	6.1.2 Valoración de riesgos de seguridad de la información
6.1.3 Tratamiento de riesgos de seguridad de la información	6.2 Objetivos de seguridad de la información y planes para lograrlo

Fuente: elaboración propia.

La valoración del riesgo es parte fundamental del SGSI, de allí que sea importante adoptar un enfoque para su desarrollo, así como definir de forma adecuada y a conciencia los parámetros de gestión del riesgo (tanto los parámetros de probabilidad como los parámetros de impacto), y en especial los criterios de aceptabilidad del riesgo, ya que es este el que determina el apetito real del riesgo de la organización y establece los niveles de riesgo a los que puede estar expuesta.

Sin duda, este es el eje principal del SGSI, y, tal como se presentó previamente, el principal referente es la norma ISO/IEC 27005. No obstante, existen diversos modelos que pueden ser utilizados para tal fin, tal como se expone en la tabla 21.

Tabla 21. Modelos de gestión de riesgos para la seguridad de la información

Metodología	Descripción	Organización	País	Año
ISO TR 13335:1997	Tecnología de la información-guías para la gestión de la seguridad de TI	ISO	Internacional (Suiza)	1997
ISO 27005:2008	Tecnologías de la información-técnicas de seguridad-gestión del riesgo de seguridad de la información	ISO	Internacional (Suiza)	2008
UNE 71504:2008	Metodología de análisis y gestión de riesgos para los sistemas de información	AENOR-Asociación Española de Normalización y Certificación	España	2008
BS 7799-3:2006	Sistemas de gestión de seguridad de la información-Parte 3: Guías para la gestión de riesgos de seguridad de la información	BSI-British Standards Institution	Reino Unido	2006
AS/NZS 4360:2004	Gestión de riesgos	AS/NZS-Australian Standards/New Zealand Standards	Australia/ Nueva Zelanda	2004
MAGERIT	Metodología de análisis y gestión de riesgos de IT	Ministerio de Administraciones Públicas	España	2006
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation	Universidad de Carnegie Mellon	Estados Unidos	2001-2007
CRAMM	CCTA Risk Analysis and Management Method	CCTA-Central Computing and Telecommunication Agency	Reino Unido	2003

Continúa en la siguiente página ▶

Metodología	Descripción	Organización	País	Año
NIST SP 800-30	Guía de gestión de riesgos para sistemas de tecnología de información	NIST-National Institute of Standards and Technology	Estados Unidos	2002
IRAM	Information Risk Analysis Methodologies	ISF-Information Security Forum	Internacional (Reino Unido)	2006
CORAS	Construct a platform for risk analysis of security critical systems	SINTEF y otros	Europeo (Noruega)	2001-2007
SOMAP	Security Officers Management & Analysis Project	SOMAP.org	Internacional (Suiza)	Beta
FAIR	Factor Analysis of Information Risk	Risk Management Insight	Estados Unidos	2005

Fuente: Matalobos (2009).

Sin embargo, y teniendo presente que existe una norma ISO para la gestión del riesgo de TIC, se utilizará como referente para el desarrollo de esta fase las etapas establecidas en la norma ISO/IEC 27005:2009, las cuales se resumieron en capítulos previos y se explicarán en detalle a continuación.

Establecimiento de contexto

Esta fase contempla la preparación de los diferentes elementos que requiere el proceso de gestión de riesgos de seguridad de la información, a partir del contexto, el alcance, las políticas, los objetivos y los parámetros de evaluación. La mayoría de ellos definidos en secciones anteriores. Una técnica recomendada para establecer el contexto en el ámbito específico en el que se va a desarrollar la gestión del riesgo tecnológico es utilizar la matriz DOFA (debilidades, oportunidades, fortalezas, amenazas) y, a partir de allí, iniciar el proceso de identificación de riesgos tomando como principales referentes de base las debilidades y las amenazas.

Con el objetivo de llevar a cabo una actividad de evaluación se requiere asignar valores. Además, con el fin de establecer estos valores de evaluación en conformidad con las condiciones de la organización, se deben establecer parámetros para evaluar los riesgos que deben ser racionales y fáciles de utilizar a lo largo del proceso de implementación del SGSI.

Estos parámetros de referencia son los siguientes: parámetros de probabilidad, parámetros de impacto, vulnerabilidad y criterios de aceptación del riesgo.

Parámetros de probabilidad

Debe establecerse una tabla de frecuencias para los eventos adversos esperados (amenazas), con suficientes niveles o rangos para que sea fácil y confiable. Por lo general, se utilizan tablas con un mínimo de tres niveles y un máximo de seis. A cada nivel se le asigna un valor de referencia cuyo único requisito es que a mayor frecuencia dicho valor sea más alto; se recomienda una escala lineal con valores enteros, consecutivos y pequeños: 1, 2, 3, 4, 5, etc. A cada nivel se le asigna un nombre que facilite su aplicación y, adicionalmente, se establecen criterios de valoración basados en el número de veces que ha ocurrido o puede llegar a ocurrir, por lo general, en el periodo de un año. La tabla 22 presenta un ejemplo de estos parámetros.

Tabla 22. Ejemplo de parámetros de probabilidad de ocurrencia

Probabilidad de ocurrencia de la amenaza		
A	100 %	Alta, certera
M+	75 %	Mayor, probable, esperado que ocurre
M	50 %	Posible, se espera que no ocurra regularmente
M-	25 %	No esperado, pero podría ocurrir algunas veces
B	10 %	Remoto, puede ocurrir en circunstancias excepcionales

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones (2011).

Parámetros de impacto

La gravedad de un siniestro no radica tan solo en cuánto dinero pueda perderse, por ejemplo, sino en cómo los diferentes eventos que surgen en la organización y que están relacionados con la información pueden llegar a afectarla en su conjunto, en algunos procesos o en algunas áreas.

Los parámetros de impacto se definen en función de las consecuencias que podría tener cualquier amenaza sobre la información o los activos de información en lo relacionado con la confidencialidad, la integridad y la disponibilidad, tal como se ha explicado en los apartados anteriores.

Algunos ejemplos de parámetros de impacto son los que establece la NIST, tal como se puede observar en la tabla 23.

Tabla 23. Parámetros para medir el impacto de la tríada CIA, de acuerdo con el NIST

Bajo	Moderado	Alto
	Confidencialidad	
La divulgación no autorizada de información podría tener un efecto adverso *limitado* sobre las operaciones de la organización, los activos relacionados o sus individuos.	La divulgación no autorizada de información podría tener un efecto adverso *serio* sobre las operaciones de la organización, los activos relacionados o sus individuos.	La divulgación no autorizada de información podría tener un efecto adverso *severo o catastrófico* sobre las operaciones de la organización, los activos relacionados o sus individuos.
	Integridad	
La modificación o destrucción no autorizada de información podrían tener un efecto adverso *limitado* sobre las operaciones de la organización, los activos relacionados o sus individuos.	La modificación o destrucción no autorizada de información podrían tener un efecto adverso *serio* sobre las operaciones de la organización, los activos relacionados o sus individuos.	La modificación o destrucción no autorizada de información podrían tener un efecto adverso *severo o catastrófico* sobre las operaciones de la organización, los activos relacionados o sus individuos.
	Disponibilidad	
La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso *limitado* sobre las operaciones de la organización, los activos relacionados o sus individuos.	La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso *serio* sobre las operaciones de la organización, los activos relacionados o sus individuos.	La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso *severo o catastrófico* sobre las operaciones de la organización, los activos relacionados o sus individuos.

Fuente: elaboración propia a partir de NIST (2004).

O bien, los establecidos por el Gobierno argentino, tal como se pueden visualizar en la tabla 24.

Tabla 24. Parámetros de impacto de un SGSI en el Gobierno argentino

	Confidencialidad	Integridad	Disponibilidad
	La información es:	Debido a modificaciones no autorizadas en la información:	El no poder acceder a la información genera:
Criticidad	Concepto	Concepto	Concepto
Nula (1)	Pública	Se puede reparar fácilmente	No afecta
Baja (2)	Reservada (uso interno)	Se puede reparar aunque puede dejar algunas pérdidas.	Durante un periodo de tiempo no menor a una semana podría causar pérdidas significativas.
Media (3)	Reservada (confidencial)	Es difícil su reparación y puede dejar pérdidas irreparables.	Durante un periodo de tiempo no menor a un día podría causar pérdidas significativas.
Alta (4)	Reservada (secreto)	No puede repararse dejando grandes pérdidas.	Durante un periodo de tiempo no menor a una hora podría causar pérdidas significativas.

Fuente: ajustado a partir de Oficina Nacional de Tecnologías de Información, Subsecretaría de Gestión Pública (Argentina) (2005).

Vulnerabilidad

Para determinar la importancia relativa de los riesgos se establece un nuevo parámetro para medir el impacto que una amenaza podría tener sobre la organización. Esta medida establece qué tan grave sería que se materialice una amenaza y cómo podría llegar a afectar la información empresarial, así como los activos tecnológicos que la soportan en términos de confidencialidad, integridad y disponibilidad. Esta medida genérica se conoce como *vulnerabilidad* y se mide en términos porcentuales, en función de los dos parámetros definidos previamente (probabilidad e impacto). Para esto se utiliza la siguiente fórmula:

$$Vx = (P \times I) / \text{máximo } (P \times I) \quad (1)$$

Donde:

Vx: vulnerabilidad del escenario de riesgo *X*

P: probabilidad de ocurrencia

I: impacto

Criterios de aceptabilidad del riesgo

Los criterios de aceptación de riesgo permiten establecer el apetito de riesgo que tiene la organización y corresponde a los parámetros para determinar si un riesgo es aceptable.

La determinación por parte de la organización de lo que es *suficientemente seguro* es lo que delimita el nivel de seguridad de la empresa y los principales recursos y esfuerzos a desarrollar a fin de mantenerse en este estado.

Es claro que la mayor dificultad en la determinación de las condiciones de seguridad de una organización radica en el hecho de definir los parámetros de "aceptabilidad", puesto que la coincidencia de múltiples intereses, así como la evaluación que realizan personas con diferentes niveles de conocimientos, experiencia y "emotividad" genera diversas percepciones sobre este.

La definición de *que es suficientemente seguro* es lo que determinará los objetivos de la seguridad, los esfuerzos y recursos requeridos para lograrlo.

Es por lo anterior que, en la práctica, la única forma real de determinar la "seguridad requerida" es establecer parámetros de medición de los niveles de aceptabilidad del riesgo (también llamado por algunos autores "apetito de riesgo"), mediante el consenso entre los especialistas y la gerencia, con lo cual se logra mantener la subjetividad en niveles racionales. Con el fin de compatibilizar todos los intereses existentes en la organización, es necesario que el equipo del SGSI, en compañía de la alta dirección, determine la aceptabilidad del riesgo de forma coherente (Vanegas y Pardo, 2014).

Unos criterios de aceptabilidad del riesgo, en el que el criterio más bajo de aceptación del riesgo sea muy alto, puede generar una baja cantidad de riesgos críticos en la organización y, a su vez, un criterio muy bajo pone una gran cantidad de riesgos críticos que deben tratarse. En este sentido, se requieren unos criterios de aceptabilidad ajustados a la organización, con conocimiento de las consecuencias que tiene su aplicación en el conjunto del proceso de gestión de riesgos y con sus efectos finales en el SGSI, para lo cual se recomienda realizar simulaciones con algunos de los riesgos más críticos y menos críticos que considera la organización pueden ocurrir, y a partir de allí, ajustarlo a la realidad y a las necesidades de la organización. Un ejemplo de criterios de aceptabilidad del riesgo se puede observar en la tabla 25.

Tabla 25. Ejemplo de criterios de aceptabilidad del riesgo

Criterio	Descripción	
Aceptable	Vulnerabilidad inferior al 20 %	Riesgos que acepta la organización y requiere el seguimiento y mejora de los diferentes controles existentes. Por lo general, no requiere la incorporación de nuevos controles.
Tolerable	Vulnerabilidad mayor al 20 % y menor al 50 %	Riesgos que requieren tratarse a través de la incorporación de controles que permitan disminuir la probabilidad o el impacto para llevarlos a un nivel aceptable de riesgo.
Inaceptable	Vulnerabilidad superior al 50 %	Riesgos críticos, prioritarios para la organización, que deben ser intervenidos lo más pronto posible.

Fuente: elaboración propia.

Valoración del riesgo

La valoración del riesgo, de acuerdo con lo establecido en la ISO 31000 y la ISO/IEC 27005 contempla tres fases: identificación de los escenarios de riesgo, estimación del riesgo y evaluación del riesgo.

Identificación de escenarios de riesgo

El propósito de la identificación de riesgos es determinar qué podría suceder que cause una pérdida potencial y llegar a comprender cómo, dónde y por qué podría ocurrir esta pérdida (Icontec, 2009b).

Si partimos del concepto de riesgo, tal como lo plantea la ISO/IEC 27000, como la incertidumbre sobre los objetivos, esta incertidumbre se materializa a través de la identificación de los eventos que pueden llevar al incumplimiento de objetivos; estos eventos se definen, tradicionalmente, como amenazas.

La identificación de riesgos es una de las fases más críticas en el proceso de seguridad de la información, de allí la necesidad de utilizar técnicas apropiadas para su adecuada identificación. Autores como Mejía Quijano (2013) dedican un libro a explicar las diferentes técnicas/metodologías para llevar a cabo una adecuada identificación del riesgo, las cuales se resumen en la tabla 26.

Tabla 26. Técnicas/metodologías para llevar a cabo un proceso de identificación de riesgos

Técnica/metodología	Descripción general
Lluvia de ideas	Identificación de riesgos y de sus características de forma grupal.
Análisis causa efecto	Identificación de causas y efectos de un riesgo.
Listas de chequeo y cuestionarios	Identificación de riesgos con guías estandarizadas, amplias y ajustables a todo tipo de empresa pueden ayudar a elaborar el catálogo general de riesgos de una empresa.
Inspección	Identificación de los riesgos que pueden ser observados en las instalaciones o en el desarrollo de un proceso.
Entrevista	Identificación de riesgos que requieren el conocimiento y la experiencia de personas clave.
Flujograma	Identificación de riesgos en los procesos.
Análisis de modo y efecto de falla (AMEF)	Identificación de posibles formas en las que puede fallar el diseño o la operación de procesos, productos o servicios y los efectos de estas fallas.
Análisis de información	Identificación de riesgos a través del análisis de información financiera, manuales técnicos, registros de siniestralidad y otros eventos, así como del estudio de contratos laborales y comerciales.
Método Delphi	Identificación de riesgos que requieren grupo de expertos y opiniones independientes.
Análisis de escenarios	Identificación de riesgos estratégicos.
Risicar	Identificación de riesgos operativos en procesos, actividades, procedimientos, productos, instalaciones, cargos o funciones.
Prest	Identificación de riesgos en la planeación estratégica.

Fuente: Mejía Quijano (2013).

Como propuesta metodológica para la adecuada construcción de un riesgo se acude en el presente texto al término *escenario de riesgo*, entendido como cualquier situación que describen personas competentes, responsables de identificarlas y se construye en un contexto, con dos componentes estructurales para su adecuada identificación: las amenazas y los activos de información afectados. El escenario de riesgo debe ser coherente y entendible por todas las personas relacionadas con el ámbito específico en el que

se desarrolla el análisis de riesgo a efectos de estar en capacidad de realizar una adecuada valoración. Ejemplos de escenarios de riesgo de tecnologías de información se presentan en la figura 30.

Identificación de amenazas

Todas las organizaciones, durante su existencia, están sometidas de forma permanente a amenazas (eventos adversos o situaciones con potencial de generar consecuencias negativas) de diversa índole, ya sean de origen natural (p. ej., terremotos), tecnológico (p. ej., incendios) o social (p. ej., atentados) que pueden afectar sus objetivos críticos. Estas amenazas, en el contexto del SGSI, pueden afectar los activos relacionados con la información que ayudan a cumplir los objetivos de la organización.

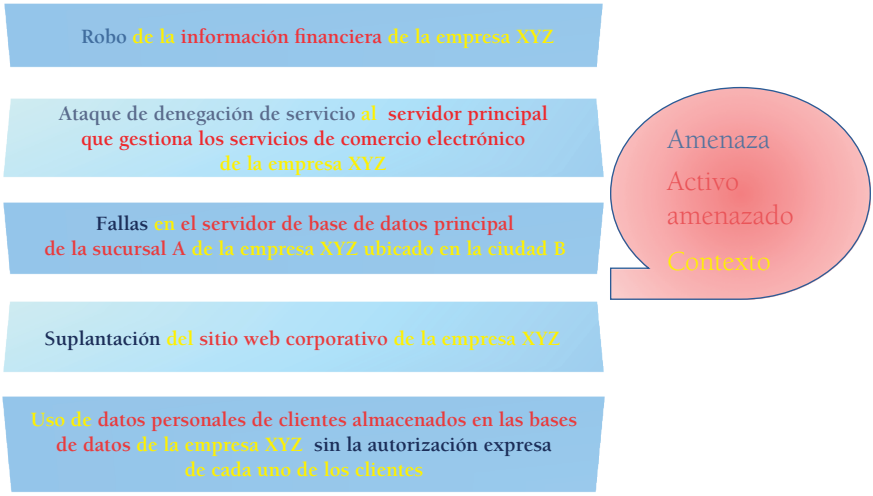

Figura 30. Ejemplos de escenarios de riesgo de tecnologías de información.
Fuente: elaboración propia.

La comunidad académica y profesional ha desarrollado durante los últimos años trabajos relacionados con la identificación de amenazas en diferentes ambientes tecnológicos. Tal es el caso de los de Albanese, López y Sánchez (2013); Georgiou y Lambrinoudakis (2015) para amenazas asociadas al *cloud computing*; Sonchan y Ramingwong (2014) en relación con amenazas asociadas a proyectos de *software*; Iqbal, Farid, Qadir y Khan (2017) para proyectos de tercerización de TI; y el de Aloini, Dulmin y Mininno

(2007) con respecto a proyectos de ERP. De igual forma, las diversas encuestas y estudios de seguridad de la información que cada año elaboran diferentes entidades tales como Cisco, IBM, Deloitte, ACIS, Ernst & Young o PWC, aportan a la identificación de las amenazas que se presentan en las diversas organizaciones que son objeto de estudio por parte de estas entidades.

A partir de estos referentes, las organizaciones pueden construir catálogos de amenazas específicos que permitan a los responsables de identificar los riesgos tomarlos como referencia en el contexto de su organización.

Algunos ejemplos de catálogos de amenazas genéricas en el ámbito de tecnologías de información se presentan en la tabla 27, proporcionados por la ISO/IEC 27005, o los establecidos en Magerit, el repositorio de vulnerabilidades del Gobierno de los Estados Unidos y el repositorio de vulnerabilidades del Instituto de Ingeniería de Software (SEI) de la Universidad Carnegie Mellon, entre otros.

Tabla 27. Ejemplos de amenazas comunes establecidos en la ISO/IEC 27005

Tipo	Amenazas	Origen
Daño físico	Fuego	A,D,E
	Daño por agua	A,D,E
	Contaminación	A,D,E
	Accidente importante	A,D,E
	Destrucción del equipo de los medios	A,D,E
	Polvo, corrosión, congelamiento	A,D,E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A,D
	Pérdida de suministro de energía	A,D,E
	Falla en el equipo de telecomunicaciones	A,D
Perturbación debida a la radiación	Radiación electromagnética	A,D,E
	Radiación térmica	A,D,E
	Impulsos electrodomésticos	A,D,E

Continúa en la siguiente página ►

Tipo	Amenazas	Origen
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A,D
	Datos provenientes de fuentes no confiables	A,D
	Manipulación con *hardware*	D
	Manipulación con *software*	A,D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A,D
	Mal funcionamiento del *software*	A
	Incumplimiento en el mantenimiento del sistema de información	A,D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del *software*	D
	Uso de *software* falso o copiado	A,D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A,D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A,D,E

*A: accidentales D: acciones deliberadas E: ambientales (naturales)

Fuente: Icontec (2009b).

Identificación y clasificación de activos

La exposición de un recurso de información a una amenaza específica configura la Unidad de Análisis Básica y recibe el nombre de "escenario de riesgo".

La construcción de los escenarios de riesgo se realiza en función de las amenazas que pueden llegar a afectar a cualquier activo identificado dentro del alcance del SGSI.

ESCENARIO DE RIESGO = AMENAZA F(ACTIVO DE INFORMACIÓN) (2)

Estimación del riesgo

Con el propósito de estimar el riesgo se pueden llevar a cabo análisis cualitativos, semicuantitativos o cuantitativos, o bien una combinación de los tres. En cualquier caso, el tipo de análisis que se lleve a cabo debe ser congruente con los criterios desarrollados en el establecimiento del contexto.

Como se mencionó en párrafos anteriores, para estimar el riesgo se acudirá a la estimación de la vulnerabilidad, en este caso, la vulnerabilidad inherente y la vulnerabilidad residual.

- *Vulnerabilidad inherente*. Representa la estimación de la vulnerabilidad, sin tener en cuenta los controles existentes.
- *Vulnerabilidad residual*. Representa la estimación de la vulnerabilidad, teniendo en cuenta el efecto que tienen los controles sobre la disminución de la probabilidad o la disminución del impacto.

Es importante considerar que, para estimar la vulnerabilidad residual, se deben definir esquemas que permitan evaluar los controles y tomar la decisión del nivel de disminución de la probabilidad o el impacto, bajo el precepto de que un control tan solo puede disminuir uno u otro parámetro y no ambos.

Selección de controles

Por lo general, se considera que seguridad es sinónimo de controles. Si bien esto es cierto parcialmente, la verdad es que los controles se requieren porque existen riesgos y, en este sentido, el concepto de seguridad se convierte en un estado a través del cual los controles permiten tener niveles aceptables de riesgo. Es muy común encontrar en las organizaciones una cantidad significativa de controles que han surgido no por respuesta a un riesgo, al menos de manera explícita, sino por una necesidad particular o en ocasiones por moda.

De acuerdo con lo anterior, un enfoque sistémico de gestión del riesgo, tal como lo plantea la ISO/IEC 27001, lleva a seleccionar los controles

a partir de una necesidad surgida de la probabilidad de ocurrencia de un riesgo o de la mitigación de su impacto; esto es lo que justifica realmente la incorporación de controles en la organización.

Todos los controles de seguridad de la información se conforman con una mezcla de procedimientos, tecnología y personas. Además, se requiere un equilibrio entre cada una de ellas para lograr los fines previstos de un SGSI. De igual forma, debería existir una adecuada combinación de controles, entre preventivos, detectivos y correctivos, manuales y automatizados, discrecionales y no discrecionales, lo que permita hacer un tratamiento del riesgo en diferentes momentos de este.

Todo control que se incorpore como parte del SGSI debe tener una adecuada relación costo/beneficio, de modo que sea viable su incorporación como parte de la infraestructura de control de la organización y satisfaga los criterios específicos para los que se incorporó.

Evaluación del riesgo

La evaluación del riesgo consiste en realizar una comparación de la vulnerabilidad resultante de cada riesgo y confrontarlos contra el nivel de aceptación de riesgo definido por la organización. En conformidad con este concepto, deben existir dos tipos de evaluaciones: antes de controles y después de controles, acorde a la estimación resultante en la fase anterior.

Los resultados arrojados de la evaluación de riesgos permiten diseñar mapas de riesgos, informes de vulnerabilidad por cada criterio de seguridad de la información y diversos indicadores que permiten monitorear el nivel de avance en la gestión del riesgo.

En relación con el proceso de valoración del riesgo residual es importante tener en cuenta cuál es el efecto que tienen los controles sobre la probabilidad o el impacto, si se tiene presente que un control no actúa sobre ambos y esto requiere realizar un adecuado análisis. De igual forma, se deben tratar los controles de forma individual en relación con la disminución del impacto o su probabilidad y no como un paquete de controles que en conjunto disminuyan ambas variables del riesgo.

Es importante diseñar mapas de riesgos inherentes y residuales como una forma de visualizar gráficamente la distribución de riesgos en la organización y, a su vez, realizar comparaciones entre ambos, como una forma de observar el impacto que tienen los controles sobre la disminución del riesgo, tal como se puede observar en la figura 31.

Figura 31. Ejemplos de matrices de riesgos.
Fuente: Villanueva (2015).

Tratamiento del riesgo

La fase de tratamiento del riesgo establece las acciones a desarrollar a través de controles propuestos para llevar el riesgo a un nivel aceptable en la organización. Para ello se debe priorizar los riesgos residuales en función de los criterios de aceptabilidad, al ser prioritarios aquellos que se encuentran en el más alto nivel de vulnerabilidad.

Es importante tener en cuenta que la elaboración del plan de tratamiento de riesgos requiere un análisis de costo beneficio de los controles a implementar y los techos presupuestales asignados para su elaboración, de allí la importancia de priorizar aquellos escenarios de riesgo que son más críticos para la organización.

Para su tratamiento se encuentran diversas opciones, las cuales han sido clasificadas por la ISO/IEC 27005 en cuatro alternativas que se enlistan a continuación.

- *Reducción del riesgo*. La reducción del riesgo consiste en la selección de controles que puedan disminuir la probabilidad o el impacto del riesgo residual hasta lograr llevarlo a un riesgo aceptable. Estos nuevos controles deben contar con una estimación de costos y tiempo, así como determinar los responsables de implementarlos en la organización.
- *Retención del riesgo*. Esta alternativa prevé asumir el riesgo, en conformidad con los niveles de aceptabilidad definidos en la organización. Lo anterior implica que no se implementarán nuevos controles y la organización deberá asumir los impactos que podrá generar el riesgo residual. Esta alternativa, por lo general, se asume cuando el nivel de riesgo residual es aceptado por la organización y considera que no se requieren controles adicionales.
- *Evitar el riesgo*. Consiste en evitar la acción o el activo que da origen al riesgo en particular. Esta alternativa se presenta, por lo general, cuando los costos de implementación de controles adicionales superan los beneficios esperados, para lo cual se pueden omitir las acciones o los activos que generan el riesgo o cambiar las condiciones que generan dichos escenarios de riesgo.
- *Transferencia del riesgo*. Esta alternativa conlleva transferir el riesgo a un tercero para compartir los riesgos de forma total o parcial, de forma tal que este tercero pueda gestionar de manera más eficaz y eficiente el riesgo. Es importante tener en cuenta que, a pesar de

que se transfiera la responsabilidad del riesgo, la organización, por lo general, no podrá transferir la responsabilidad del impacto.

Un plan de tratamiento de riesgos, generalmente, contempla la siguiente estructura:

1. Escenario de riesgo.
2. Riesgo residual (valor y calificación).
3. Alternativa de tratamiento.
4. Control a implementar.
5. Responsable de su implementación (rol).
6. Valor estimado.
7. Fechas estimadas de implementación.
8. Efecto esperado del control en función de la disminución de la probabilidad o impacto.
9. Riesgo residual esperado después del plan de mitigación.

▶ Fase 5. Diseñar el SGSI

Tabla 28. Requisitos de la ISO/IEC 27001 relacionados con el diseño del SGSI

Objetivo de la fase	
Completar el plan final de implementación del SGSI mediante el diseño de seguridad de la información con base en las opciones de tratamiento de riesgos seleccionadas, así como en los requisitos referidos a registros y documentos, el diseño de los controles que integran las precauciones de seguridad de las TIC, los procesos físicos y de la organización, y el diseño de requisitos específicos del SGSI.	
Requisitos de LA ISO/IEC 27001:2013 relacionados	
7.4 Comunicación	7.5 Información documentada
8.1 Planificación y control operacional	8.2 Valoración de riesgos de seguridad de la información
8.3 Tratamiento de riesgos de seguridad de la información	9.1 Seguimiento, medición, análisis y evaluación
9.2 Auditoría interna	9.3 Revisión por la dirección

Fuente: elaboración propia.

El diseño del SGSI contempla, básicamente, tres componentes: la documentación que debe tener el sistema, la implementación de los controles previstos en el plan de tratamiento de riesgos y el monitoreo constante de la seguridad de la información. Este último componente se puede realizar a través de dos instrumentos: la implementación de un proceso de gestión de incidentes y el desarrollo de auditorías periódicas al sistema.

Documentación del sistema

La información documentada que debe tener un SGSI comprende todos aquellos requisitos contemplados en la ISO/IEC 27001, los cuales surgen a partir de la implementación de sus diferentes fases.

Un resumen de la información que se debe documentar como parte del SGSI se puede observar en la tabla 29.

Tabla 29. Resumen de la información documentada que debe tener un Sistema de Gestión de Seguridad de la Información basado en la ISO/IEC 27001:2013

Numeral ISO/IEC 27001:2013		Documentación
4.3	Determinación del alcance del SGSI	El alcance debe estar disponible como información documentada
5.2	Política de seguridad	e) La política de seguridad debe estar disponible como información documentada
6.1.2.	Valoración de riesgos de seguridad de la información	Información documentada acerca del proceso de valoración de riesgos de la seguridad de la información
6.1.3	Tratamiento de riesgos de seguridad de la información	Información documentada acerca del proceso de tratamiento de los riesgos de seguridad de la información
6.1.3	Declaración de aplicabilidad	d) Declaración de aplicabilidad
6.2.	Objetivos de seguridad de la información y planes para lograrlos	Objetivos de la seguridad de la información
7.2	Competencia	Evidencia de la competencia de las personas relacionadas con la seguridad de la información
7.5.	Información documentada	b) La que la empresa ha determinado que es necesaria para la eficacia del SGSI

Continúa en la siguiente página ▶

Numeral ISO/IEC 27001:2013		Documentación
7.5.3	Control de la información documentada	La información documentada de origen externo
8.1	Planificación y control operacional	Información documentada para tener confianza en que los procesos se han llevado a cabo de acuerdo con lo planificado
8.2.	Valoración de la seguridad de la información	Resultados de las valoraciones de riesgos de la seguridad de la información
8.3	Tratamiento de riesgos de seguridad de la información	Resultados de los tratamientos de riesgos de la seguridad de la información
9.1	Seguimiento, medición, análisis y evaluación	Evidencia de los resultados del monitoreo y de la medición
9.2	Auditoría interna	g) Conservar la información documentada como evidencia de la implementación del programa de auditoría y de los resultados de esta
9.3	Revisión por la dirección	Evidencia de los resultados de la revisión por la dirección
10.1	No conformidades y acciones correctivas	Naturaleza de las no conformidades y cualquier acción posterior tomada
10.1	No conformidades y acciones correctivas	Resultados de cualquier acción correctiva

Fuente: Valencia Duque y Orozco Alzate (2017).

La documentación es una de las fases más extensas del total del proyecto de SGSI y, tal como se puede observar en la figura 32, está estructurada en varios niveles: el manual de seguridad que, por lo general, contiene el alcance, la política general y sus diferentes políticas operativas, así como la estructura de seguridad de la información en la empresa, la metodología de riesgos, la declaración de aplicabilidad y los procedimientos. Estos últimos son todos aquellos procedimientos obligatorios (por la ISO/IEC 27001) y corporativos relacionados con la gestión de la seguridad de la información en la organización. Algunos de ellos los comparte con los demás sistemas de gestión de la entidad. Las instrucciones, las *checklist*, los formularios y, en general, las guías técnicas, los manuales y los instructivos son el tercer nivel de documentación. El último nivel de documentación corresponde a los registros obligatorios y corporativos relacionados con la gestión de la seguridad de la información, entre los cuales se deben incluir los registros digitales.

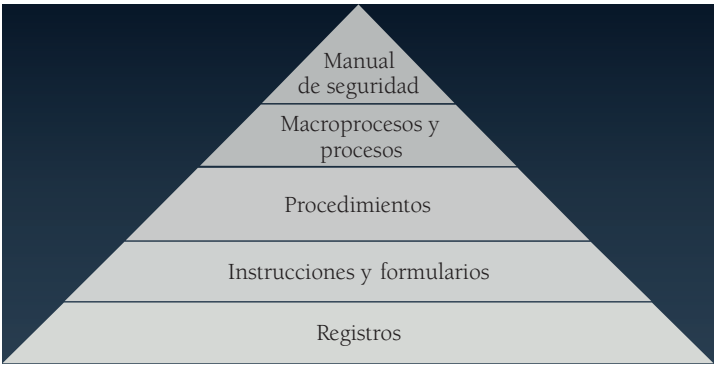

Figura 32. Estructura general de documentación de un SGSI.
Fuente: elaboración propia.

Se recomienda, en caso de que la organización cuente con otros sistemas de gestión de calidad, integrar los aspectos propios del SGSI a la documentación que ya existe.

Declaración de aplicabilidad

El segundo documento más importante de un SGSI, después de la política de seguridad, es la declaración de aplicabilidad. Este surge en relación con los controles planteados en el anexo de la ISO/IEC 27001 o la ISO/IEC 27002, especificando si se aplica o no dicho control en la organización. En caso afirmativo, describe cómo se aplican e identifican los mecanismos a través de los cuales se materializa en la organización. Una plantilla de ejemplo para tal fin se presenta en la tabla 30.

Tabla 30. Plantilla de ejemplo de declaración de aplicabilidad

Número del control (de acuerdo al Anexo 1 de la ISO/IEC 27001	Nombre del Control del Anexo 1 de la ISO/IEC 27001	(S)eleccionado/ (e)xcepción	Control/es específicos implementados o por implementar en la organización	Descripción/ justificación

Fuente: elaboración propia.

La declaración de aplicabilidad comprende los controles existentes en la organización y los controles previstos en el plan de tratamiento de riesgos, justificados, por lo general, a partir de la probabilidad y el impacto en la ocurrencia de un riesgo y de los requerimientos legales y de negocio que tenga la organización.

Implementar el plan de tratamiento de riesgos

La implementación del plan de tratamiento de riesgos aprobado por la alta dirección con los recursos asignados para tal fin y el mantenimiento de los controles existentes es lo que permite garantizar niveles aceptables de seguridad de la información en la organización.

De allí que debe existir un monitoreo permanente de los controles y de los nuevos escenarios de riesgos que surgen para mantener un SGSI pertinente y ajustado a la realidad de la organización.

▶ Aspectos complementarios que se deberían tener en cuenta al implementar un SGSI

Como complemento a la estructura planteada por la ISO/IEC 27003:2010, se recomienda contemplar tres aspectos adicionales para una adecuada implementación del SGSI: un programa de sensibilización y concientización, el establecimiento de un proceso de gestión de incidentes de seguridad y la realización de pruebas del sistema de gestión de seguridad implementado.

Programa de sensibilización y concientización del SGSI

Es necesario sensibilizar y concientizar a los diferentes miembros de la organización acerca de la importancia de la seguridad de la información, para lo cual es posible acudir a diferentes técnicas, como, por ejemplo:

- creación de escenarios ficticios en los que se recreen riesgos que pueden afectar a los miembros de la organización;
- simulaciones de ingeniería social en las que se soliciten claves con voces fingidas de directivos de la organización;
- pósteres en los que se muestre información importante del SGSI;
- capacitaciones alrededor de aspectos del SGSI;
- mensajes de sensibilización a través de la intranet;

- contratación de mimos que interpreten situaciones de inseguridad;
- creación de virus ficticios.

En general, existen muchas alternativas para sensibilizar a las personas de la organización alrededor de la importancia de la seguridad de la información. Se recomienda, a manera de ejemplo, leer el kit de concientización propuesto por el Instituto Nacional de Ciberseguridad de España (INCIBE).

La gestión de incidentes de seguridad de la información

Tradicionalmente, una vez diseñado el SGSI, las organizaciones realizan revisiones periódicas de los nuevos riesgos que surgen, así como de la efectividad de los controles implementados o por implementar, para lo cual se acude a las diversas áreas de la organización que cumplen funciones de aseguramiento. Sin embargo, por lo general, este proceso se realiza de forma tardía y no da respuesta a los incidentes que ocurren en el día a día de la operación del negocio; por tanto, una de las principales herramientas para monitorear de forma permanente los incidentes que ocurren en la organización y afectan el sistema de gestión de seguridad de la información (nuevos riesgos o incumplimiento de controles), es el proceso de gestión de incidentes de seguridad de la información, definido por ISACA (2013) como la capacidad de gestionar de forma efectiva los diversos eventos perjudiciales e inesperados, a fin de minimizar los impactos y mantener o restaurar las operaciones normales dentro de los límites de tiempo definidos.

La gestión de incidentes de seguridad de la información es la parte operativa de la gestión de riesgos del día a día y cuenta para su adecuada incorporación en la organización con la norma ISO/IEC 27035:2011, adoptada en Colombia como GTC-ISO/IEC 27035:2012 —"Gestión de incidentes de seguridad de la información"—, a través de la cual se establecen cinco fases para el desarrollo de un adecuado proceso de gestión de incidentes en la organización, cuyo resumen se presenta en la figura 33.

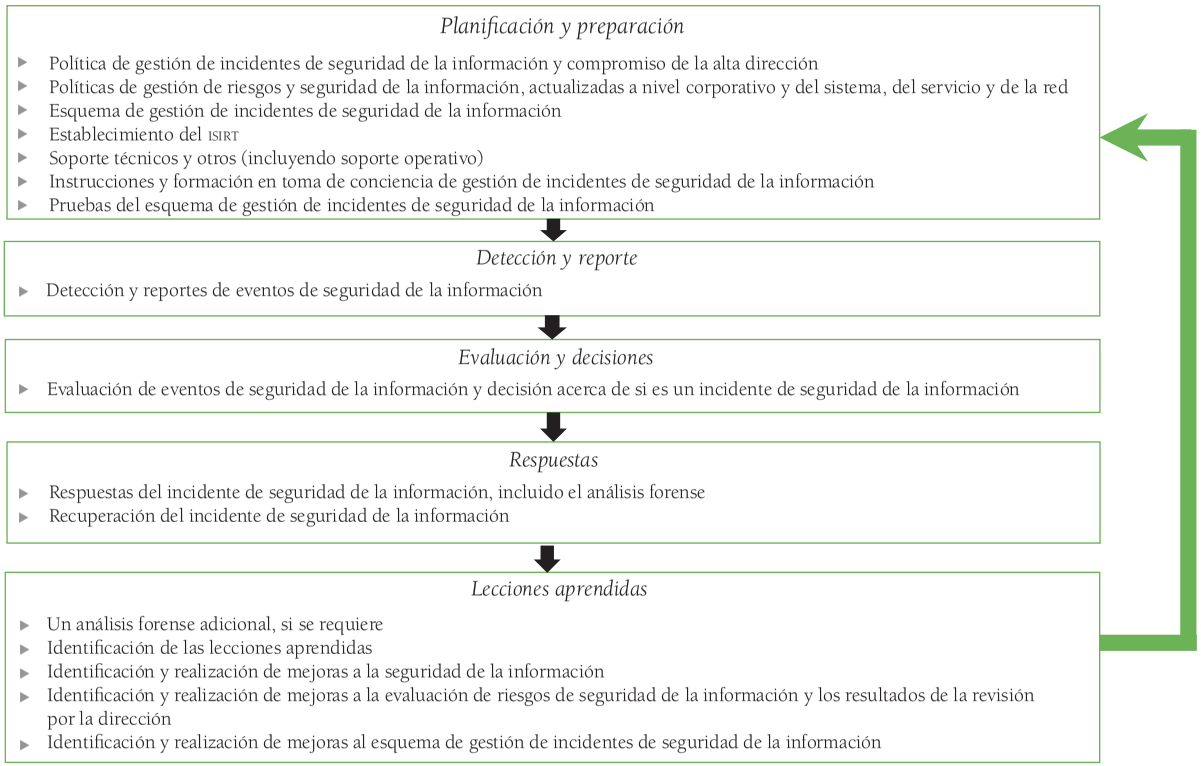

Figura 33. Fases de la gestión de incidentes de seguridad de la información de acuerdo con la ISO/IEC 27035.

Fuente: elaboración propia a partir de Icontec (2012).

Pruebas del sistema de gestión de seguridad de la información

Es importante y necesario probar el SGSI, y pasar de los aspectos documentales a los aspectos reales. Para esto se recomienda realizar ensayos a diferentes niveles, desde realizar pruebas a pequeños controles, hasta realizar pruebas de los planes de contingencia para asegurarnos de que, efectivamente, funcionan en el momento de ocurrir cualquier evento adverso en la organización. Para esto se puede acudir a auditorías en las que se realizan pruebas a los controles y se verifique que los procedimientos documentados realmente están funcionando, tal como se documentaron; también es posible recurrir a pruebas de campo en las que se verifique que los controles funcionan adecuadamente.

Una auditoría externa de certificación seguramente solicitará soportes de auditoría y documentación de las pruebas realizadas con sus respectivos resultados.

Ciberseguridad y seguridad en la nube como temas emergentes de la seguridad de la información

Bajo la premisa según la cual el proceso de implementación de un sistema de gestión de seguridad es uno solo y lo que realmente cambia es el objeto de intervención del proceso, es decir, los activos que son objeto de análisis, a continuación se incorporan como parte del objeto de análisis los procesos y activos que hacen parte de la ciberseguridad y la seguridad en la nube como dos de los temas emergentes de los últimos años en el campo tecnológico.

A fin de lograr este propósito han surgido alrededor de la ciberseguridad y la seguridad de la nube diversos marcos de referencia. Incluso Gartner lanzó en el 2017 su modelo de evaluación continua de confianza y riesgo adaptativo (CARTA) (siglas en inglés para *continuous adaptive risk and trust assessment)*, el cual viene a complementar lo establecido en el NIST 800-137 en el 2011 —Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations—.

Para esto se acudirá a los conceptos básicos de cada uno de estos componentes y los principales marcos y referentes que en materia de seguridad se han planteado a nivel internacional, con énfasis —dada la perspectiva del presente texto— en los estándares asociados a la familia de normas ISO/IEC 27000.

Ciberseguridad

Por lo general, se habla indistintamente de seguridad informática, seguridad de la información y ciberseguridad como un solo concepto. Ahora, si bien están muy relacionadas, contemplan aspectos diferentes. Las diferencias entre seguridad informática y seguridad de la información ya fueron planteadas en el primer capítulo de este texto.

Antes de presentar los aspectos diferenciadores de estos tres términos, es necesario partir del concepto de ciberseguridad, para lo cual —si se tiene en cuenta que diversas organizaciones internacionales la han definido— acudiremos a los conceptos que al respecto han establecido la Unión Internacional de Telecomunicaciones, ISACA y la ISO/IEC a través de su norma ISO/IEC 27032.

Inicialmente, la Unión Internacional de Telecomunicaciones (ITU), por medio de la recomendación ITU-T X.1205, define la ciberseguridad como:

> El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen uno o más de las siguientes: disponibilidad, integridad (que puede incluir autenticidad y el no repudio) y confidencialidad. (ITU, 2008, p. 3)

Por su parte, ISACA la define como la protección de los activos de información a través del tratamiento de las diversas amenazas que ponen en riesgo la información que se procesan, almacenan y transportan los sistemas de información que se encuentran interconectados.

Por último, la norma ISO/IEC 27032 define la ciberseguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, definiendo a su vez ciberespacio como el entorno complejo resultante de la interacción de personas, *software* y servicios en internet, a través de dispositivos tecnológicos y redes conectadas a él que no existen en ninguna forma física.

Acorde a lo anterior, la seguridad de la información tiene un alcance mayor que la ciberseguridad, debido a que la primera busca proteger la información en sus diferentes formatos y estados, mientras que la ciberseguridad se enfoca en la información digital y los sistemas interconectados que la procesan, almacenan y transmiten (Joyanes Aguilar, 2017).

Principales marcos y directrices de ciberseguridad

Dada la importancia que representa la ciberseguridad para las organizaciones y los países, diferentes organizaciones internacionales han desarrollado marcos de referencia de ciberseguridad como complemento a los marcos de seguridad de la información. Entre estos se destacan: la recomendación dada por Unión Internacional de Telecomunicaciones a través de la UIT-TX.1205 de 2008, Aspectos *generales de la ciberseguridad* y el *NIST Cibersecurity Framework*; ISACA, de forma similar, ha establecido una serie de documentos alrededor de la ciberseguridad, entre los que se destacan *Implementación del marco de ciberseguridad del NIST,* además de desarrollar programas de certificación en ciberseguridad; por último y objeto del presente texto, la ISO en compañía de IEC han desarrollado normas que complementan la familia de normas ISO/IEC 27000, entre las que se encuentran la ISO/IEC 27032 —*Tecnología de la información. Técnicas de seguridad-directrices para ciberseguridad*— y la ISO/IEC TR 27103:2018 —*Tecnología de información. Técnicas de seguridad-ciberseguridad y estándares ISO/IEC*—.

Cabe destacar la reciente actualización de la publicación del NIST denominada *Marco de referencia para el mejoramiento de la ciberseguridad de infraestructuras críticas*, en su versión 1.1, por medio de la cual se presenta un marco de referencia basado en riesgos para gestionar los riesgos de ciberseguridad, compuesto por tres partes: el núcleo del marco de referencia, las capas de implementación del marco y los perfiles asociados al marco (NIST, 2018). El núcleo del marco de referencia se presenta en la figura 34.

La estructura del marco de referencia la componen funciones, categorías, subcategorías y referencias informativas. Una relación de las categorías por cada función se observa en la tabla 31.

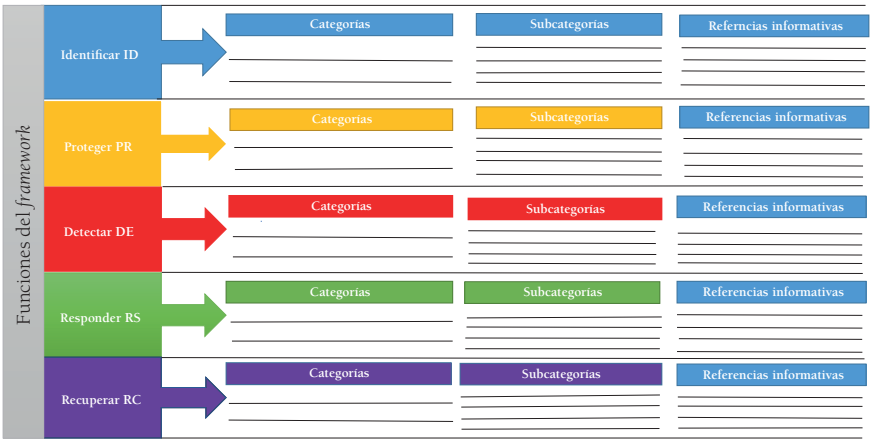

Figura 34. Núcleo del marco de referencia para el mejoramiento de la ciberseguridad de infraestructuras críticas.
Fuente: elaboración propia a partir de NIST (2018).

Tabla 31. Categorías de procesos del marco de referencia de ciberseguridad del NIST

Funciones		Categorías
Identificar	AM	Gestión de activos
	BE	Ambiente de negocios
	GV	Gobierno
	RA	Evaluación de riesgos
	RM	Estrategia de gestión del riesgo
	SC	Gestión del riesgo de la cadena de suministro
Proteger	AC	Gestión de identidad y control de acceso
	AT	Concientización y capacitación
	DS	Seguridad de datos
	IP	Procesos y procedimientos de protección de información
	MA	Mantenimiento
	PT	Protección de tecnología
Detectar	AE	Anomalías y eventos
	CM	Monitoreo continuo de la seguridad
	DP	Procesos de detección

Continúa en la siguiente página ▶

Funciones		Categorías
Responder	RP	Planeación de la respuesta
	CO	Comunicación
	AN	Análisis
	MI	Mitigación
	IM	Mejoras
Recuperar	RP	Planeación de la recuperación
	IM	Mejoras
	CO	Comunicación

Fuente: elaboración propia a partir de NIST (2018).

De igual forma, es importante mencionar los veinte controles críticos de seguridad propuestos por el Centro de Seguridad de Internet (CIS, por sus siglas para Center of Internet Security), entidad que los han relacionado con las categorías de procesos del marco de referencia de ciberseguridad de la NIST, tal como se puede observar en la tabla 32.

Tabla 32. Veinte controles críticos del SANS y su relación con el marco de referencia de ciberseguridad del NIST

Controles de seguridad críticos (versión 6.0.) (Centro de Seguridad de Internet-SANS)		Marco de referencia de ciberseguridad del NIST				
		Identificar	Proteger	Detectar	Responder	Recuperar
1	Inventario de dispositivos autorizados y no autorizados	AM				
2	Inventario de *software* autorizado y no autorizado	AM				
3	Configuración segura de dispositivos de usuario final		IP			
4	Evaluación continua de vulnerabilidades y remediación	RA		CM	MI	
5	Uso controlado de privilegios administrativos		AC			

Continúa en la siguiente página ▶

Controles de seguridad críticos (versión 6.0.) (Centro de Seguridad de Internet-SANS)		Marco de referencia de ciberseguridad del NIST				
		Identificar	Proteger	Detectar	Responder	Recuperar
6	Monitoreo, mantenimiento y análisis de *logs* de auditoría			AE	AN	
7	Protección de *e-mail* y *browsers*		PT			
8	Defensa de *malware*		PT	CM		
9	Limitación y control de puertos de red, protocolos y servicios		IP			
10	Capacidad de recuperación de datos					RP
11	Configuración segura de dispositivos de red		IP			
12	Defensa perimetral			DP		
13	Protección de datos		DS			
14	Acceso controlado basado en la necesidad de conocer		AC			
15	Control de acceso inalámbrica		AC			
16	Monitoreo y control de cuentas		AC	CM		
17	Evaluación de habilidades de seguridad y entrenamiento apropiado		AT			
18	Seguridad de aplicaciones de *software*		IP			
19	Administración y respuesta a incidentes			AE	RP	
20	Test de penetración y ejercicio de equipos rojos				IM	IM

Fuente: elaboración propia a partir de SANS (2018).

Normas y directrices de ciberseguridad en diversos países

Los diferentes países han establecido normas y directrices alrededor de la ciberseguridad, como es el caso, por ejemplo, de los Estados Unidos, que en el 2013 y por orden ejecutiva del entonces presidente Obama (OE 13636), denominada *Mejorando la ciberseguridad de las infraestructuras críticas,* desarrolló a través del NIST y otras entidades asociadas el *Marco para mejorar la ciberseguridad de la infraestructura crítica*, actualmente en su versión 1.1. De igual forma, la Unión Europea publicó la directiva UE 2016/1148 de 2016 denominada *Directiva sobre seguridad de redes y sistemas de información*, a través de la cual se pretende acabar con la fragmentación de los sistemas de seguridad cibernética entre los países y se exige a las empresas de servicios consideradas críticas (servicios esenciales), en los diferentes países, cumplir con nuevos requisitos asociados a la ciberseguridad.

Asimismo, en América Latina y el Caribe, organizaciones como la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) han elaborado diversos informes alrededor de la ciberseguridad como base para llamar la atención de los diversos gobiernos de la región. El primero, denominado *Tendencias de seguridad cibernética en América Latina y el Caribe*, se elaboró en el 2014 en compañía de Symantec y el Comité Interamericano control el Terrorismo; en este se presenta un informe integral de la seguridad cibernética en treinta países de América Latina y se proporciona una serie de recomendaciones (OEA y Symantec, 2014). También el BID y la OEA llevaron a cabo un estudio denominado *Informe de ciberseguridad 2016. ¿Estamos preparados en América Latina y el Caribe?*, por medio del cual se concluye la poca preparación con la que cuentan los países de América Latina y el Caribe para contrarrestar la amenaza del cibercrimen (OEA y BID, 2016).

Principales normas ISO asociadas a la ciberseguridad

ISO/IEC 27032

La norma ISO/IEC 27032 —*Tecnología de la información. Técnicas de seguridad-directrices para ciberseguridad*—, promulgada en el 2012, se desarrolló con el fin de cubrir aspectos no contemplados en las normas de seguridad de la información, así como elementos de comunicación entre las organizaciones y los proveedores en el ciberespacio. En particular, proporciona una guía para cubrir riesgos de ciberseguridad comunes tales como ataques

de ingeniería social, acceso secreto y no autorizado a sistemas informáticos (*hacking*), la proliferación de *software* malicioso (*malware*) y el *software* espía (*spyware*).

ISO/IEC TR 27103

Esta norma, publicada recientemente y denominada *Tecnología de información. Técnicas de seguridad-ciberseguridad y estándares ISO/IEC*, busca proporcionar una guía que permita aprovechar los estándares de seguridad existentes en el marco de la ciberseguridad, al brindar respuesta a las confusiones que podrían existir entre un sistema de gestión de seguridad de la información y la ciberseguridad, con énfasis en que ambos conceptos se pueden desarrollar de forma integrada en una organización.

▸ *Cloud computing*

La gestión de la información a través de la nube ha dejado de ser algo desconocido para las organizaciones y se convierte actualmente en una de las estrategias tecnológicas preferidas por muchas de ellas, no solo en la búsqueda de disminución de costos, sino en la utilización de recursos tecnológicos que sin el *cloud computing* sería casi imposible acceder a ellos, en especial para las pymes. De acuerdo con Joyanes Aguilar (2017), el *cloud computing* se considerad actualmente uno de los principales ejes de la transformación digital de las empresas.

En este sentido, el crecimiento del mercado de la computación en la nube se ha incrementado dramáticamente, lo que pone en el portafolio ejecutivo de la alta gerencia no solo la incorporación de este componente tecnológico en la estrategia organizacional, sino un nuevo tema a gestionar: la seguridad en la nube.

El National Institute of Standards and Technology (NIST) y la Cloud Security Alliance definen el *cloud computing* como un modelo para habilitar un acceso en red por demanda a un conjunto compartido de recursos informáticos configurables (redes, servidores, almacenamiento, aplicaciones y servicios). Por su parte, la ISO/IEC 17788 —*Information technology-cloud computing-overview and vocabulary*— la define como un paradigma que permite el acceso a la red a un conjunto escalable y elástico de recursos virtuales o físicos compartidos, con un aprovisionamiento por autoservicio y una

administración bajo demanda. Dentro de estos recursos se incluyen servidores, sistemas operativos, redes, *software*, aplicaciones y almacenamiento.

Componentes estructurales del *cloud computing*

Tanto la NIST SP 800-145 como la ISO/IEC 17788:2014 establecen los conceptos y los componentes estructurales de *cloud computing*, los cuales se articulan a través de modelos de servicios, modelos de despliegue y características esenciales, tal como se puede observar en la figura 35.

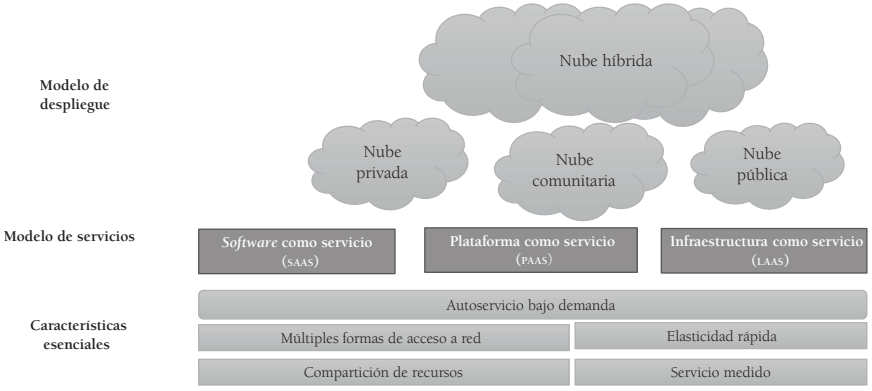

Figura 35. Componentes estructurales del *cloud computing*.
Fuente: elaboración propia a partir de Joyanes Aguilar (2017).

Modelo de servicios

El *cloud computing* cuenta con tres modelos de servicios básicos. *Software* como servicio (SaaS), consistente en la capacidad que se provee a un consumidor de usar las aplicaciones de un proveedor que corren en una infraestructura en la nube (no necesariamente del mismo proveedor). Estas aplicaciones pueden ser accesibles desde diversos dispositivos y, por lo general, utilizan un *browser*. Otro son las plataformas como servicio (PaaS), consistente en la capacidad que tiene un consumidor de desplegar aplicaciones adquiridas o desarrolladas que han sido creadas utilizando lenguajes de programación, librerías, servicios y herramientas soportadas por el proveedor. Por último, infraestructura como servicio (IaaS), por el que un proveedor ofrece a un consumidor recursos computacionales tales como capacidad de procesamiento, de almacenamiento, de comunicaciones y otra serie de recursos a través de

los cuales el consumidor puede desplegar plataformas y *software*. Estos recursos pueden incluir sistemas operativos.

Modelos de despliegue

Las cuatro formas de desplegar y operar los servicios de *cloud computing* que existen se enlistan y describen a continuación.

- *Nube privada*. Provee los servicios de forma exclusiva a una única organización y no se ofrecen al público. Los servicios allí desplegados pueden ser de propiedad de la organización, administrados y operados por esta, o por un tercero, o una combinación de ambos.
- *Nube pública*. En este caso la infraestructura la opera un proveedor que ofrece uno o varios servicios *cloud* al público en general.
- *La nube comunitaria*. Es aquella que ha sido organizada para servir a una función o propósito común de un grupo de consumidores específicos, quienes comparten, por lo general, objetivos comunes; puede ser administrada por la organización que ha constituido la comunidad o por un tercero.
- *La nube híbrida*. Es una combinación de las anteriores y puede desplegar diferentes servicios de forma pública, privada o comunitaria.

Características esenciales

Existen cinco características esenciales del *cloud computing*.

- *Autoservicio bajo demanda*. El usuario puede acceder a los diferentes servicios *cloud* en el momento en que los requiera, incluso sin necesidad de interacción humana con su proveedor.
- *Múltiples formas de acceso a la red*. También conocido como acceso ubicuo a la red, el usuario accede a los servicios en la nube por diferentes medios (PC, tabletas, teléfonos móviles, *smart TV*, estaciones de trabajo, etc.).
- *Compartición de recursos*. Los usuarios comparten los recursos que proporciona el proveedor (almacenamiento, capacidad de procesamiento, memoria, etc.), los cuales son asignados de acuerdo a la demanda y con los protocolos de seguridad respectivos para asegurar independencia.
- *Elasticidad rápida*. Los recursos con los que cuenta un proveedor son asignados y liberados de forma elástica y, por lo general, de

forma automática, lo que en ocasiones da la impresión al usuario que existen recursos ilimitados. Esta característica permite al usuario la ampliación o extensión en cantidad y calidad de los servicios *cloud*.

- *Servicio medido*. El proveedor, por lo general, cuenta con las capacidades para medir el o los servicios entregados a cada usuario; este último puede tener acceso a dichas mediciones sea para efectos de pago o de medición de la cantidad y calidad del servicio.

Servicios adicionales y emergentes del *cloud computing*

Adicional a los servicios básicos de *cloud computing* (IAAS, SAAS, PAAS), la ISO/IEC 17788:2014 establece nuevas tipologías de servicios asociados a la infraestructura, las plataformas y las aplicaciones que se despliegan en la nube, tal como se puede observar en la tabla 33.

Tabla 33. Categorías de servicios de *cloud computing* asociados a sus capacidades

Categorías de servicios *cloud*	**Tipos de capacidades de *cloud computing***		
	Infraestructura	Plataformas	Aplicaciones
Cómputo como servicio	X		
Comunicaciones como servicio		X	X
Almacenamiento como servicio	X	X	X
Infraestructura como servicio	X		
Redes como servicio	X	X	X
Plataforma como servicio		X	
Software como servicio			X

Fuente: elaboración propia a partir de ISO/IEC (2014b).

De forma complementaria, la norma establece servicios emergentes en el ámbito del *cloud computing*, aunque muchos de ellos ya están presentes en nuestra cotidianeidad. Entre ellos se incluyen los que enlistan y describen a continuación.

- *Bases de datos como servicio*. Capacidades asociadas a prestar servicios de funcionalidades de bases de datos bajo demanda, en las que el proveedor realiza la instalación y el mantenimiento de las bases de datos.
- *Escritorio como servicio*. Capacidades asociadas a la creación, la configuración, la administración, el almacenamiento, la ejecución y el desarrollo de funciones de escritorio de los usuarios de forma remota.
- *Correo como servicio*. Servicios de correo electrónico completo, lo que incluye servicios de soporte relacionados tales como almacenamiento, recepción, transmisión, respaldo y recuperación de correo electrónico.
- *Identidad como servicio*. Es la capacidad asociada con la gestión de accesos e identidades que se pueden extender y centralizar en los entornos operativos existentes, lo cual incluye el aprovisionamiento, la administración de directorios y el funcionamiento de un servicio de inicio de sesión único.
- *Gestión como servicio*. Servicios asociados a la gestión de aplicaciones, gestión de activos, gestión de cambios, gestión de la capacidad, gestión de problemas (*service desk*), gestión de cartera de proyectos, catálogo de servicios y gestión del nivel de servicio.
- *Seguridad como servicio*. Capacidades que permiten integrar un conjunto de servicios de seguridad con el entorno operativo existente, lo cual puede incluir autenticación, antivirus, *antimalware/antispyware*, detección de intrusos y administración de eventos de seguridad, entre otros.

Marcos de referencia de *cloud computing*

Al igual que ha ocurrido con la ciberseguridad, el *cloud computing* cuenta con diferentes estándares, entre los que se destacan en relación con sus definiciones y su arquitectura las normas que se presenta en la tabla 34.

Tabla 34. Marcos de referencia relacionados con *cloud computing*

Aspectos	Normas y estándares
Definiciones y vocabulario	ISO/IEC 17788:2014
	NIST SP 800-145
Arquitectura de referencia	ISO/IEC 17789:2014
	NIST SP 500-292

Fuente:

Marcos de referencia de la seguridad en la nube

Son múltiples los libros y artículos que se han escrito por parte de la comunidad académica y profesional alrededor de la seguridad en la nube, lo que denota la importancia que representa para las organizaciones este recurso en la definición de sus estrategias tecnológicas. Sin embargo, es necesario delimitar su estudio a partir de los principales referentes que al respecto se han establecido, y en particular aquellos asociados a la familia de normas ISO/IEC 27000, sin desconocer otros referentes como la *Security guidance for critical áreas of focus in cloud computing* de la CSA, complementado con la recomendación UIT-T-X.1642 de 2016 —*Directrices para la seguridad operativa de la computación en la nube*—, entre otros.

Seguridad en la nube basado en las normas ISO

Son diversas las normas ISO que se han publicado para desarrollar los diferentes componentes de seguridad en la nube. En marzo de 2014 se publicó la norma ISO/IEC 27018: 2014, *Tecnología de información. Técnicas de seguridad. Código de práctica para la protección de información persona identificable (IPI) en nubes públicas que actúan como encargadas del tratamiento*. Esta norma se considera una de las primeras normas de protección de datos personales en la nube pública.

En el 2015 se publicó la norma ISO/IEC 27017, *Tecnología de Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información basada en la ISO/IEC 27002 para servicios en la nube*. Esta norma provee una guía para la seguridad de la información en aspectos relacionados con el *cloud computing*, la cual recomienda la implementación de controles de seguridad de la información específicos para el *cloud computing*, lo que se convierte en una norma que complementa la ISO/IEC 27002.

La ISO/IEC 27036-4:2016, denominada formalmente *Tecnología de información-técnicas de seguridad-seguridad de la información para relaciones con proveedores-parte 4: guía para seguridad de servicios cloud,* provee lineamientos para todas aquellas organizaciones que adquieren o suministran servicios en la nube, proporcionando tanto a los clientes como a los proveedores de servicios en la nube orientación sobre a) visibilidad de los riesgos de seguridad de la información asociados con el uso de servicios en la nube y la gestión efectiva de esos riesgos, y b) respuestas a los riesgos específicos de la adquisición o prestación de servicios en la nube que pueden tener un impacto en la seguridad de la información en las organizaciones que utilizan estos servicios.

Capas tecnológicas y *cloud computing*

La infraestructura tecnológica ha evolucionado hacia la computación en la nube, de modo que ha transformado muchas de las operaciones que tradicionalmente desarrolla un área de TI en servicios.

Cada una de las capas tecnológicas propuestas en un modelo clásico de *cloud computing*, como se puede observar en la figura 36, pueden convertirse en cuatro tipologías de servicio, tal como se explica a continuación.

1	Procesos de negocio	BAAS
2	Servicios de TI	
3	Datos/información/conocimiento	
4	Sistemas de información transaccionales	SAAS
5	Sistemas de información soporte	
6	Motores de bases de datos	PAAS
7	Sistemas operativos	
8	PC de escritorio e impresoras	IAAS
9	Servidores (físicos, virtuales y en la nube)	
10	Centros de redes y cableado	
11	Centros de cómputo	
12	Energía	

Figura 36. Capas tecnológicas y su evolución hacia *cloud computing*.
Fuente: elaboración propia.

- IAAS-*Infrastructure-As-A-Service*. Servicio de computación que permite el uso de las capacidades de la infraestructura informática (capacidad de procesamiento, almacenamiento, etc.).
- PAAS-*Platform-As-A-Service*. Este servicio le permite a las empresas alquilar plataformas informáticas orientadas al desarrollo, testeo, lo que incluye bases de datos y sistemas operativos.
- SAAS-*Software-As-A-Service*. Este servicio permite a las empresas utilizar *software* bajo demanda, que tradicionalmente se usa a través de internet, mediante un navegador web.
- BAAS-*Business-As-A-Service*. También llamado BPAAS (*business process as a service*) consistente en la provisión de servicios de procesos de negocio altamente estandarizados.

Cada uno de estos servicios requiere el desarrollo de sistemas de seguridad que garanticen el cumplimiento de los objetivos de seguridad de la información y, al igual que el modelo base establecido en el primer capítulo, la afectación de una capa presenta un efecto cascada en las demás capas.

Riesgos de *cloud computing*

Al ser el proceso de gestión de riesgos el eje central de cualquier iniciativa de seguridad, autores como Grobauer, Walloschek y Stöcker (2011), Albanese, López y Sánchez (2013), Chou, (2015), Georgiou y Lambrinoudakis (2015), Sookhak, Gani y Buyya (2016), entre otros, han planteado diversos tipos de amenazas alrededor del cloud computing. Sin embargo, se ha tomado la propuesta planteada por Leung y Chen (2014), quienes establecen una ontología de riesgos de cloud computing agrupadas en cuatro categorías, doce subcategorías y cerca de cuarenta escenarios de riesgos, como una iniciativa que trata de integrar las diversas tipologías de riesgos que se pueden llegar a presentar en este ambiente. Esta ontología se puede observar en la tabla 35.

Tabla 35. Ontología de riesgos de *cloud computing*

Categoría	Subcategoría	Riesgo
Riesgos organizacionales	Gobierno de TI	Las empresas pierden gobierno y control de TI en la nube.
		Las empresas no pueden llevar a cabo auditorías de TI transparentes en la nube.
	Cumplimiento de regulaciones industriales	Los proveedores de *cloud computing* fallan en el soporte a las empresas usuarias, en el cumplimiento de regulaciones industriales específicas.
		Las regulaciones y procedimientos internos de seguridad de TI pasan por alto el entorno de la nube.
	Especialistas de TI *in house*	Reducida demanda de mano de obra interna de TI interna, debido a la disminución de los deberes de TI.
		Administradores internos de TI no cuentan con las competencias para asumir nuevos roles y responsabilidades en un ambiente *cloud computing*.
		Pérdida de expertos en TI con experiencia.
		Las empresas no tienen control sobre los expertos de TI del proveedor de *cloud*.
	Continuidad y resiliencia del negocio	Los proveedores de servicios en la nube interrumpen el negocio debido a quiebra o retiro del mercado.
		Dificultades de las compañías usuarias para cambiar de proveedor de servicio.
	Planeación y gestión de riesgos de sistemas de información	Las empresas usuarias carecen de herramientas eficientes de evaluación de riesgos en la nube.
		Las empresas usuarias carecen de recuperación ante desastres o plan de contingencia para hacer frente a problemas técnicas inesperados en la nube.
Riesgos operacionales	Acuerdos de nivel de servicio	SLA mal definidos o poco transparentes entre los proveedores de la nube y los usuarios del *cloud*.
		Los proveedores de *cloud* no tienen la capacidad de cumplir con los acuerdos de niveles de servicio establecidos.
	Problemas financieros	Incremento de costos ocultos debido a modelos de operación en la nube poco transparentes.
		No se establece un presupuesto financiero adecuado para los gastos basados en la nube.

Continúa en la siguiente página ▶

Categoría	Subcategoría	Riesgo
Riesgos operacionales	Movilidad de datos y aplicaciones	Dificultad de las compañías usuarias para transferir o mover los datos entre diferentes proveedores de *cloud*.
		Dificultades de las compañías usuarias para retornar sus datos y aplicaciones a las condiciones previas en que funcionaban *in-house*, una vez que se ha adoptado *cloud computing*.
	Usuarios del sistema	Resistencia de los usuarios a la adopción de servicios *cloud computing*.
		Falta de entrenamiento/capacitación en el uso de los servicios de *cloud computing*.
	Confiabilidad del servicio	Aplicaciones *cloud* no disponibles temporalmente o fuera de servicio.
		Pobres o insuficientes recursos computacionales para el funcionamiento del *cloud computing*.
Riesgos técnicos	Calidad de los datos y mantenimiento	Fragmentación o pérdida de datos a causa del uso de múltiples aplicaciones *cloud*.
		Dificultad de las compañías usuarias para acceder y procesar datos debido a técnicas de gestión de datos complejos usados por los proveedores de *cloud*.
		Compañías usuarias tienen limitado control sobre la depuración y pruebas de aplicaciones *cloud*.
	Desempeño del sistema	Desempeño de las aplicaciones *cloud* son afectadas por la velocidad de la red, tamaño de base de datos y/o capacidad del *hardware*.
		La adopción de la nube conduce a un mayor uso de recursos y costos operativos de las aplicaciones empresariales existentes.
	Integración del sistema	Sistemas/aplicaciones legados no se integran de forma adecuada con las nuevas aplicaciones *cloud*.
		Datos y aplicaciones en el *cloud* son aislados o inadecuadamente integrados.
	Seguridad de los datos	Acceso no autorizado a datos/aplicaciones empresariales en *cloud computing*.
		Vendedores de *cloud* usan ineficientes métodos de encriptación para proteger los datos.
		Ataques de denegación de servicios en ambiente *cloud*.

Continúa en la siguiente página ►

Categoría	Subcategoría	Riesgo
Riesgos legales	Privacidad de los datos	Privacidad de la empresa y datos de los clientes son puestos en peligro en *cloud computing*.
		Fallas de la arquitectura *cloud* para cumplir con regulaciones de privacidad y protección de datos requerida por la compañía.
		Diferentes leyes de protección de datos son usadas por diferentes países cuando los datos *cloud* son generados y almacenados.
	Propiedad intelectual	Problemas de propiedad intelectual generados por una inadecuada distribución de recursos de TI sobre la nube.
		Disputas legales entre empresas y proveedores de servicios *cloud* sobre la propiedad intelectual (por ejemplo, datos y *software*).
	Contratos	Acuerdos contractuales deficientes que no reflejan todos los detalles en el SLA asociado a la adopción de servicios de la nube.
		Problemas de recuperación y migración de datos empresariales con el proveedor de *cloud* al finalizar un contrato.

Fuente: elaboración propia a partir de Leung y Chen (2014).

Al igual que existen taxonomías de riesgos, la CSA (Cloud Security Alliance) ha desarrollado la matriz de controles *cloud*, la cual consiste en la incorporación de 133 controles hasta su versión 3.0.1, divididas en 16 dominios, tal como se puede observar en la tabla 36 y su descripción detallada en el Anexo 2.

Tabla 36. Dominios de controles *cloud* del Cloud Security Alliance

Cod.	Dominio	N.º de controles
AIS	Seguridad de aplicaciones e interfaces	4
ACC	Cumplimiento y aseguramiento de las auditorías	3
BCR	Gestión de la continuidad del negocio	11
CCC	Control de cambios y gestión de la configuración	5

Continúa en la siguiente página ▶

Cod.	Dominio	N.º de controles
DSI	Seguridad de los datos y gestión del ciclo de vida de la información	7
DCS	Seguridad del centro de datos	9
EKM	Gestión de claves y cifrado	4
GRM	Gobierno y gestión del riesgo	11
HRS	Seguridad de recursos humanos	11
IAM	Gestión de identidades y accesos	13
IVS	Seguridad de infraestructura y virtualización	13
IPY	Interoperabilidad y portabilidad	5
MOS	Seguridad móvil	20
SEF	Gestión de incidentes de seguridad, localización de evidencias electrónicas, investigaciones forense en la nube	5
STA	Gestión de la cadena de suministro, transparencia y responsabilidad	9
TVM	Gestión de vulnerabilidades y amenazas	3
	Totales	**133**

Fuente: elaboración propia a partir de Cloud Security Alliance (2018).

▶ Anexo 1. Clasificación de los controles de la ISO/IEC 27002:2013 en función de la tríada CIA y del recurso tecnológico

ISO/IEC 27002	Control	Objetivo principal (Carter y Treu, 2017)			Tipo de recurso tecnológico (Shojaie *et al.*, 2014)				
		Confidencialidad	Integridad	Disponibilidad	Datos	*Hardware*	*Software*	Personas	Redes
5	**Políticas de Seguridad de la Información**								
5,1	**Directrices establecidas para la seguridad de la información**								
5.1.1	Políticas para la seguridad de la información	✓	✓	✓	✓			✓	
5.1.2	Revisión de las políticas para la seguridad de la información	✓	✓	✓	✓			✓	
6	**Organización de la seguridad de la información**								
6,1	**Organización interna**								
6.1.1	Roles y responsabilidades para la seguridad de la información	✓	✓		✓			✓	
6.1.2	Segregación de funciones	✓	✓	✓	✓			✓	✓
6.1.3	Contacto con las autoridades	✓	✓	✓				✓	
6.1.4	Contacto con grupos de interés especial	✓	✓	✓				✓	
6.1.5	Seguridad de la información en la gestión de proyectos	✓			✓			✓	
6,2	**Dispositivos móviles y teletrabajo**								
6.2.1	Política para dispositivos móviles	✓	✓	✓	✓	✓			✓

Continúa en la siguiente página ▶

ISO/IEC 27002	Control	Objetivo principal (Carter y Treu, 2017)			Tipo de recurso tecnológico (Shojaie *et al.*, 2014)				
		Confidencialidad	Integridad	Disponibilidad	Datos	*Hardware*	*Software*	Personas	Redes
6.2.2	Teletrabajo	✓	✓		✓				✓
7	**Seguridad de recursos humanos**								
7,1	**Antes de asumir el empleo**								
7.1.1	Selección	✓	✓	✓	✓			✓	
7.1.2	Términos y condiciones del empleo	✓	✓	✓	✓			✓	
7,2	**Durante el empleo**								
7.2.1	Responsabilidad de la dirección	✓	✓	✓	✓			✓	
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	✓	✓	✓	✓			✓	
7.2.3	Proceso disciplinario	✓	✓	✓	✓			✓	
7,3	**Terminación y cambio de empleo**								
7.3.1	Responsabilidades en la terminación o cambio del empleo	✓	✓	✓	✓			✓	
8	**Gestión de activos**								
8,1	**Responsabilidad por los activos**								
8.1.1	Inventario de activos	✓	✓	✓	✓	✓	✓		
8.1.2	Propiedad de los activos	✓	✓	✓	✓			✓	
8.1.3	Uso aceptable de los activos	✓	✓	✓	✓	✓	✓		
8.1.4	Devolución de activos	✓	✓	✓	✓			✓	
8,2	**Clasificación de la información**								
8.2.1	Clasificación de la información		✓	✓	✓			✓	
8.2.2	Etiquetado de la información	✓	✓	✓	✓				

Continúa en la siguiente página ▶

ISO/IEC 27002	Control	Objetivo principal (Carter y Treu, 2017)			Tipo de recurso tecnológico (Shojaie *et al.*, 2014)				
		Confidencialidad	Integridad	Disponibilidad	Datos	*Hardware*	*Software*	Personas	Redes
8.2.3	Manejo de activos	✓	✓	✓	✓	✓			
8,3	**Manejo de medios**								
8.3.1	Gestión de medios removibles	✓	✓	✓	✓	✓			
8.3.2	Disposición de los medios	✓	✓	✓	✓	✓			
8.3.3	Transferencia de medios físicos			✓	✓	✓		✓	
9	**Control de acceso**								
9,1	**Requisitos del negocio para control de acceso**								
9.1.1	Política de control de acceso	✓	✓		✓				
9.1.2	Acceso a redes y a servicios en red	✓	✓					✓	✓
9,2	**Gestión de acceso a usuarios**								
9.2.1	Registro y cancelación del registro de usuarios	✓	✓		✓			✓	✓
9.2.2	Suministro de acceso de usuarios	✓	✓		✓	✓	✓	✓	✓
9.2.3	Gestión de derechos de acceso privilegiado	✓	✓		✓			✓	✓
9.2.4	Gestión de información secreta para la autenticación de usuarios	✓	✓		✓			✓	✓
9.2.5	Revisión de los derechos de acceso de usuarios	✓	✓					✓	
9.2.6	Retiro o ajuste de los derechos de acceso	✓	✓	✓	✓	✓	✓	✓	✓
9,3	**Responsabilidades de los usuarios**								
9.3.1	Uso de información secreta para la autenticación	✓	✓		✓			✓	✓

Continúa en la siguiente página ▶

ISO/IEC 27002	Control	Objetivo principal (Carter y Treu, 2017)			Tipo de recurso tecnológico (Shojaie *et al.*, 2014)				
		Confidencialidad	Integridad	Disponibilidad	Datos	*Hardware*	*Software*	Personas	Redes
9,4	**Control de acceso a sistemas y aplicaciones**								
9.4.1	Restricción de acceso a la información	✓	✓		✓	✓	✓		✓
9.4.2	Procedimiento de ingreso (Log-On) seguro	✓	✓		✓	✓	✓		✓
9.4.3	Sistema de gestión de contraseñas	✓	✓		✓		✓		
9.4.4	Uso de programas utilitarios privilegiados	✓	✓	✓		✓	✓		
9.4.5	Control de acceso a códigos fuente de programas		✓				✓		
10	**Criptografía**								
10,1	**Controles criptográficos**								
10.1.1	Política sobre el uso de controles criptográficos	✓	✓		✓				✓
10.1.2	Gestión de llaves	✓	✓		✓				✓
11	**Seguridad física y del entorno**								
11,1	**Áreas seguras**								
11.1.1	Perímetro de seguridad física	✓	✓	✓	✓	✓			
11.1.2	Controles de acceso físico	✓	✓	✓	✓	✓		✓	
11.1.3	Seguridad de oficinas, recintos e instalaciones	✓	✓	✓	✓	✓			
11.1.4	Protección contra amenazas externas y ambientales			✓	✓	✓			
11.1.5	Trabajo en áreas seguras	✓	✓	✓	✓				
11.1.6	Áreas de despacho y carga	✓	✓	✓	✓	✓		✓	

Continúa en la siguiente página ▶

ISO/IEC 27002	Control	Objetivo principal (Carter y Treu, 2017)			Tipo de recurso tecnológico (Shojaie *et al.*, 2014)				
		Confidencialidad	Integridad	Disponibilidad	Datos	*Hardware*	*Software*	Personas	Redes
11,2	**Equipos**								
11.2.1	Ubicación y protección de equipos	✓	✓	✓		✓			✓
11.2.2	Servicios de suministros			✓		✓			✓
11.2.3	Seguridad de cableado	✓		✓	✓	✓			✓
11.2.4	Mantenimiento de equipos		✓	✓		✓			✓
11.2.5	Retiro de activos	✓	✓	✓	✓	✓	✓	✓	✓
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	✓	✓	✓	✓	✓			✓
11.2.7	Disposición segura o reutilización de equipos	✓			✓	✓	✓		✓
11.2.8	Equipos de usuario desatendidos	✓	✓			✓		✓	✓
11.2.9	Política de escritorio limpio y pantalla limpia	✓			✓	✓	✓		
12	**Operación de la seguridad**								
12,1	**Procedimientos operacionales y responsabilidades**								
12.1.1	Procedimientos de operación documentados	✓	✓	✓	✓			✓	
12.1.2	Gestión de cambios	✓	✓	✓	✓	✓	✓		
12.1.3	Gestión de capacidad			✓		✓	✓		✓
12.1.4	Separación de los ambientes de desarrollo, pruebas, y producción	✓	✓	✓		✓	✓		✓
12,2	**Protección contra códigos maliciosos**								
12.2.1	Controles contra códigos maliciosos		✓	✓		✓	✓	✓	✓

Continúa en la siguiente página ▶

ISO/IEC 27002	Control	Objetivo principal (Carter y Treu, 2017)			Tipo de recurso tecnológico (Shojaie *et al.*, 2014)				
		Confidencialidad	Integridad	Disponibilidad	Datos	*Hardware*	*Software*	Personas	Redes
12,3	***Backup***								
12.3.1	Respaldo de la información		✓	✓	✓	✓	✓		
12,4	**Registro (*logging*) y seguimiento**								
12.4.1	Registro de eventos	✓	✓	✓	✓	✓	✓	✓	✓
12.4.2	Protección de información de logs	✓	✓	✓	✓	✓	✓		✓
12.4.3	Logs del administrador y del operador	✓	✓	✓	✓			✓	
12.4.4	Sincronización de relojes		✓			✓			✓
12,5	**Control de *software* operacional**								
12.5.1	Instalación de *software* en sistemas operativos	✓	✓	✓	✓	✓	✓		
12,6	Gestión de la vulnerabilidad técnica								
12.6.1	Control de las vulnerabilidades técnicas		✓		✓	✓	✓		
12.6.2	Restricciones sobre la instalación de *software*		✓		✓		✓	✓	
12,7	**Controles sobre auditoría de sistemas de información**								
12.7.1	Controles de auditoría de sistemas de información			✓	✓	✓	✓		
13	**Seguridad de las comunicaciones**								
13,1	**Administración de la seguridad en red**								
13.1.1	Controles de redes	✓	✓	✓	✓	✓	✓		✓
13.1.2	Seguridad de los servicios de red	✓	✓	✓	✓	✓	✓		✓
13.1.3	Separación de las redes	✓	✓			✓	✓	✓	✓

Continúa en la siguiente página ▶

ISO/IEC 27002	Control	Objetivo principal (Carter y Treu, 2017)			Tipo de recurso tecnológico (Shojaie *et al.*, 2014)				
		Confidencialidad	Integridad	Disponibilidad	Datos	*Hardware*	*Software*	Personas	Redes
13,2	Transferencia de información								
13.2.1	Políticas y procedimientos de transferencia de información	✓	✓	✓	✓	✓			✓
13.2.2	Acuerdos sobre transferencia de información	✓	✓		✓				✓
13.2.3	Mensajería electrónica	✓	✓	✓	✓				✓
13.2.4	Acuerdos de confidencialidad o de no divulgación	✓			✓				
14	**Adquisición, desarrollo y mantenimiento de sistemas**								
14,1	**Requisitos de seguridad de los sistemas de información**								
14.1.1	Análisis y especificaciones de requisitos de seguridad de la información	✓	✓	✓	✓	✓			
14.1.2	Seguridad de los servicios de aplicaciones en redes públicas	✓	✓		✓			✓	✓
14.1.3	Protección de transacciones de servicios de aplicaciones	✓	✓		✓		✓		✓
14,2	**Seguridad en los procesos de desarrollo y soporte**								
14.2.1	Política de desarrollo seguro	✓	✓		✓	✓	✓		
14.2.2	Procedimientos de control de cambios en sistemas		✓	✓	✓	✓			
14.2.3	Revisión técnica de aplicaciones después de cambios en plataformas operativas		✓			✓	✓		
14.2.4	Restricción de cambios sobre paquetes de *software*		✓				✓		
14.2.5	Principios de construcción de sistemas seguros	✓	✓		✓	✓			

Continúa en la siguiente página ▶

ISO/IEC 27002	Control	Objetivo principal (Carter y Treu, 2017)			Tipo de recurso tecnológico (Shojaie *et al.*, 2014)				
		Confidencialidad	Integridad	Disponibilidad	Datos	*Hardware*	*Software*	Personas	Redes
14.2.6	Ambiente de desarrollo seguro	✓	✓			✓	✓		
14.2.7	Desarrollos contratados externamente	✓	✓			✓	✓		
14.2.8	Pruebas de seguridad de sistemas		✓			✓	✓		
14.2.9	Pruebas de aceptación de sistemas			✓	✓	✓	✓		
14,3	**Datos de prueba**								
14.3.1	Protección de datos de prueba de sistemas		✓		✓				
15	**Relaciones con los proveedores**								
15,1	**Seguridad de la información en la relación con los proveedores**								
15.1.1	Información de seguridad en la relación con los proveedores	✓	✓	✓	✓			✓	
15.1.2	Tratamiento de la seguridad en los acuerdos con los proveedores	✓	✓	✓	✓	✓	✓	✓	✓
15.1.3	Cadena de suministro en tecnologías de información y comunicaciones	✓	✓	✓	✓	✓	✓	✓	✓
15,2	**Gestión de la prestación de servicios a proveedores**								
15.2.1	Seguimiento y revisión de los servicios de proveedores	✓	✓	✓		✓	✓	✓	
15.2.2	Administración de cambios de los servicios de proveedores	✓	✓	✓	✓	✓	✓	✓	
16	**Gestión de incidentes de seguridad de la información**								
16,1	**Gestión de incidentes y mejoras en la seguridad de la información**								
16.1.1	Responsabilidades y procedimientos	✓	✓	✓	✓			✓	

Continúa en la siguiente página ▶

ISO/IEC 27002	Control	Objetivo principal (Carter y Treu, 2017)			Tipo de recurso tecnológico (Shojaie *et al.*, 2014)				
		Confidencialidad	Integridad	Disponibilidad	Datos	*Hardware*	*Software*	Personas	Redes
16.1.2	Reporte de eventos de seguridad de la información	✓	✓	✓	✓			✓	
16.1.3	Reporte de debilidades de seguridad de la información	✓	✓	✓	✓	✓	✓	✓	
16.1.4	Evaluación y toma de decisiones sobre los eventos de seguridad de la información	✓	✓	✓	✓				
16.1.5	Respuesta a los incidentes de seguridad de la información	✓	✓	✓	✓				
16.1.6	Aprendizaje de los incidentes de seguridad de la información	✓	✓	✓	✓				
16.1.7	Recolección de evidencia	✓	✓	✓	✓				
17	**Aspectos de seguridad de la información en la gestión de la continuidad del negocio**								
17,1	**Continuidad de seguridad de la información**								
17.1.1	Planeación de la continuidad de seguridad de la información			✓	✓				
17.1.2	Implementación de la continuidad de seguridad de la información			✓	✓				
17.1.3	Verificación, revisión y evaluación de la continuidad de seguridad de la información			✓		✓	✓		✓
17,2	**Redundancias**								
17.2.1	Disponibilidad de instalaciones de procesamiento de la información			✓		✓	✓		

Continúa en la siguiente página ▶

ISO/IEC 27002	Control	Objetivo principal (Carter y Treu, 2017)			Tipo de recurso tecnológico (Shojaie *et al.*, 2014)				
		Confidencialidad	Integridad	Disponibilidad	Datos	*Hardware*	*Software*	Personas	Redes
18	**Cumplimiento**								
18,1	**Cumplimiento de requisitos legales y contractuales**								
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	✓	✓	✓	✓	✓			
18.1.2	Derechos de propiedad intelectual	✓			✓		✓		
18.1.3	Protección de registros	✓	✓	✓	✓				✓
18.1.4	Privacidad y protección de la información de datos personales	✓			✓			✓	
18.1.5	Reglamentación de controles criptográficos	✓			✓				✓
18,2	**Revisiones de seguridad de la información**								
18.2.1	Revisión independiente de la seguridad de la información	✓	✓	✓	✓	✓	✓	✓	✓
18.2.2	Cumplimiento con las políticas y normas de seguridad	✓	✓	✓	✓			✓	
18.2.3	Revisión de cumplimiento técnico	✓	✓		✓	✓			

▶ Anexo 2. Matriz de controles de *cloud computing* del CSA

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Seguridad de aplicaciones e interfaces								
Seguridad de aplicaciones	AIS-01	Las aplicaciones y las interfaces (APIS) deberán estar diseñadas, desarrolladas y desplegadas en conformidad con los estándares aceptados por la industria (p. ej., OWASP para aplicaciones web) y adherirse a las obligaciones de cumplimiento legal, estatutarias o reglamentarias aplicables.		X	X	X	X	X
Requerimientos de acceso de clientes	AIS-02	Antes de conceder a los clientes el acceso a los datos, activos y sistemas de información, todos los requisitos identificados de seguridad, contractuales y reglamentarios sobre el acceso de los clientes deberán ser considerados y corregidos.	X	X	X	X	X	X
Integridad de datos	AIS-03	Se deberán implantar rutinas de integridad de entrada y salida de datos (p. ej., en las rutinas de reconciliación o en las comprobaciones de edición) para los interfaces de aplicaciones y las bases de datos a fin de evitar errores manuales o sistemáticos de procesamiento, corrupción de datos o uso indebido.		X	X	X	X	X
Seguridad/integridad de datos	AIS-04	Las políticas y los procedimientos de apoyo a los procesos de negocio deberán estar establecidas, y las medidas técnicas implementadas, a fin de garantizar la protección de la confidencialidad, integridad y disponibilidad de los datos intercambiados entre uno o más interfaces de sistemas, jurisdicciones o relaciones externas del negocio para evitar la divulgación indebida, alteración o destrucción. Estas políticas, procedimientos, procesos y medidas deberán estar en conformidad con las obligaciones legales, estatutarias y reglamentarias.		X	X	X	X	X
Cumplimiento y aseguramiento de las auditorías								
Planificación de auditorías	AAC-01	Los planes de auditoría, las actividades y las operaciones centradas en la duplicación de datos, las limitaciones y el acceso a los datos deberán estar diseñados para minimizar el riesgo de interrupción de los procesos de negocio. Las actividades de auditoría deben planificarse y acordarse de antemano por los interesados.	X	X	X	X	X	X
Auditorías independientes	AAC-02	Las revisiones independientes y las evaluaciones se llevarán a cabo al menos anualmente, o en intervalos planificados, para asegurarse de que la organización resuelve cualquier no conformidad de las políticas establecidas, los procedimientos y el cumplimiento de las obligaciones contractuales, estatutarias o reguladoras.	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Mapa de regulación de los sistemas de información	AAC-03	Se deberá mantener un inventario de las obligaciones externas legales, estatutarias y reglamentarias de la organización asociada (y mapeado) con cualquier alcance y presencia geográfica, y que considere datos relevantes o información propiedad de la organización y administrada por la infraestructura de red (física o virtual) y los componentes de los sistemas, actualizado periódicamente según las necesidades del negocio (p. ej., un cambio en el alcance o un cambio en las obligaciones).	X	X	X	X	X	X
Gestión de la continuidad del negocio y resiliencia operacional								
Planificación de la continuidad de negocio	BCR-01	Debe establecerse un marco unificado y consistente para la planificación de la continuidad de negocio y debe desarrollarse un plan, documentado y adaptado, para asegurar que todos los planes de continuidad del negocio son consistentes en el tratamiento de las prioridades, las pruebas, el mantenimiento y los requisitos de seguridad de la información. Los requisitos para los planes de continuidad del negocio deben incluir los siguientes: ▶ un propósito y alcance definidos y en línea con las dependencias pertinentes; ▶ ser accesible y comprensible para los que van a utilizarlos; ▶ identificación de una/s persona/s nombrada/s que es/son responsable/s de su revisión, actualización y aprobación; ▶ las líneas de comunicación específicas, los roles y las responsabilidades deberán estar definidos; ▶ los procedimientos de recuperación, los manuales de trabajo y la información de referencia están detallados; ▶ hay un método para la invocación del plan.	X	X	X	X	X	X
Pruebas de continuidad de negocio	BCR-02	Los planes de respuesta ante incidentes de seguridad y de continuidad de negocio estarán sometidos a pruebas en los intervalos planificados o cuando se produzcan cambios organizativos o ambientales significativos. Los planes de respuesta ante incidentes deberán implicar a los clientes (arrendatarios) afectados y a otras relaciones comerciales que representen dependencias críticas de procesos de negocio dentro de la cadena de suministro.	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Servicios de infraestructura de los CPD y condiciones medioambientales	BCR-03	Los servicios de centros de procesamiento de datos y sus condiciones ambientales (p. ej., agua, electricidad, temperatura y control de humedad, telecomunicaciones y conectividad a internet) deberán ser asegurados, monitoreados, mantenidos y probados para garantizar su continua eficacia a intervalos planificados, de tal forma que se asegure la protección contra la interceptación no autorizada o el daño; además, deberán diseñarse con un balanceo automático y/o otras redundancias en el caso de interrupciones, estén planificadas o no.	X	X				
Documentación	BCR-04	La documentación del sistema de información (p. ej., guías de administrador y usuario, diagramas de arquitectura, etc.) se pondrá a disposición del personal autorizado para garantizar lo siguiente: ▶ una correcta configuración, instalación y operación del sistema de información; ▶ una utilización eficaz de las funciones de seguridad del sistema.		X	X	X	X	X
Riesgos medioambientales	BCR-05	La protección física contra el daño debido a causas naturales y desastres, así como los ataques deliberados (incluyendo incendios, inundaciones, descargas eléctricas atmosféricas, tormentas solares, vientos, terremotos, tsunamis, explosiones, accidentes nucleares, actividades volcánicas, riesgos biológicos, disturbios civiles, actividades tectónicas, y otros tipos de catástrofes naturales o de origen humano) deberán ser anticipados y diseñados, con contramedidas aplicadas.	X					
Localización del equipamiento	BCR-06	Para reducir los riesgos de las amenazas ambientales, los peligros y las oportunidades para el acceso no autorizado, el equipamiento deberá mantenerse alejado de lugares con alta exposición a riesgos ambientales y deberá proveerse de equipos redundantes situados a una distancia razonable.	X					
Mantenimiento del equipamiento	BCR-07	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo a los procesos de negocio que garanticen el mantenimiento de la continuidad y la disponibilidad de las operaciones y el personal de apoyo.	X	X	X	X	X	X
Fallos del equipamiento de alimentación	BCR-08	Se aplicarán las medidas de seguridad de la información y las redundancias necesarias para proteger los equipos de los cortes de servicios (p. ej., cortes de energía o interrupciones de la red).	X	X	X			

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Análisis de impacto	BCR-09	Deberá existir un procedimiento definido y documentado para determinar el impacto de cualquier interrupción en la organización, el cual deberá incorporar los siguientes aspectos: ▶ identificar los productos y servicios críticos; ▶ identificar todas las dependencias, incluyendo procesos, aplicaciones, socios comerciales y proveedores de servicios externos; ▶ comprender las amenazas a los productos y servicios críticos; ▶ determinar los impactos resultantes de interrupciones planificadas o no planificadas y cómo estos varían con el tiempo; ▶ establecer el periodo máximo tolerable de interrupción; ▶ establecer prioridades para la recuperación; ▶ establecer los objetivos de tiempo de recuperación para la reanudación de los productos y servicios críticos dentro de su periodo máximo tolerable de interrupción; ▶ estimar los recursos necesarios para la reanudación.	X	X	X	X	X	X
Programa de gestión	BCR-10	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo a los procesos de negocio para la resiliencia, la continuidad operativa y la gestión de los riesgos relacionados con las interrupciones de negocio, ya sean menores o catastróficas. Estas políticas, así como los procedimientos, los procesos y las medidas deben proteger la disponibilidad de las operaciones críticas del negocio y los activos de la empresa, en conformidad con las obligaciones de cumplimiento legal, estatutaria o reglamentarias aplicables. Se implementará un programa de gestión con las funciones y responsabilidades de soporte que haya sido comunicado, y en caso necesario, contractualmente convenido por todas las instalaciones afectadas, el personal y/o las relaciones comerciales externas.	X	X	X	X	X	X
Política	BCR-11	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo a los procesos de negocio que permitan un gobierno de TI adecuado y una gestión de servicios que garanticen una adecuada planificación, entrega y apoyo de las capacidades de TI, de modo que se brinde soporte a las funciones de negocio, la mano de obra y/o a los clientes, basados en normas aceptadas por la industria (como ITIL y Cobit 5). Además, las políticas y procedimientos deberán incluir roles y responsabilidades definidos, apoyados por una formación regular de la mano de obra.				X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Política de retención de activos	BCR -12	Se establecerán las políticas y los procedimientos, y se implementarán las medidas técnicas de apoyo a los procesos de negocio para definir y cumplir con el periodo de retención de cualquier activo crítico, según las políticas y procedimientos establecidos, y las obligaciones de cumplimiento legal, estatutaria o reglamentarias aplicables. Deberán incorporarse las medidas de copias de seguridad y recuperación como parte de la planificación de la continuidad del negocio y se probará su eficacia.			X	X	X	X
Control de cambios y gestión de la configuración								
Compras y nuevos desarrollos	CCC-01	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo a los procesos de negocio para garantizar que el desarrollo y/o la adquisición de nuevos datos, aplicaciones físicas o virtuales, infraestructura de redes, componentes de los sistemas, operaciones o instalaciones de centros de datos han sido autorizados previamente por el liderazgo empresarial de la organización u otro rol o función empresarial con la correspondiente rendición de cuentas.	X	X	X	X	X	X
Externalización de desarrollos	CCC-02	El uso de mano de obra subcontratada o externa al negocio para diseñar, desarrollar, probar y/o desplegar el código fuente de la organización requerirá de un mayor nivel de seguridad y confianza de las aplicaciones (p. ej., la supervisión de la gestión, la certificación independiente de la adherencia de las líneas base de seguridad, la formación obligatoria para la mano de obra subcontratada y las revisiones de seguridad del código).		X	X	X	X	X
Pruebas de calidad	CCC-03	Se establecerá un programa de seguimiento y evaluación sistemática para asegurar que se cumplen las normas de calidad y de seguridad en las líneas bases de referencia de todo el *software* desarrollado por la organización. Se establecerán y documentarán los criterios de evaluación y de aceptación de calidad para los sistemas de información, las actualizaciones y las nuevas versiones. Las pruebas de los sistemas se llevarán a cabo tanto durante el desarrollo como antes de ser aceptados, a fin de mantener su seguridad. La dirección dispondrá de una clara capacidad de supervisión durante el proceso de pruebas de calidad y se certificará el producto final como "apto para el propósito" (el producto debe ser adecuado para el propósito deseado) y "bien a la primera" (los errores deberían ser eliminados) antes de la publicación. También es necesario incorporar las revisiones técnicas de seguridad (es decir, las evaluaciones de vulnerabilidad y/o pruebas de penetración) con el fin de remediar las vulnerabilidades que puedan suponer un riesgo para el negocio o un riesgo para los clientes (arrendatarios) antes de su publicación.		X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Instalaciones no autorizadas de *software*	CCC-04	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo a los procesos de negocio con miras a restringir la instalación de *software* no autorizado en los dispositivos de usuario final pertenecientes a la empresa (por ejemplo, estaciones de trabajo, portátiles y dispositivos móviles), en la red de infraestructura TI y en los componentes de los sistemas de información.		X	X	X	X	
Cambios en producción	CCC-05	Se establecerán las políticas y los procedimientos, así como se implementarán los procesos relacionados con la gestión y el gobierno de los servicios TI para la gestión de los riesgos asociados con la aplicación de cambios en los negocios críticos o clientes (arrendatarios) que afecten a las aplicaciones (físicas y virtuales), las interfaces de los sistemas (APIS), las configuraciones y los diseños, así como a la infraestructura de red y a los componentes del sistema. Se aplicarán medidas técnicas para proporcionar la seguridad de manera que, antes de la implementación, todos los cambios correspondan directamente con una solicitud de cambio, sean críticos para el negocio o que se produzca un análisis de riesgos de los clientes, se realice una validación de los resultados esperados en el entorno, se establezca una preautorización de la dirección adecuada y se produzca la notificación, así como la autorización de los clientes, según el acuerdo de nivel de servicio (SLA).		X	X	X	X	X
Seguridad de los datos y gestión del ciclo de vida de la información								
Clasificación	DSI-01	Los datos y los objetos que contienen datos recibirán una clasificación basada en el tipo de datos, la jurisdicción de origen, la jurisdicción domiciliada, el contexto, las restricciones legales, las restricciones contractuales, el valor, la sensibilidad, la criticidad para la organización, la obligación de terceros para la retención y la prevención de divulgación no autorizada o uso indebido.			X	X	X	X
Inventario de datos/ flujos	DSI-02	Se establecerán las políticas y los procedimientos, y se implementarán las medidas técnicas para inventariar, documentar y mantener los flujos de los datos que residen (permanentemente o temporalmente) dentro de las aplicaciones y los servicios distribuidos geográficamente (físicos y virtuales), así como dentro de la infraestructura de red y componentes compartida con otros terceros, con el objeto de determinar cualquier impacto regulatorio, normativo en los acuerdos de nivel de servicio (SLA) o en la cadena de suministro, y para hacer frente a otros riesgos de negocio asociados a los sistemas de datos. Previa solicitud, el proveedor deberá informar al cliente del impacto en el cumplimiento y el riesgo, especialmente si los datos del cliente se utilizan como parte de los servicios prestados.						

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Transacciones de comercio electrónico	DSI-03	Los datos relacionados con el comercio electrónico (*e-commerce*) que atraviesan las redes públicas deberán estar debidamente clasificados y protegidos de actividad fraudulenta, divulgación no autorizada o modificación, de tal manera que se prevenga la disputa de contratos y compromisos.		X				X
Política de seguridad de manejo y etiquetado	DSI-04	Se establecerán políticas y procedimientos para el etiquetado, la manipulación y la seguridad de los datos y objetos que contienen datos. Se aplicarán mecanismos de herencia de etiquetas para los objetos que actúan como contenedores agregados de los datos.			X	X	X	X
Fugas de información	DSI-05	Se implementarán los mecanismos de seguridad para prevenir la fuga de datos.			X	X	X	X
Datos en entornos no de producción	DSI-06	Los datos de producción no se podrán replicar ni utilizar en entornos que no sean de producción.				X	X	X
Propiedad/servicio de los datos	DSI-07	Todos los datos serán designados con un servicio, con responsabilidades asignadas, definidas, documentadas y comunicadas.			X	X	X	X
Desechado seguro	DSI-08	Se establecerán las políticas y los procedimientos, así como se implementarán las medidas técnicas de soporte a los procesos de negocio, para la eliminación segura y completa de los datos de todos los medios de almacenamiento, asegurando que los datos no son recuperables por cualquier medio de informática forense.			X	X	X	X
Seguridad del centro de datos								
Gestión de activos	DCS-01	Los activos de apoyo a los entornos dinámicos y distribuidos de computación física y virtual deben clasificarse en función de la criticidad del negocio, las expectativas de nivel de servicio y los requisitos de continuidad operacional. Un inventario completo de los bienes esenciales en uso por la organización, ubicados en todos los sitios o situaciones geográficas se mantendrá y actualizará periódicamente (o en tiempo real), y se le asignará la propiedad con el apoyo de los roles y responsabilidades definidas, lo que incluye todos los activos en uso bajo propiedad o gestionados por parte de los clientes (arrendatarios).						
Puntos de acceso controlados	DCS-02	Los perímetros de seguridad física (p. ej., cercas, paredes, barreras, guardias, puertas, vigilancia electrónica, mecanismos de autenticación física, servicios de recepción y patrullas de seguridad) deberán implementarse para proteger los datos sensibles y los sistemas de información.	X					

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Identificación del equipamiento	DCS-03	La identificación automática de equipos deberá ser usada como método de autenticación. La tecnología de localización puede ser utilizada para validar la integridad de la autenticación, basada en la localización del equipamiento.	X	X	X	X	X	
Autorización para extraer activos	DCS-04	Se debe obtener autorización previa al traslado o traspaso de *hardware*, *software* o datos fuera de las instalaciones.	X			X		X
Equipamiento fuera de las instalaciones	DCS-05	Se debe establecer políticas y procedimientos apoyando los procesos de negocio implementados para el uso y la eliminación segura del mantenimiento de equipos y el uso fuera de las instalaciones de la organización.	X	X	X	X	X	X
Política	DCS-06	Se deberá establecer políticas y procedimientos apoyando los procesos de negocio implementados para mantener un entorno de trabajo seguro y protegido en oficinas, habitaciones, instalaciones y áreas seguras.	X					
Autorización de acceso a las áreas seguras	DCS-07	El acceso y la salida de las áreas seguras deben estar limitados y monitorizados por mecanismos de control de acceso físico para asegurar que solo al personal autorizado se le permita acceder.	X	X	X	X	X	X
Entrada de personas	DCS-08	En los puntos de acceso y salida como en las áreas de servicio y otros puntos a donde el personal no autorizado puede entrar, todos los permisos deber ser monitorizados, controlados y, si es posible, el entorno debe estar aislado del almacenamiento de datos y servicios de procesado, a fin de prevenir daños por acceso no autorizado a datos, su puesta en peligro y su pérdida.	X	X	X	X		
Acceso de usuarios	DCS-09	El acceso físico a los activos y las funciones de información por usuarios y personal de soporte debe estar limitado.	X					
Gestión de claves y cifrado								
Derechos	EKM-01	Todas las decisiones de derechos deberán derivarse de las identidades de las entidades involucradas. Estas identidades deberán estar gestionadas por un sistema de gestión de identidades corporativo. Las claves deben tener propietarios identificables (vinculando las claves a las identidades) y debe haber políticas de gestión de claves.						

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Generación de claves	EKM-02	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo para la gestión de claves criptográficas en los servicios (p. ej., la gestión del ciclo de vida desde la generación de la clave hasta la revocación y sustitución, la infraestructura de clave pública, el diseño del protocolo de criptografía y los algoritmos utilizados, el control de acceso en el lugar de generación de claves seguras, el intercambio y el almacenamiento con segregación de claves utilizadas para cifrar los datos o sesiones). A petición, los proveedores deberán informar a los clientes de los cambios dentro de los sistemas criptográficos, especialmente si los datos del cliente se utilizan como parte del servicio, y/o los clientes tienen alguna responsabilidad compartida sobre la implementación del control.		X		X	X	X
Protección de datos sensibles	EKM-03	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo para el uso de protocolos de cifrado con el fin de proteger datos sensibles ubicados en los sistemas de almacenamiento (p. ej., servidores de ficheros, bases de datos y estaciones de trabajo) y datos en transmisión (p. ej., interfaces de sistemas, redes públicas y mensajería electrónica). Todo esto, bajo el marco de la leyes aplicables, las obligaciones legales, reglamentarias y de cumplimiento regulatorio.		X	X	X	X	X
Acceso y almacenamiento	EKM-04	La criptografía fuerte (p. ej., AES256) en formatos abiertos/validados y los estándares de algoritmos deberán ser requeridos. Las claves no deben estar almacenadas en la nube (p. ej., en un proveedor de la nube). Las claves deberán ser mantenidas por el consumidor de la nube o el proveedor de gestión. La gestión de claves y el uso de las claves deberán tener funciones segregadas.						
Gobierno y gestión del riesgo								
Requerimientos básicos	GRM-01	Los requerimientos de seguridad básicos deberán estar establecidos para los desarrollos o adquisiciones, las propiedades o elementos gestionados por la empresa, tanto físicos como virtuales, incluyendo aplicaciones, sistemas infraestructuras y componentes de red, así como deberán estar alineados con los requisitos legales aplicables y las obligaciones de conformidad legal y normativa. Las desviaciones de la configuración estándar común deberán ser autorizadas, siguiendo políticas y procedimientos de gestión de cambios antes de su despliegue (desarrollo), abastecimiento o uso. El cumplimiento con los requerimientos de seguridad básicos deberán ser revisados al menos, anualmente, a menos que una frecuencia alternativa haya sido establecida y autorizada, basada en necesidades de negocio.	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Enfoque en los datos de las evaluaciones de riesgos	GRM-02	La evaluación de riesgos asociada con los requerimientos de gobierno de los datos se realizará a intervalos planificados y se considerarán los puntos que se enlistan a continuación. ▶ Concienciación del lugar donde los datos sensibles están almacenados y cómo se transmiten a través de las aplicaciones, las bases de datos, los servidores y la infraestructura de red. ▶ Cumplimiento con los periodos de retención definidos y los requerimientos de eliminación al final de su ciclo vida. ▶ Clasificación de datos y protección por uso no autorizado, acceso, pérdida, destrucción y falsificación.			X	X	X	X
Supervisión de la dirección	GRM-03	Los gerentes son los responsables de mantener la concienciación y cumplir con los requisitos, las políticas de seguridad, los procedimientos y las normas que son relevantes dentro de su área de responsabilidad.						
Programa de gestión	GRM-04	Un programa de gestión en seguridad de la información debe estar desarrollado, documentado, aprobado, e implementado, incluyendo medidas administrativas, técnicas y físicas dirigidas a proteger activos y datos de la pérdida, el acceso no autorizado, el uso indebido, la divulgación, la alteración y la destrucción. El programa de seguridad debe incluir, pero no debe estar limitado, por las áreas que se enlistan a continuación, desde el momento en que estas se encuentran relacionadas con las características del negocio: ▶ Gestión de riesgos. ▶ Política de seguridad. ▶ Organización de la seguridad. de la información. ▶ Gestión de activos. ▶ Seguridad de recursos humanos. ▶ Seguridad física y del entorno. ▶ Gestión de comunicaciones y operaciones. ▶ Control de acceso. ▶ Adquisición de sistemas de información, desarrollo y mantenimiento.	X	X	X	X	X	X
Soporte/implicación	GRM-05	La gerencia de línea y la dirección ejecutiva deberán tomar una acción formal para soportar la seguridad de la información a través de una dirección claramente documentada y un compromiso por el cual se asegure que todas las acciones han sido asignadas.						

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Política	GRM-06	Las políticas y los procedimientos de seguridad de la información deberán estar establecidos y estar fácilmente disponibles para su revisión por parte de todo el personal y las relaciones comerciales externas. Las políticas de seguridad de la información deberán estar aprobadas por la dirección de la empresa (u otro rol o función responsable del negocio) y deben apoyarse en un plan estratégico de negocio y un programa de gestión de seguridad de la información, lo que incluye la definición de roles de seguridad de información y responsabilidades para el liderazgo.						
Aplicación de la política	GRM-07	Deberá establecerse una política disciplinaria o sancionadora para los empleados que hayan violado las políticas y los procedimientos de seguridad. Los empleados deberán estar concienciados de que se puede tomar acciones en el caso de violación de la normativa. Asimismo, las medidas disciplinarias deberán estar declaradas en las políticas y procedimientos.						
Impacto de la política en las evaluaciones del riesgo	GRM-08	Los resultados de la evaluación de riesgos deberán incluir actualizaciones de las políticas de seguridad, de los procedimientos, de las normas y los controles, con el fin de asegurar que estos documentos permanecen relevantes y efectivos.	X	X	X	X	X	X
Revisiones de la política	GRM-09	La dirección de negocio (u otro rol o función de negocio responsable) deberá revisar la política de seguridad de la información a intervalos planificados o como resultado de cambios en la organización para asegurar su continuidad con la estrategia de seguridad, su efectividad, precisión, relevancia y aplicabilidad de las obligaciones legales, reglamentarias o de cumplimiento.						
Análisis de riesgo	GRM-10	Debe realizarse un análisis de riesgos formalizado y alineado con los objetivos de la empresa, al menos, una vez al año o a intervalos planificados, a fin de determinar la probabilidad y el impacto de todos los riesgos identificados mediante métodos cuantitativos o cualitativos. La probabilidad y el impacto asociado con el riesgo intrínseco y residual deberá estar determinado independientemente, considerando todas las categorías de riesgo (p. ej., con el resultado de las auditorías, el análisis de vulnerabilidades y amenazas y el cumplimiento normativo).	X	X	X	X	X	X
Sistema de gestión del riesgo	GRM-11	Las empresas desarrollarán y mantendrán un sistema de gestión de riesgos dirigido a mitigar el riesgo a un nivel aceptable.	X	X	X	X	X	X
Mitigación/ aceptación del riesgo	GRM-12	Los riesgos deben mitigarse a un nivel aceptable. Los niveles de aceptación basados en criterios de riesgo deben establecerse y documentarse conforme a un tiempo de resolución razonable y una aprobación ejecutiva.	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Recursos humanos								
Devolución de activos	HRS-01	A la finalización del contrato de trabajo y/o la finalización de las relaciones comerciales externas, los activos propiedad de la empresa deben ser devueltos dentro del periodo establecido.	X	X	X	X	X	X
Comprobación de antecedentes	HRS-02	Conforme a las leyes locales, las regulaciones, éticas y obligaciones contractuales, todos los candidatos a un empleo, empresa y terceras partes deberán estar sujetas a una comprobación proporcional a los datos que va a acceder, los requisitos de negocio y un riesgo aceptable.						X
Contratos laborales	HRS-03	Los contratos laborales deberán incorporar las cláusulas y/o los términos de cumplimiento para establecer el gobierno de la información y las políticas de seguridad y deberán ser firmados en las nuevas contrataciones o por el nuevo personal (p. ej., empleados a tiempo total o parcial o trabajadores eventuales), y siempre con anterioridad a proporcionar el acceso al usuario a los servicios de la empresa, recursos y activos.	X	X	X	X	X	X
Finalización de la relación laboral	HRS-04	Los roles y las responsabilidades para realizar la finalización del empleo o los cambios en procedimientos del trabajo deberán estar asignados, documentados y comunicados.						
Conocimiento de la industria y *benchmarking*	HRS-05	Deberá mantenerse un conocimiento del sector y comparativas de mercado mediante la red de contactos, los especialistas de foros de seguridad y las asociaciones profesionales.						
Gestión de dispositivos móviles	HRS-06	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo para gestionar el riesgo de negocio asociado a que esté permitido que los dispositivos móviles accedan a recursos corporativos, y pueden requerir de la implementación o controles compensatorios de seguridad más altos para su uso aceptable (p. ej., formación por mandato de seguridad, autenticación fuerte, derechos y controles de acceso y monitorización de dispositivos).	X	X	X	X	X	X
Acuerdos de confidencialidad	HRS-07	Los requerimientos para el acuerdo de no divulgación de secretos o los acuerdos de confidencialidad que reflejen las necesidades para la protección de datos y los detalles operacionales deberán ser identificados, documentados y revisados en intervalos planificados.						X
Roles/ responsabilidades	HRS-08	Los roles y las responsabilidades de contratistas, empleados y terceras partes deberán estar documentadas en lo que respecta a los activos de información y seguridad.	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Uso aceptables de la tecnología	HRS-09	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo dirigidas a definir los permisos y las condiciones que permitan el uso de dispositivos propiedad de la empresa o la gestión de los dispositivos de usuario (p. ej., estaciones de trabajo, portátiles y dispositivos móviles), la infraestructura de red IT y los componentes de sistemas. Además, los permisos y las condiciones que permitan el uso de dispositivos móviles personales y aplicaciones asociadas con acceso a recursos corporativos (p. ej., BYOD) deben ser considerados e incorporados como sea conveniente.					X	X
Formación/ concienciación	HRS-10	Un programa de concienciación debe establecerse para todos los proveedores, usuarios de terceras-partes y empleados de la empresa, así como exigirse cuando sea conveniente. Todas las personas con acceso a datos de la organización recibirán una formación de manera regular en los procedimientos de la organización, los procesos y las políticas relacionadas con su función profesional respecto a la organización.	X	X	X	X	X	X
Responsabilidad de los usuarios	HRS-11	Se deberá hacer consciente a todo el personal de sus roles y responsabilidades con miras a: • mantener el cumplimiento y concienciación respecto a las políticas y los procedimientos establecidos, así como con la legislación aplicable y las obligaciones de cumplimiento regulatorio; • mantener un entorno de trabajo seguro.	X	X	X	X	X	X
Lugares de trabajo	HRS-12	Las políticas y los procedimientos establecerán requerimientos para que en los lugares de trabajo sin personal presente no existan (p. ej., sobre la mesa) documentos de contenido sensible totalmente accesibles y las sesiones de usuario iniciadas en el equipo informático hayan sido bloqueadas tras un periodo determinado de inactividad.	X					X
Gestión de identidades y accesos								
Acceso a las herramientas de auditoría	IAM-01	El acceso y el uso de las herramientas de auditoría que interactúan con los sistemas de información de la organización estarán adecuadamente segmentados y restringidos con objeto de evitar que los datos de registro sean comprometidos o se haga un mal uso de estos.	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Ciclo de vida de las credenciales/ gestión del aprovisionamiento	IAM-02	Las políticas y los procedimientos de acceso de usuario se establecerán, así como el apoyo a los procesos de negocio y a las medidas técnicas implementadas, a fin de garantizar la identidad, el derecho y la gestión de acceso de todos los usuarios corporativos internos y del cliente con acceso a datos y aplicaciones de propiedad o administradas (física y virtual), infraestructura de red y componentes de sistemas. Estas políticas, así como los procedimientos, los procesos y las métricas deben incorporar los procesos que se describen a continuación. ▶ Procedimientos, funciones y responsabilidades de apoyo para el aprovisionamiento de los derechos de las cuentas de usuario siguiendo la regla del menor privilegio basado en la función de trabajo (p. ej., cambios en los empleados internos y eventuales, acceso controlado por el cliente, relaciones comerciales con proveedores u otras relaciones de negocio con terceros). ▶ Consideraciones de casos de negocios para los niveles más altos de garantía y autenticación de factores múltiples secretos (p. ej., consolas de administración, generación de claves, acceso remoto, segregación de funciones, acceso de emergencia, aprovisionamiento a gran escala o despliegues geográficamente distribuidos y redundancia de personal para los sistemas críticos). ▶ Segmentación de acceso a las sesiones y a los datos en arquitecturas multicliente por un tercero (p. ej., el proveedor u otro cliente). ▶ Comprobación de confianza de la identidad y de la aplicación servicio a servicio (API) y la interoperabilidad de procesamiento de información (por ejemplo, SSO y federación). ▶ Gestión del ciclo de vida de las credenciales de cuenta de instancias a través de la revocación. ▶ Minimización del almacenamiento de credenciales de cuenta y/o identidad, o reutilización cuando sea posible. ▶ Adhesión a reglas de autenticación, autorización y contabilidad (AAA) aceptables por la industria y/o de cumplimiento del regulador. ▶ Permisos y capacidades de soporte para el control del cliente sobre las reglas de autenticación, autorización y contabilidad (AAA) para el acceso a los datos y las sesiones. ▶ Cumplimiento de los requerimientos legales, estatutarios o regulatorios aplicables.	X	X	X	X	X	X
Acceso a puertos de diagnóstico/ configuración	IAM-03	El acceso de usuarios a los puertos de diagnóstico y configuración se limitará a personas y aplicaciones autorizadas.	X				X	
Políticas y procedimientos	IAM-04	Las políticas y procedimientos se establecerán para almacenar y gestionar la información de identidad sobre cada persona que accede a la infraestructura de TI y para determinar su nivel de acceso. Las políticas también deben ser desarrolladas para controlar el acceso a los recursos de red en función de la identidad del usuario.						

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Segregación de tareas	IAM-05	Las políticas y los procedimientos de acceso de usuario se establecerán, así como el apoyo a los procesos de negocio y las medidas técnicas implementadas, a fin de restringir el acceso de los usuarios de acuerdo con la segregación de las funciones definidas para hacer frente a los riesgos de negocio asociados a un conflicto de intereses de usuario.	X	X	X	X	X	X
Restricciones en el acceso al código fuente	IAM-06	El acceso a las aplicaciones desarrolladas por la propia organización, el programa, el objeto de código fuente o cualquier otra forma de propiedad intelectual (PI), así como el uso de *software* propietario será debidamente restringido siguiendo la regla del menor privilegio basado en las funciones del puesto de trabajo, así como por las políticas y los procedimientos establecidos de acceso de usuarios.			X	X	X	X
Acceso por terceros	IAM-07	La identificación, evaluación y priorización de los riesgos planteados por los procesos de negocio que requieren acceso de terceros a los datos y sistemas de información de la organización deberán ir seguidos de la aplicación coordinada de recursos para minimizar, monitorizar y medir la probabilidad y el impacto de accesos no autorizados o inapropiados. Los controles compensatorios derivados del análisis de riesgos se implantarán antes de la provisión de acceso.	X	X	X	X	X	X
Fuentes de confianza	IAM-08	Las políticas y los procedimientos se establecen con el propósito de permitir el almacenamiento y el acceso de las identidades utilizadas para la autenticación, a fin de garantizar que las identidades solo son accesibles con base en las reglas de privilegios mínimos y la limitación de la replicación, solo para usuarios definidos explícitamente como necesarios para el negocio.						
Autorización del acceso de usuarios	IAM-09	El aprovisionamiento del acceso de los usuarios (p. ej., empleados, contratistas, clientes, socios comerciales y/o proveedores) a los datos y aplicaciones de propiedad o gestionadas (físicas y virtuales), los sistemas de infraestructura y los componentes de la red deberán ser autorizados por la gestión de la organización antes de acceder a su concesión y apropiadamente restringido según las políticas y procedimientos establecidos. Previa solicitud, el proveedor deberá informar al cliente (arrendatario) de este acceso de usuario, sobre todo si los datos del cliente se usan como parte del servicio o el cliente tiene parte de la responsabilidad compartida en la aplicación del control.		X	X	X	X	X
Revisiones del acceso de usuarios	IAM-10	A intervalos planificados, el acceso del usuario estará autorizado y revalidado por la idoneidad del derecho, por la dirección de negocio de la organización u otro rol o función de negocio responsable con el apoyo de pruebas que demuestren que la organización está adherida a la regla del menor privilegio basado en la función de trabajo. Para violaciones de acceso identificadas, la remediación debe seguir las políticas y procedimientos de acceso de usuario establecidos.	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Revocación del acceso de usuarios	IAM-11	El desaprovisionamiento (revocación o modificación) del acceso de los usuarios a los datos y aplicaciones de propiedad o gestionadas (físicas y virtuales), los sistemas de infraestructura y los componentes de red, se llevará a cabo según las políticas, los procedimientos y sobre la base del cambio de estado del usuario (p. ej., finalización del empleo u otra relación de negocio, cambio de trabajo o traslado). Previa solicitud, el proveedor deberá informar al cliente de estos cambios, especialmente si los datos del cliente se utilizan como parte del servicio o el cliente tiene alguna responsabilidad compartida sobre la implementación del control.	X	X	X	X	X	X
Credenciales de identidad (ID) de usuarios	IAM-12	Las credenciales de las cuentas de los usuarios corporativos internos o de los clientes se limitarán garantizando la identidad apropiada, el derecho y la gestión de los accesos de acuerdo con las políticas y los procedimientos establecidos: ▶ comprobación de confianza de identidad y aplicación de servicio a servicio (API) y la interoperabilidad de procesamiento de información (p. ej., SSO y federación); ▶ gestión del ciclo de vida de las credenciales de cuenta de instancias a través de la revocación; ▶ minimización del almacenamiento de credenciales de cuenta y/o identidad, o reutilización cuando sea posible; ▶ adhesión a reglas de autenticación, autorización y contabilidad (AAA) aceptables por la industria y/o de cumplimiento del regulador (p. ej., multifactor robusto, caducidad, secretos de autenticación no compartidos).		X	X	X	X	
Acceso a los programas de utilidades	IAM-13	Los programas de utilidades potencialmente capaces de anular sistemas, objetos, redes, máquinas virtuales y los controles de aplicación deberán estar restringidos.		X	X	X	X	X
Seguridad de la infraestructura y virtualización								
Registros de auditoría/detección de intrusiones	IVS-01	Se requieren los niveles más altos de garantía para la protección, la conservación y la gestión del ciclo de vida de los registros de auditoría, en adhesión a las obligaciones de cumplimiento legal, estatutarias o reglamentarias aplicables y proporcionando cuentas de acceso de usuario únicas para detectar comportamientos en la red potencialmente sospechosos y/o anomalías de integridad de ficheros, así como a fin de apoyar las capacidades de investigación forense en el caso de un fallo de seguridad.	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Detección de cambios	IVS-02	El proveedor deberá garantizar en todo momento la integridad de todas las imágenes de las máquinas virtuales. Cualquier cambio realizado en las imágenes de las máquinas virtuales debe ser registrado y una alerta planteada independientemente de su estado de ejecución (p. ej., en estado latente, apagado o en funcionamiento). Los resultados de un cambio o movimiento de una imagen y la posterior validación de la integridad de la imagen deben estar inmediatamente disponibles para los clientes a través de medios electrónicos (p. ej., portales o alertas).						
Sincronización de relojes	IVS-03	De mutuo acuerdo se utilizará una fuente horaria externa fiable para sincronizar los relojes del sistema de todos los sistemas de procesamiento de información relevantes, con la finalidad de facilitar el seguimiento y la reconstitución de las líneas de tiempo de actividad.		X	X		X	
Documentación de los sistemas de información	IVS-04	La disponibilidad, calidad y capacidad adecuadas y los recursos serán planeados, preparados y medidos para ofrecer el rendimiento del sistema requerido de conformidad con las obligaciones legales, estatutarias y reglamentarias. Se llevarán a cabo simulaciones de las futuras necesidades de capacidad para mitigar el riesgo de sobrecarga del sistema.		X	X	X		X
Gestión de las vulnerabilidades	IVS-05	Los implementadores garantizarán que las herramientas o servicios de evaluación de vulnerabilidades de seguridad se adaptan a las tecnologías de virtualización utilizadas (p. ej., la virtualización).						
Seguridad de la red	IVS-06	Los entornos de red y las instancias virtuales estarán diseñados y configurados para restringir y monitorizar el tráfico entre conexiones fiables y no fiables, serán revisados a intervalos planificados, respaldados por justificaciones de negocio documentadas para el uso de todos los servicios, protocolos y puertos permitidos, lo que incluye las razones o los controles compensatorios implementados para aquellos protocolos considerados inseguros. Los diagramas de arquitectura de red deben identificar claramente los entornos de alto riesgo y los flujos de datos que pueden tener impacto en el cumplimiento legal, estatutario y reglamentario. Se implementarán medidas técnicas con el fin de aplicar técnicas de defensa en profundidad (por ejemplo, el análisis profundo de paquetes, estrangulamiento de tráfico y filtrado de agujero negro) para la detección y la respuesta oportuna a los ataques basados en red asociados con patrones de tráfico de entrada o salida anómalos (p. ej., suplantación de MAC y ataques de envenenamiento de ARP) y/o ataques de denegación de servicio distribuidos de (DDOS).	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Bastionado de sistema operativo y controles básicos	IVS-07	Cada sistema operativo deberá ser fortalecido para proporcionar solo los puertos necesarios, los protocolos y servicios que permitan satisfacer las necesidades del negocio y tener vigentes los controles técnicos de apoyo tales como antivirus, integridad de los ficheros de monitorización y el inicio de sesión como parte de su línea base de operativa estándar o plantilla.						
Entornos de producción y no producción	IVS-08	Los entornos de producción y de no producción deberá estar separados para evitar accesos o cambios no autorizados en los activos de información.	X	X	X	X	X	X
Segmentación	IVS-09	Las aplicaciones multicliente ya sean de propiedad o administradas (físicas y virtuales), y el sistema de infraestructura y componentes de red, deberán estar diseñados, desarrollados, desplegados y configurados de tal manera que el acceso del proveedor y del cliente esté adecuadamente segmentado de los demás clientes, con base en las siguientes consideraciones: ▶ políticas y procedimientos establecidos; ▶ aislamiento de los activos críticos de negocio y/o información confidencial del usuario y sesiones que exigen controles internos robustos y altos niveles de garantía; ▶ cumplimiento de las obligaciones legales, estatutarias y reglamentarias.	X	X	X	X	X	X
Seguridad de las máquinas virtuales (VM)-protección de los datos en las migraciones (vMotion)	IVS-10	Se utilizarán canales de comunicación securizados y cifrados para migrar servidores físicos, aplicaciones o datos a servidores virtualizados y, si es posible, se utilizará una red segregada de la red de producción para este tipo de migraciones.						
Seguridad VMM-bastionado del hypervisor	IVS-11	El acceso a todas las funciones de administración del hipervisor o consolas de administración para sistemas de *hosting* virtualizados estará restringido a personal con base en el principio de privilegios mínimos y apoyado a través de controles técnicos (p. ej., autenticación de dos factores, *logs* de auditoría, filtrado de direcciones IP, *firewalls* y encapsulado de comunicaciones bajo TLS a las consolas administrativas).						

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Seguridad inalámbrica	IVS-12	Se establecerán políticas y procedimientos, así como apoyo a los procesos de negocio y las medidas técnicas implementadas, para proteger los entornos de red inalámbrica, incluyendo los que se enlistan a continuación. ▶ *Firewalls* perimetrales implementados y configurados para restringir el tráfico no autorizado. ▶ Configuraciones de seguridad habilitadas con cifrado robusto para la autenticación y transmisión reemplazando la configuración por defecto del fabricante (p. ej., claves de cifrado, contraseñas y SNMP *community strings*). ▶ Acceso de usuario a dispositivos de red inalámbricos restringido a personal autorizado. ▶ Capacidad de detectar la presencia de dispositivos de red inalámbricos no autorizados (*rogue*) para una desconexión oportuna de la red.	X	X	X	X	X	X
Interoperabilidad y portabilidad								
APIS	IPY-01	El proveedor deberá usar APIS abiertas y publicadas para asegurar el más amplio apoyo con miras a la interoperabilidad entre componentes y facilitar la migración de aplicaciones.						
Peticiones de datos	IPY-02	Todos los datos no estructurados estarán a disposición de los clientes y se les proporcionará bajo petición en un formato estándar de la industria (p. ej., *.doc*, *.xls* o *.pdf*).						
Políticas y legislación	IPY-03	Políticas, procedimientos, disposiciones y/o términos de mutuo acuerdo serán establecidos para satisfacer los requerimientos del cliente (arrendatario) en su aplicación-servicio-servicio (API) y el procesamiento de información de interoperabilidad y portabilidad para el desarrollo de aplicaciones y el intercambio de información, el uso y la persistencia de integridad.						
Protocolos de red estandarizados	IPY-04	El proveedor deberá utilizar protocolos de red estandarizados y seguros (p. ej., el texto no plano y autenticado) para la importación y exportación de datos y administrar el servicio. También pondrá a disposición de los consumidores (los arrendatarios) un documento que detalle los estándares de interoperabilidad y portabilidad relevantes que estén involucrados.						
Virtualización	IPY-05	El proveedor deberá utilizar una plataforma de virtualización reconocida por la industria y formatos estándares de virtualización (p. ej., OVF) para ayudar a asegurar la interoperabilidad. A disposición del cliente, con miras a su revisión, tendrá documentados los cambios de personalización realizados en cualquier hipervisor en uso y en todos los ganchos de soluciones específicas de virtualización.						

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Seguridad móvil								
Antimalware	MOS-01	Se deberá incluir la concienciación antimalware, específica para dispositivos móviles, dentro de la formación en seguridad de la información del proveedor.						
Tiendas de aplicaciones	MOS-02	La compañía deberá tener una lista documentada e informada de las tiendas de aplicaciones aprobadas que hayan sido identificadas como aceptables para dispositivos móviles que accedan o almacenen datos y/o sistemas de la compañía.						
Aplicaciones aprobadas	MOS-03	La compañía deberá tener una política documentada que prohíba la instalación de aplicaciones no aprobadas o que aún aprobadas no hayan sido obtenidas a través de una tienda de aplicaciones identificada previamente.						
Software aprobado para BYOD	MOS-04	La política de BYOD y su correspondiente formación de concienciación sobre su uso deberán exponer claramente las aplicaciones y tiendas aprobadas que pueden ser empleadas.						
Formación y concienciación	MOS-05	El proveedor deberá tener una política de dispositivos móviles documentada que incluya una definición de dispositivos móviles, así como de su uso y requisitos aceptables. El proveedor deberá publicar y comunicar tanto la política como los requisitos a través del programa de formación y de concienciación en seguridad.						
Servicios basados en la nube	MOS-06	Todos los servicios basados en la nube empleados por los dispositivos móviles corporativos o BYOD deberán ser previamente aprobados para el uso y almacenamiento de datos de negocio corporativos.						
Compatibilidad	MOS-07	La compañía deberá tener un procedimiento documentado para la validación de aplicaciones que compruebe el dispositivo, el sistema operativo y los problemas de compatibilidad de la aplicación.						
Idoneidad de dispositivos	MOS-08	La política de BYOD deberá definir los requisitos de los dispositivos y su idoneidad para permitir su uso como BYOD.						
Inventario de dispositivos	MOS-09	Se deberá almacenar y conservar un inventario de todos los dispositivos móviles empleados para acceder y almacenar datos corporativos. Todos los cambios en el estado de estos dispositivos (p. ej., sistema operativo, niveles de parcheo, pérdida o retirada del dispositivo y a quien se asigna o permite el uso BYOD) deberán ser incluidos para cada dispositivo en dicho inventario.						
Gestión de dispositivos	MOS-10	La compañía deberá tener desplegada una solución centralizada de gestión de dispositivos móviles para todos los dispositivos permitidos para almacenar, transmitir o procesar información corporativa.						

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Cifrado	MOS-11	La política de dispositivos móviles deberá requerir el uso de cifrado bien sea para el dispositivo completo, o bien para los datos identificados como sensibles en todos los dispositivos; esta medida deberá cumplirse mediante controles tecnológicos.						
Jailbreaking y *rooting*	MOS-12	La política de dispositivos móviles deberá prohibir eludir los controles de seguridad integrados en los dispositivos móviles (p. ej., *jailbreaking* o *rooting*) y deberá cumplirse a través de controles tanto detectivos como preventivos, ya sea en el propio dispositivo o mediante un sistema de gestión de dispositivos centralizado.						
Seguridad móvil requisitos legales	MOS-13	La política de BYOD debe incluir en un lenguaje claro las expectativas de privacidad, los requisitos de litigio, la localización de evidencias electrónicas y las retenciones jurídicas. Debe a su vez exponer claramente la posibilidad de la pérdida de datos que no sean de la compañía si es necesario un borrado de los datos del dispositivo.						
Bloqueo de pantalla	MOS-14	Los dispositivos BYOD o corporativos deberán requerir un bloqueo de pantalla automático, y este requisito deberá cumplirse a través de controles técnicos.						
Sistemas operativos	MOS-15	Los cambios en los sistemas operativos, los niveles de parcheo o las aplicaciones de los dispositivos móviles deberán ser gestionados a través de los procesos de gestión del cambio de la compañía.						
Contraseñas	MOS-16	Las políticas de contraseñas aplicables a dispositivos móviles deberán estar documentadas y ejecutadas a través de controles técnicos en todos los dispositivos corporativos o aprobados para su uso como BYOD y deberán prohibir tanto el cambio de la longitud de las contraseñas/PIN como los requisitos de autenticación.						
Política	MOS-17	La política de dispositivos móviles deberá requerir al usuario de BYOD que realice copias de seguridad de los datos, prohibirle el uso de tiendas de aplicaciones no autorizadas, y requerirle el uso de programas antimalware (donde esté soportado).						
Borrado remoto	MOS-18	Todos los dispositivos móviles cuyo uso se permita a través del programa de BYOD de la compañía y/o los dispositivos corporativos deberán permitir el borrado remoto por el personal de TI corporativo de la compañía, o todos los datos corporativos deberán ser borrados por dicho personal.						
Parches de seguridad	MOS-19	Los dispositivos móviles que se conecten a redes corporativas o almacenen/accedan a información de la compañía deberán permitir la validación y descarga de los últimos parches de seguridad por parte del personal TI de la compañía. Todos los dispositivos móviles deberán de tener instalados los últimos parches de seguridad disponibles por parte del operador o el fabricante del dispositivo.						

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Usuarios	MOS-20	La política de BYOD deberá clarificar los sistemas y servidores permitidos para el uso o acceso desde de un dispositivo habilitado para BYOD.						
Gestión de incidentes de seguridad, localización de evidencias electrónicas, investigaciones forenses en la nube								
Puntos de contacto con las autoridades	SEF-01	Se deberán mantener disponibles y actualizados los puntos de contacto de las fuerzas de seguridad locales y nacionales, autoridades legislativas aplicables y otras autoridades con jurisdicción legal (sobre todo, en caso de cambios en el alcance o en las obligaciones de cumplimiento), de modo que se asegure el establecimiento directo de los enlaces correspondientes y la disposición para una investigación forense que requiera una participación rápida de las fuerzas de seguridad.	X	X	X	X	X	X
Gestión de incidentes	SEF-02	Se deberán establecer procedimientos y políticas, así como medidas técnicas y procesos de negocio de apoyo, que permitan la evaluación y clasificación de eventos de seguridad y garanticen una gestión completa y a tiempo de los incidentes así como sea establecido en las políticas y procedimientos de gestión de servicios TI.	X	X	X	X	X	X
Comunicación de incidentes	SEF-03	Se deberá informar a los trabajadores y a las empresas externas relacionadas acerca de sus responsabilidades y, si fuera necesario, deberán dar su consentimiento o aceptar contractualmente a informar prontamente de todos los eventos de seguridad. Los eventos de seguridad deberán ser comunicados a través de canales de comunicación predefinidos oportunamente cumpliendo con las obligaciones legales, reglamentarias o de cumplimiento regulatorio aplicables.	X	X	X	X	X	X
Preparaciones legales para la respuesta ante incidentes	SEF-04	En el caso de que una investigación posterior que afecte a una persona u organización después de un incidente de seguridad requiera acciones legales se exige el seguimiento de los debidos procedimientos forenses, incluyendo la cadena de custodia, para la preservación y presentación de las pruebas que apoyen dichas acciones legales ante la jurisdicción pertinente. Tras la notificación, los clientes (arrendatarios) o las relaciones con otras empresas externas que hayan sido afectadas por una violación de seguridad deberán tener la oportunidad de participar como sea legalmente posible en la investigación forense.	X	X	X	X	X	X
Métricas de la respuesta ante incidentes	SEF-05	Se deberán implantar los mecanismos que permitan monitorizar y cuantificar los tipos, las cantidades y los costes de los incidentes de seguridad de la información.	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Gestión de la cadena de suministro, transparencia y responsabilidad								
Calidad de datos e Integridad	STA-01	Los proveedores deberán inspeccionar y ser responsables de los errores y riesgos en la calidad de los datos heredados de sus socios dentro de la cadena de suministro de la nube. Los proveedores deberán diseñar e implementar controles que mitiguen y contengan los riesgos de seguridad de los datos a través de una debida separación de tareas, acceso basado en roles y acceso de mínimo privilegio para todo el personal dentro de su cadena de suministro.						
Comunicación de incidentes	STA-02	El proveedor deberá facilitar la información de incidentes de seguridad a todos los clientes y proveedores afectados de forma periódica a través de medios electrónicos (p. ej., portales).						
Servicios de red/ infraestructura	STA-03	Los componentes de la infraestructura de sistemas y redes, así como el diseño y configuración de las aplicaciones (físicas y virtuales) y de los interfaces sistema-sistema (API) que sean críticos para el negocio o que impacten al cliente (arrendatario) deberán ser diseñados, desarrollados y desplegados de acuerdo con unas expectativas de nivel de servicio y la capacidad acordadas previamente, así como de acuerdo a las políticas y procedimientos de gestión de servicio y gobernanza TI.	X	X	X	X	X	X
Evaluaciones internas del proveedor	STA-04	El proveedor deberá realizar anualmente evaluaciones internas del cumplimiento y efectividad de sus políticas, procedimientos, medidas de apoyo y métricas.						
Acuerdos relativos a la cadena de suministro	STA-05	Los acuerdos de la cadena de suministro (por ejemplo, SLA) entre proveedores y clientes (arrendatarios) contendrán al menos las siguientes mutuamente acordadas disposiciones y/o los términos: ▸ Alcance de la relación comercial y de servicios que se ofrece (p. ej., adquisición de datos del cliente (arrendatario), el intercambio y el uso, conjuntos de características y funcionalidad, el personal y la infraestructura de red y componentes de los sistemas de prestación de servicios y apoyo, roles y responsabilidades de proveedor y cliente (arrendatario) y cualquier relación comercial subcontratada o externalizada, la ubicación geográfica física de los servicios de hospedaje, y cualquier aspecto de cumplimiento regulatorio conocidos). ▸ Los requisitos de seguridad de la información, los puntos de contacto principales durante la duración de la relación comercial del proveedor y el cliente (arrendatario), y las referencias a la información detallada de apoyo y procesos de negocio relevantes y medidas técnicas implementadas para permitir el gobierno efectivo, la gestión de riesgos y cumplimiento de las obligaciones de seguridad, legales, estatutaria y normativas por todas las partes afectadas.	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Acuerdos relativos a la cadena de suministro	STA-05	▶ Notificación o pre-autorización los cambios controlados por el proveedor con impacto en el cliente (arrendatario). ▶ La notificación a tiempo de un incidente de seguridad (o brecha de seguridad confirmada) a todos los clientes (arrendatarios) y otras partes afectadas (es decir, hacia arriba y debajo de la cadena de suministro afectada). ▶ Evaluación y verificación independiente del cumplimiento de las disposiciones del acuerdo y/o términos (p. ej., la certificación aceptable para la industria, el informe de auditoría de certificación, o formas equivalentes de aseguramiento) sin representar un riesgo de negocio inaceptable de la exposición para la organización que está siendo evaluada. ▶ Finalización de la relación comercial y el tratamiento de los datos del cliente (arrendatario) afectados. ▶ El cliente (arrendatario) de una aplicación servicio a servicio (API) y los requerimientos de interoperabilidad y portabilidad de los datos para el desarrollo de aplicaciones y el intercambio de información, el uso y la persistencia de la integridad.	X	X	X	X	X	X
Revisión de la gobernanza de la cadena de suministro	STA-06	Los proveedores deberán revisar los procesos de gestión de riesgos y de gobernanza de sus socios para garantizar que sus prácticas son consistentes y alineadas con el hecho de hacerse responsables de los riesgos heredados de otros miembros de la cadena de suministro de la nube de dicho socio.						
Métricas de la cadena de suministro	STA-07	Se deberán establecer procedimientos y políticas, así como medidas técnicas y procesos de negocio de apoyo, que permitan mantener los acuerdos debidos (p. ej., SLA) entre proveedores y clientes (arrendatarios) de forma completa y precisa. Se deberá tener a su vez la capacidad de medir y abordar las no conformidades en las disposiciones o términos a lo largo de toda la cadena de suministro (hacia arriba y hacia abajo) y de gestionar los conflictos o inconsistencias en los niveles de servicio resultantes de las diversas relaciones entre proveedores.						
Evaluación por parte de terceros	STA-08	Los proveedores deberán garantizar una seguridad de la información razonable a lo largo de su cadena de suministro realizando revisiones regulares. Estas revisiones deberán incluir a todos los socios de los que dependa su cadena de suministro.						
Auditorías por parte de terceros	STA-09	Los proveedores de servicios a terceros deberán demostrar el cumplimiento con los requisitos de seguridad de la información y confidencialidad, definiciones de servicio y acuerdos de prestación de servicio incluidos en los contratos de terceros. Los informes, registros y servicios de terceros deberán someterse a revisiones y auditorías a intervalos planificados para mantener y gobernar el cumplimiento con los acuerdos de prestación del servicio.	X	X	X	X	X	X

Continúa en la siguiente página ▶

Control	CCM V3.0 Control ID	Descripción del control	Relevancia arquitectónica F: física R: red C: cálculo Am: almacenamiento A: Aplicación D: Datos					
			F	R	C	Am	A	D
Gestión de vulnerabilidad y amenazas								
Antivirus/*software* malicioso	TVM-01	Se deberán establecer procedimientos y políticas, así como medidas técnicas y procesos de negocio de apoyo que prevengan la ejecución de *malware* en dispositivos finales propiedad de la organización o gestionados por el usuario (p. ej., estaciones de trabajo asignadas, portátiles y dispositivos móviles) y en los componentes de la infraestructura de sistemas y redes TI.		X	X	X	X	
Gestión de parches y vulnerabilidades	TVM-02	Se deberán establecer procedimientos y políticas, así como medidas técnicas y procesos de negocio de apoyo para la detección temprana de vulnerabilidades dentro de los componentes de los sistemas y redes de la infraestructura propiedad de la organización (físicos o virtuales) o de las aplicaciones gestionadas, aplicando un modelo basado en riesgos que priorice la mitigación a través un control de cambios, parches del fabricante, cambios en la configuración o desarrollo seguro de *software* de la propia organización. El proveedor deberá informar, bajo petición del cliente (arrendatario) de estas políticas y procedimientos, especialmente si se usan datos del cliente (arrendatario) como parte del servicio o el cliente (arrendatario) tiene parte de responsabilidad compartida sobre el desarrollo de los controles.		X	X	X	X	
Código móvil	TVM-03	Se deberán establecer procedimientos y políticas, así como medidas técnicas y procesos de negocio de apoyo que prevengan la ejecución de código móvil no autorizado, entendido como *software* que se transfiere entre sistemas a través de una red fiable o no fiable y que es ejecutado en un sistema local sin ejecución o instalación explícitas por el destinatario en dispositivos finales propiedad de la organización o gestionados por el usuario (p. ej., estaciones de trabajo asignadas, portátiles y dispositivos móviles) y en los componentes de la infraestructura de sistemas y redes TI.		X	X		X	X

Fuente: Cloud Security Alliance (2018b).

▶ Referencias

AENOR. (2008). *Norma española UNE 71504. Metodología de análisis y gestión de riesgos para los sistemas de información*.

Albanese, D. E., López, M. de los A. y Sánchez, M. A. (2013). Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la República Argentina. *Contaduría y Administración*, *59*(3), 61-88.

Aloini, D., Dulmin, R. y Mininno, V. (2007). Risk management in ERP project introduction: review of the literature. *Information and Management*, *44*(6), 547-567. doi: https://doi.org/10.1016/j.im.2007.05.004

Almanza, A. (2019). XVIII Encuesta Nacional de Seguridad Informática. Evolución del perfil del profesional de seguridad digital. *Sistemas*, 147, 16-42. doi: https://doi.org/DOI: 10.29236/sistemas.n147a4 XVIII Encuesta Nacional de Seguridad Informática. Evolución del perfil del profesional de seguridad digital

Altamirano, J. R. y Bayona, S. (2017). Políticas de seguridad de la información: revisión sistemática de las teorías que explican su cumplimiento. *Revista Ibérica de Sistemas y Tecnologías de Información*, 25, 112-134. Recuperado de https://doi.org/DOI:10.17013/risti.25.0

SI. (2013). *Moving from ISO/IEC 27001 : 2005 to ISO/IEC 27001 : 2013*. Recuperado de https://www.bsigroup.com/LocalFiles/en-AE/Risk/ISO%2027001/ISO%20IEC%2027001%20Transition%20guide%20-%20March%202014.pdf

Buecker, A., Borrett, M., Lorenz, C. y Powers, C. (2010). *Introducing the IBM security framework and IBM security blueprint to realize business-driven security*. Recuperado de http://www.redbooks.ibm.com/redpieces/pdfs/redp4528.pdf

Calder, A. (2006). *Nueve claves para el éxito. Una visión general de la implementación de la norma NTC-ISO/IEC 27001*. Bogotá: Icontec.

Cano, J. J. (2011). Información: evolución y retos emergentes. *ISACA Journal*, 5, 1-5.

Cano, J. J. (2013). *Inseguridad de la información*. Bogotá: Alfaomega.

Cano, J. J. y Saucedo, G. (2016). *VIII Encuesta Latinoamericana de Seguridad de la Información*. Recuperado de http://acis.org.co/archivos/JornadaSeguridad/ENCUESTA LATINOAMERICANA.pdf

Cano, J. J., Saucedo M., G. M. y Chávez, R. (2014). *V Encuesta Latinoamericana de Seguridad de la Información*. Recuperado de https://es.scribd.com/document/325201865/V-Encuesta-latinoamericana-de-seguridad-de-la-informacion-Informe-2014

Carter, M. y Treu, J. (2017). *ISO/IEC 27002:2013 control cross check*. Recuperado de www.iso27001security.com/ISO27k_Controls_cross_check_2013

Chou, D. C. (2015). Cloud computing risk and audit issues. *Computer Standards and Interfaces*, 42, 137-142. doi: https://doi.org/10.1016/j.csi.2015.06.005

CISCO. (2017). *CISCO 2071 annual cibersecurity report*. Recuperado de https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

Cloud Security Alliance. (2018). *Cloud controls matrix v3.0.1*. Recuperado de https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

Díaz, A. (2010). Sistema de gestión de la seguridad de la información. *Revista Calidad*, IV, 18-20.

Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica. (2012). *Magerit-versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I-Método*. Madrid: Ministerio de Hacienda y Administraciones Públicas.

Fernández Sánchez, C. M y Piattini, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO*. Madrid: AENOR Ediciones.

Georgiou, D. y Lambrinoudakis, C. (2015). *E-democracy. Citizen rights in the world of the new computing paradigms*. Springer International Publishing Switzerland. doi: https://doi.org/10.1007/978-3-319-27164-4

Gesconsultor. (2015). *Gestor de proyectos SGSI*. Recuperado de http://www.gesconsultor.com/integracion/gestion-de-proyectos.html

Gómez Fernández, L. y Fernández Rivero, P. P. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el esquema nacional de seguridad*. Madrid: AENOR.

Grobauer, B., Walloschek, T. y Stöcker, E. (2011). Understanding cloud computing vulnerabilities. *IEEE Security and Privacy*, *9*(2), 50-57. doi: https://doi.org/10.1109/MSP.2010.115

IBM. (2011). *Gestionar las amenazas en la era digital. Abordad la seguridad, el riesgo y el cumplimiento desde la alta dirección*. Somers, NY. Recuperado de https://www-05.ibm.com/services/es/bcs/pdf/gestionarlas-las-amenazas-en-la-era-digital.pdf

Icontec. (2009a). *Compendio sistema de gestión de la seguridad de la información (SGSI)*. Bogotá.

Icontec. (2009b). *Norma Técnica Colombiana. NTC-ISO-IEC 27005. Tecnología de información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información*. Bogotá.

Icontec. (2012). *Guía Técnica Colombiana GTC-ISO/IEC 27035. Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información*. Bogotá.

Icontec. (2013). *Norma Técnica Colombia NTC-ISO-IEC 27001. Tecnologías de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos*. Bogotá.

Iqbal, J., Farid, S., Qadir, M. y Khan, M. (2017). Significant risks of outsourced IT projects. *Technical Journal*, *22*(II), 90-97.

ISACA. (2012a). *Cobit 5. A business framework for the governance and management of enterprise IT*. Rolling Meadows, Illinois.

ISACA. (2012b). *Cobit 5. Procesos catalizadores*. Rolling Meadows, Illinois.

ISACA. (2012c). Cobit 5. *Un marco de negocio para el gobierno y la gestión de las TI de la empresa*. Rolling Meadows, Illinois.

ISACA. (2012d). *Cobit for Information Security. Preview version*. Rolling Meadows, Illinois.

ISACA. (2012e). *Manual de Preparación del examen CISM 2013*. Rolling Meadows, Illinois.

ISACA. (2013). *Manual de preparación del examen CISM 2013*. Rolling Meadows, Illinois.

ISO/IEC. (2014a). *International standard ISO/IEC 27000. Information technology-Security techniques-Information security management systems-Overview and vocabulary* (Vol. 2014).

ISO/IEC. (2014b). ISO/IEC 17788. *Information technology-Cloud computing-Overview and vocabulary*.

ISO/IEC. (2018a). *International Standard ISO/IEC Information technology-Security techniques-Information security management systems-Overview and vocabulary* (vol. 2018). Recuperado de http://k504.khai.edu/attachments/article/819/ISO_27000_2014.pdf

ISO/IEC. (2018b). *International Standard ISO/IEC Information technology-Security techniques-Information security management systems-Overview and vocabulary* (vol. 2018).

ISO. (2015). *ISO/IEC 27002:2013. Information technology-Security techniques-Code of practice for information security controls*. Recuperado de http://www.iso.org/iso/catalogue_detail?csnumber=54533

ISO. (2019). *ISO Survey of certifications of ISO/IEC 27001*. Recuperado de fhttps://isotc.iso.org/livelink/livelink?slice=17917648&searchbarwidgetmode=fulltext&where1=27001&ScopeSelection=17917648%7C8853511%7CWithin+Library&lookfor1=allwords&modifier1=relatedto&boolean2=And&lookfor2=complexquery&typeDropDownId=1&boolean3=And&lookfor3=complexquery&dateDropDownId=1&func=search&objType=258&SearchBarSearch=TRUE&location_id1=8853511&facets=user&fulltextMode=allwords

ITSMF International. (2007). *IT Service Management Based on ITIL V3. A pocket guide*. Van Haren Publishing.

ITU. (2008). *Recomendación UIT-T X.1205. Aspectos generales de la ciberseguridad*. Ginebra, Suiza. Recuperado de https://www.itu.int/rec/T-REC-X.1205-200804-I

Joyanes Aguiilar, L. (2017). *Industria 4.0. La cuarta revolución industrial*. Bogotá: Alfaomega.

Leung, V. C. M., y Chen, M. (2014). Cloud computing: 4th International Conference, CloudComp 2013. Wuhan, China, October 17–19, 2013 Revised Selected Papers. *Lecture notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 133, 132-141. doi:_https://doi.org/10.1007/978-3-319-05506-0

Martínez Contreras, M. del M. (2016). *Estudio de la oferta de certificaciones en seguridad informática*. Universidad Politécnica de Madrid.

Matalobos, J. M. (2009). *Análisis de riesgos de seguridad de la información*. Madrid: Universidad Politécnica de Madrid.

Mejía Quijano, R. C. (2013). *Identificación de riesgos*. Medellín: Fondo Editorial Universidad Eafit.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2011). *Metodología de gestión del riesgo. Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0*. Bogotá.

Montenegro, L. (2015). *Seguridad de la información: más que una actitud, un estilo de vida*. Recuperado de http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/

Morán Abad, L., Pérez Sánchez, A., Trujillo Gaona, J., Bathiely Fernández, D. y González-Simancas, M. J. (2010). *ISO/IEC 20000. Guía completa de aplicación para la gestión de los servicios de tecnologías de la información*. AENOR Ediciones.

Newton, I. (2019). *Gestión del conocimiento e innovación: factores estratégicos para el desarrollo de México en la cuarta transformación. Políticas*, 121.

NIST. (2004). *FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems*. Recuperado de https://csrc.nist.gov/publications/detail/fips/199/final

NIST. (2014). *Assessing security and privacy controls in federal information systems and organizations. Building effective assessment plans. Sp-800-53Ar4*. doi: https://doi.org/10.6028/NIST.SP.800-53Ar4

NIST. (2018). *Framework for improving critical infrastructure cybersecurity note to readers on the update*. doi: https://doi.org/10.6028/NIST.CSWP.04162018

OEA (Organización de los Estados Americanos) y BID (Banco Interamericano de Desarrollo). (2016). *Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016*. Recuperado de https://publications.iadb.org/es/publications/english/document/Cybersecurity-Are-We-Ready-in-Latin-America-and-the-Caribbean.pdf

OEA (Organización de los Estados Americanos) y Symantec. (2014). Tendencias de seguridad cibernética en América Latina y el Caribe, 100. Recuperado de https://issuu.com/mirnayonis/docs/oea-symantec_b-cyber-security-trend

Oficina Nacional de Tecnologías de Información, Subsecretaría de Gestión Pública (Argentina). (2005). *Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional*. Recuperado de http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf

Osiatis. (2015). *Gestión de la seguridad*. Recuperado de http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_seguridad/introduccion_objetivos_gestion_de_la_seguridad/introduccion_objetivos_gestion_de_la_seguridad.php

Prislan, K., Lobrikar, B. y Bernik, I. (2017). Information security management practices: expectations and reality. En I. Bernik, B. Markelj y S. Vhorvec (eds.), *Advances in cibersecurity 2017* (pp. 5-22). Máribor: University of Maribor Press. doi: https://doi.org/10.18690/978-961-286-114-8.1

Rosenberg, M., Confessore, N. y Cadwalladr, C. (20 de marzo de 2018). La empresa que explotó millones de datos de usuarios de Facebook-Español. *The New York Times*. Recuperado de https://www.nytimes.com/es/2018/03/20/cambridge-analytica-facebook/

SABSA Institute. (2018). *SABSA Institute. The SABSA Institute*. Recuperado de http://www.sabsa.org/sabsa-institute

SANS. (2018). *CIS critical security controls*. Recuperado de https://www.sans.org/security-resources/posters/20-critical-security-controls/55/download

Sherwood, J., Clark, A. y Lynas, D. (2009). *Enterprise security architecture*. Recuperado de http://www.sabsa.org/whitepapers

Shojaie, B., Federrath, H. y Saberi, I. (2014). *Evaluating the effectiveness of ISO 27001: 2013 based on Annex A*. En *Proceedings. 9th International Conference on Availability, Reliability and Security, ARES 2014*, 259-264. doi: https://doi.org/10.1109/ARES.2014.41

Sonchan, P. y Ramingwong, S. (2014). Top twenty risks in software projects: a content analysis and Delphi study. En *2014 11th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, ECTI-CON 2014*. https://doi.org/10.1109/ECTICon.2014.6839820

Sookhak, M., Gani, A. y Buyya, R. (2016). A survey on vehicular cloud computing. *Journal of Network and Computer Applications*, 75, 200-222. doi: https://doi.org/10.1016/j.jnca.2013.08.004

The Open Group. (2017). *Open Information Security Management Maturity Model (O-ISM3), Version 2.0*. Reading, RU: The Open Group.

Valencia Duque, F. J. (2018). *Aseguramiento y auditoría de tecnologías de información orientados a riesgos. Un enfoque basado en estándares internacionales*. Bogotá: Editorial Universidad Nacional de Colombia.

Valencia Duque, F. J., Marulanda, C. E. y López Trujillo, M. (2015). Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional. *Gerencia Tecnológica Informática*, *15*(41), 65-77.

Valencia Duque, F. J. y Orozco Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas y Tecnologías de Información*, 22, 73-88. doi: http://dx.doi.org/10.17013/risti.22.73-88

Vanegas, A. y Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en mipymes : Mogrit. *Revista s&t*, *12*(30), 35-48.

Vargas, M. A. y Parra, I. C. (2002). Lenguaje para seguridad informática. *Sistemas*, 82, 43-50.

Villanueva, J. (2015). *Mapa de riesgos y otras herramientas prácticas*. Recuperado de http://nahunfrett.blogspot.com/2013/04/mapa-de-riesgos-y-otras-herramientas.html

▶ Índice temático

A

amenazas persistentes avanzadas 17.
arquitectura 21, 22, 52, 57-62, 132, 133, 138.

C

cloud 48, 130, 131, 134, 136-138.
ciberespacio 122, 127
ciberseguridad 29, 118, 121-125, 127, 128, 132.
cloud computing 106, 128-138.
confidencialidad 18, 28, 32-35, 37-38, 40, 47, 58, 74, 77, 81, 88-89, 95, 100-102, 122

D

defensa en profundidad 20.
disponibilidad 18, 28, 32-35, 37, 39, 40, 47, 52, 53, 58, 74, 77, 81, 88, 89, 95, 100-102, 108, 122.

E

economía de los datos 20.
escenario de riesgo 32, 102, 105, 108, 109, 113.

F

firewall/s 30, 128.

H

hacking 63, 128.

I

infraestructura 26-28, 49, 54, 58, 62, 96, 110, 127, 129-131, 134, 135, 139.
información 17-20, 23, 24, 26-30, 32-41, 43-61, 63-74, 77-102, 104-110, 113-115, 117-124, 127, 128, 133-136, 139.
  Activos de 23, 34, 54, 61, 66, 88, 91-93, 95, 100, 105, 122.
  Arquitecturas de 60.
  Gobierno de seguridad de la 33, 44, 48.
  Seguridad de la 17, 18, 28-30, 32-34, 37, 38, 40, 41, 43-60, 63-74, 77-85, 87-93, 97-99, 103, 104, 107, 110, 113-115, 117-123, 127, 128, 133-135.
integridad 18, 28, 32-35, 37, 39, 40, 47, 58, 74, 77, 81, 88, 89, 95, 100-102, 122.

M

malware 53, 126, 128
modelos 20, 24, 25, 30, 61, 93, 98, 129, 130, 136.
  de despliegue 129, 130
  de servicio 39, 49, 52, 61, 132, 134, 136, 137.

P

pirámide informacional 19, 20, 26.
plataforma 38, 131.

S

seguridad 17, 18, 20-24, 28-34, 37, 38, 40, 41, 43-74, 77-85, 87-93, 97-99, 103, 104, 107, 109, 110, 113-128, 130, 132-139.
  en profundidad 20, 21.
  en la nube 27, 121, 128-131, 133, 134, 136, 139.
  extremo a extremo 21, 22.
  multinivel 24.
  informática 29, 30, 48, 122, 135.
sistema de gestión 29, 30, 32, 34, 37, 41, 43, 47-49, 59, 65-67, 69, 73, 74, 77-79, 82, 84, 85, 88-91, 93, 97, 117, 118, 120, 121, 128.

spyware 53, 128.
sistema/s gestor/es de bases de datos 26, 96.

T

tecnología/s de la información (TI) 74, 89, 98, 100, 123, 127.
tecnología/s de la información y las comunicaciones (TIC) 17, 19, 28, 100.

▶ Índice onomástico

B

Bathiely Fernández, David 41

C

Cano, Jeimy 30, 44, 46
Chen, Min 135, 138

J

Joyanes Aguilar, Luis 29, 123, 128, 129

L

Leung, Victor 135, 138

F

Fernández Rivero, Pedro 77, 90

G

Gómez Fernández, Luis 77, 90

M

Martínez Contreras, María del Mar 63
Matalobos, Juan Manuel 99
Mejía Quijano, Rubi 104, 105
Morán Abad, Luis 41

P

Pérez Sánchez, Alejandro 41

T

Trujillo Gaona, Juan 41

Ciencias de Gestión

Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000

Hace parte de la Colección Ciencias de Gestión
Se diseñó y diagramó en la Editorial
Universidad Nacional de Colombia.
en agosto de 2021
Bogotá, D. C., Colombia.

En su composición se utilizaron caracteres
ITC Berkeley Oldstyle Std 11/14 puntos.

Otros títulos de esta colección

- ***Pensamiento ambiental en la era planetaria. Biopoder, bioética y biodiversidad***
  Ana Patricia Noguera de Echeverri, editora

- ***La gestión humana en la estrategia de manufactura. Un estudio empírico en la industria caldense***
  Jorge Andrés Vivares Vergara,
  William Sarache y
  Julia Clemencia Naranjo Valencia

- ***Tensiones entre los discursos pedagógicos y administrativos. Casos de la educaciónbásica y media en Manizales y Santa Marta***
  Germán Albeiro Castaño Duque y
  Jorge Oswaldo Sánchez Buitrago, editores

- ***Voces del pensamiento ambiental. Tensiones críticas entre desarrollo y abya yala***
  Ana Patricia Noguera de Echeverri, editora

- ***Competir y colaborar con conocimiento e innovación***
  Marcelo López Trujillo,
  Carlos Eduardo Marulanda E. y
  Juan Manuel Castaño M.

Ciencias de Gestión

Actualmente la información representa uno de los activos organizacionales más importantes, no solo por ser el insumo fundamental para toma de decisiones, sino por ser uno de los recursos críticos para la operación de las empresas, llegando incluso a convertirse en transformador de negocios. De allí la necesidad de establecer adecuados niveles de protección.

La disciplina que permite proteger la información y la infraestructura tecnológica en la cual se soporta es la seguridad de la información. Esta es integradora de la seguridad informática y la ciberseguridad como estructuras conceptuales que inciden de manera directa en la protección de los artefactos tecnológicos que generan, transforman, almacenan, procesan, recuperan, difunden y transmiten datos e información.

Acorde a lo anterior, el presente texto busca aportar con los conceptos, elementos y componentes requeridos para la implementación de un sistema de gestión de seguridad de la información desde la perspectiva de las principales normas de la familia de estándares ISO/IEC 27000, teniendo en cuenta que por lo general su incorporación en las organizaciones inicia como un proyecto pero termina como un proceso de la organización que debe ser gestionando permanentemente bajo el principio de la inexistencia de la seguridad absoluta.

9 789587 946017

editUNAD