PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS Y COMPUTACIÓN



DISERTACION DE GRADO PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

TEMA:

PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA NORMA ISO 27001 Y CIBERSEGURIDAD

AUTOR

JAIME DAVID MORA BOLAÑOS

DIRECTORA

ING. BEATRIZ CAMPOS

QUITO DM, 2021

CONTENIDO

RESUMEN 7
JUSTIFICACION 8
PLANTEAMIENTO DEL PROBLEMA 10
ALCANCE 12
MARCO TEÓRICO 13
CAPÍTULO I 13
1. Fundamentación Teórica 13
1.1 Sistemas de información 13
1.2 Seguridad de la información 17
1. Dimensiones de la seguridad de la información 17
1.3 Sistemas de gestión de la seguridad de la información 18
1.4 Norma ISO27001 20
1. Estructura de la norma ISO 27001, según (ISO tools excellence, 2019) 20
1.5 Ciberseguridad 22
1.6 Protocolos de ciberseguridad 24
1. Medidas de seguridad básicas 25
1.7 Norma ISO/IEC 27032 26
1. Estructura de la norma ISO/IEC 27032 26
CAPÍTULO II 27
2. Análisis de la norma ISO27001 y Ciberseguridad 27
2.1 Introducción a la norma ISO27001 27
2.2 Utilidad de la norma ISO27001 28
2.3 Terminología y principios de la norma ISO27001 30
2.4 Ciclo PHVA de la norma ISO27001 31
2.5 Cláusulas de la norma ISO27001 según el anexo SL 32
2.5.1. CLÁUSULA 1: Alcance 35
2.5.2. CLÁUSULA 2: Referencias normativas 35
2.5.3. CLÁUSULA 3: Términos y definiciones 35
2.5.4. CLÁUSULA 4: Contexto de la organización 37
2.5.5. CLÁUSULA 5: Liderazgo 39
2.5.6. CLÁUSULA 6: Planificación 41
2.5.7. CLÁUSULA 7: Soporte 43
2.5.8. CLÁUSULA 8: Operación 44
2.5.9. CLÁUSULA 9: Evaluación del desempeño 45
2.5.10. CLÁUSULA 10: Mejora 47

2.6 Implantación de la norma ISO27001 48
2.7 Ciberseguridad según la norma ISO/IEC 27032 51
2.8 Norma ISO/IEC 27032 52
2.9 Terminología de la norma ISO/IEC 27032 53
2.10 Controles de ciberseguridad de la norma ISO/IEC 27032 54
2.11 Modelo de seguridad para la norma ISO/IEC 27032 55
2.12 Contraste comparativo de la norma ISO27001 y ciberseguridad 56
CAPÍTULO III 57
3. Propuesta metodológica 57
3.1 Activos de Información según ISO27001 57
3.1.1. Identificación de activos 58
3.1.1. Valoración de los activos de información 59
3.2 Cláusulas de integración de ISO 27001 y Ciberseguridad 61
3.2.1. CLÁUSULA 1: Contexto/Entendimiento de la organización 61
3.2.2. CLÁUSULA 2: Liderazgo 62
3.2.3. CLÁUSULA 3: Planificación y análisis de riesgos 65
3.2.4. CLÁUSULA 4: Soporte 68
3.2.5. CLÁUSULA 5: Operación y plan de acción 70
3.2.6. CLÁUSULA 6: Evaluación de desempeño 72
3.2.7. CLÁUSULA 7: Marco de corrección y mejora 75
3.2.8. CLÁUSULA 8: Implementación iterativa 76
CAPÍTULO IV 82
4. Análisis de resultados 82
4.1 Ventajas y desventajas 82
4.2 Diagnóstico 85
4.3 Análisis de la propuesta metodológica estipulada 86
CAPÍTULO V 89
5. Conclusiones y recomendaciones 89
5.1 Conclusiones 89
5.2 Recomendaciones 90
CAPÍTULO VI 91
6. Bibliografía 91

ÍNDICE DE TABLAS

Tabla 1: Niveles del contexto de la organización 38

Tabla 2: Terminología de la norma ISO/IEC 27032 53

Tabla 3: Gestión de la evaluación del desempeño, según la propuesta metodológica integrada. 74

ÍNDICE DE ILUSTRACIONES

Ilustración 1: Diagrama de Sistema de Información Organizacional 15

Ilustración 2: Diagrama de Dimensiones de la seguridad de la información 17

Ilustración 3: Diagrama de tipos de riesgos en la información sensible 30

Ilustración 4: Diagrama de Modelo PHVA para la ISO 27001 32

Ilustración 5: Diagrama de cláusula de ISO 27001:2013 34

Ilustración 6: Diagrama del liderazgo en la organización 40

Ilustración 7: Diagrama del Tratamiento de los riesgos 42

Ilustración 8: Diagrama del Soporte de la ISO 27001 43

Ilustración 9: Diagrama de la Implementación de un SGSI correcto 48

Ilustración 10: Diagrama de Sistema de Información Organizacional 54

Ilustración 11: Grafico del modelo de seguridad norma ISO/IEC 27032 55

Ilustración 12: Grafico comparativo de la norma ISO 27001 y ciberseguridad 56

Ilustración 13: Grafico de clasificación de activos de los sistemas de información 59

Ilustración 14: Grafico del flujo del contexto/entendimiento de la organización, según la propuesta metodológica integrada. 62

Ilustración 15: Planificación y análisis de riesgos, según la propuesta metodológica integrada 66

Ilustración 16: Diagrama del Tratamiento de los riesgos 68

Ilustración 17: Diagrama del soporte de la ISO 27001l 69

Ilustración 18: Diagrama de la gestión de los procesos, según la propuesta metodológica integrada 71

Ilustración 19: Diagrama de la Gestión de la evaluación del desempeño, según la propuesta metodológica integrada Elaborado: David Mora 72

Ilustración 20: Diagrama de la implementación de un SGSI correcto, según la propuesta metodológica integrada 77

Ilustración 21: Diagrama de la implementación de un marco de gestión de Ciberseguridad, según la propuesta metodológica integrada 79

Ilustración 22: Diagrama de los objetivos de la implementación de un marco de gestión de Ciberseguridad, según la propuesta metodológica integrada..... 79

Ilustración 23: Cuadro comparativo de ventajas y desventajas, según la propuesta metodológica integrada..... 82

Ilustración 24: Cuadro comparativo, según la propuesta metodológica integrada..... 83

Ilustración 25: Diagrama sobre el diagnóstico de la propuesta metodológica integrada 85

RESUMEN

El presente trabajo de titulación tiene como objetivo proponer una metodología diseñada para la gestión de la seguridad de la información, bajo los lineamientos de la normativa ISO 27001 y ciberseguridad, bajo los marcos normativos de ISO/IEC 27032. Considérese en dicha propuesta metodológica al análisis de las vulnerabilidades existentes en los sistemas de información para, a partir de ellos, gestionar la seguridad de los mismos de manera eficiente y adecuada. Además de la interrelación total e integral entre los marcos considerados por las normativas ISO 27001:2013 e ISO/IEC 27032, focalizados en la Gestión de la Seguridad de la Información y Ciberseguridad, respectivamente. La propuesta metodológica diseñada consigue identificar a las normas, protocolos y procesos inmersos en la seguridad informática en todos los niveles de gestión.

El presente trabajo de titulación, en base al contraste, aplicación y posibilidad de certificación de cada una de las normas señaladas anteriormente, expone de manera sencilla y concreta las ventajas de implantar los protocolos de seguridad implicados para el aseguramiento de la seguridad informática y el aseguramiento de la capacidad de respuesta efectiva ante riesgos de seguridad.

JUSTIFICACION

En la actualidad, la seguridad de la información es un factor crucial en los sistemas de información existentes en todo tipo de organización. Muchas organizaciones no cuentan con las normas y protocolos necesarios para salvaguardar la integridad de la información que tienen en su posesión, por lo que dicha información puede verse afectada o corrupta. En consecuencia, en la perdida y corrupción de información sensible de gran relevancia.

La seguridad informática y la gestión de la misma es fundamental en toda empresa e incluso más actualmente dado a la integración de las Tecnologías de la Información prácticamente en todo campo laboral. La protección de la data es requerida estructuralmente en todo sistema digital, considerando que la seguridad de la información sensible o confidencial puede vulnerarse y, consecuentemente, resultar en actos inmorales que perjudiquen tanto a empresas como a personas naturales a gran escala. Hoy en día, en la época de la información, la protección de los datos es sumamente relevante y lo seguirá siendo a futuro.

La propuesta planteada es completamente viable. El estudio de la seguridad informática se encuentra presente en la actualidad y es accesible en todos sus campos de enfoque. El análisis de riesgos y vulnerabilidades, al igual que las normas que permiten la solución y prevención de dichos factores, con el objetivo de proteger la información, están disponibles en una gran variedad de fuentes fiables y utilizadas actualmente, pudiendo ser artículos, estudios, comunidades, especialistas, etc. Una de ellas es la ISO27001, misma que ofrece una certificación en el campo de la Gestión de la Seguridad de Información. Nótese que, cada día existen infinitas cantidades de ataques informáticos alrededor del mundo ejecutados por profesionales que no mantienen un juicio moral

éticamente correcto, por lo que es indispensable sumarse a la lucha contra protección de la información del lado ético – profesional.

La propuesta contará con elementos originales y novedosos. Se utilizará como base del planteamiento de la propuesta a la norma ISO27001, considerando que la evolución de los sistemas de información es constante y muy veloz, por tal razón, estos requieren de nuevas guías prácticas de aplicación que puedan focalizarse hacia diversos campos actuales y en desarrollo. Es un hecho que cada día se generan nuevas maneras de vulnerar y acceder ilícitamente a sistemas de información, por lo tanto, la constante actualización en el campo de la seguridad de la información es necesaria. De igual manera, la propuesta manejará paralelamente diversas metodologías orientadas a la ciberseguridad.

El tema de disertación responde a un interés personal y profesional, dado que siempre he querido involucrarme en el área de gestión de la seguridad de sistemas de información, al igual que la ciberseguridad. Considero que la protección de la información es crucial en el mundo moderno y es requerida en todo tipo de empresa. Personalmente, mi interés es el de contrarrestar los constantes ataques que sufren las organizaciones, brindando, con esta guía, un servicio de ethical hacking, y de esta manera garantizar la integridad de la información de terceros. Además del interés personal y profesional, el interés es mayor a nivel empresarial para proteger los activos digitales que pueden ser vulnerados ante tantas amenazas que existen en la red y la seguridad de la información, software, datos y sistemas ponen en peligro uno de los activos tecnológicos; y, que, a pesar de existir una ISO, no implementan por desconocimiento, y que justamente la tesis pretende dar una guía práctica para implementarlo.

PLANTEAMIENTO DEL PROBLEMA

La seguridad de la información es un pilar fundamental dentro de toda empresa, misma que permite garantizar el correcto funcionamiento de la misma. En otras palabras, gestionar y valorar la información adecuadamente garantiza la estabilidad de la empresa. Tanto gestionar como proteger a los sistemas de información resulta imprescindible, por lo tanto, un sistema de gestión de la seguridad de la información garantiza la confidencialidad, integración y disponibilidad de los datos (Casafranca, 2018).

Un método para garantizar la seguridad de la información, a partir de su gestión, es brindada a través de ciertas normativas. En este caso, las normativas ISO 27001 están directamente inmersas y comprometidas con el caso de estudio. La gestión de la seguridad de la información, según las ISO 27001, consiste en la preservación de confidencialidad, integridad y disponibilidad, así como los sistemas implicados en su tratamiento, dentro de una organización. Entiéndase que, garantizar un nivel de protección en su totalidad, no es posible, por lo tanto, se busca garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados. La implantación de un sistema de Gestión de la Seguridad de la información, en base a las normas ISO 27001, implica las siguientes tareas:

- Compromiso de la dirección general de la organización.
- Elaboración de un plan de Gestión de Seguridad.
- Asignación de recursos, funciones y responsabilidades.
- Formación y concienciación del personal.
- Establecer controles periódicos y mejoras.

El plan de Gestión de Seguridad consiste en:

- Identificar activos del SGSI y sus propietarios.
- Identificar amenazas de cada activo.
- Identificar vulnerabilidades del sistema.

- Identificar los posibles impactos de las vulnerabilidades.

Actualmente, en la mayoría de empresas no se puede visualizar, transparentemente, la implementación de un sistema de gestión de la seguridad de la información alienado a la norma ISO 27001 y ciberseguridad. Dado esto, es posible identificar el siguiente problema principal:

- No se cuenta con una guía de la gestión de la seguridad de la información que se encuentre alienada a la norma ISO 27001 y ciberseguridad.

Y los siguientes problemas secundarios:

- No existe una guía de gestión de la información que trate a las vulnerabilidades existentes en los sistemas de información.
- Dentro de la gestión de la seguridad de la información, no existe un enfoque total o parcial, a la norma ISO 27001 y ciberseguridad.
- No existe un registro de las normas y protocolos que se ven inmersas en la gestión de la seguridad de la información y de la ciberseguridad.
- No existe una relación directa de la gestión de la seguridad de la información en base a la norma ISO 27001 y los demás protocolos estandarizados.

En función de lo expuesto como problemática se plantean la siguiente pregunta principal:

- ¿Qué guía metodológica de gestión de seguridad de la información permite alienar a la norma ISO 27001 y ciberseguridad?

Y las siguientes preguntas secundarias:

- ¿Qué guía de gestión de la información trata a las vulnerabilidades existentes en los sistemas de información?
- ¿Qué guía de gestión de la seguridad de la información mantiene un enfoque total o parcial, a la norma ISO 27001 y ciberseguridad?
- ¿Qué registro posee normas y protocolos que se ven inmersos en la gestión de la seguridad de la información y la ciberseguridad?
- ¿Qué administración de seguridad de la información se encuentra relacionada con la norma ISO 27001 y los demás protocolos estandarizados?

ALCANCE

El presente trabajo de titulación iniciará con criterios de estudio de tipo exploratorio, dado que no se encontraron propuestas metodológicas que relacionen a la norma ISO27001, focalizada en la gestión de la seguridad de la información, y las metodologías de defensa pertenecientes a la ciberseguridad.

Posteriormente se realizarán estudios descriptivos con los cuales se pretende analizar distintas metodologías, procesos, herramientas y flujos acordes a la gestión de la seguridad de la información, específicamente, en relación a la norma ISO27001 y protocolos de ciberseguridad.

Finalmente, el trabajo de titulación culminará con la entrega de **un documento que contenga una propuesta metodológica para la gestión de la seguridad de la información alineada a la norma ISO27001 y metodologías relacionadas a la ciberseguridad.**

MARCO TEÓRICO

CAPÍTULO I

1. Fundamentación Teórica

1.1 Sistemas de información

Tomando en cuenta un punto de vista general, un sistema de información puede definirse como un conjunto de elementos focalizados a la operación y gestión de los datos e información, de manera que estos puedan utilizarse posteriormente, con el objetivo de solventar una necesidad identificada. Un sistema de información (SI) comprende una serie de elementos fundamentales para operar básicamente, estos son: recurso humano, datos, actividades, procesos, recurso material, etc. Considérese que los elementos componentes de un SI tienen la capacidad de interactuar entre sí, llevando a cabo una serie de procesos estructurados e interrelacionados para conseguir un fin en común, a partir de la información obtenida. La información puede entenderse como un recurso capaz de ser operado, distribuido, clasificado, ordenado, de la manera adecuada en función de los objetivos de una determinada organización. (Cámara Zaragoza, 2012).

A día de hoy, en la época de la información, el alcance de los sistemas de información es prácticamente ilimitado; actualmente, el objetivo de un SI se reduce a analizar, entender e interpretar el proceso de adaptación o integración de las tecnologías de información en las estructuras empresariales, específicamente en procesos relacionados a la gestión de dicha información, es decir, procesos gerenciales, administrativos, investigativos, analíticos que requieran de soporte informativo para la toma de decisiones. Los SI tiene la posibilidad de operar con una gran diversidad de elementos, tal y como son el software, hardware, bases de datos, algoritmos de inteligencia artificial, sistemas especialistas, etc. ¿Qué quiere decir esto? Los sistemas de información están inmersos en todo tipo de proceso informático, en todo tipo de disciplina

o ámbito de aplicación. La manipulación de la información debe ser adecuada para conseguir un fin determinado y objetivo, por lo tanto, los sistemas de información deberán generar información valiosa para el fin de una organización, de igual manera, esta deberá ser transparente, confiable, verificable y puntual. (Mesquita, 2019).

Dentro de las organizaciones empresariales a nivel global, los sistemas de información constituyen uno de los ámbitos de estudio más destacados en la actualidad. A día de hoy, el entorno donde se desarrollan las diferentes compañías es cada vez más hostil. La información es el bien más valioso de una organización, por lo tanto, es comprensible que el aspecto crítico de la evolución y mantenimiento de una empresa gire en torno a procesos informáticos, sin embargo, esto puede entenderse a través de varios factores influyentes que han sometido a las organizaciones en la presente época, tal y como lo es el fenómeno de la globalización, la integración multinacional de empresas, el constante incremento de la competencia en el mercado, considerando tanto bienes como servicios. El desarrollo de la tecnología de la información, la creciente incertidumbre en el entorno global, suponen un conjunto de causantes para que el recurso "información" se haya posicionado como un pilar elemental en la organización empresarial (Trasobares, 2021).

A pesar de que no existe una única definición para los sistemas de información, estos pueden conceptualizarse, según Andreu, Ricart y Valor (1991) como: "conjunto formal de procesos que, operando sobre una colección de datos estructurada de acuerdo a las necesidades de la empresa, recopila, elabora y distribuyen selectivamente la información necesaria para la operación de dicha empresa y para las actividades de dirección y control correspondientes, apoyando, al menos en parte, los procesos de toma de decisiones necesarios para desempeñar funciones de negocio de la empresa de acuerdo con su estrategia" (ANDREU, 1991).

El componente principal de los sistemas de información son los datos, mismos que serán almacenados, procesados y modificados para obtener información coherente, interpretable y consistente. La información generada será distribuida a usuarios del sistema de información, considerando que estos son parte fundamental de un SI; es decir, el recurso humano. Tras haberse distribuido la información, el proceso de retroalimentación deberá ser el siguiente, en el cual se valorará la información proporcionada. El proceso general de los sistemas de información de una organización se describe de la siguiente manera:

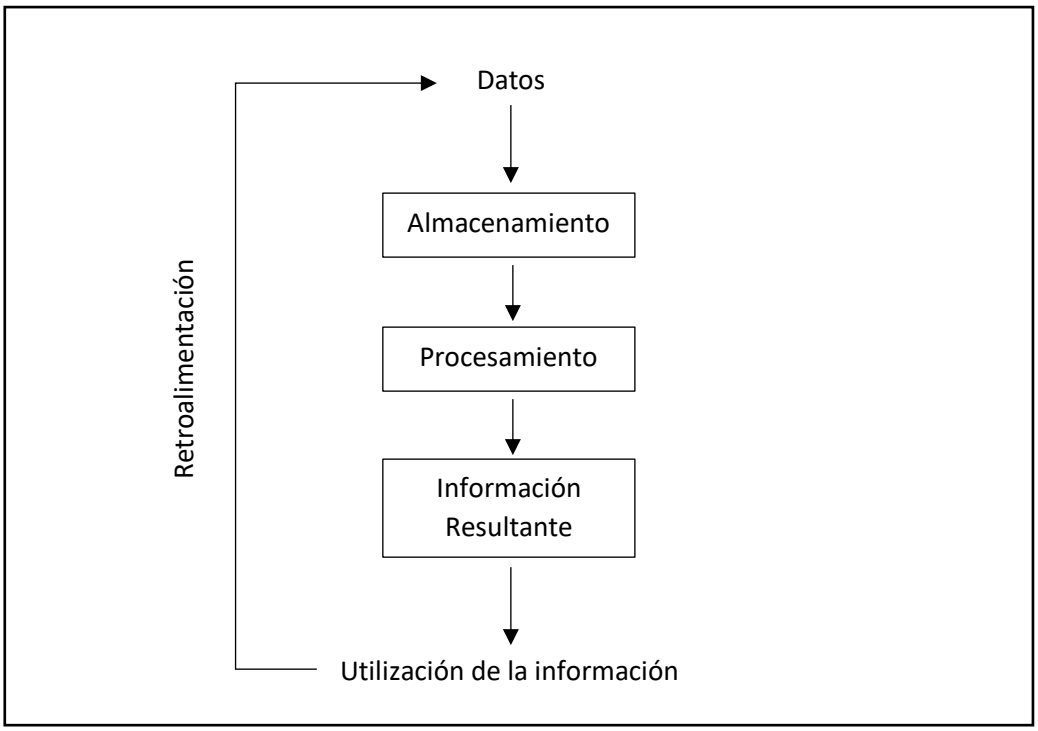


Ilustración 1: Diagrama de Sistema de Información Organizacional

Fuente: Alejandro Hernández Trasobares. Elaborado: David Mora

Es importante considerar que, a pesar de que los datos son la materia prima de un SI, este podrá ser operativo únicamente al constituirse también de los usuarios, es decir, el recurso humano. El personal o los usuarios dentro de un sistema de información serán aquellos agentes que utilicen la información generada como tal. Por último, un SI no

podrá funcionar productivamente sin equipos informáticos de hardware, software y demás tecnologías de la información y comunicación (Trasobares, 2021).

Generalmente, todo SI deberá operar bajo el criterio de ciertos objetivos, mismos que son específicos. A continuación, se mostrarán aquellos más importantes:

- Un SI deberá apoyar y alinearse a los objetivos y estrategias de la organización.
- Un SI deberá proporcionar la información necesaria y relevante para en control de las actividades empresariales en su totalidad.
- Un SI deberá acoplarse, adaptarse siempre a las necesidades de información de la empresa, en todo su proceso de evolución.
- Un SI deberá ser interactivo con los distintos agentes activos de la organización, con el objetivo de que estos empleen el sistema de información según lo que se requiera; siempre buscando satisfacer las necesidades de la empresa, tanto eficiente como efectivamente.

Un correcto sistema de información será capaz de cumplir de manera productiva con los objetivos de este, considerando siempre la meta a la cual se pretende llegar, y los recursos utilizados para que esto sea posible. Un SI será funcional, sin errores, eficiente y eficaz. Los datos de entrada que alimenten al sistema de información deberán ser evaluados, con el objetivo de asegurar la calidad de estos. Finalmente, es posible afirmar que un sistema de información será tan “bueno” como lo sean sus datos.

1.2 Seguridad de la información

Al existir información de gran valor, que, en cierto contexto, se puede validar que el contenido es relevante y necesita ser protegido se habla de seguridad de la información. Hoy en día, a la información de las empresas, gracias a los avances tecnológicos, se la almacena dentro de sistemas de informáticos, lo cual vuelve sencillo su análisis y procesamiento, pero consigo trae problemas que a lo largo del tiempo han ido evolucionando al igual que las soluciones.

Se podría definir a la seguridad de la información como: "conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de un sistema de información" (Arateco, 2015).

1. Dimensiones de la seguridad de la información

La seguridad de la información se aplica sobre los tres pilares de protección de la información:



Ilustración 2: Diagrama de Dimensiones de la seguridad de la información

Fuente: incibe.es Elaborado: David Mora

Disponibilidad

La información debe ser accesible en todo momento, sin existir impedimentos para obtener, analizar o procesar. Los tipos de dificultades de disponibilidad se pueden deber a sistema, configuración o por error humano, pero cualquiera de estas representa vulnerabilidad para la seguridad de la información.

Integridad

Limita a que la información no debe contener errores o modificaciones, además, esta deberá ser acertada. Esto se debe a que las decisiones se basan en la información y si esta tuviera algún error dentro todo lo demás sería incorrecto, por lo que, es vital que la información sea precisa.

Confidencialidad

La información debe estar destinada únicamente al personal autorizado, es decir, la técnica del "*need to know*", como fuerza de prevención ante la difusión no solicitada o robo de la información (Instituto nacional de Ciberseguridad, 2019).

1.3 Sistemas de gestión de la seguridad de la información

La información es un recurso altamente valioso, por lo tanto, con el fin de proporcionar un modelo capaz de construir, implementar, supervisar, revisar, conservar, optimizar y mejorar la protección de los activos de información, se presentan los SGSI, o Sistemas de Gestión de la Seguridad de la Información (SGSI); siempre alineados a los objetivos de negocio. ¿En qué se basa un SGSI? Una vez se conozca claramente el estado de una organización, es decir, el contexto de la misma, los SGSI están basados en la evaluación de riesgos y en el establecimiento de los niveles determinados por parte de la Dirección de la organización, siempre que estos se consideren adecuados. ¿Con qué objetivo? Determinar la aceptación de un nivel de riesgo, de manera que, los riesgos, puedan gestionarse efectiva y eficientemente.

La implementación de un SGSI será exitosa dependiendo del análisis de requerimientos para la protección de los activos de información, y la aplicación de controles específicamente adecuados para garantizar la protección de dichos activos de información (Blog de CEUPE, 2018).

La implementación de un SGSI deberá fundamentarse en los siguientes principios para que esta se considere exitosa:

1. Entendimiento de la organización, contexto y elementos relevantes para los objetivos del SGSI.
2. Entendimiento de necesidades de las partes interesadas.
3. Asignación de responsabilidades para la seguridad de la información, considerando modelos de liderazgo.
4. Formación en seguridad de la información.
5. Concienciación en seguridad de la información.
6. Liderazgo y compromiso de la Dirección organizacional.
7. Evaluación de riesgos para la determinación del estado actual de la organización, estrategias adecuadas de gestión de riesgos para alcanzar determinados niveles de aceptación.
8. Incorporación de la seguridad como elemento esencial de sistemas de información.
9. Prevención y detección de acontecimientos orientados a la vulnerabilidad de la información en marcos de seguridad.
10. Enfoque integral hacia la gestión de seguridad de la información garantizado.
11. Reevaluación continua y periódica de la seguridad de la información.
12. Focalización en la mejora continua.

Los SGSI comprenden tres dimensiones fundamentales: confidencialidad, disponibilidad e integridad, mismos que deberán priorizarse en la implementación de un SGSI.

1.4 Norma ISO27001

La norma ISO 27001 hace referencia a los requisitos para sistemas de gestión de la seguridad de la información, es un estándar internacional y permite el aseguramiento, confidencialidad e integridad de los datos y sus sistemas de gestión (ISO tools excellence, 2019).

Fue publicada el 15 de octubre de 2005, tiene su origen en la "BS 7799-2:2002" la cual quedó anulada, en su primer anexo se muestra cuáles son los controles y objetivos de control para ser aplicados en empresas sean seleccionadas por organizaciones de desarrollo del SGSI (López, 2012).

Una empresa que cuente con un sistema de gestión de seguridad de la información (SGSI) puede obtener una certificación de esta norma mediante la aprobación de una auditoria. Para estructurar el SGSI de acuerdo con la norma hay puntos que pertenecen a una etapa del proceso: Planificar – Hacer – Verificar – Actuar. La certificación es costosa y su tiempo de implementación es largo, por este motivo varias empresas no lo pueden realizar, pero es posible emplear distintos puntos, los más necesarios para la empresa y de esta manera tener un correcto nivel de seguridad. (Villa, Ladino, & López, 2011)

1. Estructura de la norma ISO 27001, según (ISO tools excellence, 2019).
    a) Objetivo y Campo de aplicación: Presenta la orientación y finalidad de la aplicación estándar de la norma.
    b) Referencias normativas: Recomienda la consulta de documentos referentes e indispensables a la aplicación de la norma.
    c) Términos y definiciones: Describe la terminología.

d) Contexto de la organización: Plantea el primer requisito de la norma referente a los conocimientos y contexto de la organización, delimitación del alcance del SGSI.

e) Liderazgo: Destaca la necesidad de que todos los que conforman la empresa se involucren en el proceso de implementación de la norma junto con el compromiso de dirección con liderazgo y compromiso.

f) Planificación: Manifiesta la importancia de la determinación de riesgos y oportunidades para planificar un SGSI y el establecer los objetivos de seguridad de la información.

g) Soporte: Señala que la organización a la cual se aplicara este esquema cuente con; recursos, competencias, información documentada y comunicación para el correcto funcionamiento de un SGSI.

h) Operación: Identifica que es necesario para cumplir con los requisitos de la seguridad de la información contar con planificación, implementación y control de los procesos de la organización. Validar los riesgos y tratamientos de la seguridad de la información.

i) Evaluación del desempeño: Establece la necesidad de tener seguimiento, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección del SGSI

j) Mejora: Muestra las obligaciones de la organización en el caso de tener una inconformidad, para asegurar la mejora continua del SGSI.

1.5 Ciberseguridad

La ciberseguridad es la práctica de proteger computadores, servidores, dispositivos móviles, en sí, sistemas, redes y programas de ataques digitales. Considérese que los ataques digitales, en la mayoría de los casos, están destinados al acceso, modificación o destrucción de la información confidencial de una organización, incluso, es posible objetar a los usuarios con el fin de extorsionarlos e interrumpir la continuidad de un determinado negocio (Cisco, 2021). ¿Por qué es necesaria la *Ciberseguridad*? Al día de hoy, en la época de la información, la necesaria implementación de medidas de seguridad digital es una consecuencia del hecho que señala que, actualmente, existen más dispositivos conectados que personas, y los ataques digitales cada día son cada vez más frecuentes y proporcionalmente inesperados (Kaspersky, 2021).

La ciberseguridad es un término que puede focalizarse en diferentes contextos, según (Kaspersky, 2021):

1. Seguridad de red: Práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista.
2. Seguridad de las aplicaciones: Mantener el software y los dispositivos libres de amenazas.
3. Seguridad de la información: Proteger la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito de los mismos.
4. Seguridad operativa: Procesos y decisiones para gestionar y proteger los recursos de datos, en base a permisos otorgados a los usuarios, procedimientos determinantes del almacenamiento de los datos.

5. Recuperación ante desastres y la continuidad del negocio: Definen la metodología con la cual una organización reacciona ante un incidente de ciberseguridad, incluso eventos catastróficos.
6. Capacitación del usuario final: Considerado como el factor de ciberseguridad fundamental. El factor determinante en la seguridad de la información es el recurso humano. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente, o malintencionadamente un virus en un sistema que de otro modo sería seguro.

Los ataques cibernéticos pueden presentarse de diversas formas, sin embargo, los tipos de amenazas cibernéticas a los que se enfrenta la ciberseguridad, según (Kaspersky, 2021), son:

- Delito cibernético: Agentes individuales o grupos que atacan a los sistemas para obtener beneficios financieros o causar interrupciones en un negocio.
- Ciberataques: Recopilación de información con fines políticos.
- Ciberterrorismo: Debilitar los sistemas electrónicos para causar pánico o temor en las organizaciones.

Puede entenderse el significado de los diferentes tipos de ciberataque, sin embargo, existe un cuestionaste. ¿Cómo puede conseguirse el control de un sistema informático? Estos son algunos de los métodos comunes utilizados para amenazar la ciberseguridad:

- Malware: virus, troyanos, spyware, ransomware, adware, etc.
- Inyección de código SQL: Tipo de ciberataque utilizado para tomar el control y robar datos de una base de datos.

- Phishing: Ataques a víctimas mediante correos electrónicos que simulan ser de una empresa legítima que solicita información confidencial, con el fin inducir a personas a que estas entreguen información confidencial.
- Ataque de tipo "Man-in-the-middle": Procesos por el cual un cibercriminal intercepta la comunicación entre dos individuos para robar datos e información.

Finalmente, existen ciertas recomendaciones que pueden tomarse para protegerse a nivel personal de ataque digitales, sin embargo, es de considerar que la amenaza de dichos ataques es permanente. La actualización continua de software es una recomendación bastante útil al tratarse de la prevención de ataques cibernéticos, considerando software antimalware o el sistema operativo. Valga la redundancia, la utilización de un software o sistema antivirus es fundamental, y podría ser determinante ante un intento de ataque cibernético exitoso. La utilización de contraseñas seguras es una técnica eficiente, dado que evitará que estas sean adivinadas incluso por algoritmos de acceso mediante fuerza bruta. Prestar atención a correos electrónicos sospechosos, vínculos en sitios web poco confiables, podría ser de gran ayuda ante las amenazas digitales, es importante tener en claro que la mayoría de ataques vendrán hacia una organización a través de vulnerabilidades en las personas.

1.6 Protocolos de ciberseguridad

Para mantener un manejo correcto de la información se ha visto como necesidad la creación de protocolos, existen diversas fuentes que proporcionan esta documentación de manera general, aunque no se pueden distinguir protocolos universales aplicables como norma sino más como consejos de prevención.

Es así que se sugiere para establecer estos protocolos se tome en cuenta lo siguiente:

a) Identificación de la información y los riesgos a los que estará expuesta.
b) Protección de la información por medio de protocolos de seguridad.
c) Detección de herramientas necesarias para una correcta infraestructura de seguridad.
d) Respuesta de la información por medio de protocolos de respuesta y mitigación.
e) Recuperación de la información que ha sufrido algún tipo de vulnerabilidad. (Ciar Global, 2020)

1. Medidas de seguridad básicas

Se enumeran siete medidas para reducir la probabilidad de que una empresa sea víctima de ataques cibernéticos, según (Gonzales, 2017).

a) Evitar la transmisión de datos personales hacia remitentes no confiables. Mantener un alto grado de confidencialidad.
b) Mantener en disposición a cuentas de correo electrónico focalizadas, es decir, tanto personales como laborales.
c) Rechazar correos de tipo *spam* y evitar ficheros desconocidos. Al igual que, debe evitarse al máximo acceder a vínculos en correos no confiables.
d) Evitar la divulgación del correo electrónico personal, al igual que datos personales.
e) Mantener todo tipo de contraseñas ocultas y seguras, de manera que no sean expuestas ni sean de fácil alcance. De igual manera, estás deberán actualizarse y alternarse periódicamente, haciendo uso de caracteres alfanuméricos, mayúsculas y simbología permitida por el entorno.

f) Evitar navegar en sitios web poco confiables, y así mismo evitar vínculos no deseados en sitios web peligrosos.

1.7 Norma ISO/IEC 27032

La norma ISO/IEC 27032 hace referencia a la ciber-seguridad, un estándar que garantiza las directrices de seguridad que asegura "proporcionará una colaboración general entre las múltiples partes interesadas para reducir riesgos en Internet" (ISO tools excellence, 2019).

Es la protección de la privacidad, integridad y accesibilidad de la información por medio del ciberespacio, se enfoca en enfatizar los roles en el ciberespacio según la información (Garcia, 2016).

1. Estructura de la norma ISO/IEC 27032

a) Alcance y campo de aplicación.

b) Aplicabilidad.

c) Referentes normativos.

d) Términos y definiciones.

e) Términos abreviados.

f) Visión general.

g) Partes interesadas en el Ciberespacio.

h) Activos en el Ciberespacio.

i) Amenazas contra la seguridad del ciberespacio.

j) Roles de las partes interesadas en la Ciberseguridad.

k) Directrices para los interesados.

l) Controles de Ciberseguridad.

m) Marco del intercambio de información y la coordinación.

CAPÍTULO II

2. Análisis de la norma ISO27001 y Ciberseguridad

2.1 Introducción a la norma ISO27001

La norma ISO 27001 fue desarrollada por la Organización Internacional de Normalización, con el objetivo de gestionar favorablemente la seguridad de la información en organizaciones y empresas. Su primera versión (ISO/IEC 27001 - 2005) se publicó en el año 2005, sin embargo, la norma de estandarización utilizada en la actualidad es la publicada en el 2013 (ISO27001, 2013).

Según la los protocolos estandarizados ISO, toda norma derivada deberá evaluarse integralmente cada cinco años, formalizando revisiones iterativas, con el objetivo de identificar los aspectos que poseen la necesidad de actualizarse. En lo que respecta a la norma ISO 27001, como se menciona anteriormente, su actualización más reciente se produjo en el 2013, considerando un cambio significativo a nivel estructural, específicamente basado en el "Anexo SL". Todo negocio, organización o empresa tiene acceso y dispone de información realmente sensible, misma que deberá ser gestionada correctamente en los diferentes procesos llevados a cabo según el giro del negocio. Es de considerar que, la inadecuada protección de la información implica consecuencias graves, tanto legales como operativas, financieras, estructurales, etc. Incluso podría llevar a la empresa a su cierre definitivo (Julian Russell, 2021).

A nivel empresarial, una de las mayores dificultades que puede presentar una organización se centra en la protección adecuada de la información. El reto consiste en asegurar, garantizar y verificar que se han identificado correctamente los riesgos a los que una determinada organización está expuesta, de manera que se consiga una respuesta de cómo gestionarlos de manera sólida, efectiva, eficiente, sostenible y proporcionada. La norma global, por defecto, destinada a la gestión de sistemas de gestión de la seguridad

de la información es proporcionada a través de la ISO 27001, misma que proporciona un marco robusto para proteger la información. ISO 27001 es viable para adaptarse a organizaciones de todo tipo, independientemente de su focalización, área de negocio o tamaño. En su mayoría, las corporaciones que mantienen un mayor margen de probabilidad a ser vulneradas por los riesgos existentes, están muy ligadas a la protección de los datos, y optan por implementar sistemas de gestión de la seguridad de la información estructurados en base a la norma ISO 27001 (Julian Russell, 2021).

2.2 Utilidad de la norma ISO27001

La ISO 27001 y la seguridad de la información como tal, están ganando más protagonismo cada vez, y aún mas hoy en día, dado que un gran margen organizacional reconoce la existencia de los riegos y agentes de vulnerabilidad, y, además son explotadas con mucha frecuencia. Hoy en día es casi certero afirmar que toda empresa, tarde o temprano, se verá afectada en lo que respecta a la seguridad de la información que esta gestione. Para la mayoría de las organizaciones debe ser fundamental implementar un SGSI y debería considerarse una prioridad lograr la certificación ISO 27001. ¿Por qué? Para aquellas empresas que mantienen la responsabilidad de gestionar información de alto valor y sensibilidad, la utilidad de la ISO 27001 puede dividirse en tres áreas generales, según (Julian Russell, 2021).

- **Comercial:** Proporcionar una ventaja competitiva a la organización y, a su vez, permitirle mantenerse a la par con sus competidores es consecuencia de la implementación de un SGSI. A día de hoy, las entidades expuestas a ser vulneradas en la seguridad de la información hacen de la certificación ISO 27001 un requisito imprescindible. Por lo tanto, al estar certificado en ISO 27001, se conseguirá colaborar únicamente con proveedores que mantengan de manera integral, los protocolos requeridos para la seguridad informática, manteniendo un

compromiso reflejado en la capacidad del cumplimiento contractual de los requerimientos y cláusulas establecidas. Para una organización, contar con un SGSI alineado a la normativa ISO 27001, es fundamental mantener e incrementar su retribución comercial y mercantil.

- **Operaciones:** Dentro de una empresa, siempre se deberá fomentar al desarrollo interno cultural que estará alerta ante todo riesgo de la vulnerabilidad de información; también que posea una perspectiva congruente para enfrentar dichos riesgos. ¿Cómo conseguir este ambiente? La ISO 27001 proporciona este enfoque en su totalidad, de manera que oriente una inspección más vigorosa y coherente en la administración de posibles amenazas. En consecuencia, el valor implícito en la implementación y mantenimiento de los mismos es altamente minimizado, además, considerando el peor de los casos, tratándose de un fallo, sus consecuencias también se verán reducidas significativamente, así, estás se mitigarán efectiva y eficientemente.
- **Tranquilidad:** La tranquilidad en una empresa es un factor necesario para que, desde la gerencia, pueda gestionarse óptimamente. Un SGSI adecuado según la ISO 27001 presenta un modelo sólido que permitirá a dicha gerencia administrar todo tipo de riesgos de la mejor manera, considerando así que no estarán expuestos a interrupciones del negocio, incluso, un SGSI correctamente implementado evitará totalmente un impacto negativamente significativo en la reputación del negocio. Las organizaciones, en su mayoría, mantienen una dependencia permanente hacia la seguridad de la información, tomando en cuenta que la economía empresarial está fundamentada en el conocimiento. A nivel mundial, ISO 27001 plantea un esquema fiable para mejorar la praxis de un SGSI en cuestión. Además, es una garantía para mejorar la imagen de una organización y generar confianza en sus clientes; consecuentemente el modelo empresarial, a

nivel competitivo en el mercado se posicionará con gran solidez (Julian Russell, 2021).

2.3 Terminología y principios de la norma ISO27001

Toda organización posee información sensible o de valor, y el objetivo de esta es proporcionarse protección, en este caso, a partir de un SGSI centralizado. La información a proteger puede segmentarse de la siguiente manera:

- Información sensible: Información sobre los empleados, clientes y proveedores.
- Información de valor: Propiedad intelectual, datos financieros, registros legales datos comerciales y datos operativos.

Los tipos de riesgos que la información sensible y de valor sufren se pueden englobar en tres diferentes categorías:



Ilustración 3: Diagrama de tipos de riesgos en la información sensible

Fuente: nqa. > ISO 27001:2013. Elaborado: David Mora

2.4 Ciclo PHVA de la norma ISO27001

La norma ISO 27001 está fundamenta en el ciclo PHVA, es decir, se basa en el ciclo de Deming, mismo que puede aplicarse a cada elemento individual del sistema de gestión para, así, proporcionar un enfoque en el proceso de mejora continua, incluso en la generalidad y globalidad del sistema (Julian Russell, 2021).

¿Qué significa PHVA? Considerando al ciclo de Deming, las siglas pueden desglosarse y detallarse de la siguiente manera, según (Julian Russell, 2021):

- Planificar: Establecimiento de propósitos, requerimientos, procesos, requisitos del usuario, legalidad organizacional, identificación de oportunidades y detección de riesgos.
- Elaborar: Implantación de la planificación.
- Verificar: Control y medición de la productividad de procesos para el establecimiento de objetivos, actividades y requerimientos, además, notificación de resultados e informes.
- Ejecutar: Intervenir con acciones conjuntas capaces de aumentar la productividad del ciclo de mejora continua, en base a lo que se determine como necesario (Julian Russell, 2021).

El modelo PHVA para ISO 27001 puede interpretarse como un sistema cerrado en círculo, a manera de un circuito. ¿Por qué? El sistema circular plantea un modelo de aprendizaje, donde todo aquello adquirido en las etapas de elaboración y verificación es utilizado en etapas de planificación y ejecución de forma segura y garantizada, por tal motivo es adecuado considerar a este sistema como un proceso cíclico (Julian Russell, 2021).

El modelo PHVA se presenta gráficamente expuesto de la siguiente manera:

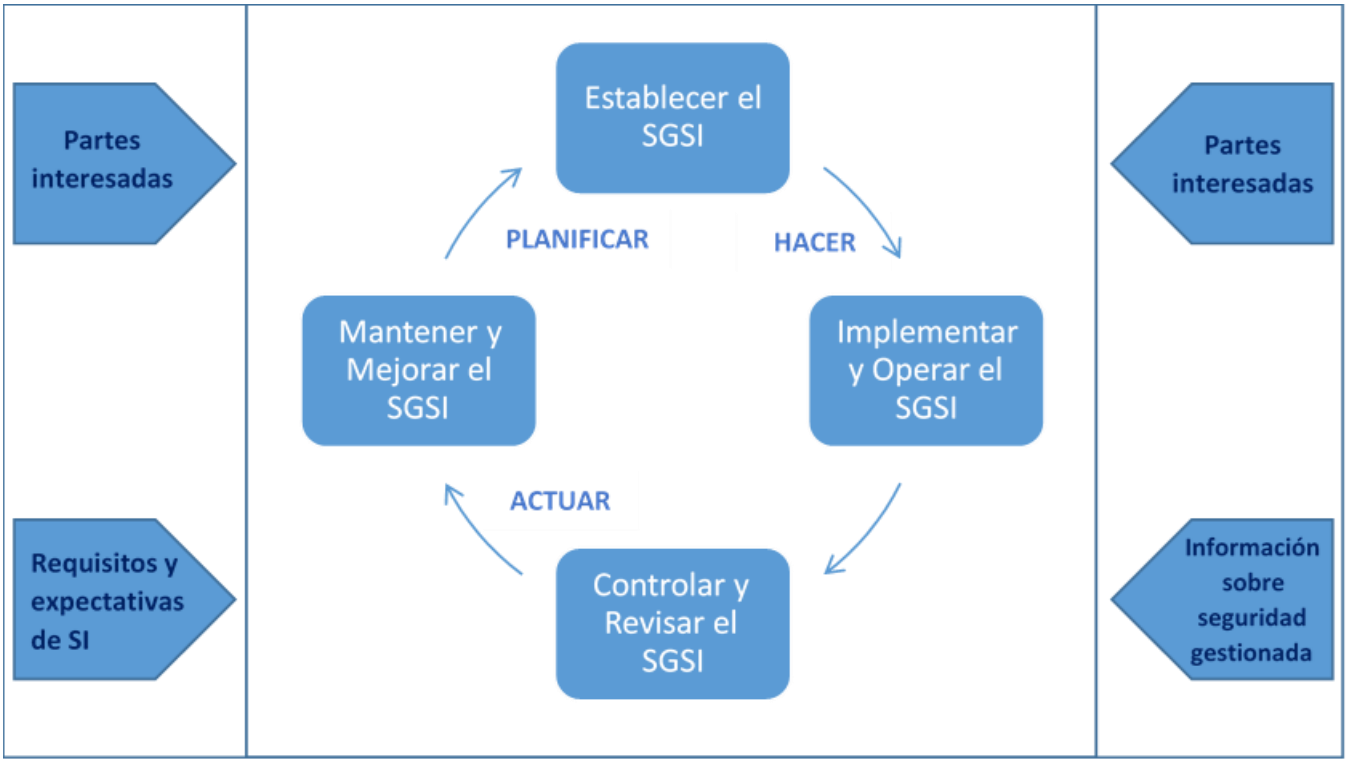


Ilustración 4: Diagrama de Modelo PHVA para la ISO 27001

Fuente: nqa. > ISO 27001:2013. Elaborado: David Mora

2.5 Cláusulas de la norma ISO27001 según el anexo SL

La estructura del Anexo SL fue el mayor cambio introducido en la revisión de la norma ISO 27001 en el año 2013. La guía 83 ISO, siendo el nombre con el que antes se conocía al Anexo SL, es aquel empleado por desarrolladores de las normativas ISO con el objetivo de proponer una estructura global o común para las normas focalizadas en los sistemas de gestión. El Anexo SL facilita la implementación y gestión de múltiples normas. Medioambiente, calidad, seguridad y salud laboral y seguridad de la información se encuentran entre las normas más comunes (Julian Russell, 2021).

Dentro de ISO 27001, el Anexo SL mantiene una estructura de alto nivel descrito en 10 términos o cláusulas:

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación de desempeño
10. Mejora (Julian Russell, 2021)

Por lo general, todo sistema de gestión integrado en una empresa requiere de las contemplaciones contextuales de dicha entidad, es decir, la agrupación de objetivos de alta relevancia organizacional estructurados según la dirección estratégica de dicha entidad, además, la definición documentada del reglamento estipulado para el soporte del SGSI y su finalidad. Finalmente, las auditorías internas son indispensables, para que, posteriormente, sean consideradas por la dirección organizacional; Es de considerar que, cuando se presentan diversas modalidades de gestión en la organización, varios de los componentes mencionados tienden a fusionarse y así conseguir abordar una o más normas (Julian Russell, 2021). Específicamente la norma ISO 27001:2013 está conformada por 10 sectores también conocidos como cláusulas. Es importante señalar que, los requisitos de la ISO 27001 especificados en las cláusulas 4 - 10 deben cumplirse obligatoriamente, por lo tanto, las entidades, como mínimo, deberán ser capaces de satisfacer las cláusulas 4 - 10, y estas no podrán descartarse o pasarse por alto (López, 2012).

Diagrama de cláusulas de ISO 27001:2013

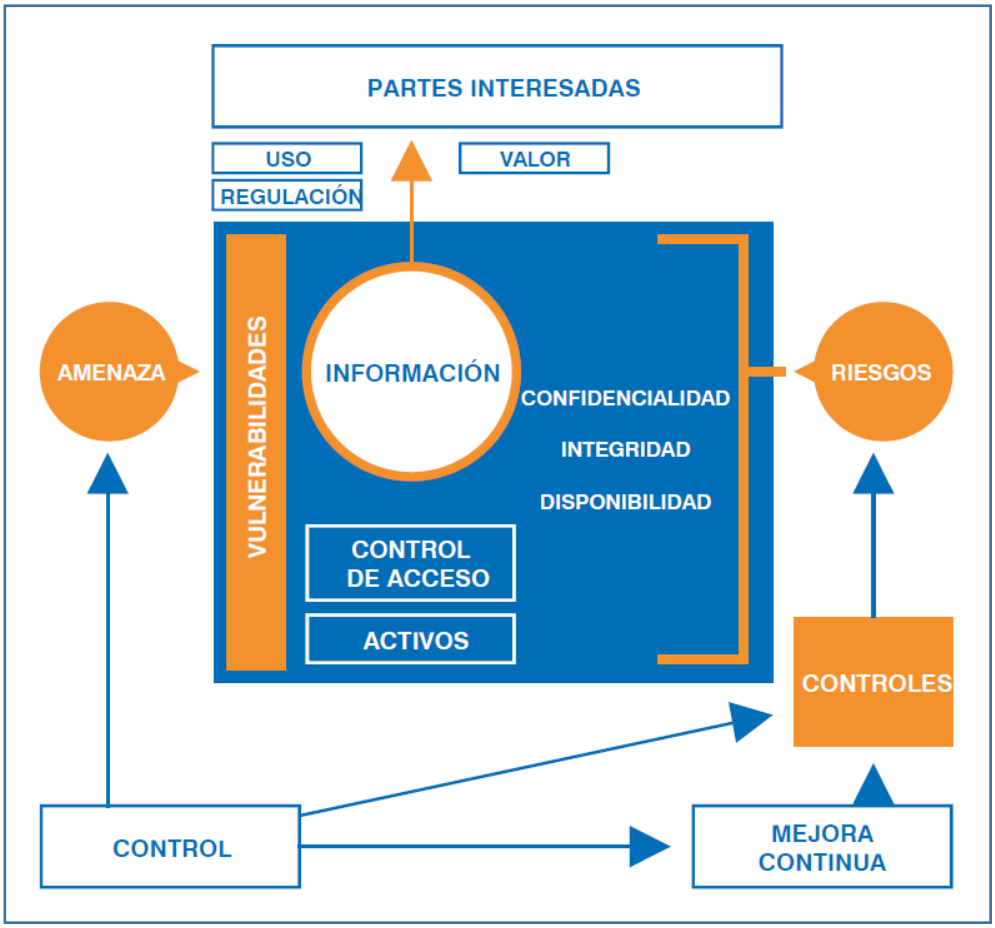


Ilustración 5: Diagrama de cláusula de ISO 27001:2013

Fuente: nqa. > ISO 27001:2013.

2.5.1. CLÁUSULA 1: Alcance

El apartado del alcance de ISO 27001:2013, según (Julian Russell, 2021) establece lo siguiente:

- El propósito de la norma.
- Los tipos de organizaciones para las que se ha diseñado.
- Las cláusulas y los requisitos que una organización debe cumplir para que la organización sea considerada como conforme con la norma.

El diseño de la ISO 27001 se destinó para ser aplicable a cualquier tipo de organización. Independientemente de la complejidad, el tamaño, el giro del negocio, el sector industrial, el propósito o la madurez. Siempre, toda organización puede implementar y mantener un SGSI alineado con la ISO 27001. (p. 11)

2.5.2. CLÁUSULA 2: Referencias normativas

La sección de referencias normativas de la ISO 27001:2013, según (Julian Russell, 2021), considera normas extra que contienen información fundamental para la determinación del cumplimiento de una organización con la norma.

- En la ISO 27001, algunos de los términos utilizados o requisitos detallados son detallados en la ISO 27000. Por lo tanto, la ISO 27000 resulta de gran utilidad para el entendimiento de los requisitos y su conclusión.

Como recomendación, por lo general los auditores externos de la organización esperan que se haya considerado la información de la ISO 27000 en el desarrollo e implantación de su SGSI alineado a la ISO 27001. (p. 12)

2.5.3. CLÁUSULA 3: Términos y definiciones

La sección de términos y definiciones de la ISO 27001:2013, según (Julian Russell, 2021) establece que, a pesar de no existir literalmente términos y definiciones en la normativa ISO 27001, hace mención a versiones actualizadas de ISO 27000. La versión más reciente de la ISO 27000 contiene 81 componentes de terminología y definición

utilizados en la ISO 27001. Aun así, a continuación, se detallan algunos de los términos más utilizados:

- Control de acceso: Conjunto de procedimientos destinados a garantizar que, únicamente, aquellos usuarios que requieran de acceso a activos específicos dispongan del acceso mencionado y, se determinará la necesidad en base a los requisitos del negocio y de la seguridad de la información.
- Efectividad: Método de medida en que las actividades planificadas son ejecutadas de manera premeditada o particular, y, además, se consiga obtener los resultados supuestos en el tiempo esperado.
- Riesgo: La posibilidad de que un determinado evento asociado con la vulneración de la seguridad de la información ocurra, al igual que las posibles consecuencias resultantes.
- Evaluación del riesgo: Fase de identificación de los riesgos existentes, en base al análisis del nivel de riesgo, considerando en particular acciones adicionales necesarias para la reducción de los mismos a niveles de tolerancia aceptables.
- Tratamiento del riesgo: Acción de tratamiento y reducción del riesgo identificado hasta un nivel de tolerancia aceptable.
- Gerencia: Entidad conformada por un grupo de personas encargadas de tomar las decisiones dentro de una empresa. En las organizaciones, son responsables de establecer la dirección estratégica, determinar y conseguir los objetivos determinados por los accionistas o partes involucradas en los niveles más altos.

Los términos expuestos no deben ser forzosamente utilizados de manera exacta o textual al momento de documentar un SGSI, sin embargo, definir los términos utilizados puede esclarecer su significado e intención. Además, es recomendable proporcionar un glosario terminológico en la documentación del sistema. (p. 13)

2.5.4. CLÁUSULA 4: Contexto de la organización

La sección del contexto de la organización de la ISO 27001:2013 establece que la forma y las áreas específicas de prioridad dependerán del contexto en el que opere la organización, considerando que, la finalidad de un SGSI es proteger los activos de información de una organización, de manera que la misma consiga sus objetivos. Los niveles de prioridad planteados pueden segmentarse en cuatro grupos:

- Interno: Engloba aquellos aspectos sobre los cuales la organización tiene control.
- Externo: Engloba aquellos aspectos sobre los cuales la organización no tiene un control directo.
- Partes interesadas.
- Alcance de la gestión del sistema.

Es fundamental analizar tan cuidadosa y detalladamente como sea posible el entorno en el que opera la organización. ¿Por qué? Únicamente de esta manera será posible identificar correctamente a todos los riesgos inherentes a la seguridad de la información. El análisis de la organización en sus niveles interno y externo representa la base que permitirá evaluar a todos los procesos que requieren de modificaciones en busca de mejoras o fortalezas, así, en consecuencia, se conseguirá construir un SGSI eficiente y efectivo. Las áreas pueden considerarse al evaluar y analizar el contexto interno y externo de la organización son nombrados a continuación:

Interno	Externo
• Madurez	• Competencia
• Cultura organizativa	• Organismos reguladores
• Gestión	• Sistema Económico
• Recursos	• Sistema Político
• Madurez de recursos	• Sistema Social
• Sensibilidad	• Accionistas
• Consistencia	• Frecuencia de ataques a la información
• Sistemas	• Estándares de la industria
• Complejidad del Sistema	• Consideraciones ambientales
• Espacio Físico	• Factores políticos y legales

Tabla 1: Niveles del contexto de la organización
Fuente: nqa. > Cláusulas ISO 27001:2013 Elaboración: David Mora

Las **partes interesadas** pueden entenderse como cualquier individuo o grupo de individuos que puedan ser considerados como afectados por la organización al llevarse a cabo una acción o la omisión de la misma. Las partes interesadas, por lo general incluirán a los propietarios, reguladores, accionistas, empleados, competidores, clientes e incluso a los usuarios generales; las partes interesadas son indispensables en el proceso de análisis de los problemas internos y externos de la organización, además, ayudarán a determinar e identificar a los requerimientos que serán totalmente necesarios para el SGSI (Julian Russell, 2021).

Finalmente, tratándose del **alcance del sistema de gestión** como último nivel de prioridad, debe señalarse que, para alinearse a ISO 27001 es necesario documentar detalladamente el alcance del SGSI, sin embargo, ¿qué comprende el alcance? ¿qué es lo que puede describirse? En la gran parte de casos, este podría describir los límites del sitio físico de la organización, límites de las redes físicas, grupos de empleados internos y externos, procesos, actividades, servicios e interfaces en los límites del alcance.

2.5.5. CLÁUSULA 5: Liderazgo

La sección del liderazgo de la ISO 27001:2013, según (Julian Russell, 2021) conlleva la participación activa en la dirección general del SGSI, además de fomentar su implementación y así garantizar apropiadamente la disponibilidad de los recursos. El liderazgo en la organización, alineado a la ISO 27001 incluye las siguientes cláusulas:

- La claridad de los objetivos del SGSI deberá asegurarse y, a su vez, se alinearán con la estrategia general de la organización.
- Garantizar la claridad sobre las responsabilidades.
- Fundamentar todo proceso de toma de decisiones en el pensamiento basado en el riesgo.
- Clarificar la comunicación en lo que respecta a información y todos los individuos que componen el alcance del SGSI (p. 16).

Según la normativa ISO 27001:2013, es sumamente importante considerar la participación activa gerencial en el SGSI, considerando a esta como crucial al momento de garantizar la implementación y mantenimiento efectivo del SGSI. Según (Julian Russell, 2021), ISO 27001, el liderazgo dentro de toda organización puede gestionarse e interpretarse desde tres enfoques y aspectos clave:



Ilustración 6: Diagrama del liderazgo en la organización

Fuente: nqa. > Cláusulas ISO 27001:2013 Elaboración: David Mora

2.5.6. CLÁUSULA 6: Planificación

La sección de la planificación de la ISO 27001:2013, según (Julian Russell, 2021) señala que la norma es una herramienta destinada para la gestión del riesgo. La herramienta conduce a una organización a la identificación de los riesgos de seguridad de información. Considerando lo mencionado, la finalidad profunda de un SGSI es:

- De manera estratégica, identificar aquellos riesgos de alta importancia, evidentes e ignorados.
- Asegurar el diseño, dirección y capacidad de actividades y procesos operativos para la gestión inherente de riesgos.
- Dar respuesta automática a la posibilidad del cambio en la organización, además de mantener la capacidad de confrontar nuevos riesgos, con la finalidad de reducir la exposición continua a los mismos. (p. 18).

Todo SGSI eficaz mantiene su núcleo focalizado en la **evaluación de riesgos**; tómese en cuenta que absolutamente todo tipo de organización tiene la posibilidad de sufrir un incidente de seguridad de la información. En consecuencia, la evaluación de riesgos es imprescindible para aumentar la probabilidad de identificar riesgos potenciales haciendo uso de técnicas de evaluación sistemática. La evaluación de riesgos propone designar recursos para cubrir las áreas de más alta prioridad y, en base a esto, llevar a cabo el proceso estratégico de toma de decisiones sobre la manera de gestionar los riesgos de seguridad de información, siempre con el fin de cumplir los objetivos de la organización (Julian Russell, 2021). Cualquier técnica utilizada para la evaluación de riesgos que sea desarrollada debe incluir ciertos elementos básicos según (Julian Russell, 2021), tal y como se muestra a continuación:

1. Avisos para la identificación sistemática de riesgos; registrar y validar la presencia de amenazas, vulnerabilidades y controles de implementación.
2. Marco de evaluación probabilístico de la ocurrencia de riesgos persistentes.

3. Marco de evaluación de las consecuencias de la aparición de un riesgo consistente.
4. Marco de clasificación de riesgos identificados, considerando su evaluación de probabilidad y respectivas consecuencias.
5. Criterios específicos de documentación del tipo de acción a tomar y el nivel o prioridad asignado.

La gestión del tratamiento de los riesgos se desarrolla en base a la identificación de cada uno de ellos y en el criterio de aplicación para definir si el riesgo será aceptado, o el proceso del mismo. En el caso que se determine el tratamiento de riesgos, este deberá considerar las opciones expuestas a continuación (p. 18).



Ilustración 7: Diagrama del Tratamiento de los riesgos

Fuente: nqa. > Cláusulas ISO 27001:2013 Elaboración: David Mora

2.5.7. CLÁUSULA 7: Soporte

La sección de soporte de la ISO 27001:2013, según (Julian Russell, 2021) hace referencia específicamente a los recursos, considerando al personal, infraestructura, materiales, recursos físicos, recursos digitales, medioambiente, herramientas, entre otros. Para la implementación eficiente de un SGSI, es necesario disponer del apoyo de recursos, dichos recursos a disposición serán capaces, competentes y disponibles en la revisión por la dirección. En lo que respecta al soporte de un SGSI, deben considerarse cuatro aspectos críticos para una implementación y mantenimiento correctos (Julian Russell, 2021).

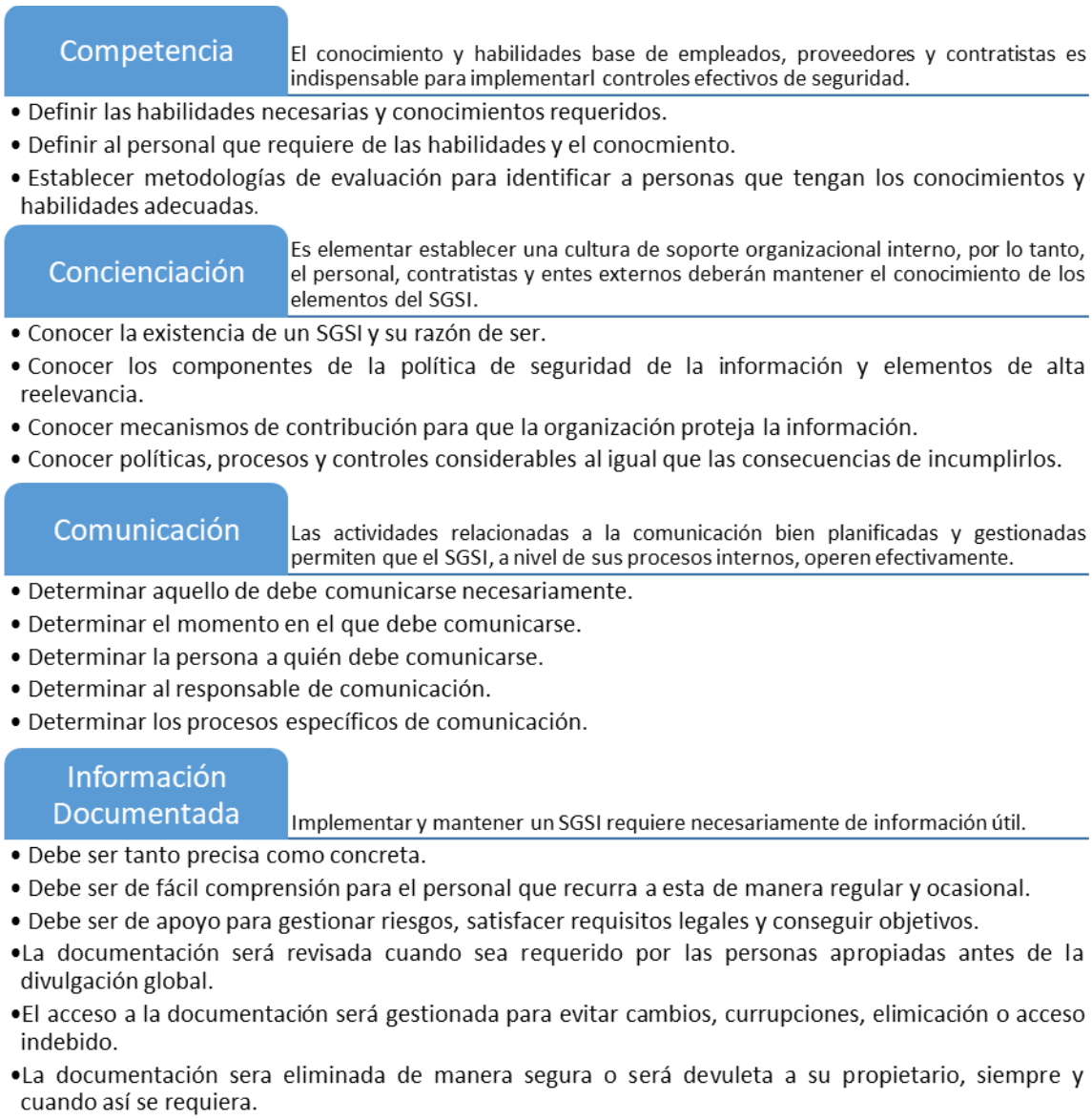


Ilustración 8: Diagrama del Soporte de la ISO 27001

Fuente: nqa. > Cláusulas ISO 27001:2013 Elaboración: David Mora

2.5.8. CLÁUSULA 8: Operación

La sección de operación de la ISO 27001:2013 hace referencia a la adecuada gestión y control del proceso de creación y entrega de un producto/servicio, según (Julian Russell, 2021).

La formalización de actividades en un conjunto de procesos claros y coherentes es necesario para administrar los riesgos de seguridad de la información y alcanzar los objetivos organizacionales. Las prácticas que se detallan a continuación son cruciales para implementar procesos efectivos, en base a lo mencionado por (Julian Russell, 2021).

1. La construcción de procesos deberá realizarse a través de la adaptación de las actividades de negocio.
2. Identificación de riesgos de seguridad de la información a nivel sistemático, siempre que estos sean relevantes para los procesos.
3. Definición, determinación y comunicación de requerimientos/actividades destinadas a gestión de riesgos al momento de generarse un evento.
4. Asignación de roles y responsabilidades para desarrollar actividades asociadas con claridad.
5. Garantía de poder completar actividades/requerimientos siempre que sea necesario a través de la asignación de recursos.
6. Evaluación consistente y seguimiento rutinario de los procesos en la gestión de riesgos de seguridad de la información, considerando su efectividad.

En la cláusula de operación de la ISO 27001, la evaluación del riesgo de la seguridad de la información y el tratamiento de riesgos de seguridad de la información debe gestionarse rigurosamente bajo los lineamientos expuestos en las cláusulas anteriores (p. 22).

2.5.9. CLÁUSULA 9: Evaluación del desempeño

Según la sección de evaluación del desempeño de la ISO 27001:2013 existen tres formas para evaluar el rendimiento del SGSI, según (Julian Russell, 2021).

- Seguimiento de la efectividad de los controles de SGSI.
- Auditorías internas.
- Durante la revisión por parte de la dirección

El seguimiento, medición, análisis y evaluación del SGSI en la organización se requerirá para controlar y asegurar que, tanto el SGSI como los controles de seguridad de la información se mantengan en operación según lo previsto (p. 24). Considerando el volumen de datos y la información en cuestión, para tomar decisiones efectivas, podrían considerarse algunas cuestionantes importantes para tener un punto de partida sólido, como lo menciona (Julian Russell, 2021).

- ¿Qué procesos/actividades se mantienen sujetos a amenazas más significativas y frecuentes?
- ¿Qué procesos/actividades están sujetos a las vulnerabilidades más relevantes?
- ¿Qué es lo más óptimo para generar información significativa y oportuna, además de controlar dicha generación?

Los procesos de control a implementar deberán definirse claramente para mantener su efectividad:

- Cómo/cuando se lleva a cabo el control.
- Quién es el sujeto responsable de llevar a cabo el control.
- Cómo/cuando y a quién se informan las soluciones y posteriores acciones.
- En caso de que los resultados de control indiquen un desempeño no aceptado, ¿cuál es el procedimiento para confrontar la situación?

Para poder alcanzar el aseguramiento de los procesos de análisis y estudio adecuados, es necesario documentar y registrar los resultados obtenidos, además de proceder con revisiones, evaluaciones y estudios pertinentes (Julian Russell, 2021).

A nivel organizacional, el proceso de auditar internamente, tiene como propósito/objetivo, evaluar las deficiencias en los diferentes procesos del SGSI, también, en base a dicha evaluación, identificar oportunidades o áreas de mejora. Las auditorías se comprometen a validar la consciencia del seguimiento de procedimientos, controles y procesos, también deben asegurar el éxito de dichos procedimientos, controles y procesos. Las auditorías internas serán capaces de comprobar lo mencionado siempre y cuando sean llevadas a cabo en base a los lineamientos de la ISO 27001 y los requisitos de las partes interesadas (Julian Russell, 2021).

¿Cómo asegurar que las auditorías son desarrolladas al más alto nivel? Para asegurar este factor, las auditorías se llevarán a cabo por personal respetado, competente, que entiendan los requerimientos de la normativa en su totalidad y tengan la capacidad de interpretar rápidamente la documentación en cuestión. Por lo general, tratándose de periodos de no más de 3 años, las auditorías deben considerar las evidencias de bajo rendimiento, la gestión de riesgos de la seguridad de la información y los procesos auditados más frecuentes. Toda acción realizada en un proceso de auditoría deberá ser registrada, revisada y validada por el personal apropiado, solo así se podrá contar con una respuesta rápida para acciones de implementación antes la aparición de algún problema significativo (Julian Russell, 2021).

La revisión por la dirección siempre será considerada prioritariamente, dado que, en este punto la gerencia evaluará la efectividad del SGSI y asegura que el sistema se encuentre alienado con la dirección estratégica de la organización.

2.5.10. CLÁUSULA 10: Mejora

Según la sección de mejora de la ISO 27001:2013, la finalidad de la implementación de un SGSI se centra en la reducción de la probabilidad de que ocurran eventos de seguridad de la información, y también de su posible impacto. Es de considerar que ningún SGSI es perfecto, sin embargo, los sistemas de gestión se diseñan con el objetivo de mejorarse con el tiempo, así aumentando la resistencia, solidez y robustez frente a los ataques de seguridad (Julian Russell, 2021).

Lo adecuado para mantener un ambiente de mejora continua es evitar la conformidad y adoptar acciones correctivas naturalmente. ¿Por qué? La mejora continua es accesible a través de la retroalimentación y la experiencia, es decir, se consigue aprendiente de los incidentes de seguridad que se presentan a lo largo de la vida del SGSI, además, aquellos que son identificados en las auditorías realizadas. Es importante mantener un registro claro de lo que ocurre en cada incidente, los eventos o consecuencias generadas tras un incidente, la causa base del incidente, las acciones tomadas para gestionar el incidente o incluso para eliminar la raíz del problema, y por último la evaluación de la efectividad de las acciones tomadas (Julian Russell, 2021).

Para poder identificar maniobras de corrección efectivas es indispensable realizar un análisis de "causa-raíz", siempre enfocado al problema. El objetivo de dicho análisis es evitar implementar soluciones que no serán efectivas. ¿Cómo identificar una solución efectiva? Esto es posible al hacer uso del enfoque de los "5 por qué". Normalmente las cinco preguntas son suficientes para llegar hasta la causa-raíz de un problema de manera certera y efectiva, de manera que, en base a cuestionarse "¿Por qué?" y dar respuesta a esta pregunta iterativamente desde la declaración del problema en cada evento puede ser de gran ayuda para identificar correctamente el causante base. Considérese siembre a la evaluación de riesgos en el análisis de causa-raíz (Julian Russell, 2021).

2.6 Implantación de la norma ISO27001

La implementación de un SGSI debe completarse con el objetivo de sacarle a este el máximo provecho, por lo tanto, la correcta implementación de un SGSI puede conseguirse considerando los siguientes aspectos, como menciona (Julian Russell, 2021).



Ilustración 9: Diagrama de la Implementación de un SGSI correcto

Fuente: nqa. > Cláusulas ISO 27001:2013 Elaboración: David Mora

Tras la correcta implementación del SGSI deben considerarse ciertos pasos post-implementación, mismos que son descritos a continuación, según (Julian Russell, 2021):

1. Formación de conciencia
    a. La institución deberá motivar conciencia sobre los estándares acaparados por SGSI.
    b. La organización deberá considerar sesiones de capacitación focalizadas en todos los niveles de gerencia, con el fin de generar un ambiente de motivación, preparado para la implantación (p. 30).
2. Objetivos y política
    a. La institución deberá desarrollar políticas integrales de calidad y objetivos de relevancia, para cumplir los requerimientos.
    b. La institución deberá ofrecer cursos con el personal en todos sus niveles de gestión, para delimitar los objetivos intrínsecos (p. 30).
3. Análisis interno (deficiencias)
    a. La institución deberá identificar y, posteriormente evaluar el grado de satisfacción de los sistemas con los requisitos de las normas del nuevo SGSI.
    b. Las operaciones de desarrollo y organización, además de las actividades del negocio, deben tener el entendimiento de todo el personal asignado de la institución. (p. 30).
4. Procesos de diseño y documentación
    a. La institución deberá documentar los procesos según los requerimientos de las normas de relevancia.

   b. La institución deberá implementar y documentar manuales, procesos funcionales, procedimientos del sistema, instrucciones de trabajo, y deberá proporcionar los términos asociados que sean necesarios.

5. Proceso de implantación y documentación
   a. Tanto los procesos, como la documentación desarrollada deberá implementarse en la organización en su totalidad además de abarcar a las actividades y departamentos en cuestión, en base a lo realizado en la documentación y proceso de diseño.
   b. La organización debe realizar talleres sobre la implementación según corresponda para los requisitos de la norma ISO (p. 30).
6. Auditoría interna
   a. Es esencial mantener un sistema interno robusto de auditoría.
   b. Con la finalidad de dar garantías de eficacia, se requiere la implementación de acciones correctivas para mejoras iterativas, además de integrar toda la documentación. (p. 30).
7. Organizar la revisión por la dirección del sistema
   a. Dar revisión a aspectos comerciales de la institución relevantes para las normas a implantar.
   b. La gerencia deberá revisar la política, objetivos, resultados de la auditoría interna y del desempeño de procesos (p. 30).
8. Análisis de sistemas implantados (deficiencias)
   a. La institución debe analizar las deficiencias que comprometen el cumplimiento y efectividad de la implantación del SGSI.

b. El análisis de deficiencias permite que la institución se prepare para el proceso final de certificación ante la auditoría (p. 30).

9. Acciones correctivas
    a. Si, en base al análisis de deficiencias, todas las inconformidades han concedido acciones de corrección, la institución estará preparada para la certificación a través de la auditoría final.
    b. Verificar que, las inconformidades significativas están cerradas (p. 30).
10. Auditoría de certificación final
    a. Una vez completada la auditoría de forma satisfactoria, la organización recibirá la certificación (p. 30).

2.7 Ciberseguridad según la norma ISO/IEC 27032

La norma ISO/IEC 27032, toma en cuenta a la ciberseguridad de un punto elevado, en el cual se enuncia la interacción de personas, software e Internet como un concepto amplio del ciberespacio. Define sus guías basadas en dos áreas: la primera es profundizar en temas que anteriores normas han dejado de lado, cubriendo vacíos en el ámbito conceptual; y, su segunda área es el proceso de colaboración en un entorno denominado “Marco de ciberseguridad o CSF”.

Este marco de ciberseguridad envuelve cuatro áreas de gestión de riesgos; prevención, protección y previsión, respuesta y comunicación, rrecuperación y aprendizaje (Isecauditors, 2012).

2.8 Norma ISO/IEC 27032

Se enfoca en distintos riesgos o problemas existentes en el ciberespacio con el único objetivo de volver sencillas las transacciones comerciales. El ciberespacio está constituido por:

- Seres humanos
- El software y el hardware
- Los servicios que se ofrecen en Internet
- Las organizaciones
- Las redes de datos (TIC)

La norma tiene presente todos estos componentes, su colaboración entre sí y los riesgos de los cuales se destacan los siguientes;

a) Los ataques de ingeniería social.
b) Los intentos de explotación de vulnerabilidades.
c) La proliferación actual de malware.
d) La existencia de software con la capacidad de espiar nuestras comunicaciones.

Para mejorar la seguridad en el ciberespacio la norma considera tres elementos importantes: compartir información, administrar incidentes relacionados a la seguridad de la información y coordinar respuestas. Como un método de mitigación de riesgos ISO propone la preparación, detección y respuesta como un ciclo continuo a lo largo del uso de la norma (Sisteseg Consulting, 2018).

2.9 Terminología de la norma ISO/IEC 27032

Para la norma y su completo entendimiento se presenta un glosario de términos, detallado en el siguiente diagrama.

Término	Definición
Avatar	Representación de una persona que participa en el ciberespacio.
Vector de ataque (attack vector)	Ruta o medio por el cual un atacante puede ganar acceso a un computador o al servidor de una red, para implementar un resultado malicioso.
Bot / robot (bot / robot)	Programa de software automatizado utilizado para llevar a cabo tareas específicas.
Botnet (botnet).	Software de control remoto, específicamente una colección de bots maliciosos, que se ejecutan de manera autónoma o automáticamente en computadoras comprometidas
Ciber intruso (cyber-squatter)	Personas u organizaciones que se registran y mantienen en direcciones URL que se asemejan a las referencias o nombres de otras organizaciones en el mundo real o en el ciberespacio
Hactivismo (hacktivism)	Acceso intencional a un sistema informático sin la autorización del usuario o el propietario
Piratería informática (hacking)	Realizar piratería informática con un propósito o motivación política o social
Seguridad en Internet (Internet security)	Preservación de la confidencialidad, la integridad y la disponibilidad de la información en la Internet.
Activos físicos (physical asset)	Activo que tiene una existencia tangible o material.
Estafa (scam)	Fraude o engaño 4.42 mensaje basura (spam). Abuso de los sistemas de mensajería
Troyano (trojan / trojan horse)	Software malintencionado que aparenta realizar una función deseable.
Zombi computador zombi drone (zombie/zombie computer/ drone)	Computador que contiene software oculto que permite a la máquina ser controlada de forma remota, por lo general para llevar a cabo un ataque a otro equipo.

Tabla 2: Terminología de la norma ISO/IEC 27032
Fuente: (Sisteseg Consulting, 2018) Elaboración: David Mora

2.10 Controles de ciberseguridad de la norma ISO/IEC 27032

Los controles de ciberseguridad se realizan como un plan de implementación por dominios, en el cual se estima el nivel de madurez y la complejidad según el tiempo de implementación, costes de mantenimiento y costes de implementación.

Se determinan cuatro controles de ciberseguridad, como se detalle en el siguiente cuadro.

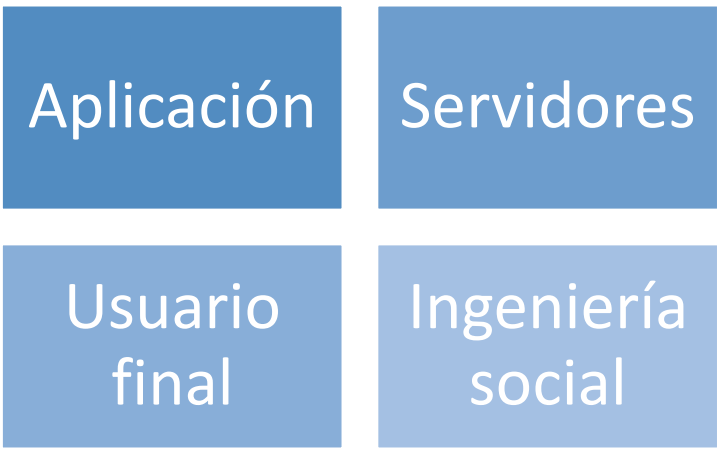


Ilustración 10: Diagrama de Sistema de Información Organizacional

Fuente: Implementación ciberseguridad ISO 27032 Elaborado: David Mora

Los controles de aplicación manejan cinco pasos para mantener la ciberseguridad, los que inician con: la presentación de políticas empresariales, continúan con el manejo de sesiones web, prevención de ataques de scripting, revisión de código y finaliza con servicios autenticados y seguros.

Protección de servidores; uso de estándares de configuración, actualizaciones periódicas, generar registros, uso de antivirus y antispyware, análisis de vulnerabilidades, revisiones periódicas de malware.

Los controles de usuario final examinan: la instalación de actualizaciones, aplicaciones actualizadas, uso de antivirus y antispyware, bloqueadores de scripts, bloque de ventanas emergentes, filtros de phishing, uso de firewall personal.

Controles para la ingeniería social; políticas de seguridad, clasificación de la información, sensibilizaciones, controles técnicos aplicables.

2.11 Modelo de seguridad para la norma ISO/IEC 27032

El modelo de seguridad convierte el proceso de implementación de controles de seguridad más sencillo. Como parte fundamental de la documentación el modelo es primordial para logar la protección total de la información.

El modelo se define como una pirámide estructurada de estándares, políticas, entre otros, tal como se puede apreciar en el gráfico.

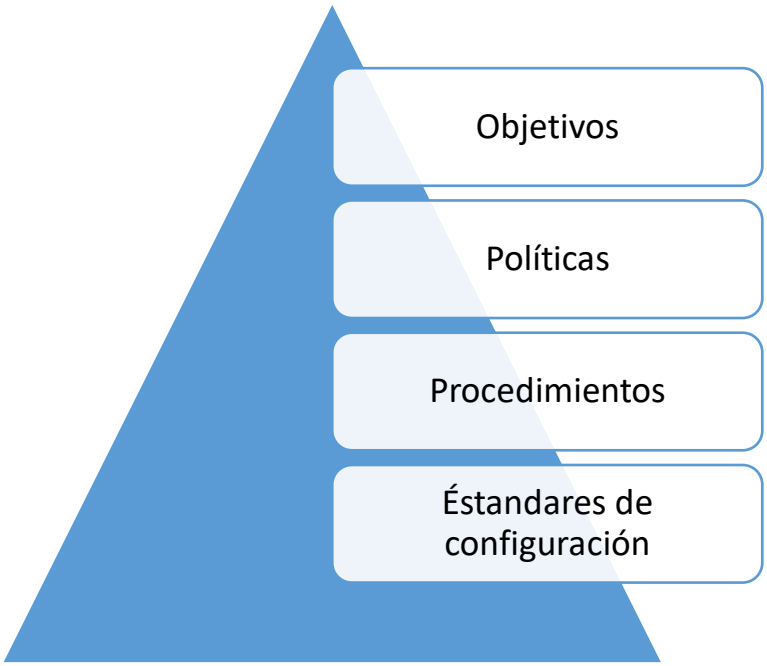


Ilustración 11: Grafico del modelo de seguridad norma ISO/IEC 27032

Fuente: incibe.es Elaborado: David Mora

2.12 Contraste comparativo de la norma ISO27001 y ciberseguridad



Ilustración 12: Grafico comparativo de la norma ISO 27001 y ciberseguridad

Fuente: incibe.es Elaborado: David Mora

CAPÍTULO III

3. Propuesta metodológica

3.1 Activos de Información según ISO27001

La gestión de los activos de la información es indispensable, considerando que estos soportan a los diferentes procesos de la organización. La norma ISO27001 lista como requisito a la correcta gestión de los activos de información (ISOwin, 2017). La gestión de dichos activos comprende:

- Identificación a través de inventarios
- Designación de responsables
- Designación de propietarios
- Determinación de la utilización de los activos
- Recuperación de activos
- Control de difusión

Los activos de información son recursos utilizados por un SGSI o Sistema de Gestión de Seguridad de la Información, con la funcionalidad destinada a la operatividad de las organizaciones, y así consigan los objetivos y metas que estas se hayan propuesto, según la alta dirección de la organización. Los activos de información siempre se encuentran asociados con las demás entidades de una empresa, sea de manera directa o indirecta (Toro, 2017).

Un proyecto de seguridad de la información exitoso mantiene, primordialmente, la finalidad de controlar la seguridad de los activos de información que generan el dominio en el estudio y desarrollo de proyectos, donde, es importante señalar que la limitación del conjunto de activos del dominio o de la organización no imposibilita la consideración de las relaciones de seguridad de los activos de información mencionados con el entorno o sistema general (Toro, 2017).

3.1.1. Identificación de activos

La norma ISO 27001 exige la construcción de un inventario de activos. Tómese en cuenta que, la única manera de conocer con exactitud las posesiones de una empresa es a través del control de activos mediante inventarios. El inventario deberá actualizarse permanentemente y a largo plazo, de manera que conllevará revisiones periódicas, además, se prestará a cambios continuos, mismos que deberán ser comunicados en todo momento (ISOwin, 2017).

Los activos de los sistemas de información pueden segmentarse en dos grandes grupos:

- Tangibles: Activos materiales que contienen información, sobre los cuales se establecerán medidas de protección definidas por la ISO/IEC 27031 y protocolos de ciberseguridad, además de medidas preventivas ante posibles riesgos físicos.
- Intangibles: Activos que soportan la información dentro de activos materiales, y, a su vez, tienen la capacidad de inutilizar la información, a pesar de que el activo físico no haya sufrido algún tipo de daño, Siendo gestionados directamente por la ISO27001.

En una organización, los inventarios generados en el área de los sistemas de información, y almacenados en una base de datos corresponden a un activo intangible.

Información de una base de datos = ACTIVO INTANGIBLE

Los servidores (hardware) en los cuales se encuentran activas las bases de datos de una organización corresponden a un activo material o tangible.

Servidores (hardware) = ACTIVO TANGIBLE

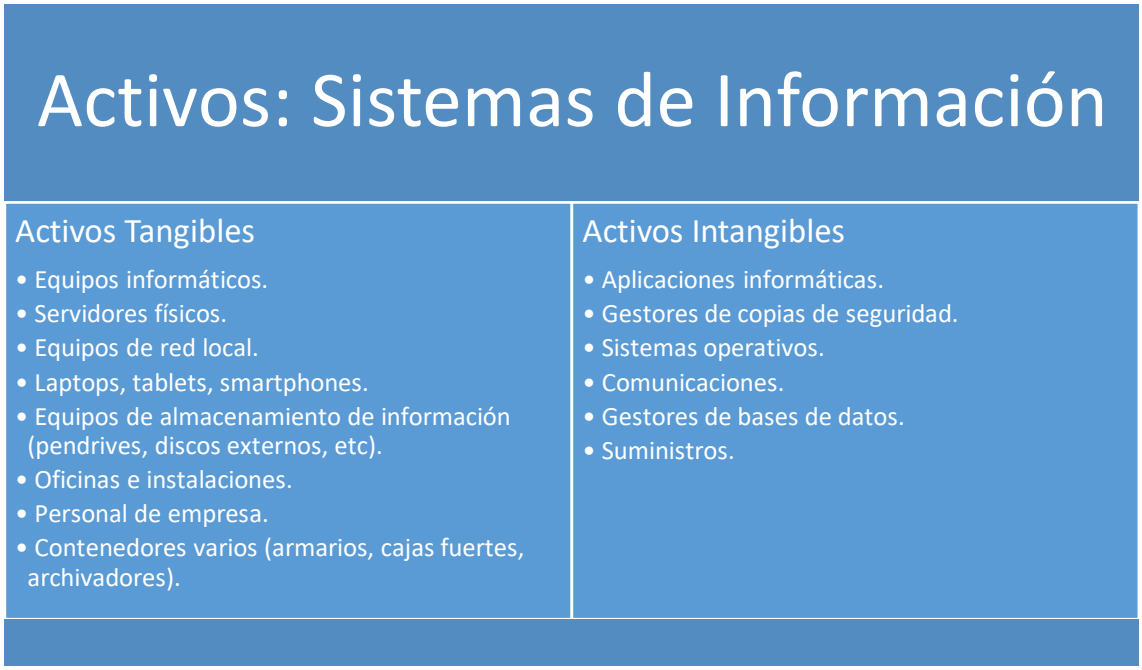


Ilustración 13: Grafico de clasificación de activos de los sistemas de información

Fuente: isowin.org Elaborado: David Mora

3.1.1. Valoración de los activos de información

Identificar la valoración de los activos de información es necesario para cuantificar la importancia de estos, dimensionando así sus aspectos o nivel de criticidad, según la información que contienen. Dentro de la ISO 27001, se consideran criterios básicos para la valoración de los activos de información. Por lo general, tomando en consideración a las metodologías CID y MAGERIT, pueden detallarse cinco principios fundamentales (ISOwin, 2017).

- Confidencialidad: Garantía de protección de la información personal, con la finalidad de impedir que esta sea divulgada sin el consentimiento de la persona. El principio de confidencialidad está condicionado por un modelo conjunto de reglas que limitan el acceso a la información.

- Integridad: Garantizar que la información contenida en el activo de información permanezca integra, es decir, fiel y completa. Además, esta no será eliminada o modificada parcial o completamente por terceras personas, incluso si se tratase de casos no intencionados.
- Autenticidad: Garantizar que la fuente de información es fiable, segura y verificable, de manera que la información a tratar no pierda su valor.
- Trazabilidad: Capacidad de gestión de las acciones y usos que se le da a un determinado activo de información, a través de controles que documenten los procesos en los que el activo de información está involucrado.
- Disponibilidad: Capacidad de acceder a la información incluida en el activo de información por parte del personal autorizado, siempre que así se requiera.

Los criterios a considera para las cinco dimensiones focalizadas en la valoración de los activos de información deben ser cuantificables, con el objetivo de establecer métricas de evaluación del desempeño. Además, los criterios a fijar deberán ser objetivos que ayudarán a determinar el valor de cada activo en la organización. Para cada una de estas dimensiones se deberán fijar criterios objetivos y cuantificables, que nos servirán para determinar su valor en cada Activo. Se suelen utilizar escalas numéricas asociadas a los distintos valores que pueda tomar la dimensión. Determinar estos criterios suele ser una labor complicada a la que deberemos dedicar tiempo, si queremos obtener resultados coherentes con la realidad de la empresa. Dentro del área de la seguridad de la información, valiéndose tanto de la gestión de la seguridad de esta, según la ISO 27001, como de la Ciberseguridad, según ISO/IEC 27032, es imprescindible desarrollar correctamente los procesos de evaluación de riesgos, así también como de su gestión, por lo cual, es de gran importancia priorizar a la identificación y clasificación de los activos de información (ISOwin, 2017).

3.2 Cláusulas de integración de ISO 27001 y Ciberseguridad

Los criterios a considera para las cinco dimensiones focalizadas en la valoración de los activos de información deben ser cuantificables, con el objetivo de establecer métricas de evaluación del desempeño (INTERNET SECURITY AUDITORS 2021, 2012).

3.2.1. CLÁUSULA 1: Contexto/Entendimiento de la organización

La integración de la norma ISO 27001:2013 y ciberseguridad, según ISO 27032, plantea lo siguiente:

- Determinación de aplicabilidad: Conocer el alcance de aplicabilidad de la metodología integrada de Gestión de Seguridad de la Información y Ciberseguridad, considerando aspectos clave.
    - Gestión de la Seguridad de la Información, según ISO 27001:
        - Aplicable a todo tipo de organización.
        - Certificable.
    - Ciberseguridad, según ISO 27032:
        - Aplicable en base al contexto organizacional.
        - No certificable.
- Inmersión en procesos de la organización: Conocer la funcionalidad y modalidades de operación de cada proceso de la empresa, además de la usabilidad del ciberespacio de cada proceso en sus servicios.
- Análisis del entorno de operabilidad de la organización: Conocer y evaluar aquellos procesos requieren considerar, fortalecer o añadir un SGSI efectivo y eficiente. Las áreas de prioridad especificas dependerán del contexto de la organización, a nivel interno y externo.
- Disposición de un inventario de activos de los servicios.

El contexto/entendimiento de la organización, según el planteamiento de la integración de la norma ISO 27001:2013 y ciberseguridad, según ISO 27032, señala el siguiente flujo de desarrollo:

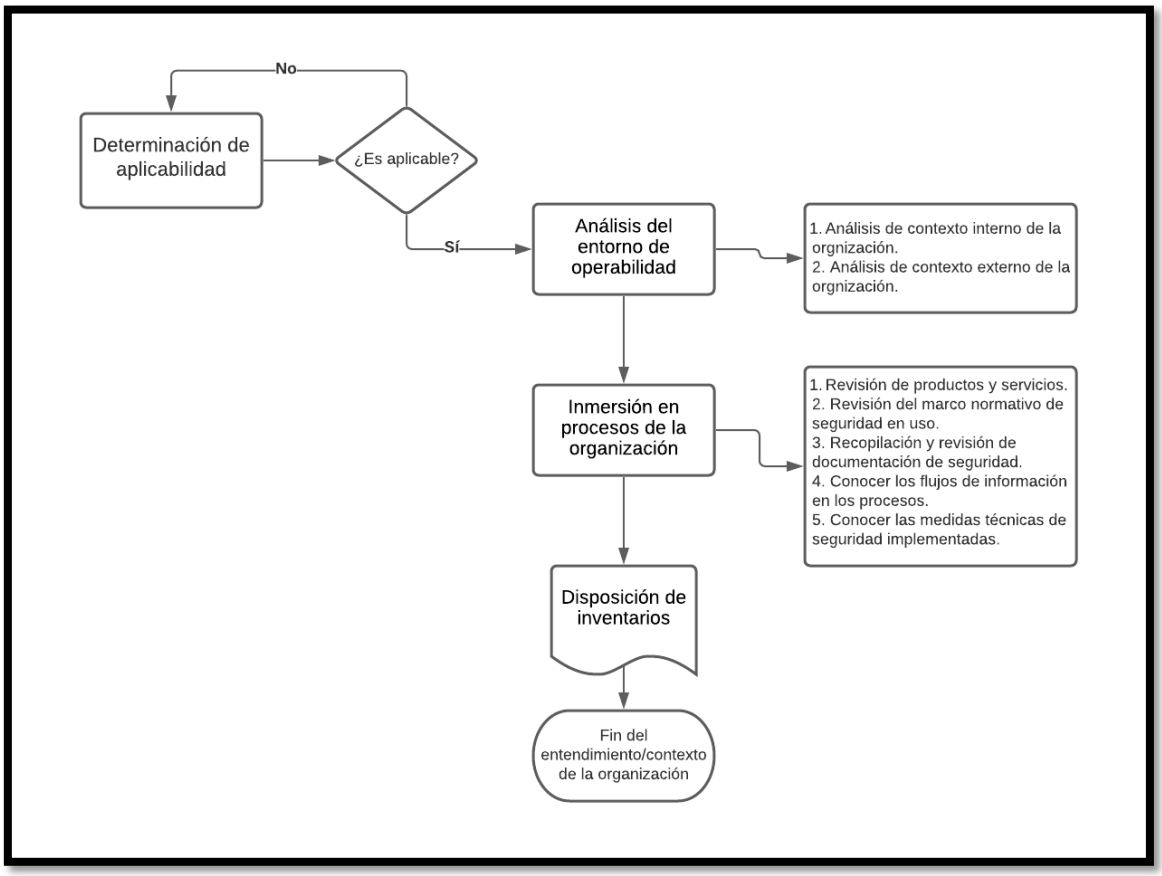


Ilustración 14: Grafico del flujo del contexto/entendimiento de la organización, según la propuesta metodológica integrada.

Elaborado: David Mora

3.2.2. CLÁUSULA 2: Liderazgo

La integración de la norma ISO 27001:2013 y Ciberseguridad, según ISO 27032, considera al liderazgo como un modelo de condición del ejercicio de la participación activa, implícito, tanto en la seguridad del Ciberespacio como en la dirección del SGSI, fomentar su despliegue e implantación, para así garantizar la disponibilidad de recursos apropiados y contar planes de acción adecuados. El liderazgo en la organización, alineado a la propuesta metodológica integrada incluye las siguientes cláusulas:

- Se ha de garantizar que, el objeto del SGSI serán evidente y se alinearán a la estrategia organizacional general.

- Asegurar la gestión de riesgos de la seguridad de los componentes implicados en el ciberespacio o entorno virtual.
- Garantizar la claridad sobre las responsabilidades.
- Fundamentar, en su totalidad, los procesos de toma de decisiones en el pensamiento basado en el riesgo.
- Clarificar los procesos de comunicación asociados a todos los individuos componentes del alcance del SGSI.
- Clarificar los procesos de comunicación asociados a los individuos involucrados en los campos comprendidos por el ciberespacio.

La participación de la gerencia es un factor clave para el éxito de la organización a nivel de la seguridad informática. En consecuencia, la gerencia y los líderes establecidos serán cruciales al momento de garantizar la implementación y mantenimiento efectivo del SGSI, al igual que al implantar los planes de acción elaborados por el plan director de ciberseguridad según ISO 27032.

El liderazgo puede gestionarse e interpretarse desde tres enfoques y aspectos clave, considerando a toda organización determinación de aplicabilidad positiva para ISO 27001 e ISO/IEC 27032. Los aspectos que considerar se describen a continuación:

- Políticas de Seguridad:
    - **Aplicable en: ISO 27001 e ISO/IEC 27032**
    - Una política de seguridad de la información alineada a los objetivos clave de la empresa deberá establecerse y documentarse.
    - La inclusión de un marco y objetivos deberá establecerse.
    - Inclusión de compromisos para cumplir requisitos aplicables relacionados con la seguridad de la información y la mejora continua del SGSI.
    - Inclusión de planes para cumplir requisitos aplicables focalizados en la gestión del riesgo relacionado al entorno digital.

- Se podrán incluir políticas y su políticas de seguridad relacionadas a la información, que de cobertura a los controles del SGSI.
- La política de ciberseguridad puede incluir subpolíticas focalizadas en la prevención, detección, protección, acción, comunicación, recuperación y aprendizaje de los riesgos.

- Roles y responsabilidades:
  - **Aplicable en: ISO 27001 e ISO/IEC 27032**
  - Las responsabilidades que tiene el personal de la organización deben definirse y comunicarse claramente.
  - El nombramiento de un representante de Seguridad de la Información no es ineludible.
  - El nombramiento de un representante de Ciberseguridad no es ineludible.
  - Es recomendable designar líderes para dirigir equipos de seguridad de la información y ciberseguridad.
  - Es recomendable que los líderes designados sean miembros de la gerencia.
  - El líder del equipo de la seguridad de la información será el agente responsable de la protección de los servicios de TI.
  - El líder del equipo de ciberseguridad, en caso de designarse, será el agente responsable de la gestión de riesgos relacionados los campos involucrados en el espacio cibernético: Personas, redes, organizaciones, hardware, software e internet.
  - El equipo de ciberseguridad puede segmentarse y gestionarse a través de sublíderes.
  - Los sublíderes serán designados y supervisados por la gerencia.

- Evidencia del liderazgo al auditor:
    - **Aplicable en: ISO 27001**
    - **Considérese que ISO/IEC 27032 Ciberseguridad no es auditable.**
    - La gerencia establecerá la dirección estratégica de la organización y admitirá la asignación de recursos según el alcance del SGSI.
    - En base a un modelo de entrevistas personales, el auditor tendrá la obligación de evaluar el desempeño del liderazgo y su nivel de participación.
    - Los aspectos por evaluar son:
        - Evaluación de riesgos/oportunidades.
        - Instauración de políticas y comunicación.
        - Objetivos.
    - La revisión del desempeño del SGSI, al igual que la asignación de recursos, serán considerados junto a los roles y responsabilidades.

3.2.3. CLÁUSULA 3: Planificación y análisis de riesgos

La sección de la planificación y análisis de riesgos de la propuesta metodológica integrada comprende que, tanto ISO 27001:2013 como ISO/IEC 27032 son normas que presentan una herramienta destinada para la gestión de riesgos, orientados a la seguridad de la información.

ISO 27001:2013 se manifiesta como una herramienta facilita la guía en el proceso de detección de riesgos de seguridad de la información a una organización. Por otro lado, **ISO/IEC27032** se presenta como una herramienta dispuesta a abordar los retos de la seguridad del entorno digital o ciberespacio, considerando la seguridad de la información, seguridad de las redes, seguridad en internet y la protección de las infraestructuras críticas

para la información. Considerando lo mencionado, el propósito de la integración de las normas se presenta de la siguiente manera:

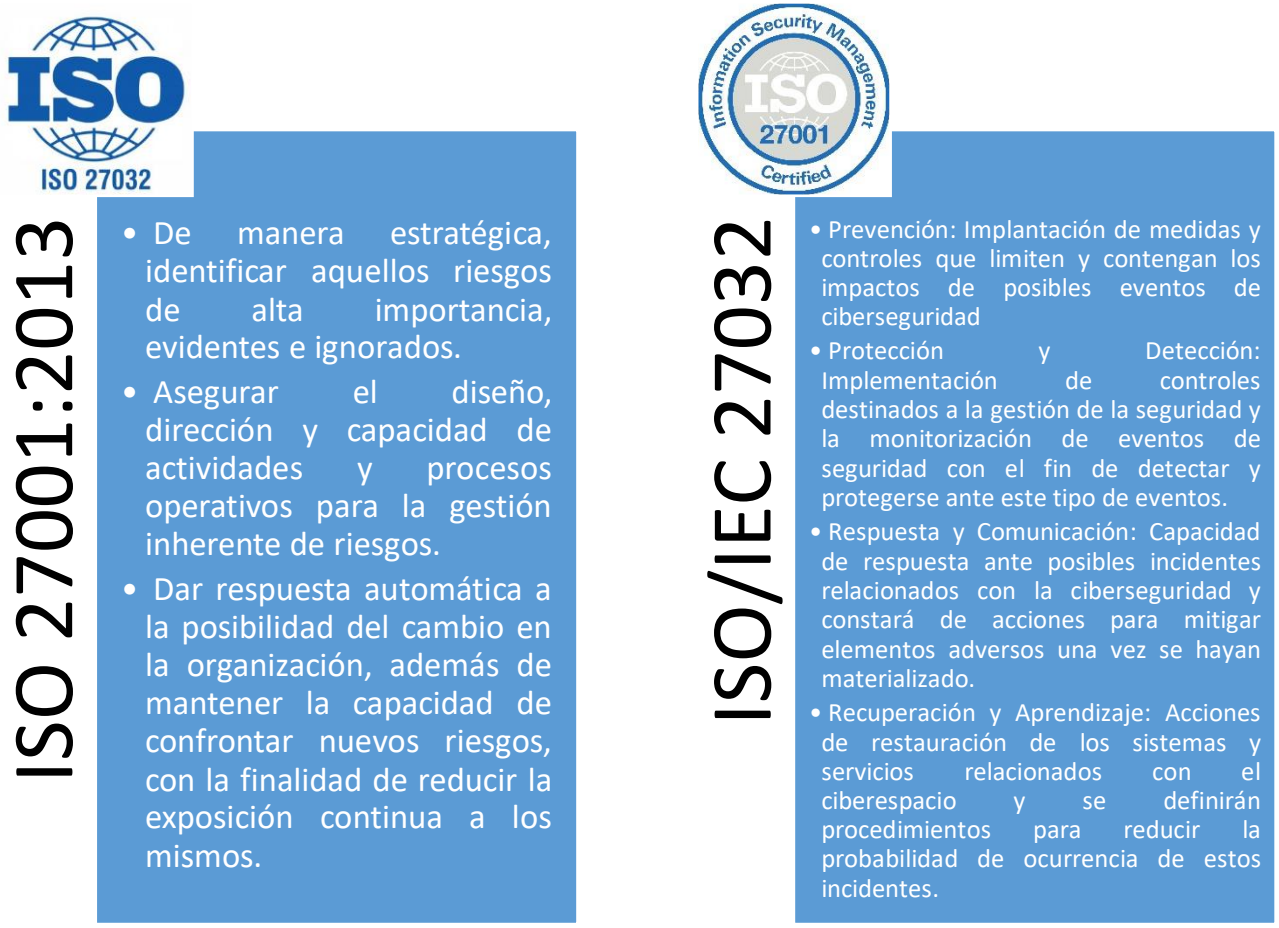


Ilustración 15: Planificación y análisis de riesgos, según la propuesta metodológica integrada

Elaborado: David Mora

La evaluación de riesgos considera la posibilidad de sufrir cualquier tipo de incidente en la seguridad de la información, en base a la correcta operatividad de un SGSI eficiente y, tomando en cuenta, la seguridad del espacio cibernético. La evaluación de riesgos es imprescindible para aumentar la probabilidad de identificar riesgos potenciales haciendo uso de técnicas de evaluación sistemática.

Según la integración de la Gestión de la Seguridad de la Información y la Ciberseguridad, los elementos básicos a incluir se detallan a continuación:

1. Fundamentar al proceso de toma de decisiones en la gestión de los riesgos y el alineamiento con las necesidades de la empresa.
2. Notificar la identificación sistemática de riesgos, considerando los activos críticos amenazados o potencialmente afectados, en base a su nivel de prioridad.
3. Verificar la comparecencia de vulnerabilidades y amenazas, documentando los controles necesarios para su posterior implementación y gestión.
4. Analizar el grado o nivel del impacto consecuente tras la aparición de amenazas determinadas, además de los riesgos presentes.
5. Considerar la posibilidad de ocurrencia de un riesgo persistente bajo un marco de evaluación consistente.
6. Marco de evaluación de las consecuencias, considerando a aquellos riesgos ocasionales.
7. Clasificar los riesgos identificados, tomando en consideración la evaluación de posibilidad y las consecuencias potenciales.
8. Documentar parámetros de especificación de los planes de acción según el nivel o prioridad determinado.
9. Asegurar las responsabilidades determinadas según los criterios de liderazgo para permitir el mantenimiento y gestión de riesgos y amenazas de manera óptima a través del tiempo.

Según ISO 27001 e ISO/IEC 27032, el tratamiento de los riesgos debe ser desarrollado individualmente, además, deberá considerarse su criterio de aplicación de manera aislada, de manera que, en caso de aceptar un determinado riesgo, este deberá ser tratado bajo la consideración de los aspectos expuestos a continuación:



Ilustración 16: Diagrama del Tratamiento de los riesgos

Fuente: nqa. > Cláusulas ISO 27001:2013 Elaborado: David Mora

3.2.4. CLÁUSULA 4: Soporte

La propuesta metodológica integrada, según ISO 27001:2013 e ISO/IEC 27032, hace referencia, de manera especial al soporte de los siguientes activos de información:

- Recursos de la organización:
  - Personal
  - Infraestructura
  - Materiales
  - Recursos físicos
  - Recursos digitales
  - Medioambiente
  - Herramientas
  - Internet
  - Redes de comunicación
  - Organizaciones

La seguridad informática deberá contar necesariamente con recursos de soporte, donde, dichos recursos deberán tener la capacidad, competencia, solidez y disponibilidad requerida por la dirección. Los aspectos para considerar para una correcta utilización, implementación de los recursos de soporte se detallan a continuación:

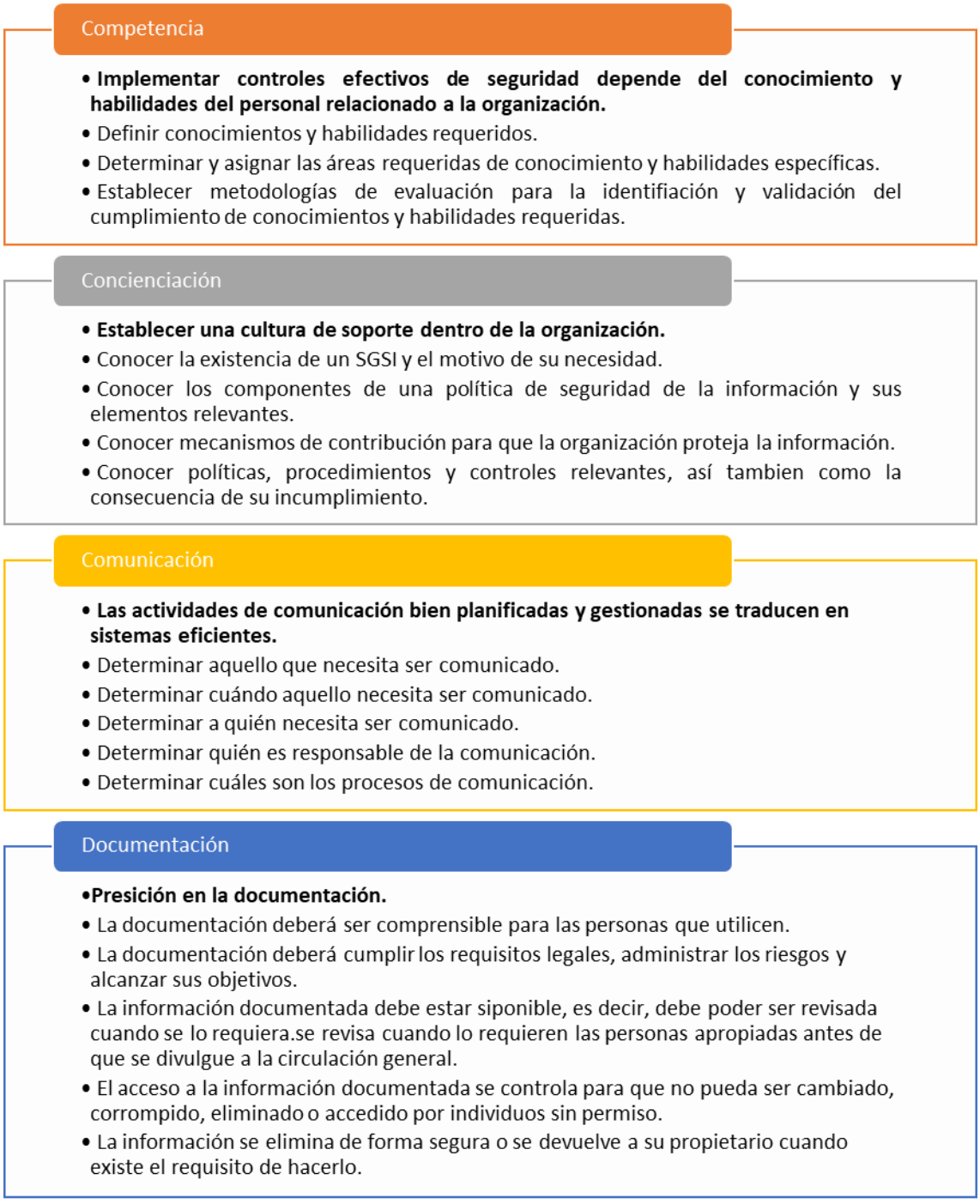


Ilustración 17: Diagrama del soporte de la ISO 27001l

Fuente: nqa. > Cláusulas ISO 27001:2013 Elaborado: David Mora

3.2.5. CLÁUSULA 5: Operación y plan de acción

La sección de operación y plan de acción de la propuesta metodológica integrada abarca, según ISO 27001:2013 e ISO/IEC 27032:2012, un plan de acción diseñado para identificar las medidas a desarrollarse para los lineamientos y exigencias del negocio, a partir de un criterio de priorización, además del control adecuado del entorno de creación y entrega de productos o servicios.

El plan de acción focalizado en el entorno cibernético considera estrategias que deberán ser aplicadas en niveles de la organización:

- Políticas
  - El plan de acción debe ajustarse con los lineamientos de la organización, además, deberá acoplarse a las políticas de esta.
  - Las políticas empresariales representan un sistema estructural y deliberado de principios que orientan el proceso de toma de decisiones, con la finalidad de alcanzar ciertas metas establecidas
- Identificación de roles
  - Dentro de toda organización, el plan de acción se desarrollará de manera segmentada y focalizada, es decir, el personal específico deberá ser determinado e identificado de acuerdo con los roles requeridos hacia una posible respuesta.
- Procesos afectados
  - Para gestionar los riesgos de la seguridad informática, dentro del plan de acción, debe priorizarse la claridad y coherencia de estos, de manera que pueda alcanzarse los objetivos de la organización. Para implementar procesos efectivos, deben considerarse los siguientes aspectos.

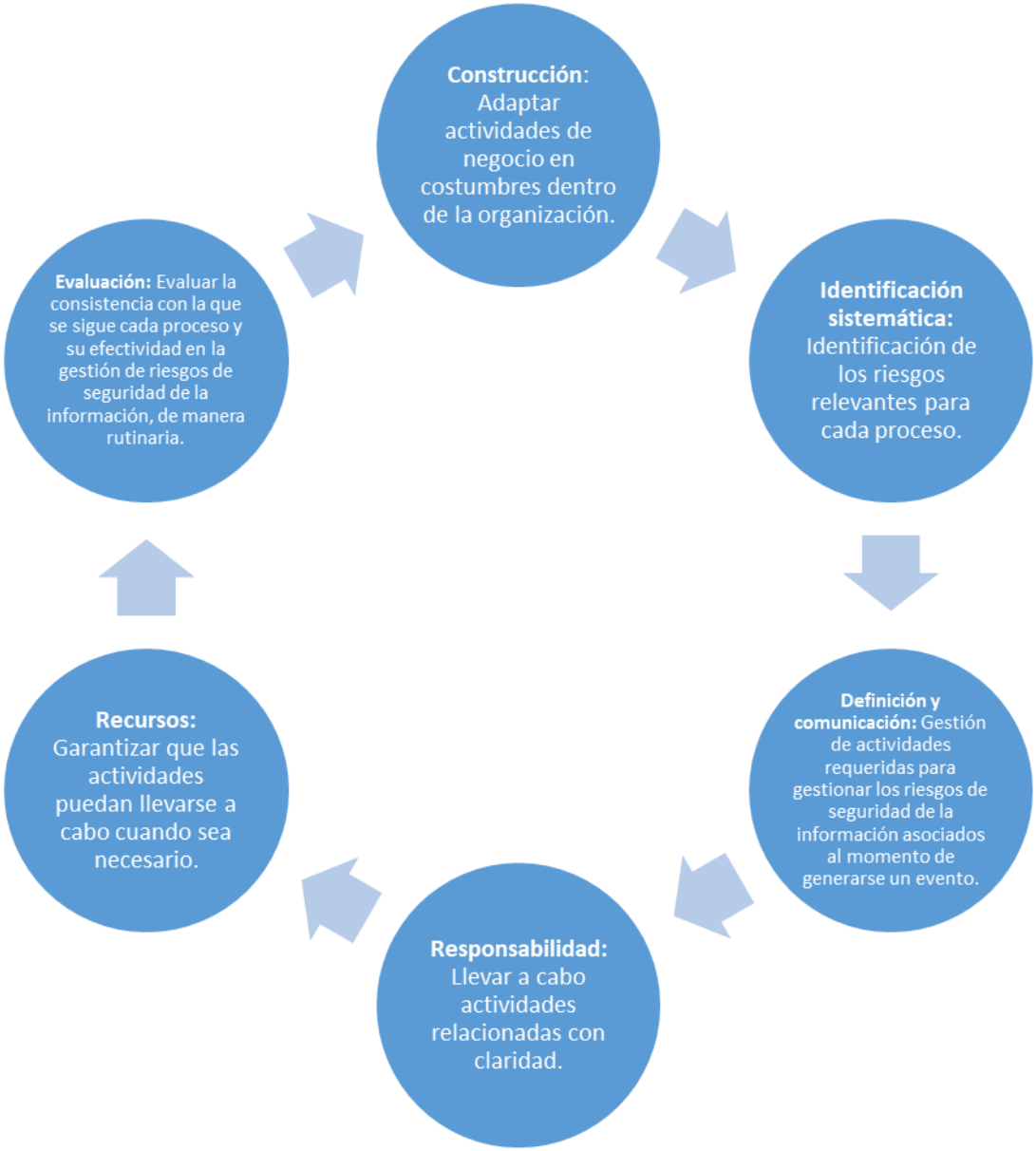


Ilustración 18: Diagrama de la gestión de los procesos, según la propuesta metodológica integrada

Elaborado: David Mora

- Controles tecnológicos
  - El proceso de gestión de los activos de una organización se llevará a cabo, dentro del plan de acción, gracias y en base a los controles tecnológicos, mismos que permiten un valor operativo altamente efectivo.

- Métodos de implementación
  - Los métodos de implementación, dentro del campo de ciberseguridad, pueden generalizarse en la detección, preparación y respuesta hacia los riesgos de seguridad de la información.

3.2.6. CLÁUSULA 6: Evaluación de desempeño

Según la sección de evaluación del desempeño de la propuesta metodológica integrada, para ISO 27001:2013 existen dos modelos de evaluación para el rendimiento del SGSI.

- **Seguimiento de efectividad:** Procesos/controles del SGSI.
- **Auditorías internas:** Llevadas a cabo a través de la gerencia de la organización durante las revisiones de control.

¿Cómo asegurar que, tanto el SGSI, como los controles y parámetros de seguridad de la información, se mantenga en orden, según lo esperado? El seguimiento, medición, análisis y evaluación del SGSI en la organización son indispensable para llevar a cabo el proceso de evaluación del desempeño. Dentro del seguimiento, análisis y evaluación del SGSI deberían poder responderse las siguientes incógnitas:

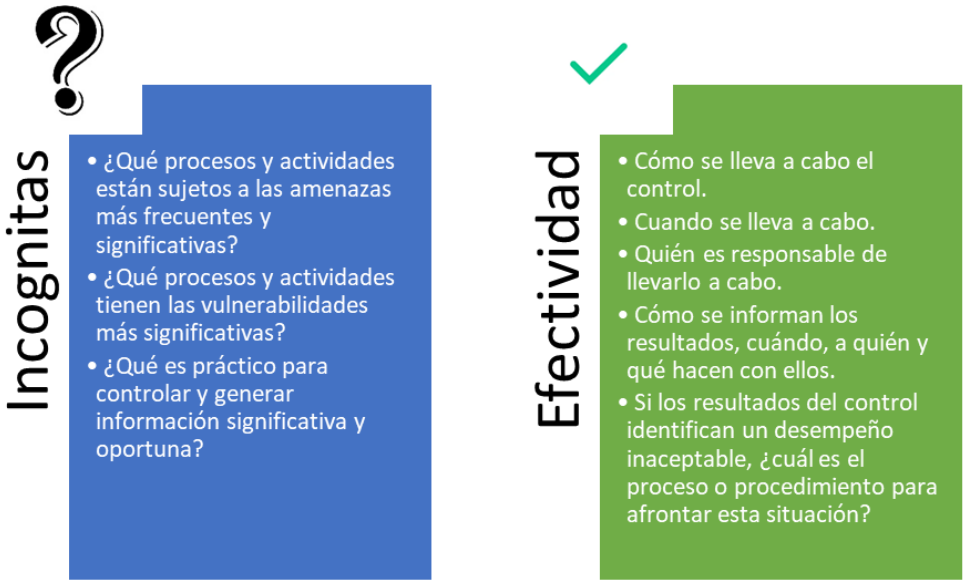


Ilustración 19: Diagrama de la Gestión de la evaluación del desempeño, según la propuesta metodológica integrada Elaborado: David Mora

ISO/IEC 27032 no es auditable, por lo tanto, la evaluación del desempeño puede llevarse a cabo a través de otros métodos. A pesar de que, alrededor del mundo, las empresas no realizar una evaluación del desempeño formal, hoy en día se recomienda considerar diferentes indicadores para profundizar en la ciberseguridad y brindar un mayor nivel de prioridad en el área de la seguridad del medio informático.

Para completar con la evaluación del desempeño de los protocolos de ciberseguridad se debe considerar los siguientes criterios, según (Editors ISOTools, 2019):

- **Criticidad del riesgo:** Evaluar las consecuencias potenciales para poder evaluar su criticidad, es decir, el riesgo aceptable y riesgo residual.
- **Riesgo aceptable:** En diversas ocasiones, resulta imposible eliminar un riesgo en su totalidad, sin embargo, puede gestionarse ocurrencia, a su vez, las consecuencias sobre la organización pueden minimizarse, a nivel económico, logístico, etc.
- **Riesgo residual:** Consideración del riesgo permanente y subsiste después de haber implementado los debidos controles y una vez se haya desarrollado por completo el SGSI de la organización. La evaluación del desempeño en esta etapa favorece en el proceso de identificar la eficacia de las medidas evaluadoras y correctoras para mitigar el riesgo inherente.
- **Compromiso del liderazgo:** El liderazgo del sistema de seguridad es imprescindible, de manera que pueda establecerse con exactitud a cada miembro del personal que tiene una determinada función, al igual que su manera de ejecutarla.
- **Dueños del riesgo:** Asociar cada amenaza potencial o real a un responsable, que es la persona que se asegura que se lleven a cabo las distintas actividades.

Las metodologías de evaluación de desempeño dentro de ISO/IEC 27032 puede llevarse a cabo a través de cuatro fases focalizados en los indicadores KPI y KRI.

- **KPI (Indicador clave de rendimiento):** Destinado a la gestión de datos históricos.
- **KRI (Indicador clave de riesgo):** Destinado a la gestión y pronósticos de datos futuros.

Los KRI, en base a los resultados obtenidos de un KPI, permiten anticipar oportunidades y problemas futuros, cimentándose en el análisis de tendencias que puedan afectar a la organización, esa positiva o negativamente. Es considerable señalar que los indicadores de rendimiento y de riesgo son relevantes para conseguir los objetivos y metas estratégicas de la organización (Cortés, 2017).

Las fases consideradas para la aplicación de la evaluación del desempeño pueden aplicarse en todos los niveles de la organización, y se exponen de la siguiente manera:

Fases para el desarrollo de KPI y KRI	**1. Establecer relevancia:** Involucrarse en la comprensión del contexto del negocio, identificar intereses en común y desarrollar combinaciones para los KPI y KRI.
	2. Generación de conocimientos: Involucrarse con la producción, calibración e interpretación de las combinaciones de KPI/KRI.
	3. Generación de impacto: Involucrarse en el desarrollo de recomendaciones relacionadas a los intereses en común y tomar decisiones respecto a los pasos a seguir.
	4. Aprendizaje y mejora: Involucrarse en el desarrollo de planes de aprendizaje y mejoras.

Tabla 3: Gestión de la evaluación del desempeño, según la propuesta metodológica integrada.
Elaboración: David Mora

3.2.7. CLÁUSULA 7: Marco de corrección y mejora

Según la sección de mejora de la propuesta metodológica integrada, ISO 27001:2013 e ISO/IEC 27032, mantienen como objetivo a la implementación de un SGSI eficiente, centrándose en la reducción del margen probabilístico de eventos de seguridad de la información indeseados ocurran, y también del impacto posible. Ninguna organización a nivel mundial estará totalmente invulnerable ante riesgos informáticos, sea en la seguridad de la información o en la seguridad del entorno cibernético, sin embargo, los sistemas de gestión y control se caracterizan por priorizar la capacidad de mejora continua a través de procesos de aprendizaje.

La gestión de la seguridad informática busca incrementar la **resistencia, solidez y robustez** frente a ataques de seguridad.

Considerar al proceso de corrección y mejora continua como un proceso que se alimenta de la retroalimentación y la experiencia, por lo tanto, la conformidad es necesariamente descartable. Para poder identificar las acciones correctivas en una organización debe considerarse el siguiente criterio:

Análisis Causa-Raíz: Focalización en el problema y la fuente de este.

- Ventajosamente, el análisis busca evitar la implementación de soluciones no efectivas.
- Impide el desperdicio de recursos aparentemente necesarios.

Para abordar el proceso de mejora en la seguridad informática de una organización deben considerarse los siguientes aspectos, sea para ISO27001:2013 e ISO/IEC 27032.

- **Prevención:** El objetivo a alcanzar es el de tener la capacidad de gestionar cualquier amenaza, por lo tanto, la inteligencia informática de seguridad es

necesaria para obtener una visión completa de todas las vulnerabilidades que puedan existir dentro de la organización, casi de manera inmediata.

- **Gestión durante un ataque:** Centralizar en un único punto el control de las amenazas.
- **Análisis para corrección de amenazas (posterior):** Es indispensable realizar un seguimiento con el objetivo de garantizar la corrección de las amenazas mediante informes y métricas.

La necesidad de gestionar la seguridad informática, en base a modelos de Ciberseguridad informática y la seguridad de la información, es evidente, por lo tanto, hoy en día, es recomendable actuar bajo estrategias mixtas de seguridad a nivel empresarial, manteniendo un enfoque ofensivo (Izertis, 2018).

3.2.8. CLÁUSULA 8: Implementación iterativa

La implementación de un marco metodológico de seguridad informático debe ser iterativo, es decir, debe mantener un proceso cíclico de mejora continua. La propuesta metodológica integrada plantea la gestión de la seguridad de la información y a su vez, de la ciberseguridad. Según ISO 27001:2013, un SGSI debe completarse efectivamente con el objetivo de obtener su máximo provecho, por lo tanto, implementar correctamente un SGSI es vital. Por otro lado, según ISO/IEC 27032, pretende obligar a las organizaciones a ser proactivos en lo que respecta a las medidas de seguridad, manteniendo un enfoque en los mecanismos y métodos de prevención hacia todos los activos involucrados en el ciberespacio, siendo uno de ellos los SGSI.

La seguridad de la información debe considerarse desde un amplio espectro, sin embargo, para que esta pueda consolidarse como un sistema robusto y sólido, debe

monitorearse de manera aislada, considerando que, el proceso crítico de implementación de un modelo de seguridad informática se desarrolla desde el plan de acción.

Implementación de ISO 27001: Para la óptima implementación de un modelo de seguridad destinado al SGSI deben considerarse los siguientes aspectos.



Ilustración 20: Diagrama de la implementación de un SGSI correcto, según la propuesta metodológica integrada
Elaborado: David Mora

Los pasos específicos para la implementación de ISO 27001 según los aspectos presentados en la ilustración 17, son los siguientes:

1. Apoyo de la alta gerencia, directores y junta directiva.
2. Establecer la metodología de implementación.
3. Definir el alcance del SGSI.
4. Redactar y establecer una política de seguridad de la información.
5. Definir el modelo de evaluación de riesgos.
6. Llevar a cabo la evaluación y el tratamiento de riesgos.
7. Dar a conocer el estado de su aplicabilidad.
8. Clarificar el plan de tratamiento de riesgos.
9. Definir los sistemas métricos para la efectividad de los controles.
10. Implementar todos los controles y procedimientos necesarios.
11. Crear/generar una cultura dentro de la empresa a través de programas de capacitación y concientización.
12. Monitorear y medir el SGSI para verificar su nivel de efectividad.
13. Realizar auditorías internas.
14. Realizar e implantar las mejoras necesarias.

Implementación de ISO/IEC 27032: La norma ISO destinada a la protección del ciberespacio plantea tres estrategias para mitigar riesgos: **detección**, **preparación** y **respuesta**. Considerando los siguientes campos de enfoque:

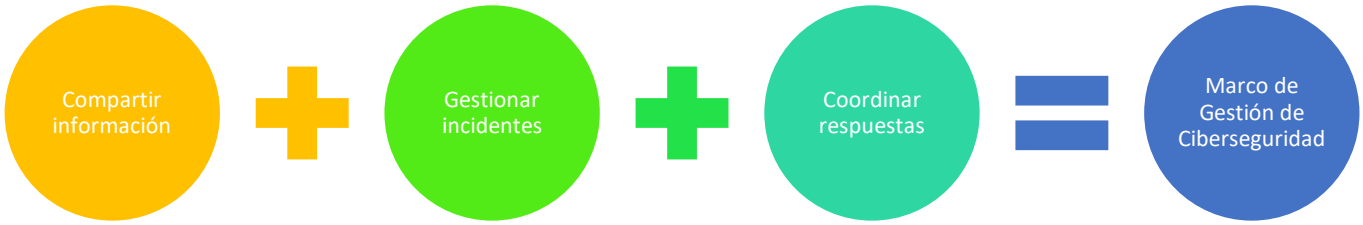


Ilustración 21: Diagrama de la implementación de un marco de gestión de Ciberseguridad, según la propuesta metodológica integrada
Elaborado: David Mora

ISO/IEC 27032, en base a la disponibilidad, confidencialidad e integridad, comprende cinco objetivos fundamentales de la seguridad en la información.

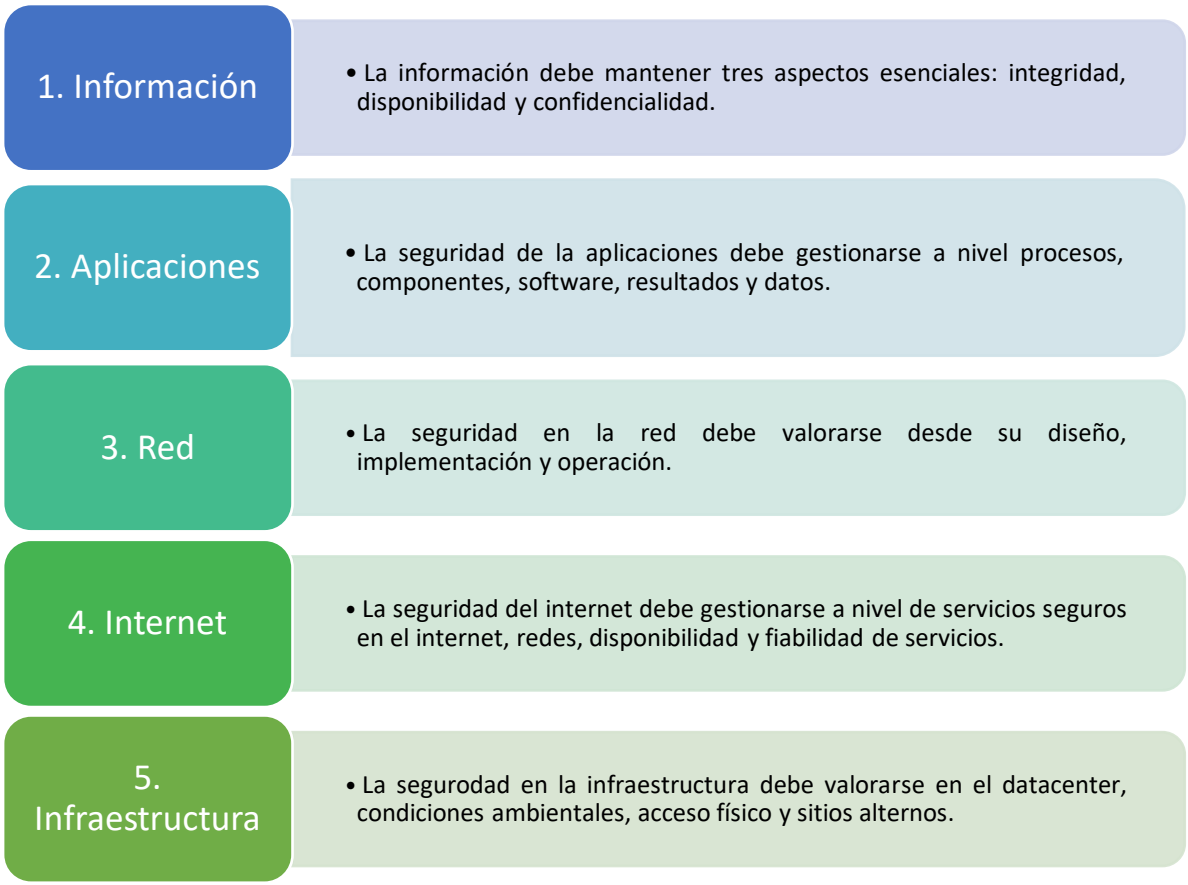


Ilustración 22: Diagrama de los objetivos de la implementación de un marco de gestión de Ciberseguridad, según la propuesta metodológica integrada
Elaborado: David Mora

La organización mantendrá un enfoque en la implementación de controles de seguridad, mismos que deberán considerar el nivel de madurez en la gestión de la seguridad. Para la implementación de controles deben considerarse los siguientes aspectos:

- Existencia de Política de Seguridad.
- Procedimientos de Seguridad en el Ciclo de Vida del Desarrollo del Sistema (SDLC).
- Marcos existentes para el intercambio de información.
- Planes de concienciación del personal.
- Metodología de análisis de riesgos (AARR).
- Monitorización de las Tecnologías de Información y Comunicación (TIC).
- Gestión de incidentes.

Según (Isecauditors, 2012), en la fase de implementación deberán establecerse los siguientes controles de seguridad:

- **Controles a nivel de aplicación:** gestión de sesiones, validación de datos, protección ante ataques, procesos de autenticación, etc
    - Presentar políticas empresariales
    - Manejo de sesiones WEB
    - Evitar ataques de scripting
    - Revisar código
    - Servicios autenticados y seguros
- **Controles a nivel de servidores:** configuraciones seguras, gestión de parches, monitorización., revisiones periódicas, etc
    - Usar estándares de configuración
    - Actualizaciones periódicas

  - Generar registros (logs)
  - Uso de antivirus y antispyware
  - Análisis de vulnerabilidades
  - Revisiones periódicas de malware

- **Controles para usuarios finales:** Actualizaciones de SO, uso de aplicaciones, antivirus, herramientas y configuraciones de seguridad, etc
  - Instalar actualizaciones del sistema operativo
  - Aplicaciones actualizadas
  - Uso de antivirus, antimalware y antispyware
  - Bloqueadores de scripts
  - Bloquear ventanas emergentes
  - Filtros de phishing
  - Uso de firewall personal
- **Controles contra ataques de Ingeniería Social:** Programas de concienciación, pruebas regulares, controles de seguridad, etc
  - Políticas de seguridad
  - Clasificación de la información
  - Sensibilizaciones
  - Controles técnicos aplicables

CAPÍTULO IV

4. Análisis de resultados

4.1 Ventajas y desventajas



Ilustración 23: Cuadro comparativo de ventajas y desventajas, según la propuesta metodológica integrada
Elaborado: David Mora



Ilustración 24: Cuadro comparativo, según la propuesta metodológica integrada
Elaborado: David Mora

La propuesta metodológica presentada plantea un conjunto de ventajas integradas, mismas que pueden beneficiar los sistemas de información como al entorno cibernético. Las ventajas por detallar se presentan a continuación:

- La privacidad de los datos es invaluable, la seguridad informática permite conservar de forma efectiva los datos privados de empleados y clientes, es de considerar que, el hecho de no proteger los datos representa un área de vulnerabilidad ante posibles ataques.
- La protección de los equipos, brindando seguridad al software y al hardware, mantendrá su integridad y prolongará su útil operatividad y funcionamiento.
- Proteger los datos y los equipos informáticos de manera integral garantiza la seguridad de la información.
- Un sistema de seguridad informática integral permite prevenir, evitar y gestionar riesgos de manera efectiva.
- Mediante modelos de autenticación, el acceso a la información puede ser limitado, cuidando la manipulación de los datos.
- Tanto la seguridad de la información, como la seguridad del entorno digital garantizará un modelo productivo de trabajo continuo.
- Los controles de seguridad posibilitan la realización de evaluaciones internas, manteniéndose alerta sobre amenazas constantes.
- A través de protocolos de seguridad, la propiedad de la accesibilidad permite que, únicamente, usuarios autorizados tengan acceso constante a los datos haciendo uso de la información siempre que lo necesiten, garantizando su disponibilidad.
- Reduce el riesgo de pérdida de la información.
- La implementación de metodologías de seguridad informática genera un valor agregado dentro de la empresa, mismo que podrá considerarse desde entidades externas, beneficiando la reputación de la organización.

4.2 Diagnóstico

El diagnóstico de la propuesta metodológica integrada puede completarse a través del seguimiento de seis pasos, los que se detallan a continuación:

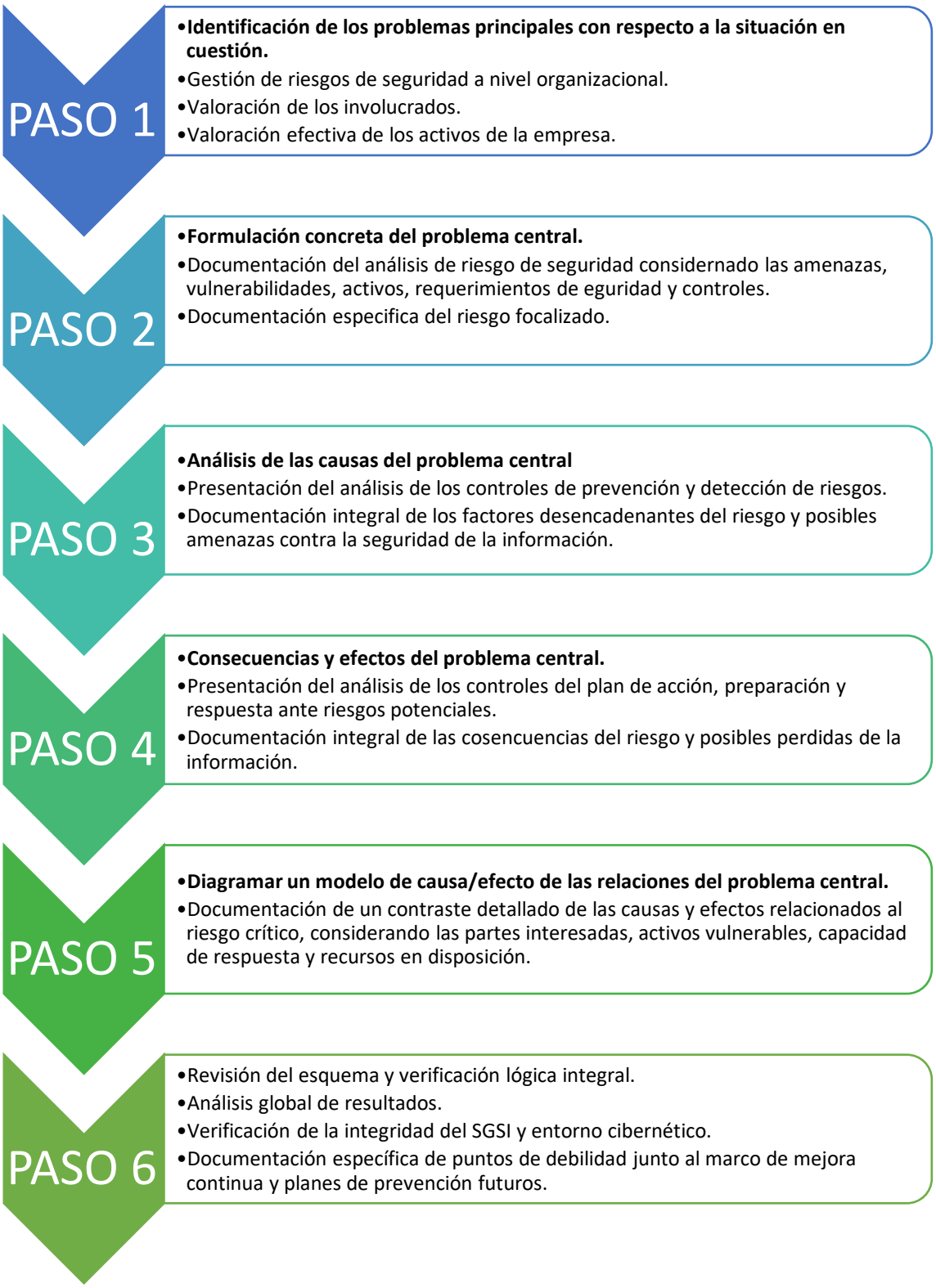


Ilustración 25: Diagrama sobre el diagnóstico de la propuesta metodológica integrada
Elaborado: David Mora

4.3 Análisis de la propuesta metodológica estipulada

El análisis de la propuesta metodológica integrada se desarrolla en la consideración de tres aspectos clave:

Integración de la Gestión de la Seguridad de la Información y Ciberseguridad

La propuesta metodológica integrada plantea un marco de implementación de controles destinados a la correcta gestión de la seguridad informática, abarcando, tanto a los sistemas de información como el entorno cibernético en el que estos se alojan. ISO 27001 e ISO/IEC 27032 mantienen un marco de referencia similar, orientado a la capacidad de gestionar los riesgos de seguridad, con el objetivo de salvaguardar la integridad y disponibilidad de la información.

ISO 27001 plantea una serie de controles para implementar un SGSI tanto correcta como eficientemente, en el que pueden identificarse herramientas que pretenden asegurar, integrar y mantener en confidencialidad toda la información de una organización, al igual que de los sistemas que la almacenan. Sin embargo, evitar y tener la capacidad de respuesta ante ciberataques no es un aspecto considerado a profundidad en ISO 27001, por lo tanto, ISO/IEC 27032 mantiene su enfoque en la ciberseguridad. Puede considerarse a la propuesta metodológica como una guía complementaria de seguridad de la información integral, misma que puede apreciar todos los niveles de una empresa.

La seguridad de la información, generalizada y considerada desde un marco global de seguridad deberá responder hacia un SGSI y el entorno cibernético, por lo que se operará sobre las políticas de seguridad de la empresa, alcance del SGSI, gestión de riesgos, tratamiento del riesgo, aplicabilidad y monitoreo, mientras que, a nivel del ciberespacio, también se consecutivamente se opera sobre la información, redes, aplicaciones, internet e infraestructura, proporcionando un modelo de seguridad integral.

Activos de la Seguridad de la Información

En base a los requisitos de la norma ISO 27001, la construcción de un SGSI correcto depende de la elaboración de un inventario de activos de información, de manera que, conocer con exactitud las posesiones de una empresa sea un factor claro. El inventario de activos es un modelo que deberá actualizarse permanentemente y a largo plazo, de manera que conllevará revisiones periódicas, además, se prestará a cambios continuos, mismos que deberán ser comunicados en todo momento. ISO/IEC 27032 propone una serie de controles y metodologías para salvaguardar los activos de información de la organización, tomando en cuenta para esto sus dos segmentos clave:

- Activos tangibles: Considera activos materiales que contienen información, sobre los cuales se establecerán medidas de protección definidas por la ISO/IEC 27031 y protocolos de ciberseguridad, además de medidas preventivas ante posibles riesgos físicos.
- Activos intangibles: Soportan la información dentro de activos materiales, y, a su vez, tienen la capacidad de inutilizar la información, a pesar de que el activo físico no haya sufrido algún tipo de daño, Siendo gestionados directamente por la ISO 27001.

La identificación total y parcial de los activos de información de una empresa resulta indispensable para la implementación de la propuesta metodológica para la gestión de la seguridad de la información y ciberseguridad. La capacidad de gestión de los riesgos a través de modelos de prevención, detección y respuesta deben considerar claramente los activos que podrían resultar afectados, siempre en base a sus niveles de prioridad y vulnerabilidad. La gestión de la seguridad de la información y ciberseguridad puede manejarse en base a los activos organizacionales dependiendo de los lineamientos, objetivos y políticas de la empresa.

Cláusulas de integración de ISO 27001 e ISO/IEC 27032

La propuesta metodológica integrada plantea ocho clausulas a considerar para su implementación e implantación en organizaciones determinadas. Las cláusulas de integración de ISO 27001 y Ciberseguridad son:

- CLÁUSULA 1: Contexto/Entendimiento de la organización
- CLÁUSULA 2: Liderazgo
- CLÁUSULA 3: Planificación y análisis de riesgos
- CLÁUSULA 4: Soporte
- CLÁUSULA 5: Operación y plan de acción
- CLÁUSULA 6: Evaluación de desempeño
- CLÁUSULA 7: Marco de corrección y mejora
- CLÁUSULA 8: Implementación iterativa

El conjunto de cláusulas de la propuesta metodológica integrada propone un modelo de implementación de un marco de seguridad destinado a la seguridad de la información. El correcto seguimiento de las ocho clausulas establecidas en la propuesta metodológica integrada pretende brindar a la organización un sistema completo de acción y rección adecuado ante riesgos de seguridad informática.

La propuesta metodológica se presenta como un sistema iterativo de mejora continua, es decir, tras aplicarse en una organización pretende fortalecer el sistema de seguridad de la información tras cada ataque potencial, considerando todos los riesgos posibles, asegurando vulnerabilidades.

La integración de ISO 27001 e ISO/IEC 27032 comparte un aspecto organizacional fundamental en base a la cultura de la empresa, basado en la educación y en la instauración de una cultura de seguridad integral y total.

CAPÍTULO V

5. Conclusiones y recomendaciones

5.1 Conclusiones

- La integración de las normas ISO 27001 e ISO/IEC 27032, enfocadas en la ciberseguridad y seguridad de la información, permitió realizar una propuesta metodológica para la gestión de la seguridad organizacional total, enfocada en la protección de la información y su medio de interacción, considerando un marco de aplicación integral para todos los niveles de la empresa, según los objetivos, políticas y lineamientos de esta.
- En la propuesta metodológica integral se consigue analizar las vulnerabilidades existentes en los sistemas de información para, a partir de ellos, gestionar la seguridad de estos de manera eficiente y adecuada, relacionando, en su totalidad, a la norma ISO 27001 focalizada en la gestión de la seguridad de la información, y gestión de ciberseguridad, según ISO/IEC 27032.
- Como conclusión, identificar las normas y protocolos que se ven inmersos en la gestión de la seguridad de la información y ciberseguridad es un aspecto clave en la integración de la gestión de la seguridad de la información y el entorno cibernético.
- La propuesta metodológica integrada consigue contrastar a la ciberseguridad según ISO/IEC 27032 con la gestión de la seguridad de la información en base a la norma ISO 20071 y demás protocolos estandarizados, de manera que la implementación de un marco de seguridad complejo es aplicable en todos los niveles de la organización.
- La gestión de la seguridad informática comprende una serie de herramientas, normas y metodologías que permiten a la organización gestionar riesgos de seguridad de manera general y parametrizada, considerando al SGSI como a los activos en los cuales se aloca, o permiten alocar, un sistema de gestión de la seguridad de la información.
- La integración de ISO 27001 e ISO/IEC 27032 comparte un modelo de educación organizacional, en el que se fomenta de manera obligatoria una cultura de seguridad en todos los niveles empresariales, siempre de acuerdo con los lineamientos y objetivos de la organización.

5.2 Recomendaciones

- Se recomienda que, previo al proceso de implementación de la propuesta metodológica integral, se consideren todas las cláusulas del modelo de dicha propuesta, considerando que, esta no es implementable en todo tipo de organizaciones, por lo tanto, la participación de la dirección y gerencia es crítica al momento de llevar a cabo el proceso de toma de decisiones para implementar un marco de seguridad adecuado.
- ISO 27001, focalizada en la gestión de la seguridad de la información en base a un SGSI correcto, es implementable en toda organización y además es totalmente auditable, sin embargo, ISO/IEC 27032 no es aplicable en toda empresa y no es auditable, por lo tanto, es recomendable analizar y comprender la estructura empresarial, al igual que sus objetivos y lineamientos, con la finalidad de determinar si la propuesta metodológica presentada es acoplable a la organización.
- Como recomendación, priorizar el entendimiento del contexto de la organización es fundamental. Considérese que, para implementar un SGSI correcto y efectivo, es necesario tener un panorama claro sobre la visión, enfoque, dirección, metas y objetivos de la empresa, el SGSI es clave para gestionar la seguridad de la información adecuadamente, consiguiendo así una capacidad de respuesta óptima ante riesgos potenciales.
- Para la gestión de la seguridad, es indispensable generar un ambiente de confianza con todos los miembros de la entidad, en todos sus niveles, es decir, clientes, empleados, proveedores, la dirección y gerencia; tómese en cuenta que, un ambiente de confianza es la consecuencia de una cultura organizacional con tendencia a la seguridad, compromiso y transparencia.
- Finalmente, al desarrollar una propuesta metodológica orientada a la seguridad de la información en las organizaciones, es de considerar que, en la Pontificia Universidad Católica del Ecuador, en la carrera de Ingeniería de Sistemas, deberían integrarse asignaturas específicamente focalizadas en el campo de administración y gerencia, donde puedan emplearse técnicas de liderazgo, gestión de sistemas complejos, asignación de roles y responsabilidades, además, de metodologías de análisis y control de la calidad total en los diferentes niveles organizacionales.

CAPÍTULO VI

6. Bibliografía

ANDREU, R. R. (1991). *Estrategia y Sistemas de Información.* Madrid: Mc Graw-Hill.

Arateco, L. C. (2015, 09 10). *Seguridad informática y seguridad de la información.* Obtenido de Universidad piloto de Colombia: http://repository.unipiloto.edu.co/handle/20.500.12277/2821

Blog de CEUPE. (2018, 07 26). *Sistema de Gestión de la Seguridad de la Información*. Obtenido de Ceupe.com: https://www.ceupe.com/blog/sistema-de-gestion-de-la-seguridad-de-la-informacion.html

Cámara Zaragoza. (2012, 02 23). *¿Qué es un sistema de información? — Cámara de Zaragoza*. Obtenido de Camarazaragoza.com: https://www.camarazaragoza.com/faq/que-es-un-sistema-de-informacion/

Ciar Global. (2020, 08 28). *Aproximación a los protocolos de ciberseguridad en el arbitraje*. Obtenido de Ciar Global: https://ciarglobal.com/aproximacion-a-los-protocolos-de-ciberseguridad-en-el-arbitraje-internacional/

Cisco. (2021, 8). *Anatomía de un ataque*. Obtenido de Cisco: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Cortés, M. (2017, 10 25). *¿Cómo medir la efectividad de la ciberseguridad?* Obtenido de CIO MX: https://cio.com.mx/medir-la-efectividad-la-ciberseguridad/

Editors ISOTools. (2019, 10 18). *Análisis y evaluación de riesgos de seguridad de la información: identificación de amenazas, consecuencias y criticidad*. Obtenido de Software ISO: https://www.isotools.org/2019/10/18/analisis-y-evaluacion-de-riesgos-de-seguridad-de-la-informacion-identificacion-de-amenazas-consecuencias-y-criticidad/

Garcia, A. (2016). *Directrices de Ciberseguridad ISO 27032*. Obtenido de UAGRM - Facultad de Ingeniería en Ciencias de la Computación y Telecomunicaciones: https://z0jde8nnyvm1b6dkizyjcq-on.drv.tw/Publico/www.A-Garcia.edu/Mod11-GITI-GCN/

Gonzales, A. (2017, 06 20). *Cómo garantizar la seguridad informática de una empresa*. Obtenido de Ayuda Ley Protección Datos: https://ayudaleyprotecciondatos.es/2017/06/20/seguridad-informatica-empresas/

Instituto nacional de Ciberseguridad. (2019). Protección de la información. *Protección de la información*, 33.

INTERNET SECURITY AUDITORS 2021. (2012). *Implementación de un Marco de Ciberseguridad ISO 27032 | Internet Security Auditors*. Obtenido de Isecauditors.com: https://www.isecauditors.com/consultoria-csf-iso-27032

Isecauditors. (2012). *mplementación de un Marco de Ciberseguridad ISO 27032 | Internet Security Auditors*. Obtenido de Isecauditors: https://www.isecauditors.com/consultoria-csf-iso-27032

ISO tools excellence. (2019, 02 08). *ISO 27001 - Software ISO 27001 de Sistemas de Gestión*. Obtenido de Software ISO: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISO27001. (2013). *ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online.* Obtenido de ISO 27001: https://normaiso27001.es/#iso27001

ISOwin. (2017, 06). *ISOwin: Los Activos de Información en la norma ISO 27001 2017*. Obtenido de Isowin.org: https://isowin.org/blog/activos-ISO-27001/

Izertis. (2018). *3 pasos imprescindibles para mejorar la ciberseguridad en tu empresa*. Obtenido de Izertis.com: https://www.izertis.com/es/-/blog/3-pasos-imprescindibles-para-mejorar-la-ciberseguridad-en-tu-empresa

Julian Russell. (2021, 09). *GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO 27001*. Obtenido de NQA. ORGANISMO DE CERTIFICACIÓN GLOBAL: https://www.nqa.com/es-mx/certification/standards/iso-27001

Kaspersky. (2021, 08 09). *¿Qué es la ciberseguridad?* Obtenido de latam.kaspersky.com: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

López, A. (2012). *Serie 27000*. Obtenido de Iso27000.es: https://www.iso27000.es/iso27000.html

Mesquita, R. (2019, 06). *Sistema de Información: definición, características y ejemplos*. Obtenido de Rock Content - ES: https://rockcontent.com/es/blog/que-es-un-sistema-de-informacion/

Sisteseg Consulting. (2018). *Implementación ciberseguridad ISO 27032.* Bogotá.

Toro, R. (2017, 02 23). *Activos de información ¿Cómo realizar un inventario?* Obtenido de PMG SSI - ISO 27001: https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

Trasobares, A. H. (2021). *Los sistemas de información: evolución y desarrollo*. Obtenido de Proyecto social: Revista de relaciones laborales: https://dialnet.unirioja.es/servlet/articulo?codigo=793097

Villa, P., Ladino, M., & López, A. (2011, 04). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia Et Technica*, 334-339. doi:https://www.redalyc.org/articulo.oa?id=84921327061