

**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN FORMULACIÓN Y EVALUACIÓN DE PROYECTOS**



**EJECUCIÓN E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA
SEGURIDAD DE LA INFORMACIÓN ISO 27001:2013 EN UN CENTRO DE
OPERACIONES DE SEGURIDAD EN EL MUNICIPIO DE GUATEMALA,
DEPARTAMENTO DE GUATEMALA, AÑO 2020.**



LICENCIADA KENNY DAMARIZ IZABEL BARILLAS RAXCACÓ

GUATEMALA, 2 DE OCTUBRE DE 2021

**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE ESTUDIOS DE POSTGRADO
MAESTRÍA EN FORMULACIÓN Y EVALUACIÓN DE PROYECTOS**



**EJECUCIÓN E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA
SEGURIDAD DE LA INFORMACIÓN ISO 27001:2013 EN UN CENTRO DE
OPERACIONES DE SEGURIDAD EN EL MUNICIPIO DE GUATEMALA,
DEPARTAMENTO DE GUATEMALA, AÑO 2020.**



Informe final del Trabajo Profesional de Graduación para la obtención del Grado de Maestro en Artes, con base en INSTRUCTIVO PARA ELABORAR EL TRABAJO PROFESIONAL DE GRADUACIÓN PARA OPTAR AL GRADO ACADÉMICO DE MAESTRO EN ARTES Aprobado por Junta Directiva de la Facultad de Ciencias Económicas, el 15 de octubre de 2015, según Numeral 7.8 Punto SÉPTIMO del Acta No. 26-2015 y ratificado por el Consejo Directivo del Sistema de Estudios de Postgrado de la Universidad de San Carlos de Guatemala, según Punto 4.2, subincisos 4.2.1 y 4.2.2 del Acta 14-2018 de fecha 14 de agosto de 2018.

AUTORA: LICENCIADA KENNY DAMARIZ IZABEL BARILLAS RAXCACÓ

GUATEMALA, 2 DE OCTUBRE DE 2021

**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
HONORABLE JUNTA DIRECTIVA**

Decano: Lic. Luis Antonio Suárez Roldán

Secretario: Lic. Carlos Roberto Cabrera Morales

Vocal I: Lic. Carlos Alberto Hernández Gálvez

Vocal II: Msc. Byron Giovanni Mejía Victorio

Vocal III: Vacante

Vocal IV: BR. CC. LL. Silvia María Oviedo Zacarías

Vocal V: P. C. Omar Oswaldo García Matzuy

**TERNA QUE PRACTICÓ LA EVALUACIÓN DEL TRABAJO PROFESIONAL DE
GRADUACIÓN**

Coordinador: MSc. Ricardo Alfredo Girón Solórzano

Evaluador: MSc. Hugo Romeo Arriaza Morales

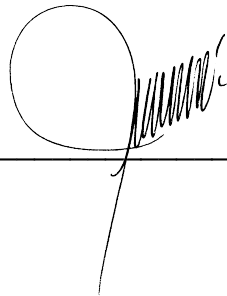
Evaluador: MSc. Dora Aracely Vivas Pérez

DECLARACIÓN JURADA DE ORIGINALIDAD

YO: **Kenny Damariz Izabel Barillas Raxcacó**, con número de carné: **201012682**.

Declaro que como autor, soy el único responsable de la originalidad, validez científica de las doctrinas y opiniones expresadas en el presente Trabajo Profesional de Graduación, de acuerdo al artículo 17 del Instructivo para Elaborar el Trabajo Profesional de Graduación para Optar al Grado Académico de Maestro en Artes.

Autor: _____

A handwritten signature in black ink, consisting of a large, stylized 'K' followed by a series of vertical, wavy lines that form the rest of the name. The signature is written over a horizontal line.

**ACTA No. MFEP-034-2021**

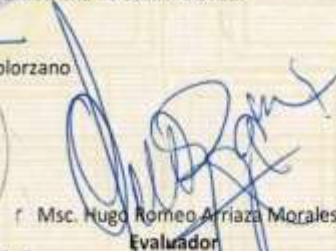
De acuerdo al Estado de Emergencia Nacional decretado por el Gobierno de la República de Guatemala y a las resoluciones del Consejo Superior Universitario, que obligaron a la suspensión de actividades académicas y administrativas presenciales en el Campus Central de la Universidad de San Carlos de Guatemala, ante tal situación, la Escuela de Estudios de Postgrado de la Facultad de Ciencias Económicas, debió incorporar tecnología virtual para atender la demanda de necesidades del sector estudiantil, por lo que en esta oportunidad nos reunimos de forma virtual los infrascritos integrantes de la Terna Evaluadora, el día sábado 2 de octubre de 2021, a las 14:00 horas, para evaluar la presentación del TRABAJO PROFESIONAL DE GRADUACIÓN del Licenciado **Kenny Damariz Izabel Barillas Raxcacó**, carné No. 201012682, estudiante de la Maestría en Formulación y Evaluación de Proyectos de la sección **B** de la Escuela de Estudios de Postgrado, como requisito para optar al grado de **Maestro en Artes** en Formulación y Evaluación de Proyectos. La presentación se realizó de acuerdo con el Instructivo, aprobado por la Junta Directiva de la Facultad de Ciencias Económicas, el 15 de octubre de 2015, según Numeral 7.8 Punto SÉPTIMO del Acta No. 26-2015 y ratificado por el Consejo Directivo del Sistema de Estudios de Postgrado -SEP- de la Universidad de San Carlos de Guatemala, según Punto 4.2, subincisos 4.2.1 y 4.2.2 del Acta 14-2018 de fecha 14 de agosto de 2018.

Cada examinador evaluó, de manera oral los elementos técnico-formales y de contenido profesional del informe final presentado por el sustentante, denominado **"EJECUCIÓN E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ISO 27001:2013 EN UN CENTRO DE OPERACIONES DE SEGURIDAD EN EL MUNICIPIO DE GUATEMALA, DEPARTAMENTO DE GUATEMALA."**, dejando constancia de lo actuado en las hojas de factores de evaluación proporcionadas por la Escuela. La presentación fue calificada con una nota promedio de 70 puntos, obtenida de los punteos asignados por cada integrante de la Terna Evaluadora. La Terna hace las siguientes recomendaciones: Que, de acuerdo a las observaciones realizadas por cada uno de los miembros de la Terna Evaluadora, en los documentos revisados y entregados al estudiante; éste debe de incorporarlos al documento final de Trabajo Profesional de Graduación. Para el efecto dispone de cinco (5) días hábiles de acuerdo con el Instructivo para Elaborar Trabajo Profesional de Graduación para optar a la Maestría en Artes.

En fe de lo cual firmamos la presente acta en la Ciudad de Guatemala el 2 de octubre 2021.


Msc. Dora Aracely Vivas Perez
Evaluador


Msc. Ricardo Alfredo Girón Solorzano
Coordinador


Msc. Hugo Romeo Arriaza Morales
Evaluador


Lic. Kenny Damariz Izabel Barillas Raxcacó
Postulante



UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE ESTUDIOS DE POSTGRADO
MAESTRIA EN ARTES EN FORMULACION Y EVALUACION DE PROYECTOS

ADENDUM al ACTA No. MFEP-034-2021

El infrascrito Examinador CERTIFICA que el estudiante **Kenny Damariz Izabel Barillas Raxcacó**, carné No. 201012682 incorporó los cambios y enmiendas sugeridas por cada miembro de la terna evaluadora.

Guatemala, 07 de octubre de 2021.



(f)

Ricardo Alfredo Girón Solorzano
Coordinador

AGRADECIMIENTO

A DIOS:

A ti que me has dado la sabiduría necesaria para llegar a cumplir este sueño en mi vida, ese amor único que me da paz y tranquilidad. Eres quien siempre guía y bendice mi camino, agradezco por cada persona, detalle y situación que has puesto en mi camino.

A MI MADRE:

Por darme la vida, su apoyo y por ser la guía en cada momento de mi vida, y lucho por dejarme la mejor herencia que es el estudio y por haberme enseñado los valores más importantes y doy gracias por tenerla conmigo.

A MI FAMILIA:

Por la paciencia y apoyo que me han brindado, esas palabras de aliento que no me dejaron caer, la distancia no ha sido impedimento para sentir ese abrazo tan especial de mi familia. A mis sobrinos por cada ocurrencia, han hecho mis días más divertidos y felices.

A MIS AMIGOS:

Que se convirtieron en mi segunda familia, muchas gracias por compartir sus conocimientos, experiencias, alegrías, frustraciones y esas inolvidables anécdotas.

Gracias por su amistad y apoyo, gracias por ser parte de este éxito.

A LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA:

Por todos los conocimientos adquiridos y la por la oportunidad de formar parte de tan importante casa de estudios y permitir mi formación como profesional.

EN ESPECIAL:

A mi hijo, Austin Alvarado por esa paciencia y amor incondicional que llena mi vida de felicidad.

CONTENIDO

Página

RESUMEN.....	i
INTRODUCCIÓN	v
1. ANTECEDENTES.....	1
1.1. Antecedentes de un centro de operaciones de seguridad	1
1.2. Antecedentes de los efectos de la implementación del sistema de gestión de la seguridad de la información ISO 27001:2013.....	2
2. MARCO TEÓRICO	6
2.1. Proyecto	6
2.1.1. Necesidad de los proyectos.....	7
2.1.2. Importancia de los proyectos	7
2.2. Tipos de proyectos	8
2.3. Etapas del proyecto	9
2.4. Ciclo del proyecto.....	10
2.5. Evaluación de proyectos	10
2.5.1. Tipos de evaluación	11
2.6. Evaluación expost	12
2.6.1. Objetivos de la evaluación expost	12
2.6.2. Tipos de evaluación expost	13
2.7. Criterios de evaluación	14
2.8. Línea base del proyecto.....	15

2.8.1. Instrumentos a implementar en la línea base del proyecto	15
2.9. Seguridad informática	16
2.9.1. Objetivos de la seguridad informática	16
2.10. Seguridad de la información	17
2.10.1. Bases de la seguridad de la información	17
2.11. Activos informáticos	18
2.12. Incidentes de seguridad	19
2.13. Ciberseguridad	19
2.14. ISO – Organización internacional para la normalización.....	19
2.14.1. Normas ISO	20
2.14.2. ISO 27001:2013	20
2.14.3. Estructura de la norma ISO 27001:2013	21
2.14.4. Sistema de gestión de la seguridad de la información (SGSI)	22
2.14.4.1. Objetivos del sistema de gestión de seguridad de la información ...	23
2.14.4.2. Alcance del sistema de gestión	23
2.14.4.3. Política del sistema de gestión	24
2.14.4.4. Controles en el sistema de gestión	24
2.14.4.5. Registros en el sistema de gestión	25
2.15. Ciclo PHVA.....	25
2.16. Centro de operaciones de seguridad (SOC).....	27
2.16.1. Actividades del centro de operaciones de seguridad (SOC)	27

2.16.2. Organización del centro de operaciones de seguridad (SOC)	28
3. METODOLOGÍA.....	30
3.1. Definición del problema	30
3.2. Objetivos.....	31
3.2.1. Objetivo general	31
3.2.2. Objetivos específicos	31
3.3. Diseño de la investigación	32
3.3.1. Unidad de análisis.....	32
3.4. Periodo histórico.....	33
3.5. Ámbito geográfico	33
3.6. Universo y muestra	33
3.7. Técnicas e instrumentos aplicados	33
3.7.1. Técnicas e instrumentos documentales	34
3.7.2. Técnicas e instrumentos de investigación de campo	34
3.8. Resumen del procedimiento aplicado	35
4. DISCUSIÓN DE RESULTADOS.....	37
4.1. Validación del cumplimiento de la Norma ISO 27001:2013 en el centro de operaciones de seguridad (SOC)	37
4.1.1. Objetivo del centro de operaciones de seguridad	42
4.2. Análisis de riesgos den los activos de información en el sistema de gestión de la seguridad de la información (SGSI), implementados en el centro de operaciones de seguridad.....	43
4.2.1. Evaluación de riesgos	44

4.2.2. Impacto y probabilidad	47
4.2.3. Criterios para la aceptación de riesgos	48
4.2.4. Plan tratamiento de riesgos	50
4.3. Controles definidos sobre los activos de información del centro de operaciones de seguridad (SOC)	51
4.4. Efecto en la demanda de servicios del centro de operaciones de seguridad a partir de la implementación de la norma ISO 27001:2013 en el año 2020	53
CONCLUSIONES	57
RECOMENDACIONES	58
FUENTES.....	59
ANEXOS.....	64
ÍNDICE DE ACRÓNIMOS	69
ÍNDICE DE FIGURAS	70
ÍNDICE DE CUADROS	71
ÍNDICE DE GRÁFICAS	72

RESUMEN

El presente trabajo de graduación está enfocado en un centro de operaciones de seguridad, cuya actividad principal es el monitoreo en tiempo real de los sistemas informáticos de los clientes, para la prevención de incidentes de seguridad y la detección de cualquier acción sospechosa. La unidad de estudio ha logrado posicionarse muy bien en el mercado, es por eso que debe ser eficiente en los controles para el resguardo de la información sensible de los clientes.

La problemática del tema de investigación surge debido a que la actualidad cada día son más las amenazas y variantes de ataques que pueden poner en riesgo la información y el buen funcionamiento en las organizaciones. No obstante, cabe mencionar que para dar solución al problema es de gran importancia realizar una evaluación de corto plazo de los efectos de la implementación del sistema de gestión de la seguridad de la información basada en la norma ISO 27001, ya que esto ayuda a la disminución de la fuga de información que es provocada por la inexistencia de una gestión eficiente del resguardo de la información. Una mala gestión provoca consecuencias operativas, financieras y legales que pueden ser graves afectando el giro del negocio.

Los activos de información son todos aquellos recursos que utiliza un sistema de gestión de la seguridad de la información, para que la organización funcione y consiga los objetivos propuestos por la dirección. Por lo que el centro de operaciones de seguridad (SOC) debe ser eficiente en la gestión de los controles implementados para el resguardo de la información de los clientes.

Derivado de la problemática expuesta en la investigación, se plantean las siguientes interrogantes: ¿Qué procedimientos pueden aplicarse para verificar que los alcances, objetivos, políticas, registros y procedimientos del sistema de gestión de seguridad de la información (SGSI) están diseñados y aplicados correctamente al tipo de organización?, ¿Cómo se pueden identificar los riesgos sobre los activos de información del centro de operaciones de seguridad (SOC)?, ¿Se tiene la información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información? ¿Cuál sería el efecto en la demanda de servicios de ciberseguridad que ha tenido la implementación de la norma ISO 27001 en el centro de operaciones de seguridad (SOC)?

Para dar respuesta a las interrogantes expuestas en el párrafo anterior, se definió como objetivo general, realizar una evaluación expost a corto plazo de la implementación del sistema de gestión de la seguridad de la información ISO 27001:2013 en un centro de operaciones de seguridad, para validar y gestionar los controles pertinentes y así asegurar la confidencialidad, integridad y disponibilidad de los activos de información.

Para llegar a cumplir el objetivo general, se plantean cuatro objetivos específicos los cuales surgieron de las interrogantes que permitieron establecer los pasos a seguir, determinando el hilo conductor de la investigación, los cuales se detallan a continuación: validación del cumplimiento de la norma ISO 27001:2013 en el centro de operaciones de seguridad (SOC); análisis de riesgos en los activos de información en el sistema de gestión de la seguridad de la información (SGSI) implementados en el centro de operaciones de seguridad; evaluar los controles definidos sobre los activos de información, puestos en marcha por la implementación de la norma ISO 27001 en el centro de operaciones de seguridad (SOC); analizar el efecto en la demanda de servicios del centro de operaciones de seguridad a partir de la implementación de la norma ISO 27001:2013 en el año 2020.

La metodología utilizada para el desarrollo de la investigación tiene un enfoque mixto con predominancia cuantitativa, esto porque se enfocó en la recolección de datos por medio de instrumentos para facilitar el proceso de recolección, cuyo fin es clasificarlos e interpretarlos. La investigación tendrá un alcance de tipo descriptivo-explicativo porque detalla las características y aspectos importantes del problema, con el fin de analizar la forma en que se manifiesta el problema de la unidad de análisis. El diseño de la investigación será no experimental debido a que se observan situaciones existentes, con el objetivo de analizar su evolución.

Para efectuar la investigación se utilizaron las diferentes fases de investigación, dentro de las cuales se pueden mencionar la fase indagatoria, para la cual se realizaron revisiones de las fuentes bibliográficas, así como técnicas e instrumentos documentales como lo son: la revisión bibliográfica a través de la lectura analítica, las citas bibliográficas y el subrayado con el fin de extraer lo más importante de cada fuente. Para la fase demostrativa se utilizó el análisis de documentos como técnica de investigación de campo, la cual servirá para la validación del alcance, objetivos,

políticas, registros, procedimientos; validación de los riesgos tras la implementación de la norma ISO 27001 en el centro de operaciones de seguridad.

Derivado de las técnicas y métodos de investigación, se lleva a cabo la presentación del trabajo de graduación, en el cual se muestran los resultados de la investigación y las principales conclusiones obtenidas. Se inicio con la recopilación de la información utilizando la entrevista no estructurada, como instrumento de guía, la cual fue realizada al especialista de seguridad de la unidad de estudio.

Como parte del planteamiento de la investigación a través de los objetivos específicos planteados, se buscó conocer por medio de la evaluación expost a corto plazo realizada al proyecto con la ayuda del análisis de documentos, validar que la implementación realizada, se encontrara estructurada y alineada a los requerimientos que solicita la norma y al giro del negocio.

Conforme al análisis de documentos que se llevó a cabo, se determinó que algunos documentos que respaldan la implementación del sistema de gestión de la seguridad de la información ISO 27001 de la unidad objeto de estudio, no contaban con las revisiones y actualizaciones periódicas correspondientes en los documentos de respaldo.

Se aplicó el análisis de documentos para la validación de la metodología de riesgos utilizados en el centro de operaciones, donde se determinó que la organización evalúa las consecuencias y probabilidades de cada riesgo, así como la decisión a tomar para cada uno de ellos por el gerente de área y el equipo de seguridad.

Por último el resultado más importante en esta evaluación realizada se percibe en las nuevas oportunidades de negocio que el centro de operaciones de seguridad (SOC) ha generado tras la implementación de este sistema de gestión para el resguardo de la información. Comparando el año 2019 que es cuando el área no contaba con la implementación de la norma, cerró el periodo de operación con 121 clientes. Tras la implementación de la norma ISO 27001 hubo un incremento del 62.81% que corresponde a 75 clientes nuevos que optaron por contratar los servicios del centro de operaciones de seguridad, por contar con una certificación que respalde los controles para el resguardo de los activos de información, cerrando ese año con 197 clientes.

Con la evaluación a corto plazo realizada a la unidad de estudio, se busca poner en marcha un plan de seguimiento, monitoreo y evaluación ya que es una herramienta fundamental para el sistema de gestión de la seguridad de la información en el centro de operaciones de seguridad. Con el fin de identificar las fortalezas y debilidades tras la implementación de la norma ISO 27001 y medir el avance, desempeño y los efectos del proyecto. Así mismo proporcionar oportunidades de mejora para buscar la eficiencia en los procesos, registros, controles y así asegurar la confidencialidad, integridad y disponibilidad de los activos de información.

INTRODUCCIÓN

En las organizaciones se maneja una gran cantidad de información, la misma es de gran vitalidad para el giro del negocio de cada una de ellas. Así mismo la tecnología está a la cabeza de la mayoría de operaciones diarias, es por ello que para garantizar la tranquilidad de las personas y organizaciones la seguridad de la información se ha convertido en algo indispensable.

El centro de operaciones de seguridad (SOC) por sus siglas en inglés, es parte de una organización de telecomunicaciones; y tiene como fin el monitoreo y análisis de las actividades irregulares que puedan dar origen a un incidente o compromiso de seguridad.

La implementación de la norma ISO 27001 en el centro de operaciones de seguridad, define buenas prácticas asociadas a la seguridad de la información. El fin primordial de esta norma es la protección y gestión de la información, ya que la misma como se mencionó anteriormente es uno de los activos más importantes para las organizaciones.

Por lo que la problemática identificada corresponde a que en la actualidad existen distintas amenazas y variantes de ataques que ponen en riesgo la información y el buen funcionamiento en la organización. No obstante realizar una implementación de un sistema de gestión de la seguridad de la información, disminuye los incidentes de seguridad que puedan originar consecuencias operativas, financieras y legales graves que afecten el negocio.

El trabajo profesional de graduación se encuentra integrado por cuatro capítulos. En el capítulo uno se desarrollan los antecedentes de la unidad de análisis, correspondientes a una empresa de telecomunicaciones con más de 32 años en el mercado, integrada aproximadamente por 5,000 empleados. La misma adquirió un centro de operaciones de seguridad (SOC) que inicio a operar en septiembre del año 2018, donde su actividad primordial es el monitoreo proactivo, para detectar incidentes de ciberseguridad y así brindar respuesta inmediata. El mayor segmento de mercado del centro de operaciones de seguridad (SOC) son las pequeñas, medianas y grandes empresas en el país.

En el capítulo dos se encuentra el marco teórico que es una base para la comprensión de conceptos relacionados con la investigación, brindando un fundamento teórico al tema abordado, dentro de los temas más importantes se pueden mencionar la definición y objetivos de los proyectos, los tipos de evaluación, la importancia del desarrollo de proyectos, las etapas y ciclos de proyectos, así como los tipos de evaluación que se aplican a los mismos. Dentro del marco también se abordaron temas relacionados a la seguridad de la información, sus objetivos, los pilares de la información, los objetivos de la seguridad informática en las organizaciones; así mismo información sobre la norma ISO 27001:2013, los objetivos de la norma en las empresas, y la clasificación de los activos de la información para el control pertinente en el centro de operaciones de seguridad.

En el capítulo tres se identifica la problemática encontrada en la unidad de análisis, la cual corresponde a que actualmente cada día son más las amenazas y variantes de ataques que pueden poner en riesgo la información y el buen funcionamiento en la organización. Sin embargo realizar una implementación de un sistema de gestión de seguridad de la información en un centro de operaciones de seguridad, disminuye los incidentes de seguridad que puedan originar consecuencias operativas, financieras, y legales graves que pueden afectar el negocio. Por esta razón se presenta el objetivo general de la investigación: Realizar una evaluación expost a corto plazo de la implementación del sistema de gestión de seguridad de la información ISO 27001:2013 en un centro de operaciones de seguridad, para validar y gestionar los controles pertinentes y así asegurar la confidencialidad, integridad y disponibilidad de los activos de información.

Esta se llevó a cabo por medio de los siguientes objetivos: validación del cumplimiento de la norma ISO 27001:2013 en el centro de operaciones de seguridad (SOC); análisis de riesgos en los activos de información en el sistema de gestión de la seguridad de la información (SGSI); evaluar los controles definidos sobre los activos de información, puestos en marcha por la implementación de la norma ISO 27001 en el centro de operaciones de seguridad (SOC); analizar el efecto en la demanda de servicios del centro de operaciones de seguridad a partir de la implementación de la norma ISO 27001:2013 en el año 2020.

La investigación se realizó bajo un enfoque mixto con predominancia cuantitativa, esto porque hace énfasis en la recolección de datos con instrumentos que faciliten la recopilación de estos , con el fin de clasificarlos e interpretarlos. La investigación es de tipo aplicada, la misma tienen un alcance de tipo descriptivo-explicativo, con un diseño no experimental.

Para la investigación, se realizaron consultas en libros, tesis, revistas, ensayos, periódicos, la norma ISO 27001; por lo que se aplicó la técnica e instrumentos documentales como la revisión de bibliografías, a través de la lectura analítica, el subrayado y las citas bibliográficas. Así mismo se aplicó la técnica de investigación de campo y el análisis de documentos.

En el capítulo cuatro se expondrán las discusiones y resultados obtenidos en la investigación, donde se revisó la documentación relacionada con el cumplimiento de la norma ISO 27001, así como la verificación de riesgos y controles implementados para el resguardo de la información; y el efecto de la implementación de la norma ISO 27001 en las ventas de servicios de ciberseguridad. El presente capítulo se estructuró con un orden alineado a los objetivos específicos planteados, por lo que se analizará y responderá a cada uno de los objetivos.

Con el fin de desarrollar los objetivos específicos se procede a dar respuesta al objetivo número uno, por lo que se procedió a realizar las evaluaciones documentales correspondientes que respaldan el alcance, objetivos, políticas y procedimientos del centro de operaciones de seguridad, verificando que los mismos estuvieran alineados a lo que indica la norma ISO 27001.

Para dar respuesta al objetivo específico número dos, se procedió a realizar la verificación de los riesgos que la unidad de análisis estableció de acuerdo a clasificación de los activos de información para la selección adecuada de los controles. Así como la metodología apropiada para la clasificación de riesgos, impactos, y probabilidades relacionados con base a la norma ISO 27001.

Con el objetivo número tres se procedió a realizar la verificación de los controles establecidos en el centro de operaciones de seguridad, con la guía del Anexo A de la norma ISO 27001; los cuales son aplicados de acuerdo al giro del negocio de la

organización y a la toma de decisiones del equipo de seguridad. Así mismo un detalle de los controles más relevantes en el centro de operaciones de seguridad.

Por último se atendió el objetivo número cuatro, en el cual se validó el efecto positivo que ha tenido la implementación de la norma ISO 27001:2013 en la demanda de servicios de ciberseguridad, la misma contribuyó a obtener nuevas oportunidades de negocio e incrementar un 62.81% en la contratación de servicios de ciberseguridad por contar con una certificación que respalda al centro de operaciones de seguridad (SOC) con el resguardo de la información de los clientes, y asegurar la confianza y credibilidad de sus operaciones.

Los resultados alcanzados indican que, a pesar de realizar la implementación del sistema de gestión de la seguridad de la información en base a la norma ISO 27001 en el centro de operaciones de seguridad, existen algunas deficiencias en algunos controles y registros. Por lo que es necesario implementar un plan de seguimiento, monitoreo y evaluación ya que es una herramienta fundamental para el sistema de gestión de la seguridad de la información implementado en el SOC, con el fin de medir el avance, desempeño y mejoras así como el logro de las metas y objetivos del proyecto.

1. ANTECEDENTES

En este capítulo se presentan los antecedentes que constituyen el marco histórico que permite la comprensión del tema a desarrollar. Se expone el marco referencial teórico y empírico de la investigación relacionada con la evaluación de corto plazo de los efectos de la implementación del sistema de gestión de la seguridad de la información ISO 27001:2013 en un centro de operaciones de seguridad ubicado en el Municipio de Guatemala, Departamento de Guatemala.

1.1. Antecedentes de un centro de operaciones de seguridad

En el año 1989 se fundó una entidad de telecomunicaciones con el objetivo de ofrecer digitalización para conectar a las personas, mejorar sus vidas y ofrecer servicios de comunicación integral a la población. A partir del año de 1992 expandió su cobertura de servicios, implementando agencias, para la atención de sus clientes en cada uno de los departamentos de Guatemala.

La organización ha logrado su objetivo de posicionarse a nivel nacional por más de 32 años como la empresa líder en telecomunicaciones y servicios digitales brindando a Guatemala la mejor tecnología y experiencia, con más 8 millones de usuarios. Para el año 2020 la organización cuenta con una planilla alrededor de 5,000 empleados, quienes por medio de su excelente trabajo brindan el soporte y la ayuda necesaria a los clientes con el producto que más se adapte a sus necesidades.

Las características que diferencian a sus empleados de otras organizaciones; es la calidad como ser humano, y su individualidad en la atención, que conectan personas y mejoran sus vidas facilitando a todos avanzar y disfrutar la vida.

La estructura organizacional de esta empresa es híbrida, esto quiere decir que la organización se encuentra estructurada por unidades de negocio que están orientadas a los tipos de productos que ofrecen en el mercado objetivo.

La organización cuenta con una sólida visión, objetivos, así como una planificación estratégica, por lo que, a través de su ejecución alcanza los objetivos definidos año con año, así como las metas de crecimiento en las ventas. Viven con gran pasión los valores organizacionales que hacen a la empresa un gran lugar para trabajar y así contribuir a mejorar la sociedad.

1.2. Antecedentes de los efectos de la implementación del sistema de gestión de la seguridad de la información ISO 27001:2013

La unidad objeto de análisis fue adquirida en la organización en el mes de septiembre del 2018. El centro de operaciones de seguridad (Security Operation Center, por sus siglas en inglés) fue ubicado en un lugar estratégico para la continuidad del negocio, con ello se daba a conocer el principal objetivo que era proteger y resguardar la infraestructura e información de las empresas a nivel nacional.

El centro de operaciones de seguridad es una unidad que está conformada por especialistas en ciberseguridad que monitorean en tiempo real todas las actividades de los sistemas informáticos de los clientes, con el fin de prever incidentes de seguridad. La unidad se especializa en proteger y resguardar la información de las organizaciones de los posibles incidentes que se presenten. Los mismos deben ser identificados, analizados e investigados para informar correctamente a los clientes.

El análisis del trabajo tiene un enfoque sobre los efectos de la implementación de un sistema de gestión de la seguridad de la información con base a la norma ISO 27001:2013, es decir un criterio sistemático en la implementación, ejecución, y monitoreo para mantener la seguridad de la información en una organización, estableciendo buenas prácticas que permitan proteger la información sensible o de valor.

En la actualidad los centros de operaciones de seguridad (SOC) han tomado importancia, porque son los que se encargan de garantizar la seguridad de los datos de los clientes.

“ISO / IEC 27001:2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO/IEC 27001:2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.”(Organización Internacional de Estandarización [ISO] 2013 párrafo 1).

La familia de normas 27000 nacen en 1995 bajo el estándar de BS 7799 emitidas por el departamento de Comercio e Industria (DTI) del Reino Unido. El sistema de gestión de la seguridad de la información ISO 27001 fue publicada en octubre de 2005 por la Organización Internacional de Normalización (ISO) y por la Comisión Electrónica Internacional (IEC), esta norma es considerada como un estándar internacional que permite a las empresas a que puedan evaluar el riesgo y así aplicar los controles necesarios para mitigar o eliminar los riesgos.

En el transcurso de los años la norma ha tenido nuevas versiones, anteriormente se utilizaba la ISO 27001:2005 la cual fue sustituida por la ISO 27001:2013, esta nueva versión proporciona una mayor flexibilidad en cuanto a la metodología de trabajo, la mejora continua así como el análisis y evaluación de los riesgos.

Es de gran importancia mencionar que los proyectos nacen a raíz de una necesidad, de esta surgen ideas para poder solventar los problemas de las personas y organizaciones.

En otras palabras los proyectos han existido desde la antigüedad, lo cual ha permitido que personas sean capaces de planificar, liderar e incluso gestionar los insumos, la mano de obra ,dentro de un espacio de tiempo determinado.

Según Baca (2013) “Un proyecto es la búsqueda de una solución inteligente al planteamiento de un problema, la cual tiende a resolver una necesidad humana.”(p. 2)

Derivado de esto podemos decir; que lo que se necesita es satisfacer la necesidad; en los proyectos existen fases para poder desarrollar los mismos, entre ellas se encuentran la fase de inicio, planificación, ejecución, seguimiento y el cierre del proyecto.

La ejecución de un proyecto se refiere a todas las tareas planificadas que se deben realizar para poder obtener los objetivos propuestos; en pocas palabras es poner en marcha todo lo que se ha escrito en papel en la fase de planificación. Según los autores Rivera y Hernández (2010) “El proceso de ejecución, coordinado por el administrador, consiste en obtener los productos entregables del proyecto, teniendo en cuenta personas y recursos y siguiendo el alcance definido.” (p.267)

Las implementaciones de proyectos van de la mano de la fase de ejecución, pues lo primordial es poner en desarrollo las tareas, procedimientos, que beneficiaran a las partes interesada del proyecto en marcha y con ello alcanzar los objetivos para las organizaciones.

No solo es importante poner en marcha los proyectos, si no también evaluarlos en el transcurso que estos avanzan, estos ayudan a identificar, cuantificar y valorar los costos y beneficios con el fin de encontrar mejoras que ayuden a las siguientes fases a ponerse en marcha.

Con el pasar de los años las nuevas tecnologías se van adaptando a cualquier ámbito de la industria en Guatemala, estas deben contar con un seguimiento adecuado para el correcto funcionamiento de sus sistemas, así como el resguardo de la información, ya que todas operan o centran gran parte de sus actividades a través de internet. Hoy en día nos queda claro que el manejo de la información es algo de suma importancia, y el mismo ya es catalogado como un activo para cualquier organización.

Con respecto al tema sujeto de estudio, se realizó investigación en los tesauros de distintas universidades incluyendo la Universidad de San Carlos de Guatemala, a continuación se mencionan algunas de las tesis a nivel de maestría que pueden contribuir al entendimiento de la unidad de análisis:

Cuadro 1
Tesis relacionadas con la investigación

No.	Tesis	Fecha	Abordaje	Aporte
1	Análisis de riesgos y políticas de seguridad de información de la oficina de tecnologías de información (OTI) una puno 2018	Octubre 2018	El documento adjunto aborda el tema sobre la seguridad de la información respecto a los activos.	Al implementar los análisis del riesgo estos ayudan a mitigar las amenazas y evitar que sea vulnerable la seguridad de la información.
2	Sistema de gestión de riesgos de activos informáticos en las medianas empresas ferreteras de la ciudad de Guatemala,	Noviembre 2017	El riesgo en los activos informáticos utilizando el método RISK IT, permite integrar las gestiones del riesgo a la toma de decisiones, así como la utilización de una matriz	La documentación necesaria para el seguimiento y verificación correcta de las actividades de gestión de riesgos, realización de matrices de riesgo así como su ponderación.

	aplicando el marco de trabajo Riskit.		para la clasificación de los mismos.	
3	Proyecto de emprendimiento empresarial en el diseño de soluciones a riesgos de seguridad de la información, basado en la teoría general de disuasión.	Mayo 2016	El diseño desarrollado contempla los siguientes aspectos: el uso de medios disuasivos, diagnósticos periódicos, los lineamientos para generar una política de seguridad de la información, capacitaciones al personal, el uso de la seguridad informática y gestionar la seguridad de la información de forma permanente.	Utilización de la teoría de disuasión general puede ser utilizada no sólo para la identificación y solución de riesgos en seguridad de la información, que puede ser aplicada a otros temas, donde se requieran métodos disuasivos para llevar el control de determinado evento, proceso o problema.

Fuente: elaboración propia, con información de Machicao (2019), Meza (2017), Ruano (2016).

Derivado del análisis de las investigaciones realizadas previamente al tema de investigación, evaluación a corto plazo de los efectos de la implementación del sistema de gestión de la seguridad de la información ISO 27001:2013 en un centro de operaciones de seguridad (SOC) ubicado en el Municipio de Guatemala, Departamento de Guatemala, se proporciona información relevante para la interpretación del tema, así como herramientas necesarias para el análisis de riesgos de los activos de la información.

2. MARCO TEÓRICO

El marco teórico contiene el análisis de las teorías, así como los enfoques conceptuales que son utilizados para fundamentar la investigación, con el objetivo de realizar una evaluación expost a corto plazo de la implementación del sistema de gestión de la seguridad de la información ISO 27001:2013 en un centro de operaciones de seguridad ubicada en el municipio de Guatemala, Departamento de Guatemala.

2.1. Proyecto

Los proyectos ayudan a resolver una necesidad sobre un bien o servicio identificado para la población objeto de estudio, para comprender el tema se presentan conceptos de valor.

Un proyecto es una búsqueda a una solución inteligente al planteamiento de un problema, la cual tiende a resolver una necesidad humana. En este sentido puede haber diferentes ideas, inversiones de monto distinto, tecnología y metodología con diverso enfoque, pero todas ellas destinadas a satisfacer la necesidad del ser humano en todas sus facetas, como pueden ser: educación, alimentación, salud, ambiente, cultura, etcétera. (Baca, 2013, p. 2)

De acuerdo con la guía del PMBOOK (2013):

Un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único. La naturaleza temporal de los proyectos implica que un proyecto tiene un principio y un final definidos. El final se alcanza cuando se logran los objetivos del proyecto, cuando se termina el proyecto porque sus objetivos no se cumplirán o no pueden ser cumplidos, o cuando ya no existe la necesidad que dio origen al proyecto. (p. 3)

Los resultados alcanzados en los proyectos pueden ser tangibles o intangibles de acuerdo al producto, servicio o el resultado que se pretende alcanzar y las necesidades que se pretender cubrir.

2.1.1. Necesidad de los proyectos

Las necesidades siempre existirán en la población y estas deben ser cubiertas, siempre y cuando se tenga una justificación y una utilidad inteligente para producir ese artículo o servicio que esté al alcance de la población.

Por lo tanto, siempre que exista una necesidad humana de un bien o un servicio habrá necesidad de invertir, hacerlo es la única forma de producir dicho bien o servicio. Es claro que las inversiones no se hacen solo porque alguien desea producir determinado artículo o piensa que al producirlo ganará dinero. En la actualidad una inversión inteligente requiere una base que la justifique. Dicha base es precisamente un proyecto estructurado y evaluado que indique la pauta a seguir. De ahí se deriva la necesidad de elaborar los proyectos. (Baca, 2013, p.2)

De lo anterior se puede concluir que para realizar un proyecto no solo debemos tomar las ideas del por qué se originaron, sino también tomar en cuenta todas las necesidades que se pretenden satisfacer, así como el tiempo en particular para que este sea exitoso. Lo ideal en los proyectos es que los mismo demoren el tiempo estipulado para el logro de los objetivos.

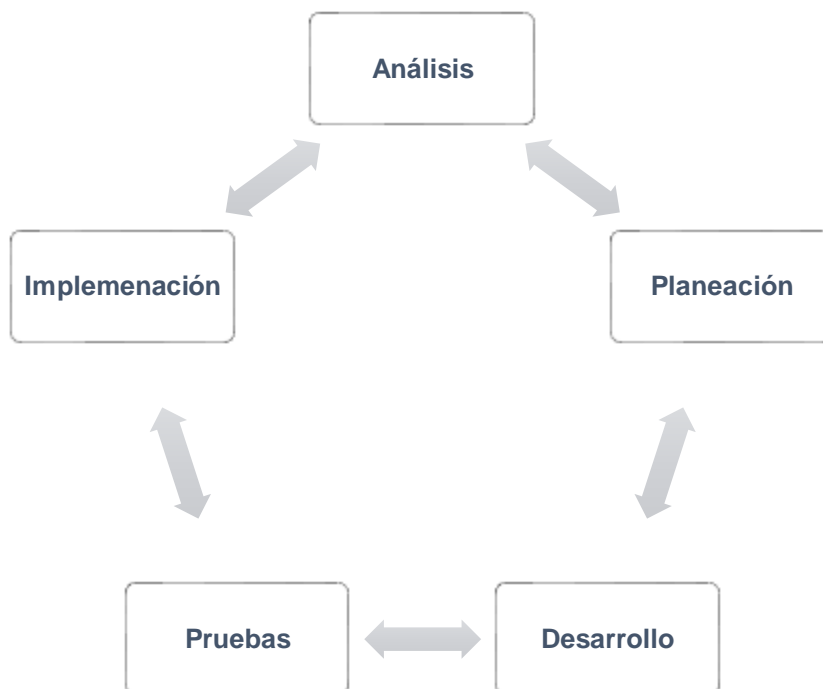
2.1.2. Importancia de los proyectos

Al crear proyectos es importante tener en cuenta cada una de las decisiones y estudios previos, pues como se menciona anteriormente el fin primordial es cubrir las necesidades o problemas identificados.

Dada la creciente importancia de gestionar proyectos complejos, es inquietante ver el gran número de proyectos que no logran satisfacer sus objetivos básicos. Este es uno de los motivos principales por el cual se debe plantear una planificación sobre la gestión de los proyectos que se deban afrontar. (Benítez, 2011, p. 7)

La importancia de los proyectos es valiosa ya que se encargan de cubrir los problemas, necesidades, que tiene la población objeto de estudio, así como beneficiar tanto al sector público como privado.

Figura 1
Gestión del proyecto



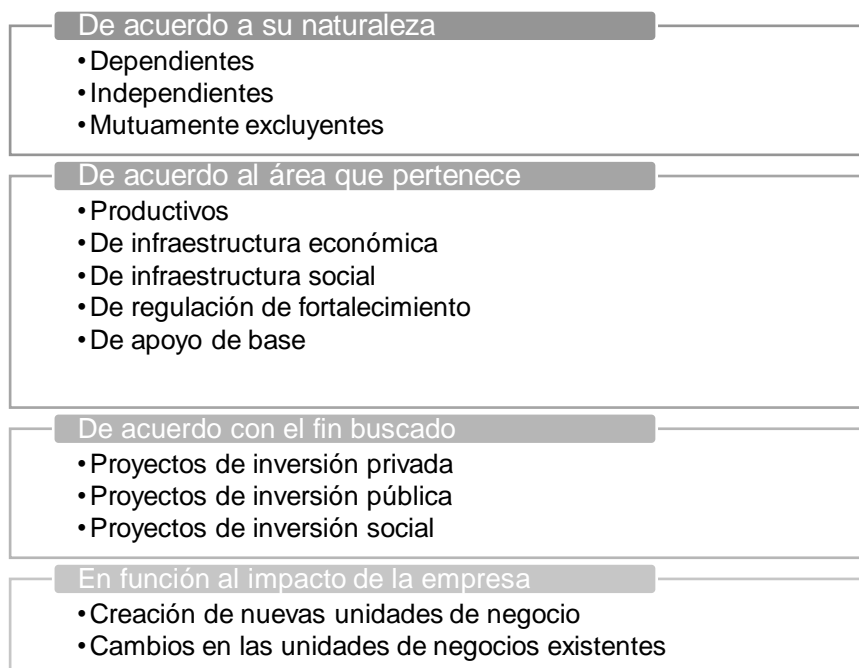
Fuente: elaboración propia, con información de Benítez (2011).

Tener una buena gestión de los proyectos es de gran relevancia, pues este da una garantía de que los mismos estén controlados, cumpliendo los plazos, presupuesto y el alcance establecido. Al realizar los proyectos correctamente se tendrá un gran impacto positivo y una garantía para la entrega del producto o servicio.

2.2. Tipos de proyectos

Existen diferentes tipos de proyecto, cada uno de ellos se enfocan en dar solución a determinadas problemáticas entre ellos se encuentran:

Figura 2
Tipos de proyectos



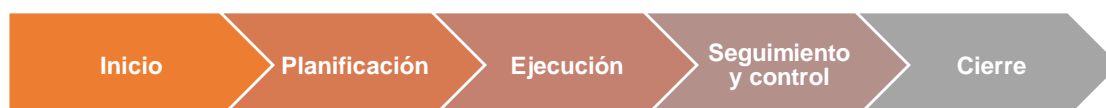
Fuente: elaboración propia, con información de Córdova (2013).

Es preciso mencionar que existe una gran variedad de proyectos, sin olvidar que los mismos son únicos y nacen por una necesidad existente en la población, estos se adaptan y están orientados a los resultados determinados.

2.3. Etapas del proyecto

Los proyectos se integran de cinco etapas principales para la ejecución, que se detallan a continuación:

Figura 3
Etapas del proyecto



Fuente: elaboración propia, con información de (OBS Business School [OBS], 2021)

Cada una de las etapas mencionadas con anterioridad son importantes al desarrollar un proyecto. En el inicio se define el alcance y la selección del personal para el proyecto, en la fase de planificación se determina los recursos, personal, equipo para realizar las actividades, así mismo en la fase de ejecución se realiza cada una de las tareas programadas para el logro de los objetivos, con el seguimiento y monitoreo se verifican el progreso de esas tareas programadas, así como la mejora que se puede realizar en el transcurso de las mismas, y en la fase de cierre no es más que la culminación de los procesos del proyecto.

Estas etapas ayudan a comprender el avance del mismo y los cambios que pueden impactar en el desarrollo del proyecto.

2.4. Ciclo del proyecto

El ciclo del proyecto se integra de las fases de Preinversión, Inversión y Postinversión es de importancia comprender cada una de ellas con los siguientes conceptos:

Durante la Fase de Preinversión de un proyecto se identifica un problema determinado y luego se analizan y evalúan - en forma iterativa - alternativas de solución que permitan encontrar la de mayor rentabilidad social. En la Fase de Inversión se pone en marcha la ejecución del proyecto conforme a los parámetros aprobados en la declaratoria de viabilidad para la alternativa seleccionada mientras que, en la Fase de Post Inversión, el proyecto entra a operación y mantenimiento y se efectúa la evaluación ex post. (PERÚ Ministerio de Economía y Finanzas, s.f, párrafo 1)

Cada una de las fases mencionadas anteriormente ayudan a la comprensión de que se debe realizar en cada una de ellas en el proyecto, así como el seguimiento que se deben realizar durante la ejecución del proyecto.

2.5. Evaluación de proyectos

Para comprender que es la evaluación de proyectos se definen los siguientes conceptos:

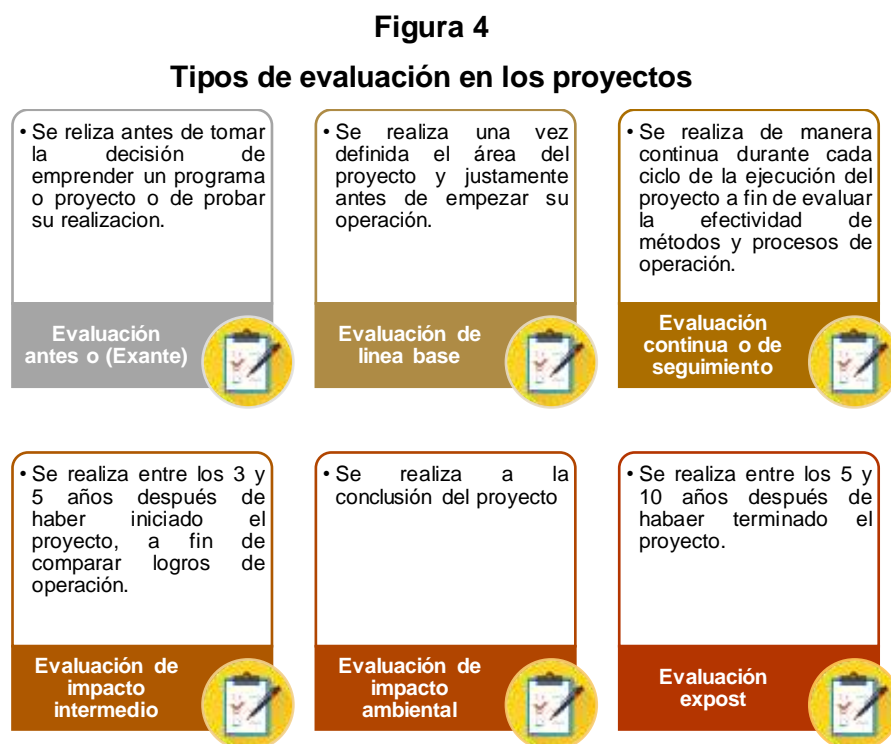
“Evaluar es fijar el valor de una cosa; para hacerlo se requiere efectuar un procedimiento mediante el cual se compara aquello a evaluar respecto de un criterio o patrón determinado” (Cohen y Franco, 1992, p. 73)

De acuerdo con Sapag et al.(2014), “La evaluación de proyectos pretende medir objetivamente ciertas variables resultantes del estudio del proyecto, las cuales permiten obtener diferentes indicadores financieros que finalmente sirven para evaluar la conveniencia económica de implementar el proyecto.” (p.6)

Evaluar un proyecto es clave para el desarrollo del mismo, esto ayuda a tener un análisis y reflexión de lo definido en el alcance y así mejorar las actividades establecidas en el transcurso del desarrollo del proyecto. En otras palabras la evaluación de proyectos es un instrumento que genera información sobre lo esperado en el proyecto para tener un juicio sobre la utilidad y confiabilidad del mismo.

2.5.1. Tipos de evaluación

En los proyectos existen distintos tipos evaluación que se adaptan y aplican dependiendo del enfoque del proyecto, estos contemplan procesos para determinar los cambios pertinentes a aplicar en el ciclo del proyecto. A continuación se desarrolla una síntesis de cada uno de ellos para tener una mejor comprensión:



Fuente: elaboración propia, con información de Díaz (s.f., pp. 4-5)

Derivado de lo anterior se puede concluir y observar que, en los proyectos cada uno de ellos ayuda a identificar, cuantificar y valorar tanto los costos como los beneficios que se generen en un determinado período de tiempo. Para efectos de esta investigación se desarrollará un poco más la evaluación *expost* para la correcta interpretación en el tema objeto de estudio.

2.6. Evaluación *expost*

La evaluación *expost* es un proceso donde se crean actividades que permitan realizar un análisis valorativo del plan, programa o proyecto que se está realizando, en otras palabras es una evaluación que se realiza durante la operación del proyecto para conocer si se logran los objetivos propuestos y cuál es el impacto logrado.

En la práctica, la evaluación *expost* se realiza normalmente algunos años después de completada la ejecución del proyecto; aun cuando este estricto rigor, solo es posible realizar esta evaluación una vez que el proyecto ha completado su vida útil. Sin embargo, este proceso requeriría una espera demasiado larga antes de poder extraer conclusiones del proceso seguido por el proyecto, con lo cual se perdería la oportunidad de la información y, por consiguiente, gran parte de su utilidad. Por esto, tal como ya se dijo en el punto anterior, resulta recomendable realizarla una vez que el proyecto esté operando en régimen normal. (Vera, 1997 p. 69)

La finalidad de la evaluación *expost* es determinar la efectividad, eficacia, impacto, sostenibilidad y la eficiencia del desarrollo del proyecto en el tiempo determinado, sin perder los objetivos establecidos al inicio del proyecto. Esta evaluación regularmente se realiza durante la fase de operación para determinar si es conveniente seguir ejecutándolo.

2.6.1. Objetivos de la evaluación *expost*

Los objetivos denominan el fin o propósito que se pretende alcanzar. El fin primordial de los objetivos en una evaluación *expost* es retroalimentar los procesos realizados en la implementación de un proyecto. Por tal motivo se detallan algunos de los objetivos para esta evaluación:

Desde el punto de vista de Cortes (2016) se debe :

1. Identificar el grado de cumplimiento de los objetivos planteados y la validez de las proyecciones ex ante.
2. Analizar el cumplimiento de los procesos y procedimientos técnicos y administrativos establecidos en la evaluación ex ante.
3. Derivar acciones correctivas para mejorar los procesos de inversión vigentes y la gestión de los proyectos
4. Generar información y lecciones para apoyar el proceso de actualización de metodologías, capacitación, criterios de formulación y evaluación ex ante. (diapositiva 3).

Tomar en consideración cada uno de los puntos mencionados anteriormente, ayudan a la identificación de las fortalezas y oportunidades en los proyectos así como determinar la conveniencia de la implementación de los mismos.

2.6.2. Tipos de evaluación expost

Esta evaluación consta de tres tipos: corto, mediano y largo plazo los cuales se describen a continuación:

Cuadro 2
Tipos de evaluación expost

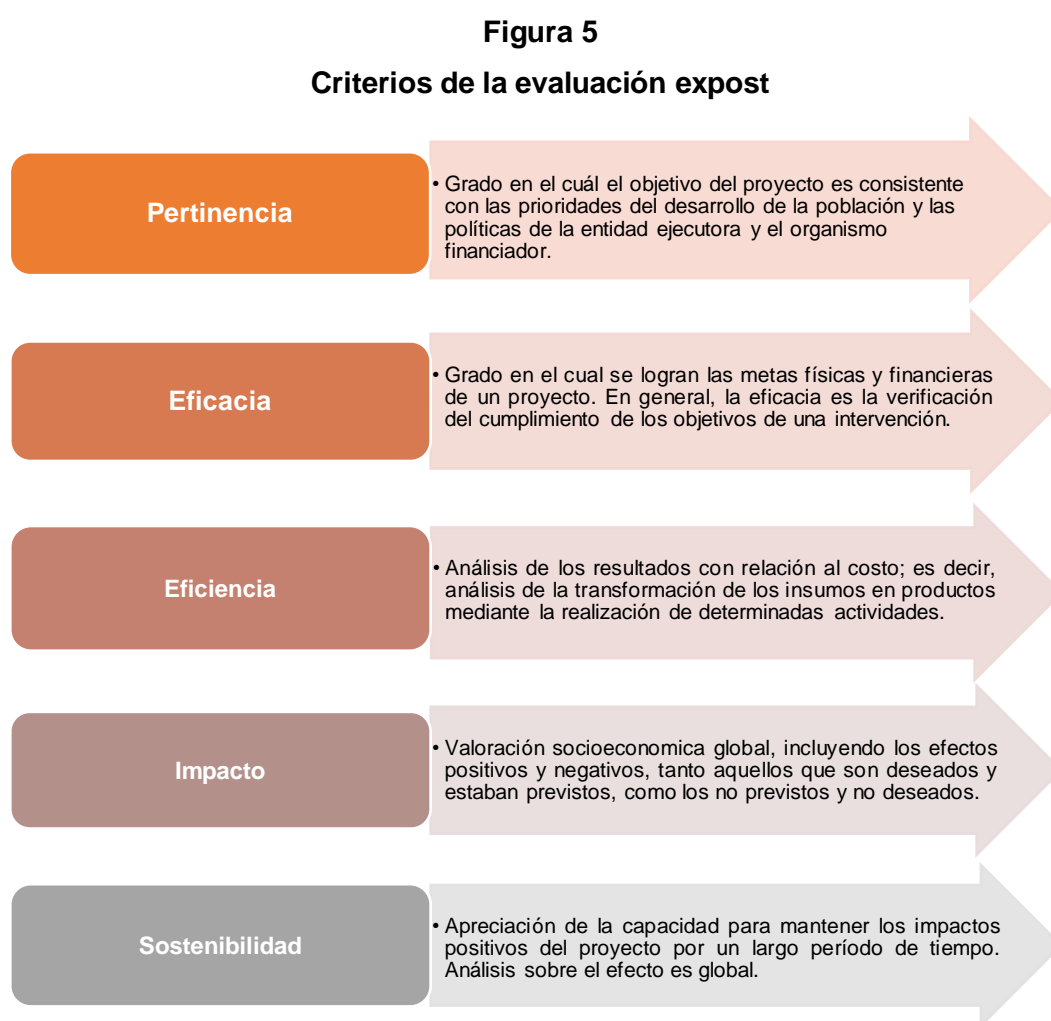
Evaluación expost	Oportunidad en que se realiza la evaluación	Alcances
Corto Plazo (Producto)	*Al término de la ejecución. *Entrada en operación (1 o 2 años).	Fase I: Medición y análisis de variables relevantes. Fase II: Visitas a terreno de proyectos en operación.
Mediano Plazo (Intermedio)	*En la etapa de operación *Proyecto con 3 a 7 años de operación.	Medición de flujos (demanda, oferta, beneficiarios, costos de operación) y efectos intermediarios. Aspectos de calidad de servicio. Análisis de la operación y modelo de gestión.
de Largo Plazo (Impacto)	*En la etapa de operación en régimen *Proyectos con más de 7 años de operación.	Levantamiento de línea base. Medición de resultados a nivel de impacto.

Fuente: elaboración propia, con información de Cortes (2016, diapositiva 4)

Cada uno de los tipos de evaluación expost tienen como fin ayudar a validar la eficiencia y eficacia en la implementación de los proyectos; así como los impactos esperados y no esperados con el fin de atenderlos adecuadamente .

2.7. Criterios de evaluación

Los proyectos tienen vida por medio de los objetivos definidos. La evaluación como se menciona anteriormente permite establecer lo que se ha logrado con los cambios establecidos. Para evaluar los resultados del proyecto se deben tomar en cuenta cinco aspectos importantes:



Fuente: elaboración propia, con información de Medianero (2014, pp. 77-78)

Al tomar en cuenta cada uno de estos criterios que son de gran relevancia en la evaluación, los mismos tienen como función principal ayudar a verificar si los proyectos producen los efectos deseados en las organizaciones a las cuales son enfocados.

2.8. Línea base del proyecto

Para comprender más sobre el término de línea base se utilizará la siguiente definición:

Las líneas base de un proyecto son un conjunto de fechas de inicio y fin, duraciones de trabajo planificadas, y los costes previstos durante la fase inicial del proyecto. Se trata de una “fotografía” del proyecto en el momento en que se realizaron las primeras estimaciones. Además, representan el plan original por donde se realizarán las mediciones y eventuales desviaciones que se produzcan a lo largo del ciclo de vida del proyecto.

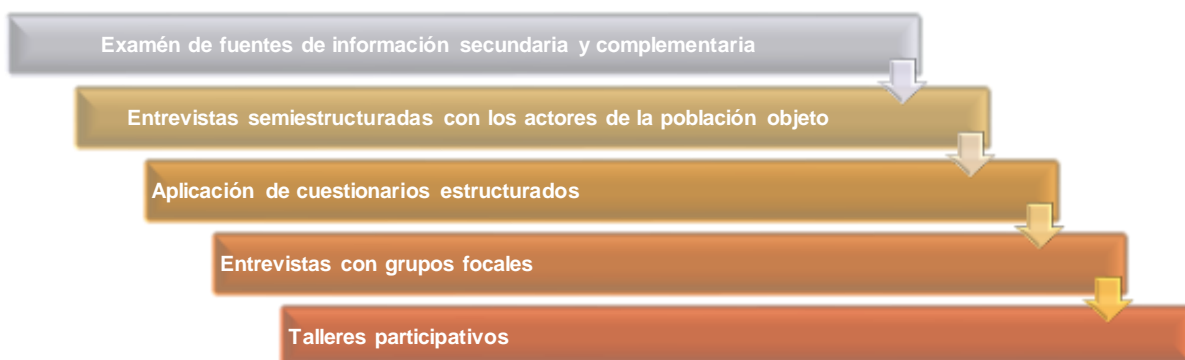
Un seguimiento correcto de las líneas base permitirá al Project Manager poner en marcha acciones preventivas o correctivas que permitan poner el proyecto otra vez dentro de la línea base original establecida. (Mármol, 2019, p. 25)

En conclusión la línea base es un conjunto de parámetros estratégicos que permiten dar seguimiento, evaluación. Este permite determinar en cualquier momento si se está dando el seguimiento oportuno al proyecto o nos desviamos de lo establecido en los objetivos.

2.8.1. Instrumentos a implementar en la línea base del proyecto

A continuación se detallan los instrumentos a seguir para realizar la línea base de los proyectos:

Figura 6
Instrumentos de la línea base



Fuente: elaboración propia, con información de Díaz, (s.f. p.8)

Los instrumentos que se utilizan en la realización de la línea base del proyecto son herramientas que ayudan a orientar el análisis evolutivo dentro del ciclo del proyecto esto con el fin de tener los resultados esperados en el plan, programa o proyecto.

2.9. Seguridad informática

Para comprender el concepto de seguridad informática se utiliza la siguiente definición:

La seguridad informática es la protección de la información y especialmente el procesamiento de la información. La seguridad de la información tiene por objeto impedir la manipulación de datos y sistemas por terceros no autorizados. El significado de esto es que los sistemas social-técnicos, es decir, las personas y la tecnología, dentro de las empresas / organizaciones y sus datos están protegidos contra daños y amenazas. Esto no sólo significa información y datos, sino también centros de datos físicos o servicios de nube. (Hornetsecurity, s.f, párrafo 3)

Para Gómez (2014) la seguridad informática son las medidas de seguridad que impiden que las operaciones que no estén autorizadas sobre cualquier sistema de informática se comprometan y afecten la confidencialidad, integridad o autenticidad de la información.

2.9.1. Objetivos de la seguridad informática

Principalmente el objetivo de la seguridad informática es mantener la confidencialidad, integridad y disponibilidad de la información, para comprender el objetivo se utiliza el siguiente concepto:

Costas (2011) define que: “La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización” (p. 19)

La seguridad de la información ayuda a minimizar, gestionar los riesgos, y amenazas. Así como la adecuada utilización de los recursos en la organización para la recuperación del sistema en caso de un incidente de seguridad.

2.10. Seguridad de la información

La seguridad de la información son todas las medidas preventivas que ayudan al resguardo de la información, es decir que son todas las políticas y procedimientos que ayuden al tratamiento y resguardo de los datos de la organización.

Gómez (2014) menciona: “La Seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.” (p. 160)

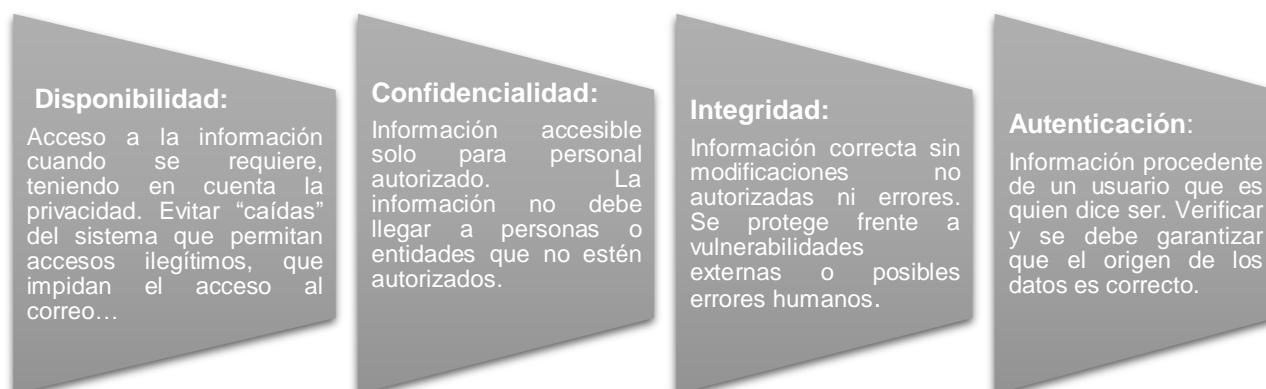
Para la protección de la información es importante contar con una clasificación para tener acceso a cierta información, entre esta clasificación se puede mencionar que existe información: crítica, valiosa, sensible, y de riesgo.

2.10.1. Bases de la seguridad de la información

Es importante no olvidar los pilares fundamentales de la seguridad de la información entre ellos se encuentran:

Figura 7

Pilares de la seguridad de la información



Fuente: elaboración propia, con información de Tecon Soluciones Informaticas (s.f, parrafo 6)

Para realizar la correcta gestión de la seguridad de la información es importante la aplicación de estos pilares en los controles y políticas de las organizaciones ya que el objetivo principal es el resguardo de los activos de información.

2.11. Activos informáticos

Lo más relevante en la implementación de un sistema de gestión de la seguridad de la información son los activos, para una mejor comprensión se utiliza el siguiente concepto:

“Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.”(ISOTools Excellens, 2017, párrafo 1).



Fuente: elaboración propia, con información de ISOTools (2015)

Los recursos en las organizaciones son las partes fundamentales para las operaciones diarias, estos se encuentran asociados ya se de forma indirecta o directa, la seguridad tiene el objetivo de resguardar los mismos y estos deben registrarse por medio de un inventario para mejor visibilidad.

2.12. Incidentes de seguridad

Para la interpretación sobre a qué se refiere un incidente se utiliza el siguiente concepto:

“Los incidentes de seguridad son eventos que pueden indicar que los sistemas o los datos de una organización han sido comprometidos o que las medidas implementadas para protegerlos han fallado”. (Rosencrance, 2019, párrafo 1).

Cuando ocurre un incidente de seguridad es de gran impacto para las organizaciones por que compromete toda la información sensible, es decir que existe la posibilidad de uso, divulgación, modificación o destrucción de la información por personas no autorizadas.

2.13. Ciberseguridad

Para la comprensión de ciberseguridad se utilizará el siguiente concepto:

“La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; extorsionar a los usuarios o interrumpir la continuidad del negocio”.(CISCO, s.f, párrafo 1).

En la actualidad todo está ligado a la tecnología y al internet, estos ataques dan como resultado desde un simple robo de identidad, hasta algo más complicado como es la extorsión por recuperar datos importantes.

2.14. ISO – Organización internacional para la normalización

Para comprender que es ISO se detalla el siguiente concepto:

“Organización Internacional de Normalización, desarrolla y pública estándares internacionales. ISO crea documentos que proporcionan requisitos, especificaciones, pautas o características que se pueden usar de manera consistente para garantizar que los materiales, productos, procesos y servicios sean adecuados para su propósito.”(ISO,2021)

Esta organización fue creada el 23 de febrero del año 1947, en Londres Reino Unido, de las cuales estaba integrada aproximadamente por 25 países en la ciudad. En la actualidad cuentan con su sede en Suiza, con 165 países miembros y un aproximado de 22,000 normas que abarcan varios sectores de la industria.

ISO (International Standardization Organization) por sus siglas en inglés es el ente regulador de los estándares y de la creación de guías desarrolladas para orientar y ordenar la gestión de la aplicación de normas técnicas, las mismas se aplican según sea la necesidad y el giro del negocio.

2.14.1. Normas ISO

Las normas ISO son documentos que especifican los requerimientos que pueden ser empleados por las partes interesadas; en otras palabras las organizaciones, las mismas son adaptadas al giro del negocio para garantizar los productos o servicios y que los mismos cumplan con los objetivos definidos. Estos documentos son de alcance nacional como internacional, los mismos son aceptados por la sociedad y el mercado.

2.14.2. ISO 27001:2013

Esta es una norma que se encarga del aseguramiento, confidencialidad e integridad de los datos e información, así como de los sistemas que administran dicha información.

Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO / IEC 27001:2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. ISO (2021)

ISO/IEC (2013) menciona: “Este Estándar Internacional especifica los requerimientos para establecer, implementar, mantener y continuamente mejorar un sistema de gestión de seguridad de la información (SGSI) en el contexto de la organización”(p. 1)

Los conceptos detallados tratan de apoyar al lector para comprender y conocer sobre la Norma ISO 27001, la importancia de esta norma como se menciona es proporcionar los controles para el resguardo de la información en las organizaciones.

En la actualidad la protección de información es algo importante no solo para las empresas, la decisión de optar por un sistema de gestión de seguridad de la información es una decisión estratégica, además estas prácticas garantizan la confidencialidad, integridad, disponibilidad y legalidad de toda información que se gestione.

2.14.3. Estructura de la norma ISO 27001:2013

Es importante mencionar que una estructura es la parte de un todo, o un conjunto de conceptos, que el fin primordial de tener una relación entre sí, que permita el funcionamiento de un sistema.

Cuadro 3

Estructura del sistema de gestión de la seguridad de la información -ISO 27001:2013

	Secciones	Incisos	Descripción
1	Alcance		Requerimientos para establecer, implementar, mantener y continuamente mejorar un sistema de gestión de seguridad de la información (SGSI), así como lineamientos para la evaluación y tratamiento de riesgos.
2	Referencias Normativas		Normativas referenciadas para la consulta de distintos documentos indispensables para la aplicación de ISO 27001
3	Términos y definiciones		Describe la terminología aplicable a este estándar
4	Contexto de la organización	4.1 Entendimiento de la organización 4.2 Entendimiento de las necesidades y expectativas de las partes interesadas 4.3 Determinación del alcance del sistema de gestión de seguridad de la información. 4.4 Sistema de gestión de seguridad de información.	La organización determina los aspectos internos y externos importantes que afectan para alcanzar lo definido.
5	Liderazgo	5.1 Liderazgo y compromiso 5.2 Política 5.3 Roles organizacionales, responsabilidades y autoridades	Se destaca la necesidad que todos los empleados contribuyan al cumplimiento de la norma y sus políticas, así como la organización demuestre compromiso y liderazgo con respecto al sistema de gestión de la seguridad de la información
6	Planificación	6.1 Acciones para atender riesgos y oportunidades 6.1.1 General 6.1.2 Valuación de riesgos de seguridad de información 6.1.3 Tratamiento de los riesgos de seguridad de información 6.2 Objetivos de seguridad de información y planificación para alcanzarlos	Esta sección indica la importancia de determinar riesgos y oportunidades a la hora de planificar el SGSI, así como establecer objetivos de seguridad y el logro de los mismos.

7	Apoyo	7.1 Recursos 7.2 Competencia 7.3 Toma de conciencia 7.4 Comunicación 7.5 Información documentada 7.5.1 General 7.5.2 Creación y actualización 7.5.3 Control de información documentada	Señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación y la información documentada y disponible para cada caso.
8	Operación	8.1 Control operacional y planificación 8.2 Valuación del riesgo de la seguridad de la información 8.3 Tratamiento del riesgo de la seguridad de la información	Este apartado de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, así como hacer una valoración de los riesgos de la seguridad de la información y el tratamiento para ellos.
9	Evaluación del desempeño	9.1 Monitoreo, medición análisis y evaluación 9.2 Auditoría Interna 9.3 Revisión gerencial	Esta sección establece la necesidad y la forma de llevar a cabo el seguimiento, medición, análisis, la evaluación, la auditoría interna y las revisiones por la dirección del SGSI para que funcione según lo planificado.
10	Mejoramiento	10.1 No conformidad y acción correctiva 10.2 Mejora continua	Las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente eficiencia del sistema de gestión de la seguridad de la información (SGSI).
	Anexo A	Objetivos de control y controles	Sección normativa que sirve como guía para implementar los controles de seguridad específicos de la norma ISO 27001.

Fuente: elaboración propia, con información de norma ISO/IEC 27001:2013

Es importante que el SGSI sea parte y este integrado con los procesos de la organización así como de la estructura de gestión y que sea integrada en los procesos para el resguardo de información. El mismo está integrado por 10 secciones que proporcionan los requerimientos para comprender, implementar, mantener y continuamente mejorar un sistema de gestión de la seguridad de la información.

2.14.4. Sistema de gestión de la seguridad de la información (SGSI)

El sistema de gestión de seguridad de la información (SGSI) es el grupo de políticas, controles y evaluaciones que ayudan a administrar la información, para entender más sobre el tema se detalla el siguiente concepto:

Gómez (2014), indica lo siguiente: “Podemos definir el Sistema de Gestión de la Seguridad de la información (SGSI) como aquella parte del sistema general de gestión que comprende políticas, la estructura organizativa, los procedimientos, los procesos, y los recursos necesarios para implantar la gestión de la seguridad de la información en una organización.” (p. 52)

Como se menciona anteriormente el SGSI son las instrucciones que se pueden adaptar a organizaciones de todo tipo y tamaño. Las organizaciones con el pasar del

tiempo están más expuestas a todo tipo de riesgo vinculado con la seguridad de la información, es por ello que la implementación de estas políticas ayudan a mantener segura dicha información de las organizaciones.

2.14.4.1. Objetivos del sistema de gestión de seguridad de la información

El propósito general de un SGSI es la protección de la información sensible o de valor.

“Para gestionar la seguridad de la información es preciso contemplar toda una serie de tareas y de procedimientos que permitan garantizar los niveles de seguridad exigibles en una organización, teniendo en cuenta que los riesgos no se pueden eliminar totalmente, pero si se pueden gestionar.” (Gómez, 2014, p. 52)

El sistema de Gestión de Seguridad de la Información busca preservar la confidencialidad, integridad y disponibilidad de la información de las organizaciones, así como informar las gestiones que se deben realizar para tratar los riesgos.

Se puede considerar como una disciplina en constante cambio, pues como se sabe el fin de la seguridad de la información es permitir que las organizaciones cumplan con los objetivos establecidos para la mejora del negocio.

Un sistema de gestión de la seguridad de la información (SGSI), basado en la norma ISO 27001 tiene como objetivo garantizar que las empresas tengan implementados todos los controles apropiados para proteger la información de las partes interesadas.

2.14.4.2. Alcance del sistema de gestión

Para comprender a que se refiere el concepto de alcance, se utilizara la siguiente definición:

“El alcance describe la extensión y los límites del SGSI, por lo que puede estar definido en términos de los activos de información, la ubicación física, las unidades organizacionales, actividades o procesos de mayor importancia para la organización, es decir, se trata de la selección de los elementos críticos a proteger.”(Mendoza, 2018, párrafo 4)

El alcance tiene con finalidad la determinación clara y sencilla de los objetivos que se pretenden alcanzar a lo largo de la implementación del sistema de gestión de la seguridad de la información, este requisito tienen la intención de aclarar todo lo que es de interés para el sistema de gestión.

2.14.4.3. Política del sistema de gestión

Para la comprensión sobre a qué se refiere una política en el sistema de gestión se tomará el siguiente concepto:

La política de seguridad consiste en desarrollar el marco de actuación apropiado para salvaguardar la información de la empresa. Su objetivo principal es indicar el propósito del Sistema de Gestión de Seguridad de la Información (SGSI) y del documento en sí. Además de indicar la finalidad de la política de seguridad, se debe señalar cómo se prevé conseguirlo, cómo ha sido aprobada y cómo se realizará su seguimiento, ya que debe revisarse de forma continua. (Guijarro, 2018, párrafo 3)

Es de gran relevancia mencionar que las políticas mencionan cada una de las actividades que deben respaldar el resguardo de la información en una organización, las mismas deben revisarse de manera continua y comunicarse a todos los interesados.

2.14.4.4. Controles en el sistema de gestión

Se tomará el siguiente concepto para la interpretación:

Desde el punto de vista de Koontz et al.(2012) “Medición y corrección del desempeño para garantizar que los objetivos de la empresa y los planes diseñados para alcanzarlos se logren” (p. 496).

La norma ISO 27001 tiene como fin primordial el aseguramiento, confidencialidad y la integridad de los datos. Implementar y poner en marcha los controles oportunos para manejar los riesgos de la seguridad de la información. Depende de la organización planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad, así como las acciones a tomar.

2.14.4.5. Registros en el sistema de gestión

Se puede definir un registro como el espacio donde se detallan distintos acontecimientos o cosas, especialmente los que son de gran relevancia para la organización. En otras palabras un registro es un espacio para evidenciar un cambio y controlarlo.

Los registros deben ser revisados de forma regular, esto ayuda a la organización a detectar posibles actividades de fraude y a saber que está sucediendo en el funcionamiento de los sistemas de información y asegurar las operaciones correctas.

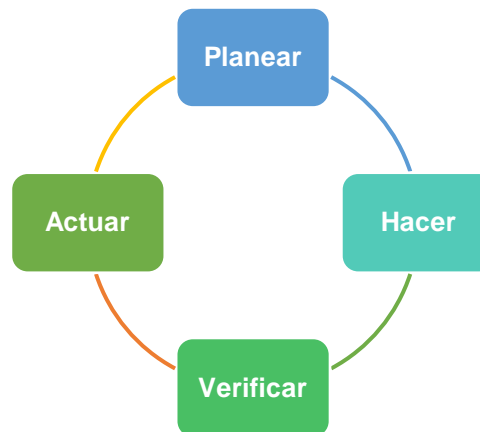
Llevar a cabo la implantación de un sistema de gestión de la seguridad de la información (SGSI) sin registros es un grave error, ya que al no contar con los mismos se incurren en sanciones por el incumplimiento de la normativa, afectando a la organización.

2.15. Ciclo PHVA

Al realizar la implementación de un sistema de gestión de seguridad de la información con base a la norma ISO 27001:2013, es necesario utilizar el ciclo de mejora continua o el ciclo PHVA.

Este ciclo constituye una de las principales herramientas de mejoramiento continuo en las organizaciones, utilizada ampliamente por los sistemas de gestión de la calidad (SGC) con el propósito de permitirle a las empresas una mejora integral de la competitividad, de los productos ofrecidos, mejorado permanentemente la calidad, también le facilita tener una mayor participación en el mercado, una optimización en los costos y por supuesto una mejor rentabilidad. (Sánchez, 2020, párrafo 2)

Figura 9
Ciclo PHVA



Fuente: elaboración propia, con información de González (2006, p. 33)

Este ciclo cuenta con cuatro fases que pueden aplicarse para la implementación de un sistema de gestión las cuales se detallan a continuación:

- **Planear:** En esta sección se definen los objetivos y se identifican los procesos necesarios para el logro de los resultados tomando en cuenta los objetivos de la organización.
- **Hacer:** Se ponen en práctica las acciones necesarias para el logro de las mejoras en la organización, con el fin de poder realizar las correcciones necesarias de los posibles errores en la ejecución y ser más eficientes.
- **Verificar:** Se establece un tiempo de prueba para poder medir los cambios implementados y así valorar la efectividad de los mismos.
- **Actuar:** Se realizan las correcciones necesarias en el caso que los resultados esperados no se ajusten a los objetivos definidos por la organización, realizando las acciones y modificaciones necesarias.

Cada una de esas fases del ciclo PHVA favorece a las organizaciones a la implementación de un sistema de gestión de la seguridad de la información, ya que brinda los pasos y las herramientas necesarias para llevarlas a cabo.

2.16. Centro de operaciones de seguridad (SOC)

Actualmente se vive rodeado de tecnología, cada una de las actividades están relacionadas a los sistemas, registros en línea o simplemente las actividades están ligadas a que se utilice el internet para realizarlas. Lastimosamente esto ha dado lugar a numerosos ataques cibernéticos, donde se pone en riesgo la información tanto de las personas como de organizaciones. De estos acontecimientos surgen los servicios SOC o Centros de operaciones de seguridad.

Para comprender que es un centro de operaciones de seguridad se utilizara el siguiente concepto:

Un SOC (Security Operations Center) o Centro de Operaciones de Seguridad está compuesto por un equipo técnico y humano que conforma una central para la seguridad informática de una determinada empresa. Sus funciones no consisten solo en defender ante posibles ciberataques, sino que también se encarga de prevenir y monitorizar toda posible actividad sospechosa en la red. (Open Data Security [ODS], 2020, párrafo 4)

El centro de operaciones de seguridad (SOC) es un departamento donde se centraliza el monitoreo y control de todo lo relacionado con la seguridad de las redes e internet, con el fin de proporcionar una atención proactiva a los posibles incidentes de seguridad.

Las empresas de todo tipo y tamaño deben hacer frente a los desafíos que presenta la tecnología con el propósito de proteger su activo más valioso: la información. La información es el objetivo principal de los ciberataques y en la actualidad las organizaciones manejan una gran cantidad de datos confidenciales.

2.16.1. Actividades del centro de operaciones de seguridad (SOC)

En los centros de operaciones de seguridad se realizan distintas actividades para el monitoreo de la información.

Morales (2014) menciona que: Realizan labores orientadas al monitoreo, aseguramiento y defensa de los activos de información por medio de equipos tecnológicos y personal especializado que monitorean en tiempo real los

eventos generados por la infraestructura tecnológica de la organización durante las 24 horas del día y los 7 días de la semana.

(p.32)

El monitoreo constante es una de las actividades que caracteriza a estos centros de operaciones ya que su fin primordial es el resguardo de la información de las organizaciones.

Morales et al. (2014) menciona que entre las actividades que realiza el centro de operaciones de seguridad se pueden mencionar:

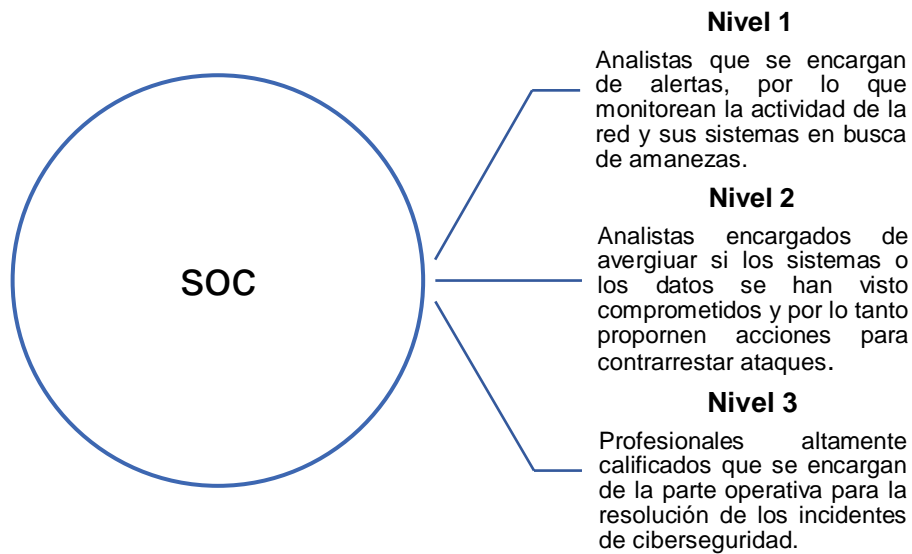
- **Prevención:** que lo que busca es la disminución de aparición de cualquier incidente de seguridad que pueda comprometer la información de las organizaciones.
- **Detección:** no es más que el monitoreo constante con el fin de descubrir las amenazas, vulnerabilidades, o ataques de seguridad.
- **Análisis:** estudia los incidentes de seguridad que surgen en la detección, ya que esto ayuda a diferenciar entre amenazas reales o falsos positivos.
- **Respuestas:** se refiere a todas las actividades o acciones que se realizan contra cualquier incidente real de seguridad.

Esta área es encargada de la detección en tiempo de las vulnerabilidades críticas que comprometan la seguridad de la información y sistemas de información. Están compuestos generalmente por analista e ingenieros de seguridad que son los que supervisan estas operaciones trabajando de la mano con los equipos necesarios para validar que el problema de seguridad se aborde adecuadamente al ser descubierto.

2.16.2. Organización del centro de operaciones de seguridad (SOC)

El centro de operaciones de seguridad se encuentra dividida en niveles según el grado de especialización de cada uno de los analistas que conforman el equipo. La estructura mencionada se detalla a continuación:

Figura 10
Jerarquía SOC



Fuente: elaboración propia, con información de Buldign solutions together [ambit], 2020, párrafo 6)

La especialización de los analistas que conforman el centro de operaciones de seguridad es de gran importancia, ya que beneficia a la organización en la atención de las alertas, incidentes de seguridad y el monitoreo constante para el resguardo de los activos de información. La experiencia de cada uno de ellos en las distintas herramientas y tecnologías.

3. METODOLOGÍA

Este capítulo contiene la metodología aplicada en la investigación que explica a detalle de qué y cómo se hizo para resolver el problema de la investigación. El conjunto de procedimientos utilizados son parte fundamental y ayudan a alcanzar los objetivos planteados en la investigación.

3.1. Definición del problema

En la actualidad cada día son más las amenazas y variantes de ataques que pueden poner en riesgo la información y el buen funcionamiento en la organización. No obstante realizar una implementación de un sistema de gestión de seguridad de la información con base a la norma ISO 27001 en un centro de operaciones de seguridad, disminuye los incidentes de seguridad para no tener consecuencias operativas, financieras, y legales graves que pueden afectar el negocio.

El problema identificado para la unidad de análisis es la fuga de información que es provocado por no contar con una gestión eficiente del resguardo de la información, buenas prácticas, políticas y procedimientos como lo recomienda la Norma ISO 27001:2013 ya que esto preocupa enormemente a las organizaciones.

Derivado de la importancia que refleja la seguridad informática en las empresas; es necesario revisar los procesos que se realizan actualmente en el centro de operaciones de seguridad (SOC) por medio de una evaluación expost a corto plazo, con el fin de determinar si cumplen con los lineamientos necesarios para el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan; con el fin de buscar la mejora continua en los procesos establecidos.

Las preguntas formuladas para dar respuesta al problema de investigación son las siguientes:

1. ¿Qué procedimientos pueden aplicarse para verificar que los alcances, objetivos, políticas y procedimientos del sistema de gestión de seguridad de la

información (SGSI) están diseñados y aplicados correctamente al tipo de organización?

2. ¿Cómo se pueden identificar los riesgos sobre los activos de información del centro de operaciones de seguridad (SOC)?
3. ¿Se cuenta con la información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información?
4. ¿Cuál sería el efecto en la demanda de servicios de ciberseguridad, a partir de la implementación de la norma ISO 27001 en el centro de operaciones de seguridad?

Las preguntas detalladas anteriormente permiten sugerir una solución al problema de investigación, por medio de una evaluación expost a corto plazo, para identificar las fortalezas y debilidades del sistema de gestión de la seguridad de la información ISO 27001:2013, implementadas en el centro de operaciones de seguridad.

3.2. Objetivos

Para el alcance de los resultados esperados, se establece el siguiente objeto general y los objetivos específicos, que serán de apoyo para la demostración de los resultados alcanzados en el proyecto objeto de estudio. Los mismos representan el propósito de la investigación y los fines que se desea alcanzar.

3.2.1. Objetivo general

Realizar una evaluación expost a corto plazo de la implementación del sistema de gestión de seguridad de la información ISO 27001:2013 en un centro de operaciones de seguridad, para validar y gestionar los controles pertinentes y así asegurar la confidencialidad, integridad y disponibilidad de los activos de información.

3.2.2. Objetivos específicos

Los objetivos específicos formulados en la presente investigación son la guía para alcanzar el objetivo general, los cuales son detallados a continuación:

- i. Validación del cumplimiento de la norma ISO 27001:2013 en el centro de operaciones de seguridad (SOC).

- ii. Análisis de riesgos en los activos de información en el sistema de gestión de la seguridad de la Información (SGSI), implementados en el centro de operaciones de seguridad.
- iii. Evaluar los controles definidos sobre los activos de información, puestos en marcha por la implementación de la norma ISO 27001 en el centro de operaciones de seguridad (SOC)
- iv. Analizar el efecto en la demanda de servicios del centro de operaciones de seguridad, a partir de la implementación de la norma ISO 27001:2013 en el año 2020.

3.3. Diseño de la investigación

El diseño de la investigación está relacionado con las técnicas utilizadas para la recolección de datos, así mismo, constituyen el plan para la obtención de información para el análisis de la evaluación expost a corto plazo de la implementación de un sistema de gestión de la seguridad de la información ISO 27001:2013 en un centro de operaciones de seguridad, cuya finalidad es obtener respuestas a las interrogantes planteadas.

Para la investigación se utilizó el diseño no experimental transversal, para lo cual se aplicaron una serie de técnicas e instrumentos. Para la obtención de información se utilizó las técnicas documentales como la revisión bibliográfica, lectura analítica, fichas de resumen y esquemas. Así mismo para las técnicas de campo se utilizó una entrevista no estructurada y el análisis de documentos.

3.3.1. Unidad de análisis

Definir la unidad de análisis es relevante para obtener la información correspondiente y así relacionarla sin problemas al tema de estudio.

La investigación objeto de estudio consideró como unidad de análisis un centro de operaciones de seguridad (SOC) ubicado en el municipio de Guatemala, departamento de Guatemala.

3.4. Periodo histórico

Para la evaluación de los resultados alcanzados por el proyecto objeto de estudio, se consultaron los archivos que fueron elaborados en el período 2,020 en el centro de operaciones de seguridad (SOC) por la implementación de la norma ISO 27001. Así mismo la entrevista no estructurada y análisis de documentos que fueron elaborados en el mes de julio del año 2021.

3.5. Ámbito geográfico

El ámbito geográfico utilizado para la realización de la investigación objeto de estudio es el Municipio de Guatemala, Departamento de Guatemala. En relación a lo antes expuesto, el lugar en el cual se realizó el trabajo de investigación es de relevancia, para los resultados que arroje la investigación.

3.6. Universo y muestra

Para la presente investigación se utilizó como universo y muestra lo siguiente:

El universo para esta investigación fueron las políticas, objetivos, procedimientos, y registros del centro de operaciones de seguridad (SOC). Así mismo el instrumento aplicado fue una guía de análisis de documentos.

La muestra de la presente investigación es no probabilística por conveniencia, por tal motivo no se consideró un número determinado de documentos implementados en el centro de operaciones para el análisis correspondiente. Adicional se aplicó una entrevista no estructurada al especialista de seguridad del SOC, por medio de una guía de entrevista conformada por 8 preguntas abiertas.

3.7. Técnicas e instrumentos aplicados

Esta sección contempla el conjunto de procedimientos y herramientas utilizadas para recopilar la información necesaria para la investigación objeto de estudio; con estas técnicas se pretende presentar los datos precisos para dar respuesta y respaldar la solución al problema objeto de estudio.

3.7.1. Técnicas e instrumentos documentales

Las técnicas de investigación documental fueron utilizadas para la recolección de información sobre la unidad de análisis y para la recopilación de teorías que sustentan el marco teórico de la investigación, por lo que se utilizaron las siguientes técnicas:

a) Revisión bibliográfica

Se realizaron consultas en libros, tesis, revistas, ensayos, periódicos, así como la consulta de la norma ISO 27001 relacionada con la implementación del sistema de gestión de la seguridad de la información.

b) Lectura analítica

Se realizó lectura analítica de libros, tesis, revistas, procedimientos relacionados con la implementación del sistema de gestión de la seguridad de la información (SGSI), así como la norma ISO 27001.

c) Fichas de resumen

Para la investigación se realizaron fichas de resumen bibliográficas sobre los temas relacionados con la implementación del sistema de gestión de la seguridad de la información en un centro de operaciones de seguridad, extrayendo lo más importante de cada documento, determinando los temas aplicados a la investigación.

d) Esquemas

En la presente investigación se presentaron distintos esquemas relacionados al tema de proyectos, así como la norma ISO 27001 donde se trató de destacar lo más relevante para la investigación.

3.7.2. Técnicas e instrumentos de investigación de campo

Entre las técnicas e instrumentos de campo utilizados para recabar la información primaria y secundaria tratadas en el presente trabajo, se encuentran las siguientes:

a) Entrevista no estructurada

La técnica de entrevista no estructurada fue aplicada a través de un instrumento conformado por una guía de entrevista estructurada integrada por 8 interrogantes, la

misma fue realizada al especialista de seguridad, con la finalidad de formalizar un criterio de un experto para obtener información sobre la implementación del SGSI en el centro de operaciones de seguridad.

b) Análisis de documentos

Se realizó un análisis exhaustivo de los documentos relacionados a la investigación, entre los instrumentos utilizados se menciona los objetivos, políticas, registros y procedimientos implementados en el centro de operaciones de seguridad (SOC); así como el análisis de riesgos definido en la unidad de estudio, de igual forma se utilizó como apoyo una guía de análisis de documentos, con el objetivo de realizar un análisis interpretativo de los mismos.

3.8. Resumen del procedimiento aplicado

La investigación corresponde a una investigación de tipo aplicada, con un enfoque mixto en donde prevalece un enfoque cuantitativo; se utilizó un diseño de investigación no experimental transversal debido a que se observan situaciones ya existentes y el objetivo es analizar la evolución que ha tenido en el tiempo, recopilando la información con el fin de investigar y describir cada una de ellas.

Se estableció un alcance descriptivo-explicativo, donde se detalló las características y aspectos importantes del problema, con la finalidad de analizar cómo se manifiesta el problema de la unidad de análisis.

En relación a las técnicas de investigación que se utilizaron, corresponden al conjunto de procedimientos y herramientas para la interpretación de la información necesaria.

a) Fase indagatoria

Para llevar a cabo la investigación se realizaron consultas de fuentes bibliográficas, informes, tesis, revistas, la norma ISO 27001, con el fin de recopilar la información necesaria e importante que se debe considerar en el análisis. Para la revisión de las fuentes bibliográficas se utilizaron las técnicas e instrumentos documentales como: la revisión bibliográfica a través de la lectura analítica, así también se utilizaron citas bibliográficas y el subrayado con el fin de extraer lo más importante de cada fuente.

b) Fase demostrativa

Esta fase en la investigación permitió planear los medios, técnicas e instrumentos para ordenar los resultados de la investigación. Se utilizó el análisis de documentos como técnica de campo, la cual sirvió para el análisis de los objetivos, políticas, registros y procedimientos del centro de operaciones de seguridad (SOC) en el periodo 2020.

c) Fase expositiva

Esta fase se desarrolló a través del informe del trabajo profesional de graduación, en el cual se expone el resultado final de la investigación relacionada con la evaluación de corto plazo de los efectos de la implementación del sistema de gestión de la seguridad de la información y también las recomendaciones y aportes que ayudarán a la solución del problema.

Según Piñola (2016) esta es la última fase del método científico en la cual se plantean los resultados para que estos puedan ser difundidos, divulgados y expuestos a la sociedad con el fin de que estos sean experimentados. (p.44)

4. DISCUSIÓN DE RESULTADOS

El presente capítulo muestra los resultados de la investigación relacionada con la realización de una evaluación a corto plazo de los efectos de la implementación del sistema de gestión de seguridad de la información con base a la norma ISO 27001 en un centro de operaciones de seguridad, para validar los controles pertinentes que aseguren la confidencialidad, integridad y disponibilidad de los activos de información.

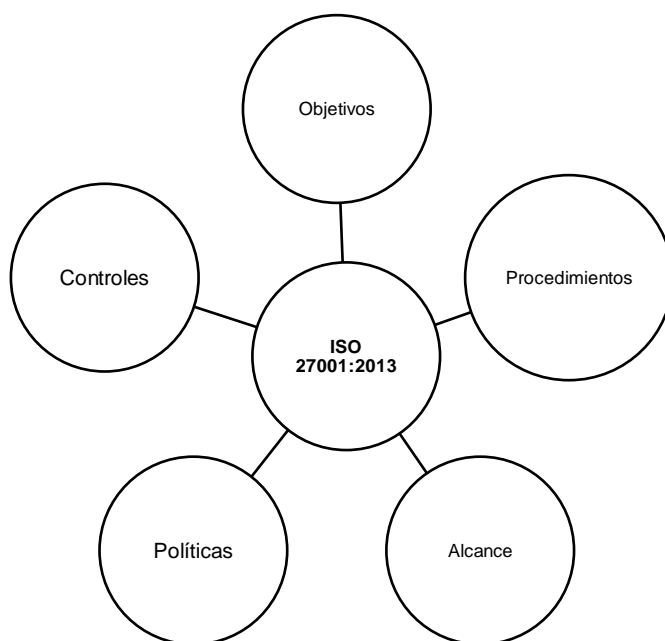
La estructura del capítulo se presenta en función al planteamiento de cada objetivo específico, por lo que se analizarán y se responderá a cada uno de ellos.

4.1. Validación del cumplimiento de la Norma ISO 27001:2013 en el centro de operaciones de seguridad (SOC)

La norma ISO 27001 establece los lineamientos para implementar y mejorar continuamente un sistema de gestión de seguridad de información en la organización. Este documento también incluye los requerimientos para la evaluación y tratamiento de los riesgos identificados.

Figura 11

Municipio de Guatemala, centro de operaciones de seguridad, esquema estructural norma ISO 27001:2013



Fuente: elaboración propia, con información obtenida de investigación de campo.

Los documentos generados por la implementación de la norma ISO 27001; como lo son el alcance, política, objetivos, registros y procedimientos en una organización son esenciales. Estos documentos proporcionan una ruta para las operaciones diarias que se realizan y ayudan a asegurar el cumplimiento de las directrices que buscan orientar los procesos internos y mejorar la toma de decisiones.

La norma ISO 27001 implementada en la unidad de estudio, fue puesta en marcha desde hace un año.

Por lo tanto para dar respuesta al objetivo número uno, se procede a realizar una revisión de documentos, los mismos fueron seleccionados de acuerdo al grado de importancia en el centro de operaciones de seguridad, se tomó como base la norma ISO 27001; donde se encuentran los requisitos de cómo gestionar la seguridad de la información en una organización.

Para esto, se seleccionaron 12 documentos que forman parte importante de la unidad de análisis, con el fin de conocer la estructura, contenido y así saber si cumplen con los lineamientos mínimos que solicita la norma. Estos se detalla a continuación:

Alcance:

- Alcance del sistema de gestión de la seguridad de la información.

Políticas:

- Política de seguridad de la información
- Política de gestión de seguridad de la información
- Política de pantalla y escritorio limpio
- Política de dispositivos móviles y teletrabajo
- Política de seguridad de proveedores

Procedimientos:

- Procedimiento de manejo de información documentada
- Procedimiento de control y accesos a sistemas y aplicaciones
- Procedimiento de respaldos

Registros:

- Registro de inducción.
- Registro de declaración y aceptación de documentos.
- Registro de salida de activos.

Cuadro 4

Municipio de Guatemala, centro de operaciones seguridad, verificación de documentos implementados versus norma ISO 27001

Documento revisado	Tipo de documento	Descripción	Sección de la norma ISO 27001 y/o Anexo A relacionado	Cumple	No cumple
Alcance del sistema de gestión de la seguridad de la información	Alcance	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de información para establecer su alcance.	4.3 Determinación del sistema de gestión de seguridad de la información.	✓	
Política de seguridad de la información	Política	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes pertinentes.	A. 5.1 Orientación de la dirección para la gestión de la seguridad de la información.	✓	
Política de gestión de seguridad de información	Políticas	Define el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.	5.2 La alta gerencia debe establecer una política que sea apropiada con el propósito de la organización	✓	
Política de pantalla y escritorio limpio	Política	Norma las condiciones en que debe mantenerse el lugar de trabajo (escritorio) y la pantalla de la computadora.	A.11.2.9 Escritorio y pantalla limpia	✓	
Política de dispositivos móviles y teletrabajo	Política	Normalización en el uso de los dispositivos móviles dentro de la organización, y definir reglas que permitan el aseguramiento de la información contenida en los mismos.	A.6.2.1 Dispositivos móviles	✓	
Política de seguridad de proveedores	Política	Define las normas para la relación con proveedores.	A.15.1.1 Seguridad de información para relaciones con suplidores	✓	
Procedimiento de manejo de información documentada	Procedimientos	Creación, actualización control de cambios, aprobación, publicación, comunicación y revisión de la información documentada.	7.5 Información documentada	✓	
Procedimiento de control y accesos a sistemas y aplicaciones	Procedimiento	Describir los pasos necesarios para la gestión de los accesos relacionados a los componentes tecnológicos utilizados para los procesos.	A.9.1.1 Control de acceso	✓	
Procedimiento de respaldos	Procedimiento	Provee los lineamientos necesarios para mantener la integridad y disponibilidad de la información donde se almacena la información de la organización.	A.12.3 Copias de respaldo de la información	✓	

Registro de salida de activo	Registro	Los equipos de información o software no deben sacarse de las instalaciones sin una autorización previa.	A.11.2.5 Traslado de activos	✓	
Registro de inducción	Registro	Se debe asegurar que los empleados estén conscientes de sus responsabilidades en la organización.	A.7.2.2 Capacitación educación y toma de conciencia para la seguridad de la información	✓	
Registro de declaración y aceptación de documentos	Registro	Define el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.	5.2 La alta gerencia debe establecer una política que sea apropiada con el propósito de la organización. A. 5.1 Orientación de la dirección para la gestión de la seguridad de la información.	✓	

Fuente: elaboración propia, con información de norma ISO/IEC 27001:2013

Se realizó una comparación de los documentos por medio de una lista de verificación, donde se validó que los documentos estuvieran estructurados de acuerdo a los lineamientos establecidos por la norma ISO 27001 y que los mismos respetaran el procedimiento para la estructura y control de los documentos, así como la aprobación.

El cuadro 4 muestra que los documentos seleccionados del centro de operaciones de seguridad (SOC), técnicamente ha cumplido con los requisitos que la norma establece en la implementación. Cabe mencionar que estos requisitos, y controles se presentan en anexo A, que es la guía para implementar los controles de seguridad, los mismos varían en su aplicabilidad ya que estos son evaluados y elegidos de acuerdo a la comodidad del departamento u organización.

Cuadro 5

Municipio de Guatemala, centro de operaciones de seguridad, hallazgos en la verificación de documentos

Documento revisado	Tipo de documento	Histórico de revisión	Observación
Alcance del sistema de gestión de la seguridad de la información.	Alcance	✓	Actualizado en el espacio de histórico de revisión.
Política de seguridad de la información.	Política	✓	Actualizado en el espacio de histórico de revisión.
Política de gestión de seguridad de información.	Políticas	☒	Pendiente de actualización de nuevos nombres oficiales validados por RR.HH. y la gerencia.

Política de pantalla y escritorio limpio.	Política	✓	Actualizado en el espacio de histórico de revisión
Política de dispositivos móviles y teletrabajo.	Política	✓	Actualizado en el espacio de histórico de revisión
Política de seguridad de proveedores.	Política	✓	Actualizado en el espacio de histórico de revisión
Procedimiento de manejo de información documentada.	Procedimiento	<input checked="" type="checkbox"/>	Pendiente de actualización de nuevos nombres oficiales validados por RR.HH. y la gerencia.
Procedimiento de control y accesos a sistemas y aplicaciones.	Procedimiento	✓	Actualizado en el espacio de histórico de revisión.
Procedimiento de respaldos	Procedimiento	✓	Actualizado en el espacio de histórico de revisión.
Registro de salida de activo	Registro	<input checked="" type="checkbox"/>	La carpeta no se encuentra actualizada con los registros de salida de equipos.
Registro de inducción	Registro	✓	Actualizado en el espacio de histórico de revisión.
Registro de declaración y aceptación y aceptación de documentos.	Registro	✓	Actualizado en el espacio de histórico de revisión.

Fuente: elaboración propia, con información obtenida de investigación de campo.

De los documentos verificados, tres se encontraba desactualizados, ya que se habían realizado modificaciones en los nombres oficiales de algunos puestos, que tiene roles y responsabilidades descritas en las política, registros y procedimientos; ya que los documentos no contemplan el cambio en la sección del histórico de revisión. Así también la carpeta donde se coloca el control de los registros de la salida de activos se encuentra desactualizada.

Es de importancia mencionar que al realizar la evaluación de los documentos del centro de operaciones de seguridad, no fue posible ubicar un control de versiones para la gestión de los cambios que puedan realizarse en los mismos y así la organización sepa en todo momento cual es la versión más actual.

La utilidad de la revisión periódica de los documentos permite al SOC contar con el diagnostico oportuno y adecuado, debido a que es necesario realizar validaciones y actualizaciones prudenciales en las políticas, procedimientos, y registros si fuera

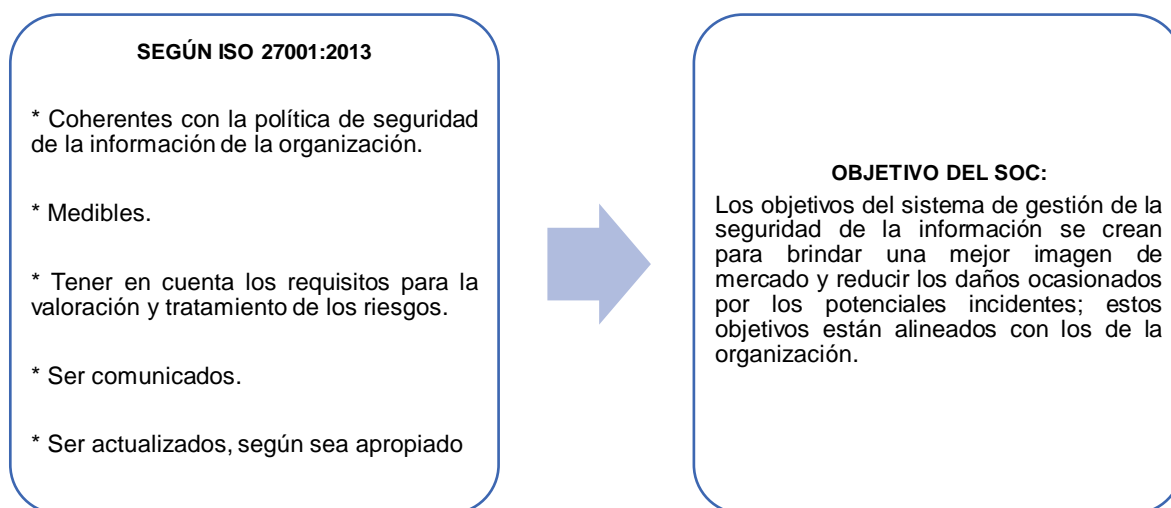
necesario, con el fin de no presentar incumplimientos que impliquen más tiempo y costo en el desarrollo de la implementación y ejecución.

4.1.1. Objetivo del centro de operaciones de seguridad

En términos generales un objetivo es un fin que se pretende alcanzar, el mismo debe estar asociado a una acción para ser cumplido.

Figura 12

Departamento de Guatemala, centro de operaciones de seguridad, estructura del objetivo de seguridad según norma ISO 27001



Fuente: elaboración propia, con información obtenida de investigación de campo.

Como se aprecia en la figura 12 al efectuar la revisión del objetivo del centro de operaciones de seguridad (SOC), este se encuentra alineado a las recomendaciones de la norma, ya que el principal fin radica en analizar y gestionar los riesgos basados en los procesos.

La importancia del objetivo en el centro de operaciones de seguridad es contar con los niveles idóneos para la integridad, confidencialidad y disponibilidad de la información para toda el área, con el fin de asegurar la continuidad de los procesos y servicios mediante el SGSI.

Para que el sistema de gestión de seguridad de la información sea útil debe cumplir con el objetivo de seguridad. La organización necesita medir, controlar, y revisar el

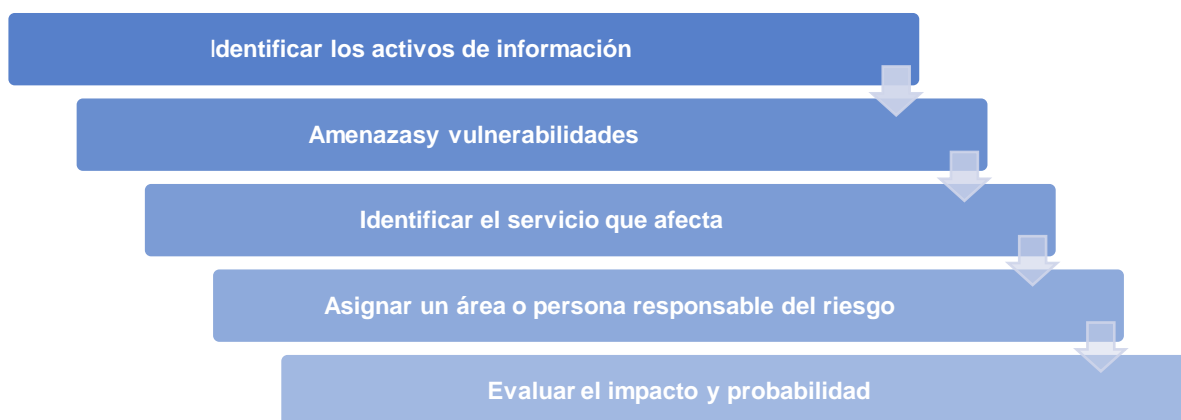
rendimiento por medio de métricas y otros métodos para calcular la efectividad y la implementación de los controles.

4.2. Análisis de riesgos de los activos de información en el sistema de gestión de la seguridad de la información (SGSI), implementados en el centro de operaciones de seguridad.

El propósito de una evaluación de riesgos es identificar y colocar una ponderación o calificación a los mismo mismos, con el fin de identificar y seleccionar los controles apropiados para los sistemas de la información, y los activos de información.

Figura 13

Departamento de Guatemala, centro de operaciones de seguridad, metodología de evaluación y tratamiento de riesgos en los activos de información



Fuente: elaboración propia, con información obtenida de investigación de campo.

Para dar respuesta al objetivo específico número dos, se recabo información sobre la metodología utilizada para la clasificación de los riesgos de la unidad de análisis; así como el análisis de los documentos internos que respaldan el proceso.

Como se muestra en la figura 13, la identificación de los riesgos del SOC se realiza por medio de la metodología de evaluación y tratamiento riesgos; la misma está dividida en cinco pasos: en la identificación de activos lo que se debe realizar es seleccionar los activos más importantes que guardan relación con las actividades del departamento. Con el tema de amenazas y vulnerabilidades no es más que identificar las amenazas a que los activos de información clasificados con anterioridad están expuestos, con la identificación del servicio afectado se debe indicar cual o cuales son los servicios relacionados al riesgo, identificar al dueño del riesgo se refiere a la

persona o unidad responsable de rendir cuentas y con la autoridad de gestionar el riesgo, una vez identificado los riesgos es necesario evaluar el impacto por cada combinación de riesgos y vulnerabilidades de un activo. Esta metodología utilizada es de gran ayuda para definir el nivel aceptable de riesgo según la norma ISO 27001, así como identificar los controles adecuados para su implementación.

La evaluación y tratamiento de riesgos fue aplicada a todo el alcance del sistema de gestión de seguridad de la información (SGSI), es decir a todos los activos de información y elementos de configuración. Dicho de otra forma, todos los activos que pueden afectar la confidencialidad, integridad y disponibilidad de la unidad de estudio.

4.2.1. Evaluación de riesgos

La evaluación de riesgos pretende identificar las amenazas y vulnerabilidades en el ambiente de trabajo, es uno de los pasos que se utiliza para el proceso de gestión de riesgos en la unidad objeto de estudio.

La evaluación de riesgos es implementada a través de los documentos: inventario de activos de información y el catálogo de servicios. Es de relevancia mencionar que los activos puede ser documentos en papel o en formato electrónico, aplicaciones, bases de datos, así como los colaboradores ya que manejan información sensible relacionada a las operaciones diarias de la organización.

Figura 14

Departamento de Guatemala, centro de operaciones de seguridad, herramientas para la evaluación de riesgos



Fuente: elaboración propia, con información obtenida de investigación de campo.

Como se observa en la figura 14, la evaluación del riesgo fue establecida a través de estos documentos, coordinado por el especialista de seguridad quien es el responsable de mantener la integridad y resguardo de la información en el centro de operaciones de seguridad (SOC).

En cuanto a la identificación de los riesgos y vulnerabilidades, así como la evaluación de probabilidad e impacto es responsabilidad del dueño del activo, quien también es el propietario del riesgo.

El análisis de riesgos con base a la norma ISO 27001 no solo es implementado en el centro de operaciones de seguridad para lograr la conformidad de la norma, o para lograr la certificación; si no para saber los controles ideales para gestionar los riesgos de pérdida por información en las actividades diarias, si existen permisos excesivos en colaboradores, vulnerabilidades en plataformas que afecten la confianza y la seguridad de la información de los clientes.

Cuadro 6

Departamento de Guatemala, centro de operaciones de seguridad, diseño de inventario de activos del SOC

Nivel de confidencialidad	Nivel de integridad	Nivel de disponibilidad
0= Pública	1= Baja	1= Baja
1= Uso interno	2= Media	2= Media
2= Confidencial	3=Alta	3=Alta
3=Restringida		

No.	Siglas del proceso	Nombre del activo	Descripción	Responsable del activo	Cantidad	Ubicación	Categoría	Nivel de confidencialidad	Nivel de integridad	Nivel de disponibilidad	Valor del activo	Riesgo actual	Riesgo residual	Mitigación
1	SGSI	Equipo de cómputo	Laptop	Especialista de seguridad	1	Zona 10	Hardware IT	2	2	2	6	30	0	30
2	SGSI	Teléfono	celular	Especialista de seguridad	11	Zona 10	Hardware IT	3	2	2	6	30	0	30

Fuente: elaboración propia, con información obtenida de investigación de campo.

Como se observa en el cuadro 6, el centro de operaciones de seguridad identifica y clasifica todos los activos de información y elementos de configuración. Es decir, todos los activos que pueden afectar la confidencialidad, integridad y disponibilidad de la información, los mismos están integrados en el registro de activos y reciben una ponderación. Seguidamente de la verificación del inventario de activos, se validó la identificación y ponderación de los riesgos y vulnerabilidades relacionados con cada activo. Estos riesgos y vulnerabilidades se identificaron utilizando los catálogos incluidos en el inventario de activos y cálculo de riesgos. Los registros utilizados en el centro de operaciones de seguridad, según verificación efectuada se encuentra debidamente actualizados e identificados.

4.2.2. Impacto y probabilidad

Es importante considerar que los impactos son el conjunto de consecuencias que originan los riesgos si llegaran a presentarse, y la probabilidad no es más que una posibilidad de que ocurra ese riesgo tomando en cuenta que ya existen controles determinados.

Cuadro 7

**Departamento de Guatemala, centro de operaciones de seguridad, matriz de riesgos-
evaluación del impacto**

Valor	Descripción	Impacto en el negocio
1	Muy Bajo	La pérdida de confidencialidad, disponibilidad o integridad no afecta las finanzas, causa daños mínimos.
2	Bajo Tolerable	La pérdida de confidencialidad, disponibilidad o integridad causa gastos adicionales y tiene consecuencias bajas o moderadas sobre obligaciones legales o contractuales o sobre el prestigio de la organización.
3	Medio (moderado)	La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias mayores en todo el negocio y está empezando a afectar la habilidad de operar de manera normal y existe ya preocupación sobre el negocio en general.
4	Medio-Alto (importante)	La pérdida de confidencialidad, disponibilidad o integridad causa daños serios sobre las operaciones, las obligaciones legales o contractuales o el prestigio de la organización. La habilidad de operar normalmente ya fue afectada seriamente. Costos altos por análisis forense, posibles multas o penalizaciones.
5	Alto (Intolerable)	La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias importantes e inmediatas sobre las finanzas, las operaciones, las obligaciones legales o contractuales o el prestigio de la organización.

Fuente: elaboración propia, con información obtenida de investigación de campo.

El cuadro 7 detalla una matriz de riesgo donde se coloca la descripción de sus impactos clasificándolos en bajos, medios y altos, con algunos intermedios. Esto permite priorizar de forma visual y es utilizado para el análisis del riesgo.

Cuadro 8

Departamento de Guatemala, centro de operaciones de seguridad, matriz de riesgos-
probabilidad u ocurrencia de riesgos

Escala de probabilidad		
Valor	Nivel	Descripción
1	Muy baja	No ha pasado en mucho tiempo.
2	Baja	Raro, posibilidad que pase tal vez 1 vez por año
3	Media	Periódico, posibilidad que pase tal vez 1 vez al trimestre
4	Media alta	Regular, posibilidad que pase tal vez 1 vez al mes
5	Alta	Frecuente, posibilidad que pase tal vez 1 vez por semana

Fuente: elaboración propia, con información obtenida de investigación de campo.

Seguidamente de la evaluación del impacto, es necesario evaluar la probabilidad de que estos riesgos se materialicen; en otras palabras, la probabilidad de que un riesgo se aproveche de las vulnerabilidades de uno o varios activos de información. Para esto de igual manera se utiliza una matriz de riesgos donde se detalla el valor en una escala de 1 a 5, clasificado la probabilidad en baja, media, alta y algunos intermedios como se observa en el cuadro 8.

4.2.3. Criterios para la aceptación de riesgos

Los criterios de aceptación son los utilizados como base para la toma de decisiones y la justificación para aceptar el riesgo.

Cuadro 9

Departamento de Guatemala, centro de operaciones de seguridad, escala de aceptación de
riesgos

DE	A	Resultado	Acciones a tomar
0	26	Riesgo Muy Bajo (MB)	Monitorear
27	44	Riesgo Tolerable (TO)	Monitorear
45	89	Riesgo Moderado (MO)	Monitorear con prioridad
90	134	Riesgo Importante (I)	Tratar
135	225	Riesgo Intolerable (IN)	Tratar de inmediato

Fuente: elaboración propia, con información obtenida de investigación de campo.

En el cuadro anterior se detalla la ponderación asignada a la clasificación de los riesgos que el centro de operaciones de seguridad utiliza al establecer la valoración. Donde se puede observar que los rangos con mayor ponderación que corresponden a: (90-134 Riesgo importante) y (135-225 Riesgo intolerable) los mismos serán priorizados y tendrán una o más opciones de tratamiento. El resto tendrá un monitoreo recurrente o se puede tratar a discreción del Especialista de Seguridad o el equipo de seguridad.

Cuadro 10

Departamento de Guatemala, centro de operaciones de seguridad, análisis de riesgos de los activos de información y su tratamiento

No.	Activo	Valor del activo	Riesgo	Vulnerabilidad	Probabilidad (P)	Impacto (I)	Nivel de riesgo expuesto	Descripción de riesgo y vulnerabilidad	Controles propuestos
1	Repositorio de datos	8	Acceso no autorizado al sistema de información	Información disponible para personas no autorizadas	2	3	32	Usuarios que ingresen a la información sin que tengan autorización a la misma.	Validar constantemente los accesos a la información de personas autorizadas.
2	Especialista de seguridad	6	Rotación de personal	Empleados motivados	2	4	40	Este año se dio el cambio de la persona que cubría el puesto y contratar a una nueva conlleva una curva de aprendizaje que vuelve más lento el SGSI	Tener una base de conocimiento identificando los documentos importantes y la secuencia como deben ser analizados.
3	teléfono celular	6	Ladrón/intruso intentado causar daño físico o robo	Equipamiento móvil propenso a ser robado	2	3	36	Debido a la movilidad entre sedes, existe el riesgo que el equipo pueda ser robado.	Evitar tener información en el equipo, recomendable tenerlo todo en OneDrive

Fuente: elaboración propia, con información de investigación de campo.

El cuadro 10 se describe un ejemplo de la estructura de análisis que se utiliza en el centro de operaciones de seguridad (SOC) para registrar los riesgos del área; para explicar el registro utilizado; se toma el activo repositorio de datos, donde se toma la columna del valor del activo que tiene una ponderación de ocho, así como la columna de probabilidad con un valor de dos y la columna de impacto con un valor de tres; estos datos son multiplicados entre sí para poder obtener el valor de 48 que corresponde al nivel del riesgo del activo. Con este resultado se utiliza la escala de

aceptación del riesgo (Cuadro 9) y el resultado es ubicado en el rango correspondiente en la tabla para poder seleccionar una acción a tomar. Con esta valoración se analiza el control que se implementa para el resguardo de la de información, como lo indica la columna de control propuesto del cuadro anterior.

En la verificación realizada se validó que el SOC están siguiendo los lineamientos de la norma ISO 27001 para el objetivo número dos, sin embargo existe activos que se encuentran duplicados en el inventario, por lo que es necesario realizar revisiones constantes para depurar ciertos errores que puedan afectar el control de riesgos implementados.

4.2.4. Plan tratamiento de riesgos

El plan de tratamiento de riesgos es un documento que detalla cómo se va a actuar en el control de los riesgos. Se detallan recursos, responsabilidades y las prioridades establecidas tras la evaluación de riesgos.

Cuadro 11
Departamento de Guatemala, centro de operaciones de seguridad, plan de tratamiento de riesgos SOC

ID plan	Riesgo	Plan y/o proyecto	Descripción	Inicio	Fin	Responsable
1	Falta de controles y de bitácoras de los cambios a realizar y realizados conteniendo los posibles riesgos y planes de rollback.	Realizar documentación de cambios en los clientes	Documentar dentro de los casos los cambios realizados entre los clientes.	20 de octubre	Enero 2021	Gerencia SOC
2	Falta de controles y de bitácoras de los cambios a realizar y realizados conteniendo los posibles riesgos y planes de rollback.	Gestionar los cambios de sistema de atención de clientes	Se solicita plan de control de cambios incluyendo el rollback, riesgos y ATP de pruebas que fueron realizadas, el cambio se deber registrar y autorizar.	20 de noviembre	20 diciembre	Gerencia SOC

Fuente: elaboración propia con información de investigación de campo.

Como se muestra en el cuadro 11 se muestran dos riesgos considerados como críticos y que necesitan la atención los cuales tienen fechas asignadas para ser trabajados

por la gerencia del SOC. El responsable del seguimiento, actualización, así como la planificación de los controles es el especialista de seguridad con el fin de gestionar adecuadamente los riesgos que puedan impactar negativamente en la organización.

El centro de operaciones de seguridad (SOC) si cuenta con un plan de tratamiento de riesgo de la seguridad de la información que permite proponer los controles necesarios para mitigar los riesgos de los activos de información.

4.3. Controles definidos sobre los activos de información del centro de operaciones de seguridad (SOC)

El centro de operaciones de seguridad está enfocado en el aseguramiento, la confidencialidad y la integridad de la información sensible de los clientes. Es de importancia mencionar que dentro de la norma ISO 27001 se encuentra el Anexo A que es el documento que norma y que sirve como guía para la implementación de los controles de seguridad.

El Anexo A de la norma ISO 27001 está integrado por 14 secciones numeradas desde la A. 5 hasta A. 18.

Cuadro 12
Departamento de Guatemala, centro de operaciones de seguridad, objetivos de control y controles de referencia

Anexo A	
Controles	Secciones implementadas en SOC
A. 5 Políticas de Seguridad de la Información	✓
A. 6 Organización para la Seguridad de la información	✓
A. 7 Seguridad de recursos humanos	✓
A. 8 Gestión de activos	✓
A. 9 Control de accesos	✓
A. 10 Criptografía	✓
A. 11 Seguridad física y ambiental	✓
A. 12 Seguridad en Operaciones	✓
A. 13 Seguridad en las comunicaciones	
A. 14 Adquisición, desarrollo y mantenimiento de sistemas	
A. 15 Relaciones con los proveedores	✓
A. 16 Gestión de incidentes en seguridad de la información	✓
A. 17 Aspectos de seguridad de la información de la gestión de continuidad del negocio	✓
A. 18 Cumplimiento	✓

Fuente: elaboración propia, con información de norma ISO/IEC 27001:2013

En el cuadro 12 se detallan las secciones que el centro de operaciones selecciono para adaptarlas a las necesidades de sus actividades. Cabe mencionar que el principal criterio para seleccionar los controles es mediante la gestión del riesgo del centro de operaciones de seguridad (SOC).

Es importante mencionar que la implementación de los controles no solo se limita al centro de operaciones de seguridad, si no involucra a otros departamentos como por ejemplo: recursos humanos, áreas comerciales, proveedores entre otros.

Para esta reevaluación se pueden describir algunos controles que son aplicados en el centro de operaciones de seguridad.

Cuadro 13

Departamento de Guatemala, centro de operaciones de seguridad, controles definidos en el SOC

Sección del anexo	Nombre	Control
A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A.6.2.1	Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles
A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados en la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes a su cargo.
A.8.1.1	Inventario de Activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información y se debe elaborar y mantener un inventario de estos activos.
A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.11.2.5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
A.12.1 2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información

Fuente: elaboración propia, con información de norma ISO/IEC 27001:2013

Como se puede apreciar en el cuadro 13, por medio de la revisión realizada y con base al Anexo A, se valida que la unidad objeto de estudio aplica los controles pertinentes definidos a las actividades que realiza el SOC; el equipo de seguridad decide que controles se ponen en marcha para garantizar la protección de datos y activos de la información.

Uno de los controles que ha aportado una mejora en las actividades de los colaboradores de la unidad de estudio es el control de teletrabajo; ya que se conocen las circunstancias en las que los empleados trabajan permitiendo identificar los riesgos a los que está expuesta la información. Sin embargo no se realizan actividades de revisión correspondientes; ya que no hay registro de las actualizaciones del control implementado.

Es recomendable llevar a cabo algunas acciones como: definir responsabilidades para la administración de los controles, medir y monitorear la efectividad de esos controles y realizar acciones para corregir fallas con el fin de lograr los objetivos propuestos.

4.4. Efecto en la demanda de servicios del centro de operaciones de seguridad a partir de la implementación de la norma ISO 27001:2013 en el año 2020

Implementar ISO 27001 impulsa a las empresas a ser más productivas, es importante que se comprenda la responsabilidad que se adquiere cuando se trata con información sensible de los clientes, demostrando que la seguridad de la información es una prioridad para la organización.

El centro de operaciones de seguridad, al iniciar de sus operaciones contaba con algunas buenas prácticas propuestas por el Gerente del área, estas obtenidas y puestas en marcha en la organización por experiencias anteriores en el resguardo de información. Las mismas no estaban respaldadas por una certificación que garantizara que los procesos de seguridad estuvieran estructurados y coordinados correctamente y que los mismos cumplieran con las expectativas de los clientes.

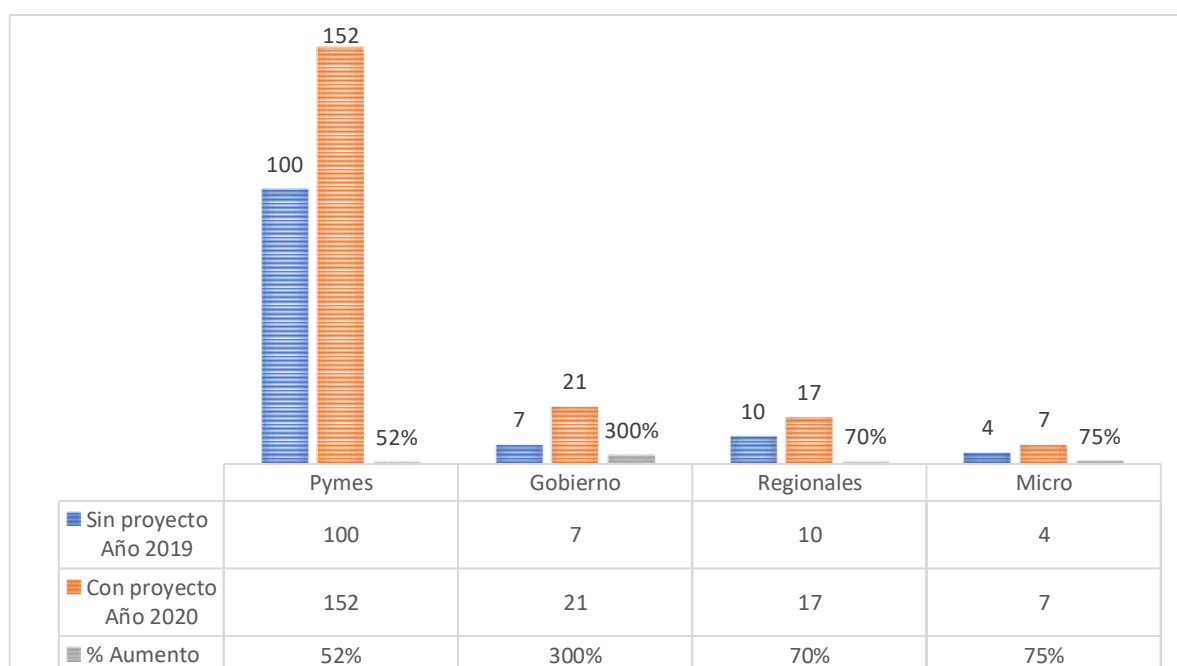
Los controles establecidos en el SOC, no se encontraban avalados por una guía para conocer si estaban implementados de manera correcta y eran funcionales a las actividades diarias. Por tal motivo se evaluó la posibilidad de certificar el área; pues

se buscaba obtener la confianza de los clientes, y la preferencia en los servicios de ciberseguridad que brinda el SOC.

La seguridad de la información se basa en preservar la confidencialidad, integridad y disponibilidad, por tal motivo la implementación de la norma ISO 27001 aporta mejoras a los procesos empresariales internos, incluyendo todos los sistemas implicados en el tratamiento de la información dentro de la empresa.

Tras la implementación del sistema de gestión de la seguridad de la información en el SOC, no solo se logró la manera correcta de resguardar la información interna y la de los clientes, si no también influyo en obtener otros beneficios como; la reducción de costos, la mejora de la reputación organizacional, lo que ha repercutido en un ingreso mayor de flujo de trabajo en el centro de operaciones de seguridad.

Gráfica 1
Departamento de Guatemala, centro de operaciones de seguridad, incremento de clientes con servicios de ciberseguridad



Fuente: elaboración propia, con información de investigación de campo.

Para establecer el efecto que ha tenido la implementación de la norma ISO 27001 en la unidad de estudio, se procedió a verificar el historial de control de clientes; dicho

historial se encuentra clasificado por tipo de empresas que adquieren los servicios SOC.

En la gráfica 1 se encuentran los clientes que poseen servicios de ciberseguridad brindados por el centro de operaciones de seguridad (SOC), estos están clasificados en cuatro grupos que son: pequeñas o medianas empresas (Pymes), empresas gubernamentales, empresas que se encuentran en el extranjero y las microempresas.

Comparando el año 2019 que es cuando no se contaba con la implementación de las ISO se cerró el año con 121 clientes. Tras la implementación de la norma ISO 27001 hubo un incremento del **62.81%** que corresponde a 75 clientes nuevos clientes que optaron por contratar los servicios del centro de operaciones de seguridad por el simple hecho de contar con una certificación que respalde los controles para el resguardo de los activos de información, cerrando ese año con 197 clientes. El efecto de la implementación es positivo, ya que ha ayudado a que se generen beneficios en el negocio y que la administración de la información de los clientes se encuentran en las mejores manos.

La norma ISO 27001:2013 brindó un peso cualitativo muy importante a la dirección, la cual es la encargada de ejercer el liderazgo del sistema de seguridad. Los beneficios logrados tras la implementación del sistema de gestión de la seguridad de la información fueron los siguientes:

- Reducir el riesgo de tener un incidente de seguridad.
- Aumento del prestigio de la organización.
- Confianza de los clientes en los servicios.
- Evitar pérdidas financieras y sanciones.
- Cumplir con los requisitos comerciales y legales para la prestación de servicios.

El efecto de la implementación es positivo, ya que ayudo a que se generen beneficios en el aumento de las ventas de servicios de ciberseguridad en un 58%. Los costos de mantenimiento de la norma ISO 27001 representan un 10% del aumento anual en los servicios. Y el ingreso neto es de 48% según la relación beneficio costo.

Derivado de los resultados obtenidos en el presente trabajo de graduación, por medio del cumplimiento del objetivo general y los objetivos específicos, los cuales fueron la

guía para el desarrollo de la investigación, se determinó que existen oportunidades de mejora en la implementación del sistema de gestión de la seguridad de la información en el centro de operaciones de seguridad, debido a que actualmente se pasan por alto algunos cambios en los registros, controles y algunas políticas implementadas con base a la norma ISO 27001. Esto permitirá la mejora continua tanto en los procesos, registros y las políticas ya establecidas en el centro de operaciones de seguridad.

CONCLUSIONES

1. Conforme a los resultados obtenidos en la investigación, se concluye que el contexto de la organización se encuentra alineado a los requisitos de la norma ISO 27001. La implementación del SGSI realizada en la organización tiene un compromiso con el cumplimiento de los requisitos legales demandado por los clientes. Sin embargo en las revisiones realizadas a los documentos vigentes del centro de operaciones de seguridad, se determinó que algunos no contaban con las actualizaciones correspondientes que afectan la eficiencia del sistema de gestión de la seguridad de la información.
2. El análisis de los riesgos que ha tenido la unidad objeto de estudio permitió determinar que la metodología adoptada para evaluar y tratar los riesgos de la información en el centro de operaciones de seguridad es la adecuada, ya que el mismo se establece de acuerdo a la identificación de los activos que tienen un valor significativo para la organización y al análisis de riesgos que ayudan a determinar las posibles situaciones y la probabilidad que estas se produzcan.
3. Conforme a la investigación realizada, se determina que el centro de operaciones de seguridad cuenta con la mayoría de los controles implementados, como lo sugiere el Anexo A de la norma ISO 27001. Permitiendo que los procesos de seguridad estén equilibrados y coordinados entre sí. Sin embargo no existe un seguimiento sobre los controles existentes para saber si son los adecuados o necesitan ser actualizados. Y así brindar oportunidades para crear metodologías que contribuyan a la mitigación de riesgos y poder incrementar el nivel de seguridad en la información.
4. Se concluye que la implementación del sistema de gestión de la seguridad de la información en el SOC basada en la norma ISO 27001, permitió una serie de beneficios como una mejora en la estructura, un mejor enfoque en los servicios; y un incremento de la cartera de clientes de 62.81%.

RECOMENDACIONES

1. Según los resultados obtenidos en la investigación, se recomienda al gerente del centro de operaciones de seguridad (SOC) y al especialista de seguridad realizar la revisión periódica de los documentos vigentes y estar al pendiente de las actualizaciones. Es por ello que es necesario implementar un control de versiones para poder conservar cada modificación de las políticas, registro, y procedimientos implementados a lo largo del sistema de gestión de la seguridad de la información.
2. La metodología implementada en el centro de operaciones de seguridad para el análisis de los riesgos es el adecuado para el tipo de negocio. Sin embargo se recomienda realizar talleres de trabajo que mantenga concientizado al equipo, ya que están relacionados con las operaciones diarias, así como con el sistema de gestión de la seguridad de la información. La falta de concientización y capacitación es una de los principales amenazas y motivos de fracaso de los proyectos de seguridad de la información en las organizaciones.
3. Se recomienda que los resultados de las evaluaciones internas realizadas en el centro de operaciones de seguridad se comuniquen con claridad y precisión, de manera que, las partes interesadas y la alta dirección utilicen esa información para la toma de decisiones y mejora de los controles establecidos para la organización. Se trata entonces de mantener actualizados los controles de la seguridad de la información con el fin de que sean los adecuados para el aseguramiento, confidencialidad e integridad de los datos.
4. Se aconseja implementar un plan de seguimiento monitoreo y evaluación ya que es una herramienta fundamental para el sistema de gestión de la seguridad de la información implementado en el SOC, con el fin de medir el avance, desempeño y los efectos del proyecto. Así mismo poder identificar los problemas y poder tomar las medidas preventivas o correctivas en los controles establecidos para no afectar los objetivos de la organización. Esto con el fin de no perder la credibilidad y confianza de los cliente y no afectar las ventas en los servicios de ciberseguridad por temas de pérdida de reputación.

FUENTES

- Baca, G. (2013). *Evaluación de Proyectos*. Editorial Mcgraw-Hill.
https://www.uachatec.com.mx/wp-content/uploads/2019/05/LIBRO-Evaluaci%C2%A2n-de-proyectos-7ma-Edici%C2%A2n-Gabriel-Baca-Urbina-FREELIBROS.ORG_.pdf
- Benítez Cascajares, J. (2011) *Gestión de proyectos: enfoque más comercial de la fase de definición de un proyecto informático*. [Monografía].
<https://hdl.handle.net/10609/6102>
- Cartes, F. (2016). *Evaluación Ex Post -SIN* [Diapositivas de PowerPoint]. Repositorio Observatorio de participación Cepal.
https://observatorioplanificacion.cepal.org/sites/default/files/session/CHILE_Fernando_Cartes.pdf
- Cohen, E. y Franco, R. (1992). *Evaluación de Proyectos Sociales*. Editorial Siglo XXI editores, s.a. de c.v.
- Córdoba, M. (2013). *Formulación y Evaluación de Proyectos*. Editorial Digiprint Editores E. U.
- Costas. J. (2011). *Seguridad Informática*. Editorial Ra-Ma
- Díaz Padilla, G. (s.f). *Proceso metodologico línea base* .Editorial Instituto nacional de investigaciones forestales agrícolas y pecuarias.
- Gómez, A.(2014). *Enciclopedia de la seguridad informática*. Editorial RA-MA, S.A.
https://books.google.com.gt/books?id=SofDwAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- González, A. (2006). *Métodos de compensación basados en competencias*. Editorial Ediciones Uninorte.
<https://books.google.com.gt/books?id=v3qclemGtvkC&lpg=PA32&dq=ciclo%20phva&pg=PP7#v=onepage&q=ciclo%20phva&f=false>

- Hornetsecurity. (2021). Seguridad informática-¿ *Qué es la seguridad informática y por qué es tan importante?*
<https://www.hornetsecurity.com/es/knowledge-base/seguridad-informatica/>
- Koontz, H., Weihrich, H., Cannice, M. (2012). *Administración una perspectiva global y empresarial*. Editorial Mcgraw-Hill.
- Mármol, A. (2019). *Project Management*. Editorial Elearning S.L.
<https://books.google.com.gt/books?id=wXfIDwAAQBAJ&pg=PA25&dq=que+es+la+linea+base+en+los+proyectos&hl=es-419&sa=X&ved=2ahUKEwibg6HitsjxAhXhnGoFHW38CLAQ6AEwBHoECAUQAg#v=onepage&q=que%20es%20la%20linea%20base%20en%20los%20proyectos&f=false>
- Medianero Burga, D. (2014). Metodología de evaluación ex post. *Pensamiento crítico No. 13* (pp. 77-78)
- Norma Técnica NTC-ISO-IEC 27001. (2013). *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos*. Editorial ISO/IEC.
- Piñola, G. (2016). *Guía práctica sobre métodos y técnicas de investigación documental y de campo*. Editorial CIMGRA
- Project Management Institute, Inc. (2013) *Guía de los fundamentos para la dirección de proyectos*. Editorial Project Management Institute.
- Rivera Martínez, F., Hernández Chávez, G. (2010). *Administración de Proyectos*. Editorial Prentice-Hall Hispanoamericana.
- Sampieri, H. (2014). *Metodología de la investigación*. Editorial Mcgraw-Hill.
- Sapag, N., Sapag, R., Sapag, J. (2014). *Preparación y Evaluación de Proyectos*. Editorial Mcgraw-Hill.

Universidad de San Carlos de Guatemala.(2018). *Instructivo para elaborar el trabajo profesional de graduación para optar al grado académico de maestro en artes. Guatemala*

Vera, P. (1997) *Guía metodológica para la evaluación ex post de proyectos*. Editorial Instituto latinoamericano y del caribe de planificación económica y social [ILPES].

Tesis

Machicao Mollocondo, S. G. (2019). *Análisis de riesgo y políticas de seguridad de información de la oficina de tecnología de información (OTI)- Una Puno 2018*. [Tesis de Maestría, Universidad Nacional del Altiplano]. http://repositorio.unap.edu.pe/bitstream/handle/UNAP/13958/Machicao_Mollocondo_Saulo_Gustavo.pdf?sequence=1&isAllowed=y

Meza Morales, J.A. (2017). *Sistema de gestión de activos informáticos en las medianas empresas ferreteras de la ciudad de Guatemala, aplicando el marco de trabajo RISKIT*. [Tesis de Maestría, Universidad de San Carlos de Guatemala].http://www.biblioteca.usac.edu.gt/tesis/03/03_5797.pdf

Morales González, C.A., Moreno Sánchez, O. E., Ortigoza Pérez, J.N. (2014). *Propuesta de un modelo de centro de operaciones de seguridad (SOC) para la fuerza aérea colombiana*. [Tesis de Maestría, Universidad Piloto de Colombia]. <http://polux.unipiloto.edu.co:8080/00001627.pdf>

Ruano Aguilar, A. E. (2010). *Proyecto de emprendimiento empresarial en el diseño de soluciones a riesgos de seguridad de la información basado en la teoría general de disuasión*. [Tesis de Maestría, Universidad de San Carlos de Guatemala].<http://www.repositorio.usac.edu.gt/5222/1/Alicia%20Eugenia%20Ruano%20Aguilar.pdf>

Páginas Web

Cisco. (2021). *¿Qué es la ciberseguridad?*

https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Guijarro.H. (29 octubre 2018). ISO 7001 y su política de seguridad de la

información.itgovernance.<https://www.itgovernance.eu/blog/es/iso-27001-y-su-politica-de-seguridad-de-la-informacion>

Organización Internacional de Normalización (octubre de 2013). *Tecnología de*

la información -Técnicas de seguridad- Sistemas de gestión de seguridad de la información-Requisitos. <https://www.iso.org/standard/54534.html>

ISOTools Excellence. (6 mayo 2015). *¿Cómo clasificar los activos de seguridad en*

un SGSI? <https://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/>

ISOTools Excellence. (23 febrero 2017). *¿Cómo realizar un inventario de activos*

de información? <https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/>

Mendoza, M. (9 junio 2018). *¿Como definir el alcance del sistema de gestión?*

Welivesecurity by eset. <https://www.welivesecurity.com/la-es/2018/01/09/definir-alcance-sgsi/>

Open Data Security ODS. (5 enero 2020). *¿Que son los servicios SOC o Centro*

de Operaciones de Seguridad? <https://opendatasecurity.io/soc-que-es-y-por-que-es-interesante-para-tu-empresa/>

Pérez, A. (21 abril 2021). *¿Cuáles son las etapas de un proyecto?* OBS

Business School.<https://www.obsbusiness.school/blog/cuales-son-las-etapas-de-un-proyecto-te-lo-contamos-en-esta-infografía>

PERÚ Ministerio de Economía y Finanzas.(2021). *Ciclo del Proyecto*.

https://www.mef.gob.pe/es/?option=com_content&view=article&id=876&Itemid=100884

Rosencrance, L. (23 julio 2019). *10 tipos de incidentes de seguridad y cómo*

manejarlos.TechTarget.<https://searchdatacenter.techtarget.com/es/tutoriales/10-tipos-de-incidentes-de-seguridad-y-como-manejarlos>

Sánchez, Y. (3 diciembre 2020). *¿Qué es el ciclo PHVA?*.Gerencie.com.

<https://www.gerencie.com/ciclo-phva.html>

Tecon Soluciones Informáticas. (2021). *La seguridad de la información.-¿En que*

se basa la seguridad de la información? <https://www.tecon.es/la-seguridad-de-la-información/>

Zona Económica. (2021) *Concepto de control*.

<https://www.zonaeconomica.com/control>

ANEXOS

Los presentes instrumentos revelan datos estrictamente con fines académicos, así como confidenciales y su propósito es evaluar la implementación y ejecución del sistema de gestión de seguridad de la información ISO 27001:2013.

Anexo 1. Entrevista estructurada sobre la evaluación de riesgos realizada en el centro de operaciones de seguridad, para su respuesta se considera un aproximado de 8 preguntas.



Universidad San Carlos de Guatemala
Facultad de Ciencias Económicas
Escuela de Estudio de Postgrado



GUÍA DE ENTREVISTA ESTRUCTURADA		
Día:	Fecha:	Lugar:
Entrevistado:	Entrevistador:	
Tema: Ejecución e implementación del sistema de gestión de la seguridad de la información ISO 27001:2013 en un centro de operaciones de seguridad en el Municipio de Guatemala, Departamento de Guatemala, año 2020.		
Objetivo Especifico: Análisis de riesgos en los activos de información en el sistema de gestión de la seguridad de la información (SGSI), implementados en el centro de operaciones de seguridad.		
PREGUNTAS	ANOTACIONES	
1. ¿Cómo se identifican los riesgos de la seguridad de la información?		

2. ¿Como realizan la valoración del riesgo de la seguridad de la información?	
3. ¿Qué criterio utilizan para aceptar los riesgos en el centro de operaciones de seguridad?	
4. ¿Como se establecen los controles para el tratamiento del riesgo de la seguridad de la información?	
5. ¿Cómo se documentan los resultados del tratamiento de riesgos de la seguridad de la información?	
6. ¿Se cuenta con la información documentada que acredite como se realiza el proceso de valoración y riesgo y sus resultados?	
7. ¿Como se realiza la identificación de amenazas y vulnerabilidades de la seguridad de la información?	
8. ¿Antes de implementar la ISO 27001 como se evaluaban los riesgos de la información?	

Anexo 2. Guía de análisis documental realizada al centro de operaciones de seguridad.



Universidad San Carlos de Guatemala
Facultad de Ciencias Económicas
Escuela de Estudio de Postgrado



GUÍA DE ANÁLISIS DOCUMENTAL

Tema: Ejecución e implementación del sistema de gestión de la seguridad de la información ISO 27001:2013 en un centro de operaciones de seguridad en el Municipio de Guatemala, Departamento de Guatemala, año 2020.

Objetivos Específicos:

- Validar el cumplimiento de la norma ISO 27001:2013 en el centro de operaciones de operaciones de seguridad (SOC).
- Análisis de riesgos en los activos de información en el sistema de gestión de la seguridad de la información (SGSI), implementados en el centro de operaciones de seguridad.
- Evaluar los controles definidos sobre los activos de información, puestos en marcha por la implementación de la norma ISO 27001 en el centro de operaciones de seguridad (SOC).

	Documento	Sección	Anotaciones
Base para validación: Norma ISO 27001:2013 Sistema de Gestión de la Seguridad de la Información y Anexo A	Objetivos	6.2	
	Políticas	5.2 A. 5	
	Procedimientos	A.12.1	
	Valoración de tratamiento de riesgos	6.1.2 literal a-e 8.2 8.3	
	Control de activos de información	A. 8	

Anexo 3. Matriz Metodológica

Tema:	EVALUACIÓN DE CORTO PLAZO DE LOS EFECTOS DE LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ISO 27001:2013 EN UN CENTRO DE OPERACIONES DE SEGURIDAD EN EL MUNICIPIO DE GUATEMALA, DEPARTAMENTO DE GUATEMALA, AÑO 2020.				
Problemática: Explique la problemática y el efecto que ésta tiene en el sector sujeto de estudio. (causa-efecto) Subrayar elementos clave = la causa y el efecto	En la actualidad cada día son más las amenazas y variantes de ataques que pueden poner en riesgo la información y el buen funcionamiento en la organización. No obstante realizar una ejecución e implementación de un sistema de gestión de seguridad de la información en un centro de operaciones de seguridad, disminuye los incidentes de seguridad que puedan originar consecuencias operativas, financieras, y legales graves que pueden afectar el negocio.				
Objetivo General: Debe indicar que hará y para qué lo hará Subrayar los elementos claves= la causa y el efecto.	Realizar una evaluación expost a corto plazo de la implementación de un sistema de gestión de seguridad de la información ISO 27001:2013 en un centro de operaciones de seguridad, para validar y gestionar los controles pertinentes y así asegurar la confidencialidad, integridad y disponibilidad de los activos de información.				
Preguntas de investigación (revisar su concatenación con objetivos específicos)	Objetivos Específicos (En su conjunto permiten alcanzar el OBJETIVO GENERAL)	Técnicas	Instrumento	Tipo de análisis	Muestra es necesaria para aplicar la técnica.
¿Qué procedimientos pueden aplicarse para verificar que el alcance, objetivo, políticas, registros y procedimientos del sistema de gestión de seguridad de la información (SGSI) están diseñados y aplicados correctamente al tipo de organización?	Validación del cumplimiento de la norma ISO 27001:2013 en el centro de operaciones de seguridad (SOC).	*Análisis de documentos	*Guía de análisis de documentos para validar objetivos, políticas y procedimientos del SGSI	Análisis interpretativo del alcance, objetivos, políticas y procedimientos para validar que cumplan con la norma ISO 27001:2013 numerales: 4.3, 5.2, A. 5, A.12.1	Muestra no probabilística por conveniencia.

<p>¿Cómo se pueden identificar los riesgos sobre los activos de información del centro de operaciones de seguridad (SOC)?</p>	<p>Análisis de los riesgos en los activos de información en el sistema de gestión de la seguridad de la información (SGSI), implementados en el centro de operaciones de seguridad.</p>	<p>*Análisis de documentos</p> <p>*Entrevista estructurada</p>	<p>*Guía de análisis de documentos para realizar plan de Tratamiento de Riesgos.</p> <p>*Guía de entrevista estructurada con el responsable del SGSI del centro de operaciones de seguridad (SOC)</p>	<p>Análisis interpretativo de la valoración y tratamiento de riesgo en base a la norma de ISO 27001:2013 Numerales :6.1.2 literal a-e, ,8.2, 8.3</p>	<p>Muestra no probabilística por conveniencia</p>
<p>¿Se tiene la información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información?</p>	<p>Evaluar los controles definidos sobre los activos de información, puestos en marcha por la implementación de la norma ISO "7001 en el centro de operaciones de seguridad (SOC).</p>	<p>*Análisis de documentos</p>	<p>*Guía de análisis de documento de los controles sobre los activos de información del centro de operaciones de seguridad (SOC)</p>	<p>Análisis interpretativo de los controles en base a la norma ISO 27001:2013 y anexo Numeral 8</p>	<p>Muestra no probabilística por conveniencia</p>
<p>¿Cuál sería el efecto en la demanda de servicios de ciberseguridad que ha tenido la implementación de la norma ISO 27001 en el centro de operaciones de seguridad (SOC)?</p>	<p>Analizar el efecto en la demanda de servicios del centro de operaciones de seguridad por la implementación de la norma ISO 27001:2013 el año 2020</p>	<p>*Análisis de documentos</p>	<p>*Guía de análisis de documentos sobre las políticas y procedimientos para validar que estén alineados a los objetivos de control y controles de referencia Anexo A ISO 27001:2013.</p>	<p>Análisis interpretativo de la ISO 27001:2013 Numeral: 5.2, A. 5 y Anexo A Objetivos de control y controles de referencia Numeral: A.12.1</p>	<p>Muestra no probabilística por conveniencia</p>

ÍNDICE DE ACRÓNIMOS

A continuación se presenta las siglas utilizadas para referirse de forma abreviada a los organismos, instituciones que fueron utilizados para el presente trabajo de investigación.

ABREVIATURA	SIGNIFICADO
IEC	Comisión Electrónica Internacional
ISO	Organización Internacional de Normalización
SGSI	Sistema de Gestión de Seguridad de la Información.
SOC	Centro de operaciones de Seguridad

ÍNDICE DE FIGURAS

No. Titulo	Página
Figura 1 Gestión del proyecto	8
Figura 2 Tipo de proyectos.....	9
Figura 3 Etapas del proyecto	9
Figura 4 Tipos de evaluación en los proyectos	11
Figura 5 Criterios de la evaluación expost	14
Figura 6 Instrumentos de la linea base.....	15
Figura 7 Pilares de la seguridad de la información	17
Figura 8 Clasificación de los activos de información	18
Figura 9 Ciclo PHVA.....	26
Figura 10 Jerarquía SOC	29
Figura 11 Esquema estructural norma ISO 27001:2013.....	37
Figura 12 Estructura del objetivo de seguridad según norma ISO 27001:2013	42
Figura 13 Metodología de evaluación y tratamiento de riesgos en los activos de información.	43
Figura 14 Herramientas para la evaluación de riesgos.....	44

ÍNDICE DE CUADROS

No. Titulo	Página
Cuadro 1 Tesis relacionadas con la investigación	4
Cuadro 2 Tipos de evaluación expost.....	13
Cuadro 3 Estructura del sistema de gestión de la seguridad de la información -ISO 27001:2013	21
Cuadro 4 Validación de documentos versus norma ISO 27001	39
Cuadro 5 Hallazgos en la verificación de documentos	40
Cuadro 6 Diseño de inventario de activos del SOC	46
Cuadro 7 Matriz de riesgo – evaluación del impacto	47
Cuadro 8 Matriz de riesgo – probabilidad y ocurrencia del riesgo	48
Cuadro 9 Escala de aceptación del riesgo	48
Cuadro 10 Análisis de riesgo de los activos de información y su tratamiento	49
Cuadro 11 Plan de trataminto del riesgo SOC	50
Cuadro 12 Objetivos de control y controles.....	51
Cuadro 13 Controles definidos en el SOC.....	52

ÍNDICE DE GRÁFICAS

No. Titulo	Página.
Gráfica 1 Incremento de clientes con servicios de ciberseguridad	54