Universidad Continental

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de Ingeniería Industrial

Trabajo de Investigación

Implementación de un sistema de gestión de la seguridad de información en empresa de outsourcing Helpdesk, Arequipa 2017- 2018

Wilber Jackson Pachao Pizarro

Para optar el Grado Académico de
Bachiller en Ingeniería Industrial

Arequipa, 2019

AGRADECIMIENTO

Primeramente, agradecer a Dios por la sabiduría impartida para la culminación de proyecto a toda mi familia, por todo el apoyo brindado durante este transcurso que se realizó el proyecto, a mí a asesor Ing. Leydi Beatriz Manrique por todo su apoyo y tiempo invertido como asesor.

DEDICATORIA

Dedicado a mi Madre Rosa Pizarro García, por el cariño y el apoyo para la culminación de este proyecto de investigación.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Proteger a toda costa la comunicación , es importante a cualquier clase de organización porque se basa en salvaguardar la información que es vital para la organización, el objetivo de esta investigación va ser centrada en la realización de un procedimiento de administración protectora de comunicación esta implementación, el método a usarse llama MAGERIT, el cual parte de la identificación de los activos de una organización el mismo permitirá un aumento sustancial del nivel de seguridad de los activos de la empresa Outsourcing Helpdesk, el cual garantiza de peligros de protección de la comunicación han de ser expuestos, distinguidos, minimizados, y evaluados en forma documentadas sistemáticamente, también administre eficientemente, que sea adaptable a frecuencias que ocasionen peligros , alrededor y de desarrollo existente.

La protección comunicativa hoy en día es un arma esencial para cualquier organización, específicamente en el asegurar la información de la empresa, la seguridad es vital ya que toda la información que se maneja es física y virtual y está presente en la intranet de la organización y es considerada un activo, lo cual se considera de mucha importancia, la cual debería ser resguardada como lo que es, porque de tal depende el crecimiento de la misma, es por ello se le debe dar toda la seguridad posible, contra posibles ataques que existen en la red privada de la empresa ya sean estos externos o internos.

La presente investigación está constituida por cuatro capítulos los cuales están estructurados de la siguiente manera:

En el presente capítulo I se despliega el planteamiento del problema, los objetivos y la justificación así mismo se desarrolló el capítulo II que engloba el marco teórico y el Capitulo III en la cual se describen los aspectos metodológicos utilizados en la investigación finalmente se desarrolló del capítulo IV en la cual se desarrolla la propuesta.

ABSTRACT

Protect communication at all costs, it is important to any kind of organization because it is based on safeguarding the information that is vital for the organization, the objective of this research will be focused on the implementation of a procedure of protective administration of communication this implementation, the method to be used calls MAGERIT, which, based on the identification of the assets of an organization, will allow a substantial increase in the level of security of the assets of the company Outsourcing Helpdesk, which guarantees the dangers of communication protection. be exposed, distinguished, minimized, and evaluated in a systematically documented way, also manage efficiently, that is adaptable to frequencies that cause dangers, around and of existing development.

The communicative protection nowadays is an essential weapon for any organization, specifically in securing the information of the company, the security is vital since all the information that is handled is physical and virtual and is present in the intranet of the organization and It is considered an asset, which is considered very important, which should be protected as it is, because it depends on the growth of it, that is why it should be given all possible security, against possible attacks that exist in the private network of the company, whether these are external or internal.

The present investigation is constituted by four chapters which are structured in the following way:

In the present chapter I the problem statement, the objectives and the justification are developed, as well as the chapter II that includes the theoretical framework and the Chapter III in which the methodological aspects used in the research were finally developed. IV in which the proposal is developed

INTRODUCCIÓN

La siguiente tesis, establece un prospecto para implementar una operación administrativa para proteger la comunicación además de etapas o procedimientos que vienen a desarrollar todas las actividades de la organización, y nos permitirá seleccionar las alternativas de control respectivas acerca de seguridad e información.

Es así que resguardar dentro de la comunicación en teoría más específicos es conocida como, como todas las alternativas para prevenir y constantes del responsable sobre seguridad, incluso de empresas y medios desarrollados, que permita proteger la comunicación, busca proteger a toda costa la imparcialidad de comunicación. Se puede decir que un activo está estimado para toda información dentro de una organización teniendo su valor ya dicho propiamente definido.

La principal característica de operación de administración de protección en Informaciones como preservar imparcialidad al igual que la información de una organización, se llega por medio del estudio de análisis de peligros la visión que se encuentran los acelerados encima interactuando por medio de una organización, a continuación, colocar inspecciones útiles para desaparecer, mitigar los riesgos encontrados, para asegurar la información.

Por esto en la empresa Outsourcing Helpdesk, tiene como objeto hacer, un grupo de herramientas, operaciones y normas para asegurar toda confiabilidad integridad hasta disposición como fuente de información, para así confiar a entrar cualquier testimonio, entonces los usuarios asignados, que están disponibles es para cuando ya se necesite por los supuestos usuarios accesibles y este a igual que se creó por los dueños originales, brindar seguridad de cada actualización posible.

CAPITULO I

PLANTEAMIENTO DEL ESTUDIO

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

1.1.1. PLANTEAMIENTO DEL PROBLEMA

Es bien sabida la evolución constante y avance tecnológico ha transformado las operaciones de varias empresas hasta organizaciones en forma en cómo se comunican las personas, a cierta raíz han ocasionado riesgos y dificultades en cuanto a la integridad comunicativa. Según el informe acerca de peligros globales para 2018 publicado por Foro Económico Mundial, indicando esto a continuación. “Entonces van aumentando cada riesgo en cuanto a ciberseguridad, como palabras de su dominio como en potencia disruptivo. Los asaltos a las organizaciones grandes están por han duplicarse en cinco años y los incidentes que anteriormente se estimaban algo fuera de lo común se ha vuelto algo común.

El acceso financiero de todo incumplimiento contra la ciber seguridad está creciendo hasta notan algunos precios altos en 2017 interactuados a atraques con ransom ware, que contienen el 64% de mayoría los e-mails dañinos. Se tienen muchos ejemplos vistos se incluye el golpe de wantcry dañando a 300.000 pc en 150 estados, y el NotPetya, que provoco extravíos trimestrales de U$S 300 millones a demasiadas empresas afectadas. Una tendencia más elevada consta sobre el uso de ciberataques denominados a infraestructura de esencia y de factores industriales ,

eso hace tomar una medida a estar temido siendo lo más trágico que pueda ocasionar casos probables donde atracan podrían ocasionar un desenfreno de operaciones que tienen constantes varias sociedades complejas ".(World Economic Forum, 2018) los ataques cibernéticos han sido considerado como el principal peligro en el planeta entre lo más trágico que puede tener graves consecuencias , en los últimos años han aumentado más atacando negocios de empresas, gubernamentales y financieros etc., para ello se necesita estar al tanto de las tecnologías para así idealizar nuevas directivas que garanticen seguridad eliminando riesgos de ataques cibernéticos.

1.1.2. PLANTEAMIENTO DEL PROBLEMA

A) General

¿Cómo la implementación de una (SGSI) puede controlar o minimizar los riesgos de los ciberataques en la empresa de Outsoursing helpdesk?

B) Problemas Específicos

- ¿Cuáles son los problemas que se enfrenta la empresa de Outsoursing helpdesk en temas de seguridad de la información, periodo 2017 - 2018?

- ¿Cómo prevenir los riesgos de los ataques cibernéticos en la empresa de Outsoursing helpdesk, 2017 - 2018?

1.2. OBJETIVO

1.2.1. OBJETIVO GENERAL

Ejecutar y asegurar la implementación del sistema de gestión de la seguridad de información, para la empresa Outsourcing Helpdesk, Arequipa 2017 -2018

1.2.2. OBJETIVOS ESPECÍFICOS

- Realizar la implementación de un plan del tratamiento de riesgo de la empresa de Outsoursing helpdesk, el cual identifique y detalle las accione a apropiadas a tomar por la alta gerencia, responsabilidades y propiedades para el manejo de riesgos de la seguridad.

- Implementar controles seleccionados, para así satisfacer los objetivos.

- Implementar un programa de capacitación y conocimientos.

- Manejar las operaciones del SGSI.

- Manejar los recursos del SGSI.

- Implementar los recursos y controles que aseguren una rápida respuesta ante cualquier incidente de seguridad.

1.3. JUSTIFICACIÓN

Con esta investigación ayudaremos a fomentar una cultura para prevenir y hacer detección de peligros de la comunicación, de la organización de Outsoursing helpdesk, se brinda a conocer sobre el peligro para presentar y al no estar preparado para los diferentes atraques y peligros de varios perjuicios de información o ataques cibernéticos que aparecen actualmente y al elaborar ciertos planes, hasta en prevención para evitar los riesgos mayores.

La dividimos en dos justificaciones:

Justificación tecnológica, porque es necesario estar a la vanguardia de la tecnología ya podamos asegurar nuestro activo como información, una administración de en la comunicación expresa el compromiso acerca de organización a salvaguardar su contenido , y provee elementos necesarios para la gestión eficiente a los peligros, que puedan atentar, en la protección de la información de la

organización, dando indicio confianza en todas las partes interesadas, y esto es muy importante, y esencial para el fundamental para el progreso, incremento y la sostenibilidad de una organización.

Realizar una operación administrativa de resguardo quiere decir que la empresa siempre va comprometida relacionada a la confiabilidad de la información, y hacer un procedimiento, modelo de seguridad, el cual tiene como objetivo una estrategia eficaz, la cual tiene que ser especificada sobre la ejecución del plan.

La tecnología está al alcance de todos, la vulneración de cualquier información también se encuentra en todo lugar, dentro de nuestros hogares, familia, amigos etc. por tal motivo la realización de gestionar reguardo comunicativo permitirá a cada organización fortalecer integralmente a cada colaborador, los puntos fundamentales de seguridad corresponden a la disposición de comunicación, los cuales encaminan para forjar y fomentar informes y llegar a todo su entorno.

1.3.1. DESCRIPCIÓN DE VARIABLES

Las variables por las que optaremos para esta investigación son fundamentales para la realización de hechos que propondremos; basándose en seguridad de información así tanto en la infraestructura y software.

Variable Independiente

- Implementación de un (SGSI).

Variable Dependiente

- Riesgo de seguridad dentro de la empresa de Outsoursing helpdesk.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DEL PROBLEMA

De acuerdo a Bustamante, Cano, J. (2014). En su artículo: Técnicas **acerca de resguardo de anuncio a microempresas. Cuaderno Activa, 6, pp 71-77**.

Entonces el hecho acerca de las tecnologías de la información, se da la necesidad de resguardar o proteger la información manejada por varios sistemas en la relevancia fundamental para toda organización. En este concepto nacen ciertos grupos de administración en comunicación (SGSI), siendo importantes para una realización de sistemas y constante. En el presente apartado se hace la connotación de técnicas que ocasiona constancia acerca de los más resaltante siendo protectora en cualquier información y la aplicabilidad de acuerdo a las microempresas. La metodología en investigaciones relacionadas con el anuncio: ISO 27001:2005 y el tiempo PHVA. La metodología usada en esta investigación es la siguiente:

La técnica ciclo Deming o PDCA, es una organización que abarca la administración protectora de información (SGSI), que localiza lugares débiles adentro de la estructura y organización y verifica recursos valiosos para idear procedimientos de protección eficiente. Esta técnica ha siendo confiada a disposición del activo de cualquier organización sólida.

En conclusión, Bustamante, G. & Cano lleva acerca de la metodología del ciclo de Deming, en gestiona miento de seguridad enunciativa permitiendo abarcar pilares vulnerables dentro de una organización ,posee herramientas de evaluación a desarrollar operaciones medios

de protección posibles a una estructura también al bajo presupuesto.(Maldonado, Andrés y Cano, 2014)

Referirnos a la realización e evolución constante de las nuevas tecnologías de la información se demandan mayor esfuerzo a garantizar la reguardarían informativa en una compañía, hoy día está expuesto a constantes peligros y amenazas que están en contra de la información de una organización, hoy en día hay normas vigentes que regulan y exigen mayor protección a privacidad en una organización, las organizaciones se debe gestionarla información, especificado en estándares de seguridad óptimos adecuado para cado uno de ellos, el propósito es entablar y mantener un estado de seguridad del activo llamado información, alineando objetivos y necesidades dentro de la organización, compuesto con estructura adentro de la organización designado responsabilidades y roles, en conjunto de políticas, procedimientos y procesos permitiendo gestionar cualquier riesgo de manera óptima y adecuada que atenten con la autenticidad, confiabilidad, y disposición de cualquier información.

Hacer la óptima realizable de protección de comunicación muy predecible, para empresas que realicen una estructura técnica firme y notable, a fin de tratar de prevenir ataques con objeto de saber el actual estado de seguridad de bienes dentro de la empresa de Outsoursing helpdesk.

- Diagnosticar ataques que coloquen un total riesgo para cualquier medio de testimonio de una empresa.
- Determinar las alternativas de seguridad y mecanismos a implantar una minoría del impacto en lugar de probables extracciones de eficacia e disponibilidad hasta la fiabilidad de información dentro de una organización.

2.2. BASES TEÓRICAS

La empresa de Outsoursing helpdesk, es una estructura que se dedica a brindar servicios relacionados con la tecnología de y Outsourcing, especializada de tercerización de gestión de mesa en ayuda hasta soporte en sitio, otorgando un servicio continuo e integral, la gestión de este servicio permite que nuestros clientes, no se preocupen por la administración va del

proceso de ciertas solicitudes en soporte, ya sea presencia o a distancia, se brinda tres niveles de gestión de mesa de ayuda.

- Primer nivel: técnico de modo remoto para consultas o atenciones de incidentes que no se requiera en forma presencial.
- Segundo nivel: soporte presencial en el sitio para incidentes que se requiera atender en forma presencial, para la solución del problema.
- Tercer nivel: cuando las soluciones de los problemas son más complejos a resolver, y se requiera de especialistas.

Por tales motivos la organización se enfrenta a riesgos como el hacking, ataques informáticos, phising etc.

Hacking: Se puede definir como la busca permanente del conocimiento en relación a los medios comunicativos, sus puntos de protección, al igual que lo resaltante, a manera de prever y las tenacidades para evitar a cualquier que conoce apara aplicarlo.

Ataques informáticos: Un golpe de información es un ataque idealizado e intencionado ocasionado por uno o más individuos a una maquina comunicativa. Los ciberataques en grupo pueden ser sucesos por individuos llamados **piratas de la informática** dedicándose a dañar para hurtar información, espionaje, con fines de lucro ya sean económicos, el hecho en procedencia de atacar consiste en tomar alcance de una debilidad del software, por medio del hardware, hasta en individuos relacionados al lugar, y a cambio sacar provecho ya que está comprobado q los ciber ataques se hacen con una finalidad económica.

Phishing: Se utiliza para señalar la técnica más utilizada por los ladrones de computadoras, para engañar y cometer actos fraudulentos con información confidencial de manera fraudulenta, como contraseñas, información detallada sobre la tarjeta de crédito o datos del banco de un sujeto que llegan a su destino. la víctima El estafador se llama phisher, utiliza métodos de ingeniería social que el sujeto transfiere a una empresa confiable, aparece la comunicación electrónica oficial, incluso mediante correos electrónicos, mensajes rápidos en redes sociales, etc. Empieza a enviar malware o llamadas telefónicas

.

La compañía de Outsoursing helpdesk maneja información clasificada de las compañías que realizan los niveles que llegan, por lo que es importante contar con un SGSI de la organización.

Tener seguridad comunicativa. Es la protección de la integridad, la confianza y la disposición de un testimonio, y el intérprete es tan confiable y accesible. "Fundamentos de la seguridad de la información": (Peltier, 2005), las reglas de salvaguardas comunicativas, las reglas de seguridad en la información y la información.

Otro punto que toca (Peltier, 2005) en su libro "Fundamentos de la seguridad de la información": que indica varias alternativas de protección de la capacidad, como una piedra angular de la construcción perfecta de la seguridad en la organización, debido a los mismos documentos de documentos. El papel externo. y el papel interno

El medio de operación informativa es una herramienta que presenta la alta gerencia de una organización para llevar y relacionarse con un área determinada, así como el área de TI. El propósito principal de un SGSI, es el de proteger los sistemas de información dentro de la organización, contra amenazas y eventos que intentan, como la divulgación, destrucción o interrupción, de una manera no autorizada. La interacción de una organización se considera uno de los activos más valiosos de toda la compañía, lo que implica protegerla de cualquier amenaza que exista en diferentes medios físicos y electrónicos dentro de una organización, por este motivo debe asegurarse con la protección necesaria, durante el almacenamiento, el tratamiento el regojo y uso.

La implementación de una SGSI de una organización es una actividad de mejora y constante, el cual involucra a toda la organización y busca la preservación de los principios siguientes:

- **Confiabilidad,** se tiene que asegurar que solo los colaboradores capacitados, tengan los accesos a la información dentro de la organización.

- **Disponibilidad,** Es el aseguramiento del total de la información y a su vez, que esta esté disponible y a disposición de todos los colaboradores autorizados.

- **Integridad,** Se debe asegurar que la información no sea corregida, sin el debido permiso.

- **Autenticidad,** Se tiene que proteger la tenacidad informativa, eso quiere decir que el emisor de la información sea quien dice ser, y no un suplantador.

- **Trazabilidad,** Se usa con un monitoreo e identificación de cualquier proceso que se realice en la información, desde el inicio hasta el destino final.

2.2.1. FUNDAMENTOS TECNOLÓGICOS

Los controles de protección informativa, no solo vienen a ser técnicas que se encuentra relacionados con el sistema tecnológico informativo, es una combinación de varios tipos de controles, como documentación, procedimientos controles que son necesarios dentro de una organización.

Cuando inicia una interacción de protección informativa se generan conjuntos de reglas en seguridad responsabilidades hasta controles necesarios adentro de una estructura. El Sistema informativo de anuncio consta de varios procesos de la seguridad que se encuentran unidos en conjunto y relacionados entre sí.

En un grupo administrativo se necesita participación activa de toda estructura, para así evalúa e implementar le planeamiento, la identificación y la implementación de todos los medios de protección a tomar para la seguridad de base informativa.

Cada recurso tecnológico de cada empresa, así como La empresa de Outsoursing helpdesk, están en relacional con el conocimiento y los procesos aprendidos hasta el día de hoy, y combinado con los avances tecnológicos que ayudan a una organización el aseguramiento de la información, como activo muy importante dentro de ella.

Cada recurso y patrimonio de una empresa puede ser físico por ejemplo ordenadores servidores firewall etc. y también tenemos los lógicos como software licencias cloud, servidores virtuales, antivirus etc. estos varían dependiendo del rubro de cada organización o empresa.

Dentro los físicos (Hardware) tenemos los siguientes

Servidor de datos: En términos informáticos un servicio viene a ser una clase se software que se ejecuta varias tareas, el termino también se va a referir a la carpeta que se emplea como este software, un equipo con el propósito de brindar datos de modo que algunos que están en su misma red para que puedan utilizarlos. Ejemplo los servidores web, en este

momento este término se puede referir a todos los equipos que almacenan y manejan los sitios web, en este momento el más utilizado por las compañías es el hosting, y como alternativa el servidor HTTP, que tiene la función de un equipo el cual maneja la entrega de los componentes de la página web como respuesta a solicitudes y peticiones y solicitudes de todos los navegadores de los usuarios. Los documentos de cada sitio web que se almacenan y realizan el proceso en una misma carpeta. Hay mucha connotación de personas, pero posee la función a la misma de compartir y proporción entrada a los servicios.

Firewall: Identificar un término en español corta fuegos, viene a ser equipo o dispositivo que va a configurarse configura con especificas reglas y siguiendo algunos de los criterios que forman parte de una red o sistema, posee la capacidad de impedir el acceso termino firewall es de origen inglés, y en estos últimos años ha adquirido un uso especializado en el ámbito de la informática. El firewall viene a ser un aparato configurado con determinadas normas y siguiendo diversos criterios que forman gestionada o red, se busca impedir la entrada que no llegue tener autorización como contrapartida permite interacciones autorizadas sin impedimentos.

El firewall está yendo a ser para los usuarios que navegan y no son autorizados de internet que no estén autorizados e ingresen a la red privada (intranet). Así mismo realizara el bloqueo de aquellas aplicaciones que con anterioridad se haya prohibido el ingreso, prevalece el firewall que otorga protección correcta a cualquier red, pero no debe destinarse incorrecta, y a veces se necesita añadir más elementos de seguridad para realizar de una fuerte manera y menos vulnerable.

Dentro los Lógicos (Software) tenemos los siguientes:

Cloud computing: Viene a ser una manera de almacenar información importante a través de internet, la cual estará disponible para los usuarios sin necesidad de tener un amplio conocimiento para usarla, es conocida también como computación en la nube.

Es una nueva forma de ampliar el negocio ofreciendo los servicios a través de internet, todas las personas en todos los países que tengan acceso a la red pueden acceder a la información colgada en la nube, sin necesidad de contar con una gran infraestructura.

Cloud Computing son servicios que se realizan desde internet encargados de atender las peticiones de los clientes en cualquier momento y lugar.

Antivirus: Son aplicaciones de software que serán ideadas y diseñadas como medida de seguridad contra los malware, virus informáticos y resguardar datos hasta se encarga del

correcto funcionamiento de los sistemas informáticos, contra aquellas opciones que tengan un código maligno, también software malintencionado que se presenta para alterar o destruir el desempeño de los equipos de cómputo.

El funcionamiento de este antivirus consta de la comparación el nombre o código de cada archivo que se revisa en cierta forma de información donde se vienen almacenando los conocidos códigos virus y seleccionar el elemento que pueda dañar cualquier sistema. y eso determina si se trata de un elemento que podría perjudicar un sistema.

Algunos recursos lógicos permiten la relación seleccionada con personas, también la realizan hacia los colaboradores de cierta organización, los recursos humanos, colaboradores combinados con tecnológicos, vienen a ser puntos importantes dentro de una organización, la combinación varios recursos garantiza siendo posible establecer un sistema para gestionar eficientemente incluso posible para organizar algún proceso de cada organización o servicio brindado o de un producto específico.

Dentro todo el sistema de seguridad, cada personal contratado y dedicado a esta área en la empresa deben ser personas idóneas e integras ya que ellos manejan información muy importante de la organización, así como confidencial, los personales tienen que tener certificaciones ya necesarias las cuales garanticen los cumplimientos de varios estándares que acrediten el nivel de protección que pueden brindar a la empresa.

Se tiene como parte de la seguridad, tecnologías de autentificación tales al control accesos, reconocimiento de voz o fácil o de retina implando en áreas donde la seguridad debe validarse por esas métodos, como por ejemplo el área de servidores o todos aquellas áreas que generen recursos valiosos para la organización, se deben implantar tecnología necesaria, para mitigar la vulnerabilidad y el acceso a personas no autorizadas, también lograr el óptimo funcionamiento de los módulos de la empresa el cual conlleva el funcionamiento correcto y que cada uno de estos recursos se utilicen en el momento justo, generar estándares de calidad. Tanto los recursos humanos y tecnológicos entre más actualizados estén con diversos estándares y normativas el funcionamiento de la seguridad en cualquier organización será optimo, para garantizar la seguridad de la organización se debe entablar los mecanismos que actúen en medida de medios de la empresa, los recursos tecnológicos como los humanos son el eje fundamental de para no dejar en peligro a la información de la organización y los demás activos de una estructura , tienen que ser estructurar reglas y normas que indiquen los debidos usos que pueden ser según su clasificación, tenemos los

detectivos, correctivos y preventivos. Cada uno de los mencionados cumple una función única y se utilizan en un momento determinado,

Detectivo.- Detecta o identifica, algún evento no autorizado y lo registra en la bitácora de incidencias.

Correctivos. - corrige las anomalías presentadas en un sistema o eventos de errores.

Preventivo. - previene antes que se suscite algún incidente ya sea un peligro o proceso peligroso que sea perjudicial que afecte directamente ala una organización.

Se debe considerar incluso todas las herramientas y procedimientos de alguna a otra forma que ayudan al control de seguridad de una organización, entonces no se convierte en un sistema totalmente seguro, puede ser que esta sea un sistema robusto y libre de los ciberataques, pero no se puede confiarse por completo la seguridad de una organización, ya que se debe tener en cuenta de lo tecnológico avanzando de una manera mucho más rápida y todo lo aplicado a una empresa va quedando obsoleto e inseguro y vulnerable mientras los años van pasan a la organización debe estar actualizada ya sea en recurso humano como tecnológico viene a ser un tema de mucha importancia para una organización que debe importar la información además tiene como un activos más dentro de ella, las nuevas tecnologías ayudan a contra restar cualquier amenaza ya sea externa o interna, en conclusión entre más se minimice los riesgos en una organización, se evidenciara la mejoría de su sistema de seguridad.

Todos los atraques cibernéticos informáticos, se vienen dando hace ya tiempo atrás y con paso del tiempo y el avance se han vuelto mucho más fuertes y frecuentes, eficaces y difíciles de identificar debido a varios tipos de herramientas desarrolladas por quien tira un atraco, quien tiene como objetivo vulnerar o robar información puede ser para modificarla, comercializarla y desestabilizar una organización, por eso es tan importante a implantación de una SGSI.

También estas amenazas pueden venir de un miembro de la organización no capacitado que no tenga los procedimientos claros y establecidos dentro de un sistema, ya sea cómo contraseñas expuestas, sesiones abiertas descuidos de seguridad, etc. estos ya sean intencionales o no intencionales.

Se registras variedad de ataques que atentan con los recursos de una organización ya sean estos los humanos y tecnológicos, tales trashing, phishing, ataques de autentificación, todos con el fin de atacar un proceso o modulo específico dentro de la organización. Hoy en

día los ataques cibernéticos son muy comunes en cualquier tipo de organización, ninguna organización o persona común esta excepto de un ataque informático, por tal motivo se necesita implantar las técnicas o mecanismos para salvaguardar la seguridad personal o de una organización, es muy importante contrarrestar o evitar los ataques, ya que se podrían producir perdidas incalculables dentro de una organización, siempre se debe dar importancia a la protección de la seguridad de la información para cualquier organización y que no se puede olvidar porque esta es un pilar dentro de ella y estar en una continua mejora de todo el manejo de gestión de la información, si no existiera la seguridad tampoco habría confiabilidad en la información

2.2.2. METODOLOGÍAS EXISTENTES

En la empresa existe normas se seguridad en base a manuales de buenas prácticas que ayudan a la empresa a disminuir los impactos de amenaza de un posible ataque cibernético para ello tenemos las siguientes

Por ejemplo, en análisis de riesgo podemos tomar métodos como:

2.2.2.1. MÉTODO DE ANALISIS DE RIESGOS

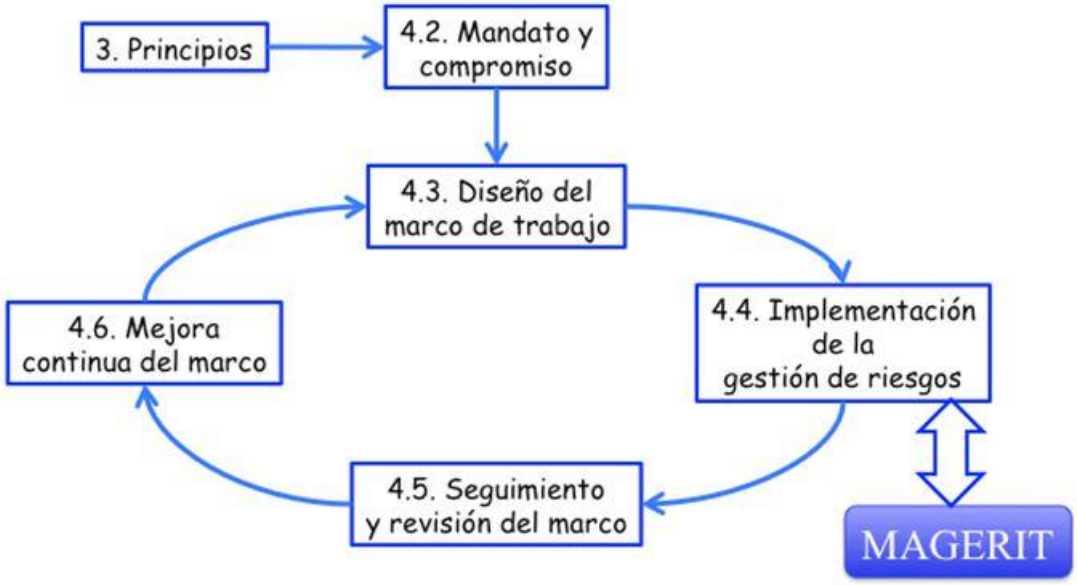
Entre los métodos tenemos el siguiente:

MAGERIT

Magerit es un método de gestión y análisis de riesgo que implica la evaluación del impactó en un ataque de seguridad, e identificándolas amenazas que asechan al sistema de información, dentro un marco de un proceso de administración, el objetivo de Magerit es la implementación del procedimiento de la gestión de riesgos dentro de una estructura de trabajo, para que los órganos del directorio acaten y se tome las decisiones respectivas teniendo en cuenta los riegos expuestos del uso de los métodos de información.

Tiene distintos enfoques que son compatibles con TI, por ejemplo, sistemas seguros o inseguros y en la realidad de la empresa. Magerit persigue un enfoque metódico, que no tiene nada que ver con la improvisación, ni depende de la resolución de los analistas.

Ilustración 1:Magerit



Fuente: ISO 31000 – Marco de trabajo para la gestión de riesgo.

2.2.3. NORMAS Y ESTÁNDARES

ISO/IEC 27000:

La presente norma facilita una visión de todos los componentes de la serie 27000, la cual indican, Esta norma proporciona una visión general de las normas que componen la serie de normas 27000 y un corta descripción de los métodos y pasos a seguir para la implementación, establecimiento, monitorización y Mejora de una SGSI.

ISO/IEC 27004:

En su introducción la norma ISO 27004 se define como: “El empleo de este estándar permitirá a las organizaciones dar respuesta a los interrogantes de cuán efectivo y eficiente es el SGSI y qué niveles de implementación y madurez han sido alcanzados. Estas mediciones permitirán comparar los logros obtenidos en seguridad de la información sobre períodos de tiempo en áreas de negocio similares de la organización y como parte de continuas mejoras”.

ISO/IEC 27005:

Publicada la tercera edición en Julio de 2018 con actualizaciones respecto a requisitos de norma ISO/IEC 27001:2013. La presente norma proporciona las direcciones para una gestión

de riesgo de la seguridad de la información. Y está hecha como ayuda a la aplicación de una SGSI.

ISO/IEC 27006:

La presente norma define los requisitos para una acreditación y certificación de un SGSI

ISO/IEC 27007:

La presente norma son los pasos de auditoria de un SGSI, como complemento en ISO19011.

ISO/IEC TR 27008:

La presente norma, se dan los pasos para la auditoria y todos los controles establecidos para la implementación de una SGSI.

ISO/IEC 27009:

La presente norma define los requisitos para el uso de la norma ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector industrial).

ISO/IEC 27010:

La presente norma se dan los pasos para la gestión de seguridad de la información cuando se intercambian entre organizaciones o empresas, se aplica a cualquier forma de intercambio y como la difusión de la información importante en las empresas privadas como públicas.

ISO/IEC 27011:

La presente norma son los pasos de la interpretación y la implementación de una SGSI en las organizaciones del rubro de telecomunicaciones.

ISO/IEC 27014:

La presente norma sigue los pasos del gobierno corporativo de la seguridad.

ISO/IEC TR 27015:

Desde 24 de Julio, de 2017 se anuncia que no será actualizada en relación a las novedades de la norma ISO/IEC 27002:2013 aunque sigue disponible para su adquisición por parte de los interesados.

ISO/IEC 27017:

La presente norma son los pasos de la seguridad para el cloud computing formada con la norma 27002 y controles puntuales de los entornos de la nube.

ISO/IEC 27018:

Publicada el 29 de Julio de 2014. Es un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.

ISO/IEC 27021:

En desarrollo, el desarrolla los requisitos de las competencias requeridas para los profesionales dedicados a los sistemas de gestión para la seguridad de la información.

ISO/IEC 27001

La presente norma es ideada en los aspectos tecnológicos como también de los aspectos organizativos de una SGSI, cuyo objetivo es la aplicación y implementación de un sistema de gestión de la seguridad de la información (SGSI).

La presente norma incluye el ciclo de Demming el cual consiste: planificar, hacer, verificar, actuar, resumiendo (PHVA) los cuales se pueden aplicar en cada uno de los procesos, los cuales se describen en coy se puede ser aplicado a todos los procesos. Y se describe de la siguiente forma:

PLANIFICACIÓN

La planificación debe ser realizada en base a la implementación del servicio de gestión

La trascendencia se puede definir como parte del plan del servicio. La gestión de los servicios debe planificarse incluyendo los siguientes puntos.

- Alcance de los servicios de gestión
- Cumplimiento de objetivos y requisitos.
- Se debe incluir al responsable de cada proceso
- La interfaz entre los procesos y la coordinación de actividades.
- Centrarse en lo necesario para la identificación y evaluación.

HACER

Es importante que la empresa implante servicios asegurando que la información este protegido incluyendo lo siguiente.

- Inclusión de presupuesto y fondo
- Inclusión de responsabilidades
- Identificación de riesgos
- Gestión de documentos
- Gestión de equipos

VERIFICAR

Debe verificar todas las metas planeadas de la administración de servicios establecidos por la empresa para que las mismas se cumplan y se verifiquen.
La organización debe llevar una planeación para la implementación, verificación y supervisión, de todos los procesos y servicios asociados.
Entre todos los elementos que se evaluarán y analizarán:

• Los logros en cuanto a los objetivos de los servicios definidos.
• Satisfacción de los usuarios.
• Uso de los recursos.
• Nuevas tendencias.
• No conformidades.
• Análisis de resultados los cuales conllevan a la mejora.

ACTUAR

El objetivo a alcanzar en esta etapa es el mejoramiento de la eficiencia en los servicios.
Las mejoras de servicio de la organización deben pasar por una revisión, de la misma manera registrada, priorizada y autorizada, puede hacer y usar un plan para mejorar el servicio para controlar la actividad.

La organización puede llevar a cabo una serie compromisos y actividades con las cuales se recabara datos para la realización de las evaluaciones tanto comparativas y de capacidad de la organización, también actuar en la implementación e identificar y planificar las mejoras

necesarias, es necesario considerar las contribuciones realizadas en el sistema de gestión de seguridad de la información ISO 27001. La política y los procedimientos de seguridad deben revisarse cuando sea necesario.

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS

TRASHING: Una forma de delito informático que tiene que ver con el robo, hurto y falsificación, el cual involucra un medio informático para cometer el hecho delictivo.

CONFIDENCIALIDAD: se considera a una propiedad que tiene algún tipo de información garantizando su ingreso a ella a personas autorizadas a conocerla.

ISO: Son las siglas que representa a la OI para la Estandarización organismo encargado de regular las normas de fabricación.

RIESGO: Es toda exposición a una situación donde hay una posibilidad de sufrir un daño o que ocurra un evento con efectos negativos.

VULNERABILIDAD: Es la cualidad que posee alguien o algo para poder ser herido, o recibir una lesión tanto física como emocional.

SGSI: Se utiliza para hacer mención al Sistema de Gestión de Seguridad relacionada a la información.

HACKER: Es aquel sujeto que utiliza sus conocimientos en tecnología e informática y tecnología para tener acceso de manera ilegal a sistemas q no le pertenecen.

CAPÍTULO III

METODOLOGÍA

3.1. MÉTODO DE INVESTIGACIÓN

Riesgo relativo se define como la razón de una incidencia expresa lo probabilidad de sufrir un ataque y la formula se expresa de la siguiente manera.

3.2. MÉTODO Y ALCANCE DE LA INVESTIGACIÓN

El método a usar es el descriptivo, La organización y todos los colaboradores deben tener en cuenta la seguridad de toda la información importante de la empresa. La investigación es de nivel aplicativo, ya que el objetivo de la investigación es el de implementar un SGSI en la empresa y así a su vez supervisar y monitorear los procesos en que se involucran la información esencial de la empresa siendo importante tener bien segura la información.

3.3. DISEÑO DE LA INVESTIGACIÓN

3.3.1. DISEÑO GENERAL

El diseño general empleado para esta investigación es de pre y pos prueba de las áreas de la empresa de Outsoursing helpdesk, para el presente tipo de investigación, el recojo de información importante se de forma objetiva de observación directa.

3.3.2. DISEÑO ESPECÍFICO

El diseño específico, se trabajará con un solo grupo de individuos, para ello tenemos las siguientes variables:

Y= Grupo de investigación (áreas de la empresa)

X = Aplicación (SGSI)

3.4. UNIDAD DE ESTUDIO

3.5. POBLACIÓN

La población y muestra está compuesta por las áreas administrativas y operativas de la empresa de Outsoursing helpdesk

3.6. MUESTRA

Nuestra muestra está representada en la cantidad de trabajadores de la empresa de Outsoursing helpdesk:

Tabla 1 : Áreas de Empresa

AREA	CANTIDAD
Gerencia General	1
Gerencia Administrativa	2
Área de Contabilidad	2
Área de Marketing y Publicidad	3
Área de ventas	8
Área de sistemas	3
TOTAL	19

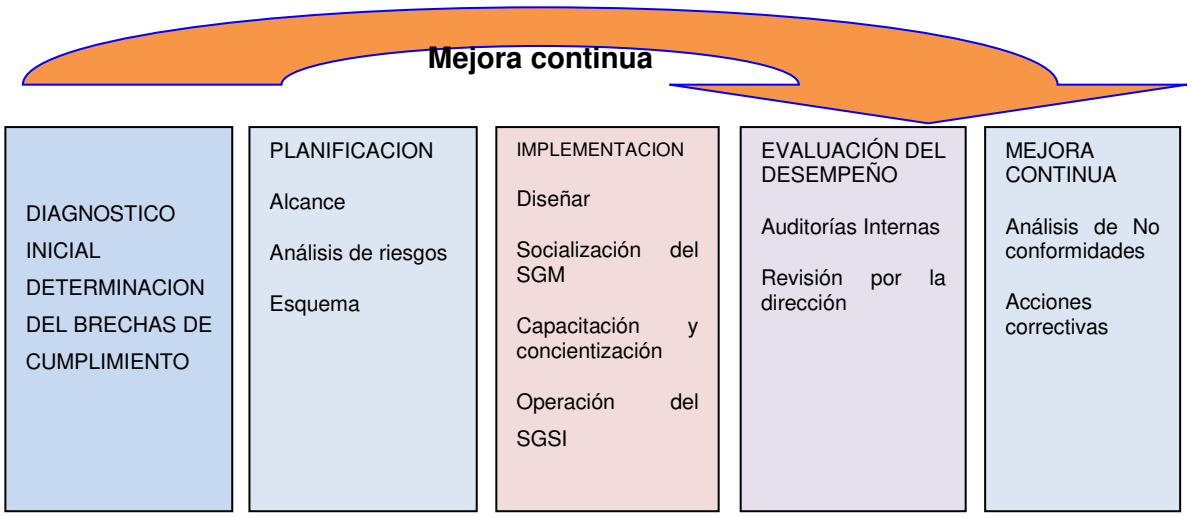
Fuente: Elaboración Propia.

CAPÍTULO IV

APLICACIÓN DE LA NORMA ISO 27001

En el presente capítulo se desarrolla el contexto de la organización, realizando el reconocimiento de ésta, así como un análisis de la situación, en las interfaces de la seguridad de la información en la empresa de Outsoursing helpdesk, con respecto a la norma ISO/IEC 27001:2015, donde se evaluará los adecuados cumplimientos de los dominios.

Ilustración 2:Cuadro de mejora



Fuente: Elaboración Propia.

4.1. ANÁLISIS DE DISEÑO

4.1.1. CONTEXTO DE LA EMPRESA

4.1.1.1. Reconocimiento de la organización

La empresa Outsoursing helpdesk es una empresa de servicios relacionada a la tecnología de la información, el cual brinda soporte técnico en tres niveles en todos los proyectos que está ubicada en la Región Arequipa, la Outsoursing helpdesk, cuenta con una infraestructura la cual se detalla en el siguiente cuadro.

Tabla 2 : Activos de la Empresa

Activo	Descripción
APLICACIONES	Software de gestión de equipos e inventarios sistemas operativos (win 7, win 10, linux) Antivirus, ,(Licencia de win7y Win 10)
HARDWARE	desktop, laptop, Ups, Firewall , servidor, camaras de vigilancia , Impresora

Fuente: Elaboración Propia.

4.1.1.2. Descripción

Inicia sus operaciones relacionadas con la tecnología y otros servicios, en el año 2006 empresa de Outsoursing helpdesk brindando diferentes servicios relacionados a las gestiones de operaciones, call center y tecnología de la información. A partir del año 2011 empresa de Outsoursing helpdesk toma su actual nombre y se especializa en servicios de información relacionados con la gestión de aplicaciones y servicios de soporte.

El sentido de ética merece destacarse como el pilar fundamental de nuestra empresa donde descansa nuestra cultura organizacional y está formada por un conjunto de valores que soportan nuestra visión y misión y guían nuestro accionar diario en la empresa.

Misión

Proporcionar servicios y soluciones que faciliten y ayuden el logro de los resultados de nuestros clientes.

Visión

Ser una de las mejores organizaciones de profesionales líderes en el servicio de suministro de tecnologías de la información para empresas corporativas de primer nivel.

Nuestros Valores

Desde sus inicios la empresa ha mantenido tres valores fundamentales: Compromiso, Excelencia y Transparencia. Estos valores ahora han sido descompuestos en seis valores individuales que responden a la mayor madurez de nuestra organización para perseguir nuestra visión y misión.

Integridad

Mantener y cumplir nuestros compromisos hacia los clientes y la empresa con transparencia y honestidad.

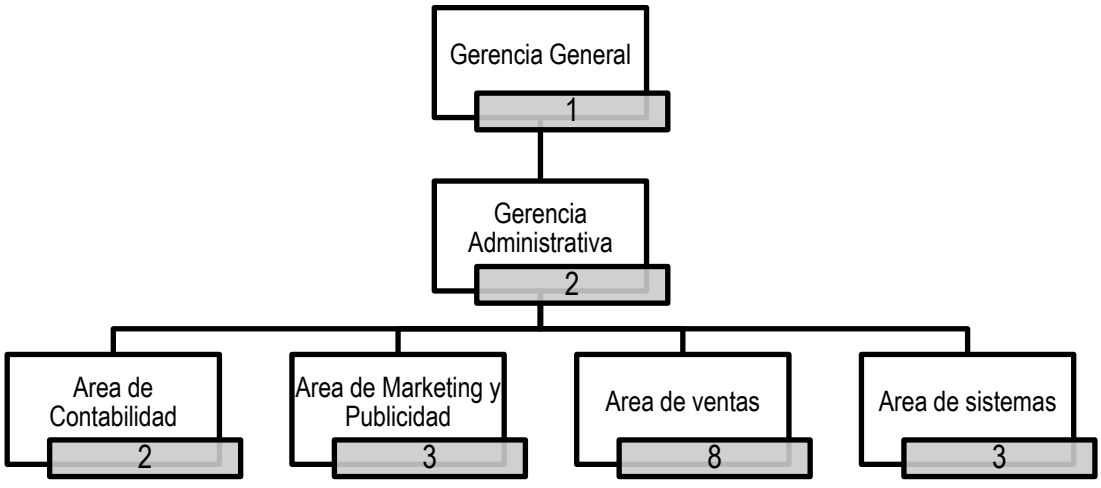
Pasión

Por ser los mejores profesionales, por nuestra empresa y por nuestros clientes.

Respeto

Tratar a los demás con paciencia, imparcialidad y dignidad.

Ilustración 3: Organigrama



Fuente: Elaboración Propia.

4.1.2. ESTADO ACTUAL CON RESPECTO ISO/IEC 27001

Para el desarrollo de la implementación de un SGSI se debe realizar pasos basados en ISO/IEC 27001:2015 después del análisis de evaluación del contexto de la planificación,

operación, soporte y evaluación de desempeño y mejoras, los cuales se convierten en elementos esenciales para actuar según la norma.

En el "Diagnóstico Inicial" se encuentra en la observación aplicada a la empresa de Outsoursing helpdesk, la cual fue realizada a Gerente, gerente de proyectos de la organización, sobre el cumplimiento de los ítems relacionados con los 12 dominios de seguridad que establece ISO/IEC 27001:2015. Las respuestas posibles están dadas por: NC, CP, CS. De acuerdo a la información que se presenta en la siguiente tabla:

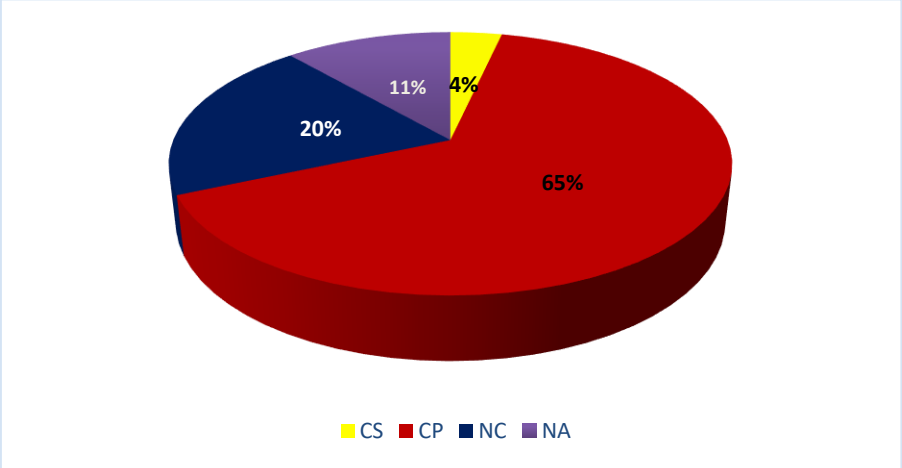
Tabla 3: Parámetros de respuesta a la encuesta

Sigla	Estado de evaluación	Descripción
NC	NO CUMPLE	No existe y/o no se está haciendo
CP	CUMPLE PARCIALMENTE	Lo que la norma requiere (ISO/IEC 27001 CP versión 2013) se está haciendo de manera parcial, se está
CS	CUMPLE SATISFACTORIAMENTE	Existe, y se está gestionando, se está cumpliendo con la norma ISO/IEC 27001 versión 2013 solicita, está documentado, es conocido y aplicado por todas las partes involucradas en el SGSI se cumple al 100%

Fuente: AutodiagnosticoSGSI_v2_09072015

Tras el análisis se obtienen los siguientes resultados:

Ilustración 4 :Gráfico Resultado Evaluación inicial



Fuente: Elaboración Propia.

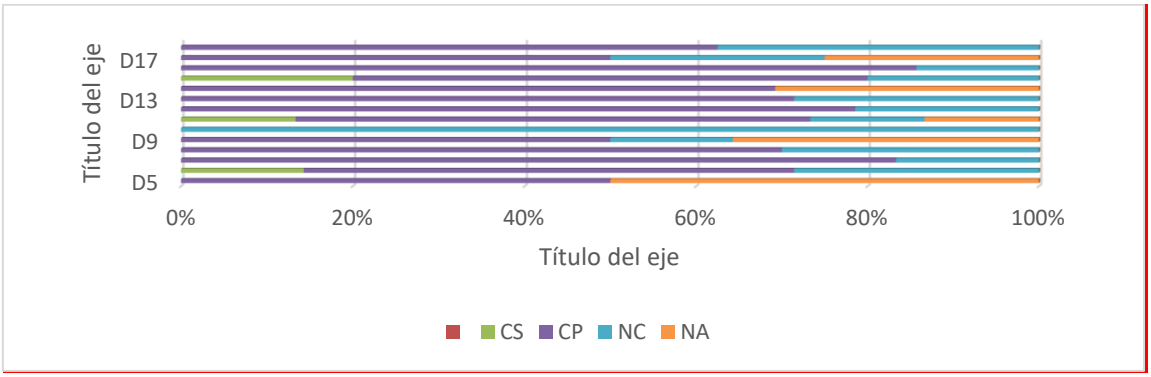
25 de los ítems evaluados no se cumplen. 68 de los ítems evaluados son cumplidos parcialmente. 4 de los ítems evaluados se cumplen satisfactoriamente y 13 no se aplica

Tabla 4: Resultados de Evaluación Inicial I&S 27001:2013

NOMBRE DOMINIOS DE CONTROL	Cumple satisfactoriamente	Cumple parcialmente	No cumple	Ninguna de las Anteriores	Items Evaluados
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	0	1	0	1	2
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	1	4	2	0	7
SEGURIDAD DE LOS RECURSOS HUMANOS	0	5	1	0	6
GESTIÓN DE ACTIVOS	0	7	3	0	10
CONTROL DE ACCESO	0	7	2	5	14
CRIPTOGRAFÍA	0	0	2	0	2
SEGURIDAD FÍSICA Y DEL ENTORNO	2	9	2	2	15
SEGURIDAD DE LAS OPERACIONES	0	11	3	0	14
SEGURIDAD DE LAS COMUNICACIONES	0	5	2	0	7
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	9	0	4	13
RELACIÓN CON LOS PROVEEDORES	1	3	1	0	5
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	6	1	0	7
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	0	2	1	1	4
SEGURIDAD DE LAS COMUNICACIONES	0	5	3	0	8
Suma total	4	68	23	13	114

Fuente: Elaboración Propia.

Ilustración 5: Resultados Evaluación Inicial



Fuente: Elaboración Propia.

La evaluación Inicial deja ver que gran parte de los elementos mínimos requeridos para el cumplimiento de la norma son inexistentes o se cumplen de forma parcial en Interfaces y Soluciones. A continuación, se describe dominio a dominio los hallazgos obtenidos por medio de la información entregada por el gerente de proyectos y algunos miembros de la organización.

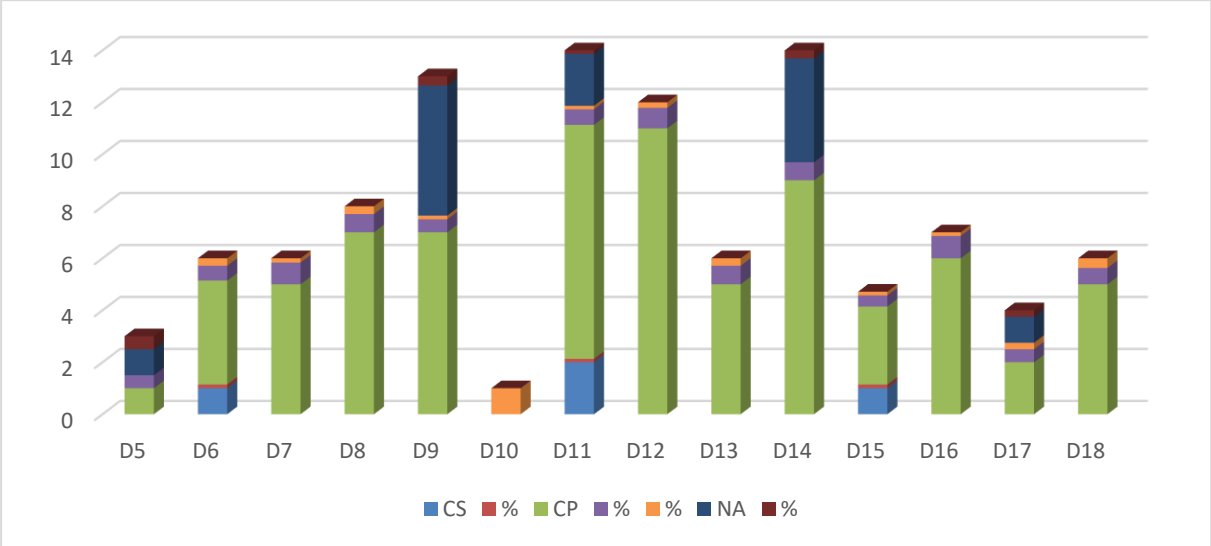
Tabla 5: Resultados de los hallazgos

NOMBRE DOMINIOS DE CONTROL	Cumple satisfactoriamente	%	Cumple parcialmente	%	No cumple	%	Ninguna de las Anteriores	%
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	0	0%	1	50%	0	0%	1	50%
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	1	14%	4	57%	2	29%	0	0%
SEGURIDAD DE LOS RECURSOS HUMANOS	0	0%	5	83%	1	17%	0	0%
GESTIÓN DE ACTIVOS	0	0%	7	70%	3	30%	0	0%
CONTROL DE ACCESO	0	0%	7	50%	2	14%	5	36%
CRIPTOGRAFÍA	0	0%	0	0%	2	100%	0	0%
SEGURIDAD FÍSICA Y DEL ENTORNO	2	13%	9	60%	2	13%	2	13%
SEGURIDAD DE LAS OPERACIONES	0	0%	11	79%	3	21%	0	0%
SEGURIDAD DE LAS COMUNICACIONES	0	0%	5	71%	2	29%	0	0%
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	0%	9	69%	0	0%	4	31%

RELACIÓN CON LOS PROVEEDORES	1	14%	3	43%	1	14%	0	0%
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	0%	6	86%	1	14%	0	0%
total	4	100%	74	100	23	100%	13	100%

Fuente: Elaboración Propia.

Ilustración 6: Resultados de los hallazgos



Fuente: Elaboración Propia.

Política de seguridad.

Se busca que la dirección brinde orientación y una base segura para garantizar que la información de la empresa este seguro por medio de requisitos, leyes y reglamentos. Se observa que la empresa tiene carencia documental de políticas, procedimientos y controles para garantizar el cumplimiento de la seguridad de información.

Organización de la seguridad de la información.

Se tiene como referencia a los controles de implementación de la gestión de la seguridad en las operaciones de la información.

Seguridad de los RRHH.

Como parte de la política de seguridad de información es importante tener garantías para para todo el personal de la empresa Outsoursing helpdesk, en base a los roles y funciones de todos los colaboradores.

Gestión de activos.

Se debe identificar cada uno de los activos de la empresa Outsoursing helpdesk, y definir el grado de responsabilidad adecuada en base a la protección, también se asegura que toda la información reciba el nivel adecuado de seguridad, determinando su importancia.

Control de accesos.

Se encarga de limitar el acceso a la información de la empresa, asegurando el acceso solo a los usuarios autorizados.

Criptografía.

Es una medida criptografía que asegura el apropiado uso del sistema de información

Seguridad física y ambiental.

Se observa que se ha tomado medidas básicas para evitar que personas no autorizadas tengan acceso físico que pueda traer como consecuencia el daño a los sistemas

Seguridad en las operaciones.

Con la seguridad en las operaciones se busca obtener correctas operaciones de procesamiento de información en la empresa. Aquí se incluyen e implementan controles contra códigos maliciosos, Backup de la información, la separación de los ambientes de operación, pruebas y registro de eventos.

Seguridad en las Comunicaciones.

Este sistema se enfoca en la protección de la información en todas las redes y sub-redes que se encargan de la transferencia de la información.

Adquisición de sistemas, desarrollo y mantenimiento.

El personal ha implementado tareas correspondientes a los procesos de adquisición de sistemas, desarrollo y mantenimiento basados en el sentido común.

Relación con proveedores.

La relación con los proveedores se ha basado en una confidencialidad asumida pero no se ha establecido un acuerdo y/o contrato formal en el que se estipulen todos los pasos de seguridad pertinente.

Continuidad del negocio.

En este dominio se hace necesario la planificación, implementación, la verificación, revisión y la evaluación planificar, implementar, verificar, revisar y evaluar la continuidad de seguridad para la información y de la existencia de los elementos esenciales para ello.

Cumplimiento con requerimientos legales y contractuales.

Se realiza con el fin de evitar el incumplimiento de las obligaciones dentro del marco legal y reglamentario relacionado con seguridad de la información optado por tomar medidas para el resguardo de los registros y de la propiedad intelectual de la empresa.

Con relación a las políticas de seguridad la empresa no cuenta con toda la documentación necesaria relativa a los procedimientos de ayuda para la seguridad de la información, con un 50 % de cumplimiento parcial y un 50 % de no aplicable; por otro lado, se realizó el análisis de la seguridad , lo cual se cumple satisfactoriamente en un 14 %, mientras que se observa un 57 % que no se cumple parcialmente, puesto que se cuenta con acuerdos de confidencialidad, sin embargo, no se tiene una claridad en los roles para el control adecuado de la operación de la seguridad. Adicional se observa que la seguridad de los RRHH solo se cumple con un 83%, debido a que no se cuenta con un adecuado control de procesos en relación a la terminación de contratos y la detección de vulnerabilidades; en la protección de activos, contando con un 70 % de cumplimiento parcial y 30 % que no se cumplen. En el control de accesos únicamente se observa un 50 % de cumplimiento parcial, un 14 % de cumplimiento inadecuado y un 36 % de no aplicado, puesto que se cuenta con el uso de contraseñas, sin embargo, no se cuenta con documentación formal; mientras que en lo que respecta a la criptografía se observa un 100 % de no cumplimiento, ya que no existen procedimientos en todo lo relacionado al uso de las llaves criptográficas. En la seguridad física y ambiental no se cuenta con una protección completa en la alimentación eléctrica, lo que evidencia inseguridad en el cableado y restricciones del uso de los equipos móviles; así mismo se detectan falencias en la seguridad en las operaciones, puesto que no se cuenta con logros y/o controles en la gestión de medios informáticos. En la relación con los proveedores no se cuenta con un control adecuado referente a los requisitos de seguridad, teniendo en cuenta toda la comunicación, para el aseguramiento y salvaguarda de los activos de la empresa; así como en la gestión de los incidentes de seguridad falta una adecuada gestión, para la recolección de evidencia. Según el análisis realizado, se observa a nivel general, que se requiere una intervención inmediata a nivel de los dominios relacionados con políticas de

seguridad, continuidad del negocio, criptografía y relación con los proveedores, puesto que son los que tienen mayor índice de incumplimiento con la norma y afectan la seguridad de la información que se requiere.

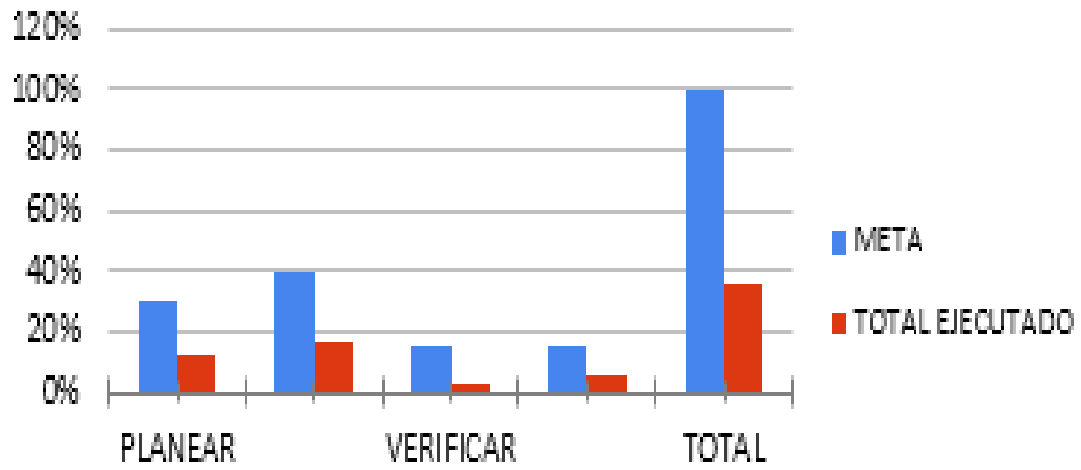
Se presenta entonces la fase final por trabajar

Tabla 6: Resultados de Logros

	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	11,9%
LOGRO2	HACER	40%	16,2%
LOGRO3	VERIFICAR	15%	2,5%
	ACTUAR	15%	5,0%
	TOTAL	100%	35,7%

Fuente: Elaboración Propia.

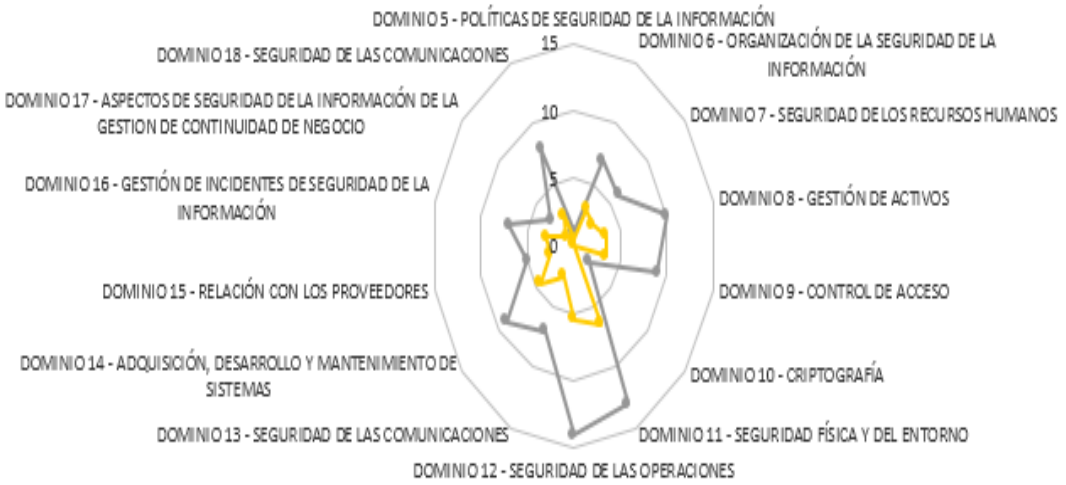
Ilustración 7: Avance de los logros



Fuente: Elaboración Propia.

Se evidencia que se debe trabajar según los resultados de cada logro

Ilustración 8: Avances por dominio



Fuente: Elaboración Propia.

4.1.3. IDENTIFICACIÓN DE PARTES INTERESADAS

Se debe tener en cuenta al SGSI y sus requerimientos

Tabla 7: partes interesadas y sus requerimientos frente la SGSI.

Parte interesada	**Requerimientos**
Entes de control	La cumplimiento de la legislación en concernientes a la seguridad de la información, alusivo al rubro de la organización.
Clientes	Protecciones de las operaciones
Proveedores	Continuidad en la contratación y asegurar el cumplimientos en los haberes y el cuidado de la información remitida.

Comunidad aledaña	Seguridad presencial cerca de las operaciones de la organización.
Filiales	Son lineamientos y acompañamientos para una propia implementación.
Competencia	Indica la conservación de las operaciones de la organización.
Alta dirección	Presentar un proceso de seguridad con estándares establecidos para un óptimo funcionamiento de las operaciones.
Colaboradores contratistas	Tener o contar con las estipulaciones de la seguridad lógica y física y las funciones dentro de la organización sin hacer sentir los derechos a la privacidad.
Control interno	Realizar el cumplimento de la responsabilidad social

Fuente: Elaboración Propia.

4.1.4. DETERMINAR EL ALCANCE

Para definir la importancia del SGSI primero se debe identificar los de la empresa considerando los más importantes, por lo tanto, delimitar el SGSI en función de ellos. Una vez identificados, los servicios de TI y los activos de información que se en el soporte de dichos procesos deben definirse para luego realizar el análisis de riesgo correspondiente.

Los procesos críticos son aquellos que proporcionan el mayor valor a la empresa; Es decir, son la parte principal del negocio. Estos son procesos que, si no existen o no funcionan con una regularidad controlada, la empresa no podría alcanzar sus metas y objetivos. Por lo tanto, la protección y continuidad de estos procesos es fundamental para cualquier organización.

Definición e implementación del SGSI respalda los procesos o actividades de generación de energía y gestión tecnológica de activos críticos para la empresa Outsoursing helpdesk el cual incluye procesos de gestión de mantenimiento, sistemas transaccionales o tecnológicos, teleprocesamiento, TI y nuevos proyectos de modernización.

4.2. LIDERAZGO

4.2.1. COMPROMISO DE LA ALTA GERENCIA

El gerente general de la empresa de Outsoursing helpdesk es completamente responsable de la verificación y aprobación del (SGSI).

Además de ello:

- Seguimiento y verificación a las políticas de seguridad por periodos mensuales
- Apoyar la divulgación y aprobación del cumplimiento del SGSI, enfocándose en los controles que aplican para cada caso.
- Establecer un monitoreo anual, en donde se realice auditoría al sistema integrado (SGSI), para determinar que amenazas existen y mitigarlas.
- Tener como prioridad a la información

4.2.2. POLÍTICAS DE SEGURIDAD

Está representada por el compromiso de la empresa de Outsoursing helpdesk con relación a la seguridad crítica de sus procesos; los cuales se deben ser definido y aceptado por la alta dirección.

Aunque la norma establece con un requisito en la sección 5.2, esta política trasciende el sistema porque ya sea que está documentada o no, cada organización tiene una política intrínseca a la naturaleza del negocio, en relación con: la importancia del conjunto o un subconjunto de información crítica para sus procesos de la empresa de Outsoursing helpdesk.

El alcance general de la política de seguridad de la información de la empresa Outsoursing helpdesk es aplicado a todos los recursos, dependencias, procesos internos y externos, servicios, funcionarios, proveedores y clientes, para garantizar adecuadamente los sistemas tecnológicos de la empresa.

• Cumplimiento de principios congruentes con toda la política de seguridad de información.

• Evaluar los riesgos identificados en la información de los procesos de la organización.

• Realizar la evaluación de los riesgos de acuerdo con los requisitos de seguridad aplicables, los resultados de la evaluación y el tratamiento del riesgo.

• Fortalecer una cultura de seguridad en la empresa Outsoursing helpdesk.

• Comunicar y actualizar las políticas y procedimientos de seguridad de la información.

• Generar confianza en los funcionarios, proveedores, clientes y terceros en materia de la seguridad de la información.
• Verificar la efectividad del SGSI.
• Mejorar y llevar a cabo acciones preventivas y correctivas para el sistema de gestión de la información de la empresa de Outsoursing helpdesk. • Garantizar la continuidad del negocio ante incidencias.

4.2.3. ROLES Y RESPONSABILIDADES

Con base en los controles proporcionados por la norma ISO- IEC 27001:2013 y el diseño de una matriz RASCI12 se intenta que todos los miembros de la empresa comprendan claramente sus roles y responsabilidades correspondientes a la seguridad de la información. La matriz cuenta con los siguientes roles:

- **Encargado – Responsible (R)**

  Corresponde a quien realiza la tarea. Normalmente existe un solo encargado(R) por tarea.

- **Responsable – Accountable (A)**
  Es quien se hace responsable de que la tarea se realice y por lo tanto debe rendir cuentas sobre su ejecución.
- **Apoyo – Support (S)**

  Son recursos asignados al encargado(R) para cumplir la tarea. Estos también trabajan en ella.
- **Consultado – Consulted (C)**

  Suministra información o alguna capacidad necesaria para la realización de la tarea.
- **Informado - Informed(I)**

Es el rol correspondiente a quien se le debe informar sobre el avance y los resultados de la ejecución de la tarea.

Así, con el objeto de desarrollar los roles y responsabilidades al interno de la empresa Outsoursing helpdesk, para la implementación del SGSI. Se fijan los roles que los implicados deben asumir frente a cada uno de los controles de la norma. Entre los implicados se incluye:

- Propietarios de los activos de información, todos aquellos a quien ha sido asignado un activo de información en específico. Debe existir registro de ello.
- Personal, todos aquellos que mantienen una vinculación laboral con Interfaces y Soluciones.
- Director General, encargado de planificar y controlar las actividades relacionadas con el SGSI, así como todas las actividades administrativas y financieras
- Jefe de RRHH, encargado del manejo de toda la documentación enviada y/o recibida, así como de las relaciones con los proveedores y/o clientes, incluyendo las quejas y/o reclamos de los mismos, en el momento asumido por gestión humana
- Delegado de gestión de las instalaciones, encargado de la seguridad física y del entorno, así como de la implementación de técnicas para el correcto control de trabajo en áreas seguras.

4.3. PLANIFICACIÓN

4.3.1. ANÁLISIS DE RIESGO

Gestión de riesgos, para que los órganos reactores tomen decisiones correctas de acuerdo a cada uno de los riesgos expuestos de la tecnología de la información, así como el inventario de activos de la organización y la valoración de estos, entendiendo y tomando en consideración la integridad, confiabilidad, disponibilidad e integridad de la información. Realizando así el análisis de amenazas y la evaluación de riesgos, estimando así los riesgos a los que la organización puede estar expuesta.

4.3.1.1. Valoración de Activos

La confidencialidad

Indica a que la información solo debe llegar a las personas autorizadas. Esta es definida según las características de la información gestionada y procesada por el activo. Para la presente valoración se toma en cuenta los siguientes criterios de clasificación.

Tabla 8: Valoración Y Calificación

Escala de Valoración	Valor	Confidencialidad	
3	Alto	El activo gestiona y/o procesa Información Reservada, su uso inadecuado puede generar consecuencias graves para la organización.	La información que está disponible solo para un proceso de la empresa de Outsoursing helpdesk.
2	Medio	El activo gestiona y/o procesa Información Clasificada, su uso inadecuado puede generar medianas consecuencias a la organización, como por ejemplo, reclamaciones de las áreas que soporta.	La información disponible para todos los procesos de la empresa de Outsoursing helpdesk. La información vertida a continuación es propia de la organización o de terceros y podrá ser utilizada únicamente por los trabajadores de la entidad y que se encuentren dentro de sus funciones del propietario de la cuenta que requiera realizar acción alguna.
1	Bajo	El activo gestiona y/o procesa Información Pública, no genera consecuencias negativas para la organización	La información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la de la organización.
0	No calificada	Activos de Información que se incluirán en el recuento y que aún no han sido catalogados.	Debe ser tratada como activos de información reservada hasta el momento en que se defina una valoración entre la escala del 1-3 definida.

Fuente: Elaboración los Autores.

Integridad

La integridad es una característica o propiedad de la información que garantiza que ésta no ha sido alterada (modificada o destruida) de manera no autorizada. Todos los criterios de valoración de integridad para los activos de la empresa de Outsoursing helpdesk de integridad para los activos se describen a continuación:

Tabla 9: Criterios de valoración de integridad

Escala de Valoración	Valor	Confidencialidad
3	Alto	El activo gestiona la información cuya perdida de exactitud puede conllevar un impacto negativo de índole legal o económico, retrasa las facciones puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generan pérdidas de imagen severas a la organización. Es información que apoya la toma de decisiones estratégicas de la organización. Los errores deben ser solucionados los errores deben ser solucionados inmediatamente.
2	Medio	El activo gestiona la información cuya pérdida de exactitud y complejidad, pude conllevar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar pérdida de imagen moderada a funcionarios de la organización. La información gestionada por el activo permite una brecha de errores que pueden ser solucionados a corto plazo.
1	Bajo	El activo gestiona información cuya pérdida de la exactitud y completitud conlleva un impacto no significativo para la organización o entes externos. Los errores pueden ser solucionados en un mediano plazo
0	No calificada	El activo de información debe ser incluido en el inventario y aún no ha sido clasificado. Debe ser tratado como activo de Integridad nivel 3 hasta el momento en que se defina una valoración entre la escala del 1-3 definida

Fuente: Elaboración los Autores.

4.3.1.2. Valoración del riesgo

La valoración del riesgo es la estimación de las magnitudes o riesgos a los que puedes estar expuesta la empresa de Outsoursing helpdesk. La materialización de una amenaza consta de dos elementos: probabilidad e impacto, estos determinan el nivel del riesgo.

Punto de vista de valoración:

Tabla 10: Punto de Vista de valoración según probabilidad

Escala de Valoración	Valor	Confidencialidad
3	Alto	La amenaza se puede materializar mínimo una vez al mes
2	Medio	La amenaza se puede materializar a lo sumo una vez en el semestre
1	Bajo	La amenaza se puede materializar a lo sumo una vez al año

Fuente: Elaboración autores.

Según el impacto se determinan los siguientes criterios de valoración:

Tabla 11: Punto de vista de valoración en base a Impactos

Escala de Valoración	Valor	Confidencialidad
3	Alto	La ocurrencia del evento tiene impacto en todos los niveles como son integridad, confiabilidad e disponibilidad de la información poniendo en riesgo la reputación de la empresa y/o inconvenientes legales
2	Medio	La ocurrencia del evento tiene en todos los niveles como son integridad, confiabilidad e disponibilidad

		de la información sin poner en riesgo la reputación de la empresa o necesidad de medidas legales.
1	Bajo	La ocurrencia del evento no tiene consecuencias relevantes para la organización

Fuente: Elaboración los Autores.

Por la combinación probabilidad - impacto se define el mapa de riesgo que se presenta a continuación, los números en el interior de las celdas son calculados por la multiplicación de la probabilidad por el impacto. Indican junto con los tonos de colores la criticidad del riesgo.

Una vez que se identifica el nivel de riesgo, en dimensión de los activos de la organización se procede con el promedio, se ha establecido que los activos que tengan un promedio de 3 serán considerados para realizar un análisis de riesgo. Y buscar medidas para mitigar el riesgo establecido.

Tabla 12: Valorización de activos

COD	Nombre	Confidencialidad	Disponibilidad	Integridad	Valor Final
R1	Gerencia General	**0**	**2**	**0**	**1**
R2	Gerencia Administrativa	**0**	**2**	**0**	**1**
R3	Área de contabilidad	**0**	**2**	**0**	**1**
R4	Marketing y publicidad	**0**	**2**	**0**	**1**
R5	Área de ventas y Área de sistemas	**1**	**2**	**0**	**1**
R6	Tesorero	**0**	**2**	**0**	**1**
R7	Almacén	**0**	**2**	**0**	**1**
R8	office 2016	**1**	**1**	**2**	**2**
S1	SQL Base de Datos	**3**	**3**	**3**	**3**
S2	Servidor de intranet	**2**	**2**	**3**	**3**
S3	servidor de correo	**3**	**3**	**3**	**3**
S4	Desktop	**1**	**2**	**2**	**2**
H1	laptops	**1**	**3**	**3**	**3**
H2	impresora	**2**	**2**	**2**	**2**
H3	Cañón Multimedia	**0**	**1**	**0**	**1**

H4	Facturación electrónica	**2**	**2**	**3**	**3**
H5	Internet	**1**	**2**	**3**	**3**
H6	soporte	**0**	**2**	**0**	**1**

Fuente: Elaboración los Autores.

El siguiente paso es el plan de tratamiento de riegos, el cual indica que se debe identificar las amenazas como las vulnerabilidades de la empresa de Outsoursing helpdesk, alas que se está expuesto.

Tabla 13: Vulnerabilidades y amenazas de activos

ID Activo	Nombre de Activo	Vulnerabilidad	Amenaza
S1	SQL Base de Datos	falta de respaldo	falta de espacio en el NAS
		falta de documentación	error en el manejo
		problema en distribución de accesos	abusos de derechos
		falta de cierre de sección de usuarios	abusos de permisos
S2	Servidor de intranet	falta de mantenimientos	incumplimiento en el mantenimiento lógico y físico
		suba ya baja tención de energía	equipo obsoleto
		deficiencia en conexión del cableado de red	saturación de la red
		inseguridad de arquitectura de red	interceptación de la señal
S2	Servidor de intranet	falta de mantenimientos	incumplimiento en el mantenimiento lógico y físico
		suba ya baja tención de energía	equipo obsoleto
		Sensibilidad al polvo y la humedad	corrosión, saturación
		deficiencia en conexión del cableado de red	saturación de la red
H1	laptops	falta de mantenimiento	incumplimiento en el mantenimiento lógico y físico
		suba ya baja tención de energía	equipo obsoleto
		subeptiviliadad al polvo y la humedad	corrosión, saturación
		deficiencia en conexión del cableado de red	corrosión, saturación
		falta de protección en la infraestructura	robo de equipo
		almacenamiento sin seguridad	perdida de información
H4	Facturación electrónica	falta de procedimientos para manejo de información confidencial	incidente grave

	distribución de accesos	abusos de derechos
	falta de backup	perdida de información
	almacenamiento sin seguridad	perdida de información

Fuente: Elaboración los Autores

Terminando el análisis se procede con el análisis de riesgos, y sus posibles consecuencias

4.3.2. OBJETIVOS DE SEGURIDAD

Las principales metas de la SGSI son:

• Defender toda la infraestructura y los procesos de la empresa de Outsoursing helpdesk, contra los riesgos que afectan la seguridad informática.

• Demostrar a los inversores y partes interesadas que están cubiertos a cada aspecto de la informacion y las tecnologías para el negocio de la organizacion.

• Realizar la implementación y administración de acciones, para precaver, remediar y mitigar los efectos de los peligros de la seguridad informática.

• Cumplir con todos los requisitos de privacidad y de protección de datos establecidos en el Perú.

• Fomentar una cultura de seguridad dentro de la empresa para el cuidado de los datos informáticos donde los roles y las responsabilidades en el mantenimiento de la reserva de datos, disponibilidad e integridad.

Por cada objetivo se definió en un plan. La alineación entres los propositos y la, politica.

4.4. SOPORTE

4.4.1. CULTURA DE SEGURIDAD

La cultura de prevención parece estar estrechamente relacionada con la cultura empresa de Outsoursing helpdesk, por lo tanto, comenzamos hablando de organizaciones. A menudo se sostiene que la cultura es el verdadero corazón de una organización. Para algunos el desarrollo de una cultura de seguridad que tiene que llegar a cada miembro de la organización, la cultura de la organización se conforma por las intercomunicaciones internas de cada uno de los participantes y el sentido que conceden las acciones y eventos de la organización. El colectivo subyace al espíritu que determinará la cultura. Los vehículos que sirven para

sostener y transmitir una cultura son las declaraciones de principios, los símbolos, las historias, las ceremonias, la jerga, los rituales, los líderes, los procesos de socialización de los miembros y el establecimiento de objetivos comunes. Existen al menos dos enfoques del concepto de cultura organizacional: uno, desde la perspectiva socio antropológica y el otro, desde la psicología organizacional.

4.4.2. COMUNICACIÓN

La siguiente investigación tiene como objetivo introducir al lector en el amplio alcance de la comunicación organizacional. en la empresa de Outsoursing helpdesk la comunicación es vital para que todas las áreas dentro de la organización estén a lineadas y es con el objetivo de toda comunicación eficaz y a tiempo.

4.5. OPERACIÓN

4.5.1. CONTROL Y PLANIFICACIÓN

Tras la identificación, estimación y priorización de riesgos se ha desarrollado una investigación y definición de los controles recomendados a utilizar para su tratamiento.

La determinación de controles se ha basado en los dominios del Anexo A de la norma ISO 27001:2013.

Documentación de Políticas

Debido que la gran mayoría de vulnerabilidades detectadas en la organización están relacionadas con la carencia de políticas y/o documentos formales de seguridad, se han desarrollado un grupo de políticas asociadas a los dominios de la norma con las cuales se busca disminuir la probabilidad e impacto de materialización de alguna amenaza.

- RB: Riesgo Bajo
- RA: Riesgo Alto
- RM: Riesgo Medio

Tabla 14: Documentación de políticas

ID	Política	Amenaza	Nivel de Riesgo		
			RB	RC	RM
001	Política de Seguridad de la Información	Abuso de información privilegiada y actos no autorizados		X	
		Errores y Omisiones		X	
002	Política de Seguridad de los Recursos Humanos	Abuso de información privilegiada y actos no autorizados			
003	Política de Control de Accesos	Abuso de información privilegiada y actos no autorizados		X	
		Intrusión física y/o robo			X
004	Política de Controles Criptográficos	Abuso de información privilegiada y actos no autorizados		X	
005	Política de Seguridad Física y del Entorno	Fallos de dependencia	X		
006	Política de escritorio y pantalla limpios	Abuso de información privilegiada y actos no autorizados			X
007	Política de Almacenamiento y respaldo	Abuso de información privilegiada y actos no autorizados		X	
008	Política de Transferencia de Información	Errores y Omisiones		X	
009	Política de Desarrollo Seguro	Abuso de información privilegiada y actos no autorizados			X
010	Política de S.I aplicable a proveedores	Abuso de información privilegiada y actos no autorizados		x	
011	Política de Gestión de Incidentes	Abuso de información privilegiada y actos no autorizados			X
012	Política de Gestión de la continuidad del negocio	Abuso de información privilegiada y actos no autorizados		X	

Fuente: Elaboración Propia.

4.5.2. EVALUACIÓN DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

La principal estrategia en el tratamiento de riesgos es estudiar la situación y determinar en cuáles de los siguientes casos se ubica el riesgo, con el propósito de enfocarse en el objetivo correcto.

A partir de lo anterior y la valoración de riesgos se definen las siguientes estrategias:

ESTRATEGIAS PARA TRATAMIENTO DE RIESGO

Tabla 15: Estrategias para el Tratamiento de Riesgos

Probabilidad	3 - Alta	3.Zona de riesgo Moderado Tratamiento: Reducir la probabilidad de ocurrencia Evitar el riesgo	6. Zona de riesgo extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir	9.Zona de riesgo Extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir
	2 - Media	2. Zona de riesgo Bajo Tratamiento: Reducir la probabilidad de ocurrencia	4.Zona de riesgo Moderado Tratamiento: Reducir el riesgo Evitar el riesgo	6. Zona de riesgo extremo Tratamiento: Reducir el riesgo Evitar el riesgo Compartir o transferir
	1 - Bajo	1. Zona de riesgo Bajo Tratamiento: Asumir el riesgo	2. Zona de riesgo Bajo Tratamiento: Reducir el riesgo Evitar el riesgo	3.Zona de riesgo Moderado Tratamiento: Reducir el riesgo Evitar el riesgo
		1 - Bajo	2 – Medio Impacto	3 - Alto

Fuente: Elaboración los Autores

De acuerdo a las prioridades de la organización y el nivel de riesgo detectado se definen diferentes técnicas como parte del tratamiento del riesgo:

Aceptar (A): Indica una aceptación del riesgo tras una decisión informada a favor de tomar el riesgo que tiene una muy baja probabilidad de ocurrencia. Esta técnica reconoce el riesgo. La aceptación es una técnica "pasiva" que se centra en permitir que cualquier resultado ocurra sin tratar de prevenir ese resultado. Esta técnica se utiliza normalmente para los riesgos "bajos" o "muy bajos" en los que no es evidente un medio eficiente de reducir el riesgo.

Evitar (E): Se intenta evitar la ocurrencia del riesgo puesto que presenta una probabilidad media o alta y puede ocasionar daños graves a la organización. Aquí se encuentran las salvaguardas preventivas en la que se establece anticipadamente políticas, normas, controles y procedimientos que buscan mitigar alguna circunstancia que provoca y reduce las posibilidades de ocurrencia. Las ideales son las que impiden completamente la materialización de la amenaza.

Controlar (C): Esta técnica se compone de acciones que deben tomarse para reducir la probabilidad de riesgo o el impacto. Por lo general, identifican una acción o producto que se convierte en parte de los planes de trabajo y que son supervisados e informados como parte del análisis de desempeño regular y el informe de progreso del Programa.

Investigar (I): Esta técnica difiere todas las acciones hasta que se realiza más trabajo y/o se conocen hechos. Todas las respuestas basadas en la presente investigación, no definen ninguna mitigación para reducir un riesgo individual, son respuestas a los riesgos en los que se identifica una solución clara la cual requiere más investigación.

Mitigar (M): Se establecen salvaguardas que actúan en el momento que se presenta o materializa la amenaza. Son las medidas que limitan la posible degradación y a su vez frenar cualquier posible daño, se usa para la detección temprana a los ataques.

Transferir (T): Se busca pasar parcial o totalmente el riesgo a otra compañía, ya sea por medio de una póliza de seguro o un contrato de outsourcing. Es una medida en la que se busca compartir el riesgo. Hay dos formas básicas de compartir riesgo.

4.5.3. TRATAMIENTO DEL RIESGO

Tabla 16: Dominio de control

Dominio	Control	A	C	E	I	M	T
A6	Acuerdo de confidencialidad.		X	X			
	Base de Datos que permita gestionar personas, responsabilidades, acuerdos, riesgos, activos, etc.			X			
	Designar un líder para la administración de la seguridad y comité de seguridad.		X				
7	Aplicación de medidas disciplinarias		x				
	Fijar roles y responsabilidades antes de contratación		x				
	Fijar términos y condiciones del contrato		X				
	Generación de conciencia y compromiso con la seguridad de la información.		x				

	Revocar derechos tras finalización de contrato		x			
	Verificación de hojas de vida		x			
8	Clasificar y etiquetar la información		x	x		
	Inventario de Activos				x	x
9	Gestión de Contraseñas					
	Gestión(creación, modificación, bloqueado, eliminación) de Usuarios basada en roles		x			
	Firmas digitales			x		
10	Control de refrigeración y ventilación	x				
	Medidas Contra Incendios(extintores)					x
11	Registro de Ingresos					
	Seguridad Perimetral				x	
12	Control de software operacional			x		
	Respaldo de la información			x		
	Separación de los ambientes de desarrollo, pruebas y operación			x		
13	Análisis periódico del tráfico de la red			x		
14	Protección de datos de prueba			x		
	Validación en la entrada y salida de datos			x		
15	Cláusulas de seguridad para proveedores				x	
16	Reporte de debilidades de seguridad de la información				x	
	Reporte de debilidades de seguridad de la información			x		
17	Control técnico de las pólizas de segur			x		
18	Privacidad y protección de información de datos personales			x		

Fuente: ISO 27001

4.5.4. MONITOREO Y MEDICIÓN, ANÁLISIS Y MEDICIÓN

La unión del plan de tratamiento junto con un plan de monitoreo permite conocer cuán pertinentes son las estrategias implementadas, para así ejecutar acciones oportunas que permiten anticiparse a los problemas, garantizar la sostenibilidad de los proyectos y retroalimentar los procesos de toma de decisiones. En la siguiente tabla se establecen las medidas para monitorear los riesgos y los responsables a cargo:

*Tabla 17:*Tratamiento de riesgos

Riesgo	nivel	tratamiento				Plan de monitoreo	Responsable	
		A	E	M	T			
Abuso de privilegios de acceso	RC		X			Auditoría interna de las funciones de los empleados	Gerente de proyectos Gerente comercial	
Acceso no autorizado	RC				X	Registro y evaluación periódica de logs de aplicaciones críticas	Gerente de proyectos Coordinador de proyectos	
Corte del suministro eléctrico						Evaluación periódica de los suministros eléctricos Evaluación al proceso de respaldo externo	Gerente comercial Auxiliar Administrativa	
Indisponibilidad del personal	RC					Auditoría interna en cuanto al proceso de bienestar y garantías del empleado	Gerente comercial Gerente de proyectos	

Fuente: Elaboración Propia.

4.5.5. MEJORA

La auditoría de cumplimiento está realizada bajo la metodología PHVA y el uso de CMM (Modelo de Capacidad y Madurez). Este modelo facilita el control sobre los procesos y así el desarrollo y la permanencia de un mejor SGSI. CMM es un modelo apoyado en la mejora continua de los procesos.

Por consiguiente, trata la identificación de elementos actuales y deseables en la organización que permitan evaluar el progreso o no del cumplimiento de los controles

aplicables definidos para la implementación del SGSI. De manera que, los elementos identificados para el proceso de evaluación de la auditoría de cumplimiento son:

- Procedimientos Empíricos(PEmp)
- Documentos Formales(DF)
- Procedimientos Estandarizados(PEst)
- Capacitaciones(C)
- Mejora continua(MC)
- Monitoreo(M)
- Herramientas Automatizadas(HA)

También se ve reflejada una mejora significativa con los controles por dominio.

la cual indica la siguiente tabla:

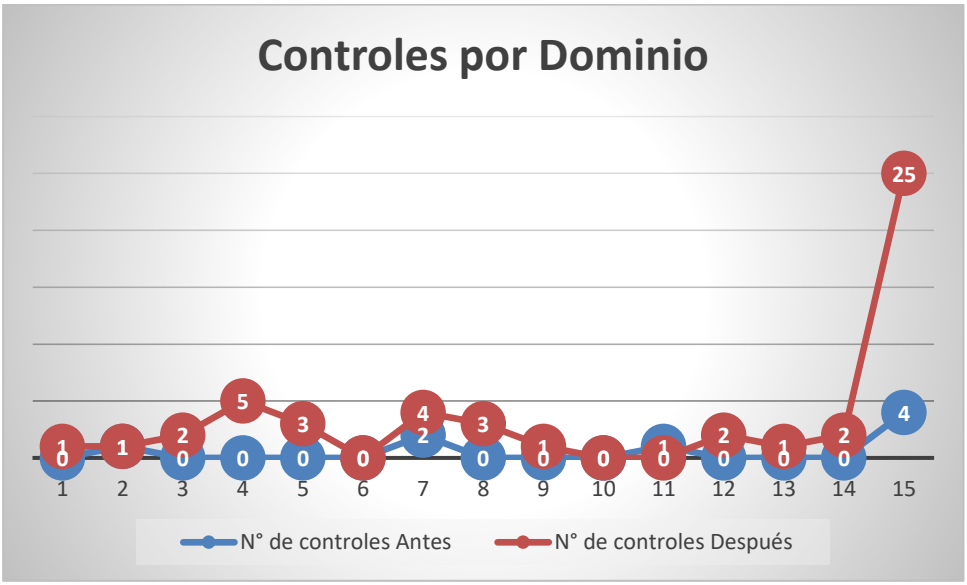
Tabla 18: Controles por dominio

Dominios ISO/IEC 27002	**N° de controles Antes**	**N° de controles Después**
políticas de seguridad	**0**	**1**
Organización de la seguridad	**1**	**1**
seguridad en Capital Humano	**0**	**2**
Gestión de Activos	**0**	**5**
Control de accesos	**0**	**3**
Criptografía	**0**	**0**
Seguridad Física del entorno	**2**	**4**
Seguridad en los proceso	**0**	**3**
Seguridad de las comunicaciones	**0**	**1**
Desarrollo y tecnologías de sistemas	**0**	**0**
Relación con proveedores	**1**	**0**
Gestión de incidentes	**0**	**2**
Continuidad del rubro	**0**	**1**
Cumplimiento	**0**	**2**
Total	**4**	**25**

Fuente: Elaboración Propia.

Gráfico de resultados:

Ilustración 9: Controles por Dominio



Fuente: Elaboración Propia.

Se verifica que antes de la implementación del SGSI, concerniente a los controles de domino, se encontraron en la empresa Outsourcing Helpdesk, un total de 6 valores el cual se incrementó a 25 después de su implementación, el cual significa un aumento significativo en la organización.

4.6. RESULTADO Y DISCUSIONES

Después de la implantación de SGSI, se buscó comparar resultados anteriores y experiencias pasadas con la implementación de un sistema de gestión de seguridad de la información.

Según la experiencia de (Aguirre David, 2014) en su tesis “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA SERVICIOS POSTALES DEL PERÚ S.A.” el cual concluye e indica que es de vital importancia el apoyo de la alta gerencia, como de todos los jefes de áreas, y dueños de procesos, los cuales entendieron la importancia de la implantación de SGSI, la cual se encarga de salvaguardar la información crítica, vital del negocio de la organización. También concluyo que es necesario mejorar la comunicación

entre toda área de la organización especialmente en logística, para el aceleramiento de procesos de compra de activos que ayuden para el fortalecimiento de la seguridad de información

También concuerdo con la tesis .(Barrantes Porras y Hugo Herrera, 2012) “Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos” la cual indica que muchas veces las empresas se extienden y maduran de forma desorganizada, sin un procedimiento o planificación establecida o adecuada, además de contar con paradigmas que no suelen obviarse de manera oportuna y eficiente, ante tales conceptos la presente tesis concluye, que la documentación en todos los procesos, sirven y se convierten en una herramienta importante, para la mejora y el mantenimiento respectivo para cualquier sistema de gestión.

También se considera que los resultados obtenidos, después de la implementación, que el factor humano y el compromiso de cada colaborador, es de vital importancia, para la implementación de un SGSI, ya que ellos son los que manejan la información confidencial de la organización

También se concluye que un SGSI puedes ser aplicado a cualquier organización, de cualquier rubro ya se grande o pequeña.

CONCLUSIONES

Se logró cumplir con el objetivo principal el cual fue la implementación del sistema de gestión de seguridad de la información (SGSI) en la empresa Outsourcing Helpdesk, y a su vez se redujo los riesgos a la que estaba expuesto, los hallazgos iniciales de la implementación sobre las política para la seguridad de la información contaba con un 50 % de cumplimiento parcial y un 50 % de no aplicable; según (tabla 5) tras la implementación de un cumplimiento de total de 35.7% más de lo encontrado Inicialmente (tabla 6).

También se concluye que, para una buena implementación de sistema de seguridad de la información, es de vital importancia, el compromiso de la alta gerencia, como tanto los gerentes de área, dueño de procesos y todos los colaboradores de la empresa Outsourcing Helpdesk. Los cuales entiendan la importancia del manejo de la seguridad de la información en la organización, el cual es vital para el crecimiento de la misma.

Se concluye tras la realización del análisis de riesgo antes de la implementación de las políticas de seguridad la empresa no se contaba con toda la documentación y los procesos necesarios relativos a las formas y técnicas de mejora o ayuda para la seguridad de la información, concerniente a los controles de domino, se encontraron en la empresa Outsourcing Helpdesk, un total inicial de 6 valores (tabla 4) el cual se incrementó a 25 valores (tabla 18- anexos) después de su implementación, el cual significa un aumento significativo en la organización.

En conclusión, la sensibilización sobre seguridad y la implantación de un sistema de gestión de seguridad de la información, contribuyen a que los colaboradores, cometan errores básicos de seguridad como sesiones abiertas, seguridad en sus contraseñas, fugas de información, la implementación ayuda con todo esto expuesto, pero no se puede lograr sin un plan de capacitaciones continuas sobres riesgos de seguridad y nuevas tecnologías.

.

RECOMENDACIONES

Se recomienda seguir con la capacitación continua a todos los trabajadores de la organización, en temas basados en la seguridad tanto como la información como los activos para así lograr que todos se involucren y tengan los procedimientos claros y concisos.

Se recomienda la realización de la documentación de todos los procesos de la empresa para poder gestionar los mismos de manera rápida y óptima ante cualquier cambio que se pueda dar en la organización.

Es importante un pleno apoyo de la alta gerencia, y que esta entienda y dé a conocerlas políticas de seguridad de la información a toda la organización.

REFERENCIAS BIBLIOGRÁFICAS

AGUIRRE_DAVID_SISTEMA_GESTION_SEGURIDAD_INFORMACION_SERVICIOS_POSTALES.pdf.crdownload, [sin fecha]. S.l.: s.n.

BARRANTES PORRAS, C.E. y HUGO HERRERA, J.R., 2012. Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos. , pp. 1-314.

CON, S., AL, B., SEGURIDAD, M.D.E., LA, Y.P.D.E., SEGUN, I., DEL, L. y LAS, M.D.E., 2018. No Title. ,

MALDONADO, G.B., ANDRÉS, J. y CANO, O., 2014. Metodología de la seguridad de la información como medida de protección en pequeñas empresas. Methodology of Information Security as a Measure of Protection Small Business. *Enero -Diciembre*, pp. 2027-8101.

WORLD ECONOMIC FORUM, 2018. *Informe de riesgos mundiales 2018. edición 13*. S.l.: s.n. ISBN 978-1-944835-15-6.

ISO27000.es - El portal de ISO 27001 en español.2019. *Iso27000.es* [acceso 25 enero 2019],http://www.iso27000.es/iso27000.html

.

ANEXOS

DIAGNOSTICO INICIAL DE LOGRO 1: DEFINICIÓN DE MARCO DE SEGURIDAD Y PRIVACIDAD DE LA ENTIDAD (30%)

PLANEAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
1	La entidad cuenta con un autodiagnóstico realizado para medir el avance en el establecimiento, implementación, mantenimiento y mejora continua de su SGSI (Sistema de Gestión de Seguridad de la información?	Cumple parcialmente	Existe noción de la implementación del sistema de SGSI mas no lo mantiene	Asegurar autodiagnósticos de seguridad de la información.
2	La entidad creó un caso de estudio o plan inicial del proyecto, donde se incluyen las prioridades y objetivos para la implementación del SGSI?	Cumple parcialmente	Acta de reunión y aprobación para inicio de proyecto SGSI	Crear caso de estudio o plan inicial del proyecto que incluya prioridades y objetivos del SGSI, estructura del SGSI.
3	La entidad contó con la aprobación de la dirección para iniciar el proyecto del SGSI?	Cumple satisfactoriamente	Conta de Acta asignado por la gerencia para iniciar el proyecto	Se verifica la existencia del documento de aprobación firmado por la gerencia para el inicio del proyecto.
4	La entidad ha identificado los aspectos internos y externos que pueden afectar en el desarrollo del proyecto de implementación del sistema de gestión de seguridad de la información?	No cumple		Se deben identificar los temas tanto externos como internos que pueden afectar el desarrollo de los resultados del sistema.
5	La entidad ha identificado las partes interesadas, necesidades y expectativas de estas respecto al Sistema de Gestión de Seguridad de la Información?	No cumple		Se requiere que se identifiquen las partes interesadas tanto internas como externas, detallando cuáles son sus necesidades y expectativas en la implantación del Sistema de Gestión de Seguridad de la Información.
6	La entidad ha evaluado los objetivos y las necesidades respecto a la Seguridad de la Información?	No cumple		Realizar la identificación de los objetivos y las necesidades que tiene la entidad respecto a la seguridad de la Información.
7	En la entidad se ha definido un Comité de Seguridad de la Información?	Cumple parcialmente	Existe una persona responsable como responsable de salvaguardar la seguridad de la información en el SST	Definir responsabilidades de cada miembro del comité de seguridad.

8	La entidad cuenta con una definición del alcance y los límites del Sistema de Gestión de Seguridad de la Información?	No cumple		Crear un documento de alcance del Sistema de Gestión de Seguridad de la Información y sus respectivos límites en cuanto a TIC, límites físicos, temas internos y externos.
9	En la entidad existe un documento de política del Sistema de Gestión de Seguridad de la Información, el cual ha sido aprobado por la Dirección?	Cumple satisfactoriamente	Base de información con políticas generales del sistema de gestión de seguridad de información dentro del marco regulatorio	Crear un documento que defina la política general del Sistema de Gestión de Seguridad de la Información y sus respectivos límites. Tener en cuenta objetivos del SGSI, marco regulatorio, el cual debe estar debidamente documentado y socializado.
10	En la entidad existe un documento de roles, responsabilidades y autoridades en seguridad de la información?	No cumple		Se deben definir roles y responsabilidades para cada etapa de la Implementación.
11	La entidad tiene establecido algún proceso para identificar, analizar, valorar y tratar los riesgos de seguridad de la información?	Cumple parcialmente	cuenta con documento de metodología de gestión de riesgos de información	Se debe seleccionar una metodología para gestionar los riesgos y describir en una matriz de riesgos los resultados de acuerdo a los criterios de aceptación de los mismos. Nota: Si la entidad ya tiene una matriz de riesgos, se deben identificar los riesgos que apunten a la seguridad de la información.
12	La entidad ha realizado una declaración de aplicabilidad que contenga los controles requeridos por la entidad?	Cumple parcialmente	Consta de un documento de aplicabilidad que presenta datos de controles requeridos	Crear documento de declaración de aplicabilidad donde se justifique la inclusión y exclusión de controles del Anexo A de la norma ISO27001 versión 2013.
13	La entidad ha evaluado las competencias de las personas que realizan, bajo su control, un trabajo que afecta el desempeño de la seguridad de la Información?	No cumple		Se debe conservar la información que evidencie las competencias del personal que se encuentre involucrado con la seguridad de la información de la entidad. Se debe definir un plan de capacitación con el fin de que dichas personas adquieran las competencias respectivas.
14	La entidad tiene definido un modelo de comunicaciones tanto internas como externas respecto a la seguridad de la información?	Cumple parcialmente	se utiliza una base de datos codificada	Se debe desarrollar un modelo que indique el contenido de la comunicación; fechas, a quién se comunica y quién comunica.
15	La entidad tiene la información referente al Sistema de Gestión de Seguridad de la Información debidamente documentada y controlada?	Cumple parcialmente	exisre documentacion generada de los principales procesos los cuales estan ordenadas	Toda la documentación generada del Sistema de Gestión de Seguridad de la Información debe estar debidamente documentada.

DIAGNOSTICO INICIAL DE LOGRO 2: IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ANEXO			ESTADO	EVIDENCIA
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**			
A5.1	Orientación de la dirección para la gestión de la seguridad de la información			
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes				
A5.1.1	Políticas para la seguridad de la información	Control: 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.	Cumple parcialmente	existe un documentos con todos los requerimientos procesados
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	No aplica	
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**			
A6.1	Organización interna			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.				
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Cumple parcialmente	Se evidencia un documento que designa a las personas que cumplen cada rol, por lo que existe seguimiento pero de estandarizado
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	Cumple parcialmente	Existe una evidencia del cumplimiento de funciones por roles

A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	Cumple satisfactoriamente	Existe actas de las reuniones
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	No cumple	
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	Cumple parcialmente	Se presenta un documentos de gestión para el manejo de información segura
A6.2	Dispositivos móviles y teletrabajo			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles				
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Cumple parcialmente	se aplica solo en casos presentados, pero no existe una política
A6.2.2	Teletrabajo	Control: 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.	No cumple	
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
A7.1	Antes de asumir el empleo			
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.				
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	Cumple parcialmente	Se considera certificados de antecedentes para ejercer el cargo, y se realiza un seguimiento constante
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Cumple parcialmente	Se realiza una firma de confidencialidad en base a lo digital y en los archivos esenciales
A7.2	Durante la ejecución del empleo			
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.				

A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Cumple parcialmente	Aplica principalmente los principios deontologicos y eticos
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de 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 para su cargo.	No cumple	
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Cumple parcialmente	Se aplica en en RIT de trabajo de la entidad
A7.3	Terminación y cambio de empleo			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo				
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Cumple parcialmente	Este presente esta especificado en el contrato de trabajo y de los principios eticos
A8	**GESTION DE ACTIVOS**			
A8.1	Responsabilidad por los activos			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.				
A8.1.1	Inventario de activos	Control: 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.	No cumple	
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	Cumple parcialmente	Por el proceso que realizan deferentemente
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	No cumple	

A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Cumple parcialmente	Se lleva el control mediante un inventario chico
A8.2	Clasificación de la información			
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	No cumple	
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Cumple parcialmente	Existe un inventario para el cumplimiento de las funciones
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Cumple parcialmente	Existe un sistema de calificación
A8.3	Manejo de medios			
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios				
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Cumple parcialmente	Se requiere de un procedimiento formal
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Cumple parcialmente	Se utiliza un documento donde se presenta los materiales
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Cumple parcialmente	Se presenta claves pero para toda la organización
A9	**CONTROL DE ACCESO**			
A9.1	Requisitos del negocio para el control de acceso			
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.				

A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Cumple parcialmente	Se aplica la politica de los medios confidenciales
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Cumple parcialmente	A traves de un usuario clave
A9.2	Gestión de acceso de usuarios			
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	No aplica	
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	No aplica	
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	No aplica	
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	No aplica	
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Cumple parcialmente	Con la política general
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Cumple parcialmente	Solo para algunos trabajadores con que cuenta la organización
A9.3	Responsabilidades de los usuarios			
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.				
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	No cumple	Debido a que los clientes externos pueden manejar la información de manera favorable para ellos no se regula

A9.4	Control de acceso a sistemas y aplicaciones			
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.				
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Cumple parcialmente	Se tiene control de la información por la plataformas del administrador
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	No cumple	Solo cuentan con contraseñas
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Cumple parcialmente	A nivel plataforma principales
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	No aplica	No cuenta con sistemas
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	Cumple parcialmente	Existe un sistema de responsabilidad de una empresa
A10	**CRIPTOGRAFIA**			
A10.1	Controles criptográficos			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información				
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	No cumple	
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	No cumple	No tiene sistema propio
A11	**SEGURIDAD FISICA Y DEL ENTORNO**			
A11.1	Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	Cumple parcialmente	A traves de contrseñas

A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Cumple parcialmente	A traves de contrseñas
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones..	Cumple parcialmente	A traves de contraseñas
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	No aplica	
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	No cumple	
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	No cumple	
A11.2	Equipos			
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Cumple parcialmente	A través de contraseñas
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Cumple satisfactoriamente	
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Cumple parcialmente	Existe un sistema adecuado de generadores de energía
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Cumple parcialmente	Existe equipos de mantenimiento de computo
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	Cumple satisfactoriamente	Los equipos son de propiedad de la empresa

A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	Cumple parcialmente	Existe equipo para protección de equipos móviles
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso.	Cumple parcialmente	Se aplica con la prioridad permanente posible
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	No aplica	
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	Cumple parcialmente	No todos aplican la iniciativa
A12	**SEGURIDAD DE LAS OPERACIONES**			
A12.1	Procedimientos operacionales y responsabilidades			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	Cumple parcialmente	Existe procedimientos y documentos de gestión por los usuarios
A12.1.2	Gestión de cambios	Control: 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.	Cumple parcialmente	Se cumple conforme anuncios de la gerencia
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	No cumple	
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Cumple parcialmente	No existe un software apropiado
A12.2	Protección contra códigos maliciosos			
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.				

A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Cumple parcialmente	Se tiene control en los sistemas de congelamiento de equipos
A12.3	Copias de respaldo			
Objetivo: Proteger contra la perdida de datos				
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Cumple parcialmente	El proveedor tiene respaldo mensual de base de datos
A12.4	Registro y seguimiento			
Objetivo: Registrar eventos y generar evidencia				
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Cumple parcialmente	Se está implementando un sistema de control de eventos
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Cumple parcialmente	Se está implementando de un sistema de autenticación
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	Cumple parcialmente	Depende de un proveedor
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	No cumple	
A12.5	Control de software operacional			
Objetivo: Asegurarse de la integridad de los sistemas operacionales				
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Cumple parcialmente	Se implementan procedimientos mediante software instalado
A12.6	Gestión de la vulnerabilidad técnica			
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas				

A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Cumple parcialmente	Existe un sistema de informacion tecnica
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Cumple parcialmente	Presenta procedimientos a traves del software
A12.7	Consideraciones sobre auditorias de sistemas de información			
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos				
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	No cumple	
A13	**SEGURIDAD DE LAS COMUNICACIONES**			
A13.1	Gestión de la seguridad de las redes			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Cumple parcialmente	
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Cumple parcialmente	Se verifica a traves de sistemas y de expensas del proveedor
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	No cumple	
A13.2	Transferencia de información			
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				

A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Cumple parcialmente	La parte administrativa cuenta con un sistema
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	No cumple	no se identifica
A13.2.3	Mensajería Electronica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Cumple parcialmente	Cumple con politicas de seguridad de informacion
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Cumple parcialmente	Documeta la parte administrativa
A14	**Adquisición, desarrollo y mantenimiento de sistemas**			
A14.1	Requisitos de seguridad de los sistemas de información			
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes .				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	No aplica	
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La informacion involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Cumple parcialmente	Cumple con base de datos de proteccion
A.14.1.3	Protección de transaccciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Cumple parcialmente	Existe una herramienta dentro del cual no se evidencia funcion exitosa
A14.2	Seguridad en los procesos de Desarrollo y de Soporte			

Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	No aplica	
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	No aplica	Se hace con los externos
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Cumple parcialmente	Se coordina con los proveedores
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	Cumple parcialmente	Todo se relaciona con las facilidades
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Cumple parcialmente	Se desarrolla un sistema de institucionalización
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	No aplica	
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Cumple parcialmente	Por medio de coordinaciones
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	Cumple parcialmente	Se cumple a traves de seguridad
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Cumple parcialmente	Existe criterios de aceptacion
A14.3	Datos de prueba			
Objetivo: Asegurar la protección de los datos usados para pruebas.				

A.14.3.1	Protección de datos de prueba	Control:Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Cumple parcialmente	Se desarrollan sistema de data
A15	**RELACIONES CON LOS PROVEEDORES**			
A15.1	Seguridad de la información en las relaciones con los proveedores.			
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	Cumple parcialmente	Se realiza con la normativa vigente y del proveedor del contrato
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	Cumple parcialmente	Se realiza con la normativa vigente y del proveedor del contrato
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Cumple parcialmente	La base de políticas de proveedor
A15.2	Gestión de la prestación de servicios de proveedores			
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores				
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	No cumple	
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	Cumple satisfactoriamente	Gestiona, coordina la información
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**			
A16.1	Gestión de incidentes y mejoras en la seguridad de la información			

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Cumple parcialmente	Se gestion por la parte administrativa y de sistemas
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Cumple parcialmente	Se realiza las posibles comunicacines de informacion lo cual lograr mejoras
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Cumple parcialmente	A traves de una serie de informaciones y documentos
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	Cumple parcialmente	Realiza la parte administrativa
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Cumple parcialmente	Se documenta a traves de terminaciones de contrato
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	No cumple	No existe infraestructura propia
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Cumple parcialmente	A traves de gestiones de informacion
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**			
A17.1	Continuidad de Seguridad de la información			
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.				

A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	No cumple	
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Cumple parcialmente	Se aplica documentacion con base de datos correspondientes
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Cumple parcialmente	Esta informacion verifica informacion de continuidad
A17.2	Redundancias			
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.				
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	No aplica	
A18	**CUMPLIMIENTO**			
A18.1	Cumplimiento de requisitos legales y contractuales			
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Cumple parcialmente	Se anotan todos los procesos
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de	No cumple	

		propiedad intelectual y el uso de productos de software patentados.		
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.(Con et al., 2018)	Cumple parcialmente	Existe garantia para la informacion
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	No cumple	
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	Cumple parcialmente	Existe documentacion según reglamentos
A18.2	Revisiones de seguridad de la información			
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.				
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Cumple parcialmente	Existe informacion y procesamientos
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	No cumple	
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Cumple parcialmente	Existe revision periodica

DIAGNOSTICO INICIAL DE LOGRO 3: MONITOREO Y MEJORAMIENTO CONTINUO (30 %)

VERIFICAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
1	La entidad tiene una metodología para realizar seguimiento, medición y análisis permanente al desempeño de la Seguridad de la Información.?	No cumple	No existe un SGSI	Se debe tener en cuenta que se desea medir, cuando, quien realizará la medición y cuando se analizaran los resultados.
2	La entidad ha realizado auditorías internas al Sistema de Gestión de Seguridad de la Información?	No cumple	No existe un SGSI	Se deben programar auditorias en un intervalo de tiempo con el fin de evaluar y verificar la conformidad y cumplimiento del Sistema de Gestión de Seguridad de la Información.
3	La entidad cuenta con programas de auditorías aplicables al SGSI donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes?	No cumple	No existe un SGSI	Se debe planificar, establecer, implementar y mantener uno o varios programas de auditoría donde se incluye frecuencia, métodos, responsabilidades, elaboración de informes.
4	La alta dirección realiza revisiones periódicas al Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	Realiza periódicamente	Se deben realizar revisiones a intervalos planificados del Sistema de Gestión de Seguridad de la Información.
5	En las revisiones realizadas al sistema por la Dirección, se realizan procesos de retroalimentación sobre el desempeño de la seguridad de la información?	Cumple parcialmente	Realiza proceso de medición continua	
6	Las revisiones realizadas por la Dirección al Sistema de Gestión de Seguridad de la Información, están debidamente documentadas?	No cumple		Se debe documentar las revisiones realizadas por la Alta Dirección con el fin de verificar el estado del sistema de seguridad de la información, cambios que se presenten a nivel interno o externo que puedan afectar la seguridad de la información y evaluacion de las no conformidades y acciones correctivas. Esta revisión debe incluir las decisiones relacionadas con las oportunidades de mejora

ACTUAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
7	La entidad da respuesta a las no conformidades referentes a la seguridad de la información presentadas en los planes de auditoria?	Cumple parcialmente	Se realiza correccines necesarias por las relaciones formadas	Se deben tomar acciones para eliminar las causas de las no conformidades, para que no vuelvan a ocurrir.
8	La entidad ha implementado acciones a las no conformidades de seguridad de la información presentadas?	Cumple parcialmente	Existe una base de acciones en la parte administrativa	Toda la información de acciones realizadas al Sistema de Gestión de Seguridad de la Información debe ser documentada.
9	La entidad revisa la eficiacia de las acciones correctivas tomadas por la presencia de una no conformidad de seguridad de la información?	Cumple parcialmente	A base de los usuarios se realizan las correcciones	Se debe evaluar la eficacia de las acciones correctivas con el fin de verificar que la no conformidad no se vuelva a presentar.
10	La entidad realiza cambios al Sistema de Gestión de Seguridad de la Información despues de las acciones tomadas?	No cumple		Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.
11	La entidad documenta la información referente a las acciones correctivas que toma respecto a la seguridad de la información?	Cumple parcialmente	Existe informacion para cambios de gestion de seguridad	Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.
12	La entidad realiza procesos de mejora continua para el Sistema de Gestión de Seguridad de la Información?	No cumple		Toda la información de mejora al Sistema de Gestión de Seguridad de la Información debe ser documentada.

Fuente: NTC-ISO-IEC 27001:2013

DIAGNOSTICO FINAL DE LOGRO 1: DEFINICIÓN DE MARCO DE SEGURIDAD Y PRIVACIDAD DE LA ENTIDAD (30%)

PLANEAR				
ITEM	**PREGUNTA**	**VALORACIÓN**	**EVIDENCIA**	**RECOMENDACIÓN**
1	La entidad cuenta con un autodiagnóstico realizado para medir el avance en el establecimiento, implementación, mantenimiento y mejora continua de su SGSI (Sistema de Gestión de Seguridad de la información?	Cumple satisfactoriamente	Según la implementación de la metodología de información	Diligenciar autodiagnóstico de seguridad de la información.
2	La entidad creó un caso de estudio o plan inicial del proyecto, donde se incluyen las prioridades y objetivos para la implementación del SGSI?	Cumple satisfactoriamente	Es definida según la aplicación de la investigación	Crear caso de estudio o plan inicial del proyecto que incluya prioridades y objetivos del SGSI, estructura del SGSI.
3	La entidad contó con la aprobación de la dirección para iniciar el proyecto del SGSI?	Cumple satisfactoriamente	Acta de reunión y aprobación	Debe existir un documento preliminar de aprobación firmado por parte de la dirección donde se aprueba el inicio del proyecto.
4	La entidad ha identificado los aspectos internos y externos que pueden afectar en el desarrollo del proyecto de implementación del sistema de gestión de seguridad de la información?	Cumple parcialmente	Acta de reunión en la comisión	Se deben identificar los temas tanto externos como internos que pueden afectar el desarrollo de los resultados del sistema.
5	La entidad ha identificado las partes interesadas, necesidades y expectativas de estas respecto al Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	Plan de trabajo con la empresa	Se requiere que se identifiquen las partes interesadas tanto internas como externas, detallando cuáles son sus necesidades y expectativas en la implantación del Sistema de Gestión de Seguridad de la Información.
6	La entidad ha evaluado los objetivos y las necesidades respecto a la Seguridad de la Información?	Cumple parcialmente	Existe documentos de gestión	Realizar la identificación de los objetivos y las necesidades que tiene la entidad respecto a la seguridad de la Información.
7	En la entidad se ha definido un Cómite de Seguridad de la Información?	Cumple parcialmente	Acta de signada por la gerencia	Definir mediante acto administrativo el comite de seguridad de la informacion que describa las responsabilidades de los integrantes, reuniones entre otros.
8	La entidad cuenta con una definición del alcance y los límites del Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	Acta de autoridades	Crear un documento de alcance del Sistema de Gestión de Seguridad de la Información y sus respectivos límites en cuanto a TIC, límites físicos, temas internos y externos.

9	En la entidad existe un documento de política del Sistema de Gestión de Seguridad de la Información, el cual ha sido aprobado por la Dirección?	No cumple		Crear un documento que defina la política general del Sistema de Gestión de Seguridad de la Información y sus respectivos límites. Tener en cuenta objetivos del SGSI, marco regulatorio, el cual debe estar debidamente documentado y socializado.
10	En la entidad existe un documento de roles, responsabilidades y autoridades en seguridad de la información?	Cumple satisfactoriamente	Existe un documento de roles	Se deben definir roles y responsabilidades para cada etapa de la Implementación.
11	La entidad tiene establecido algún proceso para identificar, analizar, valorar y tratar los riesgos de seguridad de la información?	Cumple satisfactoriamente	Consta de documentos de metodologia de selección	Se debe seleccionar una metodología para gestionar los riesgos y describir en una matriz de riesgos los resultados de acuerdo a los criterios de aceptación de los mismos. Nota: Si la entidad ya tiene una matriz de riesgos, se deben identificar los riesgos que apunten a la seguridad de la información.
12	La entidad ha realizado una declaración de aplicabilidad que contenga los controles requeridos por la entidad?	Cumple parcialmente	Consta de documentos de metodologi de gestion de riesgos	Crear documento de declaración de aplicabilidad donde se justifique la inclusión y exclusión de controles del Anexo A de la norma ISO27001 versión 2013.
13	La entidad ha evaluado las competencias de las personas que realizan, bajo su control, un trabajo que afecta el desempeño de la seguridad de la Información?	Cumple parcialmente	Consta de documentos	Se debe conservar la información que evidencie las competencias del personal que se encuentre involucrado con la seguridad de la información de la entidad. Se debe definir un plan de capacitación con el fin de que dichas personas adquieran las competencias respectivas.
14	La entidad tiene definido un modelo de comunicaciones tanto internas como externas respecto a la seguridad de la información?	Cumple parcialmente	Utiliza medios de comunicaciones seguras	Se debe desarrollar un modelo que indique el contenido de la comunicación; fechas, a quién se comunica y quién comunica.
15	La entidad tiene la información referente al Sistema de Gestión de Seguridad de la Información debidamente documentada y controlada?	No cumple	Pendiente	Toda la documentación generada del Sistema de Gestión de Seguridad de la Información debe estar debidamente documentada.