# FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

## ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

## TESIS

# Modelo de la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 orientado a las microempresas

**PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS**


**Autor(a) (es):**

**Bach, Sandoval Chero Cesar Arturo**

**ORCID: https://orcid.org/0000-0002-8445-2439**

**Asesor(a):**

**Mg. Jaime Arturo Bravo Ruiz**

**ORCID: https://orcid.org/0000-0003-1929-3969**


**Línea de Investigación:**

**Infraestructura, Tecnología y Medio Ambiente**

**Pimentel – Perú 2023**

**Modelo de la Gestión de la Seguridad de la Información Alineada a la Norma ISO/IEC 27001 Orientado a las Microempresas**

**Aprobación del jurado**

DR., VASQUEZ LEIVA OLIVER

**Presidente de Jurado de Tesis**

Mg., Bravo Ruiz Jaime Arturo

**Secretario de Jurado de Tesis**

Dr., Tuesta Monteza Victor Alexci

**Vocal de Jurado de Tesis**

## DECLARACIÓN JURADA DE ORIGINALIDAD

Quien(es) suscribe(imos) la **DECLARACIÓN JURADA**, soy(somos) Sandoval Chero Cesar Arturo del Programa de Estudios de Ingeniería de sistemas. de la Universidad Señor de Sipán S.A.C, declaro (amos) bajo juramento que soy (somos) autor(es) del trabajo titulado:

**Modelo de la Gestión de la Seguridad de la Información Alineada a la Norma ISO/IEC 27001 Orientado a las Microempresas**

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán (CIEI USS) conforme a los principios y lineamientos detallados en dicho documento, en relación a las citas y referencias bibliográficas, respetando al derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firman:

| | | |
|---|---|---|
| Sandoval Chero Cesar Arturo | DNI: 71870391 |  |

Pimentel, 08 de Febrero de 2023.

**Dedicatorias**

A mis padres Norma Chero B, Santos Sandoval Z.
Hermanos Oscar y Sofía. Y mis angelitos en el cielo
En especial, Juana, Miguel y Carlos Chero, los que forjaron mi camino e impusieron bases de responsabilidad y deseo de superación, la cual me veo reflejado y soy la persona que debo ser.

**Agradecimientos**

A mis padres Norma Chero B, Santos Sandoval Z. Hermanos Oscar y Sofía, quienes me acompañan en cada paso que doy y siempre están ahí para enmendar mis errores.

A mis amigos, compañeros de trabajo y de estudios USS por el apoyo incondicional y motivarme a seguir adelante.

## Resumen

Las Pymes en Perú no están preparadas para identificar la brecha de estabilidad y el 51% de las organizaciones han sido atacadas. Es notable el crecimiento acelerado de internet, en pequeñas y gigantes organizaciones (pymes). Por consiguiente, permanecen sujetos a amenazas y vulnerabilidades novedosas y potencialmente altas que amenazan su sistema de información y muchas otras zonas relevantes. Sin embargo, la mayoría de las pequeñas y gigantes empresas no piensan como una inversión fundamental el hecho de llevar a cabo políticas y mecanismos para el buen desempeño de la compañía. En el desarrollo del presente trabajo de tesis se diseñó y se puso en práctica un modelo propuesto la cual se divide en cinco fases donde cada fase se relaciona con la metodología del Ciclo de Deming (PHVA), la cual se divide en cuatro fases: planear, hacer, verificar y actuar; para establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI). Para la obtención de la información se consideró conveniente el uso de las técnicas de recolección de datos tales como las encuestas, y también ficha de observación para su posterior interpretación; y de esta manera medir la realidad problemática apoyado en el uso de la Norma ISO 27001, lográndose identificar las deficiencias para mejorar los niveles de seguridad y confiabilidad en los sistemas de información de la empresa Seisystem Consultores. Se buscó facilitar las tareas que dificultan a la empresa debido a los recursos limitados con los que cuentan en presupuesto, conocimiento y personal. Como resultado, se consiguió mejorar la seguridad de la información(SI), para lograrlo se identificó el estado de cumplimiento inicial y final de la ISO/IEC 27001:2013 en la empresa. Donde se puede obtener porcentajes pre test y post test de cumplimientos dominios con respecto a la ISO/IEC 27001:2013. De los 114 controles, se tuvo 78 controles de aplicabilidad la cual 50 controles aplicados en la empresa, 28 controles por implementar. Además, se implementó un software como complementación de modelo, se realizó la evaluación de riesgos, la implementación de los controles, el cumplimiento de los requisitos y la concientización del personal. La investigación permitió concluir en la importancia de contar con un SGSI en cualquier empresa, ya que independientemente de su tamaño o sector, el sistema ayuda a proteger los activos de información, gestionando los riesgos que generan.

**Palabras Clave:** Norma ISO 27001, PYMES, Riesgos, Seguridad de la información

## Abstract

Currently, SMEs in Peru are not prepared to identify the stability gap and 51% of organizations have been attacked. The accelerated growth of the internet, in small and giant organizations (SMEs), is remarkable. Consequently, they will become subject to new and potentially high threats and vulnerabilities that threaten their system and many other relevant areas. However, the majority of small and giant companies do not think of carrying out policies and mechanisms for the good performance of the company as a fundamental investment. In the development of this thesis work, a proposed model was generated and put into practice, which is divided into five phases where each phase is related to the Deming Cycle methodology (PHVA), which is divided into four phases: plan , do, check and act; to establish, implement, maintain and improve the Information Security Management System (ISMS). To obtain the information, the use of data collection techniques such as surveys, and also an observation sheet for later interpretation will be conveniently adjusted; and in this way measure the problematic reality supported by the use of the ISO 27001 Standard, being able to identify the deficiencies to improve the levels of security and reliability in the information systems of the company Seisystem Consultores. It sought to facilitate the tasks that make it difficult for the company due to the limited resources they have in budget, knowledge and personnel. As a result, information security will be improved, to achieve this the initial and final compliance status of ISO/IEC 27001:2013 in the company was identified. Where you can obtain pre-test and post-test percentages of domain compliance with respect to ISO/IEC 27001:2013. Of the 114 controls, there were 78 applicability controls, of which 50 controls applied in the company, 28 controls to be implemented. In addition, software was implemented as a complement to the model, risk assessment, implementation of controls, compliance with requirements and staff awareness were carried out. The investigation allowed us to conclude on the importance of having an ISMS in any company, since regardless of its size or sector, the system helps protect information assets, managing the risks they generate.

**Keywords:** ISO 27001 Standard, SMEs, Risks, Information Security

**Índice**

# I. INTRODUCCIÓN

## 1.1. Realidad Problemática.

Según la investigación realizada por Computer Fraud & Security (2021) en EE. UU. Informa que el grupo Lazarus apuntó recientemente a dos empresas en un intento de hurtar investigaciones en relación con las vacunas Covid-19, según estudios de Kaspersky. Ambos ataques utilizaron diferentes estrategias, técnicas y procedimientos (TTP), pero Kaspersky dijo que encontró suficientes puntos en común, incluidas similitudes en el proceso subsiguiente a la explotación, para convencerlo de que el mismo embestidor estaba detrás de los dos incidentes y el Malware utilizado de manera directamente al grupo Lazarus. Por lo tanto, la FTC (Comisión Federal del Comercio) de EE. UU. Señala que más de 275,000 residentes han reportado pérdidas financieras por bastante más de $ 211 millones gracias a las estafas en relación con Covid-19 a partir de inicios del 2020. (Computer Fraud & Security, 2021).

Según el estudio realizado Shinde & Kulkarni, (2021). El minorista estadounidense Target experimentó un grave ataque de seguridad cibernética en el 2013. El motivo primordial detrás del incidente fue que hubo una falta de relación, mal control y administración de incidentes de planificación. En última instancia, costó $ 18.5 mil millones para solucionar las secuelas legales y pensamiento del incidente.

En otro caso, según los datos de la agencia transnacional Equifax se hizo un incidente de incumplimiento ocurrido en 2017 que produjo graves perjuicios a la marca. Lo que terminó en un compromiso involucrado de 147 millones de datos de los consumidores de la organización. Equifax acordó en costear $ 425 millones a las personas dañadas por el percance. (Shinde & Kulkarni, 2021).

Según el estudio realizado por Carnero, Carbajal, J, & Madrid, (2020). En el Perú el 80% de las pequeñas empresas, tienen una vida útil promedio de 3 años, esto se debe al descuido de los elementos de SI (seguridad de la información) que dañan su vida. Las investigaciones aseguran que el 90% de microempresas

en Perú no se encuentran dispuestas para descubrir brechas de SI, mientras que el 51% de las microempresas han sido afectadas y solo el 10% de las microempresas retienen señalizador de gestión de riesgos.

En Indonesia, según los estudios realizados por (Rahmawati, Yudhiyati, & Putritama, (2019). Las PYMES que ignoran los riesgos de seguridad de la tecnología tienen la posibilidad de afrontar diversos peligros. El primer riesgo es una pérdida financiera directa, ya sea provocado por el hurto de activos comerciales. El segundo riesgo es la pérdida indirecta, como el daño al comercio de reputación, perturbación en el funcionamiento, hurto de negocios información confidencial y un chantaje donde el estafador asume la entrada y el control de la indagación empresarial tecnología y exige una indemnización.

En Alemania, según la investigación realizada por Heidenreich, (2019). Da conocer por medio de una encuesta representativa oficial en el área de seguridad informática desarrollada en el año 2017. Muestra que empresas pequeñas tienden a subestimar su seguridad de TI (Tecnología de la Información). Por lo cual la organización alemana con hasta 250 empleados padeció aproximadamente de 55.000 dólares estadounidenses en pérdidas por ataques cibernéticos en 2017.

Las PyMEs en Perú no están preparadas para identificar la brecha de estabilidad y el 51% de las organizaciones han sido atacadas. Según el informe anual de 2017, las pérdidas de la organización peruana superaron los US $ 4 millones. (Garay, C, Armas-Aguirre, & Molina, 2020).

Es evidente el incremento acelerado de internet, en pequeñas y grandes empresas (pymes). Por lo tanto, están sujetos a amenazas y vulnerabilidades nuevas y potencialmente altas que amenazan su sistema de información y muchas otras áreas importantes. No obstante, la mayor parte de las pequeñas y grandes organizaciones no consideran como una inversión importante el hecho de implementar políticas y mecanismos para el buen funcionamiento de la empresa. (Reyes, Muñoz, & Guarda, 2018).

En varios estudios realizados por Rahmawati, Yudhiyati, & Putritama, (2019). Se encontraron que la inquietud por la seguridad es por cierto una de las primordiales barreras para las PYMES al momento de adoptar tecnología de la información.

Por otro lado, las resoluciones disponibles en el mercado son bastante complejos y costosos para ser utilizados por microempresas. No hay resoluciones que consientan a la microempresa acceder a un subjetivo y objetivo de auto medición y comparar ambos puntos entre sí. Por lo que, inclusive si las empresas empresas quieren mejorar su seguridad de TI, es complicado hallar una solución adecuada. (Heidenreich, 2019).

Hoy en día existen distintas metodologías para desarrollar un plan de SGSI. (Dieguez, Cares, & Cachero, 2017). Da conocer sobre la metodología “Action Research” la cual crea cambios en las prácticas de los actores relacionados, Esto lo convierte en un instrumento potente en la gestión de operaciones, por lo consiguiente, los resultados obtenidos evaluaran diferencias en efectividad, efectividad y satisfacción, respecto de la utilización.

Garay, C, Armas-Aguirre, & Molina, (2020). La aplicación del método MAGERIT hace estudios de riesgos para que pueda entender las vulnerabilidades y amenazas que tiene la organización y las medidas de estabilidad que permiten evadir o prever los peligros detectados.

La implementación de la metodología PDCA (Planificar - Hacer - Verificar - Actuar). Se caracteriza por la gestión de procesos y su optimización continua, con una aplicación sencilla y usada correctamente, lo que puede beneficiar mucho en la ejecución de ocupaciones, tanto productivas como administrativas, de una forma más estructurada y positiva. (Leguizamón, Bonilla, & C., 2020)

Muchos de estos modelos de SGSI están basados en estándares internacionales y aseguran buenos resultados cuando se implementan en cualquier microempresa, sin embargo, pocos estudios científicos son aplicables

a las microempresas peruanas, lo que demuestra la falta de conocimiento. Sin embargo, se plantea un Modelo de la administración de la SI alineada a la norma ISO/IEC 27001 orientado a las microempresas debido a que cabe señalar que las políticas de seguridad aplicada a redes informáticas resultan muy relevantes en una microempresa, ya que el más grande tráfico de información circula por internet.

### 1.2. Antecedentes de estudio.

Heidenreich, (2019), realizo un estudio Conceptualization of a measurement method proposal for the assessment of IT security in the status quo of micro-enterprises en Germany. Se tienen que hallar maneras y resoluciones para contribuir a las microempresas a mejorar su seguridad informática. El método se diseñará según los requisitos de la brecha de averiguación con el método presentado según Gutzwiller. Hay dos roles, la organización y un análisis futuro para evaluar el crecimiento del grado de seguridad de TI por medio de este método, con el experto. DESCRIPCIÓN DE LOS MÉTODOS: Por un lado, el método procedimiento de medición simplificado para organizaciones y, sin embargo, el método de procedimiento de medición extendido para el análisis con el experto y su evaluación. En el área “solo en estudio” está diseñada para fases posteriores del trabajo una vez que se hace el método. En este punto, el experto deberá probar la eficacia de este método en un análisis. Al usar el método, la microempresa debe poder medir su seguridad de TI de manera semiautomática. Este proceso se hace por medio de un estudio interno y externo. Perspectiva interna: la conciencia subjetiva que se mide por medio de formularios y la conciencia objetiva se mide por medio de una lista de verificación. Perspectiva externa: está determinada con la ayuda de un instrumento de software. Donde las dos perspectivas se albergan en plantillas de documentos y permanecen accesibles. En la verificación del procedimiento y la información brindada se hace un análisis con un experto en el tiempo de seis meses por esto se hace una segunda medición en el mismo intervalo de tiempo en la cual el experto no hace ni una recomendación. MODELO DE PROCEDIMIENTO DE LA EMPRESA: Se usa modelo (“Área de estudio”), el

cuestionario conduce para evaluar la autopercepción de la organización de su propia seguridad de TI y la herramienta de software establece automáticamente datos acerca de la PC. La finalidad primordial de esta comparación es enseñar la diferencia entre la seguridad de TI fiel y la real seguridad informática. Desde ello se hace la segunda medición y se comparan ambos resultados. MODELO DE PROCEDIMIENTO DEL EXPERTO: Él va seguir estando neutral y no hace ni una recomendación para perfeccionar la seguridad informática de la organización, hace la comparación de la vista interna y externa y es extendido por el experto comparando la medición de los valores subjetivos y objetivos de la organización y al final el experto hace la evaluación de la utilización de medidas de derivación de acción. AGENDA DE INVESTIGACIÓN: Se agendan las labores de indagación considerado en el método propuesto. Se concluye que, con el apoyo del método propuesto, una organización puede medir de manera libre y semiautomática el grado de su seguridad informática. El nivel subjetivo se mide mediante un cuestionario. El nivel objetivo está siendo medido mediante una lista de verificación y un software herramienta y al final el método va a ser evaluado por un experto para identificar la recopilación de datos y detectar cambios en la seguridad de TI a lo largo del lapso establecido.

Yasin, Arman, & Edward, (2020). Realizó un estudio titulado Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ). En Indonesia. La utilización de esta tecnología aún todavía no lo hace tener un grado de capacidad para la administración de SI. Por lo que, se requerirá diseñar recomendaciones y una hoja de ruta ideal para la gobernanza de la información basada en COBIT 2019 e ISO / IEC 27001: 2013 sobre (SGSI). Se usó un método de investigación en Ciencias del Diseño (DSRM) en modo de IDENTIFICAR PROBLEMAS Y MOTIVAR: El objetivo de esta fase es obtener una formulación específica del problema referente con laSI, además se intentará descubrir la solución que se centrará en DitreskrimsusPolda XYZ. DEFINIR OBJETOS DE UNA SOLUCIÓN: En esta fase determinará el objetivo de la formulación del problema referente con la gobernanza de la SI. DISEÑO Y DESARROLLO: Esta fase se describe la implementación del artefacto o el

desarrollo y diseño de un modelo, método o rasgo nuevo de recursos técnicos, sociales o de información mapeando la cláusula y control de fines de la ISO / IEC 27001: 2013 en el dominio del modelo central de COBIT 2019. La cual esta indagación escoge un dominio de modelo central de COBIT usando la cascada de fines de COBIT 2019 y el componente de diseño. DEMOSTRACIÓN: En esta fase, el dominio del modelo central de COBIT 2019 seleccionado de los resultados del diseño se implementará y se usará para evaluar el grado de capacidad con un objetivo del nivel tres. Esta investigación evaluó para revelar la disparidad en la administración de SI esperada y la administración actualmente implementada en Ditreskrimsus Polda XYZ. EVALUACIÓN: En esta fase, habrá observación, medición y mejora del modelo de gobernanza de la SI que hemos implementado. COMUNICACIÓN: En esta fase, los resultados de la evaluación comunicarán su efectividad para brindar una solución para la construcción de un Hoja de ruta de gobernanza de la SI para DitreskrimsusPolda XYZ Los resultados de esta evaluación presentan actualmente que la gobernanza de la SI en Ditreskrimsus Polda XYZ no ha alcanzado el grado de capacidad objetivo 3. El grado de capacidad tres se puede consumar si la definición de un proceso o actividad consigue sus objetivos de una forma estructurada usando activos organizacionales y estar bien determinada. La evaluación de la gobernanza de la SI usando 29 dominios seleccionados del modelo central de COBIT 2019 presentan que el grado de capacidad de Ditreskrimsus Polda XYZ no alcanzó grado de capacidad 3, para conseguir aquel grado, se tiene que llevar a cabo las sugerencias a modo de hoja de ruta, las sugerencias cubren la composición organizativa, compra de recursos humanos y procedimientos que deben cumplirse entre 2021 y 2025.

Velasco, y otros, (2018). En su investigación titulada Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry. En Ecuador. La enorme proporción de información y el bajo grado de seguridad en los procesos críticos de la construcción de industria, ponen en peligro la productividad en la organización. No obstante, la carencia de conciencia sobre los inconvenientes de seguridad dentro de los SI de la entidad ha creado una enorme brecha de vulnerabilidad que, si se explota, podría

colocar en riesgo el adecuado manejo del comercio. Esta investigación se fundamenta en el Plan-Do-Check-Act (PDCA) para la utilización de la Norma ISO 27001 para la industria manufacturera. Primero se da conocer sobre la DEFINICIÓN DEL CICLO DE DEMING: Se muestra una breve explicación de las generalidades del ciclo de Deming, PDCA. CICLO DE DEMING ALINEADO CON ISO 27001: 2013: se muestra la interrelación en medio de las fases del ciclo de Deming y la composición de los capítulos de la norma ISO 27001: 2013. PLANIFICACIÓN: Se explica la idealización aplicada a la organización y el desarrollo de las pautas para cada procedimiento. IMPLEMENTAR Y OPERAR (DO): Instituye los requisitos para medir el desempeño del SGSI, las expectativas de la gestión y sus comentarios sobre ellos. AUDITORÍA Y PRUEBA (VERIFICACIÓN): Define requisitos para medir y evaluar; Revisar SGSI; Medir Efectividad; Comprobar periódicamente la evaluación de riesgos; Realizar análisis internos con regularidad; Registrar acciones y eventos; Revise periódicamente la eficacia del SGSI. MANTENER Y MEJORAR (ACT): Instituye el proceso de optimización del SGSI, con base en las no conformidades identificadas en la organización. Desde de ello se hace un caso de análisis usando MAGERIT que da un método para examinar los peligros y contribuir a hallar y planear las medidas convenientes para mitigar y conservar los peligros bajo control. Desde ello se obtendrán beneficios e importancia de la administración y utilización de controles derivados de la ISO 27001:20013. En esta situación, se han examinado diversos activos en los procesos de la organización. Todo el estudio involucra un enorme esfuerzo para que el SGSI funcione de manera correcta. Todo el estudio y relevamiento de la información llevado a cabo de esta Investigación va ser en vano si la entidad no tiene una clara expectativa de seguridad ya que no toda la información puede protegerse del mismo modo. En esta investigación se ejecutó un SGSI para una industria, se escogió a que se use la norma ISO 27001: 2013 y se usó MAGERIT para la administración de peligros.

Alkilani & Qusef, (2021). Realizó una investigación titulada OSINT Techniques Integration with Risk Assessment ISO/IEC 27001. En Al Jubayhah. Varios estudios mostraron que parte de la información, que forma parte de los

individuos y empresas, está categorizada como información confidencial y privada, y lo más inseguro es que todos tienen la posibilidad de entrar a ella, debido a que permanecen accesibles públicamente en Internet gracias a una mala configuración de los activos o un ciberataque En este artículo, se sugiere un proceso de incorporación en medio de las técnicas seleccionadas de OSINT (inteligencia de código abierto) y la norma ISO 27001 en ciertos dominios importantes para una seguridad adicional (Aramex caso de estudio). Por otro lado, la norma ISO /IEC 27001: 2013 da específicamente requisitos para un SGSI, cuando se identifican los peligros en la evaluación inicial, se seleccionan e implementan controles para mitigarlos, teniendo presente que hay 114 controles establecidos. El proceso de adhesión de OSINT planteado se centrará en los próximos dominios: Primer dominio A.6 Organización de la SI : El propósito es entablar un marco de administración para empezar y mantener el control del logro y el manejo de la SI en la entidad. Segundo dominio A.7 Seguridad de los recursos humanos: El propósito general es garantizar que los trabajadores y contratados se encuentren calificados y comprendan sus papeles y responsabilidades. tercer dominio A.15 Relaciones con los proveedores: el propósito de este anexo es utilizar los controles técnicos y contractuales necesarios e implementar un proceso claro con todos los proveedores externos para afirmar la defensa de los activos de la organización. OSINT además se empleara presentarán técnicas, primera técnica :primer técnica: Recolección de los nombres completos de los empleados, el grado de enseñanza, el historial laboral, los roles laborales e identifique los teléfonos móviles y correos electrónicos de las redes sociales, se puede utilizar la herramienta Hunter.io, segunda técnica: utilización de Google Dorks para monitorear la información del motor de búsqueda, tercera técnica: Detectar los perfiles de redes sociales usados por la organización o el usuario objetivo, cuarta técnica: Identifique cualquier información valiosa que resida en el bucket de S3 de la nube pública, quinta técnica: utilización de herramientas automatizadas como Maltego y Shodan para comprender la estructura de la entidad. Luego de elegir la técnica correcta, el siguiente paso es iniciar datos y empezar el proceso de estudio de la información recopilada y al final, se hace el paso de pivotar e informar, en este paso, se definen nuevos requisitos pivotando los datos recopilados o para

finalizar la indagación y redactar el informe final. Se empezó el estudio de OSINT con relación a la ISO A.6 y se ha podido localizar diversos servidores expuestos en Internet y tienen la posibilidad de ser atacados por fuerza bruta, en el siguiente estudio de la ISO A.7, través de herramientas gratuitas para revisar el historial de ocupaciones maliciosas, esto debe ser esencial, debido a que los estudios mostraron que el 53% de las organizaciones encontraron que los perjuicios provocados por ataques internos eran más dañinos que los ataques externos. Por último, la exploración de la ISO A.15, la herramienta primordial usada ha sido Should-I-Trust para evaluar la madurez del abastecedor y asegurarse de que desempeñen con las normas de seguridad de la compañía. El estudio se hizo contra el abastecedor clave de la organización internacional Aramex llamado Tata Consultancy Services que otorga servicios de operación de SAP. No obstante, no encontramos ni una información importante para detener el contrato con ellos. En esta investigación, se manifestó un grupo de técnicas OSINT que se ocupan de la administración del SGSI, al final las estadísticas presentan que hay un número creciente de información confidencial relacionada con personas y organizaciones disponible públicamente y cómo se puede recopilar y borrar.

Schmitz & Pape, (2020). En su investigación titulada LiSRA: Lightweight Security Risk Assessment for Decision Support in Information Security. En Alemania. La evaluación de peligros de seguridad es una labor desafiante que comúnmente necesita una comprensión fuerte de los escenarios de ataque importantes y entendimiento técnico sobre los efectos mitigantes de cada una de las medidas de seguridad implementadas en las PYMES. Para abordar dichos inconvenientes, se sugiere LiSRA, un marco ligero y específico de dominio para la ayuda a las decisiones en seguridad de la información. LiSRA está diseñado con una perspectiva especial en las necesidades especiales de las PYMES. El marco consta de cuatro fases. ETAPA 1: ENTRADA EXPERTA: En la primera etapa, los profesionales en el dominio establecieron al principio el marco para dominios particulares por medio de la obra de árboles de ataque parametrizados que están ligados a los controles de seguridad. ETAPA 2: ENTRADA DEL USUARIO: Las únicas entradas al cliente correctas son los

niveles de madurez de los controles de seguridad de la entidad. ETAPA 3: CÁLCULO DE RIESGOS: Anterior a que logre empezar el cálculo de peligro se resuelven las dependencias de control. ETAPA 4: APLICACIÓN DE RECOMENDACIÓN: identifica las ocupaciones de seguridad más eficaces y rentables. No obstante, se evalúan diversos puntos relevantes del marco como su aplicabilidad, que ha sido analizada por medio de pruebas de desempeño, análisis de robustez y evaluaciones cualitativas iniciales. Además, revisa la utilidad percibida, así como las preocupaciones de compartir datos confidenciales. Por consiguiente, se planteó LiSRA, un marco ligero para la ayuda a las elecciones en la SI, además se puede usar para detectar las ocupaciones de seguridad futuras más efectivas y rentables.

Subakti & Putra, (2020). En su investigación titulada Integration of TOGAF 9.1 ADM in Enterprise Architecture Smart City Design in the Tourism Domain with ISO 27001. En Indonesia. El método usado en esta indagación ha sido la adhesión de ISO 27001 como un modelo internacional de la SI en el ADM TOGAF 9.1 usado como marco para el diseño de la arquitectura empresarial. El marco TOGAF define la Arquitectura Empresarial en cuatro dominios: AE, AD, AAP, AT. La brecha del diseño de arquitectura en Arquitectura empresarial: se obtuvo la unión de nuevos actores como Smart City Council que se acomoda e interviene en el desarrollo de las localidades inteligentes. Y el proceso de desarrollo de TI se enfoca en la implementación de los datos recolectados. Arquitectura de datos: La interacción de áreas temáticas de información y nuevas entidades de datos en relación además la integración de interacciones de datos big data entre áreas temáticas de información en relación con la unión de nuevos actores. Arquitectura de la aplicación: Se añadieron cinco novedosas aplicaciones, la aplicación de reserva de servicios turísticos incluidos, el panel de control de la actividad turística con base en GIS, la aplicación de monitoreo de la industria del turismo, el portal de la ciudad inteligente y la administración de recursos humanos. Arquitectura Tecnológica: La integración de nueva infraestructura tecnológica para respaldar aplicaciones y negocios y reemplazo de la infraestructura tecnológica por sistemas más sofisticados. Después se hace identificación de los controles de peligro de seguridad de la información

que se refieren al Anexo sobre ISO 27001: 2013, los controles de contestación que fueron creados para dar garantías de elegibilidad fundamentadas en la seguridad de la información. En conclusión, el Diseño de Arquitectura Empresarial de Smart City en el Dominio del Turismo se ha producido junto con las brechas que aparecen utilizando ADM 9.1 TOGAF para obtener una alta seguridad de la información, se han realizado controles y respuestas con base a los límites del Anexo A en ISO 27001: 2013.

Lopez-Leyva, Kanter-Ramirez, & Morales-Martinez (2020). En su investigación titulada Customized Diagnostic Tool for The Security Maturity Level of The Enterprise Information Based on ISO/IEC 27001. En México. Si bien hay herramientas de software que permiten establecer el grado de la SI para las microempresas, estas posibilidades además son costosas y no permanecen accesibles para muchas pequeñas y medianas organizaciones. Esta investigación muestra el diseño de un instrumento digital personalizado centrado en la norma ISO / IEC 27001 para expresar el nivel de madurez de la SI en las entidades. Los procesos de la metodología de diseño: Verificar los requisitos de la norma, priorizar fines y controles, generar el instrumento de diagnóstico, crear el diagrama de flujo, crear los diagramas de interfaz de uso, desarrollar interfaces y bases de datos, desarrollando el código del sistema, realizar prueba funcional, hacer prueba de usuario, realizar pruebas beta (Early-Adopter). Con la ejecución de la metodología propuesta se hizo el desarrollo de la aplicación, la investigación de requisitos, el diseño de interfaces y el flujo general del sistema, que fueron recursos clave para obtener el resultado anhelado, además una buena composición de proyecto y diversas pantallas de selección de fines de control, realización de diagnósticos y resultados de diagnósticos. En conclusión, el diseño de una aplicación virtual para el diagnóstico inicial de seguridad de la información ayuda como alusión inicial para una organización pionera. Esto se hizo por medio de la creación de una herramienta de diagnóstico con base en los 114 controles de la norma ISO / IEC 27001 y el diseño de un procedimiento de flujo específico y de calidad.

Tanovic & Marjanovic, (2019). En su investigación titulada Development of a new improved model of ISO 20000 standard based on recommendations from ISO 27001 standard. En Opatija Croacia. Se implementó un nuevo SGI de TI mejorado basado en el estándar ISO 20000 (una nueva versión mejorada del estándar ISO 20000) en el ámbito real del servicio IPTV / VoIP en el operador de telecomunicaciones de Bosnia y Herzegovina y la utilización de los procesos de la norma ISO 27001 junto con el grupo de ocupaciones, métricas y resultados de métricas. Primero se recibe el modelo de referencia la cual se tomó el servicio de IPTV / VoIP con el operador de Telecom. Después se hace la UTILIZACION DEL SISTEMA DE GESTIÓN DE SERVICIOS DE TI EN EL MODELO DE REFERENCIA: UTILIZACION DE LA NORMA ISO 20000 EN EL ENTORNO EMPRESARIAL DEL SERVICIO IPTV / VOIP DE TELECOMUNICACIONES OPERADOR , por último, se realizan el DESARROLLO DE LA NORMA ISO 27001 EN EL ENTORNO EMPRESARIAL DEL SERVICIO DE IPTV / VOIP DE TELECOMUNICACIONES OPERADOR por medio de una matriz de la norma ISO 27001 con los próximos campos: Nombre de proceso, Actividades necesarias para la implementación, Desempeño o clave Indicador (KPI), Los porcentajes del Medido costo. Los resultados de los procesos dentro de las normas ISO 27001: 2013 han logrado un triunfo de utilización del 98,50%, lo cual es un resultado importante y bueno. Es notable que el proceso de GSI de la norma ISO 20000-1: 2011 consiguió el resultado del 65% del rendimiento, en lo que los procesos en ISO 27001: 2013 lograron el resultado de 98,50%, bastante más de un 33,50% de mejor rendimiento en comparativamente con el proceso correcto en la norma ISO 20000. Se concluye que a partir de esto, es bastante evidente que se ha desarrollado un nuevo modelo mejorado de ISO 20000-1: 2011 para el proceso de GSI con base en las sugerencias y ocupaciones clave de la norma ISO 27001: 2013. Fue creado el modelo mejorado se creó en el modelo de servicio IPTV / VoIP.

Khan, Khan, & Nisar, (2017). Realizo un studio llamado Novice Threat Model using SIEM System forThreat Assessment. En Rawalpindi. Los ataques a la seguridad de la red son el problema primordial y bastante común al que se afrontan los estudiosos de seguridad, así como los usuarios de la red. El

programa LogRhythm SIEM disponible comercialmente realmente otorga un procedimiento bastante maduro para la adición de datos, así como un marco de estudio para examinar, normalizar y recopilar datos proporcionados por los dispositivos de red que, si se necesitan, para la utilización de modelos ontológicos, la parte analítica del programa funciona. AGENTE DE COBRANZA: Este módulo es identificar, sustraer o recibir datos de diferentes dispositivos heterogéneos. ADMINISTRADOR DE RESGISTROS: Esta unidad obtiene y después examina los datos del sensor como transmitido por el representante de cobranza. MOTOR DE INTELIGENCIA AVANZADA (AIE): Establecer las normas de diversas capas para los ataques. GERENTE DE EVENTOS: Ayuda en la correlación de los datos de registro normalizados de fuentes desiguales en ciertos conjuntos lógicos según las normas hechas dentro del módulo AIE. ADMINISTRADOR DE ALARMAS Y RESPUESTAS (ARM): Da cálculos ponderados además conocidos como Prioridad basada en el peligro (RBP) a los datos del acontecimiento transmitidos por el administrador de eventos y además establece si el acontecimiento justifica la obtención o notificación de las actividades de contestación. Los resultados a lo largo de las pruebas se provocaron cerca de 894 alarmas. Alrededor del 48,7% de las alarmas se conocían como alarmas de condición crítica que presentan que la mayor parte de los registros realmente coincidían con las normas de correlación genéricas. Se concluye que las alarmas indicadas por el programa fueron sencillamente categorizadas bajo amenazas de estabilidad y eventos operativos que sencillamente pasan desapercibidos por los administradores. Empero todavía hace falta desarrollar un laboratorio esterilizado para evaluar la efectividad de la jerarquía de normas SIEM iniciativa y borrar los inconvenientes.

Mena, (2018). En su investigación titulada Framework to implement information security management systems: An asset to project management processes En Santiago. La información de las empresas está expuesta a un enorme conjunto de peligros a lo largo del procesamiento, almacenamiento y transmisión entre entidades por medio de Internet. El procedimiento de los colaboradores para acrecentar el marco ya que es de gran beneficio del articulo ha sido de tipo diligente. En seguida las próximas etapas: REVISIÓN BIBLIOGRÁFICA: Se

aplicó la norma ISO / IEC 27001: 2005. SELECCIÓN DEL ENFOQUE METODOLÓGICO DEL MARCO DE TRABAJO: Se indago de los siguientes puntos: SPEM 2.0, metamodelo que será para gestión de entendimiento y (EPFC), la cual se aprendió a usar este programa debido a que lleva a cabo planes para la gestión de procesos. SELECCIÓN DE PROCESOS CRÍTICOS DE UN SGSI: Se escogieron desde los reconocidos requerimientos en la regla ISO / IEC 27001: 2005. Por ello, se utiliza el juicio de profesionales con materiales de referencia, así como los manuales y guías del SGSI. Además, también se ha incorporado el proceso del marco de referencia relacionado con el SGSI. Específicamente, el proceso de orientación de Octave relacionado con el área de evaluación de peligros se ha incluido en el SI. IMPLEMENTACIÓN DEL MARCO DE TRABAJO: Se utilizan procedimientos EPFC, que se derivan de las normas ISO / IEC 27001: 2005 y buenas prácticas derivadas de las Directrices de Evaluación de Peligros de SI: RESULTADOS RELACIONADOS CON LA GESTIÓN DE LA CALIDAD: Los resultados son que se logran junto con la efectividad y el comportamiento de la carga relacionado La programación del proceso es más eficiente. Enfoque procedimental de una sola dirección: los recursos de contenido del marco están disponibles durante el ciclo de vida del producto, incluso a través de las etapas de planificación, ejecución, control, aseguramiento y optimización continua: RESULTADOS RELACIONADOS CON EL DESARROLLO DEL PRODUCTO: De acuerdo con la situación de trabajo, se configuran 35 pasos, y la estructura de cada paso incluye propósito, explicación, entrada, salida, causa y efecto, conceptos y pautas. Hay 10 relacionados con la guía. RESULTADOS RELACIONADOS CON LA GESTIÓN DE PROYECTOS: los activos de esta naturaleza pueden promover una ejecución más clara y rápida de las tareas de gestión de proyectos, reflejando la comprensión sistemática y la línea de base del proceso de puesta en marcha y organización. El desenvolvimiento de este marco demuestra que el proceso de uso de SGSI y los aprovechamientos de las ocupaciones relacionadas con la gestión de proyectos.

Jaramillo, Guaman, & Salazar, (2015). En su investigación titulada Information Security in implementing web applications for small businesses based on

COBIT5-SI. En Indonesia. Con las crecientes amenazas relacionadas con la información importante que la empresa está procesando actualmente, es necesario asegurar que el sistema de información contenga las prácticas correctas para reducir el riesgo de pérdida de información para las PYMES. Estos riesgos pueden provenir de diferentes fuentes, como el personal, procesos o tecnología. El marco de SI está integrado con Cobit 5. Sin embargo, el modelo UWE y el Plan de Estabilidad Abierta de OWASP han obtenido prácticas adecuadas, permitiendo que SI se vea en la implementación de aplicaciones web de microempresas. Así mismo, se incorporó de las reglas y/o normas ISO/IEC 27001, ISO/IEC 27002. COBIT5 – SI: En una tabla muestra de forma general los elementos de todas las reglas mencionadas que fueron la base para elegir la regla de trabajo, da 7 catalizadores de las cuales 3 se analizarán: Catalizador de Procesos, de Servicios, aplicaciones e infraestructura. Por otra parte, tenemos UWE: El desafío en todos dichos casos es dar un instrumento más intuitiva y eficaz para el desarrollo de los sistemas Web, así como garantizar la SI facilitada para el desarrollo de todos los modelos: Estudio de intimación, Modelo Contenido, de presentación. OWASP: representa una secuencia de pruebas que permanecen vinculadas a un ámbito de ocupaciones. Desde ello se unen los controles de estabilidad de la referencia en aplicaciones web. Las etapas a continuar son: Planear (F1P), Edificar (F2C), Validar (F3V), Llevar a cabo (F4E): Realizar (F4E). Como resultados poseemos que el en la evaluación de las técnicas y las reglas propuestas el marco de COBIT 5 para la SI, Permite que la máxima cantidad de control se dirija a la implementación de políticas y estándares de aseguramiento de la información, desde la etapa de desarrollo hasta la implementación y administración de aplicaciones Web de pequeñas empresas. En resumen, además de brindar pautas correctas, las ocupaciones descritas también brindan información sobre los distintos períodos de desarrollo de aplicaciones Web (COBIT 5, OWASP, y finalmente UWE, que brinda ocupaciones para asegurar la información).

Safonova, Lontsikh, Golovina, Elshin, & Koniuchov, (2020). En su investigación titulada Methodology for Creating, Implementing and System Effectiveness Evaluation of the Business Processes' Information Security System. En Rusia. Un crecimiento en el número de ataques a la SI, la administración inadecuada de enormes porciones de datos golpea el desempeño de la organización disminuyendo su productividad y funcionalidad. Los autores propusieron requisitos para un SGSI, incluida una metodología general para producir, llevar a cabo y evaluar (PDCA) la efectividad de los mecanismos del SGSI tomando en cuenta ambos de los estándares más conocidos para la utilización de SGSI, a saber, ISO / IEC 27001: 2013 e ISO / IEC 27005: 2018. LA CONSTRUCCIÓN DEL SGSI DE ACUERDO CON LOS REQUISITOS DE ISO / IEC 27001 SE BASA EN EL MODELO PDCA (CICLO DE DEMING): Planificar (planificación) - fase de construcción de SGSI, estudio de peligros y selección de medidas para eliminarlos.; Hacer (acción) - ase de utilización de las medidas importantes. Verificar (verificación) - la fase de evaluación a causa de los auditores internos de la efectividad de la utilización del SGSI. Actuar (mejora): la etapa de construcción e utilización de actividades correctivas. PROCESO DE GESTIÓN DE RIESGOS BASADO EN EL MODELO EN ISO / IEC 27005: 2018: El estándar bajo importancia usa el mismo modelo de proceso que el estándar descrito antes, incluyendo planeación, utilización, verificación, ocupaciones, mientras tanto que ISO 27001 explica un periodo de administración de estabilidad constante común, ISO / IEC 27005 tiene su proyección sobre los procesos de administración de peligros de estabilidad de la información. En la etapa de "planificación", el sistema de administración de estabilidad de la información de peligros establece la política y metodología de administración de peligros. En la etapa de "implementación" se hace un estudio de peligros y utilización de herramientas de control. En la etapa de "verificación" se monitorea el manejo de los instrumentos de control, se analizan los cambios en los componentes de peligro (activos, amenazas, vulnerabilidades). En la etapa de "acción", según las percepciones de las verificaciones, se toman las ocupaciones correctivas elementales. Por consiguiente, la construcción de un SGSI es un proceso bastante complejo y prolongado. Al generar esta clase de

sistema, no olvide que debería poder gestionar los peligros implementando el enfoque más conveniente para borrar dichos peligros.

Mercaldo, (2021). En su investigación titulada. A framework for supporting ransomware detection and prevention based on hybrid analysis. El ransomware es un malware capaz de encriptar documentos, en esencia bloqueando a los usuarios fuera de sus pc's. Los atacantes para regresar los datos originales tratan de extorsionar para restablecer la entrada. Se presenta un marco híbrido, que combina análisis estático y dinámico, aprovechando las API para prevenir y mitigar las amenazas de ransomware. Y también se presenta la arquitectura del marco propuesto para la mitigación y prevención de ransomware. Mediante análisis estático, obtenemos del ejecutable bajo estudio una lista de las API y librerías que se permanecen invocando. Si la información recopilada coincide con la almacenada en el repositorio de conocimientos de SA (que tiene información relacionada con API y bibliotecas de muestras de ransomware generalizadas), la muestra analizada se marcará como "ransomware"; de lo opuesto, se marcará como "sospechosa" y va a ser enviado al módulo de estudio dinámico. A partir del Análisis dinámico, obtenemos la frecuencia de las API invocadas en tiempo de ejecución. Por cierto, técnicas como la carga dinámica (es mencionar, un mecanismo por el que un programa de PC puede en tiempo de ejecución cargar, llevar a cabo y bajar una biblioteca en la memoria) o la meditación (es mencionar, la función de un programa de PC para analizar, introspectiva y cambiar su propia composición y comportamiento en tiempo de ejecución) puede evadir de forma sencilla la exploración estática. Si las API invocadas recopiladas de este módulo concuerdan con las almacenadas en el repositorio de conocimientos de DA (que tiene información relacionada con las API invocadas por muestras de ransomware), el ejecutable bajo estudio se marcará como "ransomware"; de lo opuesto, la aplicación evaluada se marcará como "legítima". Además, el marco postulado otorga un sistema de retroalimentación: cuando se identifica un ransomware, las propiedades recopiladas (tanto del estudio estático como dinámico) se almacenan en el repositorio de entendimiento que corresponde, con el objeto de incrementar el rendimiento de la identificación y minimizar la era de contestación de los

usuarios. Evaluamos 500 muestras de todo el mundo real originarios del núcleo familiar wannacry y 500 aplicaciones legítimas conocidas (250 de ellas con capacidad de cifrado y los 250 restantes sin capacidad de cifrado). Los resultados logrados de esta indagación demuestran que la utilización de denominadas e invocaciones API para discriminar entre ransomware y aplicaciones legítimas parece ser una forma posible y prometedora de identificación de ransomware. Se concluye que el marco híbrido que explota las denominadas API (por estudio estático) y las invocaciones (por estudio dinámico) está pensado para prevenir la amenaza de ransomware.

Yun, Hur, Shin, & Koo, (2017). En su investigación titulada CLDSafe: An Efficient File Backup System in Cloud Storage against Ransomware. En los últimos años, el ransomware se ha vuelto conocido entre los ciberdelincuentes. El ransomware bloquea la PC de la víctima hasta que ejecuta un pago para recobrar la entrada a sus datos. Se plantea CLDSafe, un sistema de copia de seguridad de archivos novedoso y eficiente contra ransomware. El esquema propuesto cuenta con carga de datos, copias de seguridad y detección de ataques. La cual conserva archivos instantáneos y da una reposición segura por medio del almacenamiento en la nube una vez que una PC está infectada por ransomware. Luego de que nuestro sistema mide las similitudes de archivos entre un documento nuevo en el comprador y un documento antiguo en el servidor, se hace una réplica de seguridad del documento antiguo en el servidor una vez que el documento nuevo se cambia sustancialmente. Y después, solo los usuarios autenticados tienen la posibilidad de restablecer los archivos de respaldo por medio de la utilización del mecanismo de reto contestación. Desde ello se hace una evaluación con fronteras con θ F(a) donde se muestra la sobrecarga de almacenamiento con diversos tipos de archivos, que son pptx, xlsx, docx y hwp. Primero, medimos el espacio solicitado una vez que θ es 100. Y, sin embargo, la F(b) muestra la sobrecarga de almacenamiento aproximadamente entre todos los almacenamientos necesarios en F(a). Una vez que θ es 90, ejecuta una réplica de seguridad del 72% de cada una de las variantes aproximadamente. Esto quiere decir que los archivos que poseen menos del 90% de semejanza son, aproximadamente, el 72% de cada una de

las variantes. Una vez que θ es 80, ejecuta una réplica de estabilidad del 51% de cada una de las variantes aproximadamente. En CLDSafe, establecemos θ en 80 ya que almacena casi el 51% de cada una de las variantes de archivos, y todas ellas es solo un 20% distinto, que es el punto más alto de productividad. En conclusión, CLDSafe puede ahorrar un 41% de espacio de almacenamiento comparativamente con el mecanismo de réplica de estabilidad de las variantes enteras, que es un plan de réplica de estabilidad clásica de varios servicios comerciales de almacenamiento en la nube. Por consiguiente, CLDSafe es más eficiente que los almacenamientos comerciales en la nube contra los ataques que consumen recursos de almacenamiento. Para prevenir el ransomware, propusimos CLD-Safe, un sistema de réplica de estabilidad de archivos novedoso y eficiente. Preserva instantáneas de archivos y otorga la reposición segura una vez que una PC es infectada por un ransomware.

Nechai, Pavlova, Batova, & Petrov, (2020). En su investigación titulada implementation of Information Security System in Service and Trade. En Rusia. En la sociedad moderna es difícil imaginar una empresa que no tenga un sitio web o al menos cuentas en las redes sociales. Sin duda, despierta el interés de la competencia y los piratas informáticos que pueden utilizar los datos para sus propios fines. Para llevar a cabo un sistema de SI, se necesita formular ciertos requisitos: En primer lugar, debemos reconocer el área temática de la siguiente utilización y llevar a cabo un modelo conceptual. El esquema es un diagrama de interacción entre entidades que ilustra las interacciones entre numerosas entidades, como programa, contraseña, host y otras. En segundo lugar, se debería edificar una red semántica. Las redes semánticas representan procesos de toma de elecciones en zonas temáticas seleccionadas. Esta red ayuda a representar los datos que tienen que almacenarse en el futuro sistema de la SI. Luego de edificar esta clase de esquemas, debemos examinar los requisitos de ISO 27001 y planear cómo seguirlos. Con los requisitos formulados y la zona temática analizada, tenemos la posibilidad de equiparar los sistemas de información para la SI y escoger uno para llevar a cabo en el servicio y el negocio. La utilización del sistema de SI en el servicio y el negocio puede producir beneficios tanto cuantitativos como cualitativos. Los resultados

positivos de la utilización del estándar además tienen la posibilidad de ser internos y externos. La SI principalmente se estima un costo sin una ganancia financiera. En conclusión, la obra de un modelo conceptual y una red semántica del área temática se muestra como una gran parte para automatizar los procesos comerciales involucrados con la SI.

## 1.3. Teorías relacionadas al tema.

### 1.3.1 Seguridad de la información.

En ISO Tools exellence, (2021). Se refiere a la triada de la SI, disponibilidad, integridad y confidencialidad, esto debido a que es suficientemente sobresaliente para una microempresa.

La finalidad primordial es conservar el constante mantenimiento de la tríada de la SI debido a que asegura y protege de los activos relevantes de la entidad

### 1.3.2 Gestión de la seguridad de la información

Los controles de SI no son solo técnicas, son controles relacionados con TI. Mezclan diferentes tipos de control y registran el proceso de control físico. Además, la única forma de abordar todas las medidas de seguridad es establecer procesos estables y aclarar responsabilidades. (ISO Tools exellence, 2021)

### 1.3.3 Sistema de gestión de seguridad de la información

El SGSI representa una gran agrupación de políticas de seguridad, técnicas y otras modalidades necesarias para el control de e llevar a cabo todas las reglas de SI de una compañía. (ISO Tools exellence, 2021)

### 1.3.4 Normas familia ISO/IEC 27001.

Este grupo de normas permanecen encargadas de conceder un marco de SGSI y podría ser usado por cualquier organización. (ISO27000.ES, 2021)

Entre las principales normas que se encuentran en la norma ISO/IEC 27000 son:

**ISO 27000:** Tiene las definiciones y aquellos términos que se utilizan a la extensión de toda la serie 27000. Es gratuita a diferencia de las otras reglas que suponen un precio para su implementación. (ISO Tools exellence, 2021)

**ISO 27001:** Es la regla fundamental de toda la cadena ya que esta incluye el grupo de los requisitos del SGSI en las entidades. (ISO Tools exellence, 2021)

**ISO 27002:** Es un manual de afables vivencias en donde se describen los fines de un control y de las evaluaciones aconsejables referente a la SI. (ISO Tools exellence, 2021) . Además, implementa y gestiona controles, teniendo presente el ambiente de peligro de SI de la entidad. (ISO, 2021)

### 1.3.5 Metodología Magerit para gestión de riesgos

Ministerio de hacienda y administraciones públicas - Gobierno de España, (2012). La metodología Magerit tiene como finalidad, desarrollar el desarrollo de gestión de peligros que se adecue mejor a la compañía, así la forma las superficies de gerencia de una compañía puedan tomar elecciones teniendo presente los riesgos que se puedan exponer en la entidad. Esta metodología se apoya en la regla estándar mundial lSO/IEC 31000.

### 1.3.6 Octave Allegro

Mena, (2018). Informa que Octave Allegro (Evaluación de vulnerabilidades, activos y amenazas operacionalmente críticas) es un método para evaluar y detectar peligros de seguridad de la información. (Mena, 2018) da conocer los próximos fines de esta metodología:

- Implementar criterios de evaluación cualitativa del peligro para implantar riesgo operacional de las microempresas.
- Determinar los activos que son de valor de mayor importancia para la labor de las microempresas.
- Decidir las amenazas y vulnerabilidades de los activos de la información.
- Implantar y evaluar los efectos potenciales para las microempresas si los peligros se crean.

Mena, (2018). También da conocer que Octave Allegro se enfoca comunicaciones, peligros, adquisiciones e interesados, principalmente en los activos de información y en el ámbito de cómo son usados, dónde son almacenados, transportados y procesados, además, como estos se expresan amenazas, detenciones y vulnerabilidades como resultado de su uso.

### 1.3.7 PDCA(Ciclo-Deming)

Mena, (2018). Esta regla aplica el método "Planificar-Hacer-Verificar-Actuar" para conformar todo el SGSI.

1. Planificar: Mena, (2018). Informa que es el proceso de fijación de conocimientos sobre la SI organizacional y la necesidad de políticas y fines de la SI.
2. Hacer: Mena, (2018). Informa dice que esta etapa se desarrolla a cabo determinando la manera en que opera, controla, procesos y métodos de la política del SGSI.
3. Verificar: Mena, (2018). Informa dice que esta etapa se desarrolla a cabo repasando y midiendo el funcionamiento del proceso contra las políticas, fines, prácticas en la ejecución del SGSI y reportando los resultados para la evaluación de su efectividad.
4. Actuar: Mena, (2018). Informa que esta etapa se realiza por medio de la adopción de actividades correctivas y preventivas fundamentadas en los resultados de las evaluaciones, auditorías internas y revisión de la gestión sobre la seguridad de la gestión u otras ocupaciones de seguimiento para poder hacer la optimización continua.

### 1.3.8 Metodología Ebios.

Restrepo, (2018), sugiere que Ebios es un método de estudio y administración de peligros de estabilidad de sistemas de información que comprende un grupo de guías y herramientas de código independiente, enfocado a gestores del peligro de TI. Elaborada en un inicio por el régimen francés.

**Fases**

Restrepo, (2018), indica las fases de la Metodología mencionada:

**Fase 1.** Restrepo, (2018) Informa que encontramos estudio del entorno, estudiando cuales son las dependencias de los procesos del comercio en relación con los sistemas de información.

**Fases 2 y 3,** Restrepo, (2018) Informa que encontraremos el estudio de las necesidades de estabilidad y de las amenazas, determinando los aspectos del problema.

**Fases 4 y 5,** Restrepo, (2018) Informa que en esta fase encontráremos Resolución del problema, estableciendo las metas de estabilidad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los peligros residuales.

### 1.4. Formulación del Problema.

¿Cuál sería el efecto de la implementación de un nuevo Modelo de la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en las microempresas?

### 1.5. Justificación e importancia del estudio.

Este proyecto de investigación está en la línea de investigación infraestructura, Tecnología y medio ambiente de la escuela de ingeniería de sistemas de la Universidad Señor de Sipán. Se necesita que toda Microempresa que busca excelencia en los servicios o productos que da, adopte un Modelo de SGSI para el desempeño correcto de la información, garantizando de esta forma su disponibilidad, confidencialidad e integridad. Ya que cada vez hay más microempresas y sistemas expuestos a diversos tipos de amenazas aprovechándose de muchas vulnerabilidades existentes, logren llegar a controlar y/o influir de forma crítica la información en distintas maneras como fraude, espionaje o sabotaje.

El plan se realizará debido a que se cuenta con información para el desarrollo de este, que dejará la implementación de la regla de estabilidad informática ISO

27001 permitiendo mejorar la disponibilidad, confidencialidad e integridad de los sistemas de información y comunicación.

Para la fijación de la regla de la SI ISO 27001 se cuenta con la siguiente Información:

- ISO 27001
- SGSI-en-Microempresas.

La norma de la SI ISO 27001 ayudará al ordenamiento del comercio por consiguiente obligará a conceptualizar de manera bastante rigurosa tanto las responsabilidades como las obligaciones que se debe hacer y consumar y, así, se ayudará a reforzar la organización interna.

La información, los procesos son activos bastante relevantes, donde destaca la triada de la información: disponibilidad, confidencialidad e integridad la cual son fundamentales para conservar niveles de conformidad legal, productividad e imagen bastante representativa para poder hacer estos fines de la microempresa y afirmar beneficios económicos.

La implementación del modelo de la administración de la SI alineada a la regla ISO/IEC 27001 generará ahorros para la microempresa, ya que los costos van a ser sustentados por el creador del plan de tesis.

## 1.6. Hipótesis.

La Implementación de un nuevo Modelo de la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 mejorara significativamente la seguridad de la información en las microempresas.

## 1.7. Objetivos.

### 1.7.1. Objetivo general.

Implementar un nuevo Modelo de la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en las microempresas.

### 1.7.2. Objetivos específicos.

- Diagnosticar la situación de las microempresas con respecto a la gestión SI.
- Realizar una revisión sistemática de modelos sobre gestión de la SI.
- Diseñar el modelo de gestión de la SI alineado a la norma ISO 27001.
- Validar el modelo de gestión de la SI.
- Implementar un software para el soporte operativo al modelo de gestión de la SI.

## II. MATERIAL Y MÉTODO

### 2.1. Tipo y Diseño de Investigación.

Esta averiguación es de un tipo cuantitativa puesto que se va a examinar, entender y medir y desde ello sacaremos resultados estadísticos en el plan de indagación, está con base en una averiguación empírico-analista debido a que los estudios poseemos números estadísticos para ofrecer contestación a unas causas-efectos específicas. Sinnaps (2020)

Dependiendo del tipo de estudio, el diseño a utilizar es cuasi-experimental en el sentido de que en aquellos escenarios donde la asignación de unidades no es aleatoria, existe un conjunto de métodos o estrategias de investigación orientados a evaluar los efectos del tratamiento y analizar a los sujetos observados en función de tiempo. Turmero (s.f),

### 2.2. Población y muestra.

La unidad de investigación de este estudio son las metodologías, marcos de trabajo relacionados con la gestión de riesgos y aplicación de dominios alienada

con las normas ISO/IEC 27001 para microempresas, y luego la población que existe aparecerá en la lista.

**Población**

1. Metodología Magerit para la gestión de riesgos, basado en PDCA, alienado a la norma ISO 27001:2013.
2. Metodología Octave para la gestión de riesgos, ISO 27001:2013.
3. Metodología Action Research para la Gestión de controles de seguridad de la información.
4. Marco COBIT 2019 para evaluación de la gobernanza de la seguridad de la información, alineado a la norma ISO/IEC 27001.

**Muestra**

Para la adecuada elección de la muestra, se realizará un muestreo no probabilístico por conveniencia, de tal forma que se tomaran los 4 modelos relacionados a la norma ISO/IEC 27001 con sus respectivas metodologías encontradas, se analizaran y se tomará cual más se adecue a la organización.

*Tabla 1: Estándares para la gestión de seguridad de la información y metodologías para la gestión de riesgos*

| **Estándares para la gestión de seguridad de la información y metodologías para gestión de riesgo** | | | | |
|---|---|---|---|---|
| **Estándares y metodologías** | **País de origen de la metodología para gestión de riesgo** | **Entorno** | **Finalidad** | **Referencias** |
| Norma ISO/IEC 27001 y metodología Magerit para gestión de riesgos. | Ecuador | Medianas y grandes empresas | Análisis de los riesgos en los sistemas de seguridad de la información. | Velasco J; Ullauri R; Pilicita L; Jácome B; Saa P & Moscoso O. (2018) |
| PDCA para implementar un SGSI según la norma ISO 27001 | Ecuador | Pequeñas y medianas empresas | Permite que las personas se involucren en las estrategias de protección de la información. | Velasco J; Ullauri R; Pilicita L; Jácome B; Saa P & Moscoso O. (2018) |
| Norma ISO 27001/2005 para el desarrollo e implementación de un SGSI y OCTAVE para la gestión de riesgos | Santiago | Medianas y grandes empresas | Análisis de los riesgos en los sistemas de seguridad informática para descubrirlos oportunamente. | Mena A. (2018). |

| | | | | |
|---|---|---|---|---|
| Norma ISO 27001: 2013 y el marco de COBIT 2019 para evaluación de la gobernanza de la seguridad de la información | Indonesia | Pequeñas y medianas empresas | Permite que las personas se involucren en las estrategias de protección de la información. | Yasin M; Ahmad, A; Edward I; Shalannanda W. (2019). |

Nota: Elaboración propia

Según el analisis por conveniencia se llegó a seleccionar un modelo con su respectiva metodología para la gestion de riesgos.

1.- Metodología Magerit para la gestión de riesgos, basado en PDCA, alienado a la norma ISO 27001:2013.

## 2.3. Variables, operacionalización.

| Variables | Indicador | Ítem | Técnica e instrumentos de recolección de datos |
|---|---|---|---|
| Modelo de Gestión de la seguridad de la información (V.I) | Valoración de activos de información. (Unidad) | $V.A = \frac{C+I+D}{3}$ | **Técnica:** Observación **Instrumento** Ficha digital de observación |
| | Nivel riesgo (Unidad) | $Nivel\ de\ riesgo = NI * POR$ | |
| | Número de controles aplicados (Unidad) | $TCA = \sum si$ | |
| Gestión de la Seguridad de la información (V.D) | Estado de cumplimiento de políticas de seguridad de la información en la empresa. | $TRP = \sum Si$ | **Técnica:** Encuesta |
| | | $TRN = \sum No$ | |
| | Grado de la seguridad de la información y los equipos de cómputo. | | |
| | Grado de verificación de control de acceso. | | |

*Tabla 2: Variables, operacionalización*

Nota: Elaboración propia

## 2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

*Tabla 3: Técnicas e instrumentos de recolección de datos, validez y confiabilidad.*

| TECNICA | INSTRUMENTO | DETALLE |
|---|---|---|
| Observación | Ficha digital | |
| Encuesta | Cuestionario | Se utilizará esta técnica para recopilar información sobre el estado de la seguridad de la información. |

Nota: Elaboración propia

## 2.5. Procedimiento de análisis de datos.

Para el indicador nivel de cubrimiento del SGSI en activos de información se necesitan dos variables, V.A, C, I y D las cuales representan lo siguiente:

Valoración de activos = V.A
Confidencialidad = C
Integridad = I
Valoración de activos del SGSI: V. A=(C+I+D) /3
El resultado de esta operación mostrara el nivel de valoración de los activos del SGSI de la organización.

Para el indicador del nivel de riesgo tenemos las siguientes variables NR, NI, POR las cuales representan lo siguiente:
Nivel de Riesgo = NR
Nivel de impacto = NI
Probabilidad de ocurrencia de riesgo = POR
Para calcular el nivel de riesgo: Nivel de riesgo=NI*POR

El resultado será que por cada amenaza de calculará el valor del riesgo

Variables que participan: Probabilidad (Tabla 13), Impacto (Tabla 14)

Para el indicador de Número de controles aplicados se representa lo siguiente:

Total de controles aplicados = TCA

Para calcular el número de controles aplicados:

$$TCA = \sum si$$

Para el indicador Estado de cumplimiento de políticas de seguridad de la información en la empresa. Se utilizarán dos variables con valores dicotómicos (dos valores). A continuación, se presentan las variables:

La empresa tiene definido una política general de seguridad de la información = EPGSI

La empresa realiza las actividades de control y protección de la información = EACPI

Formula:

EPGSI = NO; EPGSI = SI

EACPI = NO; EACPI = SI

En donde el valor NO representa a una respuesta negativa y el valor SI representa una respuesta positiva.

Calculando el total:

Total de repuesta Positiva: TRP

Total de repuesta Negativa: TRN

$$TRP = \sum Si$$

$$TRN = \sum No$$

Para el indicador Grado de la S.I y los equipos de cómputo posee dos variables dicotómicas que se explicaran a continuación:

La empresa tiene lineamientos a través del responsable de seguridad para que los trabajadores cumplan las políticas de seguridad = ELSTPS

La empresa tiene normas para la protección de instalaciones físicas = ENPIF

Formula:

ELSTPS = NO; ELSTPS = SI

ENPIF = NO; ENPIF = SI

En donde el valor NO representa a una respuesta negativa y el valor SI representa una respuesta positiva.

Calculando el total:

Total de repuesta Positiva: TRP

Total de repuesta Negativa: TRN

$$TRP = \sum Si$$

$$TRN = \sum No$$

Para el indicador grado de verificación de control de acceso tiene dos variables con valores dicotómicos a continuación se especifican:

La empresa tiene normas para controlar el acceso de los usuarios a datos almacenados en los servidores = NAUAS

La empresa tiene estándares para controlar el acceso y uso a las aplicaciones de la empresa = ECAUA

Formula:

NAUAS = NO; NAUAS = SI

ECAUA = NO; ECAUA = SI

En donde el valor NO representa a una respuesta negativa y el valor SI representa una respuesta positiva.

Calculando el total:

Total de repuesta Positiva: TRP

Total de repuesta Negativa: TRN

$$TRP = \sum Si$$

$$TRN = \sum No$$

### 2.6. Criterios éticos.

Toda la información proporcionada por la empresa, para fines de investigación en el presente trabajo de tesis, no debe prestarse para otros fines que no sean la de lograr resultados en el trabajo de investigación.

### 2.7. Criterios de Rigor Científico.

En este trabajo de investigación se deben tener en cuenta los siguientes factores: puntos de certeza y afirmación, 2 criterios de rigor científico más adecuado para este trabajo. La credibilidad es la realidad percibida y expresado por todos los empleados de la organización en el momento de su presentación tomar una encuesta o completar una encuesta. Sin embargo, la declaración no una alusión a afirmaciones veraces y directas sobre las que el investigador percibido dentro del sitio de análisis, en esta situación en la organización Seisystem Consultores.

## III. RESULTADOS.

### 3.1. Resultados en Tablas y Figuras.

Después de haber aplicado las medidas de seguridad dentro de la empresa Seisystem consultores, se procedió a realizar el cálculo de los indicadores previamente seleccionados.

Para el indicador se realizó la valoración de activos en la organización Seisystem Consultores. Se valorizaron según los 3 pilares de la SI (Confidencialidad, Disponibilidad e Integridad) y se obtuvo la valoración de cada activo usando la siguiente formula:

$$V.A = \frac{C + I + D}{3}$$

*Tabla 4: Valoración de activos*

| Categoría | ID de Riesgo | Activo | Criterios | | | Total | Impacto |
|---|---|---|---|---|---|---|---|
| | | | C | I | D | | |
| DATOS | D-001 | **Datos del personal** | 7 | 7 | 8 | 7 | A |
| | D-002 | **Control de salarios** | 10 | 9 | 9 | 9 | A |
| | D-003 | **Datos de los clientes** | 10 | 7 | 7 | 9 | A |
| | D-004 | Datos de inventario de equipos | 4 | 4 | 4 | 4 | M |
| | D-007 | **Registros de órdenes de compras** | 7 | 10 | 8 | 8 | A |
| | D-010 | **Reporte de acceso de usuarios Radmin VPN Y ANYDESK** | 8 | 9 | 9 | 9 | A |
| | D-011 | **Registros de órdenes de ventas** | 7 | 10 | 8 | 8 | A |
| | D-012 | **BD Empresa/ BD Clientes** | 7 | 10 | 9 | 9 | A |
| | S-002 | Internet | 4 | 7 | 9 | 7 | M |
| | S-003 | Correo electrónico | 7 | 6 | 7 | 7 | M |
| SOFTWARE | SW-001 | **Lista de instaladores de Software** | 7 | 9 | 10 | 9 | A |
| | SW-003 | **Software “Scan web”** | 9 | 9 | 9 | 9 | A |
| HARDWARE | HW-003 | **Laptop de desarrollo** | 9 | 9 | 10 | 9 | A |
| MEDIA | MED-001 | **Documentación administrativa** | 8 | 9 | 9 | 9 | A |
| INSTALACIÓN | INS-001 | **Oficina Alfonso Ugarte** | 8 | 6 | 9 | 8 | A |

Nota: Elaboración propia

En la Tabla 5 se encuentran los activos que es de gran efecto y permanecen referente al desarrollo core, solo 3 de ellos son medio y de gran efecto para la organización, además se encuentran ligados al core, o sea, que dichos activos se admitirán en importancia en la evaluación de peligro.

Para el indicador de evaluación de riesgo se aplicó la siguiente formulara con respecto a los activos de la información ya antes mencionados.

$$Nivel\ de\ riesgo = NI * POR$$

*Tabla 5: Pre Evaluación de riesgo*

| PROCESO | ACTIVO | ID DEL RIESGO | AMENAZA | | OCURRENCIA | | RIESGO | |
|---|---|---|---|---|---|---|---|---|
| | | | IMPACTO | VALOR | PROBABILIDAD | VALOR | TOTAL | ZONA RIESGO |
| CONTABILIDAD | Datos del personal | ALT006 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT013 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | MOD002 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | MOD003 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | MOD004 | BAJO | 1 | PROBABLE | 3 | 3 | M |
| | | MOD05 | BAJO | 1 | PROBABLE | 3 | 3 | M |
| | Control de salarios | BAJ001 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT014 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT028 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT051 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT053 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT007 | MEDIO | 2 | PROBABLE | 3 | 6 | A |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | ALT011 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | MOD002 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | MOD008 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | ALT002 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | **Registros de órdenes de compras** | ALT008 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT012 | ALTO | 3 | PROBABLE | 2 | 6 | A |
| | | ALT013 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | **Persona** | EXT002 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT015 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT002 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | **Registros de órdenes de Ventas** | ALT008 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT012 | ALTO | 3 | PROBABLE | 2 | 6 | A |
| | | ALT013 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT015 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT019 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| **GERENCIA GENERAL** | **Correo electrónico Toda la** | ALT022 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT024 | MEDIO | 2 | PROBABLE | 3 | 6 | A |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | **documentación información** | | | | | | | | |
| | **Oficina Alfonso Ugarte** | MOD010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | **Datos del cliente** | EXT009 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT001 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| **CONSULTORIA Y DESARROLLO DE SOFTWARE** | **Lista de instaladores** | ALT001 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT011 | MEDIO | 2 | CASI SEGURO | 4 | 8 | A |
| | **Reporte de acceso de usuarios Radmin VPN Y ANYDESK** | EXT001 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT011 | ALTO | 3 | PROBABLE | 4 | 12 | E |
| | | EXT014 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT017 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT023 | ALTO | 3 | CASI SEGURO | 4 | 12 | E |
| | | EXT024 | ALTO | 3 | CASI SEGURO | 4 | 12 | E |
| | | EXT026 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT048 | ALTO | 3 | CASI SEGURO | 4 | 12 | E |
| | | ALT010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT021 | MEDIO | 2 | CASI SEGURO | 4 | 8 | A |
| | | EXT002 | ALTO | 3 | CASI SEGURO | 4 | 12 | E |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **Persona** | EXT015 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT005 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | **Laptops de desarrollo** | EXT014 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT022 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT025 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT027 | ALTO | 3 | CASI SEGURO | 4 | 12 | E |
| | | EXT031 | ALTO | 3 | PROBABLE | 3 | 3 | E |
| | | EXT040 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT052 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT001 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT005 | MEDIO | 2 | CASI SEGURO | 4 | 8 | A |
| | **Software Scan Web** | EXT032 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT049 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | **BD Empresa / BD Clientes** | EXT049 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT003 | ALTO | 3 | PROBABLE | 3 | 6 | A |
| **TODOS LOS PROCESOS** | **Oficina Alfonso Ugarte** | EXT050 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT001 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT017 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | MOD007 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |

Fuente: Elaboración Propia

En la tabla 6 se puede observar la evaluación de riesgo de cada activo dependiendo el área involucrada, para ello se aplicaron planes de acción (Anexo 10). La cual el nivel del riesgo se muestra así:

*Tabla 6: Post Evaluación del riesgo*

| PROCESO | ACTIVO | ID DEL RIESGO | AMENAZA | | OCURRENCIA | | RIESGO | |
|---|---|---|---|---|---|---|---|---|
| | | | IMPACTO | VALOR | PROBABILIDAD | VALOR | TOTAL | ZONA RIESGO |
| CONTABILIDAD | Datos del personal | ALT006 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | ALT013 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | MOD002 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | MOD003 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | MOD004 | BAJO | 1 | RARO | 1 | 1 | B |
| | | MOD005 | BAJO | 1 | IMPROBABLE | 2 | 2 | B |
| | | BAJ001 | BAJO | 1 | RARO | 1 | 1 | B |
| | Control de salarios | EXT014 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | EXT028 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT051 | ALTO | 3 | IMPROBABLE | 2 | 6 | M |
| | | EXT053 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | ALT007 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | ALT011 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | MOD002 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | MOD008 | MEDIO | 2 | RARO | 1 | 2 | B |
| | Registros de órdenes de compras | ALT002 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | ALT008 | MEDIO | 2 | IMPROBABLE | 2 | 4 | A |
| | | ALT010 | MEDIO | 2 | IMPROBABLE | 2 | 4 | A |
| | | ALT012 | MEDIO | 2 | RARO | 1 | 2 | B |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ALT013 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | Persona | EXT002 | MEDIO | 2 | IMPROBABLE | 2 | 4 | A |
| | | EXT015 | BAJO | 1 | RARO | 1 | 1 | B |
| | | ALT002 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | Registros de órdenes de Ventas | ALT008 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | ALT010 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | ALT012 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT013 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | ALT015 | BAJO | 1 | RARO | 1 | 1 | B |
| | | ALT019 | MEDIO | 2 | RARO | 1 | 2 | B |
| GERENCIA GENERAL | Correo electrónico | ALT022 | MEDIO | 2 | RARO | 1 | 2 | B |
| | Toda la documentación información | ALT024 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | Oficina Alfonso Ugarte | MOD010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | Datos del cliente | EXT009 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT001 | MEDIO | 2 | RARO | 1 | 2 | B |
| CONSULTORIA Y DESARROLLO DE SOFTWARE | Lista de instaladores | ALT001 | BAJO | 1 | RARO | 1 | 1 | B |
| | | ALT011 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT001 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT011 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | Reporte de acceso de usuarios | EXT014 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT017 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT023 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **Radmin VPN Y ANYDESK** | EXT024 | ALTO | 3 | RARO | 1 | 3 | M |
| | | EXT026 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT048 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | ALT010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT021 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT002 | MEDIO | 2 | RARO | 1 | 2 | B |
| | **Persona** | EXT015 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT005 | ALTO | 3 | IMPROBABLE | 2 | 6 | M |
| | **Laptops de desarrollo** | EXT014 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT022 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT025 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT027 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | EXT031 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT040 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT052 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT001 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT005 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | **Software Scan Web BD Empresa / BD Clientes** | EXT032 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | EXT049 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT049 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT003 | ALTO | 3 | PROBABLE | 3 | 6 | A |
| **TODOS LOS PROCESOS** | **Oficina Alfonso Ugarte** | EXT050 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT001 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT017 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | MOD007 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |

Nota: Elaboración propia

En la tabla 6 se visualiza que aplicando PLAN DE TRATAMIENTO DE RIESGOS (Anexo 9) logró el grado de peligro de cada uno de ellos disminuyera esto debido a los procesos y/o áreas involucradas. Para ver generalmente los detalles de la evaluación de riesgos, que se encuentran en el Anexo 7. Para obtener la información fue solicitada se realizó a la Cámara de Comercio y producción de Lambayeque (CCLAM), se listó a todas las microempresas que se localiza en la ciudad de Chiclayo, posteriormente se establecieron tres criterios de evaluación, los cuales son: Procesos, uso de tecnologías y accesibilidad a datos, siento este último criterio, determinante para de esta manera poder implementar correctamente el SGSI.

A partir de ello se seleccionó la empresa para poder aplicar el modelo de SGSI, la cual fue la organización Seisystem consultores, que se localiza en la ciudad de Chiclayo. La cual se diagnosticó el estado actual de la microempresa. Se aplicó el instrumento de ficha de observación donde obtenemos los siguientes resultados con respecto a los dominios según la ISO/IEC 27001:2013 existentes en la empresa Seisystem consultores.

**Cuadro Porcentaje de Cumplimiento por Dominios Pre Test.**

*Tabla 7: Porcentaje de Cumplimiento por Dominios Pre Test.*

| N° | DOMINIOS EVALUDOS SEGÚN ISO 27001 | ANALISIS INICIAL | |
|---|---|---|---|
| **A.5** | Políticas de seguridad de la información | **0%** | **No existe** |
| **A.6** | Organización de la seguridad de la información | **0%** | **No existe** |
| **A.7** | Seguridad de los recursos humanos | **6.7%** | **Inicio** |
| **A.8** | Gestión de activos | **8%** | **Inicio** |
| **A.9** | Control de acceso | **8.6%** | **Inicio** |
| **A.10** | Criptografía | **0%** | **No aplica** |
| **A.11** | Seguridad física y ambiental | **7.3%** | **Inicio** |
| **A.12** | Seguridad de las operaciones | **5%** | **Inicio** |
| **A.13** | Seguridad de las comunicaciones | **26.6%** | **Inicio** |
| **A.14** | Adquisición, desarrollo y mantenimiento de sistemas | **0%** | **No existe** |
| **A.15** | Relación con los proveedores | **13.3%** | **Inicio** |
| **A.16** | Gestión de Incidentes de seguridad de la información | **0%** | **No existe** |
| **A.17** | Aspectos de seguridad de la información en la gestión de continuidad del negocio | **13%** | **Inicio** |
| **A.18** | Cumplimiento | **8%** | **Inicio** |

Nota: Elaboración propia

Continuando con los dominios se realizó un Post Test aplicando el instrumento de ficha de observación (ANEXO 11) obteniendo los siguientes resultados. Aplicando formula básica para calcular el porcentaje: $RRC = \frac{\sum va}{np}$

PRC: Porcentaje

VA: valor de aplicación

NP: número de controles aplicado

**Cuadro Porcentaje de Cumplimiento por Dominios Post Test.**

*Tabla 8: Porcentaje de Cumplimiento por Dominios Post Test.*

| N° | DOMINIOS EVALUDOS SEGÚN ISO 27001 | ANALISIS INICIAL | |
|---|---|---|---|
| **A.5** | Políticas de seguridad de la información | **62.5%** | **Inicio** |
| **A.6** | Organización de la seguridad de la información | **47.2%** | **inicio** |
| **A.7** | Seguridad de los recursos humanos | **41.3%** | **Inicio** |
| **A.8** | Gestión de activos | **71%** | **Inicio** |
| **A.9** | Control de acceso | **45%** | **Inicio** |
| **A.10** | Criptografía | **0%** | **No aplica** |
| **A.11** | Seguridad física y ambiental | **31%** | **Inicio** |
| **A.12** | Seguridad de las operaciones | **55.6%** | **Inicio** |
| **A.13** | Seguridad de las comunicaciones | **60%** | **Inicio** |
| **A.14** | Adquisición, desarrollo y mantenimiento de sistemas | **90%** | **inicio** |
| **A.15** | Relación con los proveedores | **40%** | **Inicio** |
| **A.16** | Gestión de Incidentes de seguridad de la información | **57%** | **inicio** |
| **A.17** | Aspectos de seguridad de la información en la gestión de continuidad del negocio | **60%** | **Inicio** |
| **A.18** | Cumplimiento | **50%** | **Inicio** |

*Nota: Elaboración propia*

Estos resultados lo obtuvimos aplicando el modelo de SGSI, realizando el proceso respectivo y aplicando PLAN DE TRATAMIENTO DE RIESGOS (ANEXO 9). Con ello conseguimos mejorar los procesos de la organización con respecto a los componentes importantes que brinda la ISO/IEC 27001:2013 que son disponibilidad de la confidencialidad, indagación e integridad, En la siguiente tabla se muestra en PRE TEST y un POST TEST de nuestro indicador Número de controles aplicados de los controles con la unidad de medida (UND) correspondiente aplicada en los indicadores. La cual se realizó la siguiente fórmula: $TCA = \sum si$

*Tabla 9: Resumen de los números de controles aplicados Pre-Post Test*

| TABLA DE RESUMEN | | | | |
|---|---|---|---|---|
| INDICADOR: NUMERO DE CONTROLES | | | | |
| N° CONTROLES TOTALES APLICAN/ EXISTEN | CONTROLES | PRE TEST (UND) | | POST TEST (UND) TCA = 78 |
| 114 | NO EXISTE | 102 | | 36 |
| | SI EXISTE | 12 | | **78** |
| NO APLICA | | | | |
| 36 | | | | |

Nota: Elaboración propia

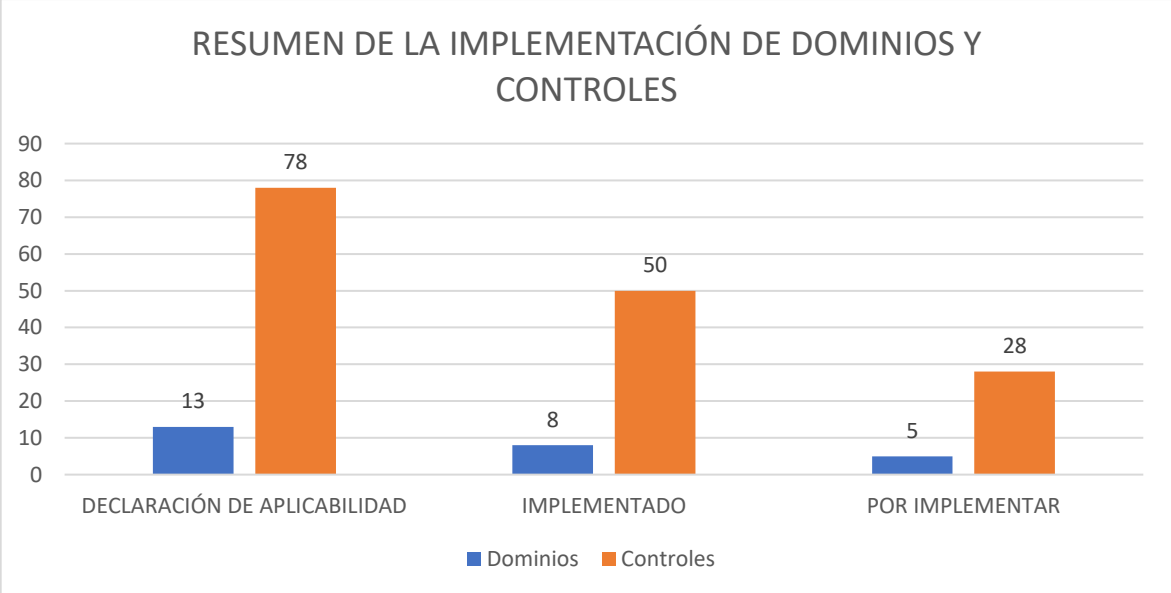
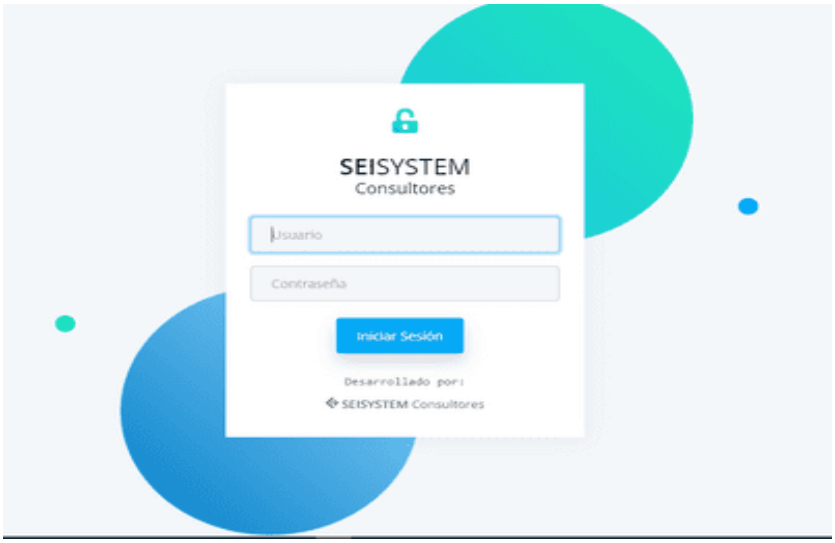



*Ilustración 1: En la ilustración 1 se muestra el resumen con respecto a los dominios y controles aplicados dentro de la empresa Seisystem consultores, la cual 50 controles que equivalen a 8 dominios se han implantado y 28 controles que equivalen a 6 dominios quedan por implementar en el segundo grupo que se planteó en el desarrollo de un Plan de ejecución de medidas de seguridad" (Anexo 10).*

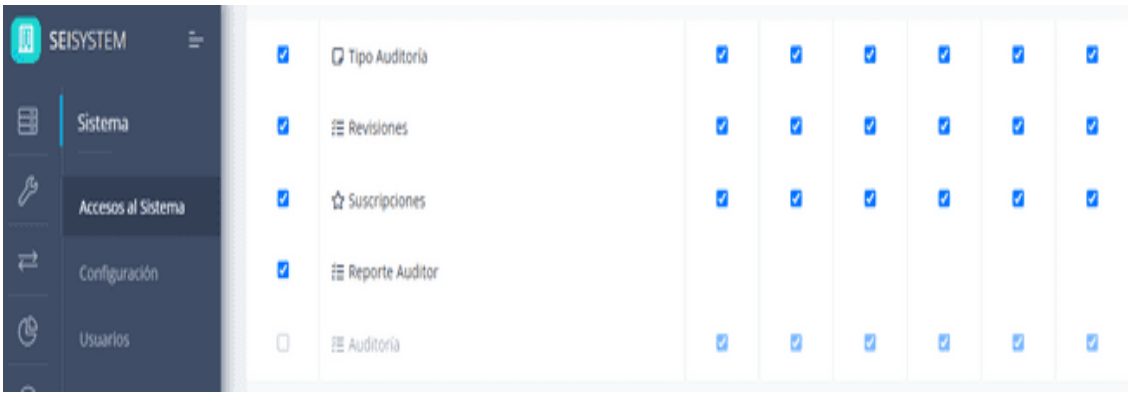
La ejecución de la prueba piloto del modelo de SGSI alienada respecto a la norma ISO/IEC 27001 propuesto. Se implementó un software de tres módulos referente a lo que es el proceso de auditoría la cual se puso en práctica y un módulo aparte solicitado para la administración de clientes de la empresa Seisystem consultores bajo la aprobación del gerente general y el apoyo de los involucrados que son los trabajadores.

**A continuación, se presenta el proceso:**

En primera instancia se tiene el Login, donde él auditor interno tendrá que iniciar con su usuario y contraseña brindado por el gerente general.

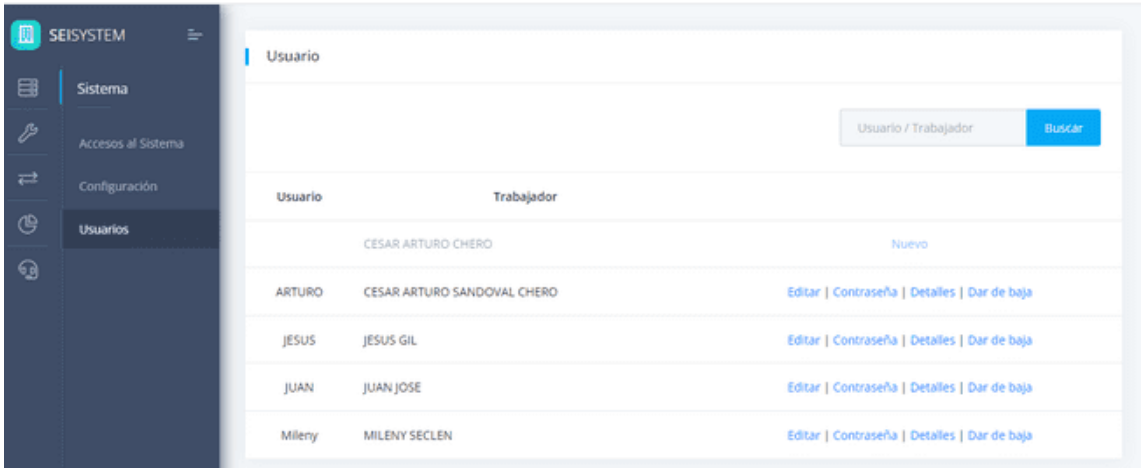



Se tiene la gestión de permios y/o acceso al sistema por usuario (ACCESOS AL SISTEMA) que se le puede habilitar a cada usuario.

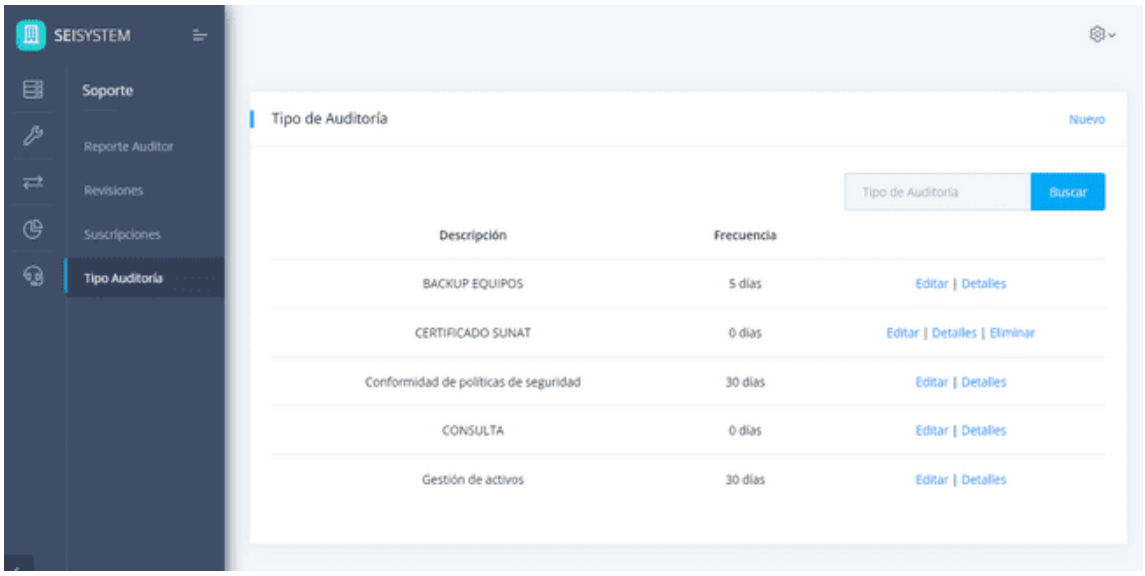


Para la asignación de un usuario, primero se tiene que crear como trabajador.

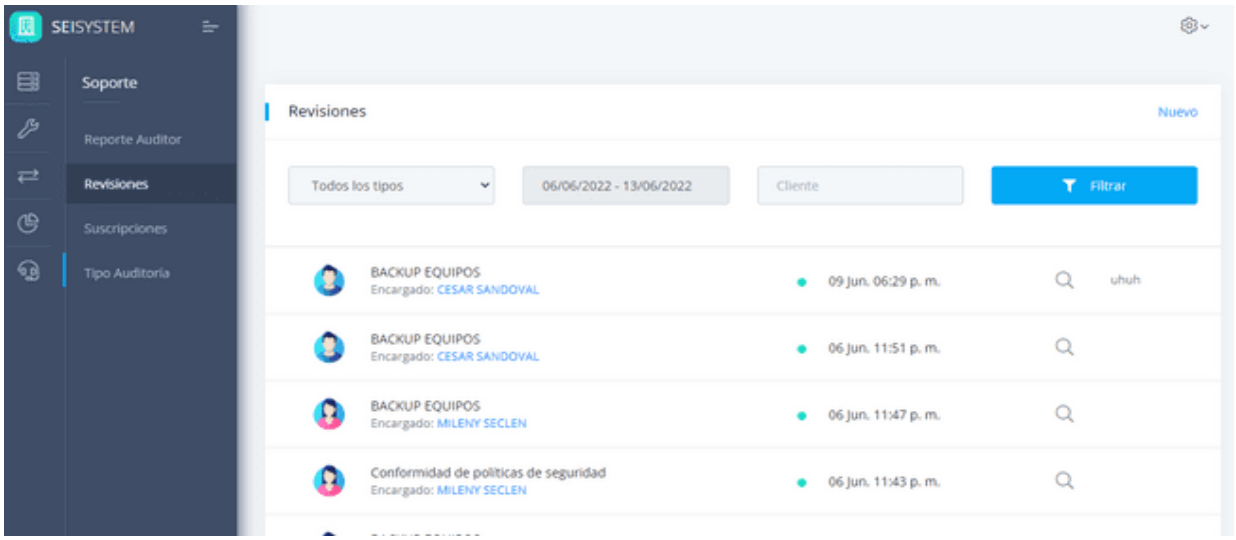

De una vez creado el trabajador, en esta parte se asigna el usuario al trabajador donde podemos asignarle su contraseña, editarlo, ver su detalle, y darle de baja al usuario.



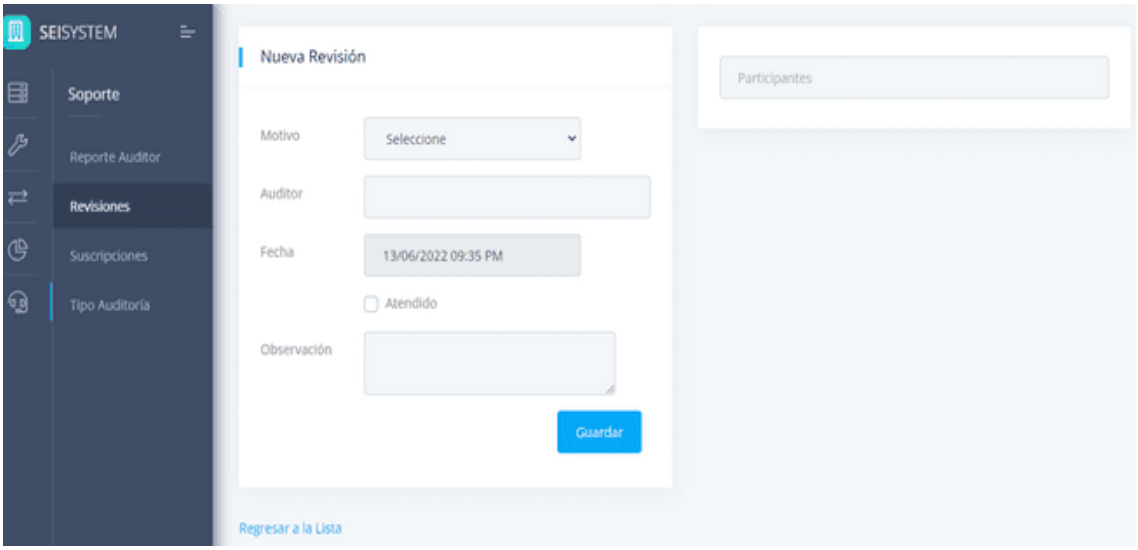
Luego de ingresar con las credenciales, el auditor tiene los diferentes módulos a navegar en el sistema. Como **TIPO AUDITORIA** Se irán registrando los tipos de auditorías y/o temas a tratar con los participantes.



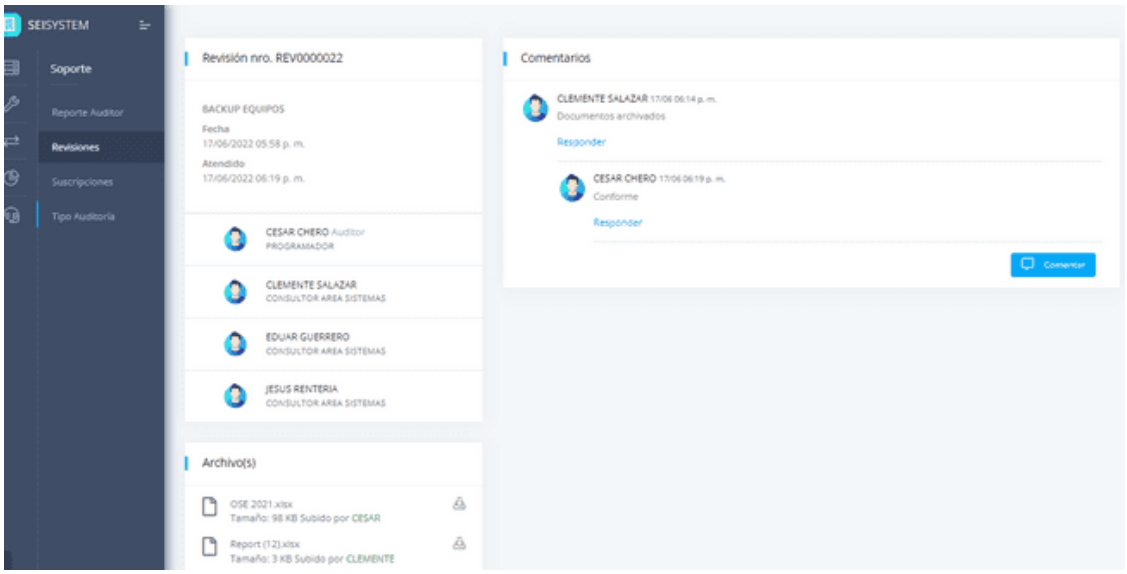

Luego se tiene el módulo de **REVISIONES donde después de seleccionar sus** tipos de auditoría puede crear las revisiones que se darán en la auditoría.



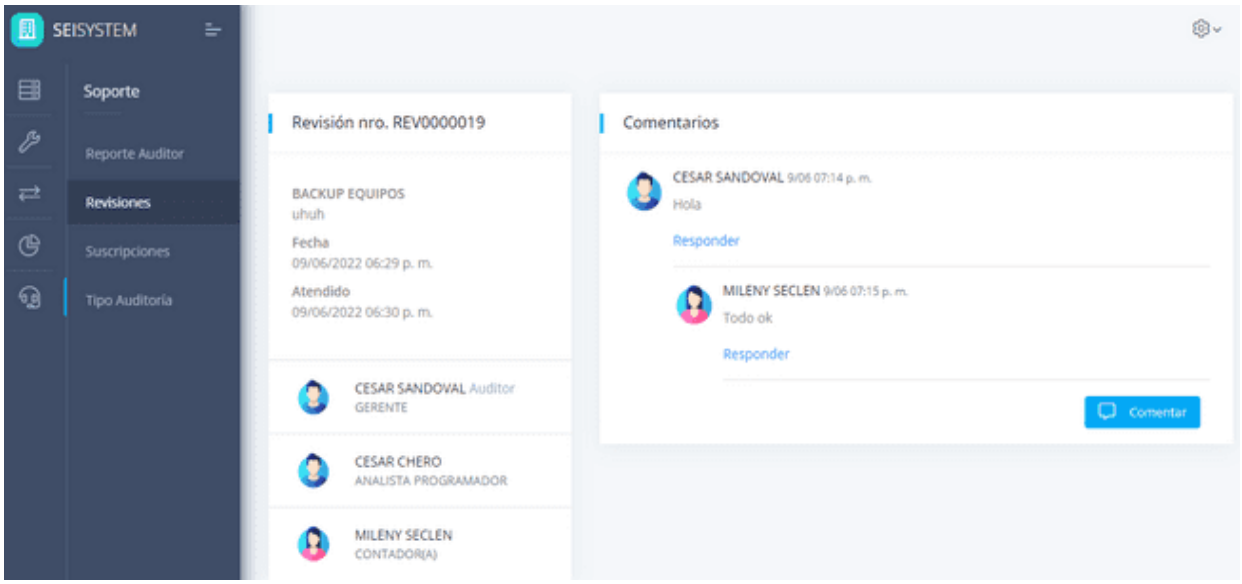
A partir de ello en la pantalla que se muestra seleccionara el motivo, el auditor, la fecha la toma en tiempo real y en la parte izquierda se tiene la asignación de participantes donde se irán agregando con respecto a las áreas de la empresa o donde se llevará acabo la auditoría.



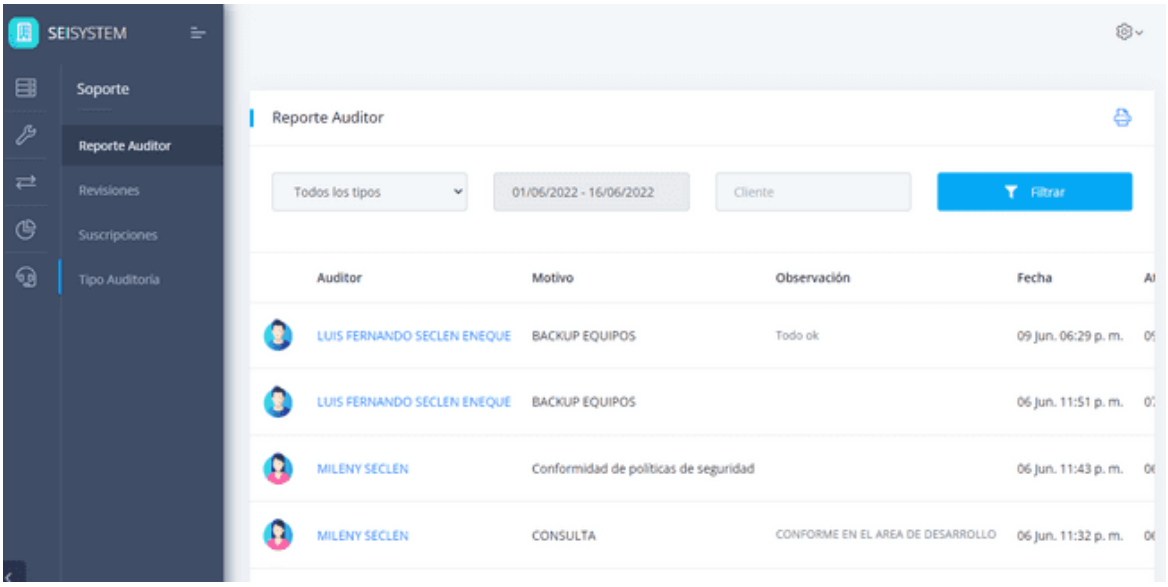

En el proceso de la auditoría con los involucrados de cada área se proceden adjuntar archivos para la muestra al auditor y corroborar con el cumplimiento.



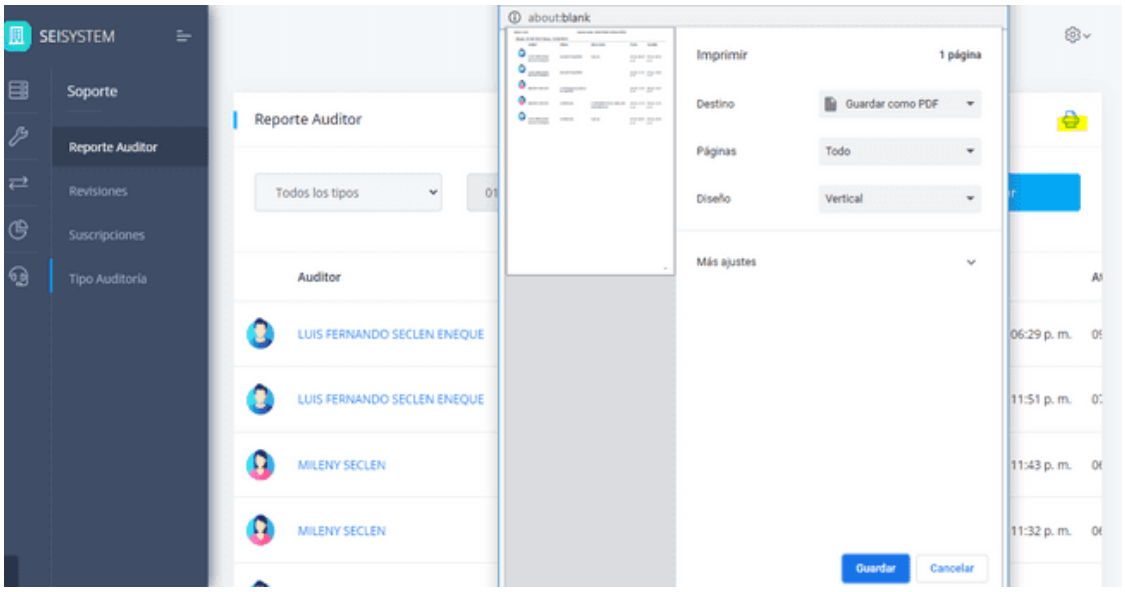
Luego de finalizar la auditoría se tiene un detalle donde se agregarán comentarios por parte del auditor y de los participantes, se puede observar la interacción.




Por último, se tiene un reporte general del auditor, aquí el auditor visualiza de manera rápida las reuniones que se realizó y en las que puede estar involucrado recordando que el auditor puede cambiar de acorde a la asignación del gerente general.



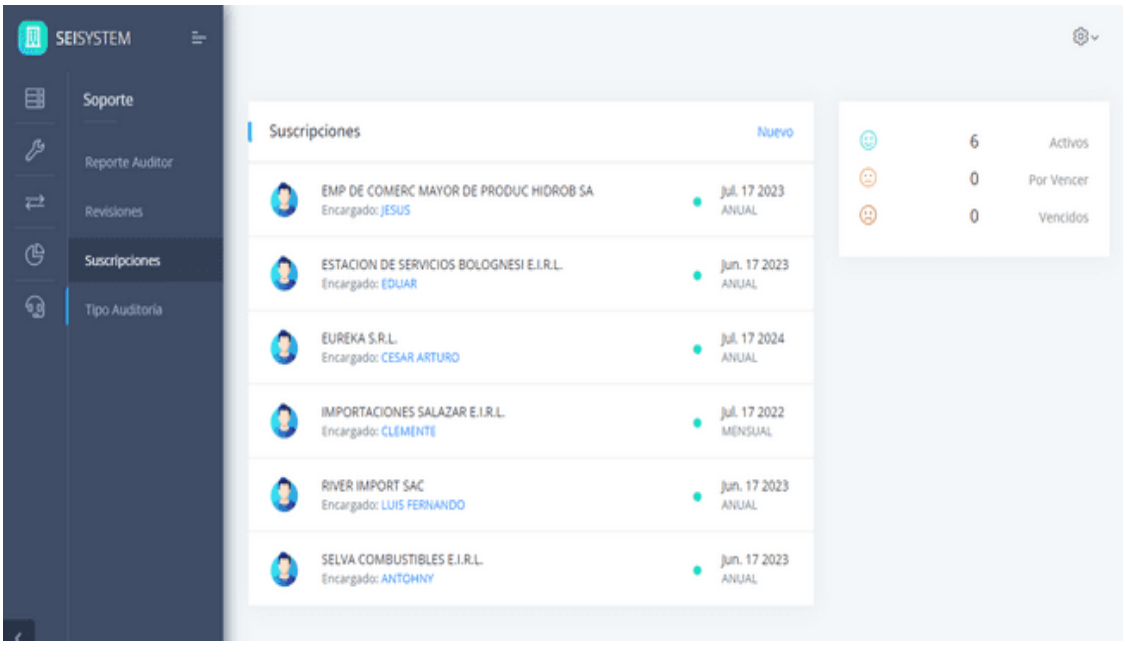
Donde se tiene un botón en la parte superior derecha para poder imprimirlo



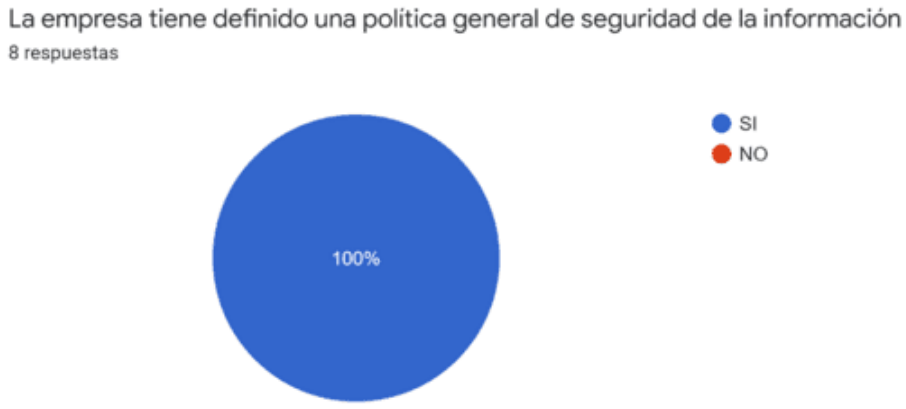

Actualmente los datos de los clientes a los que se les brinda el servicio lo tienen en Excel y genera enormes confusiones con respecto las suscripciones que toman al adquirir el sistema, e incluso se da soportes a empresas que ya vencieron su tiempo de soporte. El módulo de suscripciones va referente en cuando a los clientes a los que se les brinda el servicio, relacionado con los trabajadores de la empresa. La cual sirve para que registren cada uno, las empresas que tienen asignadas y así llevar un control sobre el tipo de suscripciones que se lleva con el cliente. Se muestra el ejemplo de la prueba piloto con empresas reales que se manejan dentro de la empresa seisystem consultores.

Como se puede observar este es el último módulo desarrollado y puesto en práctica en la empresa seisystem consultore mostrando datos reales de los que maneja la empresa, especificando no todos los datos, pero se tomó ciertos clientes como prueba, mejorando el tema de la gestión de los clientes que tiene a cargo la empresa seisystem consultores. Con eso se culminaría el tema del desarrollo del software que se propuso en los objetivos.

A partir de ellos se continuará con las evaluaciones de los indicadores restantes.



Para el indicador estado de cumplimiento de políticas de seguridad de la información en la empresa, con sus variables involucradas se realizó una encuesta a los involucrados donde se muestran los siguientes resultados:





Aplicando la fórmula planteada para el indicador estado de cumplimiento de políticas de seguridad de la información en la empresa: $TRP = \sum Si$ y $TRN = \sum No$

EPGSI = NO = 0 EACPI = NO = 0

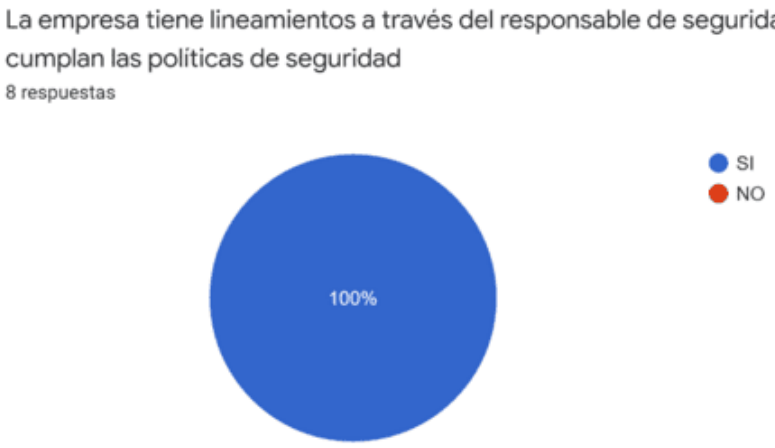
EPGSI = SI = 8 EACPI = SI = 8

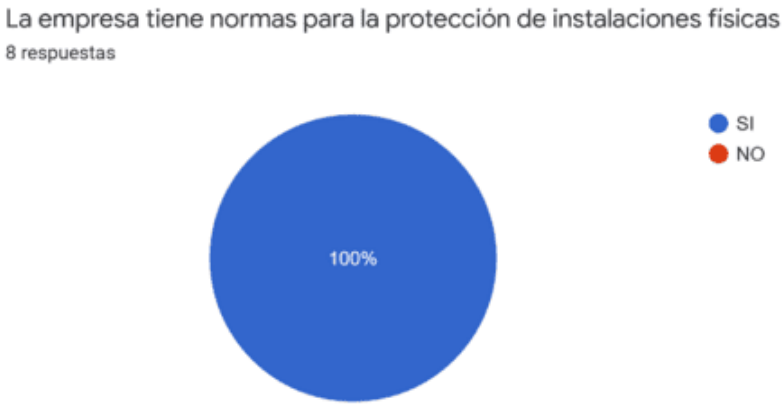
$TRP = 8$ $TRP = 8$

$TRN = 0$ $TRN = 0$

Demostrando el estado de cumplimiento al 100% con respecto a los indicadores y sus variables involucradas. Para tener más información se puede ubicar en el anexo 17.

Para el Indicador grado de la SI y los equipos de cómputo se tienen los siguientes resultados



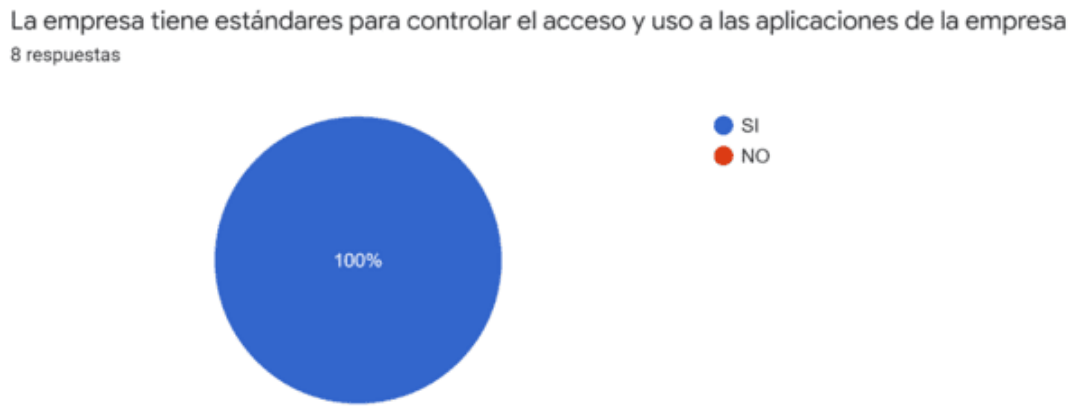




Aplicando la fórmula planteada para el indicador grado de la SI y los equipos de cómputo: $TRP = \sum Si$ y $TRN = \sum No$

| | |
|---|---|
| ELSTPS = NO = 0 | ENPIF = NO = 0 |
| ELSTPS = SI = 8 | ENPIF = SI = 8 |
| $TRP = 8$ | $TRP = 8$ |
| $TRN = 0$ | $TRN = 0$ |

Demostrando el estado de cumplimiento al 100% con respecto a los indicadores y sus variables involucradas. Para tener más información se puede ubicar en el anexo 9.

Para el Indicador grado de verificación de control de acceso se tienen los siguientes resultados.


Aplicando la fórmula planteada para el indicador estado de cumplimiento de políticas de seguridad de la información en la empresa: $TRP = \sum Si$ y $TRN = \sum No$

| | |
|---|---|
| NAUAS = NO = 0 | ECAUA = NO = 0 |
| NAUAS = SI = 8 | ECAUA = SI = 8 |
| $TRP = 8$ | $TRP = 8$ |
| $TRN = 0$ | $TRN = 0$ |

Demostrando el estado de cumplimiento al 100% con respecto a los indicadores y sus variables involucradas. Para tener más información se puede ubicar en el anexo 9.

## 3.2. Discusión de resultados.

Para Tagarev (2012), la implementación del ciclo para una mejora continua es positiva, luego de la creación de un SGSI, útil por el hecho de que las políticas de seguridad deben implementarse de acuerdo con el escenario en el que se ejecutara. En tal medida que la empresa seisystem consultores cumple con identificar las políticas de SI que mejor se adapten a sus necesidades, como lo demuestra el indicador del estado de cumplir las políticas de seguridad dentro de la empresa.

Estos resultados se pueden comparar con el estudio de Ramírez, (2017), gracias a la ejecución del sistema basado en web se logró mejorar los procesos de gestión. De igual forma, existe un estudio de Justino (2015), quien también diseñó un sistema basado en web que permite un mayor control sobre su gestión de seguridad. Y con respecto a los reportes del sistema web se puede comparar con el estudio de (Ríos, 2018) la cual hace referencia a que el sistema web contribuye a centralizar la información, de manera que se tiene reportes confidenciales y partir de ello se puede organizar de forma idónea.

Estos resultados se comparan con un estudio realizado por Benites, (2019) en una su tesis titulada "Implementación de los SGSI -Estándares ISO27001 para las plantas de Radiadores Fortaleza". Su investigación establece que la creación de un plan SGSI beneficiará a su empresa. Esto ayuda a las organizaciones a evitar la mayoría de los posibles problemas relacionados con la SI, ya que ISMS sugiere que el control debe ir acompañado de políticas de seguridad adecuadas.

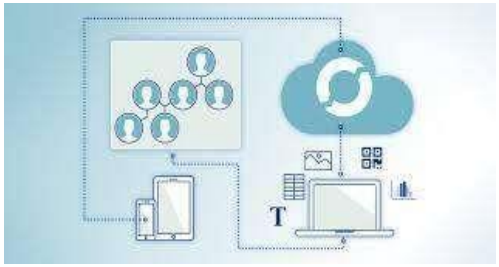
La ejecución del Plan de SI basado en la norma ISO27001:2013 ayuda alcanzar los niveles adecuados en las áreas de SI dentro de la empresa, para consolidar la continuidad efectiva de las operaciones y servicios a través del SGSI.

### 3.3. Aporte práctico.

A. Recopilar información del estado actual de las microempresas


A. Validación del modelo (3 Exp)


A. Revisar artículos científicos.
B. Sistematizar la información.
C. Realizar un cuadro con las mejores propuestas de métodos, metodologías para la seguridad de la información.



A. Seleccionar el entorno de desarrollo
B. Seleccionar lenguaje de programación
C. Seleccionar librerías a utilizar
D. Poner aprueba el sistema con el nuevo modelo.
E. Aplicar prueba piloto.


A. Aplicar ciclo de Sistema de seguridad de la información PDCA
    A. Planificar
    B. Hacer
    C. Verificar
    D. Actuar
A. Aplicar metodología magerit – para análisis de riesgos
    A. Definir alcance
    B. Identificar los activos
    C. Identificar amenazas
    D. Identificar vulnerabilidades
    E. Evaluar riesgos
    F. Tratar el riesgo

**Diagnosticar la situación de las microempresas con respecto a la gestión de seguridad de la información.**

Para aquella elección de la organización se realizó la ejecución de un SGSI. Se tuvo que llevar a cabo un proceso de selección, el cual se describe a continuación. En primer lugar, solicitando información a la CCLAM, se listó a todas las microempresas los cuales esta ubicados en Chiclayo, posteriormente se establecieron tres criterios de evaluación, los cuales son: Procesos, uso de tecnologías y accesibilidad a datos, siendo este último criterio, determinante para de esta manera poder implementar correctamente el SGSI.

*Tabla 10: Relación de microempresas en Chiclayo, caracterizadas por sus procesos, uso de tecnologías y accesibilidad a datos.*

| Empresas de Chiclayo | Procesos | Uso de tecnologías | Accesibilidad a datos |
|---|---|---|---|
| SECLEN ENEQUE LUIS FERNANDO | Desarrollo de sistema | Servicios cloud, Redes sociales | Permitido |
| BURMEO S.A.C. | CONSULTORIA Y DESARROLLO DE SOFTWARES TECNOLÓGICOS PARA EMPRESAS | Redes sociales | Restringido |
| INGENIO Y TALENTO S.A.C. | Desarrollo de soluciones tecnológicas | codificación de bots de software | Restringido |
| SANCHEZ FERNANDEZ MIGUEL ANGEL | Desarrollo de páginas web | Redes sociales | Restringido |

Nota: Elaboración propia

**Realizar una revisión sistemática de modelos sobre gestión de la seguridad de la información**

La metodología de investigación se sostiene en las directrices Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) y un proceso de estudio de mapeo sistemático, en el que se utiliza un protocolo de búsqueda bien diseñado para buscar en cuatro bases de los datos científicas, para identificar, extraer y analizar todas las publicaciones relevantes. La revisión muestra que varios estudios han propuesto diferentes metodologías, técnicas sobre la SI; sin embargo, hay una falta de implementaciones y estudios adecuados para caracterizar la efectividad de estas metodologías, técnicas propuestas.

Al realizar e informar esta revisión, adoptamos las pautas para la verificación sistemática de la literatura y el proceso de estudio cartográfico sistemático, así como las pautas descritas en la declaración PARSIFAL. El objetivo de un análisis de mapeo sistemático es obtener una visión que sea general del área de investigación y complementar investigando el estado de la evidencia en temas específicos. En este caso, los resultados del estudio de mapeo nos ayudarían a identificar y mapear las metodologías para la ejecución del nuevo modelo de SGSI con relación a MYPES. La revisión sistemática nos permitiría nuevamente investigar las tendencias actuales en términos de enfoques técnicos, metodologías y conceptos empleados en el Modelo GSI. En lo que sigue, pasamos por el proceso de mapeo sistemático como se observa en la Figura siguiente.

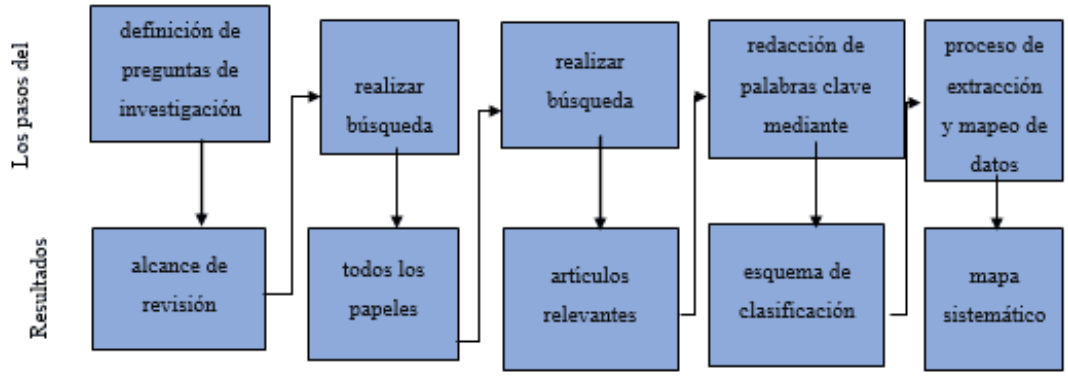



*Ilustración 2: proceso de mapeo sistemático*

Fuente: Elaboración propia

#### 3.3.2.1 definición de preguntas de investigación

Como primer paso del proceso en el estudio de mapeo sistemático, definimos las siguientes tres preguntas de investigación de acuerdo con nuestro objetivo, que es ejecutar una verificación sistemática de la literatura de la ejecución de un nuevo modelo de GSI alineado con la norma ISO / IEC 27001 en microempresas.

#### 3.3.2.2 ¿Cuáles son los modelos de GSI?

La pregunta principal en esta investigación es comprender los diferentes modelos existentes enfocados a la SGSI. Al revisar los artículos relevantes de las bases de datos científicas, podemos identificar qué problemas hay hoy en día con respecto a la SI dada en cada área de la microempresa y, al hacerlo, aislar aquellos problemas que se resuelven mejor con otras técnicas y metodologías.

#### 3.3.2.3 ¿Cuál es el modelo de GSI más reciente?

Esta pregunta busca identificar modelos actuales empleados en microempresas que se enfrentan a los ataques informáticos. Por lo tanto, Esta pregunta de investigación analiza las tendencias actuales en términos de enfoques técnicos y metodologías que se emplean en modelo de GSI para las MYPES, por último, es importante comprender el alcance de los modelos y la eficacia que pueden tener estos modelos recientes aplicados.

#### 3.3.2.4 ¿Cuáles son las etapas de los modelos de GSI?

La última pregunta aborda sobre las etapas de los modelos de GSI. La cual es importante enfocarse en cada una de ellas ya que de ello depende la solución de los problemas con respecto a SI.

## 3.4 Realización de la investigación

En el segundo paso del proceso para el estudio de mapeo sistemático, los artículos principales para el estudio se seleccionan explorando en las bases de datos científicas usando una cadena de búsqueda o palabras clave. Se incluyeron cuatro bases de datos científicas en nuestra búsqueda, a saber; ACM Digital Library, IEEE Digital Library, Science@Direct, Scopus, Al elegir estas bases de datos, nuestra intención era centrarnos únicamente en artículos revisados por pares que se hayan publicado en revistas, conferencias, libros o simposios de renombre. Para buscar en las bases de datos, usamos la siguiente cadena de búsqueda: ("GSI" OR "Estabilidad" OR "investigación" OR "Modelo" OR "Estándar" OR "Guía") AND ("Metodología" OR "Metódica" OR "Norma ISO" OR "ISO 27001" OR "Riesgo" OR "Peligro" OR "Técnica" OR "Procedimiento") AND ("Pequeñas Empresas" OR "MYPE"). Esta selección de cadena de búsqueda se basa en búsquedas piloto en las que probamos algunos términos y acrónimos relacionados con la GSI, así como SGSI (sistema de gestión de la seguridad de la información), MYPE (Micro y pequeña empresa), ISO (Internacional Organization for Standardization). Se observó que todos estos términos relacionados con la SI y sus derivados, como los acrónimos, se capturan en nuestra cadena de búsqueda, ya que ninguno de ellos, cuando se combina con gestión de SI, devuelve ningún efecto nuevo que no se devuelva con nuestra cadena de búsqueda.

## 3.5 Proyección de artículos relevantes

Después de recuperar los artículos de las bases de datos según nuestro protocolo de búsqueda, el siguiente paso fue analizar su relevancia. La primera fase de este paso del proceso fue evaluar la relevancia de los artículos en función de sus títulos. Se descartaron los artículos recuperados cuyos títulos indican claramente que no son relevantes para nuestro estudio. Algunos de los artículos devueltos por nuestro protocolo de búsqueda no estaban relacionados con SGSI y fueron eliminados. En situaciones en las que la relevancia del artículo no podía determinarse fácilmente a partir del título, el artículo pasaba a la siguiente etapa para su posterior selección. La segunda fase de la proyección implicó la lectura de los resúmenes de los trabajos que pasaron por la primera

fase. En algunos casos, nuestros criterios de exclusión nos obligaron a descartar lo siguiente: (1) Artículos cuyo enfoque principal no está relacionado con la SI; (2) Artículos en español; (3) Artículos que no sean de investigación. Los artículos que pasaron estos criterios de exclusión y que se consideró que se centraban en la gestión de la SI se incluyeron en el siguiente paso del proceso de estudio.

### 3.6 Palabras clave sobre la base del resumen

Este paso del proceso tenía como objetivo mapear los artículos de investigación relevantes en la literatura en categorías. Al hacer esto, seguimos el proceso descrito como se muestra en la Figura. Este proceso implica extraer de los resúmenes de los artículos algunas palabras clave y conceptos que reflejan las contribuciones de los artículos. Sobre la base de estas palabras clave, los artículos se agruparon en diferentes categorías. Después de agrupar los artículos en los diferentes rangos, cada artículo se leía en detalle y si el contenido del artículo revelaba que pertenece a una categoría diferente, se actualizaban las categorías. Ocasionalmente, se crea un nuevo rango si se observa que el artículo no encaja en ninguna de las categorías existentes. El resultado final de este proceso es un mapeo de todos los artículos relevantes en varias categorías diferentes.

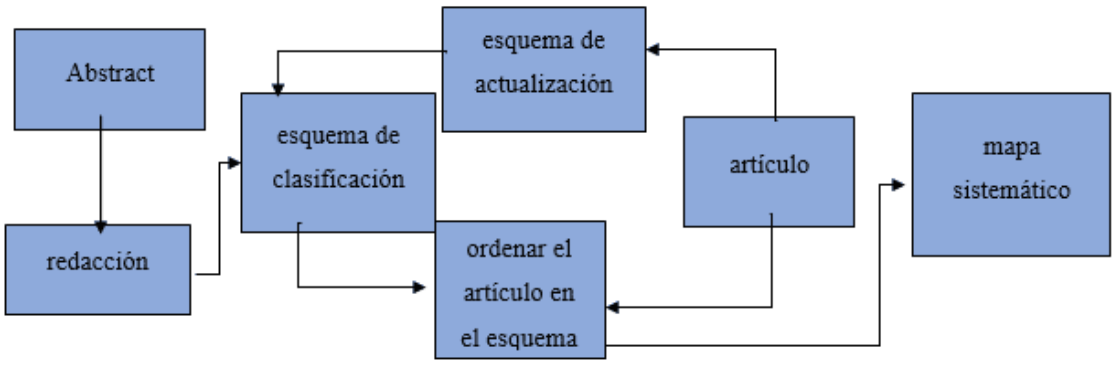



*Ilustración 3: Proceso de clasificación*

Fuente: Elaboración propia

### 3.7 Proceso de extracción y mapeo de datos

En esta última etapa del proceso de mapeo sistemático, se extrajo información de los trabajos de indagación para el meta análisis y para abordar las preguntas de investigación. Se extrajeron un total de 06 elementos de datos de cada artículo, como se muestra en la Tabla. Los elementos se extrajeron del artículo, que incluye el autor (es), título del artículo, año de publicación, la Fuente del articulo (Revista, Conferencia, Simposio) el país donde se escribió el artículo (para autores de varios países, el país del autor correspondiente, o se utiliza el primer autor), y la procedencia del artículo (empresa o academia).

*Tabla 11: Elementos de datos extraídos*

| # | Elemento de datos | Descripción |
|---|---|---|
| 1 | Año | Año de publicación del articulo |
| 2 | Titulo | Título del articulo |
| 3 | Autores | Los autores del articulo |
| 4 | Fuente | Fuente del articulo (Revista, Conferencia, Simposio) |
| 5 | País | País de afiliación de los autores |
| 6 | Procedencia | Procedencia del articulo (empresa o academia) |

Nota: Elaboración propia

En esta sección se muestra los resultados de la revisión sistemática. Usando nuestro protocolo de búsqueda, pudimos recuperar un total de 248 artículos de las bases de datos científicas así se muestra en la Figura. Después de la primera selección, que se basó en los títulos de los artículos, se excluyeron 128 artículos, dejando 120 artículos para una revisión adicional. Los trabajos que fueron excluidos fueron los que no están relacionados con la SI; Yendo más allá, eliminamos los duplicados fusionando los 120 artículos en Mendeley, y esto

redujo los artículos seleccionados 110. En el siguiente paso de selección, leemos los resúmenes de los artículos seleccionados y, en algunos casos, la introducción y la conclusión para examinar más los artículos de acuerdo con los puntos de vista definidos en la Sección 3.3. Esto resulto en la selección de 68 artículos.

Después de leer todos los artículos seleccionados en su totalidad, se excluyeron veintinueve artículos más por no estar enfocados en GSI. Estos documentos solo mencionan acerca de la SI, robo de información, phishing y la importancia de la ejecución de un modelo de GSI en MYPES. Al final del proceso de selección, se seleccionaron 68 artículos para su inclusión en el estudio. La lista completa de artículos seleccionados y algunos de los elementos de datos extraídos se incluyen en la tabla 2.

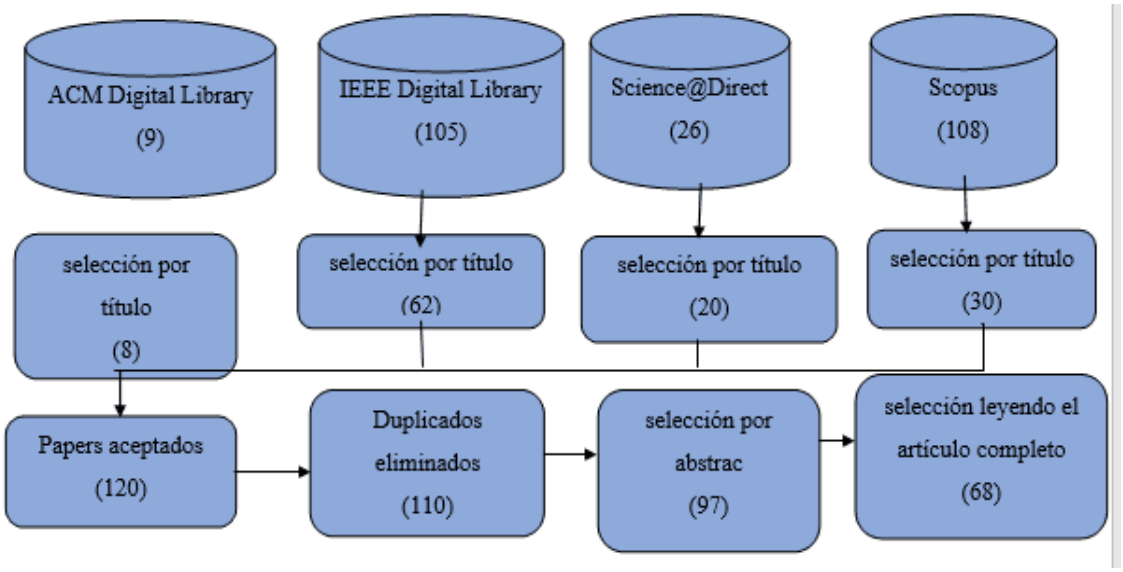



*Ilustración 4: Proceso de selección de los trabajos relevantes*

Fuente: Elaboración propia

*Tabla 12:Lista de trabajos seleccionados sobre la SI*

| # | AUTOR | AÑO | Tipo de publicación | Caso de uso |
|---|---|---|---|---|
| 1 | Kaburuan, E & Lindawati, A | 2019 | Revista | SI de Empresa comercial “Fundación Dompet Dhuafa" |
| 2 | Mena, A | 2018 | Conferencia | Ámbito en seguridad en microempresas |
| 3 | Angraini. et. Al | 2018 | Conferencia | Relacionada con los activos dentro de una aplicación académica en una universidad. |
| 4 | Al-Karaki J et. Al | 2020 | Revista | Seguridad cibernética en organizaciones |
| 5 | Monev, V | 2020 | Conferencia | servicios SKCK en línea basados en la seguridad de la información en Ditintelkam Polda ABC |
| 6 | De Hert, P. et. Al | 2016 | Revista | Seguridad entorno computación en la nube |
| 7 | Schmitz, C. et. Al | 2021 | Revista | SGSI en industrias |
| 8 | Meriah, I. et. Al | 2019 | Revista | Estándares de seguridad basados en ontología |
| 9 | Tanović, A. et. Al | 2019 | Conferencia | SGIS operador de telecomunicaciones en Bosnia y Herzegovina |
| 10 | Velasco, J et. Al | 2018 | Conferencia | SGSI en la industria manufacturera |
| 11 | Jaramillo, H et. Al | 2015 | Conferencia | SI en aplicaciones web para pequeñas empresas |
| 12 | Yun, J et. Al | 2017 | Revista | Rasomware en Sitos web |

| | | | | |
|---|---|---|---|---|
| 13 | Yong, K, Chiew, K. et al | 2019 | Conferencia | Phishing en la web |
| 14 | Yasin, M. et al | 2020 | Conferencia | SGSI en la organización Ditreskrimsus Polda XYZ |
| 15 | Wijayanti, F. et al | 2020 | Conferencia | seguridad y disponibilidad en la República Democrática del Congo del Ministerio XYZ |
| 16 | Wash, R | 2020 | Revista | correos electrónicos fraudulentos de phishing en MYPES |
| 17 | Tjirare, D & Shava, F | 2017 | Conferencia | Caso cualitativo con organizaciones críticas para la seguridad en Namibia |
| 18 | Szczepaniuk, E. et al | 2020 | Revista | GSI en las unidades de la administración pública |
| 19 | Syreyshchikova, N. et al | 2019 | Revista | procesos de información de la organización industrial Enterprise JSC "K" |
| 20 | Sindhu, S | 2021 | Revista | Phishing en los sitios web |
| 21 | Shukla, S & Sharma, P | 2020 | Conferencia | Phishing en URL en organizaciones |
| 22 | Shinde, N & Kulkarni, P | 2021 | Revista | Seguridad en microempresa |
| 23 | Safonova, O. et al | 2020 | Conferencia | SGSI en Proceso comerciales |
| 24 | Rimawati, Y & Sutikno, S | 2017 | Conferencia | GSI en agencia gubernamental |
| 25 | Rienzo, A. et al | 2019 | Conferencia | SGSI en Instituciones sanitarias |
| 26 | Ramalingam, D. et al | 2018 | Revista | Seguridad en procesos de |

| | | | | |
|---|---|---|---|---|
| | | | | gobernanza en organizaciones |
| 27 | Mercaldo, F | 2021 | Revista | SGSI en microempresas |
| 28 | Lyashenko, V et. Al | 2019 | Conferencia | técnicas anti-phishing en redes informáticas |
| 29 | Lopez-L et. Al | 2020 | Conferencia | SGSI para tamaño y línea de negocio de la empresa en particular |
| 30 | Lopes, I et. Al | 2019 | Conferencia | Seguridad en sitios web |
| 31 | Livshitz, I et. Al | 2016 | Conferencia | Seguridad de TI para los servicios electrónicos |
| 32 | Li, J & Wang, S | 2018 | Conferencia | Detección de sitios web de phishing |
| 33 | Kobayashi, N et. Al | 2019 | Conferencia | SGSI en políticas por las empresas |
| 34 | Huang, Y et. Al | 2019 | Conferencia | Phishing en sitios web |
| 35 | Hsu, C et. Al | 2016 | Conferencia | ISO 27001 en Microempresas |
| 36 | Hajdarevic, K et. Al | 2017 | Revista | organizaciones que sufren grandes pérdidas debido a la materialización del riesgo |
| 37 | Garay, D et. Al | 2020 | Conferencia | mitigar el impacto en las PYMEs |
| 38 | Faris, H & Yazid, S | 2021 | Conferencia | Detección de phishing de páginas web |
| 39 | Fadhil, M & Hidayat, F | 2021 | Conferencia | Seguridad de identidad en empresas de transporte |
| 40 | Danielis, P et. Al | 2020 | Conferencia | Riesgos en dispositivos IoT |

| | | | | |
|---|---|---|---|---|
| 41 | Dalgic, F et. Al | 2018 | Conferencia | Phishing en páginas web |
| 42 | Da Silva, M & De Barros, R | 2017 | Revista | Seguridad en el ámbito de desarrollo de software |
| 43 | Churi, T et. Al | 2018 | conferencia | Phishing en transacciones bancarias |
| 44 | Chen, C & Wang, C | 2019 | Conferencia | vulnerabilidades para la computación en la nube |
| 45 | Cascavilla, G et. Al | 2021 | Revista | Phishing en Servicio Nacional de Salud |
| 46 | Carvalho, C et. Al | 2019 | Revista | ISO 27001 en institución publica |
| 47 | Carvalho, C & Marques, E | 2019 | Conferencia | Seguridad en app web |
| 48 | Calder, A & Watkins, S | 2019 | Revista | Seguridad cibernética en organizaciones |
| 49 | Briliyant, O et. Al | 2018 | Conferencia | SGSI organizaciones de Indonesia llamada instituto XYZ |
| 50 | Breda, G & Kiss, M | 2020 | Revista | SI de procesos en empresa industrial |
| 51 | Baykara, M & Gürel, Z | 2018 | Simposio | Phishing en sitios web a través de URL |
| 52 | Barafort, B et. Al | 2018 | Revista | Riesgos integrados para organizaciones de TI |
| 53 | Barafort, B et. Al | 2017 | Revista | Gestión de riesgos de capacidades organizativas en las empresas |
| 54 | Aravindhan, R et. Al | 2016 | Conferencia | Sistemas Avanzados de Computación y Comunicación |
| 55 | Alkilani, H & Qusef, A | 2021 | Conferencia | Serie de actas de conferencias internacionales de ACM |
| 56 | AlFikri, M et. Al | 2019 | Revista | Escenarios de riesgos de una organización |

| | | | | |
|---|---|---|---|---|
| 57 | Aginsa, A et. Al | 2016 | Conferencia | Seguridad de la informacion en Empresas comerciales |
| 58 | Velasco, J et. Al | 2018 | Conferencia | Seguridad en un data center |
| 59 | Muh Sidratul, M et. Al | 2019 | Conferencia | SGSI en el Ministerio de Finanzas |
| 60 | Yasin M; et. Al | 2019 | Conferencia | Estrategias de protección de la información |
| 61 | Velasco, J et. Al | 2018 | Conferencia | Suplantación de identidad en sitios web |
| 62 | Parthiban, R et. Al | 2020 | Conferencia | Phishing en páginas web |
| 63 | Patino, S et. Al | 2018 | Conferencia | La gestión de riesgo de TIC para organizaciones gubernamentales |
| 64 | Nabeel, M. et al | 2020 | Revista | Entorno de sistemas de dominios DNS |
| 65 | Greitzer, F. et al | 2021 | Revista | Entorno web relacionado a correo electrónico |
| 66 | Yazhmozhi, V | 2020 | Conferencia | Entorno web, compras y bancas electrónicas, |
| 67 | Su, Ya | 2020 | Conferencia | Phishing en sitios web |
| 68 | Toapanta, S. et al | 2020 | Revista | ciberseguridad en organismos públicos de la República del Ecuador |

Nota: Elaboración propia

Por otro lado, se realizó un cuadro con los estándares y metodologías más utilizados para la GSI.

*Tabla 13:Estándares para la gestión de SI y metodologías para gestión de riesgo*

| **Estándares para la gestión de SI y metodologías para gestión de riesgo** | | | | |
|---|---|---|---|---|
| **Estándares y metodologías** | **País de origen de la metodología para gestión de riesgo** | **Entorno** | **Finalidad** | **Referencias** |
| Norma ISO/IEC 27001 y metodología Magerit para gestión de riesgo. | Ecuador | Medianas y grandes empresas | Análisis de los riesgos en los SGSI. | Velasco J; Ullauri R; Jácome B ; Pilicita L; Saa P & Moscoso O. (2018) |
| PDCA para ejecutar un SGSI de acuerdo a la norma ISO 27001 | Ecuador | medianas y pequeñas empresas | Permite que las personas se involucren en las estrategias de resguardo de la información. | Velasco J; Ullauri R; Pilicita L; Jácome B; Saa P & Moscoso O. (2018) |
| Norma ISO 27001/2005 para el desarrollo y ejecución de un SGSI y OCTAVE para la gestión de riesgos | Santiago | Grandes y Medianas empresas | Estudio de los riesgos en los SI informática para descubrirlos oportunamente. | Mena A. (2018). |
| Norma ISO 27001: 2013 y el marco de COBIT 2019 para evaluación de la gobernanza de la SI | Indonesia | Pequeñas y medianas empresas | Permite que las personas se involucren en las estrategias de resguardar la información. | Yasin M; Ahmad, A; Edward I; Shalannanda W. (2019). |

Nota: Elaboración propia

**Diseñar el modelo de gestión de la SI alineado a la norma ISO/IEC 27001**

A la hora de desarrollar el modelo GSI se tiene en cuenta la Norma ISO/IEC 27001:2013 junto con el enfoque PDCA y el enfoque Magerit para la gestión de riesgo ya que se considera que tienen fases similares a las necesidades de la empresa. Sin embargo, es necesario personalizar los modelos y obtener de cada modelo el que mejor se acople a la situación actual de la empresa.

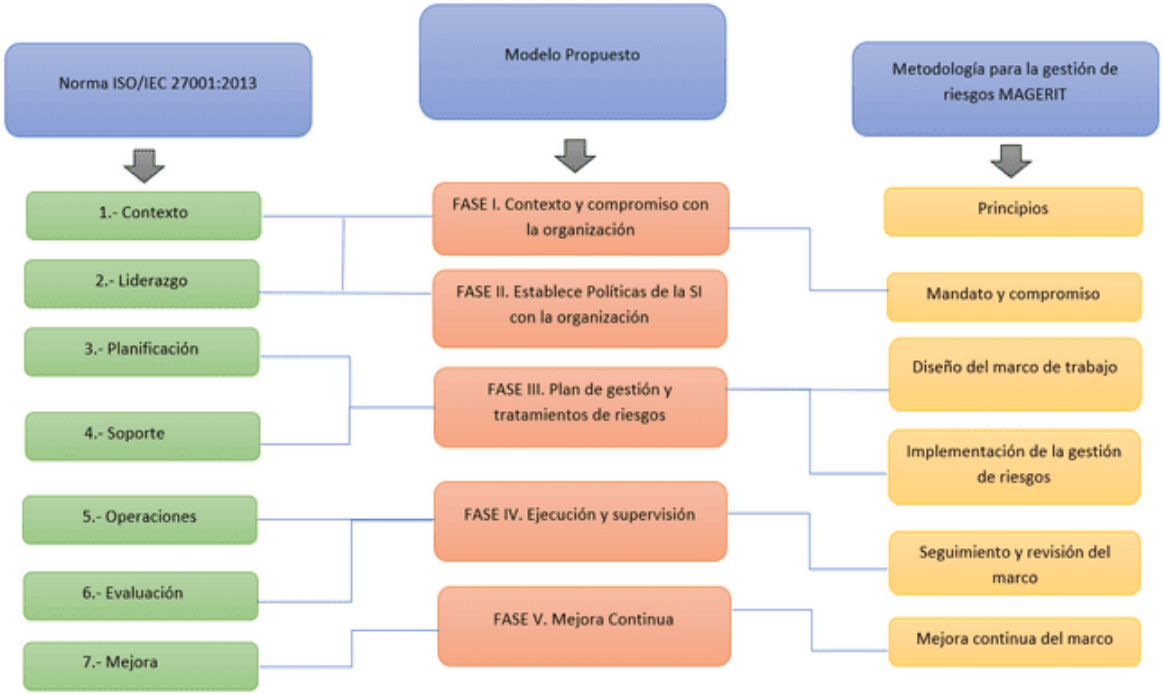



*Ilustración 5: Proceso de elaboración del modelo de GSI*

Fuente: Elaboración propia

Todas sus etapas de la norma ISO/IEC 27001:2013 están tomadas del enfoque PDCA y todas sus etapas están tomadas del enfoque de gestión de riesgos de Magerit, siendo estas fases similares, se optó por unirlas. En esta etapa se tendrá el convenio con la alta dirección de la organización lo cual se especificará aquellos puntos que se comprometen para implantar, realizar, perseverar y mejorar el SGSI.

La tercera fase llamada plan de gestión y tratamiento de riesgos, une la fase de plan de gestión y soporte de la norma ISO/IEC 27001:2013 con la etapa de diseño del marco de trabajo y ejecución de la gestión de riesgos, perteneciente con la segunda fase HACER de la metodología PDCA, Para ello se hará una

selección de activos de la información y valorarlos de acuerdo a como se encuentran en la empresa, para de esta manera enlazar de una mejor forma la parte de planificación con el tratamiento de riesgos y buscar la efectividad al momento de cumplir con lo planificado. Donde obtendremos propuestas con costros aproximados a las soluciones que involucran el desarrollo del software, medidas de seguridad, entre otros con respecto al plan de gestión la cual ayudaran a mitigar los riesgos en los activos de la información.

La ejecución y supervisión continua forma parte de la cuarta etapa del modelo GSI, esta etapa salva la etapa de operaciones y evaluaciones de la norma ISO/IEC 27001:2013, y además utiliza la metodología Magerit, seguimiento y revisión de la estructura, llevándonos a la etapa de revisión de la metodología PDCA. En esta etapa, se prioriza la política de seguridad y, nuevamente, se debe dar retroalimentación a todo el contenido aplicado para mejorar la política y mitigar el riesgo de manera efectiva, se realizan auditorías internas para corroborar lo propuesto y los resultados se revisan con la alta dirección.

La quinta fase del modelo de gestión de SI se denomina mejora continua, donde toma la etapa de mejora de la norma ISO/IEC 27001:2013 como también es perteneciente a la metodología Magerit, estando ya en la fase de ACTUAR de la metodología PDCA. Cabe señalar que ambas etapas son referencias al proceso de recopilación de información y datos para determinar si las salvaguardas se están aplicando correctamente y, obviamente, darán buenos resultados cuando se presenten ciertos riesgos.

En toda organización con activos vulnerables ante cualquier atentado informático, modificación, fraude y hurto, se recomienda implementar un modelo de SI aplicando la norma ISO/IEC 27001 para salvaguardar los activos de información en la organización Seisystem Consultores para asegurar una mejor protección. su organización asegurando su integridad, confidencialidad y disponibilidad.

Con este modelo de gestión de SI conforme a la norma ISO/IEC 27001, el propósito es comprender el estado actual de una organización en términos de seguridad de los activos, identificando las características de los activos, el valor y su impacto en la organización con áreas que describen cada activo.

**Fases de un SGSI**

Después del listado con los Estándares más utilizados para la gestión de SI y metodologías para gestión de riesgo se da la elección de la metodología PDCA O PHVA, para implementar el Modelo de la GSI alineada a la norma ISO/IEC 27001.

**1. PLANIFICAR O PLAN**: Está establecido dichas tareas a realizar para implantar el SGSI. Para eso, debemos hacer las próximas ocupaciones:

- Análisis de los controles de la norma ISO/IEC 27001:2013.
- Compromiso de la Alta Dirección
- Determinar los alcances del SGSI.
- Determinar las Políticas de SI.
- Determinar Metodología de análisis de riesgos.
- Crear procedimiento de auditoría interna.
- Determinar la declaración de aplicabilidad.

**2. HACER O DO**: Se hace lo planificado antes. Luego poner en marcha o estar ejecutado, se consigue visitar la siguiente etapa. Las ocupaciones por hacer en esta etapa las siguientes:

- Ejecutar plan de tratamientos de riesgos.

**3. VERIFICAR O CHECK**: se evalúan los resultados obtenidos. Las ocupaciones por hacer en esta etapa son:

- Preparar la auditoría interna.
- Efectuar la auditoría.
- Verificar efectos obtenidos con la alta dirección.

**4. ACTUAR O ACT:** Conservar y mejorar el SGSI. Las actividades que se realizaran en la fase son las siguientes:

- Crear plan de acciones correctivas y mejoras

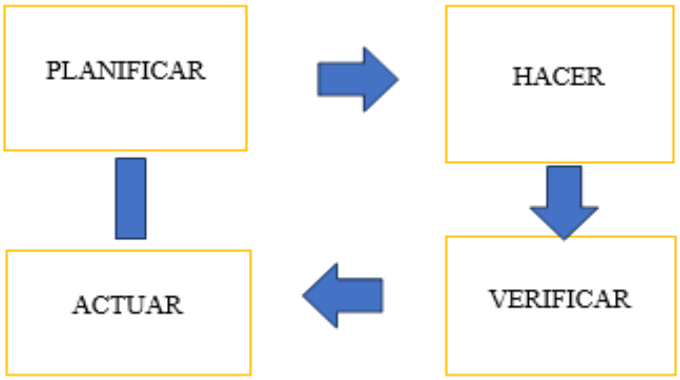



*Ilustración 6: Ciclo de Deming*

Fuente: Elaboración propia

**Situación Actual**

**Datos de la Empresa:**

- Razón Social: SEISYSTEM CONSULTORES
- Localización: (dirección y mapa):

Está ubicada en Alfonso Ugarte 633 int (205).

- **Visión:**

Nos vemos como una empresa consolidada en la Región Norte del Perú en el ámbito de consultoría, desarrollo de SI y soluciones empresariales integrales, brindando servicios de buena calidad, que nos permita lograr un elevado grado de conocimiento y especialización avalado por una cartera de clientes, los cuales muestren mejoras importantes a nivel organizacional, de imagen e incrementar de rentabilidad. Durante los próximos años, SEI SYSTEM estará enfocado en la búsqueda de alianzas estratégicas (partners), que nos permitan diversificar nuestra cartera con productos y/o servicios rentables, así como expandir nuestra participación en el mercado de TI.

- **Misión:**

Somos una organización formada por un grupo de profesionales, dedicada a ofrecer servicios especializados a empresas, brindando soluciones integrales de alto nivel en TI en el ámbito Empresarial. Nuestra orientación al Cliente nos permite ofrecer a nuestros aliados de negocios resultados confiables que representan ventajas competitivas estratégicas diferenciadas en este entorno empresarial competitivo.

- Organigrama General de la empresa/organización:

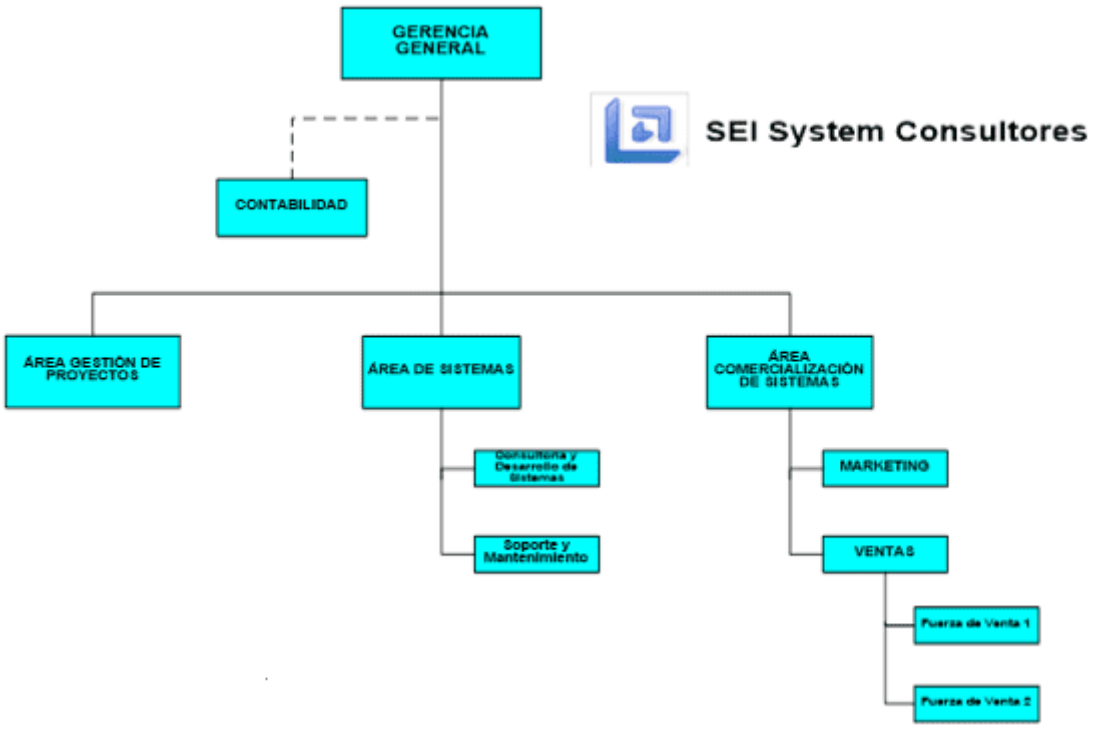



*Ilustración 7: Organigrama de SEISystem Consultores*

Fuente: SEISystem Consultores

## 3.8 Fases

### 3.8.1 Fase I: Contexto y compromiso con la organización

**a) Planificar**

Esta fue la primera fase de la búsqueda de un SGSI, para lo cual se exploró entender el caso inicial de las condiciones y controles de Seisystem para la norma

ISO/IEC 27001:2013, además de los documentos ocupacionales y que son precisos, estos son los siguientes:

a. Análisis inicial de controles

Se hizo la exploración de controles, ya que era de gran importancia contar con una idea precisa y clara de que los controles no se hallaban ejecutadas y cuales, si lo estaban, así mismo conoces cuales son o no necesarias, por lo cual se evaluó para aplicar los controles los detalles se observan en el Anexo 11

b. Compromiso de la Alta Dirección

Se debería considerar que este es un paso elemental para el SGSI, como ya se ha indicado previamente. Se hizo el “Acta de Compromiso” (Anexo 3), sugiere los puntos de vista propio a los que se comprometen para ejecutar, llevar a cabo, mejorar y conservar el SGSI. Después se procedió a ser firmada por el Gerente General.

c. Alcance sistema de gestión de la SI

La empresa SEISYSTEM CONSULTORES el alcance de un SGSI pertenece a los puntos de vista más relevantes debido a que tienen que ser los más exactos y que englobe a toda la empresa. Se procedió a decidir los parámetros del alcance del SGSI, diciendo los desarrollos que serían integrados y los que no. Además, se le comunicó al Ger. Gral. para su correspondiente aceptación.

Procesos involucrados son los siguientes:

- Gerencia General
- Contabilidad
- Área de sistemas
- Consultoría y desarrollo de sistemas
- Soporte y mantenimiento.

Procesos que NO están incluidos en el alcance son:

- Área de gestión de proyectos
- Área comercialización de sistemas
- Marketing
- Ventas

### 3.8.2 Fase II Establecer Políticas de la SI con la organización

**a) Políticas de SI**

Para decretar la política de SI se tuvo en cuenta todo lo antedicho. Este archivo "Política de SI" (Anexo 17), incluye dicho objetivos y compromisos de SI, acorde con el sector de la empresa. Además, fue aprobada por el Ger. Gral.

### 3.8.3 Fase III Plan de gestión y tratamientos de riesgos

**B) Hacer**

**Metodología de análisis de riesgos**

El objetivo de gestión de SI alineada a la norma ISO/IEC 27001 es alcanzar un proyecto de método para los peligros de los activos de la organización Seisystem Consultores, para poder realizar este proyecto se requiere de la metodología Magerit ya que cuenta con varias fases las cuales son:

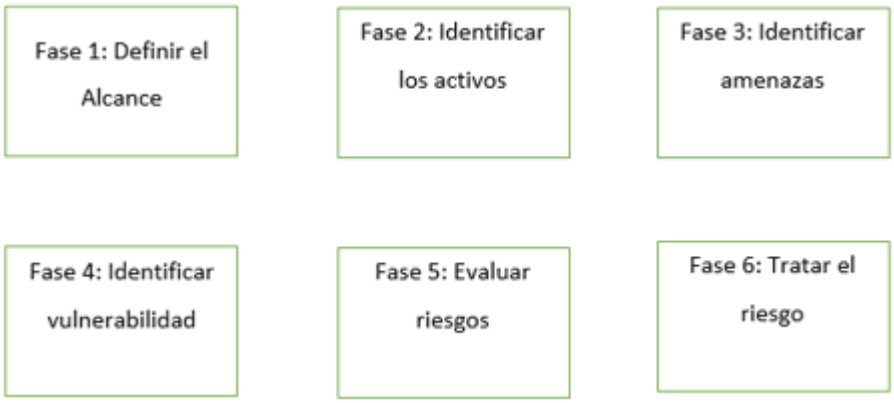



*Ilustración 8: Fases de la metodología de Magerit*

Fuente: Elaboración propia

**Identificar los activos**

Es imprescindible hacer un inventario de aquellos activos contenidos de la empresa. Los activos son todos los elementos que forman parte de un SI, los cuales son (software, recursos administrativos hardware, datos, servicios, comunicaciones, etc.).

Los activos se determinan según el método Magerit**.**

*Tabla 14: Descripción de activos de la información*

| **Activos** | **Descripción** |
|---|---|
| Datos | Concretar la información. |
| Software | Las aplicaciones informáticas ya que permitirá el manejo de los datos. |
| Hardware | Los equipos informáticos que autorizan aplicaciones, hospedar datos y servicios |
| Instalaciones | Acogen equipos de comunicaciones y informáticos. |
| Soportes de Información | Los dispositivos de almacenamiento de datos. |
| Personas | Estas son las personas que dirigen o gestionan todo lo anterior. |
| Servicios | Servicios auxiliares que se necesiten para desarrollo de procesos y/o servicios |

***Fuente**: De la sota C & Mechan J. (2018).*

Para estimar el costo del efecto de la pérdida de todas las 3 aristas de valoración del activo, se emplea la siguiente escala. **(Ver Tabla 15)**

*Tabla 15: Valoración de los activos*

| **Rango** | **Valor** | **Confidencialidad** | **Integridad** | **Disponibilidad** |
|---|---|---|---|---|
| 7-10 | ALTO | Las investigaciones relacionadas con los activos solo deben ser accedidas por el | El activo no puede tolerar la pérdida o cambio de su | Se requiere que el activo no esté disponible al menos |

| | | | | |
|---|---|---|---|---|
| | | jefe o gerente del área responsable, ya que su divulgación puede impactar **significativamente** a la organización. | componente del 5% porque al cambiar La integridad puede afectar **significativamente** a la organización. | una hora, pues su carencia afectaría **significativamente** a la organización. |
| 4-6 | MEDIO | La averiguación asociada al activo es **confidencial** y solo a los trabajadores de algunas áreas del interior pueden ceder a ella, pues su divulgación afectaría **considerablemente** a la organización. | El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 50%, pues la alteración de su integridad afectaría **considerablemente** a la empresa. | Se considera que como máximo el activo puede estar no disponible por un día, pues su carencia afectaría **considerablemente** a la empresa. |
| 1-3 | BAJO | La averiguación asociada al activo es de uso interno y solo el trabajador de la organización puede acceder a ella o pública, esto quiere decir que puede acceder cualquiera, pues su divulgación afectaría de manera **baja** a la organización | El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 95%, pues la alteración de su integridad afectaría de manera **baja** a la organización. | Se considera que Como un límite el activo puede estar no disponible por un tiempo indefinido, pues su escasez afectaría de manera **baja** a la organización. |

*Fuente:* (De La Sota & Mechan, 2018)

Luego de realizar un inventario de activos, debemos tener conocimiento que el valor de un activo se estima promediando los efectos de disminución de integridad, disponibilidad y confidencialidad, de la siguiente manera:

$$V.A = \frac{C + I + D}{3}$$

**Análisis de riesgos o amenazas**

El objetivo es entender la exposición de los activos de indagación que tiene las conminaciones, en otras palabras, entender los peligros que enfrenta la organización Seisystem Consultores.

Un riesgo se puede identificar de diferentes maneras:

*Tabla 16: Análisis de riesgos o amenazas*

| Tipo de Amenaza | Descripción |
|---|---|
| Defectos de las aplicaciones y los equipos | La presencia de defectos técnicos o de fabricación en los equipos, defectos en su diseño o en alguna parte en particular puede tener consecuencias desfavorables para el crecimiento de la organización. |
| Origen Natural e Industrial | Hay percances naturales tal como inundaciones y terremotos y percances industriales como los cortes de energía y la contaminación. |
| Causadas de formas deliberadas | Personal con entrada a los SI pueden causar dificultades intencionales como ataques informáticos; Obteniendo así una ventaja desleal o con el fin de perjudicar al titular |
| Causadas de formas accidentales | Las personas que tienen entrada al SI pueden cometer causar problemas inesperados |

Nota: Elaboración propia

El grado de influencia de un activo se logra un determinando el "valor del activo" dentro de un rango de valores en la tabla 16.

*Tabla 17: Matriz de Impacto*

| ID | RANGO | VALOR | | CRITERO |
|---|---|---|---|---|
| 3 | 7-10 | ALTO | A | Valor alto |
| 2 | 4-6 | MEDIO | M | Valor medio |
| 1 | 1-3 | BAJO | B | Valor bajo |

Nota: (ORJUELA & CÁRDENAS, 2017)

De acuerdo con la definición del estándar de impacto de activos, los que ingresan a la etapa de valoración de riesgo son solo aquellos de indagación con un grado de impacto de "ALTO" (valoración de activos).

**Evaluación de Riesgos**

**PROBABILIDAD.** - Para calcular la probabilidad se debe determinar un número entre 1a 4.

*Tabla 18:Criterios de probabilidad*

| ID | VALOR | CRITERO | FRECUNCIA |
|---|---|---|---|
| 4 | **CASI SEGURO** | El evento probablemente ocurre en la mayoría de las circunstancias | Más de una vez al año |
| 3 | **PROBABLE** | El evento probablemente ocurrirá en todas las circunstancias | Al menos una vez en los últimos 3 años |
| 2 | **IMPROBABLE** | El evento probablemente puede ocurrir en algún momento | Al menos una vez en los últimos 5 años |
| 1 | **RARO** | El evento probablemente ocurre solo en circunstancias excepcionales | No se ha presentado en los últimos 5 años |

Nota: (De La Sota & Mechan, 2018)

**IMPACTO**. - Para el cálculo del impacto se debe elegir un número entre 1 a 3.

*Tabla 19: Criterios de impacto*

| ID | RANGO | DESCRIPCION |
|---|---|---|
| 3 | ALTO | 1.- Esto es perjudicial por medio de una alta continuidad desde el inicio de los servicios prestados por la organización.<br>2.- Las pérdidas financieras resultan del alto costo y gasto de los activos o recursos de la organización.<br>3.- Esto es perjudicial y daña significativamente la reputación, la imagen, los deberes y los intereses de la organización. |
| 2 | MEDIO | 1.- Perjuicio medio para la continuidad del inicio de los servicios prestados por la organización.<br>2.- Esto da como resultado una pérdida financiera moderadamente recuperable de los activos o recursos de la organización.<br>3.- Perjudica y daña la reputación de la imagen, objetivos e intereses de la organización. |
| 1 | BAJO | 1.- Todo ello sin perjuicio de la continuidad del lanzamiento de los servicios prestados por la organización.<br>2.- Esto da como resultado una pérdida financiera mínima de activos o recursos en la organización.<br>3.- Mal insignificante para la gloria de la imagen, la misión y los intereses de la organización. |

Nota: (De La Sota & Mechan, 2018)

El costo del peligro se cuenta conforme a la siguiente fórmula matemática:

$$Nivel\ de\ riesgo = NI * POR$$

Por la probabilidad – impacto se delimita el mapa de peligro que se muestra posteriormente, los números en el centro de las celdas son calculados al multiplicar la posibilidad por el efecto.

*Tabla 20: Valoración de activos probabilidad – impacto*

| Mapa de Riesgo | | | | |
|---|---|---|---|---|
| PROBABILIDAD | 4 Casi seguro | 4 | 8 | 12 |
| | 3 Probable | 3 | 6 | 9 |
| | 2 Improbable | 2 | 4 | 6 |
| | 1. Raro | 1 | 2 | 3 |
| | | 1. bajo | 2. Media | 3. Alta |

Nota: (De La Sota & Mechan, 2018)

Para visualizar la apreciación de Riesgos **(Anexo 7).** Una vez analizadas las vulnerabilidades se establece la valoración del riesgo, esto permitirá definirla aplicación de controles ISO 27001:2013.

**Criterios de aceptación de riesgos**

Una vez realizado la exploración la apreciación del peligro, se debería dictaminar qué ocupaciones se han de tomar con los activos que permanecen sujetos a peligros reales y significativos para la organización. Por lo cual se utiliza lo siguiente:

*Tabla 21:Criterios de aceptación de riesgos*

| **Medida frente al riesgo** | |
|---|---|
| **ASUMIR** | Admitir la probabilidad de que logre suceder el peligro si no se toma medidas de acción específicas. |
| **REDUCIR** | Minimizar la posibilidad o la impresión del suceso mediante la ejecución de controles de SI. Se usa al realizar el control trae muchas cosas satisfactorias que superan a la inversión ejecutada. |
| **EVITAR** | Eliminar la fuente de desarrollo que representa una amenaza. Se utiliza porque el nivel de peligro es alto y el SI o la actividad de desarrollo que crea el peligro no tiene un impacto significativo en el negocio de la organización y, por lo tanto, puede retirarse operativamente. |
| **TRANSFERIR** | Transferir los efectos de los peligros a terceros (organizaciones de seguros o proveedores de servicios). Hágalo cuando la probabilidad de un peligro no se reduzca, pero el impacto sea inminente. |

***Fuente:*** (De La Sota & Mechan, 2018)

El criterio de peligros se hace con base al grado de peligro evaluado según se describe en la siguiente Tabla 22:

*Tabla 22: Zona de riesgos*

| ID | RANGO | ZONA | CRITERIOS DE ACEPTACION |
|---|---|---|---|
| B | 1-2 | Zona de riesgo baja | Asumir el riesgo |
| M | 3-5 | Zona de riesgo moderada | Asumir el riesgo, evaluar reducir el riego |
| A | 6-8 | Zona de riesgo alta | Reducir el riesgo, evitar, compartir el riesgo |
| E | 9-12 | Zona de riesgo extrema | Reducir el riesgo, evitar, compartir el riesgo |

Nota: (De La Sota & Mechan, 2018).

**Procedimiento de Auditoría Interna**

Se ha implantado un “Procedimiento de Auditoría Interna” (Anexo 12), que establece que pasos para comprobar el cumplimiento del SGSI por adelantado Norma ISO/IEC 27001:2013

**Plan de tratamiento de riesgos**

Para ello, se define quién es el responsable de ejecutar cada control, cuándo y qué. Se desarrollará un plan de acción de cumplimiento (Anexo 9). Además, este documento debe ser aprobado por la alta dirección, lo que lleva mucho tiempo. y el esfuerzo depende de la dificultad de ejercer este control, sin su compromiso se obtendrán los recursos necesarios.

**Inventario de Activos de Información**

Inicialmente, la organización no tenía ningún inventario, por lo que se realizan cuestionarios para identificar todas las áreas del activo para su uso posterior. Registrarlo en la "Lista de Activos de Información" (Anexo 5). entonces valoran todos los activos (Anexo 6) de estos se quedan con todos los de impacto alto y 3 de impacto MEDIO que son muy influyentes en la organización (Tabla 23).

*Tabla 23:Activos de la información*

| Categoría | ID de Riesgo | Activo | Criterios | | | Total | Impacto |
|---|---|---|---|---|---|---|---|
| | | | C | I | D | | |
| DATOS | D-001 | **Datos del personal** | 7 | 7 | 8 | 7 | A |
| | D-002 | **Control de salarios** | 10 | 9 | 9 | 9 | A |
| | D-003 | **Datos de los clientes** | 10 | 7 | 7 | 9 | A |
| | D-004 | Datos de inventario de equipos | 4 | 4 | 4 | 4 | M |
| | D-007 | **Registros de órdenes de compras** | 7 | 10 | 8 | 8 | A |
| | D-010 | **Reporte de acceso de usuarios Radmin VPN Y ANYDESK** | 8 | 9 | 9 | 9 | A |
| | D-011 | **Registros de órdenes de ventas** | 7 | 10 | 8 | 8 | A |
| | D-012 | **BD Empresa/ BD Clientes** | 7 | 10 | 9 | 9 | A |
| | S-002 | Internet | 4 | 7 | 9 | 7 | M |
| | S-003 | Correo electrónico | 7 | 6 | 7 | 7 | M |
| SOFTWARE | SW-001 | **Lista de instaladores de Software** | 7 | 9 | 10 | 9 | A |
| | SW-003 | **Software “Scan web”** | 9 | 9 | 9 | 9 | A |
| HARDWARE | HW-003 | **Laptop de desarrollo** | 9 | 9 | 10 | 9 | A |
| MEDIA | MED-001 | **Documentación administrativa** | 8 | 9 | 9 | 9 | A |
| INSTALACIÓN | INS-001 | **Oficina Alfonso Ugarte** | 8 | 6 | 9 | 8 | A |

Nota: Elaboración propia

**Evaluación de Riesgos**

Después de completar la lista de activos de información, "Evaluar riesgo" (Anexo 7), que evalúa el impacto de las probabilidades y de las amenazas que están ocurriendo, para que obtenga el peligro multiplicando los dos, excepto el área de riesgo Indique qué activos tienen un riesgo muy bajo. Esto ayuda a usar y considerar, aceptar, evitar, minimizar o desviar este peligro.

**Declaración de Aplicabilidad**

En esta actividad de la "Declaración de Aplicabilidad" (Anexo 8), Controles y controles enumerados en el Anexo 16, de conformidad con las normas de ISO/IEC 27001, Comprender qué controles se aplican o no a la empresa y, lo más importante, evaluar sus razones de elección

Matriz de Comunicación Interna

Se detalla en la Tabla 24, que explica qué, cuándo, con quién, con quién y cómo se debe comunicar en términos del SGSI.

*tabla 24: matriz de comunicación interna*

| N° | ¿Qué se debe comunicar? | ¿Cuándo Comunicar? | ¿Quién debe comunicar? | ¿A quién comunicar? | Tipo | Registro | Proceso de Comunicación |
|---|---|---|---|---|---|---|---|
| 1 | Organización de la SI (Roles y Responsabilidades) | Cuando se renueva y aprueba los Roles y Responsabilidad de SGSI | Responsable de área | Jefe inmediato / Gerente | Interna | Correo electrónico institucional | Comunicación de la empresa de SI, por medio del correo institucional (C.I) |
| 2 | Manual del SGSI | Cuando se actualiza y aprueba el Manual del SGSI | Responsable de área | Jefe inmediato / Gerente | Interna | Correo electrónico institucional | Información del Manual de SGSI, a través del C.I |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3 | Plan de capacitación y concientización en SI | Semestral | Responsable de área | Todos los colaboradores. | Interna | Correo electrónico institucional | Información del plan de capacitación y concientización a través del C.I |
| 4 | Informe del estado de la Implementación de los controles de SI. | Mensual | Responsable de área | Jefe inmediato / Gerente | Interna | Acta de reunión | Informe del estado de ejecución de controles, por medio de correo o reunión. |
| 5 | Informe de la revisión del SGSI por la dirección | Bimestral | Responsable de área | Alta dirección | Interna | Acta de reunión | Reporte del informe del SGSI con la alta dirección. |
| 6 | Informe de la gestión de incidentes de SI | Bimestral | Responsable de área | Alta dirección Todos los colaboradores | Interna | Correo electrónico institucional | Comunicación del estado de incidentes de SI, en las reuniones. Información del reporte del estado de incidentes de SI a través del C.I |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | Informe de resultados de las auditorías Internas del SGSI | De acuerdo al proceso de Auditorías Internas | Oficial de SI | Alta Dirección | Interna | Acta de reunión Correo electrónico | Comunicación de la consecuencia de las auditorías internas del SGSI, en una junta. Por medio del C.I Comunicar el reporte de actividades correctivas y de a través del C.I |
| 8 | Informe de los resultados de procesos de corrección y de mejora | Después de las auditorias | Oficial de SI | Alta Dirección Responsablecada área | Interna | Acta de reunión | |
| 9 | Resultados de la auditoría del SGSI | De acuerdocon lo programado | Oficial de SI | Alta Dirección | Interna | Acta de reunión | Informar los resultados a través del C.I |

Nota: Elaboración propia

Implementación del Plan de Tratamiento de Riesgo

Para el uso de elementos del programa peligrosos, se aplican las siguientes medidas de estabilización. Solo se realizaron controles pertenecientes al “Grupo 1”, no al “Grupo 2” ya que requería una estimación mayor, en su lugar se realizó un “Plan de Utilización de Seguridad” (Anexo 10) Grupo 2” Lineamientos para desarrollo futuro. La Tabla 25 muestra los elementos de acción tomados para cada control de estabilidad considerado necesario para investigar:

*Tabla 25: Plan de acción*

| MÉDIDAS DE SEGURIDAD | DESCRIPCIÓN | CONTROL | ACTIVOS | GRUPO |
|---|---|---|---|---|
| **Memorándum (llamadade atención)** | Llamada de atención a ese personal que infringe este control. | 6.1.1<br>7.2.3<br>9.1.2 | - Control de salarios<br>- Reporte de acceso de usuarios Radmin VPN Y ANYDESK<br>- Lista de instaladores de software<br>- Persona | 1 |
| **Organigrama de puestos** | Detectar cuáles son los causantes de cada área para secretar labores para evadir la utilización errónea de los activos. | 6.1.2 | - Persona | 1 |
| **Ficha de puestos** | Buscar a personas con entendimiento en estabilidad de la información en caso de que no secretar la labor de registrar, actualizar y eludir el mal uso de activos. | 6.1.2 | - Persona | 1 |
| **Proveedores de instalación de medidas de seguridadpara oficinas.** | Disponer de un listado externo que se encargue en la custodia de incendios y además de orientación al personal para que logre desempeñarse adecuadamente frente a un aviso de incendio. | 6.1.3 | - Oficina de Alfonso Ugarte | 2 |

| MÉDIDAS DE SEGURIDAD | DESCRIPCIÓN | CONTROL | ACTIVOS | GRUPO |
|---|---|---|---|---|
| **Empresas aseguradoras contra desastres naturales y no naturales (incendios, inundaciones, cortocircuito, entre otros)** | Disponer de una compañía aseguradora que posibilite defender el comercio contra incendios, terremotos, actos de terrorismo, huelgas, inundaciones, cortocircuitos, entre otros. | 6.1.3<br>11.1.4<br>17.1.2<br>17.1.3 | - Oficina de Alfonso Ugarte<br>- Laptops de desarrollo | 2 |
| **El acuerdo de confidencialidad de la seguridad de la información** | Cláusula que señale la utilización conveniente de la información expuesta en la correspondencia institucional de los ayudantes para eludir fugas de información, accesos no autorizados. Cláusula que señale la utilización adecuada de la información de otorgados al personal al principio y a lo largo de su contratación, incluye la política de estabilidad de la información de la compañía y los procedimientos de trabajo apropiados. Cláusula que señale la utilización conveniente de la información de datos del personal para eludir fugas de talentos. | 6.1.5<br>6.2.2<br>7.1.1<br>7.1.2<br>7.2.1<br>7.2.3<br>9.2.2<br>9.2.4<br>9.3.1<br>13.2.2<br>13.2.4 | - Reporte de acceso de usuarios Radmin VPN Y ANYDESK<br>- Documentación administrativa<br>- Persona<br>- Laptops de desarrollo<br>- Registro de órdenes de compras<br>- Registro de órdenes de ventas<br>- Correo electrónico<br>- Datos del personal<br>- Control de salarios<br>- Datos del cliente | 1 |
| **Auditorias** | Hacer auditorías para visualizar los cumplimientos que se conducen a cabo y llevar su control conveniente. | 6.1.5<br>6.2.2<br>7.1.1<br>7.1.2<br>7.2.1<br>7.2.3<br>9.2.2<br>9.2.4<br>9.3.1<br>13.2.2<br>13.2.4<br>12.7.5 | -Todos los procesos involucrados | 1 |

| MÉDIDAS DE SEGURIDAD | DESCRIPCIÓN | CONTROL | ACTIVOS | GRUPO |
|---|---|---|---|---|
| **Política de seguridaddde correo electrónico** | Política para la implementación correcto de la correspondencia electrónica, recalcando que la indagación es confidencial y no se debe usar para fin propio. | 6.1.5<br>6.2.2<br>9.1.1<br>9.2.1<br>13.2.3 | - Datos del personal<br>- Listado de órdenes de ventas y compras<br>- Listado de instaladores de software<br>- e-mail | 1 |
| **Política de teletrabajoy penalidades** | Política para empleados que trabajan de forma remota o cuando se toman computadoras portátiles para realizar actividades fuera del sitio la oficina. | 6.2.2<br>8.1.4<br>11.2.5<br>11.2.6 | - Laptops de desarrollo | 1 |
| **Formato de entrega de equipos** | Formato en el que se proporciona el nombre de los trabajadores, las especificaciones del dispositivo designado, las normas de uso adecuado, información sobre el estado del dispositivo, otros accesorios y el tiempo de entrega del dispositivo. | 6.2.2<br>11.2.4<br>11.2.7 | - Laptops de desarrollo | 1 |
| **Contratar una empresa aseguradora (Póliza de equipos)** | Disponer de una compañía de seguros que te posibilite defender los conjuntos electrónicos (computadoras, laptops, etcétera.) contra hurto, vandalismo o perjuicios internos. . | 6.2.2<br>8.3.1<br>17.1.2<br>17.1.3 | - Laptops de desarrollo<br>- Oficina de Alfonso Ugarte | 2 |
| **Lista de contacto de autoridades** | Lista de autoridades relevantes a contactar en caso de un incidente mayor. | 6.1.3 | - Oficina de Alfonso Ugarte | 2 |
| **Listado de contactos con grupos de interés en SI** | Lista de partes interesadas relevantes para contactar si surgen inquietudes sobre la SI en las empresas. | 6.1.4 | - Persona | 2 |
| **Política de uso y el manejo de información confidencial y pérdida en Seisystem** | Definir los estándares para proteger la indagación del uso, divulgación o divulgación no autorizados. | 7.1.2 | - Reporte de acceso de usuarios Radmin VPN Y ANYDESK<br>- Documentación administrativa | 1 |

| | | | | |
|---|---|---|---|---|
| **Política de proveedores** | Política basada en el establecimiento de las condiciones primordiales en caso de ingreso a la información de la organización de parte de los proveedores. | 7.2.1<br>15.1.1<br>15.1.2<br>15.1.3 | - Persona<br>- Laptops de desarrollo | 1 |

| MÉDIDAS DE SEGURIDAD | DESCRIPCIÓN | CONTROL | ACTIVOS | GRUPO |
|---|---|---|---|---|
| **Planificación de capacitaciones y concientización con los involucrados** | Política en la que cada colaborador debería conocer las metas fijadas que debería consumar en funcionalidad de la confidencialidad, totalidad y disposición de la estabilidad de la indagación. Composición de las carpetas de las zonas personales de la organización con detalle de los individuos autorizadas. Considera copias de estabilidad de la BD de la organización y de las bases de los consumidores | 7.2.2<br>8.1.3<br>9.1.1<br>11.2.8<br>11.2.9 | - Persona<br>- Reporte de acceso de usuarioVPN Y ANYDESK<br>- Laptops de desarrollo<br>- Datos de cliente<br>- Información administrativa<br>- Registro de órdenes de compras<br>- Listado de los instaladores de softwares<br>- Información y/o datos de trabajador | 1 |
| **Política de SI** | Política en la que cada trabajador debería conocer las metas fijados que debería consumar en funcionalidad de la confidencialidad, totalidad y disponibilidad de la estabilidad de la indagación. | 7.2.2 | - Control de salarios<br>- Reporte de acceso de usuarioVPN Y ANYDESK<br>- Laptops de desarrollo<br>- Datos de usuarios<br>- Lista de instaladores de software | 1 |
| **Estructura ordenada de carpeta parael acceso a usuarios** | Estructura de las carpetas de las áreas individuales de la organización con detalle de las personas autorizadas. | 7.2.2<br>9.1.1<br>9.2.1<br>9.2.5 | - Control de salarios<br>- Reporte de acceso de usuarioVPN Y ANYDESK<br>- Laptops de desarrollo<br>- Información administrativa<br>- Lista de instaladores de software<br>- Listado y/o órdenes deventas y compras. | 1 |

| | | | | |
|---|---|---|---|---|
| **Aplicación de metodologías** | Métodos seleccionados para el desarrollo de software en la empresa seisystem consultores | 14.2.1 | - Laptops de desarrollo | **1** |
| **Respaldos de BD / BD Clientes** | Considera copias de estabilidad de la BD de la organización y de los consumidores para los que se otorga el servicio. | 14.2.4<br>14.2.9 | - Todos los procesos involucrados | **1** |

| MÉDIDAS DE SEGURIDAD | DESCRIPCIÓN | CONTROL | ACTIVOS | GRUPO |
|---|---|---|---|---|
| **Modelos de sanciones de acuerdo a la SI** | Registrar modelos de sanciones en la normativa interna que atenten contra la estabilidad de la indagación de la compañía, y por consiguiente tomar elecciones acertadas al aplicarlas. | 7.2.3<br>18.2.1 | - Persona | 1 |
| **Informe de terminación y cambiode cargo** | Notificar a todos los empleados, la culminación de un contrato. | 7.3.1 | - Reporte y/o informe de acceso de usuarioVPN Y ANYDESK | 1 |
| **Inventariado de activos** | Registrar los activos más importantes en su periodo de vida y documentar su trascendencia, además requiere ser actualizado de manera estricta y constante. | 8.1.1<br>8.1.2<br>12.6.1 | - Todos los procesos | 1 |
| **Clasificación y valorización de activosde información** | Se realiza valorización de los activos según los 3 criterios: disponibilidad confidencialidad, integridad (D, I, C) | 8.2.1<br>12.6.1 | - Todos los activos involucrados | 1 |
| **Etiquetado de información** | Se realizará etiquetado a los activos con mayor importancia en la organización. | 8.2.2<br>8.2.3 | - Todos los activos mencionados | 1 |
| **Proceso de entrega de activos del personal enel proceso de desvinculación con la empresa** | En el proceso de despido de empleados, se requieren trámites adicionales ya que los empleados deben devolver todos los bienes del consultor.<br>Ya sea por contrato o acuerdo. | 8.1.4 | - Laptops de desarrollo | 1 |

| MÉDIDAS DE SEGURIDAD | DESCRIPCIÓN | CONTROL | ACTIVOS | GRUPO |
|---|---|---|---|---|
| **Implantar controlesde seguridad cuandose cambien a la siguiente oficina** | Disponer de controles de estabilidad como huelleros de autenticación de control de ingreso exclusivo por cada trabajador, cámaras de vigilancias. | 11.1.2<br>11.1.3 | - Oficina de Alfonso Ugarte | 2 |
| **Procedimiento de gestión de incidentes** | Este proceso se tiene con el fin de tener un listado de incidentes para futuras revisiones. | 16.1.1<br>16.1.2<br>16.1.3<br>16.1.4<br>16.1.5<br>16.1.6<br>16.1.7 | - Todos los activos mencionados | 1 |
| **Plan de continuidad dela SI** | Tiene como fin mantener la estabilidad de indagación en la compañía frente a situaciones adversas. | 17.1.1 | - Laptops de desarrollo | 1 |
| **Procedimiento de control de información documentada** | Tiene como fin explicar las ocupaciones para implantar, documentar, mantener el control de y conservar los documentos. | 18.1.3 | - Control de procedimiento<br>- Registros de órdenes de compras y facturas<br>- Datos del personal<br>- Control de salarios<br>- | 1 |
| **Revisión de laSI** | Implantar la revisión de la estabilidad de indagación periódica para detectar dichas oportunidades de optimización. | 18.2.2 | - Toda la documentación referente a la SI. | 2 |

Nota: (De La Sota & Mechan, 2018)

### 3.8.4 Fase IV Ejecución y supervisión

#### C) Verificar

En cuanto a la implementación del plan de SI propuesto, es importante destacar que, utilizando únicamente las medidas de seguridad antes mencionadas, la probabilidad de éxito es entre alta, ya que la empresa opta por minimizar el costo y recomienda la idoneidad de las Plan propuesto a ejecutar en el menor tiempo posible. Luego de determinada la política de seguridad, se aplicaron todas las medidas detalladas en la tabla anterior, las evidencias se adjuntan en la sección de anexos de este trabajo, y en la siguiente tabla se relacionan los anexos correspondientes a las evidencias de la política de seguridad aplicada.

*Tabla 26: política de seguridad*

| Activo | Política de seguridad o salvaguarda | Evidencia |
|---|---|---|
| Datos de clientes | Software desarrollado | |
| Software “Scan web” | Manuales de instalación | **Anexo 15** |
| Discos externos | Etiquetados para equipos | **Anexo 13** |
| | Copias de seguridad periódicas | **Anexo 14** |
| | Plantes de contingencia y continuidad | |
| | Cuentas de administración | |
| BD empresa/ BD clientes | Copias de seguridad | **Anexo 14** |

Nota: Elaboración propia

La ejecución de la auditoría se realiza en el siguiente objetivo ya que se realizó un software con ese proceso.

### 3.8.5 Fase V Mejora continua

#### D) Actuar

Luego de aplicar las medidas oportunas, se decidió realizar una encuesta a los trabajadores de la empresa sobre las medidas implementadas, cuyo resultado fue una importante optimización del SI de la empresa, como se puede apreciar en el Anexo 11.

Se encontró que era imperativo actualizar las políticas de resiliencia aplicadas ya que la empresa tiene un flujo de información cada vez mayor y de igual manera se sentó un precedente en la empresa ya que nunca antes había tenido una política formal de resiliencia protegiendo sus activos clave.

**Herramientas de desarrollo**

Para este plan se utilizará SQL SERVER 2016. NEXTECH (2021). Informa que es un SGBD relacionado al desarrollo como servidor que da en otras aplicaciones del programa. Es igualmente posible que estos se ejecuten en nuestra PC o en otra PC a través de la red.

Además, se usará Microsoft Visual Studio. EspacioHonduras (2021). Muestra que es un alcance que incluye desarrollo, es fabricado por Microsoft, se puede usar en los múltiples sistemas operativos y es compatible con diversos idiomas de programación. En lenguaje de programación c#. Microsoft (2021). Informa que es un lenguaje de programación nuevo, con base en objetos y con seguridad. C# permite crear diversos tipos de aplicaciones a los desarrolladores de forma segura y sólidas las cuales se ejecutan en .NET.

Asp. Net. RedUsers (2021). Informa que hablamos de un ámbito que posibilita a los desarrolladores producir toda clase de sistemas con orientación a la Web dentro del Framework .NET. Este es un ámbito de trabajo de código abierto realizado por Microsoft para el desarrollo de diversos tipos de aplicaciones.

Razor. TechClub. (2018). Plantea que es una sintaxis de programación ASP.NET usada para generar páginas web dinámicas con los idiomas de programación C # o Visual Basic .NET.

Arquitectura Modelo – Vista – Controlador

MarketiWeb.com (2021). Informa que la arquitectura MVC (modelo, vista, controlador) consta de un jefe de diseño de programa que se usa para dividir los datos, los procedimientos y la interfaz gráfica de la aplicación en 3 elementos.

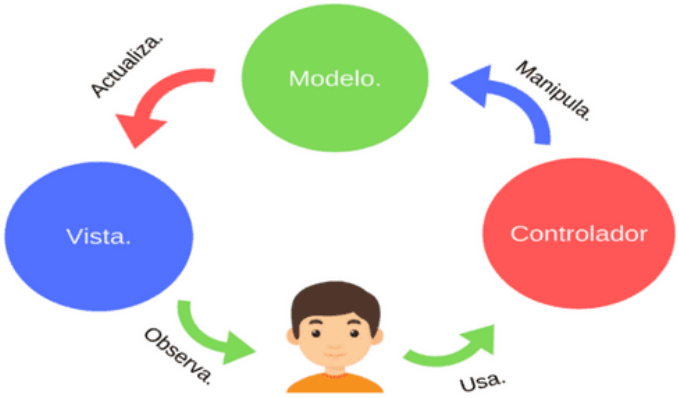
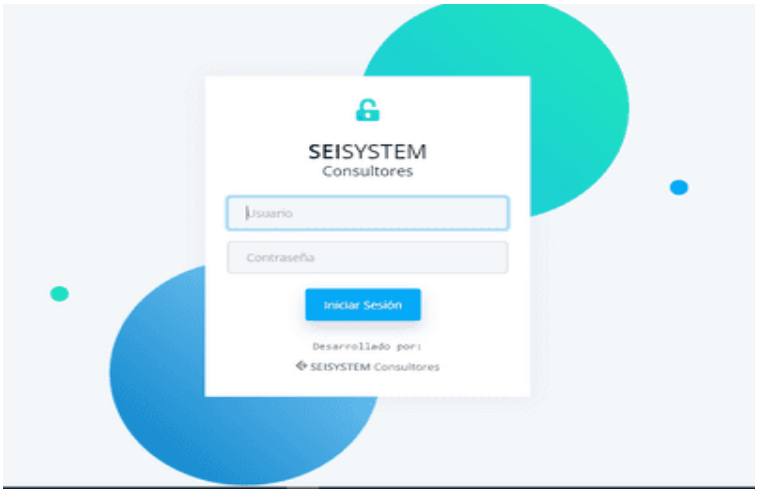


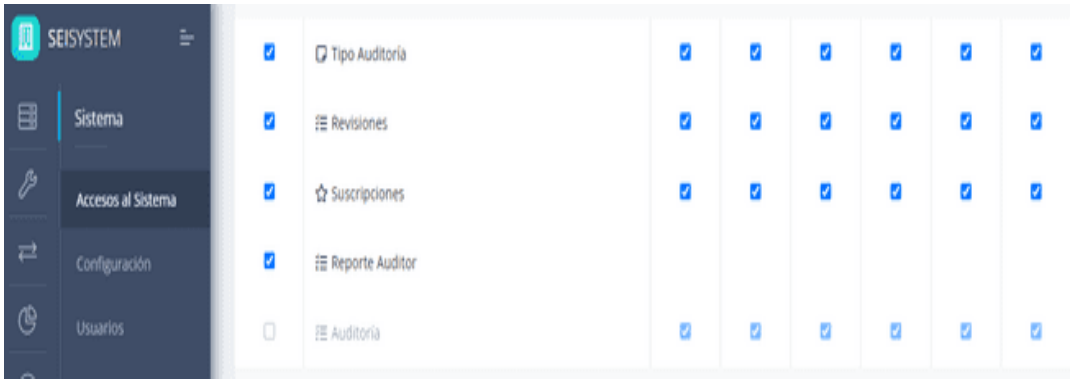

*Ilustración 9: Patrón de diseño de software*

**Desarrollo y aplicación**

En primera instancia se tiene el Login, donde él auditor interno tendrá que iniciar con su usuario y contraseña brindado por el gerente general.



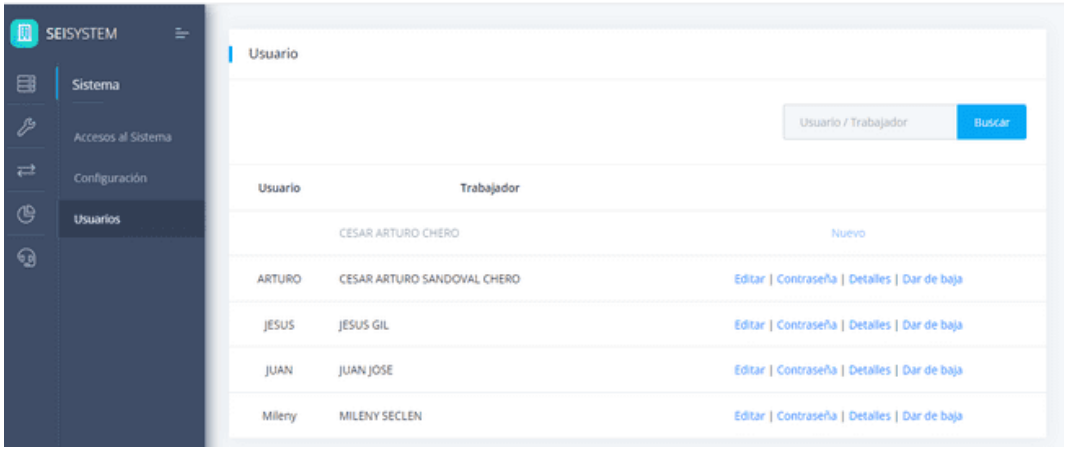

Se tiene la gestión de permios y/o acceso al sistema por usuario (ACCESOS AL SISTEMA) que se le puede habilitar a cada usuario.



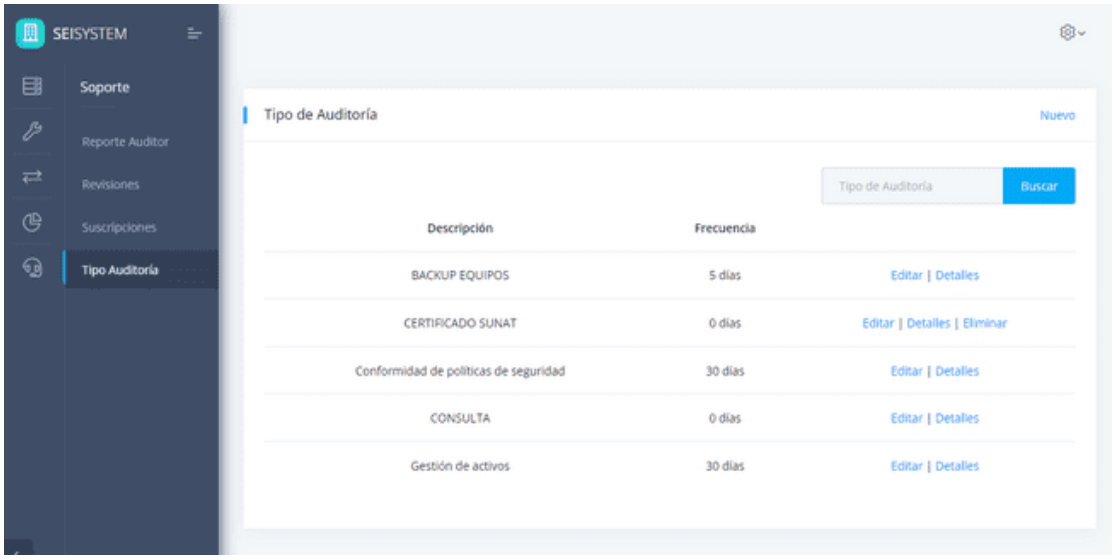

Para la asignación de un usuario, primero se tiene que crear como trabajador.

De una vez creado el trabajador, en esta parte se asigna el usuario al trabajador

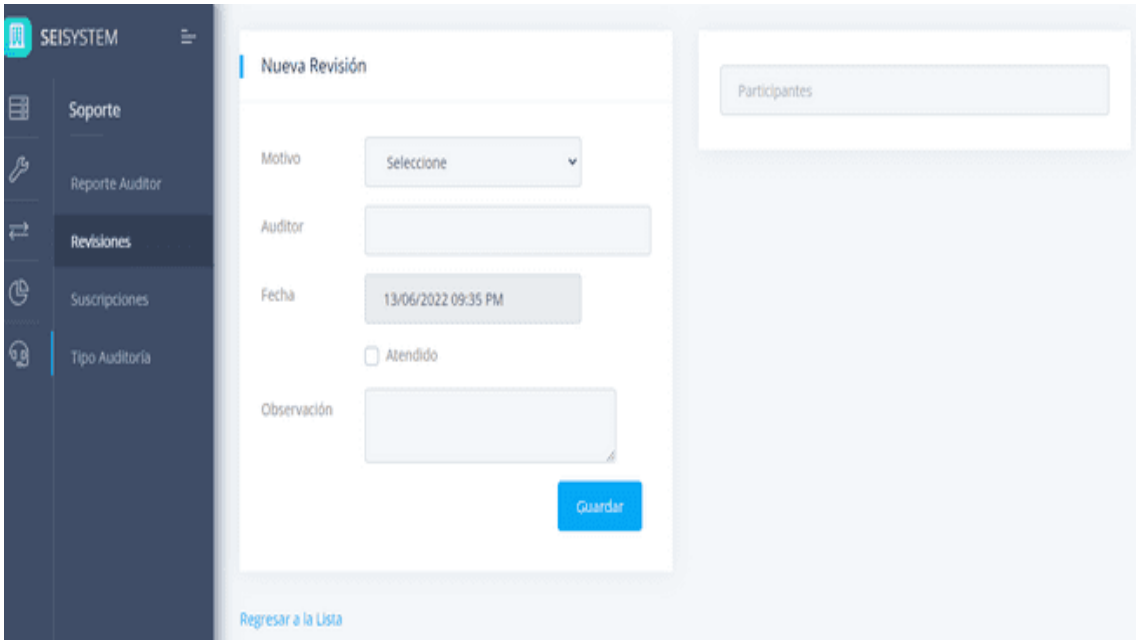

donde podemos asignarle su contraseña, editarlo, ver su detalle, y darle de baja al usuario.



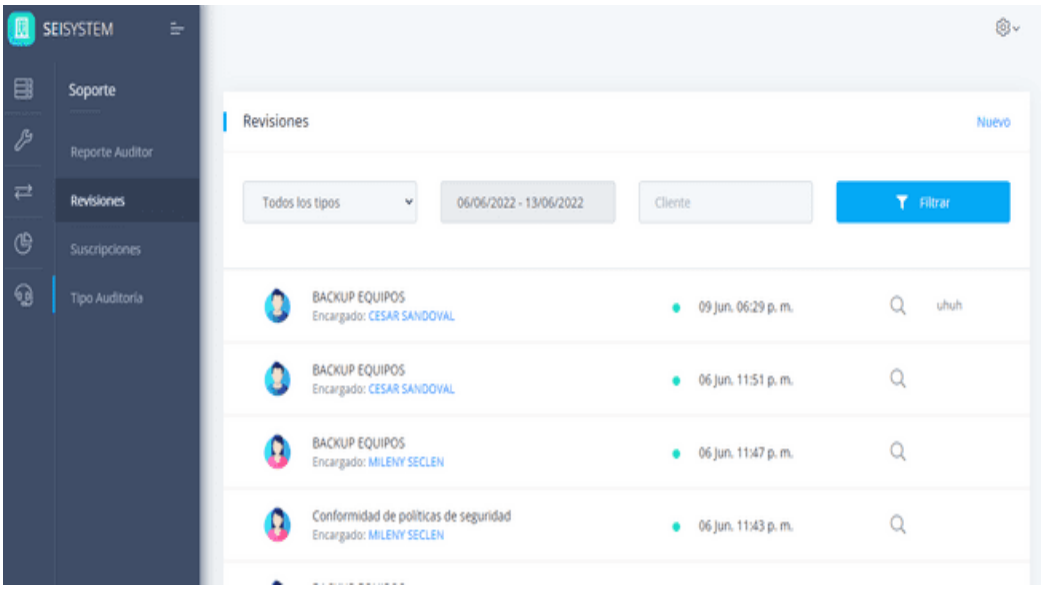
Luego de ingresar con las credenciales, el auditor tiene los diferentes módulos a navegar en el sistema. Como **TIPO AUDITORIA** Se irán registrando los tipos de auditorías y/o temas a tratar con los participantes.



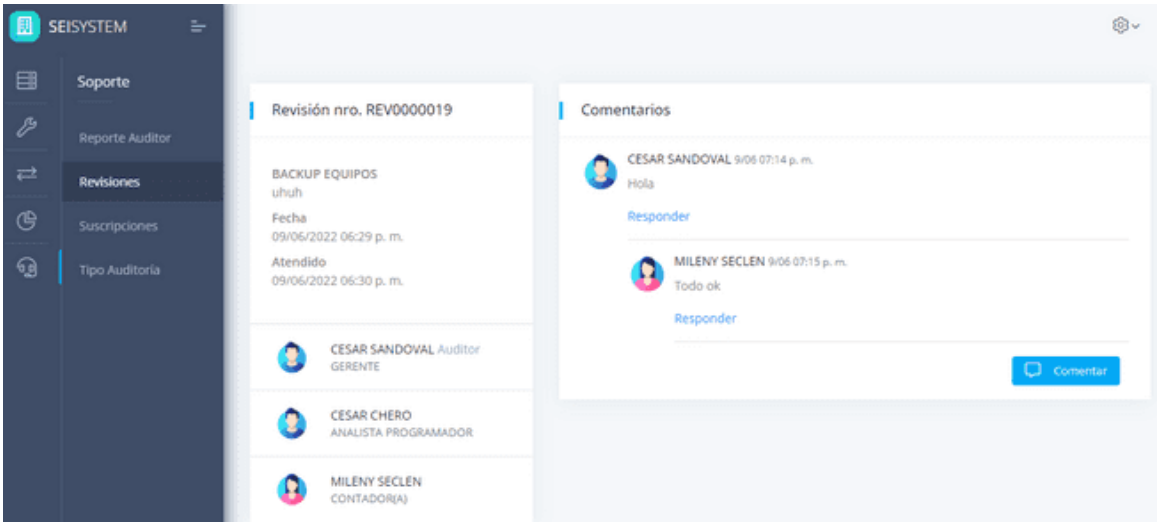

Luego se tiene el módulo de **REVISIONES donde después de seleccionar sus** tipos de auditoría puede crear las revisiones que se darán en la auditoría.



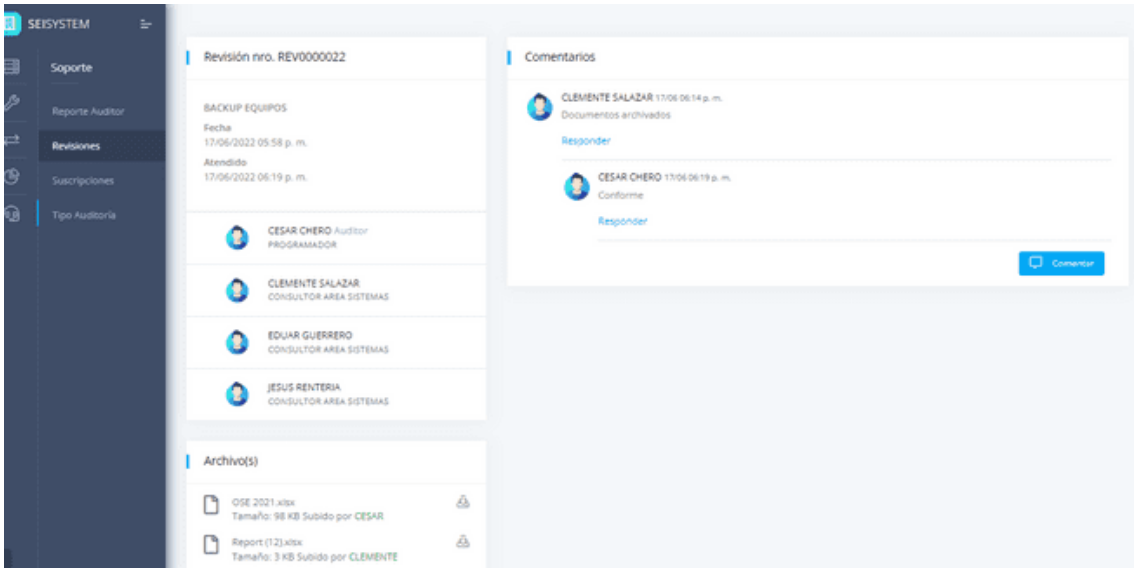
A partir de ello en la pantalla que se muestra seleccionara el motivo, el auditor, la fecha la toma en tiempo real y en la parte izquierda se tiene la asignación de participantes donde se irán agregando con respecto a las áreas de la empresa o donde se llevará acabo la auditoría.



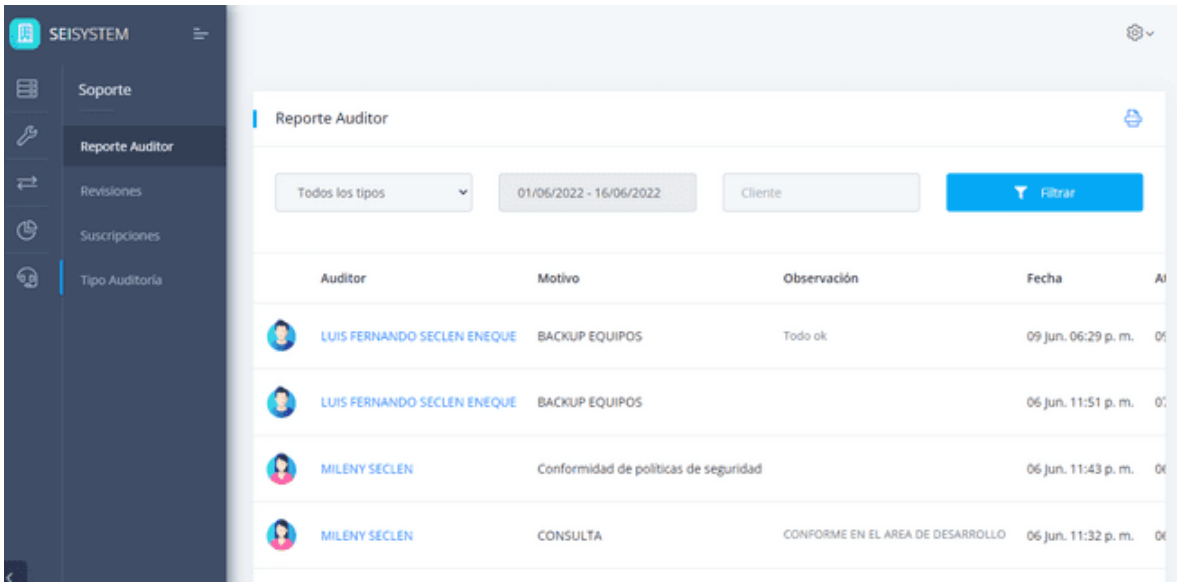

En el proceso de la auditoría con los involucrados de cada área se proceden adjuntar archivos para la muestra al auditor y corroborar con el cumplimiento.



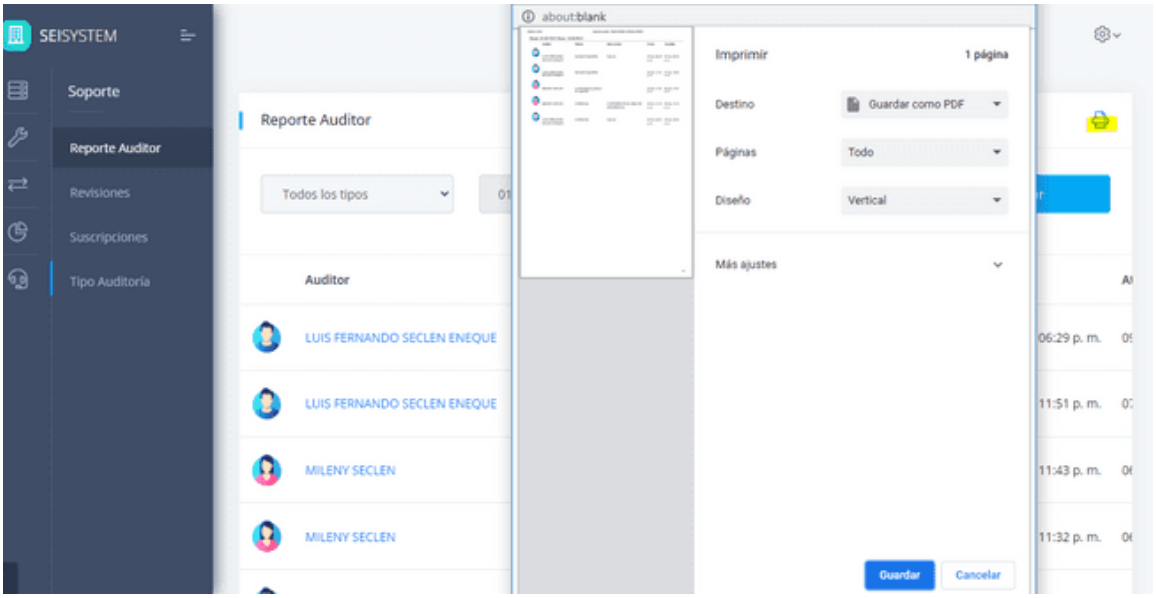
Luego de finalizar la auditoría se tiene un detalle donde se agregarán comentarios por parte del auditor y de los participantes, se puede observar la interacción.




Por último, se tiene un reporte general del auditor, aquí el auditor visualiza de manera rápida las reuniones que se realizó y en las que puede estar involucrado recordando que el auditor puede cambiar de acorde a la asignación del gerente general.



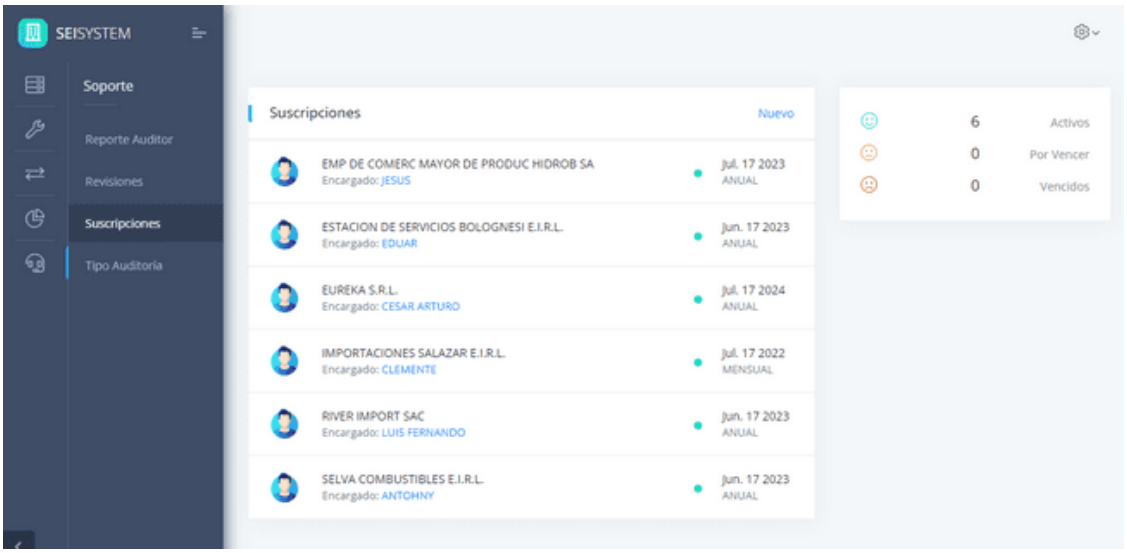
Donde se tiene un botón en la parte superior derecha para poder imprimirlo




Actualmente los datos de los clientes a los que se les brinda el servicio lo tienen en Excel y genera enormes confusiones con respecto las suscripciones que toman al adquirir el sistema, e incluso se da soportes a empresas que ya vencieron su tiempo de soporte. El módulo de suscripciones va referente en cuando a los clientes a los que se les brinda el servicio, relacionado con los trabajadores de la empresa. La cual sirve para que registren cada uno, las empresas que tienen asignadas y así llevar un control sobre el tipo de suscripciones que se lleva con el cliente. Se muestra el ejemplo de la prueba piloto con empresas reales que se manejan dentro de la empresa seisystem consultores.

Como se puede observar este es el último módulo desarrollado y puesto en práctica en la empresa seisystem consultores mostrando datos reales de los que maneja la empresa, especificando no todos los datos, pero se tomó ciertos clientes como prueba, mejorando el tema de la gestión de los clientes que tiene a cargo la empresa seisystem consultores. Con eso se culminaría el tema del desarrollo del software que se propuso en los objetivos.

A partir de ellos se continuará con las evaluaciones de los indicadores restantes.



# IV. CONCLUSIONES Y RECOMENDACIONES

## 4.1. Conclusiones.

La estabilidad de la información de Seisystem Consultores, previo a la utilización de un modelo de administración de estabilidad de la indagación acorde a la regla ISO/IEC 27001, era casi nula, lo cual provocaba que, en las superficies de sistemas y soporte técnico, la contabilidad de la organización pudiera ser atacada por diferentes virus pertenecientes al tipo malware, realizando que la información que maneja la organización se encuentre en peligro.

La revisión sistemática ayudó a extraer estándares de la norma IS/IEC 27001 con diversas metodologías, la cual se pudo identificar una de ellas muy potentes como MAGERIT para la gestión de riesgos y así poder aplicarla en el presente trabajo.

El modelo planteado, fue aprobado por tres expertos la cual dicho modelo contenía 5 fases donde se enlazó MAGERIT para la gestión de riesgos alineada a la norma ISO/IEC 27001.

El modelo desarrollado se caracterizó por rescatar los periodos más primordiales de la regla ISO/IEC 27001:2013 con la metodología PDCA y la metodología Magerit para gestión de riesgos, aunados a las necesidades primordiales que tiene la compañía para poder hacer defender su información.

La implementación y aplicación del software en la empresa Seisystem Consultores, se obtuvo una mejora con respecto al tema de las auditorías internas. La cual todo el personal es partícipe de acuerdo al área perteneciente, donde pueden interactuar en tiempo real en el software. Por otro lado, se obtuvo ordenamiento, seguridad con respecto a los accesos a la información y/o asignación de credenciales.

## 4.2. Recomendaciones.

El modelo desarrollado en esta averiguación fue aplicado a una micro compañía Seisystem consultores, para obtener resultados semejantes a los encontrados en esta averiguación, se debería priorizar el tipo de indagación que maneja la empresa, así como además la proporción de trabajadores, y finalmente el flujo de información que manejan.

Es importante señalar que la organización en cuestión no tenía ninguna política ni regla de SI, el modelo desarrollado en esta indagación se usó para realizar políticas que se adecuen a la realidad de la organización y a sus necesidades, en este caso específico la organización tiene como prioridad proteger su información ante cualquier eventualidad.

La prioridad de la organización Seisystem Consultores, es la de obtener de manera instantánea, protección para la indagación que se maneja la organización, es por ello que el modelo concentra lo más importante y fundamental de la regla ISO/IEC 27001:2013 y la metodología Magerti para gestión de riesgo. La elección de los periodos se toma con base a la mera necesidad de la compañía en cuestión.

Se ofrece mejorar el software que va referente al proceso fundamental que es la Auditoría interna y todo cambio que se haga deberá se ser documentado.

**REFERENCIAS.**


Ahmad Z., Song T., Hui T., & Norhashim M. (2019). Security monitoring and information security assurance behaviour among employees An empirical analysis. *Information & Computer Security*, 165-188.

Alkilani, H., & Qusef, A. (2021). Osint techniques integration with risk assessment ISO/IEC 27001. *ACM International Conference Proceeding Series*, 82-86.

Baca, V. (2016). Diseño de un sistema de gestión de la seguridad de la Información para la unidad de gestión educativa local - Chiclayo. *Ingeniería: Ciencia, Tecnología e Innovación*, 42-45.

Carnero, D., Carbajal, M., J, & Madrid, A.-A. J. (2020). Information security risk management model for mitigating the impact on SMEs in Peru. *Iberian Conference on Information Systems and Technologies, CISTI*.

Computer Fraud & Security. (18 de Enero de 2021). North Korea attacks Covid-19 research bodies. *Computer Fraud & Security*, pág. 3.

De La Sota, K., & Mechan, Y. (2018). IMPLEMENTACIÓN DE CONTROLES Y CUMPLIMIENTO DE IMPLEMENTACIÓN DE CONTROLES Y CUMPLIMIENTO DE DE INFORMACIÓN EN UNA PYME CONSULTORA. *TESIS.* Universidad San Martín de Porres, Lima-Perú.

Dieguez, M., Cares, C., & Cachero, C. (2017). Methodology for the information security controls selection. 1-6.

Garay, D., C, M., Armas-Aguirre, J., & Molina, J. (2020). Information security risk management model for mitigating the impact on SMEs in Peru. *Iberian Conference on Information Systems and Technologies, CISTI*.

Heidenreich, M. (2019). Conceptualization of a measurement method proposal for the assessment of IT security in the status quo of micro-enterprises. *Proceedings - 2019 International Conference on Computing, Electronics and Communications Engineering, iCCECE 2019*, 187-192.

Hurtado, M. (2020). Gestión de riesgo metodologías octave y magerit. *Universidad Piloto de Colombia - Metodología de Análisis de Riesgo.*, 1-12.

ISO. (6 de Mayo de 2021). *ISO*. Obtenido de ISO: https://www.iso.org/standard/54533.html

ISO Tools exellence. (6 de Mayo de 2021). *ISO Tools exellence*. Obtenido de ISO Tools exellence: https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

ISO Tools exellence. (6 de Mayo de 2021). *ISO Tools exellence*. Obtenido de ISO Tools exellence: https://www.isotools.org/2016/07/07/sistema-gestion-seguridad-la-informacion-basado-la-norma-iso-27001/

ISO27000.ES. (6 de Mayo de 2021). *ISO27000.ES*. Obtenido de ISO27000.ES: https://www.iso27000.es/iso27000.html

Jaramillo, H., Guaman, B., & Salazar, E. (2015). Information security in implementing web applications for small businesses based on COBIT5-SI [Seguridad de la Información en la implementación de aplicaciones web para pequeñas empresas en base a COBIT5-SI]. *2015 10th Iberian Conference on Information Systems and Technologies, CISTI 2015*. Obtenido de https://www.scopus.com/inward/record.uri?eid=2-s2.0-84943279820&doi=10.1109%2FCISTI.2015.7170390&partnerID=40&md5=9542f55634f822a4bd8bb37d5f3d84f7

Jimenez, H., Rodriguez, R., & Tiparra, J. (1978). *Diagnóstico de TEA.* Madrid: Latinoamérica SA.

Khan, A., Khan, R., & Nisar, F. (2017). Novice threat model using SIEM system for threat assessment. *International Conference on Communication Technologies, ComTech 2017*, 72-77.

Leguizamón, M., Bonilla, M., & C., L. (2020). Análisis de ataques informáticos mediante Honeypots en laUniversidad Distrital Francisco José de Caldas. *Ingenieria y competitividad, 22*.

Lopez-Leyva, J., Kanter-Ramirez, C., & Morales-Martinez, J. (2020). Customized diagnostic tool for the security maturity level of the enterprise information based on ISO/IEC 27001. *Proceedings - 2020 8th Edition of the*

*International Conference in Software Engineering Research and Innovation, CONISOFT 2020*, 147-153.

Mejia, I., Ramirez, R., Jimenez, H., & Rosas, J. (2019). A new method a architecture entreprise. *Conference IEEE bussines*, 200-215.

Mejia, I., Tuesta, M., & Forero, M. (2020). A new method of enterprise archicture small organizations. *Computer Science Techology*, 150-170.

Mena, A. (2018). Framework to implement information security management systems: An asset to project management processes. *Proceedings - International Conference of the Chilean Computer Science Society, SCCC, 2018-Novem*, 1-8.

Mercaldo, F. (2021). A framework for supporting ransomware detection and prevention based on hybrid analysis. *Journal of Computer Virology and Hacking Techniques, 17*, 221-227. doi:10.1007/s11416-021-00388-w

Ministerio de hacienda y administraciones públicas - Gobierno de España. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de hacienda y administraciones públicas - Gobierno de España.

Nechai, A., Pavlova, E., Batova, T., & Petrov, V. (2020). Implementation of Information Security System in Service and Trade. *IOP Conference Series: Materials Science and Engineering, 940*. Obtenido de IOP Conference Series: Materials Science and Engineering.

Palma, J., & Marín, R. (2008). *Inteligencia Artificial.* Madrid: McGrawHill. doi:978-84-481-5618-3

Rahmawati, D., Yudhiyati, R., & Putritama, A. (2019). How Micro and Small Enterprises Perceive Information Technology Fraud: A Study of Indonesian' Small Businesses. *How Micro and Small Enterprises Perceive Information Technology Fraud: A Study of Indonesian' Small Businesses*.

Restrepo, D. (2018). *Prezi*. Obtenido de https://prezi.com/p/sccr7ktzwcry/metodologia-ebios/

Reyes, J., Muñoz, C., & Guarda, T. (2018). Computer security for small and medium-sized enterprises of the province of santa elena. *RISTI - Revista Iberica De Sistemas e Tecnologias De Informacao*, 144-152.

Rojas, K. (2018). Identificación de efectos negativos de la TEA en el aprendizaje. *IEEE conference Techology children especial*, 200-215.

Rojas, K. (2018). Identificación de efectos negativos de la TEA en el aprendizaje. *IEEE conference Techology children especial*, 200-215.

Safonova, O., Lontsikh, N., Golovina, E., Elshin, V., & Koniuchov, V. (2020). Methodology for creating, implementing and system effectiveness evaluation of the business processes' information security system. *Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020*, 127-131.

Schmitz, C., & Pape, S. (2020). LiSRA: Lightweight Security Risk Assessment for decision support in information security. *Computers and Security, 90*.

Shinde, N., & Kulkarni, P. (2021). Cyber incident response and planning: a flexible approach. *Computer Fraud & Security*, 14-19.

Subakti, P., & Putra, Y. (2020). Integration of TOGAF 9.1 ADM in Enterprise Architecture Smart City Design in the Tourism Domain with ISO 27001. *IOP Conference Series: Materials Science and Engineering, 879*.

SZNAJDLEDER, P. (2012). *Java a fondo - estudio del lenguaje y desarrollo de aplicaciones - 2a ed.* México: Alfaomega.

Tanovic, A., & Marjanovic, I. (2019). Development of a new improved model of ISO 20000 standard based on recommendations from ISO 27001 standard. *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2019 - Proceedings*, 1503-1508.

Velasco, J., Ullauri, R., Pilicita, L., Jacome, B., Saa, P., & Moscoso-Zea, O. (2018). Benefits of implementing an ISMS according to the ISO 27001 standard in the ecuadorian manufacturing industry. *Proceedings - 3rd*

*International Conference on Information Systems and Computer Science, INCISCOS 2018*, 294-300.

Yasin, M., Arman, A., & Edward, I. &. (2020). Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ). *Proceeding of 14th International Conference on Telecommunication Systems, Services, and Applications, TSSA 2020*, 3-7.

Yun, J., Hur, J., Shin, Y., & Koo, D. (2017). CLDSafe: An efficient file backup system in cloud storage against ransomware. *IEICE Transactions on Information and Systems*, 2228-2231.

**ANEXOS.**

**Anexo 1.** Resolución de aprobación del proyecto de investigación

UNIVERSIDAD SEÑOR DE SIPÁN

**FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO**

**RESOLUCIÓN N°1179--2021/FIAU-USS**

Pimentel, 10 de diciembre de 2021

**ANEXO**

| N° | AUTOR(ES) | TEMA DE TESIS |
|---|---|---|
| 1 | CABRERA SANCHEZ KEVIN ALONSO<br>MENDOZA FERRE ESPERANZA NATALY | DESARROLLO DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS PARA MEJORAR LA DISPONIBILIDAD DE SERVICIO DE TI DE UN MUNICIPIO DISTRITAL |
| 2 | ROJAS ARRUNATEGUI JOEL ENRIQUE<br>YAFAC LAU CESAR LEONIDAS | DESARROLLO DE UN MODELO DE PROCESOS PARA LA ADQUISICIÓN DE SOFTWARE BASADO EN LA NTP-ISO/IEC 12207 PARA MEJORAR LA GESTIÓN DE LAS ADQUISICIONES DE SOFTWARE EN MICROEMPRESAS PERUANAS |
| 3 | FERNANDEZ MALUQUIS JOSE EFRAIN | ANALISIS DE ALGORITMOS BALANCEADORES DE CARGA PARA UN CLÚSTER DE SERVIDORES PARA MEJORAR LA DISPONIBILIDAD DE UN SERVIDOR |
| 4 | RAMOS SANDOVAL FABIOLA ARACELY<br>CANTORAL MONTEJO CESAR ENRIQUE | DESARROLLO DE UN MÉTODO DE CLASIFICACIÓN AUTOMÁTICA PARA LA DETECCIÓN EFICIENTE DEL RIESGO DE ANEMIA INFANTIL A PARTIR DE HÁBITOS DE ALIMENTACIÓN Y CUIDADOS |
| 5 | BOCANEGRA GUERRERO YERSON<br>HUAMAN HUANCAS DERBIS | ANÁLISIS COMPARATIVO DE ARQUITECTURAS DE APRENDIZAJE PROFUNDO PARA LA CLASIFICACIÓN DE ROYA AMARILLA EN HOJAS DE CAFÉ |
| 6 | SANDOVAL CHERO CESAR ARTURO | MODELO DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA NORMA ISO/IEC 27001 ORIENTADO A LAS MICROEMPRESAS |
| 7 | DENNIS MAURICIO AVILES ODAR | APLICACIÓN DE BUENAS PRÁCTICAS PARA ENTORNOS DE DESARROLLO DE SOFTWARE BASADOS EN DEVOPS PARA MEJORAR LA INTEGRACIÓN Y DESPLIEGUE DE PROYECTOS EN UNA EMPRESA CONSULTORA DE LA CIUDAD DE CHICLAYO |
| 8 | RIVAS PLATA CASAS CARLOS GUALBERTO | DETECCIÓN DE CÁNCER DE PULMÓN EN IMÁGENES DE TOMOGRAFÍAS MEDIANTE PROCESAMIENTO DE IMÁGENES Y APRENDIZAJE AUTOMÁTICO |
| 9 | PECHE SANCHEZ CHRISTIAN WILFREDO | DISEÑO DE ARQUITECTURA DE MICROSERVICIOS PARA OPTIMIZAR PROCESOS EN LA GESTIÓN DE VENTAS ONLINE |
| 10 | SEVERINO HERNÁNDEZ YAMPIER GILBERTO | EVALUACIÓN DEL RENDIMIENTO DE UNA APLICACIÓN WEB CON ARQUITECTURA DE MICROSERVICIOS SOPORTADOS EN LA NUBE EN UN AMBIENTE DE ALTA CONCURRENCIA |
| 11 | CHANG HIDALGO HAWARD MIGUEL | COMPARACIÓN DE TÉCNICAS DE ESTIMACIÓN BASADAS EN MACHINE LEARNING PARA PREDECIR COSTOS EN LOS PLANES DE ADQUISICIONES DE LAS ENTIDADES PÚBLICAS DEL PERÚ |
| 12 | PUICON PISFIL MIRIAN ALICIA<br>VILCHEZ CHANGANAQUI RICHARD ALEXIS | DESARROLLO DE UN MODELO DE PROCESOS BASADO EN ESTÁNDARES PARA LA EVALUACIÓN DE LA USABILIDAD WEB PARA MICROEMPRESAS PERUANAS |
| 13 | LOPEZ ABANTO GUILLERMO ANTONIO | EVALUACIÓN DE LA SEGURIDAD DE UN SISTEMA DE VOTACIÓN ELECTRÓNICA CON BLOCKCHAIN |
| 14 | CALDERON ZUÑIGA JESUS<br>TELLO TANTARICO DILSON GUZMAN | DESARROLLO DE UN MODELO DE GOBERNANZA DE TI BASADO EN MARCOS DE GOBIERNO Y GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN PARA INSTITUCIONES PÚBLICAS PERUANAS |

**Anexo 2.** Carta de aceptación de la institución para la recolección de datos.

**SOLICITO**: PERMISO PARA LA RECOLECCION DE LOS DATOS.

ING. LUIS FERNANDO SECLEN ENEQUE
Gerente General

Yo **CESAR ARTURO SANDOVAL CHERO**
Identificado con el DNI: N° **71870391** con el domicilio en UNION #237 STO DOMIGNO distrito de Lambayeque provincia de Lambayeque ante usted respetuosamente me presento y expongo.

Que siendo estudiante del décimo ciclo de la carrera Profesional de Ingeniería de Sistemas de la Universidad Señor de Sipán solicito a usted me conceda el permiso para la recolección de datos para mi proyecto de investigación titulado "MODELO DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA NORMA ISO/IEC 27001 ORIENTADO A LAS MICROEMPRESAS" ya que es necesario para la presentación de informe final.

Por lo expuesto:
Ruego a usted acceder a mi petición.

Lambayeque, 16 de junio del 2022

Firma del investigador
Cesar Arturo Sandoval Chero

Luis Fernando Seclen Eneque
Sei System Consultores
GERENTE GENERAL

Firma del Gerente General
Ing. Luis Fernando Seclen Eneque

SEISYSTEM
CONSULTORES

Alfonso Ugarte 633 Dpto 205
Lambayeque - Chiclayo - Chiclayo

(074) 476790 - 978815887
www.seisystemperu.com
ventas@seisystemperu.com

DE: SECLEN ENEQUE LUIS FERNANDO

**Venta de computadoras, impresoras, suminitros y accesorios.**
**Asesoramiento e instalación de redes - Soporte técnico - Desarrollo de sistemas**

CONSENTIMIENTO INFORMADO DE RECOLECCION DE DATOS PARA PROYECCION DE INVESTIGACION

EL GERENTE GENERAL DE LA EMPRESA SEISYSTEM CONSULTORES, QUE SUSCRIBE Y OTORGA LA PRESENTE:

Se solicita dar consentimiento para que el joven CESAR ARTURO SANDOVAL CHERO identificado con el DNI N°71870391 con domicilio UNION #237 STO.DOMINGO Distrito LAMBAYEQUE, Provincia LAMBAYEQUE participe en el estudio de investigación titulado: "MODELO DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA NORMA ISO/IEC 27001 ORIENTADO A LAS MICROEMPRESAS" El estudio de investigación incluirá: (recolección de datos, etc.), en el cual autorizo voluntariamente para que lleve a cabo su proyecto de investigación en esta institución.

Por lo expuesto:
Acceder a mi petición
Chiclayo, 17 de junio del 2022

Luis Fernando Seclen Eneque
Sei System Consultores
GERENTE GENERAL

Firma del Gerente General

17 de junio 2022
Fecha

Nombre del investigador que obtiene el consentimiento

Cesar Arturo Sandoval Chero

Firma del investigador

17 de junio 2022
Fecha

## ANEXO 3 ACTA DE COMPROMISO

SEISYSTEM
CONSULTORES

Alfonso Ugarte 633 Dpto 205
Lambayeque - Chiclayo - Chiclayo

(074) 476790 - 978815887
www.seisystemperu.com
ventas@seisystemperu.com

DE: SECLEN ENEQUE LUIS FERNANDO

Venta de computadoras, impresoras, suminitros y accesorios.
Asesoramiento e instalación de redes - Soporte técnico - Desarrollo de sistemas

**ACTA DE COMPROMISO DE LA ALTA DIRECCIÓN PARA LA IMPLEMENTACIÓN DE LA NORMA ISO 27001:2013- SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN (SGSI)**

En mi calidad de gerente general, manifiesto el compromiso y respaldo a la implementación del Modelo de la gestión de seguridad de la información (SGSI) alineado a la norma ISO/IEC 27001:2013 en SEISYSTEM COSULTORES.

Para dicho fin nos comprometemos a:

- Asignar los recursos para la implementación del SGSI.
- Realizar reuniones periódicas para verificar que la política seguridad y los objetivos de la seguridad de información estén alineados con la dirección estratégica de la organización.
- Comunicar la importancia de la gestión de la información mediante correos y reuniones.
- Realizar reuniones para identificar oportunidades en el SGSI.
- Verificar que los requisitos del SGSI están integrados en los procesos pertinentes de la organización mediante reuniones.
- Garantizar que el SGSI va a lograr alcanzar los resultados previstos mediante un seguimiento continuo.

Firma en señal de conformidad, en la ciudad de Chiclayo, a los 21 días del mes de MAYO del 2022

GERENTE GENERAL

Luis Fernando Seclen Eneque
Sei System Consultores
GERENTE GENERAL

## ANEXO 4

**TECNICA**: Observación

**INSTRUMENTO**: FICHA DE OBSERVACION

| | | | |
|---|---|---|---|
| | **FICHA DE OBSERVACION N°01: XXXXXXXXXXXXX** | | |
| | **FASE:** POST TEST | **CODIGO:** F0-01 | **VERSION:** V1 |
| | **Fecha de recolección:** | 11/06/2022 | |
| | **Investigador:** | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

***Fuente:*** (Agurto & Melgar, 2019)

**FICHA DE VALIDEZ DE CONTENIDO QUE MIDE EL MODELO DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADO A NORMA ISO/IEC 27001:201**

| DIMENSIONES / INDICADORES | PERTENENCIA | | RELEVANCIA | | CLARIDAD | |
|---|---|---|---|---|---|---|
| **VALORACION DE ACTIVOS** | SI | NO | SI | NO | SI | NO |
| 1.- Categoría | | | | | | |
| 2.- ID del riesgo | | | | | | |
| 3.-Activo | | | | | | |
| 4.Criterios (Confidencialidad, integridad, disponibilidad) | | | | | | |
| 5.-Impacto | | | | | | |
| **EVALUACION DEL RIESGO (Nivel del riesgo)** | | | | | | |
| 1.- Proceso involucrado | | | | | | |
| 2.- Activo crítico de información | | | | | | |
| 3.- ID del riesgo | | | | | | |
| 4.- Amenazas | | | | | | |
| 5.- Vulnerabilidades | | | | | | |
| 6.- Impacto | | | | | | |
| 7.-Probabilidad | | | | | | |
| 8.- Riesgo | | | | | | |
| **TRATAMIENTO DEL RIESGO (Número de controles aplicados)** | | | | | | |
| 1.-Título del control | | | | | | |
| 2.-Preguntas | | | | | | |
| 3.-Aplicación | | | | | | |
| 4.-Rango | | | | | | |
| 5.- Comentario | | | | | | |

Observaciones (Precisar si hay suficiencia) .....

Opciones de aplicabilidad: Aplicable ( ) Aplicable después de corregir ( ) No aplicable ( )

Apellidos y nombres del juez validador: ..... DNI:.....

Especialidad del validador: .....

1.- **Pertenencia**: El ítem corresponde al concepto teórico formulado.

2.- **Relevancia**: El ítem es el apropiado para representar al componente o dimensión específica del constructo.

3.- **Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

**Nota**: Suficiencia. Se dice suficiencia cuando los ítems planeados son suficientes para medir la dimensión.

_____

FIRMA

## Ficha firmada por los expertos

**FICHA DE VALIDEZ DE CONTENIDO QUE MIDE EL MODELO DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADO A NORMA ISO/IEC 27001:2013**

| DIMENSIONES / INDICADORES | PERTENENCIA | | RELEVANCIA | | CLARIDAD | |
|---|---|---|---|---|---|---|
| **VALORACION DE ACTIVOS** | SI | NO | SI | NO | SI | NO |
| 1.- Categoria | X | | X | | X | |
| 2.- ID del riesgo | X | | X | | X | |
| 3.-Activo | X | | X | | X | |
| 4.Criterios (Confidencialidad, integridad, disponibilidad) | X | | X | | X | |
| 5.-Impacto | X | | X | | X | |
| **EVALUACION DEL RIESGO (Nivel del riesgo)** | | | | | | |
| 1.- Proceso involucrado | X | | X | | X | |
| 2.- Activo critico de información | X | | X | | X | |
| 3.- ID del riesgo | X | | X | | X | |
| 4.- Amenazas | X | | X | | X | |
| 5.- Vulnerabilidades | X | | X | | X | |
| 6.- Impacto | X | | X | | X | |
| 7.-Probabilidad | X | | X | | X | |
| 8.- Riesgo | X | | X | | X | |
| **TRATAMIENTO DEL RIESGO (Número de controles aplicados)** | | | | | | |
| 1.-Titulo del control | X | | X | | X | |
| 2.-Preguntas | X | | X | | | X |
| 3.-Aplicación | X | | X | | X | |
| 4.-Rango | X | | X | | X | |
| 5.- Comentario | | X | | X | X | |

Observaciones (Precisar si hay suficiencia) En evaluación de riesgo, considerar una columna para "controles existentes"

Opciones de aplicabilidad: Aplicable ( ) Aplicable después de corregir (X) No aplicable ( )

Apellidos y nombres del juez validador: Cochay Maco Junior Eugenio DNI: 44404838

Especialidad del validador: ING. INGENIERO DE SISTEMAS. MG. COMPUTACIÓN E INFORMÁTICA

1.- **Pertenencia:** El ítem corresponde al concepto teórico formulado.

2.- **Relevancia:** El ítem es el apropiado para representar al componente o dimensión específica del constructo.

3.- **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

**Nota:** Suficiencia. Se dice suficiencia cuando los ítems planeados son suficientes para medir la dimensión.

JUNIOR EUGENIO COCHAY MACO
ING. EN COMPUTACIÓN E INFORMÁTICA
Reg CIP 179375

FIRMA

FICHA DE VALIDEZ DE CONTENIDO QUE MIDE EL MODELO DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADO A NORMA ISO/IEC 27001:2013

| DIMENSIONES / INDICADORES | PERTENENCIA | | RELEVANCIA | | CLARIDAD | |
|---|---|---|---|---|---|---|
| **VALORACION DE ACTIVOS** | SI | NO | SI | NO | SI | NO |
| 1.- Categoria | X | | X | | X | |
| 2.- ID del riesgo | X | | X | | X | |
| 3.-Activo | X | | X | | X | |
| 4.Criterios (Confidencialidad, integridad, disponibilidad) | X | | X | | X | |
| 5.-Impacto | X | | X | | X | |
| **EVALUACION DEL RIESGO (Nivel del riesgo)** | | | | | | |
| 1.- Proceso involucrado | X | | X | | X | |
| 2.- Activo critico de información | X | | X | | X | |
| 3.- ID del riesgo | X | | X | | X | |
| 4.- Amenazas | X | | X | | X | |
| 5.- Vulnerabilidades | X | | X | | X | |
| 6.- Impacto | X | | X | | X | |
| 7.-Probabilidad | X | | X | | X | |
| 8.- Riesgo | X | | X | | X | |
| **TRATAMIENTO DEL RIESGO (Número de controles aplicados)** | | | | | | |
| 1.-Titulo del control | X | | X | | X | |
| 2.-Preguntas | X | | X | | X | |
| 3.-Aplicación | X | | X | | X | |
| 4.-Rango | X | | X | | X | |
| 5.- Comentario | X | | X | | X | |

Observaciones (Precisar si hay suficiencia) Sí hay Suficiencia

Opciones de aplicabilidad: Aplicable (X) Aplicable después de corregir ( ) No aplicable ( )

Apellidos y nombres del juez validador: Santamaría Santamaría Walter DNI: 16655450

Especialidad del validador: Ingeniero de Sistemas.

1.- **Pertenencia**: El ítem corresponde al concepto teórico formulado.

2.- **Relevancia**: El ítem es el apropiado para representar al componente o dimensión específica del constructo.

3.- **Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

**Nota**: Suficiencia. Se dice suficiencia cuando los ítems planeados son suficientes para medir la dimensión.

FIRMA

WALTER ARMANDO SANTAMARÍA SANTAMARÍA
INGENIERO DE SISTEMAS
Reg. CIP. 179422

**FICHA DE VALIDEZ DE CONTENIDO QUE MIDE EL MODELO DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN ALINEADO A NORMA ISO/IEC 27001:2013**

| DIMENSIONES / INDICADORES | PERTENENCIA | | RELEVANCIA | | CLARIDAD | |
|---|---|---|---|---|---|---|
| VALORACION DE ACTIVOS | SI | NO | SI | NO | SI | NO |
| 1.- Categoría | X | | X | | X | |
| 2.- ID del riesgo | X | | X | | X | |
| 3.-Activo | X | | X | | X | |
| 4.Criterios (Confidencialidad, integridad, disponibilidad) | X | | X | | X | |
| 5.-Impacto | X | | X | | X | |
| EVALUACION DEL RIESGO (Nivel del riesgo) | | | | | | |
| 1.- Proceso involucrado | X | | X | | X | |
| 2.- Activo crítico de informacion | X | | X | | X | |
| 3.- ID del riesgo | X | | X | | X | |
| 4.- Amenazas | X | | X | | X | |
| 5.- Vulnerabilidades | X | | X | | X | |
| 6.- Impacto | X | | X | | X | |
| 7.-Probabilidad | X | | X | | X | |
| 8.- Riesgo | X | | X | | X | |
| TRATAMIENTO DEL RIESGO (Número de controles aplicados) | | | | | | |
| 1.-Título del control | X | | X | | X | |
| 2.-Preguntas | X | | X | | X | |
| 3.-Aplicación | X | | X | | X | |
| 4.-Rango | X | | X | | X | |
| 5.- Comentario | X | | X | | X | |

Observaciones (Precisar si hay suficiencia) Si hay suficiencia

Opciones de aplicabilidad: Aplicable (X) Aplicable después de corregir ( ) No aplicable ( )

Apellidos y nombres del juez validador: Rojas Ayde Cala Pilli DNI: 16779254

Especialidad del validador: Ingeniero de Sistemas

1.- **Pertenencia**: El ítem corresponde al concepto teórico formulado.

2.- **Relevancia**: El ítem es el apropiado para representar al componente o dimensión específica del constructo.

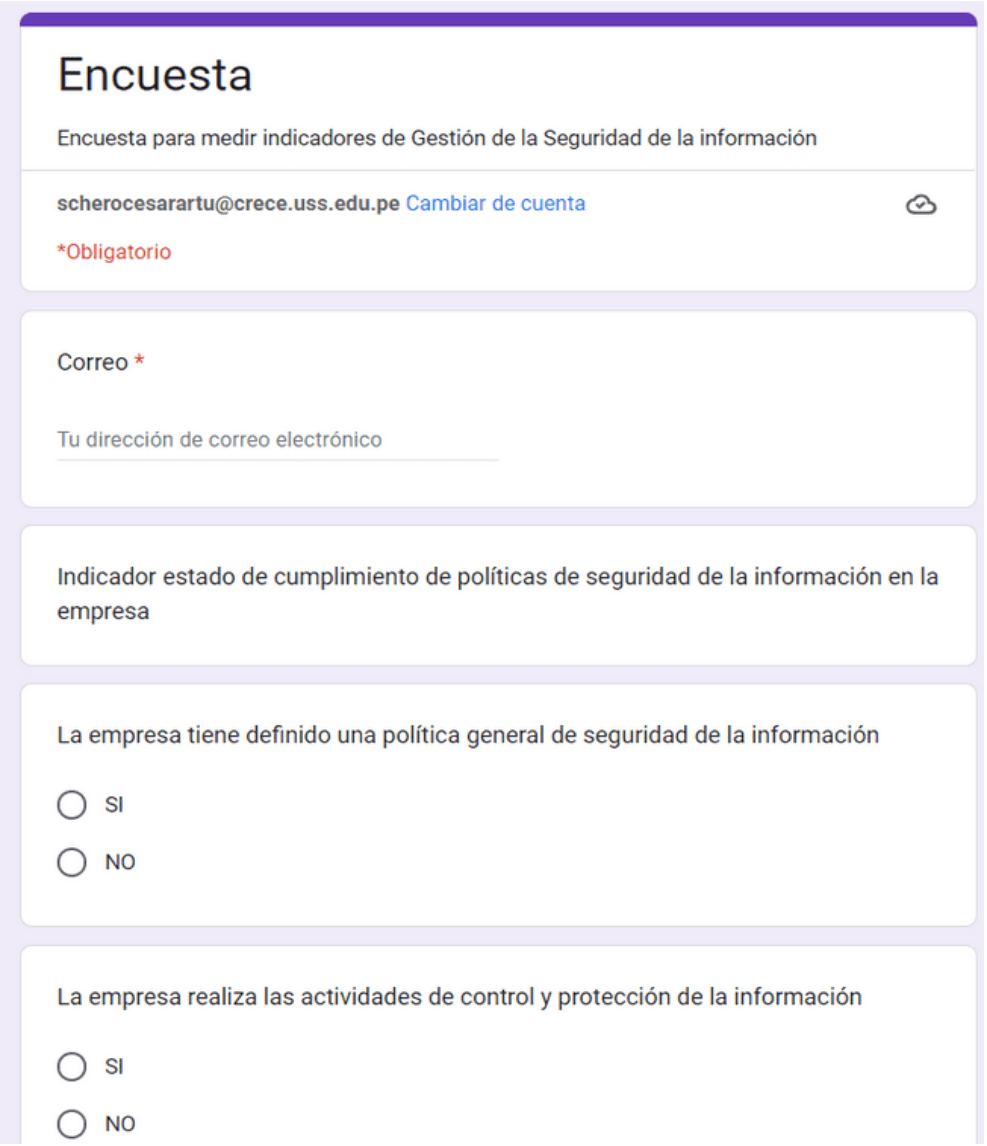
3.- **Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

**Nota**: Suficiencia. Se dice suficiencia cuando los ítems planeados son suficientes para medir la dimensión.

FIRMA

10 de JUN del 20 22

**Encuesta para medir indicadores de gestión de la seguridad de la información**



Encuesta

Encuesta para medir indicadores de Gestión de la Seguridad de la información

scherocesarartu@crece.uss.edu.pe Cambiar de cuenta

*Obligatorio

Correo *

Tu dirección de correo electrónico

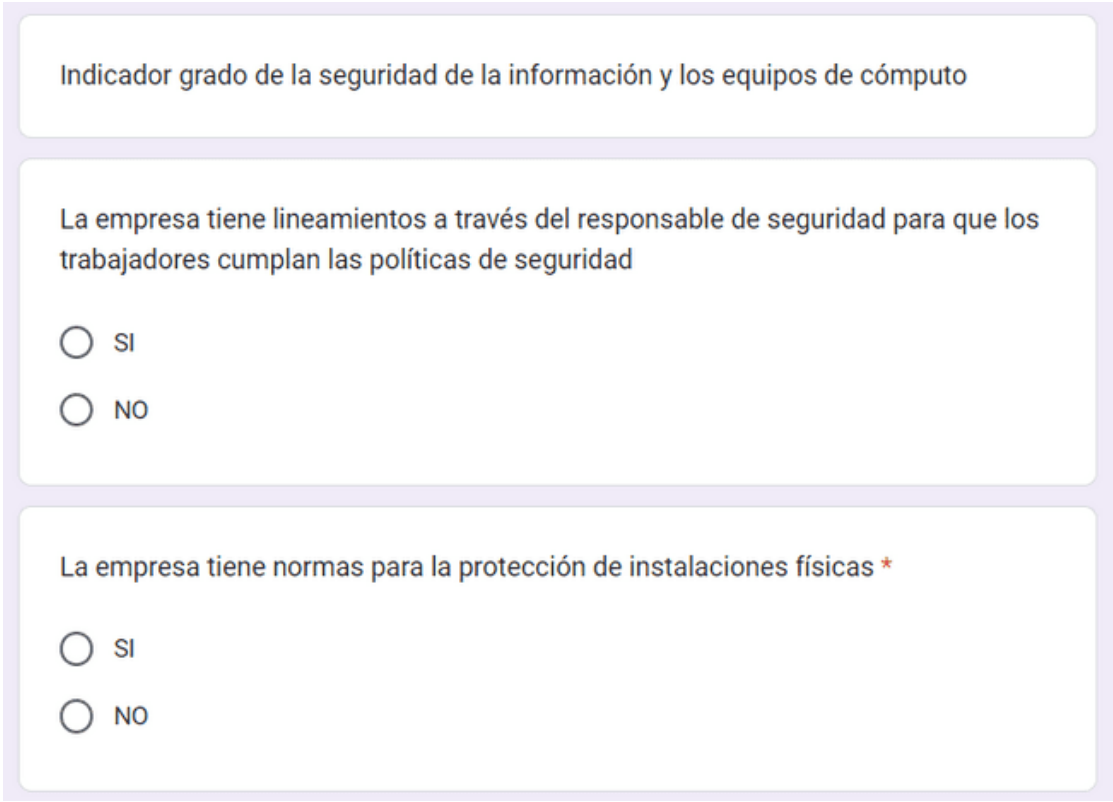
Indicador estado de cumplimiento de políticas de seguridad de la información en la empresa

La empresa tiene definido una política general de seguridad de la información

- SI
- NO

La empresa realiza las actividades de control y protección de la información

- SI
- NO



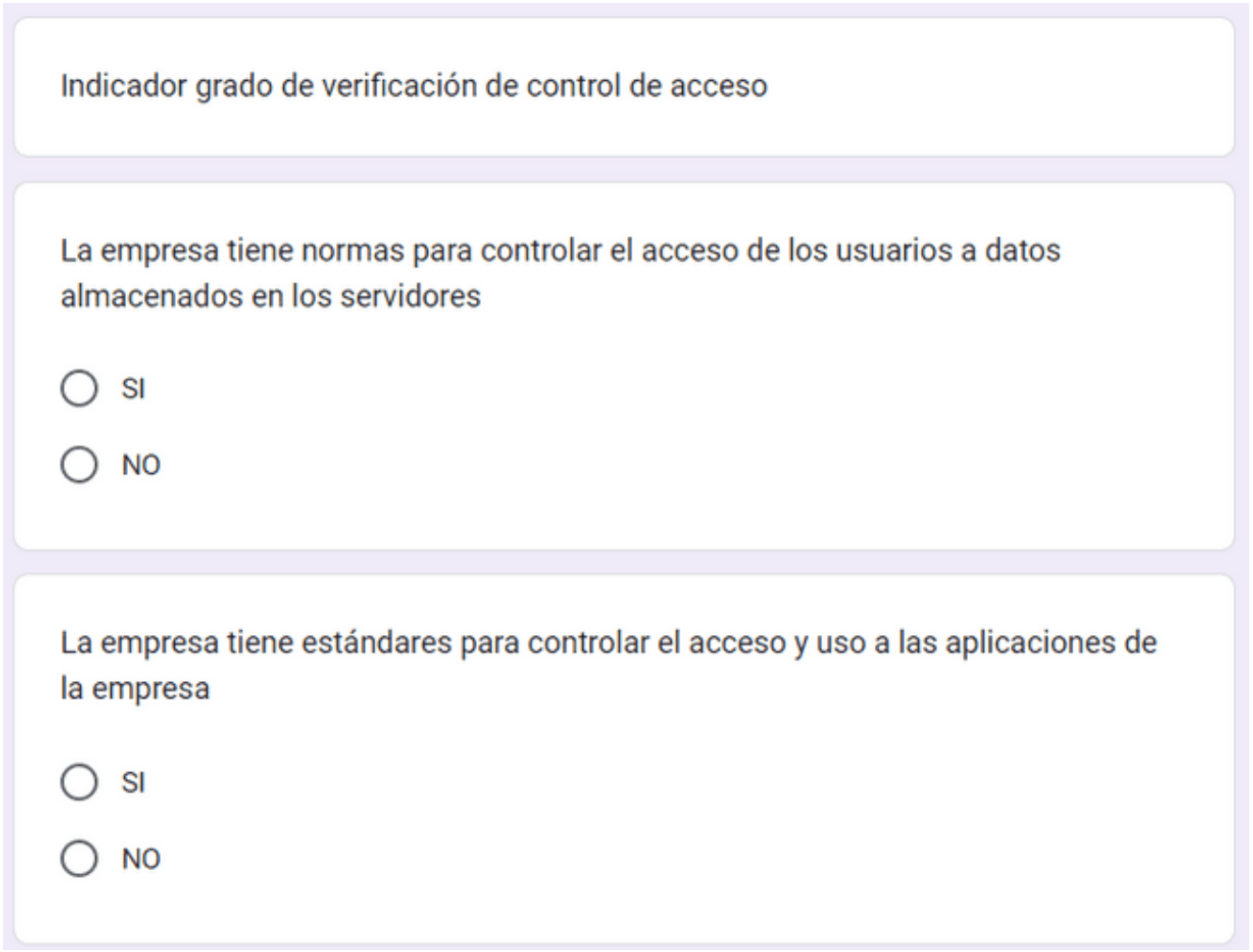
Indicador grado de la seguridad de la información y los equipos de cómputo

La empresa tiene lineamientos a través del responsable de seguridad para que los trabajadores cumplan las políticas de seguridad

- SI
- NO

La empresa tiene normas para la protección de instalaciones físicas *

- SI
- NO




***Fuente:*** (VÁSQUEZ ZEVALLOS & DELGADO SAAVEDRA, 2019)

## ANEXO 5 LISTA DE INVENTARIO DE ACTIVOS DE INFORMACIÓN

| Categoría | ID de Riesgo | Activo | Descripción | Responsable | Ubicación |
|---|---|---|---|---|---|
| DATOS | D-001 | Datos del personal | Información acerca del personal de la empresa como nombres, apellidos, DNI, dirección, correo, cargo, puesto, grado, entre otros. | Consultoría | Servidor Nube |
| | D-002 | Control de salarios | Información de los contratos del personal como la lista de salario | Consultoría | Servidor Nube |
| | D-003 | Datos de los clientes | Información de los contratos de los clientes con el sistema adquirido, Credenciales de acceso. | Consultoría | Microsoft Excel |
| | D-004 | Datos de inventario de equipos | Información acerca del inventario de equipos como laptops, mouses, USB, discos duros, impresoras, mochilas, audífonos entre otros. | Consultoría | Servidor Nube / Ubicación Física |

| | | | | |
|---|---|---|---|---|
| D-005 | Registro de caja chica | Información de los ingresos y gastos de la empresa | Contabilidad | Servidor Nube / Ubicación Física |
| D-006 | Registro de notas de créditos | Información acerca de las facturas anuladas | Contabilidad | Servidor Nube |
| D-007 | Registros de órdenes de compras | Información acerca de las ordenes de compras y facturas de nuestros clientes | Contabilidad | Servidor Nube |
| D-008 | Registro de cuentas por Pagar | Información de los comprobantes que faltan por pagar | Contabilidad | Servidor Nube |
| D-009 | Registro de cuentas por cobrar | Información de los comprobantes que faltan por cobrar | Contabilidad | Servidor Nube |
| D-010 | Reporte de acceso de usuarios Radmin VPN Y ANYDESK | Lista de usuarios de acceso de VNP y Anydesk de los clientes | Consultoría | Microsoft Excel |
| D-011 | Registros de órdenes de ventas | Información acerca de las ventas a los clientes | Contabilidad | Servidor Nube |
| D-012 | BD empresa/ BD clientes | Información acerca de la empresa y de los clientes | Consultoría, desarrollo | Servidor Nube |

| | | | | | |
|---|---|---|---|---|---|
| SERVICIOS | S-001 | Pagos a servicios a terceros | Servicio intermediario OSE (Facturación electrónica) | Contabilidad | Servidor Nube |
| | S-002 | Internet | Servicio contratado al proveedor CLARO | Contabilidad | - |
| | S-003 | Correo electrónico | Correo con dominio institucional @seisystemperu.com, este servicio es externo. | Contabilidad | CPANEL |
| SOFWTARE | SW-001 | Lista de instaladores de Software | Sistemas operativos, programas, office, entre otros | Consultoría | Servidor Nube |
| | SW-002 | Antivirus | Antivirus ESET NOD32 10 unidades licencias | Consultoría | Servidor Nube/Ubicación física |
| | SW-003 | Software “Scan Web” | Software que brinda la empresa a distintos rubros de negocios | Desarrollo | Servidor Nube |

| | | | | | |
|---|---|---|---|---|---|
| HARDWARE | HW-001 | Laptops administrativos | 4 unidades | Consultoría, Contabilidad | Ubicación Física |
| | HW-002 | Laptops gerenciales | 1 unidad | Gerencia | Ubicación Física |
| | HW-003 | Laptop de desarrollo | 2 unidades | Desarrollo de software | Ubicación Física |
| EQUIPAMIENTO AUXILIAR | AUX-001 | Impresora | Impresora EPSON L380 1 unidad | Todos los procesos | Ubicación Física |
| | AUX-002 | UBS | Dispositivo para guardar información | Todos los procesos | Ubicación Física |
| | AUX-003 | Pizarra | Material que usan internamente para presentaciones | Todos los procesos | Ubicación Física |
| | AUX-004 | Proyector | Material que usan internamente para presentaciones | Todos los procesos | Ubicación Física |

| | | | | | |
|---|---|---|---|---|---|
| | AUX-005 | Armarios | Lugar en donde se guardan información confidencialidad de la empresa | Contabilidad | Ubicación Física |
| | AUX-006 | Discos externos | Dispositivo para guardar información | Todos los procesos | Ubicación Física |
| | AUX-007 | Archivadores | Material para separar informaciones depende de su valorización | Contabilidad, consultoría | Ubicación Física |
| MEDIA | MED-001 | Documentación administrativa | Documentos internos en papel como contratos, Guías de pedidos a proveedores, recibos. | Contabilidad / consultoría | Ubicación Física |
| | COM-001 | Red de telefonía fijo | Teléfono fijo de la oficina principal | Todos los procesos | Ubicación Física |
| REDES DE COMUNICACIÓN | COM-002 | Red Inalámbrica | Wifi para oficina | Todos los procesos | Ubicación Física |
| | COM-003 | Telefonía móvil | Celulares que son asignados para proyectos de desarrollo | Desarrollo de software | Ubicación Física |
| INSTALACIÓN | INS-001 | Oficina Alfonso Ugarte | Todos los materiales y equipos que se encuentran en la oficina | Todos los procesos | Ubicación Física |

## ANEXO 6 VALORACIÓN DE ACTIVOS

## FICHA DE OBSERVACIÓN: INDICADOR VALORACIÓN DE ACTIVOS DE LA INFORMACIÓN

| | FICHA DE OBSERVACION N°01: INDICADOR: VALORACIÓN DE ACTIVOS | | |
|---|---|---|---|
| | **FASE:** POST TEST | **CODIGO:** F0-01 | **VERSION:** V1 |
| | **Fecha de recolección:** | 11/06/2022 | |
| | **Investigador:** | SANDOVAL CHERO CESAR ARTURO | |

| Categoría | ID de Riesgo | Activo | Criterios | | | Total | Impacto |
|---|---|---|---|---|---|---|---|
| | | | C | I | D | | |
| DATOS | D-001 | **Datos del personal** | 7 | 7 | 8 | 7 | A |
| | D-002 | **Control de salarios** | 10 | 9 | 9 | 9 | A |
| | D-003 | **Datos de los clientes** | 10 | 7 | 7 | 9 | A |
| | D-004 | Datos de inventario de equipos | 4 | 4 | 4 | 4 | M |
| | D-005 | Registro de caja general | 6 | 6 | 7 | 6 | M |
| | D-006 | Registro de notas de créditos | 6 | 3 | 4 | 4 | M |
| | D-007 | **Registros de órdenes de compras** | 7 | 10 | 8 | 8 | A |
| | D-008 | Registro de cuentas por pagar | 7 | 5 | 7 | 6 | M |
| | D-009 | Registro de cuentas por cobrar | 7 | 5 | 7 | 6 | M |
| | D-010 | **Reporte de acceso de usuarios Radmin VPN Y ANYDESK** | 8 | 9 | 9 | 9 | A |
| | D-011 | **Registros de órdenes de ventas** | 7 | 10 | 8 | 8 | A |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | D-012 | **BD Empresa/ BD Clientes** | 7 | 10 | 9 | 9 | A |
| | S-001 | Pagos a servicios a terceros | 6 | 4 | 5 | 5 | M |
| | S-002 | Internet | 4 | 7 | 9 | 7 | M |
| SERVICIOS | S-003 | Correo electrónico | 7 | 6 | 7 | 7 | M |
| | SW-001 | **Lista de instaladores de Software** | 7 | 9 | 10 | 9 | A |
| SOFTWARE | SW-002 | Antivirus | 6 | 5 | 6 | 5 | M |
| | SW-003 | Software “Scan web” | 9 | 9 | 9 | 9 | A |
| | HW-001 | Laptops administrativos | 6 | 7 | 7 | 7 | M |
| HARDWARE | HW-002 | Laptops gerenciales | 6 | 7 | 7 | 7 | M |
| | HW-003 | **Laptop de desarrollo** | 9 | 9 | 10 | 9 | A |
| | AUX-001 | Impresora | 1 | 2 | 2 | 2 | B |
| | AUX-002 | UBS | 6 | 7 | 6 | 6 | M |
| EQUIPAMIENTO AUXILIAR | AUX-003 | Pizarra | 2 | 1 | 2 | 2 | B |
| | AUX-004 | Proyector | 1 | 2 | 1 | 2 | B |
| | AUX-005 | Armarios | 1 | 2 | 2 | 2 | B |
| | AUX-006 | Discos externos | 6 | 7 | 6 | 6 | M |
| | AUX-007 | Archivadores | 2 | 1 | 3 | 2 | B |
| MEDIA | MED-001 | **Documentación administrativa** | 8 | 9 | 9 | 9 | A |
| | COM-001 | Red de telefonía fijo | 2 | 1 | 4 | 2 | B |
| REDES DE COMUNICACIÓN | COM-002 | Red Inalámbrica | 3 | 7 | 7 | 6 | M |
| | COM-003 | Telefonía móvil | 5 | 5 | 6 | 5 | M |
| INSTALACIÓN | INS-001 | **Oficina Alfonso Ugarte** | 8 | 6 | 9 | 8 | A |

## ANEXO 7 EVALUACIÓN DE RIESGOS
## ANTES DE LA APLICACIÓN DE MEDIDAS DE SEGURIDAD

## FICHA DE OBSERVACION: INDICADOR NIVEL DE RIESGO

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **FICHA DE OBSERVACION N°02: INDICADOR: NIVEL DE RIESGOS** | | | | | | | |
| | **FASE:** POST TEST | | **CODIGO:** F0-01 | | **VERSION:** V1 | | | |
| | **Fecha de recolección:** | | 11/06/2022 | | | | | |
| | **Investigador:** | | SANDOVAL CHERO CESAR ARTURO | | | | | |
| **PROCESO** | **ACTIVO** | **ID DEL RIESGO** | **AMENAZA** | | **OCURRENCIA** | | **RIESGO** | |
| | | | **IMPACTO** | **VALOR** | **PROBABILIDAD** | **VALOR** | **TOTAL** | **ZONA RIESGO** |
| **CONTABILIDAD** | **Datos del personal** | ALT006 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT013 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | MOD002 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | MOD003 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | MOD004 | BAJO | 1 | PROBABLE | 3 | 3 | M |
| | | MOD05 | BAJO | 1 | PROBABLE | 3 | 3 | M |
| | | BAJ001 | MEDIO | 2 | RARO | 1 | 2 | B |
| | **Control de salarios** | EXT014 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT028 | ALTO | 3 | PROBABLE | 3 | 9 | E |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EXT051 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT053 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT007 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT011 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | MOD002 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | MOD008 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | **Registros de órdenes de compras** | ALT002 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT008 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT012 | ALTO | 3 | PROBABLE | 2 | 6 | A |
| | | ALT013 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | **Persona** | EXT002 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT015 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | **Registros de órdenes de Ventas** | ALT002 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT008 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT012 | ALTO | 3 | PROBABLE | 2 | 6 | A |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ALT013 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| **GERENCIA GENERAL** | **Correo electrónico** | ALT015 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT019 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT022 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | **Toda la documentación información** | ALT024 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | **Oficina Alfonso Ugarte** | MOD010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| **CONSULTORIA Y DESARROLLO DE SOFTWARE** | **Datos del cliente** | EXT009 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | **Lista de instaladores** | EXT001 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT001 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT011 | MEDIO | 2 | CASI SEGURO | 4 | 8 | A |
| | **Reporte de acceso de usuarios Radmin VPN Y ANYDESK** | EXT001 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT011 | ALTO | 3 | PROBABLE | 4 | 12 | E |
| | | EXT014 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT017 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT023 | ALTO | 3 | CASI SEGURO | 4 | 12 | E |
| | | EXT024 | ALTO | 3 | CASI SEGURO | 4 | 12 | E |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EXT026 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT048 | ALTO | 3 | CASI SEGURO | 4 | 12 | E |
| | | ALT010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT021 | MEDIO | 2 | CASI SEGURO | 4 | 8 | A |
| | **Persona** | EXT002 | ALTO | 3 | CASI SEGURO | 4 | 12 | E |
| | | EXT015 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | **Laptops de desarrollo** | EXT005 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT014 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT022 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT025 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT027 | ALTO | 3 | CASI SEGURO | 4 | 12 | E |
| | | EXT031 | ALTO | 3 | PROBABLE | 3 | 3 | E |
| | | EXT040 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT052 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT001 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT005 | MEDIO | 2 | CASI SEGURO | 4 | 8 | A |
| | **Software Scan Web** | EXT032 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT049 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | **BD Empresa / BD Clientes** | EXT049 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| **TODOS LOS PROCESOS** | **Oficina Alfonso Ugarte** | EXT003 | ALTO | 3 | PROBABLE | 3 | 6 | A |
| | | EXT050 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT001 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT017 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | MOD007 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |

**FICHA DE OBSERVACION: INDICADOR NIVEL DE RIESGO**

**DESPUES DE LA APLICACIÓN DE MEDIDAS DE SEGURIDAD**

| PROCESO | ACTIVO | ID DEL RIESGO | AMENAZA | | OCURRENCIA | | RIESGO | |
|---|---|---|---|---|---|---|---|---|
| | | | IMPACTO | VALOR | PROBABILIDAD | VALOR | TOTAL | ZONA RIESGO |
| CONTABILIDAD | Datos del personal | ALT006 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | ALT013 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | MOD002 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | MOD003 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | MOD004 | BAJO | 1 | RARO | 1 | 1 | B |
| | | MOD005 | BAJO | 1 | IMPROBABLE | 2 | 2 | B |
| | | BAJ001 | BAJO | 1 | RARO | 1 | 1 | B |
| | Control de salarios | EXT014 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | EXT028 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT051 | ALTO | 3 | IMPROBABLE | 2 | 6 | M |
| | | EXT053 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | ALT007 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ALT011 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | MOD002 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | MOD008 | MEDIO | 2 | RARO | 1 | 2 | B |
| | **Registros de órdenes de compras** | ALT002 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | ALT008 | MEDIO | 2 | IMPROBABLE | 2 | 4 | A |
| | | ALT010 | MEDIO | 2 | IMPROBABLE | 2 | 4 | A |
| | | ALT012 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | ALT013 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | **Persona** | EXT002 | MEDIO | 2 | IMPROBABLE | 2 | 4 | A |
| | | EXT015 | BAJO | 1 | RARO | 1 | 1 | B |
| | **Registros de órdenes de Ventas** | ALT002 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | ALT008 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | ALT010 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | ALT012 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | | ALT013 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | ALT015 | BAJO | 1 | RARO | 1 | 1 | B |
| | | ALT019 | MEDIO | 2 | RARO | 1 | 2 | B |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **GERENCIA GENERAL** | **Correo electrónico** | ALT022 | MEDIO | 2 | RARO | 1 | 2 | B |
| | **Toda la documentación información** | ALT024 | MEDIO | 2 | PROBABLE | 3 | 6 | A |
| | **Oficina Alfonso Ugarte** | MOD010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| **CONSULTORIA Y DESARROLLO DE SOFTWARE** | **Datos del cliente** | EXT009 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | **Lista de instaladores** | EXT001 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | ALT001 | BAJO | 1 | RARO | 1 | 1 | B |
| | | ALT011 | MEDIO | 2 | RARO | 1 | 2 | B |
| | **Reporte de acceso de usuarios Radmin VPN Y ANYDESK** | EXT001 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT011 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | EXT014 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT017 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT023 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | EXT024 | ALTO | 3 | RARO | 1 | 3 | M |
| | | EXT026 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT048 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | ALT010 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ALT021 | MEDIO | 2 | RARO | 1 | 2 | B |
| | **Persona** | EXT002 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT015 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | **Laptops de desarrollo** | EXT005 | ALTO | 3 | IMPROBABLE | 2 | 6 | M |
| | | EXT014 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | EXT022 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT025 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT027 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | EXT031 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | | EXT040 | MEDIO | 2 | RARO | 1 | 2 | B |
| | | EXT052 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT001 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | ALT005 | MEDIO | 2 | IMPROBABLE | 2 | 4 | M |
| | **Software Scan Web** | EXT032 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | EXT049 | MEDIO | 2 | RARO | 1 | 2 | B |
| | **BD Empresa / BD Clientes** | EXT049 | MEDIO | 2 | RARO | 1 | 2 | B |
| **TODOS LOS PROCESOS** | **Oficina Alfonso Ugarte** | EXT003 | ALTO | 3 | PROBABLE | 3 | 6 | A |
| | | EXT050 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT001 | ALTO | 3 | PROBABLE | 3 | 9 | E |
| | | ALT017 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |
| | | MOD007 | ALTO | 3 | IMPROBABLE | 2 | 6 | A |

# ANEXO 8 APLICABILIDAD DE CONTROLES

| ID | Controles según la norma ISO 27001 | Aplicabilidad (SI/NO) | Justificación de elección/no elección |
|---|---|---|---|
| **5.1 Dirección de la gerencia para la seguridad de la información.** | | | |
| A.5.1.1 | Políticas para seguridad de la información. | SI | Es necesario establecer una "Política de Seguridad de Información", ya que es un requisito para establecer el SGSI. Además, sirve como base para el establecimiento del SGSI |
| A.5.1.2 | Revisión de políticas para seguridad de la información. | SI | Es necesario contar con una "Política de Seguridad de Información" que sea revisada y aprobada por la Alta Dirección para asegurar que sea la adecuada para la organización. |
| **6.1 Organización Interna** | | | |
| A.6.1.1 | Roles y responsabilidades sobre seguridad de la información. | SI | En la consultora no cuentan con roles definidos en seguridad de información, es necesario definirlos para tener identificados quienes serán los encargados de las actividades y así evitar sobrecargas de actividades. |
| A.6.1.2 | Segregación de deberes | SI | Es necesario segregar funciones entre los roles de la consultora, de esta manera evitar la sobrecarga de tareas y la ineficiente ejecución de los procesos. |
| A.6.1.3 | Contacto con autoridades | SI | Es necesario que exista un documento de contactos con autoridades en donde se indique cómo y cuándo se debería informar de los incidentes de la seguridad de la Información. |
| A.6.1.4 | Contacto con grupos de interés especial. | SI | Es necesario que exista contactos con grupos de interés especial, foros, asociaciones o entidades que incentiven y apliquen la seguridad de información |
| A.6.1.5 | Seguridad de la información en gestión de proyectos. | SI | La empresa cuenta con una metodología de gestión de proyectos, pero no están alineadas con los objetivos de la seguridad de la información ya que no existe una política de seguridad de información. Es necesario incluir los objetivos de la política de seguridad de Información en el método de la gestión de proyectos. |
| **6.2 Dispositivos móviles y teletrabajo** | | | |
| A.6.2.1 | Política sobre dispositivos móviles. | NO | No aplica |

| | | | |
|---|---|---|---|
| A.6.2.2 | Teletrabajo | SI | La empresa tiene trabajadores que están vía remota. |
| **7.1 Antes de empleo** | | | |
| A.7.1.1 | Investigación de antecedentes. | SI | En el área de Consultoría, y como parte del proceso de selección y reclutamiento no se tiene mapeado los antecedentes penales y policiales de cada uno de los candidatos a un puesto laboral. Es por esa razón que es necesario realizar una búsqueda o investigación más exhaustiva si el puesto laboral tiene mayor rango. |
| A.7.1.2 | Términos y condiciones de empleo. | SI | Como parte de las cláusulas del contrato firmado por los colaboradores no se tiene establecido una de confidencialidad hacia la empresa; tampoco no se establece la confidencialidad respectiva a los datos personales del trabajador; es por ello que es necesario incluir ciertas cláusulas que cumplan con la ley de Protección de datos Personales. |
| **7.2 Durante el empleo** | | | |
| A.7.2.1 | Gestión de responsabilidades. | SI | Es necesario hacer que los colaboradores apliquen la seguridad de información con relación a las políticas y procedimientos de la empresa. |
| A.7.2.2 | Concienciación, educación y capacitación en seguridad de la información. | SI | La empresa no toma en cuenta algunos aspectos de seguridad de información en la cultura organizacional, es por ello que es necesario que todos los colaboradores de la organización deban recibir una adecuada concientización, entrenamiento y actualizaciones regulares en los procesos y políticas organizacionales, como acciones relevantes de su función laboral. |
| A.7.2.3 | Proceso disciplinario. | SI | Es necesario que haya sanciones para aquellos colaboradores que cometan una violación a la seguridad o que hayan incumplido con la política de seguridad de información aprobada. |
| **7.3 Finalización del empleo o cambio en el puesto de trabajo** | | | |
| A.7.3.1 | Terminación o cambio de condiciones del empleo | SI | Una vez que culmine el contrato de un colaborador, las responsabilidades de seguridad de la información y funciones deben seguir vigentes después del término o cambio de empleo. Asimismo, estas responsabilidades deben ser definidas, y comunicas al trabajador o contratista. |
| **8.1 Responsabilidad de los activos** | | | |

| | | | |
|---|---|---|---|
| A.8.1.1 | Inventarios de activos | SI | Es necesario realizar un listado de activos de información en la organización, con el fin de hacer seguimiento y monitorearlos. |
| A.8.1.2 | Propiedad de los activos | SI | Es necesario realizar un listado de activos de información en la organización, con el fin de hacer seguimiento y monitorearlos, asimismo se especifican las propiedades de cada uno. |
| A.8.1.3 | Uso aceptable de los activos | SI | La empresa no cuenta con una regla del correcto uso de activos de información, es por eso que es necesario realizarlo y ser difundido correctamente. |
| A.8.1.4 | Devolución de activos | SI | La empresa no cuenta con un procedimiento de devolución de activos, es por eso que se debe definir en un procedimiento para la devolución de los activos de la organización que están en posesión de algún colaborador cuando termine su contrato. |
| **8.2 Clasificación de la información** | | | |
| A.8.2.1 | Clasificación de la información. | SI | De acuerdo al inventario de activos de información se debe clasificar en términos de su importancia aplicando en los tres criterios de la seguridad de la información. |
| A.8.2.2 | Etiquetado de la información. | SI | No se ha definido un procedimiento para etiquetar o clasificar los activos de información, por eso es necesario identificarlos con etiquetas de nomenclatura y tener una lista maestra para saber que activos de información se tiene por cada área. |
| A.8.2.3 | Manejo de activos. | SI | No se ha definido un procedimiento para etiquetar o clasificar los activos de información, por eso es necesario identificarlos con etiquetas de nomenclatura y tener una lista maestra para saber que activos de información se tiene por cada área y si pertenecen a la empresa o no |
| **8.3 Manipulación de los soportes** | | | |
| A.8.3.1 | Gestión de medios removibles. | SI | El uso de laptop para la realización de los servicios fuera de la oficina central requiere que estos tipos de activos sean protegidos y asegurados. |
| A.8.3.2 | Eliminación de medios | SI | No se cuenta con procedimientos formales para la eliminación segura de elementos o información cuando ya no es necesaria, es por esa razón que se |

| | | | |
|---|---|---|---|
| | | | necesita tener un procedimiento en donde indique si el elemento o información no contiene información confidencial y proceda a ser eliminada |
| A.8.3.3 | Transferencia de medios físicos. | SI | En la empresa todas las laptops son entregadas al personal, pero no se ha tenido un control correcto. Es por eso que es necesario un control de registro de materiales que se haya entregado a cada colaborador y que se comprometa a cuidar y regresarlos cuando no esté en uso. |
| **9.1 Requisitos de la empresa para el control de acceso** | | | |
| A.9.1.1 | Política de control de acceso | SI | No cuentan con políticas actualizadas con respecto al control de acceso, es por eso que es necesario ya que en la empresa se tiene demasiada información de alta importancia. |
| A.9.1.2 | Acceso a redes y a servicios de red. | SI | Debido a que la empresa cuenta con acceso de VPN Y ANYDESK de los clientes a los que se les presta el servicio de software para su negocio, es necesario contar con una política de acceso seguro de VPN Y ANYDESK. |
| **9.2 Gestión de acceso de usuarios** | | | |
| A.9.2.1 | Registración y baja de usuarios | SI | De acuerdo al análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de acceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad. |
| A.9.2.2 | Concesión de acceso de usuarios. | SI | No hay un procedimiento en el que se abastezcan de usuarios de acceso. Solo se cuenta con la plataforma de Google Suite en donde se tiene un control de acceso a los correos institucionales. |
| A.9.2.3 | Gestión de derechos de acceso privilegiado. | SI | Es necesario realizar un procedimiento documentado, en el cual se indique que cada jefe de área, debe solicitar los permisos adecuados para cada colaborador que se le autorice. |
| A.9.2.4 | Gestión de información secreta de autentificación de usuarios. | SI | Es necesario establecer lineamientos para la adecuada gestión de autenticación de usuarios. |
| A.9.2.5 | Revisión de los derechos de acceso del usuario. | SI | De acuerdo con el análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de acceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad. |

| | | | |
|---|---|---|---|
| A.9.2.6 | Eliminación o ajustes de derechos de acceso. | SI | De acuerdo con el análisis de riesgo desarrollado, se ha identificado la ausencia de una matriz de perfiles de acceso actualizada, lo que ha ocasionado a que la información se exponga a varios riesgos de seguridad. |
| **9.3 Responsabilidades del usuario** | | | |
| A.9.3.1 | Uso de información secreta de autenticación. | Si | No hay una cultura de seguridad en los colaboradores de la organización, esto hace que las vulnerabilidades se vean expuestas, es por ello por lo que es necesario que cada trabajador sea responsable de su usuario y contraseña. |
| **9.4 Control de acceso a sistema y aplicación** | | | |
| A.9.4.1 | Restricción al acceso a la información. | SI | No hay una cultura de seguridad para el acceso del código fuente del software que brinda y/o que desarrolla la empresa seisystem |
| A.9.4.2 | Procedimiento de registro en el terminal. | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI. |
| A.9.4.3 | Sistema de gestión de claves | SI | No se cuenta con una gestión de claves para el ingreso al sistema scan web, por lo que hace vulnerable la informacion. |
| A.9.4.4 | Uso de programas de utilidad privilegiada | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI. |
| A.9.4.5 | Control de acceso al código fuente del programa. | SI | No hay una cultura de seguridad para el acceso del código fuente del software que brinda y/o desarrolla la empresa seisystem |
| **10.1 Controles criptográficos** | | | |
| A.10.1.1 | Política del uso de controles criptográficos. | NO | No aplica debido a que por ahora no está tomando en cuenta los controles criptográficos para el alcance del SGSI. |
| A.10.1.2 | Gestión clave. | NO | |
| **11.1 Áreas seguras.** | | | |
| A.11.1.1 | Perímetro de seguridad física. | NO | No aplica debido a que la empresa se encuentra alquilando lugar, por ahora se está trabajando en un edificio de 2do piso. |
| A.11.1.2 | Controles físicos de ingreso | SI | La empresa como encuentra en un edificio de 2do piso, pero como se tiene información valiosa no cuenta con controles de entrada y acceso al personal como cerraduras, alarmas, etc. |
| A.11.1.3 | Seguridad de oficinas, habitaciones e instalaciones. | SI | La empresa se encuentra en un edificio de 2do piso y está separado por áreas, pero no se cuenta con controles de |

| | | | |
|---|---|---|---|
| | | | entrada y acceso al personal como barras, alarmas, cerraduras, etc. |
| A.11.1.4 | Protección contra amenazas externas y ambientales. | SI | No se cuenta con un reglamento o asesoramiento para evitar daños causados por juego, inundación, etc. |
| A.11.1.5 | Trabajo en áreas seguras | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI. |
| A.11.1.6 | Áreas de entrega y carga | NO | |
| **11.2 Seguridad de los equipos** | | | |
| A.11.2.1 | Emplazamiento y protección de los equipos | SI | Los equipos no saben dónde ubicarlo ni cómo protegerlos de los riesgos ambientales por eso es necesario establecer políticas del uso correcto de los equipos. |
| A.11.2.2 | Servicios de suministro | SI | Establecer políticas para definir acuerdos de servicio de soporte a las demás áreas. |
| A.11.2.3 | Seguridad en el cableado | NO | No aplica por que actualmente la empresa las Áreas se conectan por wifi. |
| A.11.2.4 | Mantenimiento de equipo | SI | Es necesario establecer lineamientos para realizar regularmente el mantenimiento de los servidores. |
| A.11.2.5 | Remoción de activos | SI | Los colaboradores se llevan las laptops fuera de las instalaciones de la oficina debido al teletrabajo. |
| A.11.2.6 | Seguridad de equipos y activos fuera de las instalaciones. | SI | No se cuenta con medidas de seguridad de las laptops y materiales entregados fuera de las instalaciones. |
| A.11.2.7 | Disposición o reutilización de equipos. | SI | No existen políticas que especifican que los equipos, información y otras aplicaciones no deben ser retirados fuera de la organización, sin previa autorización y tampoco se cuenta con un procedimiento de copia de seguridad, back up antes de ser reutilizada. |
| A.11.2.8 | Equipo de usuario desatendido | SI | No existe una política de aseguramiento en los equipos desentendido. |
| A.11.2.9 | Política de escritorio limpio y pantalla limpia | SI | Es necesario establecer lineamientos para realizar mantener un escritorio limpio y pantalla limpia. |
| **12.1 Procedimientos y responsabilidades operacionales** | | | |
| A.12.1.1 | Procedimientos documentados de operación. | SI | Establecer lineamientos para garantizar que la información esté disponible. |
| A.12.1.2 | gestión de cambios. | SI | Debido a que no aplicaban la seguridad de información no contaban con procedimiento de gestión de cambios |

| | | | |
|---|---|---|---|
| | | | de incidentes es por eso que es necesario que se tenga una gestión de cambios para identificar y controlar los incidentes |
| A.12.1.3 | gestión de capacidad | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI. |
| A.12.1.4 | Separación de ambientes de desarrollo, prueba y operacionales. | NO | |
| **12.2 Protección contra el software malicioso (malware)** | | | |
| A.12.2.1 | Controles contra software malicioso | SI | No existen políticas de seguridad con respecto al uso de correo electrónico, respecto a páginas de internet de contenido dudoso. |
| **12.3 Copias de la seguridad de la información** | | | |
| A.12.3.1 | Copia de seguridad de la información | SI | Los colaboradores no realizan backup del desarrollo de su trabajo, por eso es necesario establecer políticas de respaldo de información, realización de back up. |
| **12.4 Registro de eventos** | | | |
| A.12.4.1 | Registro de eventos | NO | No se aplica debido a que en la empresa no cuentan con sistemas, está a futuro establecer sistemas para acelerar los procesos internos. |
| A.12.4.2 | Protección de la información del registro. | NO | |
| A.12.4.3 | Registros del administrador y operador. | NO | |
| A.12.4.4 | Sincronización de relojes | NO | |
| **12.5 Control de software operacional** | | | |
| A.12.5.1 | Instalación de software en sistemas operativos. | SI | No se tiene un proceso y/o guía para instalaciones del software que se brinda a los clientes. |
| **12.6 gestión de vulnerabilidad técnica.** | | | |
| A.12.6.1 | gestión de vulnerabilidad técnicas | SI | No cuenta con un inventario de activos en donde indiquen que vulnerabilidades se ha tenido hasta el momento, es por eso que es necesario identificar los riesgos asociados y qué medidas tomar. |
| A.12.6.2 | Restricciones sobre instalación de software | SI | No existen políticas de restricción de software para personal no autorizado, debido a que se le asigna las laptops nuevas, los mismos colaboradores se encargan de crear su usuario (administrador) y ellos lo manejan. |
| **12.7 Consideraciones para la auditoria de los sistemas de información.** | | | |

| | | | |
|---|---|---|---|
| A.12.7.1 | Controles de auditoría sobre los sistemas de información. | SI | No se cuentan con auditorías para ver el cumplimiento de diversos procesos dentro de la empresa. |
| **13.1 gestión de la seguridad de la red** | | | |
| A.13.1.1 | Controles de red | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, a demás en la empresa no se cuentan con sistemas de información y de red. |
| A.13.1.2 | Seguridad de los servicios de red | NO | |
| A.13.1.3 | Segregación en redes | NO | |
| **13.2 Transferencia de información** | | | |
| A.13.2.1 | Procedimientos y políticas sobre transferencia de información. | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, a demás en la empresa no se cuentan con sistemas de información y de red. |
| A.13.2.2 | Acuerdos sobre transferencia de información. | SI | Es necesario establecer acuerdos para el intercambio de información del negocio entre todos de la organización y los terceros. |
| A.13.2.3 | Mensajes electrónicos. | SI | Es necesario establecer políticas sobre la transferencia de información. |
| A.13.2.4 | Acuerdos de confiabilidad o no divulgación. | SI | Existen políticas de confidencialidad de información en la organización por parte de nuestros clientes, pero interno están en proceso. |
| **14.1 Requisitos de seguridad de los sistemas de información** | | | |
| A.14.1.1 | Análisis y especificación de los requerimientos de seguridad de la información | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, a demás en la empresa no se cuentan con sistemas de información. |
| A.14.1.2 | Seguridad de servicios de aplicación en redes públicas. | NO | |
| A.14.1.3 | Protección de transacciones de servicios de aplicaciones. | NO | |
| **14.2 Seguridad en los procesos de desarrollo y soporte** | | | |
| A.14.2.1 | Política de desarrollo | SI | Es necesario establecer metodologías para el desarrollo de software. |
| A.14.2.2 | Procedimiento para control en cambio de sistema | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI |
| A.14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma operativa. | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI |

| | | | |
|---|---|---|---|
| A.14.2.4 | Restricciones sobre los cambios en los paquetes de software.60 | SI | No se cuenta con un versiona miento de paquetes del software que se tiene en la empresa Seisystem |
| A.14.2.5 | Principios de ingeniería para sistema seguro. | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI |
| A.14.2.6 | Ambientes de desarrollo seguro | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI |
| A.14.2.7 | Desarrollo externalizado | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI |
| A.14.2.8 | Prueba de seguridad del sistema | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI |
| A.14.2.9 | Prueba de aceptación del sistema. | SI | Es necesario pasar por pruebas de calidad y pruebas de aceptación al sistema. |
| **14.3 Datos de prueba** | | | |
| A.14.3.1 | Protección de datos de prueba | NO | No aplica |
| **15.1 Seguridad de la información en las relaciones con los proveedores** | | | |
| A.15.1.1 | Política de seguridad de la información para relaciones con proveedores. | SI | Establecer condiciones para el caso de acceso a activos de información mediante el servicio. |
| A.15.1.2 | Tratamiento de la seguridad de contratos con proveedores | SI | Es necesario establecer políticas con los proveedores, llegar a un acuerdo del uso correcto de almacenar, comunicar, tratar, acceder o proporcionar la información brindada y recepcionada. |
| A.15.1.3 | Cadena de suministro de tecnología de información y comunicación | SI | Es necesario que los acuerdos con los proveedores deban incluir requisitos para evitar riesgos de seguridad de la información. |
| **15.2 Gestión de entrega de servicios del proveedor** | | | |
| A.15.2.1 | Monitoreo y revisión de los servicios de proveedores | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI. |
| A.15.2.2 | gestión de cambios en los servicios de proveedores | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI. |
| **16.1 gestión de incidentes de seguridad de la información y mejoras** | | | |
| A.16.1.1 | Responsabilidades y procedimientos | SI | Se requiere identificar responsabilidades y un procedimiento para la gestión de incidentes. |

| | | | |
|---|---|---|---|
| A.16.1.2 | Reporte de eventos en la seguridad de la información | SI | Se debe mantener evidencia de cada incidencia de seguridad, para generar un histórico de eventos o incidentes, que luego se tomará como retroalimentación. Asimismo, se deben mantener procesos actualizados. |
| A.16.1.3 | Reporte de debilidades en la seguridad de la información | SI | Se requieren reportes sobre los incidentes identificados para poder evaluar si es un problema o no. |
| A.16.1.4 | Evaluación y decisión sobre eventos de seguridad de la información. | SI | Establecer pasos a seguir según las decisiones tomadas para la seguridad de la información, para tener una idea clara de qué hacer. |
| A.16.1.5 | Aprendizaje a partir de los incidentes en la seguridad de la información | SI | Es necesario saber a quién comunicar los incidentes de la seguridad de información y dar respuesta al contacto responsable. |
| A.16.1.6 | Recolección de evidencia | SI | Es necesario cuantificar y supervisar los tipos, volúmenes y costos de los incidentes de seguridad de la información para evaluarlos y aprender de estos |
| **17.1 Continuidad de seguridad de la información** | | | |
| A.17.1.1 | Planificación de la continuidad de la seguridad de la información | SI | Es necesario determinar las necesidades de la seguridad de la información. |
| A.17.1.2 | Implementación de la continuidad de la seguridad de la información | SI | Es necesario establecer, documentar, implementar y mantener los procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información. |
| A.17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | SI | Es necesario verificar y revisar la continuidad de la seguridad de la información. |
| **17.2 Redundancias** | | | |
| A.17.2.1 | Disponibilidad de instalaciones de procesamiento de información | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI. |
| **18.1 Cumplimiento con requisitos legales y contractuales** | | | |
| A.18.1.1 | Identificación de legislación y requerimientos contractuales aplicables | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI |

| | | | |
|---|---|---|---|
| A.18.1.2 | Derechos de propiedad intelectual | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, además en la empresa no se cuentan con sistemas de información |
| A.18.1.3 | Protección de registros | SI | Es necesario tener un procedimiento de control documentada para tener registrado y mapeado toda información y así evitar pérdida, alteración, falsificación, entre otros. |
| A.18.1.4 | Privacidad y protección de información personalmente identificable. | SI | Es necesario establecer un acuerdo de confidencialidad sobre la privacidad de las personas y la protección de datos de carácter personal de la organización. |
| A.18.1.5 | Regulación de controles criptográficos. | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, además en la empresa no se cuentan con sistemas de información. |
| **18.2 Revisiones de seguridad de la información** | | | |
| A.18.2.1 | Revisión independiente de la seguridad de la información | SI | Es necesario realizar una revisión periódica de la seguridad de la información. |
| A.18.2.2 | Cumplimiento con las políticas y estándares de seguridad.77 | SI | Es necesario que los encargados de cada área se aseguren que todos los procedimientos de la seguridad se estén cumpliendo tanto políticas y controles, en todo caso aplicar sanciones. |
| A.18.2.3 | Revisión de cumplimiento técnico | NO | No aplica debido a que por ahora no está tomando en cuenta este control para el alcance del SGSI, a demás en la empresa no se cuentan con sistemas de información. |

## ANEXO 9 PLAN DE TRATAMIENTO DE RIESGOS

| Cláusula del control ISO/IEC 27001 | Control ISO/IEC 27001 | Activo | ID del riesgo | Descripción del riesgo | Nivel de riesgo | Estrategia de propuesta | Propietario de riesgo | Plan de acción | Responsable de control | Grupo |
|---|---|---|---|---|---|---|---|---|---|---|
| 6. Organización de la seguridad de la información. | 6.1.1 | Control de salarios | EXT001 | Descuido del responsable de no actualizar los datos y/o error al ingresar los datos correspondientes:<br>-Errores en las boletas de pagos o en el costeo de recursos en los proyectos.<br>-Equivocación o pérdida de tiempo al ejecutar los procedimientos de os procesos internos.<br>-Pérdida de oportunidades de negocio.<br>-Estimaciones de proyectos incorrectos. | EXTREMA | REDUCIR | Contabilidad | **1.Memorandum (llamada de atención)**<br>Documentación en el cual se comunicará al personal de la actualización obligatoria de su información, así mismo este documento servirá como una llamada de atención al personal que infringe este control.<br>**2.Aviso vía correo de actualización de información**<br>Enviar un correo masivo indicado o haciendo recordar que deben actualizar su información, es decir subirla a la carpeta drive compartida de su área correspondiente. Además, recordarles deben hacer copias de respaldo a los equipos.<br>**3.Ficha de puestos** | Gerente | 1 |
| | | Reporte de acceso de usuarios Radmin VPN Y ANYDESK | | | | | Encargado de consultoría y desarrollo | | Gerente | |
| | | Lista de instaladores de software | | | | | Encargado de soporte y | | Encargado de área corr | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | -Accesos no autorizados a los sistemas externos de los clientes.<br>-Retrasos en los proyectos al no encontrar el software requerido o no estar con la versión reciente.- Retrasos en el desarrollo de los proyectos debido a la falta actualización de los manuales de procedimientos, técnicas. | | | manten imiento | Buscar a personas con conocimiento en seguridad de la información en caso de que no segregar la tarea de registrar, actualizar y evitar el mal uso de activos. | espo ndie nte | |
| | 6.1 .2 | Persona | EXT0 02 | Los encargados de áreas no supervisan a su personal con respecto a los accesos de usuarios ocasionando alteración o modifican de datos. | EXTR EMA | RED UCIR | Todo el person al | **1.Organigrama de puestos.**<br>Identificar cuáles son los responsables de cada área para segregar tareas para evitar el uso incorrecto de los activos. | Enca rgad o del área corr espo ndie nte | 1 |
| | 6.1 .3 | Oficina Alfonso Ugarte | EXT0 03 | Posible accidente que se producen sin la intervención humana como incendios en las instalaciones, además accidentes como desastres naturales (terremotos, sismos, tsunami, entre otros) | EXTR EMA | TRA NSFE RIR | Encarga do de logístic a | **1.Proveedores de instalación de medidas de seguridad para oficinas.**<br>Contar con una empresa externa que se encargue en la protección de incendios y además de asesoramiento al personal para que pueda desenvolverse adecuadamente ante un aviso de incendio. | Gere nte | 2 |
| | | | EXT0 04 | Además, no cuentan con proveedores en donde haya intercambio de información | EXTR EMA | TRA NSFE RIR | Encarga do | **2.Empresas aseguradoras contra desastres naturales y no naturales (incendios, inundaciones, cortocircuitos, entre otros)** | Gere nte | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | para mejorar los asuntos de la seguridad de la información. | | | | Contar con una empresa aseguradora que permita proteger el negocio contra incendios, terremotos, actos de terrorismo, huelgas, inundaciones, cortocircuitos, entre otros.<br>**3.Lista de contacto de autoridades**<br>Lista en la cual se encuentran las autoridades pertinentes a contactar de presentarse un incidente mayor. | | |
| | 6.2.2 | Laptops De desarrollo | EXT005 | Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas, ocasionando fuga de información. | EXTREMA | REDUCIR | Encargado | **1.Politica de teletrabajo y penalidades**<br>Política para los colaboradores que trabajan en remoto o cuando se llevan las laptops para realizar actividades desde a fuera de la oficina.<br>**2.Formato de entrega de equipos.**<br>Formato en donde indique el nombre del personal, las especificaciones del equipo asignado, las normativas del uso correcto, especificaciones del estado del equipo, otros accesorios y cuando se entregó el equipo. | Gerente | 1 |
| | | | EXT006 | Alteración intencionada del funcionamiento de sistemas de los clientes, persiguiendo un beneficio indirecto. | EXTREMA | REDUCIR | Encargado de servicios | | Gerente | |
| | | | EXT007 | La sustentación de equipamiento provoca directamente la carencia de un medio para prestar los servicios, ocasionando una fuga de información. | EXTREMA | REDUCIR | Encargado de servicios | | Gerente | |
| | | | EXT008 | Víctimas de vandalismo, terrorismo que haga perder la información llevada en el activo. | EXTREMA | TRANSFERIR | Encargado de | **3.Contratar una empresa aseguradora (póliza de equipos)** | Gerente | 2 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | servicios | Contar con una empresa aseguradora que permita proteger los equipos electrónicos (computadoras, laptops, etc) contra robos, vandalismo o daños internos. | | |
| 7. Seguridad de los recursos humanos | 7.1.2 | Datos de los clientes | EXT009 | Fuga de información (accidental o intencional) ocasionando pérdida de clientes y problemas financieros. | EXTREMA | RED UCIR | Contabilidad | **1.El acuerdo de confidencialidad de la seguridad de la información** Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados. **2.Politica de uso, manejo de información confidencial y perdida de información SEISYSTEM** Definir los estándares para salvaguardar la información contra uso no autorizado, divulgación o revelación. **3.Agregar investigación de antecedentes al proceso de contratación del personal** En el procedimiento de contratación debe señalar en que momento, quien y como se pedirán o realizan las investigaciones de antecedentes penales de los futuros colaboradores debido a que se asignara información clasificada de confidencial | Gerente | 1 |
| | | Documentación administrativa | EXT010 | | | | Contabilidad | | Encargado del área correspondiente | |
| | | Reporte de acceso de usuarios Radmin VNP/Anydesk | EXT011 | Divulgar los accesos de usuarios Radmin VNP/Anydesk ocasionaría desconfianza de nuestros clientes al momento de utilizar sus sistemas y proceder con multas penales. | EXTREMA | RED UCIR | Encargado | | Oficina de consultoría | |
| | | Documentación administrativa | EXT012 | Divulgar la documentación técnica afectaría solución estratégica de nuestros servicios siendo una gran desventaja frente a nuestros competidores | EXTREMA | RED UCIR | Contabilidad | | Gerente | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 7.2.1 | Persona | EXT013 | No se cuentan con acuerdos con los colaboradores, proveedores y terceros ocasionando un daño considerable a la organización. | EXTREMA | REDURCIR | Todos los encargados | **1.El acuerdo de confiabilidad de la seguridad de la información**<br>Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados.<br>**2.Politica de proveedores**<br>Política basada en establecer condiciones necesarias en caso de acceso a la información de la empresa por proveedores | Encargado del área correspondiente | 1 |
| | 7.2.2 | Control de salarios | EXT014 | Debido a que en la consultora no cuentan con una política o capacitación sobre la seguridad de la información sucede las siguientes incidencias:<br>-Perdida de la información (accidental o intencional) tanto física y/o digital<br>-Acceso de usuarios no autorizados en el control de salarios, formatos de gestión de oportunidades, propuestas para fines propios.<br>-Alteración en la gestión de oportunidades, en los usuarios Radmin VPN Y ANYDESK, en el versionamiento, en los sistemas | EXTREMA | REDUCIR | Consultoría y desarrollo | **1.Plan de capacitación y concientización.**<br>Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito de la seguridad de la información, además de ayudarles a identificar incidencias, explicación de los controles de seguridad que se implementaran en otros | Gerente | 1 |
| | | Reporte de acceso de usuarios VNP Y ANYDESK | | | | | Consultoría y desarrollo | | Oficina de área de sistemas | |
| | | Laptos de desarrollo | | | | | Consultoría y desarrollo | | Gerente | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | de los clientes, ocasionando perdida en la cartera de clientes perjuicio. | | | | | | |
| | 7.2.3 | Persona | EXT015 | No contaban con la clasificación de sanciones de acuerdo a la falta ocasionando perdida de toma de decisiones | EXTREMA | REDUCIR | Todos los encargados | **1.Memorandum (llamada de atención)** Documento en el cual se comunicará al personal la actualización obligatoria de su información, así mismo este documento servirá como una llamada de atención a aquella personal que infringe este control. **2.Tipos de sanciones de acuerdo a la seguridad de la información** Contar con sanciones que infringen la seguridad de la información de la empresa si tomar decisiones correctas al momento de aplicarlas. | Gerente | 1 |
| | 7.3.1 | Reporte de acceso de usuarios VNP Y Anydesk | EXT016 | Descuido del responsable de no realizar en constante actualización el acceso de usuarios VNP de los clientes | EXTREMA | REDUCIR | Consultoría y desarrollo | **1.El acuerdo de confidencialidad de la seguridad de la información** Indica el uso correcto de los usuarios de VPN Y ANYDESK y que sanciones aquel personal que infringe este acuerdo **2.Comunicado de terminación y cambio de empleo** Comunicar a todo el personal tanto a gerentes y colaboradores la terminación de un contrato de un personal para que estén informados y actualizados | Oficina de área de sistema | 1 |
| | | | EXT017 | Tener acceso al reporte de acceso de usuarios Radmin VNP/ANYDESK, puede ocasionar figas de información, robo de información, fraudes | EXTREMA | REDUCIR | Consultoría y desarrollo | | Oficina de área de | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | sistema | |
| 8. Gestión de activos | 8.1.4 | Laptops de desarrollo | EXT0018 | Carencia de recursos de equipos provoca carga de trabajo o prestación de servicios ocasionando atrasos en los proyectos<br>Carencia del procedimiento de desvinculación del personal ocasionando pérdida de recursos o demora en la entrega de material a los nuevos colaboradores | EXTREMA | REDUCIR | Consultoría y desarrollo | **<u>1.Formato de entrega de equipo</u>**<br>Formato en donde indique el nombre del personal, las especificaciones del equipo asignado, las normativas del uso correcto. Especificaciones del estado del equipo, otros accesorios y cuando se entregó el equipo.<br>**<u>2.Agregar el procedimiento de entrega de activos en el proceso de desvinculación del personal</u>**<br>En el proceso de desvinculación del personal se debe agregar el procedimiento en donde el personal debe retomar todos los activos de la consultora ya sea por contrato o acuerdo. | Gerente | 1 |
| | 8.2.1 | Todos los activos mencionados | EXT019 | Al no tener clasificada los activos de información, la empresa no sabe que activos son más relevantes de riesgos y cuales no ocasionando inseguridad en sus activos | EXTREMA | REDUCIR | Todos los encargados | **<u>1.Clasificacion y valoración de activos de información</u>**<br>Se debe valorizar los activos de acuerdo a los tres criterios: confidencialidad, integridad y disponibilidad, además la clasificación y valorización se debe actualizar cuando cambie su valor a lo largo de su ciclo de vida. | Encargado de la seguridad de la información | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 8.2.2 | | EXT020 | No cuentan con etiquetado de información que sus activos, es decir que no identifican que activo debe ser desarrollado e implementado. | EXTREMA | REDUCIR | Todos los encargados | **1.Procedimiento de control de información documentada**<br>Tiene como objetivo describir las actividades para establecer, documentar, controlar y mantener los documentos (procedimiento, formatos, registros, etc) de acuerdo con los requisitos establecidos por la organización.<br>**2.- Aplicación de metodologías en los procesos de desarrollo**<br>Seleccionar metodologías para el desarrollo de software en la empresa seisystem consultores | Encargado de la seguridad de la información | |
| | 8.2.3 | | EXT021 | No cuentan con procedimientos de desarrollo e implementación de activos | EXTREMA | REDUCIR | Todos los encargados | | | |
| | 8.3.1 | Laptops de desarrollo | EXT022 | Por el debido uso de laptop para la realización de los servicios fuera de la oficina pueden ser víctimas de vandalismo, terrorismo que haga perder la información llevada en el activo | EXTREMA | REDUCIR | Encargado del area de desarrollo | **1.Soporte técnico interno para el mantenimiento preventivo y correctivo de los equipos**<br>Realizar periódicamente mantenimiento, diagnóstico y reparación a los equipos informáticos (laptops, impresoras, monitores, cargadores, entre otros)<br>**2.Inventario de equipos**<br>**En el inventario** se encuentra la lista de los equipos, su estado, responsable, etc | Encargado del área correspondiente | 1 |
| 9. Control de acceso | 9.1.1 | Control de salarios | EXT023 | Carencia de una política de control de acceso ocasionando perdida de información confidencial, discriminación de cartera de clientes, fuga de talentos, desconfianza en los clientes | EXTREMA | REDUCIR | Contabilidad | **2.Politica de control de acceso**<br>Contar con una política en donde indique cuales son los responsables que deben tener acceso a las carpetas de drive y que información pueden acceder.<br>**1.Plan de capacitación y concientización** | Gerente | 1 |
| | | Reporte de acceso de | | | | | Encargado de gestión de | | Consultoría | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | usuarios VNP<br><br>Documentación administrativa | | | | | proyectos<br><br>contabilidad | Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito de la seguridad de la información, además de ayudarles e identificar incidencias, explicación de los controles de seguridad que se implementaran, entre otros.<br>**3.Arbol de carpeta para el acceso a usuarios**<br>Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas. | <br><br>Gerente | |
| | 9.1.2 | Reporte de acceso de usuarios Radmin VPN/anydesk | EXT024 | Acceso no autorizado al reporte de acceso de usuarios Radmin VPN / Anydesk, pueden ocasionar fugas de información, fraudes hacia nuestros clientes, entre otros | EXTREMA | REDUCIR | Encargado de gestión de proyectos | **1.Tipos de sanciones de acuerdo a la seguridad de la información**<br>Contar con sanciones que infringe la seguridad de la información de la empresa y así tomar decisiones correctas al momento de aplicarlas | Consultoría | 1 |
| 9.-Control de accesos | 9.2.1 | Laptops de desarrollo | EXT025 | Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas, alteración o fuga de información. | EXTREMA | REDUCIR | Encargado | **1.Arbol de carpeta para el acceso a usuarios**<br>Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas | Gerente | 1 |
| | 9.2.2 | Reporte de acceso | EXT026 | Divulgar los accesos de usuarios Radmin VPN Y ANYDESK ocasionaría desconfianza de | EXTREMA | REDUCIR | Encargado | **1.El acuerdo de confidencialidad de la seguridad de la información** | consultoría | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | de usuarios VNP | | nuestros clientes al momento de utilizar sus sistemas | | | | Indica el uso correcto de los usuarios de VPN Y ANYDESK y que sanciones aquel personal que infringe este acuerdo. | | |
| | 9.2.4 | Laptops de desarrollo | EXT027 | Alteración intencionada del funcionamiento de sistemas de los clientes, persiguiendo un beneficio indirecto | EXTREMO | REDUCIR | Encargado | **1.El acuerdo de confiabilidad de la seguridad de la información**<br>Cláusula que señale la firma de compromiso de mantener la confiabilidad de la información brindada en forma secreta para la autenticación personal<br>**2.Politica de seguridad de pantallas, escritorios limpios y contraseñas seguridad**<br>Política del correcto uso de equipos con respecto a la seguridad de la información como salva pantallas, escritorios limpios, contraseñas seguras | Gerente | 1 |
| | 9.2.5 | Todos los activos mencionados | EXT028 | No cuentan con un directorio de acceso en donde indica quienes son los usuarios que tienen acceso a tal carpeta, lo que ocasiona perdida de información confidencial | EXTREMA | REDUCIR | Todos los encargados | **1.Arbol de carpeta para el acceso a usuarios**<br>Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas<br>**2.Aviso vía correo de actualización de información**<br>Enviar un correo masivo indicando o haciendo recordar que deben actualizar su información, es decir subirla a la carpeta drive compartida de su área correspondiente. Además, recordarles que deben hacer copias de respaldo a los equipos | Encargado de la seguridad de la información | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 9.2.5 | Todos los activos mencionados | EXT028 | No cuentan con un directorio de acceso en donde indica quienes son los usuarios que tienen acceso a tal carpeta, lo que ocasiona perdida de información confidencial | EXTREMA | REDUCIR | Todos los cargos | **1.Arbol de carpeta para el acceso a usuarios** Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas. **2.Politica de seguridad de pantallas, escritorios limpios y contraseñas seguridad** Política del correcto uso de equipos con respecto a la seguridad de la información como salva pantallas, escritorios limpios, contraseñas seguras | Gerente | 1 |
| | 9.2.6 | | EXT029 | No cuentan con un proceso en que indiquen que los trabajadores que no pertenecen a la empresa hayan dejado accesos o se haya desvinculad de las credenciales de usuarios. Esto ha ocasionado pérdida de información. | EXTREMA | REDUCIR | Todos los cargos | **1.Arbol de carpeta para el acceso a usuarios** Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas. **2.Politica de seguridad de pantallas, escritorios limpios y contraseñas seguridad** Política del correcto uso de equipos con respecto a la seguridad de la información como salva pantallas, escritorios limpios, contraseñas seguras | Gerente | 1 |
| | 9.3.1 | | EXT030 | Toda la información es visible para todos, el uso de contraseñas es muy baja causando divulgación entre los colaboradores. | EXTREMA | REDUCIR | Todos los cargados | **1.El acuerdo de confidencialidad de la seguridad de la información** Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados. | Gerente | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | **2.Politica de uso, manejo de información confidencial y perdida de información SEISYSTEM**<br>Definir los estándares para salvaguardar la información contra uso no autorizado, divulgación o revelación | | |
| 9. Control de acceso a sistema y aplicación | 9.4.1 | Laptop de desarrollo | EXT031 | | EXTREMA | REDUCIR | DESARROLO | **1.El acuerdo de confidencialidad de la seguridad de la información**<br>Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados. | GERENTE | 1 |
| | 9.4.3<br>9.4.5 | Software Scan Web | EXT032 | | | | | | | |
| 11.Seguridad física y ambiental | | Laptops de desarrollo | | . Los equipos no cuentan con mantenimiento<br><br>. Suciedad en los equipos debido al más uso por parte de los colaboradores ocasionando retrasos en el trabajo<br>. La mayoría de los colaboradores dejan sus laptops se manera visible sin suspenderlo lo que ocasionaría pérdida de información | EXTREMA | REDUCIR | Todos los cargados | **1.Formato de entrega de equipos.**<br>Formato en donde indique el nombre del personal, las especificaciones del equipo asignado, las normativas del uso correcto, especificaciones del estado del equipo, otros accesorios y cuando se entregó el equipo.<br>**2.Politica de seguridad de pantallas, escritorios limpios y contraseñas seguridad**<br>Política del correcto uso de equipos con respecto a la seguridad de la información como salva pantallas | | 1 |
| | 11.2.1 | | EXT033 | | | | | | | |
| | 11.2.4 | | EXT034 | | | | | | | |
| | 11.2.4 | | EXT035 | | | | | | | |
| | 11.2.5 | | EXT036 | | | | | | | |
| | 11.2.6 | | EXT037 | | | | | | | |
| | 11.2.7 | | EXT038 | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 11.2.8 | | EXT039 | | | | | | | |
| | 11.2.9 | | EXT040 | | | | | | | |
| | 11.1.4 | Oficina Alfonso Ugarte | EXT041 | Posible accidente que se producen sin la intervención humana como incendios en las instalaciones, accidentes como desastres naturales (sismos, terremotos, etc) | EXTREMA | TRASNFERIR | GERENTE | **1.- Empresas aseguradoras contra desastres naturales y no naturales (incendios, inundaciones, cortocircuito, entre otros)** Contar con una empresa aseguradora que permita proteger el negocio contra incendios, terremotos, entre otros. | GERENTE GENERAL | 2 |
| 12. Seguridad de operaciones | 12.1.1 | Laptops de desarrollo | EXT042 | No realizan copias de respaldos ni mantenimiento de equipos causando problemas al querer buscar información. | EXTREMA | REDUCIR | TODOS LOS ENCARGADOS | **1.- Gestión de cambio** Contar con una gestión de cambio para que ayude a la organización a adaptar exitosamente nuevas formas o tecnologías de hacer negocio y mejorar procesos internos **2.- Control de software's instalados** Tener un control de los software's autorizados para evitar daños en los equipos y fugas o perdidas de información | GERENTE GENERAL | 2 |
| | 12.1.2 | | EXT043 | No cuentan con una gestión de cambio en los procesos internos y de negocio de la empresa, ocasionando desconocimiento del personal y eventos imprevistos. | | REDUCIR | | | | 2 |
| | 12.2.1 12.5.1 | | EXT044 | No cuentan con un control de los software's instalados debido a que el mismo personal instala, dándoles algunos errores. | | REDUCIR | | | | |
| | 12.3.1 | | EXT045 | No cuentan con una gestión de vulnerabilidad debido a que no contaban con un inventario de activos por el cual no evaluaban | | | | | | 1 |
| | 12.6.1 | | EXT046 | | | | | | | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 12.6.2 | | EXT047 | para ver las vulnerabilidades, causando amenazas y riesgos. | | | | | | |
| 13. Seguridad de las comunicaciones | 13.2.2<br>14.2.4 | Reporte de acceso de los usuarios Radmin VPN Y ANYDESK | EXT048 | Fuga de información (accidental o intencional) ocasionando pérdida de clientes y problemas financieros | EXTREMA | REDUCIR | CONTABILIDAD | **1.El acuerdo de confidencialidad de la seguridad de la información**<br>Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados. | GERENTE | 1 |
| 14. Seguridad n en los procesos de desarrollo y soporte | 14.2.1<br>14.2.4<br>14.2.9 | Software scan web<br>BD Empresa / BD clientes | EXT049 | Fuga de información ocasionando pérdida de reputación a la empresa | EXTREMO | REDUCIR | DESARROLLO | **1.El acuerdo de confidencialidad de la seguridad de la información**<br>Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados.<br>**2.- Manuales, procedimientos y configuraciones**<br>Contar con manuales de usuario para los softwares utilizados.<br>**Respaldos de BD / BD Clientes**<br>Realizar respaldos de BD tanto de la empresa, como las BD de los clientes a los que se les brinda servicio | GERENTE | 1 |
| 15. Relacion | 15.1.1 | Documentos | EXT050 | Fuga de información al no tener identificado y documentado los | EXTREMA | REDUCIR | | **1.El acuerdo de confidencialidad de la seguridad de la información** | | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| es con los proveedores | 15.1.2<br>15.1.3 | administrativos | | tipos de proveedor que puedan acceder a nuestra información | | | CONTABILIDAD | Indica el uso correcto de la información de la empresa brindada y recibida por ambas partes para cumplir con los requisitos de la seguridad de la información. | GERENTE | |
| 16. Gestión de incidentes de la seguridad de la información | 16.1.1<br>16.1.2<br>16.1.3<br>16.1.4<br>16.1.5<br>16.1.6<br>16.1.7 | Todos los activos mencionados | EXT051 | Carencia de identificación de responsables y procedimientos de la gestión de incidentes. Inexistente evidencia de históricos de incidentes | EXTREMA | REDUCIR | TODO EL PERSONAL | **<u>1.-Procedimiento de gestión de incidentes</u>**<br>Este procedimiento tiene como objetivo la gestión adecuada de los incidentes reportados. Es decir, identificarlos, evaluarlos, ejecutar acciones para corregirlos y mantener un informe de estos para futuras revisiones | GERENTE GENERAL | 1 |
| 17. Aspectos de seguridad de la información en la gestión | 17.1.1<br>17.1.2<br>17.1.3 | Laptops de desarrollo<br>Oficina de | EXT052 | Incidentes que se producen sin intervención humana tales como: incendios, inundaciones, entre otros | EXTREMA | TRANSFERIR | TODO EL PERSONAL | **<u>1.- Empresas aseguradoras contra desastres naturales y no naturales (incendios, inundaciones, cortocircuito, entre otros)</u>**<br>Contar con una empresa aseguradora que permita proteger el negocio contra incendios, terremotos, entre otros.<br>**<u>2.-Plan de continuidad de la seguridad de la información</u>** | GERENTE GENERAL | 2 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| de continuidad del negocio | | Alfonso Ugarte BD | | | | | | Tiene como objetivo preservar la seguridad de información en la empresa ante situaciones adversas. | | |
| 18. Cumplimiento | 18.1.3 | Reporte de acceso de usuarios<br>Control de salarios | EXT053 | Pérdida de información, es decir no contar con backup.<br>Acceso de usuarios no autorizados para beneficio propio o fines maliciosos | EXTREMA | REDUCIR | GERENTE | **1.Procedimiento de control de información documentada**<br>Tiene como objetivo describir las actividades para establecer, documentar, controlar y mantener los documentos (procedimiento, formatos, registros, etc) de acuerdo con los requisitos establecidos por la organización. | GERENTE | 1 |
| 6. Organización de la seguridad de la información | 6.1.3 | Lista de instaladores de software<br>Laptops de desarrollo | ALT001 | Averías debido al fallo de equipos de clientes y/o de la misma empresa que dejan al área de soporte.<br>Desactualizaciones de los instaladores de programas ocasionando retraso en el tema de entrega de equipos.<br>Posible incidente que se producen sin la intervención humana como inundaciones, cortocircuito, etc. | ALTA | REDUCIR | GERENTE | **1.- Actualizaciones de los drivers o instaladores**<br>Cronograma de actualizaciones de drivers o instaladores de los programas que son necesarios para el desarrollo de proyectos | GERENTE | 2 |
| | | Oficina Alfonso Ugarte | | | | TRANSFERIR | GERENTE | **2.- Empresas aseguradoras contra desastres naturales y no naturales (incendios, cortocircuito, entre otros)**<br>Contar con una empresa aseguradora que permita proteger el negocio contra incendios, inundaciones, cortocircuitos, entre otros | GERENTE | 2 |
| | 6.2.2 | Registro de órdenes | ALT002 | Fuga de información (accidental o intencional) puede causar | ALTA | REDUCIR | Contabilidad | **1.El acuerdo de confiabilidad de la seguridad de la información** | GERENTE | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | de compras Registro de órdenes de ventas | | problemas financieros y desconfianza en los clientes | | | | Cláusula que señale la firma de compromiso de mantener la confiabilidad de la información brindada en forma secreta para la autenticación personal<br>**2.Politica de seguridad de pantallas, escritorios limpios y contraseñas seguridad**<br>Política del correcto uso de equipos con respecto a la seguridad de la información como salva pantallas, escritorios limpios, contraseñas seguras | | |
| | | Correo electrónico | | | | | consultoría | | | |
| | 6.2.2 | Laptop de desarrollo | ALT003 | Descuido del trabajador en tener en malas condiciones el equipo. | ALTA | RED UCIR | Conultoría | **1.El acuerdo de confidencialidad de la seguridad de la información**<br>Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados.<br>**2.Politica de uso, manejo de información confidencial y perdida de información SEISYSTEM**<br>Definir los estándares para salvaguardar la información contra uso no autorizado, divulgación o revelación.<br>**3.Agregar investigación de antecedentes al proceso de contratación del personal**<br>En el procedimiento de contratación debe señalar en que momento, quien y como se pedirán o realizan las investigaciones de | GERENTE | 1 |
| | | | ALT004 | Uso no previsto para intereses personales como juegos, afectando la disponibilidad, integridad y confidencialidad | ALTA | RED UCIR | Conultoría | | | |
| | | | ALT005 | El atacante consigue el acceso al activo sin tener autorización | ALTA | RED UCIR | Consultoría | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | antecedentes penales de los futuros colaboradores debido a que se asignara información clasificada de confidencial | | |
| 7 seguridad de los recursos humanos | 7.1.1 | Datos del personal | ALT006 | Revelar los datos de los salarios de los trabajadores, causando molestias entre los mismos. | ALTA | REDUCIR | CONTABILIDAD | **1.El acuerdo de confidencialidad de la seguridad de la información**<br>Indica el uso correcto de la información de la empresa brindada al personal, al inicio, durante y al finalizar el empleo por un tiempo determinado, incluye la política de seguridad de la información y los métodos de trabajo apropiados. | GERENTE | 1 |
| | 7.1.2 | Control de salarios | ALT007 | | | | | | | |
| | | Registro de órdenes de compra y venta | ALT008 | Fuga de información (accidental o intensional) pueden ocasionar pérdida de clientes y problemas financieros | ALTA | REDUCIR | | | | |
| | | Reporte de acceso de usuarios Radmin VPN Y ANYDESK | ALT009 | Fuga de información (accidental o intensional) pueden dañar la confianza de los clientes al momento de que utilicen sus sistemas por personas no autorizadas | ALTA | REDUCIR | | | | |
| | 7.2.2 | Datos del personal | ALT010 | Debido a que la organización no cuenta con una política de capacitación sobre la seguridad de la información sucede las siguientes incidencias: | ALTA | REDUCIR | CONTABILIDAD/ CONSULTORÍA Y | **1.Plan de capacitación y concientización**<br>Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito de la seguridad de la información, además de ayudarles e identificar incidencias, | GERENTE | 1 |
| | | Datos de los clientes | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Registro de órdenes de compra y venta<br>Reporte de acceso de usuarios Radmin VPN Y ANYDESK<br>Lista de instaladores de software | | -Modificación intencionalmente del registro de credenciales de acceso VPN Y ANYDESK<br>-Pérdida de información (accidental o intensional) tanto física y/o digital (no sincronizada en la nube) es decir no contar con un backup. | | | DESARROLLO | explicación de los controles de seguridad que se implementaran, entre otros.<br><br>**2.Politica de control de acceso**<br>Política en que todo personal debe saber los objetivos planteados que se deben cumplir de acuerdo a la confidencialidad, integridad y disponibilidad de la seguridad de la información<br>**3.Arbol de carpeta para el acceso a usuarios**<br>Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas. | | |
| 8. Gestión de activos | 8.1.3 | Lista de instaladores de software<br>Laptop de desarrollo | ALT011 | | ALTA | REDUCIR | CONSULTORÍA/SOPORTE | **1.- Política de uso, manejo de información confidencial y pérdida de información en Seisystem**<br><br>Definir los estándares para salvaguardar la información contra el uso o autorizado dentro de la empresa y así no sea divulgada con otros fines.<br><br>**2.- Formato de entrega de equipos** | GERENTE | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Formato donde se indique el nombre del personal, las especificaciones a detalle, accesorios y fecha de entrega de equipo. | | |
| | 8.3.2<br>8.3.3 | Registro de órdenes de compras y ventas | ALT012 | El no contar con procedimientos formales para la eliminación segura de elementos o información cuando ya no sea necesario dentro de la empresa, ocasionará pérdida de información y desconfianza entre el gerente y trabajadores. | ALTA | REDUCIR | CONTABILIDAD | **1.- Procedimiento de destrucción o eliminación de documentos**<br><br>Contar con procedimientos que permitan eliminar de forma segura los documentos que contienen información que ya o sean necesarias ni relevantes para así evitar fugas de información de usuarios no autorizados | | 1 |
| 9.Control de acceso | 9.1.1 | Datos cliente | ALT013 | Carencia de políticas de control de accesos, políticas sin autorización, fuga de información, pérdida en desarrollos de proyectos | ALTA | REDUCIR | CONSULTRÍA | **1.Politica de control de acceso**<br>Contar con una política en donde se indique cuáles son los responsables que deben tener acceso a las carpetas del drive y a que información pueden acceder<br>**2.Arbol de carpeta para el acceso a usuarios**<br>Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas. | GERENTE | 1 |
| | | Datos personal | | | | | | | | |
| | | Registro de órdenes de compras y ventas | | | | REDUCIR | CONTABILIDAD | | | |
| | | Lista de instaladores | ALT014 | | | | | | | |
| | 9.2.1 | Correo electrónico | ALT015 | Uso de correo electrónico para fines propios o robo de información | ALTA | REDUCIR | CONTABILIDAD | **1.- Política de seguridad de correo electrónico**<br>Política para el uso correcto del correo electrónico, identificando y/o recalcando que | GERENTE | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | la información es confidencial y no debe ser usada para otros fines | | |
| | 9.2.3 | Laptop de desarrollo | ALT016 | Cada usuario tiene asignado sus credenciales para el uso adecuado de los propósitos, cuando el usuario abusa de su nivel de privilegios para realizar otro tipo de cosas ocasiona pérdida de información. | ALTA | REDUCIR | CONSULTORÍA Y DESARROLLO | **1.-Polítca de control de acceso**<br>Política donde indique el control de derechos acceso privilegiados asociados a cada proceso, que la asignación de usuario debe estar restringida y controlada. | GERENTE | 1 |
| 11. Seguridad física y ambiental | 11.2.2 | Oficina Alfonso Ugarte | ALT017 | Cuentan con fallos de alimentación de energía eléctrica, fallos en conexión a internet entre otros | ALTA | TRANSFERIR | GERENTE | **1.- PROVEEDOR EXTERNO EN INSTALACIONES DE SUMINISTROS**<br>Contar con un proveedor que se encargue de las instalaciones (energía, ventiladores, entre otros) que aseguren que estén en correcto funcionamiento y así evitar problemas | Encargado de la seguridad de la información | 2 |
| 12. Seguridad de operaciones | 12.2.1<br>12.5.1<br>12.7.1 | Documentación administrativa | ALT018 | No cuentan con manuales de usuario, procedimientos y configuraciones ya sea instaladores de los softwares que deben de instalar en máquinas clientes. | ALTA | REDUCIR | CONSULTORIA Y CONTABILIDAD | **1.- Manuales, procedimientos y** configuraciones<br>Contar con manuales de usuario para los softwares utilizados.<br>**1.- Auditorias**<br>Realizar auditorías para visualizar los cumplimientos que se llevan a cabo y llevar su control adecuado. | GERENTE | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 13. Seguridad de las comunicaciones | 13.2.3 | Correo electrónico | ALT019 | Uso del correo para fines propios o robo de información | ALTA | REDUCIR | CONTABILIDAD | **<u>1.- Política de seguridad de correo electrónico</u>**<br>Política para el uso correcto del correo electrónico, identificando y/o recalcando que la información es confidencial y no debe ser usada para otros fines | GERENTE | 1 |
| | 13.2.4<br>13.2.2 | Control de salarios | ALT020 | Revelar datos de salarios generando una inquietud entre empleados | ALTO | REDUCIR | GERENTE | **1.- Acuerdo de confidencialidad de la seguridad de la información**<br>Indica el uso correcto de la información de la empresa brindada al personal durante su contratación, incluye puntos de transferencia de información y confidencialidad de estos | GERENTE | 1 |
| | | Reporte de acceso VPN Y ANYDESK | ALT021 | Fuga de información (accidental o intencional) ocasionando pérdida de clientes y problemas financieros. | ALTO | REDUCIR | | | | |
| | | Correo electrónico | ALT022 | Uso del correo para fines propios o robo de información | ALTO | REDUCIR | CONTABILIDAD | | | |
| 18. CUMPLIMIENTO | 18.1.3 | Datos cliente | ALT023 | Acceso de usuarios no autorizados.<br>Divulgar datos personales que afectaría al secreto comercial de la empresa siento una desventaja frente a nuestros competidores. | ALTO | REDUCIR | CONSULOTORÍA Y DESARROLLO | **<u>1.- Procedimiento de control de la información documentada</u>**<br>Tiene como objetivo describir actividades para establecer, documentar, controlar y mantener documentos (formatos, registros, etc.), de acuerdo con los requisitos establecidos por la organización | GERENTE | 1 |
| | | Datos del personal | | | | | GERENTE | | | |
| | 18.2.1<br>18.2.2 | Toda la documentación referent | ALT024 | Incumplimiento de política, controles, procedimientos para la seguridad de la información | ALTO | REDUCIR | GERENTE | **<u>1.Tipos de sanciones de acuerdo a la seguridad de la información</u>**<br>Contar con sanciones que infringe la seguridad de la información de la empresa y | GERENTE | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | e a la seguridad de la información | | | | | | así tomar decisiones correctas al momento de aplicarlas<br>2.- Revisión de la seguridad de la información<br>Establece la revisión de la seguridad de la información periódica para identificar oportunidades de mejora | | |
| **6. Organización de la seguridad de la información** | 6.1.4 | Persona | MOD001 | No contar con una asesoría o apoyo en seguridad de la información | MODERADO | REDUCIR | Todos los encargados | **1.Lista de contacto con grupos de interés en seguridad de la información**<br>Lista en la cual se encuentra los grupos de interés pertinentes a contactar de presentarse alguna inquietud respecto a la seguridad de la información en la empresa | Encargado del área correspondiente | 2 |
| | 6.2.2 | Datos del personal<br>Control de salarios | MOD002 | Fuga de información (accidental o intensional) pueden ocasionar daños de reputación, fugas de talentos, desconfianzas de gerentes hacia los colaboradores debido a que no cuentan con una política o un acuerdo de uso correcto de los dispositivos móviles. Solo la política de seguridad de la información es de acceso interno y/o externo | MODERADO | REDUCIR | Contabilidad | **1.El acuerdo de confidencialidad de la seguridad de la información**<br>Indica el uso correcto de la información expuesta en el correo institucional de los colaboradores para evitar fugas de información, accesos no autorizados, entre otros | Gerente | 1 |
| | 7.2.2 | Datos del personal | MOD003 | Debido a que en la consultora no cuentan con una política o capacitación sobre la seguridad | MODERADO | REDUCIR | Contabilidad | **1.Plan de capacitación y concientización**<br>Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito | Gerente | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Registros de órdenes de compra y facturas | | de la información sucede las siguientes incidencias:<br>-Fuga de información (acidental o intensional) pueden dañar la reputación de la empresa ya sea con fine maliciosos o económicos.<br>-Perdida de la información (accidental o intensional) tanto física y/o digital (no sincronizada al servidor de la nube), es decir, no contar con backup, puede ocasionar mal seguimiento de oportunidades entre otros. | | | | de la seguridad de la información, además de ayudarles a identificar incidencias, explicación de los controles de seguridad que se implementan, entre otros.<br>**2.Politicas de seguridad de la información**<br>Política en que todo colaborador debe saber los objetivos planteados que se debe cumplir de acuerdo a la confidencialidad, integridad y disponibilidad de la seguridad de la información.<br>**3.Arbol de carpeta para el acceso a usuarios**<br>Estructura de las carpetas de cada área de la empresa, especificando las personas autorizadas al uso de cada una de ellas | Gerente | |
| **8.Gestion de activos** | 8.3.2 | Datos personal | MOD004 | Al no contar con procedimientos formales para la eliminación segura de elementos o información cuando ya no es necesaria, ocasionando fuga de información, reputación de la consultora, mal manejo de información, desconfianza entre la empresa y los colaboradores | MODERADO | REDUCIR | Contabilidad | **1.Procedimiento de destrucción o eliminación de documentos**<br>Contar con procedimientos que permitan eliminar de forma segura de los documentos que contienen información que ya no sean necesarios para así evitar fugas de información de usuarios no autorizados | Gerente | 1 |
| | | Control de salarios | | | | | Contabilidad | | Gerente | |
| | 8.3.3 | Datos del cliente | MOD005 | El acceso de los datos de los clientes divulgada por usuarios no autorizados | MODERADO | REDUCIR | Consultoría y desarrollo | | Gerente | 2 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **9.Control de acceso** | 9.1.1 | Reporte de accesos de usuarios Radmin VPN Y ANYDESK | MOD006 | El reporte accesos de usuarios Radmin VPN Y ANYDESK solo tienen acceso al personal de consultoría y gerencia | MODERADO | REDUCIR | Consultoría | **<u>1.Politica de control de acceso</u>**<br>Contar con una política en donde indique cuales son los responsables que deben tener acceso a las carpetas de drive y que información pueden acceder | Gerente | 1 |
| **11. Seguridad física y ambiental** | 11.1.2 | Oficina de Alfonso Ugarte | MOD007 | Las áreas de la consultora no cuentan con controles de entrada, debido a que poca vez vienen usuarios externos, la mayoría pertenece a la consultora. Además, se encuentran en remodelación de lugar | MODERADO | TRANSFERERIR | Encargado de todas las áreas | **<u>1.Establecer controles de seguridad cuando se trasladen en la siguiente oficina</u>**<br>Contar con controles de seguridad como tarjetas de control de acceso con numero único por cada personal y acceso a las áreas correspondiente | Gerente | 1 |
| | 11.1.3 | | | | | | | | Gerente | 2 |
| **13. Seguridad de las comunicaciones** | 13.2.4 | Control de salarios | MOD008 | Fuga de información (accidental o intencional) pueden dañar la reputación de la empresa ya sea con fines maliciosos o económicos. | MODERADO | REDUCIR | Contabilidad | **<u>1.Acuerdo de confidencialidad de la seguridad de la información</u>**<br>Indica el uso correcto de la información de la organización brindada al personal durante su contratación, incluye puntos de transferencia de información y confidencialidad de estos. | Gerente | 1 |
| | 13.2.2 | Lista de instaladores de software | MOD009 | Los instaladores se tiene acceso del área de soporte y mantenimiento | MODERADO | REDUCIR | Área de Soporte | | Gerente | |
| **18. Cumplimiento** | 18.1.4 | Datos personal | MOD010 | Se modifica intencionalmente la lista personal afectando la gestión documentaria (sunat, | MODERADO | REDUCIR | Contabilidad | **<u>1.Acuerdo de confidencialidad de la seguridad de la información</u>** | Gerente | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | ministerio de trabajo entre otros) | | | | Indica el uso correcto de la información de datos del personal para evitar fugas de talentos | | |
| **7. Seguridad de los recursos humanos** | 7.2.2 | Datos del personal<br>Control de salarios | BAJ001 | Debido a que en la consultora no cuentan con una política o capacitación sobre la seguridad de la información sucede las siguientes incidencias:<br>-Perdida de la información (accidental o intensional) tanto física y/o digital (no sincronizada al servidor nube), es decir, no contar con un backup, puede ocasionar pérdida, gestión documentaria, control de acceso al VPN y Anydesk, entre otros. | BAJA | RED URCIR | Contabilidad<br>Contabilidad | **<u>1.Plan de capacitación y concientización</u>**<br>Tiene como objetivo concientizar y capacitar al personal para que entiendan el propósito de la seguridad de la información, además ayudarles a identificar incidencias, explicación de los controles de seguridad que se implementaran, entre otros.<br>**<u>2.Politica de seguridad de la información</u>**<br>Política en que todo colaborador debe saber los objetivos planteados que se deben cumplir de acuerdo a la confiabilidad, integridad y disponibilidad de la seguridad de la información. | Gerente<br>Contabilidad | |
| **13. Seguridad de las comunicaciones** | 13.2.4<br>13.2.2 | Documentación administrativa | BAJ002 | Posible robo de documentación técnica de los proyectos en donde se encuentra los procedimientos, manuales de usuarios de los realizados. | BAJA | RED UCIR | contabilidad | **<u>1.Acuerdo de confidencialidad de la seguridad de la información</u>**<br>Indica el uso correcto de la información de la organización brindada al personal durante su contratación, incluye puntos de transferencia de información y confiabilidad de estos. | Gerente general | 1 |

## ANEXO 10 PLAN DE IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

# Medidas de seguridad

### Instalación de medidas de seguridad para la oficina en Alfonso Ugarte

Se debe contar con la instalación de un sistema de alarma contra incendios para que pueda desenvolverse adecuadamente ante un aviso de incendio en la oficina.Para ello, tenemos el costo de la implementación considerando la cotizaciónobtenida de la misma empresa, en la Tabla 1. Además, se identificó como responsable de esta medida a la encargada del área de contabilidad.

***Tabla 1. Costo total de la implementación***

| Descripción | Valor Nuevos Soles S/ |
|---|---|
| Kit Sistema de alarma contra incendios +sensores de humo | S/ 2,879.00 |
| Instalación | S/ 0.00 |
| **Total, de la implementación** | **S/** 2,879.00 |

***Fuente: Elaboración propia***

### Seguro contra desastres naturales y no naturales

Se debe contar con una empresa, la cual se encargará de proteger la oficina contra incendios, daño malicioso, vandalismo, terremoto, huelgas, inundaciones, cortocircuitos, entre otros. Para ello se cotizó un Seguro para PYME de la empresa Pacífico, sobre ello se indica el costo en la Tabla 2 y se identificó como responsablede a la encargada del área de contabilidad.

***Tabla 2. Costo total de la implementación***

| Descripción | Valor Nuevos Soles S/ |
|---|---|
| Seguro para PYME (Incluye laptops) | S/ 150.00 |
| **Costo total mensual** | **S/ 150.00** |

***Fuente: Elaboración propia***

### Póliza de equipos electrónicos

Se debe contar con una empresa, la cual se encargará de proteger los equipos electrónicos contra perdida y daño físico accidental. Para ello se cotizó un Seguro de todo riesgo de equipo electrónico de la empresa MAPFRE, sobre ello se indicael costo en la Tabla 3 y se identificó como responsable a la encargada del área de contabilidad.

***Tabla 3. Costo total de la implementación***

| Descripción | Valor Nuevos Soles S/ |
|---|---|
| Seguro de todo riesgo de equipo electrónico | S/ 200.00 |
| **Costo total mensual** | **S/ 200.00** |

***Fuente: Elaboración propia***

### Sanciones de acuerdo con la seguridad de la información

Se debe contar con sanciones claras y específicas, en el reglamento interno, a favorde la seguridad de la información de la empresa, y a su vez estas deben ser comunicadas y explicadas. Para ello se identificó como responsable de la medida al Oficial de seguridad de información que se encargará de que se cumplan las sanciones establecidas por la empresa.

### Soporte técnico para el mantenimiento preventivo y correctivo de los equipos

Él encargado de soporte técnico se encargará del mantenimiento, diagnóstico y reparación de los equipos (laptops, impresoras, monitores, cargadores, entre otros) periódicamente. Para ello se cotizó este servicioen la misma empresa, sobre ello se indica el costo en la Tabla 4

***Tabla 4. Costo total de la implementación***

| Descripción | Valor Nuevos Soles S/ |
|---|---|
| Mantenimiento de equipos (bimestral) | S/ 00.00 |
| Diagnóstico de equipos | S/ 0.00 |
| Reparación de equipos (trimestral)* | S/ 300.00 |
| **Costo total** | **S/ 300.00** |

***Fuente: Elaboración propia***

### Creación de perfil de usuarios

Al momento de asignar un equipo a un recurso, se debe disponer de un perfil de usuario, dependiendo de la configuración deseada, es decir, crear un perfil “admin” que es el único responsable de instalar, actualizar los dispositivos autorizados, y otro perfil “local”. que el usuario crea en el dispositivo cuando inicia sesión, pero no puede cambiar o instalar el programa no está autorizado por el responsable, en este caso el responsable del área de soporte técnico.

### Instalación de suministros

Debe haber una empresa responsable del suministro de equipos (energía, electricidad, calefacción, ventiladores, aire acondicionado, etc.) para la nueva oficina de la empresa. Para ello, se cotizaron los costos previstos en la Tabla 6 y se identificó al responsable del área contable como responsable de la medida.

***Tabla 6. Servicios brindados***

| Descripción | Valor Nuevos Soles S/ |
|---|---|
| Servicio de electricidad | S/ 850.00 |
| Servicio de gasfitería | S/ 356.00 |
| Bombas de aguas | S/ 275.00 |
| Ventiladores | S/ 198.00 |
| Calefacción y aire acondicionado | S/ 756.00 |
| Instalación | S/ 65.00 |

***Fuente: Elaboración propia***

### Manuales, procedimientos y configuraciones

Manuales, procedimientos y configuraciones de servicios que nuestros clientes ya han realizado en la empresa deben estar disponibles para futuros servicios. Para ello, se identificó al responsable de Seguridad de la Información como responsable de la medida y con la ayuda del Coordinador del Área de Consultoría de Sistemas, además de velar por que toda la información procesada debe estar en la nube, también velar por que estos documentos estén cumplidos. Las carpetas compartidas dependen de las carpetas de acceso.

### Controles de seguridad en la nueva oficina

Se debe contar con controles de seguridad para la nueva oficina que se trasladará en el transcurso del año, como control de ingreso, cámaras de vigilancias, entre otros. Para ello se cotizó

***Tabla 7. Costo total de la implementación***

| Descripción | Valor Nuevos Soles S/ |
|---|---|
| Tarjetas de autenticación c/u | S/ 20.00 |
| 4 cámaras de vigilancias | S/ 880.00 |
| Sistema de control de ingreso | S/ 1105.00 |
| **Costo total** | S/ 2,005.00 |

***Fuente: Elaboración propia***

**Revisión de la seguridad de la información**

Se debe establecer una revisión de seguridad de la información para identificar oportunidades de mejora, para lo cual se implementará un plan de revisión bimensual para garantizar que el oficial de seguridad de la información garantice que se cumpla con el plan anterior y que se revise el cumplimiento de toda la documentación relacionada con la seguridad de la información.

**Lista de contactos con grupos de interés en seguridad de la información**

Se debe incluir una lista de contactos de cualquier grupo de interés relacionado con un incidente de seguridad, ya que la dama en el campo de la contabilidad será responsable de contactar al proveedor, la empresa proveedora en tal situación, realizan charlas, eventos, reuniones sobre seguridad de la información de la empresa.

**Desarrollo de software**

Se hace un aproximado en el costo del desarrollo del software para la empresa Seisystem Consultores. Donde el SQL Server Express se descarga la versión gratuita al igual que el visual studio 2019 y la laptop que es brindada por la empresa.

***Tabla 8. Costo desarrollo software***

| Descripción | Valor Nuevos Soles S/ |
|---|---|
| SQL Server Express | S/ 00.00 |
| Laptop AMD Ryzen 7 5700U with Radeon – 16 GB | S/ 00.00 |
| Desarrollo de software | S/ 850.00 |
| Visual Studio 2019 | S/ 00.00 |
| **Costo total** | S/ 850.00 |

***Fuente: Elaboración propia***

## ANEXO 11 INFORME DE ANÁLISIS INICIAL DE CONTROLES

## FICHA DE OBSERVACIÓN: INDICADOR NÚMERO DE CONTROLES APLICADOS

### 1. Tablas

Las tablas detallan los controles evaluados durante el análisis, los resultados y los gráficos de cumplimiento.

**A.1 Tabla 1 –** Resultados.

**A.2 Tabla 2 –** Gráficos de cumplimiento.

**Valoración del Nivel de Cumplimiento de Controles**

**Tabla de Aplicabilidad de Controles**

| ¿ES NECESARIO? | DESCRIPCIÓN | DETALLE |
|---|---|---|
| **Sí** | **APLICA** | El control sí es necesario para la organización |
| **No** | **NO APLICA** | El control no es necesario para la organización. |

**Nivel de Cumplimiento de Controles**

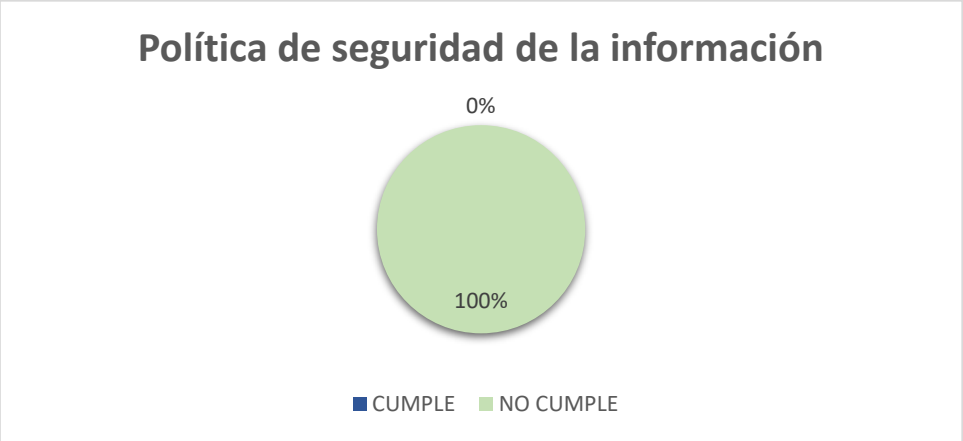
| DESCRIPCIÓN | PUNTAJE | PUNTUACIÓN | DETALLE |
|---|---|---|---|
| | | Porcentual | |
| **Completo** | 4 | **100%** | El control está implementado, ha sido aprobado por la alta dirección |
| **En proceso** | 3 | **70%** | El desarrollo de control está en procesode implementación. |
| **Inicio** | 2 | **40%** | Se ha identificado la necesidad delimplementar un control. El control apenas está iniciando. |
| **No existe** | 1 | **0%** | El control está ausente, no existe. |

Fuente: (De La Sota & Mechan, 2018)

## A1. Tabla 1 – Resultados

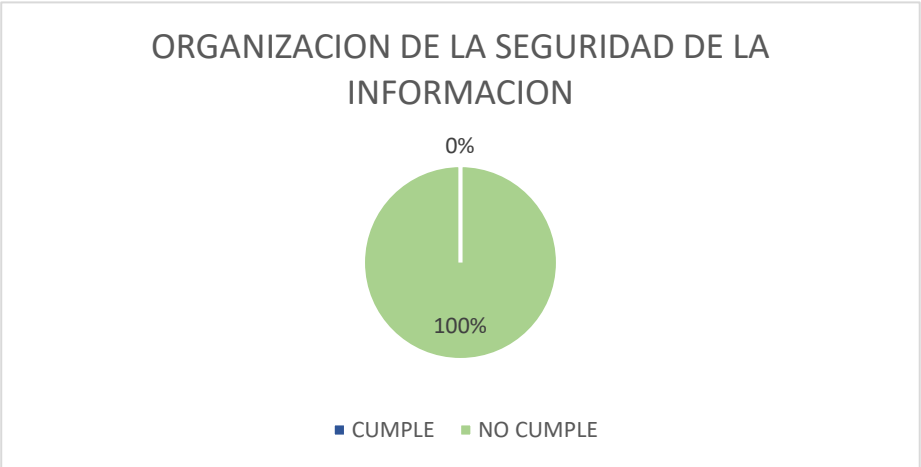
| | FICHA DE OBSERVACION N°03: NUMERO DE CONTROLES APLICADOS | | |
|---|---|---|---|
| | **FASE:** PRE TEST | **CODIGO:** F0-01 | **VERSION:** V1 |
| | **Fecha de recolección:** | 11/06/2022 | |
| | **Investigador:** | SANDOVAL CHERO CESAR ARTURO | |

| TÍTULO DE CONTROL | | PREGUNTAS | ¿APLICA? | RANGO | | | | COMENTARIOS |
|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | |
| **A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN** | | | | | | | | |
| **A.5.1. DIRECCIÓN DE LA GERENCIA PARA LA SEGURIDAD DE LA INFORMACIÓN** | | | | | | | | |
| **A.5.1.1** | **Políticas de seguridad de la información** | ¿Existe un documento denominado Política de Seguridad de la información y que esté aprobado por la alta dirección? | SI | X | | | | Debido a que no hay un área de tecnología de información, creían que no era necesario alguna política de seguridad. |
| | | ¿Considera que los empleados conocen las políticas de seguridad de su organización? | SI | X | | | | Solo el personal administrativo maneja esa información |
| **A.5.1.2** | **Revisión de las políticas de seguridad de la información** | ¿Su organización planifica intervalos de tiempo para la revisión de las políticas de seguridad de información? | SI | X | | | | Debido a que la política de seguridad no está bien establecida. |
| | | Cuando se realizaron las revisiones de las políticas de seguridad de la información, ¿se evalúa la efectividad, adecuación y conveniencia de las políticas? | SI | X | | | | Debido a que solo se enfocaron en el control de acceso de usuario y no todo en general. |



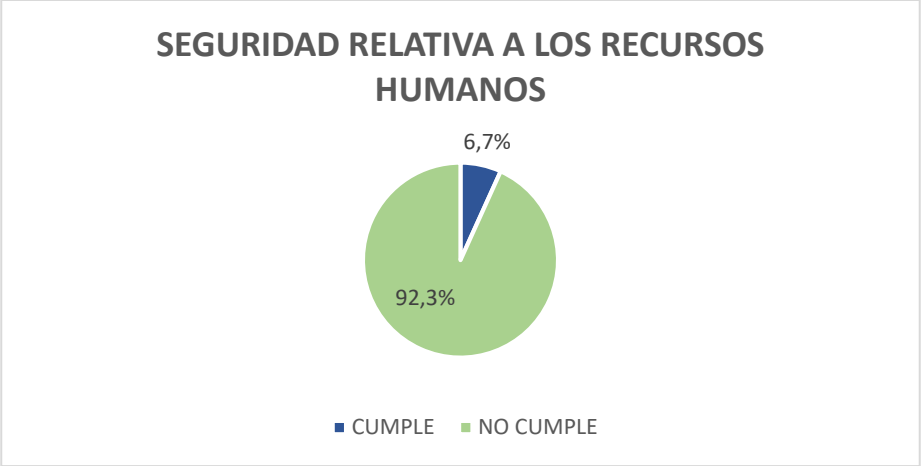

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.6 ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION** | | | | | | | | |
| **A.6.1. ORGANIZACIÓN INTERNA** | | | | | | | | |
| **A.6.1.1** | **Roles y responsabilidadades para la seguridad de la información** | ¿Tienen definidos los roles que existen en la organización referentes a la seguridad de la información? | SI | X | | | | Se tiene establecido los roles en un organigrama, más no todas las funciones del comité de seguridad. |
| | | ¿Se han asignado responsabilidades a los roles de la organización referentes a la seguridad de la información? | SI | X | | | | Debido de que aún no se asignado esas responsabilidades |
| **A.6.1.2** | **Segregación de funciones** | ¿La organización segregó algunas funciones a los roles en los activos de información? | SI | X | | | | Debido a que aún las funciones están en revisión |
| **A.6.1.3** | **Contacto con autoridades** | ¿Existe un documento que indique cuales son las autoridades por contactar al momento que exista un incidente en la seguridad de la información? | SI | X | | | | No existe ese documento |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.6.1.4** | **Contacto con grupos especiales de interés** | ¿La organización tiene algún contacto con un grupo de interés que le asesoren con problemas de seguridad de información? | SI | X | | | | Se han buscado asesores, pero no han llegado a un acuerdo. |
| **A.6.1.5** | **Seguridad de la información en la gestión de proyectos** | ¿La seguridad de la información se está integrando dentro del método de la gestión de proyectos de la organización? | SI | X | | | | Cuentan con un método más no están vinculando la seguridad de la información. |
| **A.6.2 DISPOSITIVOS MOVILES Y TELETRABAJO** | | | | | | | | |
| **A.6.2.1** | **Política de dispositivos móviles** | ¿Se usan medidas de seguridad contra los riesgos en los dispositivos móviles que pertenezcan a la organización? | NO | X | | | | No Aplica. |
| **A.6.2.2** | **Teletrabajo** | ¿Se usan medidas de seguridad con respecto a la información quese envía, recibe o almacena en el teletrabajo? | SI | X | | | | No existe medidas de seguridad respecto a la información compartida. |



| A.7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.7.1. ANTES DEL EMPLEO** | | | | | | | | |
| **A.7.1.1** | **Investigación de antecedentes** | ¿Los encargados en la selección del personal verifican los antecedentes de los candidatos a empleados y contratistas para prevenir algún mal uso de la información de la organización (Ej. Referencias, DNI, comprobación del CV, etc.)? | SI | | X | | | Hace unas semanas se ha iniciado la validación de la información colocada en sus CV'S. |
| **A.7.1.2** | **Términos y condiciones del empleo** | ¿Dentro del contrato se estipulan las responsabilidades del colaborador y la organización con respecto a la seguridad de la información? | SI | X | | | | Debido a que no está correctamente detallado en las cláusulas del contrato. |
| **A.7.2. DURANTE EL EMPLEO** | | | | | | | | |
| **A.7.2.1** | **Responsabilidades de gestión** | ¿La gerencia exige a los colaboradores y contratistas aplicar de seguridad de información de acuerdo con sus políticas y procedimientos establecidos? | SI | X | | | | No existe un documento o acuerdo que defina la aplicación de información. |
| **A.7.2.2** | **Conciencia, educación y capacitación sobre la seguridad de la información** | ¿Los colaboradores han tenido alguna capacitación sobre la conciencia de la seguridad de la información? | SI | X | | | | No hay capacitaciones respecto a la seguridad de información |

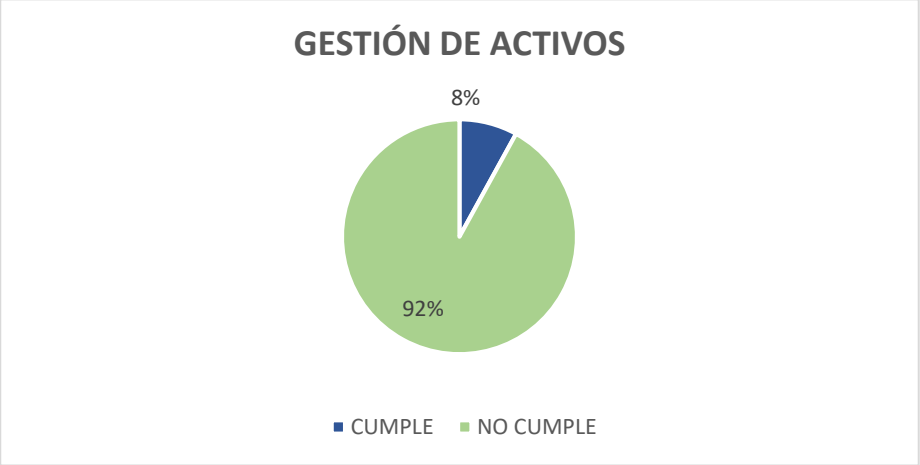
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ¿Se comunican a los colaboradores las actualizaciones sobre políticas o procedimientos de seguridad de la información, según sea relevante para la función del trabajo que cumpla? | SI | X | | | | Debido que no se encuentra formalizada la política de seguridad de información. |
| **A.7.2.3** | **Proceso disciplinario** | ¿La organización tiene algún proceso disciplinario formal para los colaboradores que hacen el mal uso de la información? | SI | X | | | | No tiene un proceso disciplinario |
| | | ¿Se ha comunicado este proceso disciplinario a los colaboradores? | SI | X | | | | Porque no tiene un proceso disciplinario |
| **A.7.3. FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO** | | | | | | | | |
| **A.7.3.1** | **Responsabilidad antes la finalización o cambio** | ¿Se definen y comunican las responsabilidades y obligaciones sobre la seguridad de la información que siguen vigentes después del cambio o finalización del empleo? | SI | X | | | | No se tiene definido ni comunicado las responsabilidades |




| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.8. GESTIÓN DE ACTIVOS** | | | | | | | | |
| **A.8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS** | | | | | | | | |
| **A.8.1.1** | **Inventario de activos** | ¿Se tienen identificados y documentados los activos de la información relevantes? | SI | X | | | | No se tiene identificado y documentado los activos. |
| **A.8.1.2** | **Propiedad de los activos** | ¿Se tiene algún registro con los propietarios que manejan los activos de la información en la organización? | SI | | X | | | No se tiene. |
| **A.8.1.3** | **Uso aceptable de los activos** | ¿Se han establecido, documentado e implantado reglas para asegurar el buen uso de los activos de información? | SI | X | | | | No, todavía. |
| **A.8.1.4** | **Devolución de activos** | ¿Cuentan con algún documento en donde se especifique los activos de la información y activos que se usaron durante el trabajo? | SI | X | | | | No, todavía. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ¿Tienen algún documento formal (proceso de desvinculación) que asegure la devolución del activo físico o electrónico que sea de propiedad de la organización? | SI | | X | | | Hace una semana se ha iniciado con el proceso de desvinculación del personal que implica devolución de activos. |
| **A.8.2. CLASIFICACIÓN DE LA INFORMACIÓN** | | | | | | | | |
| **A.8.2.1** | **Clasificación de la Información** | ¿La empresa tiene clasificadasu información según su importancia de revelación? | SI | X | | | | No existe |
| **A.8.2.2** | **Etiquetado de Información** | ¿Usan un manual de procedimientos para etiquetar la información? | SI | X | | | | No tienen. |
| **A.8.2.3** | **Manipulado de la información** | ¿Existe algún manual para manejar la información? | SI | X | | | | No tienen. |
| **A.8.3. MANIPULACIÓN DE LOS SOPORTES** | | | | | | | | |
| **A.8.3.1** | **Gestión de medios removibles** | ¿Se tiene documentado un procedimiento para la gestión de medios removibles? | SI | X | | | | No tienen. |
| **A.8.3.2** | **Disposición de medios** | ¿Tienen algún procedimiento formal en donde destruyen o eliminan la información de los medios electrónicos de la organización? | SI | X | | | | No tienen. |

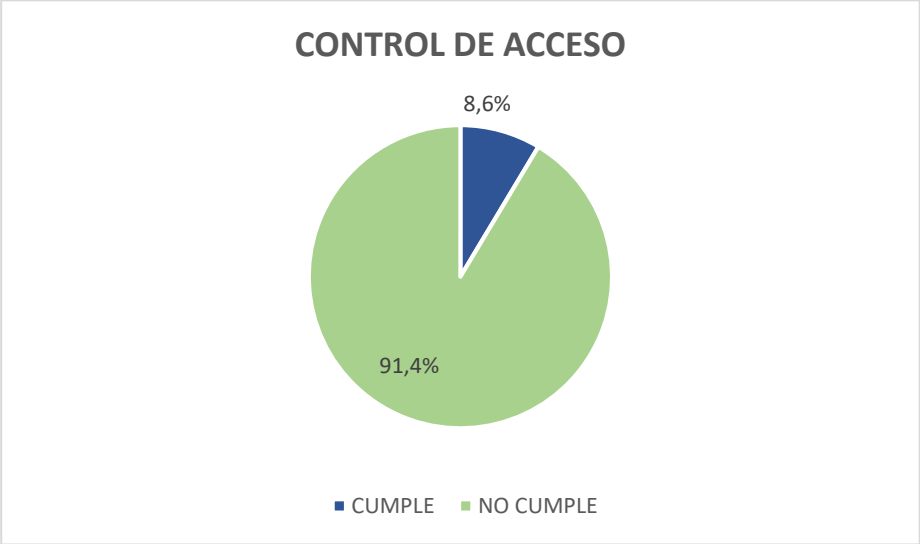
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.8.3.3** | **Transferencia de medios físicos** | ¿Existe alguna medida de seguridad para el uso de equipos físicos fuera o dentro de la empresa? | SI | | X | | | Se tiene un formato de entregas de materiales de trabajo. |




| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.9. CONTROL DE ACCESO** | | | | | | | | |
| **A.9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO** | | | | | | | | |
| **A.9.1.1** | **Política de control de acceso** | ¿Existen políticas en la organización de control de accesos con respecto a las necesidades de seguridad y negocio de la organización? | SI | | X | | | Se tiene solo para el control de acceso que se tienen con los clientes. |
| **A.9.1.2** | **Acceso a redes y servicios de red** | ¿Controlan los servicios de red en los usuarios en la organización? | SI | X | | | | No tienen. |
| **A.9.2. GESTIÓN DE ACCESO DE USUARIO** | | | | | | | | |
| **A.9.2.1** | **Registro y baja de usuarios** | ¿Existe algún proceso formal que permita el registro y la baja de usuarios para permitir la asignación de accesos? | SI | X | | | | No se tiene un proceso formal, solo es actuado. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.9.2.2** | **Aprovisionamiento de acceso a usuario** | ¿Se utiliza algún sistema que permita el ingreso y eliminación de los usuarios? | SI | | X | | | Se tiene en el mismo Google en la parte de administrador. |
| **A.9.2.3** | **Gestión de privilegios de acceso** | ¿Se tiene algún control del uso de accesos privilegiados? | SI | X | | | | No tienen |
| **A.9.2.4** | **Gestión de la información secreta de autentificación de los Usuarios** | ¿Se tienen políticas para la creación de las contraseñas? | SI | X | | | | No tienen |
| **A.9.2.5** | **Revisión de derechos de acceso de usuarios** | ¿El monitoreo de los accesos de los usuarios son realizados en la organización? | SI | | X | | | Se tiene un control de monitoreo respecto a los clientes más no interno de la organización. |
| **A.9.2.6** | **Retirada o reasignación de los derechos de acceso** | ¿Existe algún contrato o acuerdo que permita la exclusión al acceso de información a todos los empleados? | SI | X | | | | No tienen |
| **A.9.3. RESPONSABILIDADES DE LOS USUARIOS** | | | | | | | | |
| **A.9.3.1** | **Uso de información secreta de autentificación secreta** | ¿La organización presenta algún acuerdo que permita que el uso de la información sea secreta? | SI | X | | | | Solo se tiene un acuerdo por parte de nuestros clientes más no interno de la organización. |
| **A.9.4. CONTROL DE ACCESO A SISTEMA Y APLICACIÓN** | | | | | | | | |
| **A.9.4.1** | **Restricción de acceso a la información** | ¿La organización restringe el acceso a la información relevante? | SI | X | | | | No restringe |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.9.4.2** | **Procedimientoos de ingreso seguro** | ¿Existe algún procedimiento de ingreso seguro en la organización para el acceso a los sistemas de forma segura? | NO | X | | | | No aplica |
| **A.9.4.3** | **Sistema de gestión de contraseñas** | ¿Cuentan con un sistema de gestión en donde puedan establecer las contraseñas de manera segura y robustas? | SI | X | | | | No restringe |
| **A.9.4.4** | **Uso de programas utilitarios privilegiados** | ¿Se restringe o controla rigurosamente el uso de utilidades que puedan invalidar los controles del sistema? | NO | X | | | | No aplica |
| **A.9.4.5** | **Control de acceso al código fuente de los programas** | ¿Existe código fuente del cual no se permita poder manipular dentro de la organización, o sea que sea restringido? | SI | X | | | | No restringe |

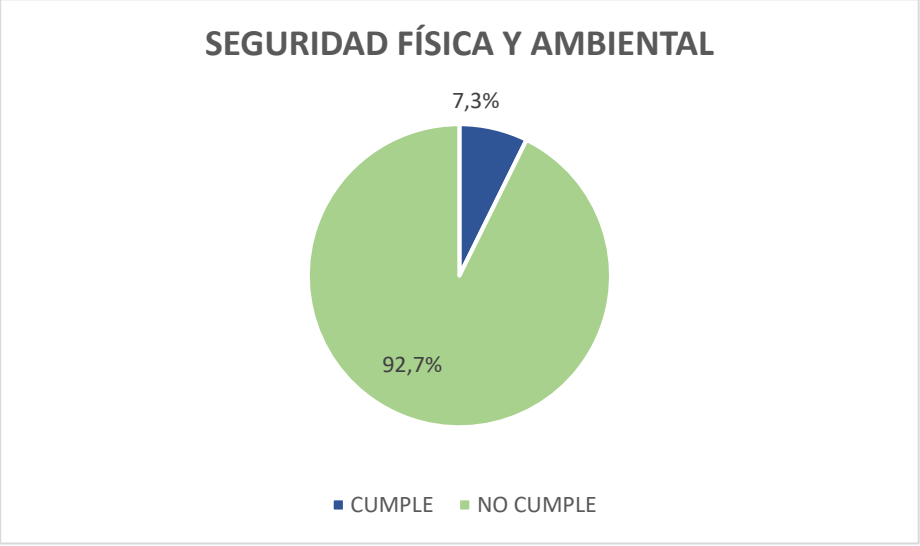



**A.10. CRIPTOGRAFÍA**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.10.1 CONTROLES CRIPTOGRÁFICOS** | | | | | | | | |
| **A.10.1.1** | **Política de uso de los controles criptográficos** | ¿La organización cuenta con una política sobre el uso de controles criptográficos para la protección de la información? | NO | X | | | | No aplica |
| **A.10.1.2** | **Gestión de claves** | ¿Se cuenta con especialistas para determinar el nivel apropiado de protección? | NO | X | | | | No aplica |
| **A.11. SEGURIDAD FISICA Y AMBIENTAL** | | | | | | | | |
| **A.11.1. ÁREAS SEGURAS** | | | | | | | | |
| **A.11.1.1** | **Perímetro de Seguridad Física** | ¿Aseguran los perímetros de seguridad en las áreas de información sensible, será suficiente para controlar el riesgo de pérdida y/robo de información? | NO | X | | | | No aplica |
| **A.11.1.2** | **Controles de Ingreso Físico** | ¿Detectan el acceso no autorizado, es decir aplicar algún medio de autenticación únicamente a personal autorizado? | SI | X | | | | No tienen |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.11.1.3** | **Asegurar oficinas, áreas e instalaciones** | ¿Previenen filtraciones en las oficinas, despachos y recursos, es decir se evita el acceso al público en general para prevenir cualquier pérdida y/robo de información? | SI | X | | | | No tienen |
| **A.11.1.4** | **Protección contra amenazas externas y ambientales** | ¿Establecen las políticas contra las amenazas externas y ambientales? | SI | X | | | | No tienen. |
| **A.11.1.5** | **Trabajo en áreas Seguras** | ¿Es seguro el área de trabajo de la organización? | **NO** | X | | | | No aplica |
| **A.11.1.6** | **Áreas de despacho y carga** | ¿La organización cuenta con áreas de carga y descarga? | **NO** | X | | | | No aplica |
| **A.11.2. SEGURIDAD DE EQUIPOS** | | | | | | | | |
| **A.11.2.1** | **Emplazamiento y protección de los equipos** | ¿Considera importante el emplazamiento y la protección de equipos? | NO | X | | | | No aplica |
| **A.11.2.2** | **Servicio de suministro** | ¿Se inspeccionan las instalaciones de suministros para su bien funcionamiento de la organización? | SI | X | | | | No se inspeccionan |
| **A.11.2.3** | **Seguridad del cableado** | ¿Tienen disponibilidad de los servicios de cableado eléctrico y telecomunicaciones de forma segura en la organización? | SI | X | | | | Si, pero para los equipos. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.11.2.4** | **Mantenimiento de equipos** | ¿Realizan periódicamente mantenimientos de equipos? | SI | | X | | | Se inició en mandar a mantenimiento los equipos. |
| **A.11.2.5** | **Remoción de equipos** | ¿Se realiza una buena logística en la seguridad de los equipos fuera de la organización? | SI | X | | | | No se realizan |
| **A.11.2.6** | **Seguridad de equipos y activos fuera de las instalaciones** | ¿Cuentan con un plan de seguridad con los activos que se encuentran fueras de las instalaciones? | SI | X | | | | No tienen |
| **A.11.2.7** | **Disposición o reutilización segura de equipos** | ¿Cuenta con una reutilización o eliminación segura de equipos? | SI | X | | | | No tienen |
| **A.11.2.8** | **Equipos de usuario desatendidos** | ¿Hay medidas de seguridad cuando el equipo es desatendido? | SI | | X | | | Se inició en que deben bloquear los equipos cuando no estén en uso |
| **A.11.2.9** | **Política de escritorio limpio y pantalla limpia** | ¿Se cumplen políticas de puesto de trabajo despejado y pantalla limpia? | SI | X | | | | No cumplen |



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.12 SEGURIDAD DE LAS OPERACIONES** | | | | | | | | |
| **A.12.1.1** | **Procedimientos operativos documentados** | ¿Se tienen documentado los procedimientos de operación? | SI | X | | | | Solo se tiene aún el flujo y está en proceso. |
| | | ¿Estos procedimientos se tienen a disposición de los usuarios que los necesiten? | SI | X | | | | No lo tienen |
| **A.12.1.2** | **Gestión del cambio** | ¿Se tiene alguna herramienta para controlar los cambios de los sistemas de procesamiento de información? | SI | X | | | | No lo tienen. |
| **A.12.1.3** | **Gestión de la capacidad** | ¿Monitorea el uso de recursos de la organización? | NO | X | | | | Todo es manualmente. |
| **A.12.1.4** | **Separación de los entornos de desarrollo, pruebas y operaciones** | ¿La organización tiene entornos de desarrollo, pruebas y operación? | NO | X | | | | No aplica porque no se está desarrollando software. |
| **A.12.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS** | | | | | | | | |
| **A.12.2.1** | **Controles contra códigos maliciosos** | ¿Se tiene un software para protegerse de las amenazas cibernéticas? | SI | | X | | | Se limita el uso de licencias de antivirus solo al personal de alto uso de información. |
| **A.12.3. RESPALDO** | | | | | | | | |
| **A.12.3.1** | **Respaldo de la información** | ¿Se realiza de forma automática o manual el back up de la información? | SI | X | | | | Se realizan el back up de información cuando se realiza la desvinculación del personal. |
| **A.12.4. REGISTROS Y MONITOREO** | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.12.4.1** | **Registro de eventos** | ¿Se revisa periódicamente los registros relacionados con eventos de actividad del usuario? | NO | X | | | | No aplica |
| **A.12.4.2** | **Protección de información de registros** | ¿Cuentan con un servidor de respaldo de la información de toda la organización? | NO | X | | | | No aplica |
| **A.12.4.3** | **Registros del administrador y del operador** | ¿Se cuenta con un sistema de actividad de intrusos? | NO | X | | | | No aplica |
| **A.12.4.4** | **Sincronización de reloj** | ¿Se tiene un servidor establecido para la sincronización de relojes en los sistemas de la organización? | NO | X | | | | No aplica |
| **A.12.1. CONTROL DEL SOFTWARE OPERACIONAL** | | | | | | | | |
| **A.12.5.1** | **Instalación de software en sistemas operacionales** | ¿Tienen procedimiento que se deben implementar para controlar la instalación de software en sistemas operacionales? | SI | X | | | | No cuentan con manuales de instalaciones de software. |
| **A.12.6. GESTION DE VULNERABILIDAD TECNICA** | | | | | | | | |
| **A.12.6.1** | **Gestión de vulnerabilidades técnicas** | ¿Se cuenta con un registro, control y monitoreo de vulnerabilidad de los activos de información? | SI | X | | | | No se tiene. |
| **A.12.6.2** | **Restricción en la instalación de software** | ¿Se cuenta con procedimiento de control y monitoreo de uso de software instalado? | SI | X | | | | No cuentan. |
| **A.12.7. CONSIDERACIONES PARA LA AUDITORIA DE LOS SISTEMA DE INFORMACION** | | | | | | | | |

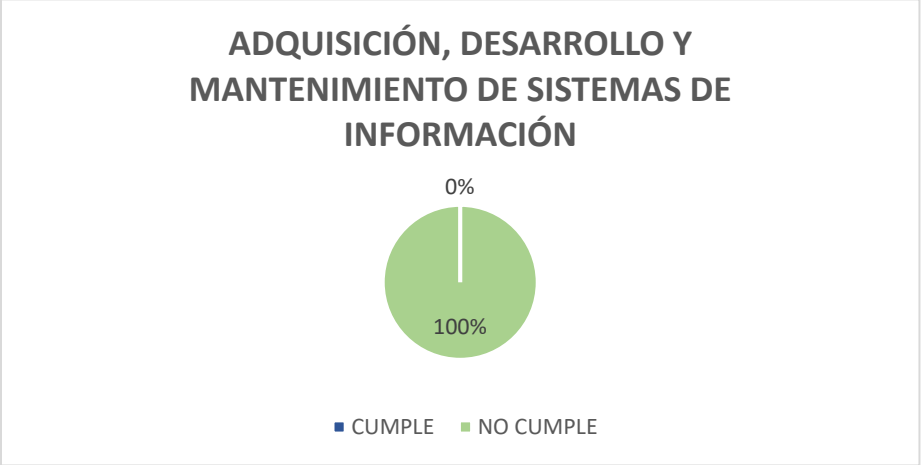
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.12.7.1** | **Controles de auditoría de sistemas de información** | ¿Se tiene un registro de auditoría de sistemas de información? | SI | X | | | | No cuentan con auditorías. |


| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.13. SEGURIDAD DE LA COMUNICACIONES** | | | | | | | | |
| **A.13.1. GESTION DE SEGURIDAD DE LA RED** | | | | | | | | |
| **A.13.1.1** | **Controles de la red** | ¿Las redes de la organización son gestionadas y controladas? | NO | X | | | | No aplica. |
| **A.13.1.2** | **Seguridad de servicios de red** | ¿Los servicios de red se gestionan internamente o es tercerizado? | NO | X | | | | No aplica. |
| **A.13.1.3** | **Segregación en redes** | ¿Tienen segregada la red? ¿Cómo está planificado la segregación de red? | NO | X | | | | No aplica. |
| **A.13.2. TRANSFERENCIA DE INFORMACIÓN** | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.13.2.1** | **Políticas y procedimientoos de transferencia de la información** | ¿Se tiene establecido las políticas o procedimientos para el intercambio de información? | NO | X | | | | No aplica. |
| **A.13.2.2** | **Acuerdo sobre transferencia de información** | ¿Se tienen acuerdos de intercambio de información de la organización con entidades externas? ¿Con todas las identidades se maneja el mismo procedimiento? | SI | X | | | | No tienen |
| **A.13.2.3** | **Mensajes electrónicos** | ¿Se tiene un sistema para la protección de mensajes electrónicos sospechosos? | SI | | X | | | Se tiene el antivirus Avast, pero no lo gestionan adecuadamente. |
| **A.13.2.4** | **Acuerdos de confidencialidad o no divulgación** | ¿Usan algún documento de requisitos para los acuerdos de confidencialidad? | SI | | X | | | Las políticas hacen mención a las leyes gubernamentales relacionadas a las telecomunicaciones. |

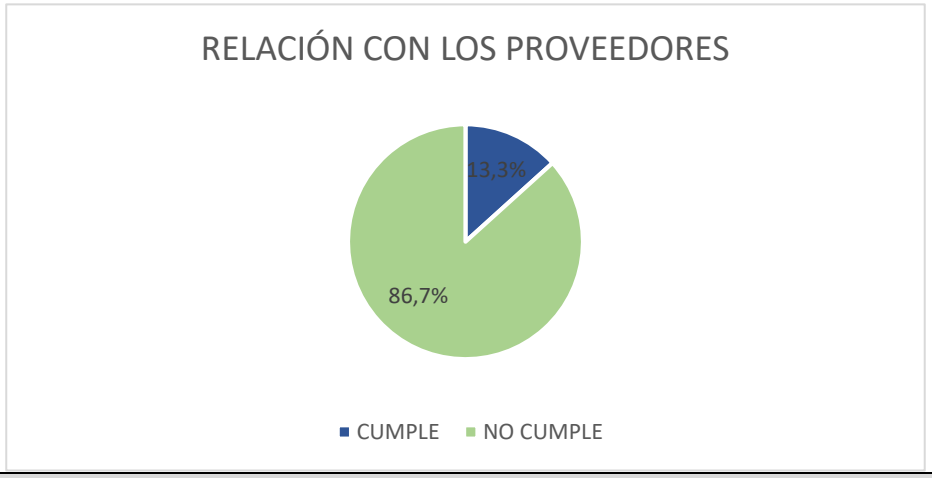
| A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.14.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN** | | | | | | | | |
| **A.14.1.1** | **Análisis de requisitos y especificaciones de seguridad de la información** | ¿Existen un análisis de los requisitos de seguridad de la información para nuevos sistemas o mejoras a los existentes? | NO | X | | | | No aplica. |
| **A.14.1.2** | **Asegurar los de servicios de aplicaciones en redes públicas** | Ante un eventual ataque a las redes, ¿poseen algún tipo de seguridad para protegerlas ante fraudes o robo de información? | NO | X | | | | No aplica. |
| **A.14.1.3** | **Protección de transacciones en servicios de aplicaciones** | Si al momento de transferir información se perdieran datos, ¿Se tiene algún plan de aseguramiento para que los datos no se pierdan? | NO | X | | | | No aplica. |
| **A.14.2. SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE** | | | | | | | | |
| **A.14.2.1** | **Política de desarrollo seguro** | ¿Cuentan con políticas la organización para el desarrollo de software / sistemas? | SI | X | | | | No tienen |
| **A.14.2.2** | **Procedimientos de control de cambios del sistema** | ¿Toman en cuenta las políticas que tiene la organización al realizar ambos alo largo de ciclo de vida del desarrollo del software / sistemas? | NO | X | | | | No aplica. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.14.2.3** | **Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo** | ¿Se realiza la revisión técnica de aplicaciones críticas para el negocio? | NO | X | | | | No aplica. |
| **A.14.2.4** | **Restricciones sobre cambios a los paquetes de software** | ¿Cuentan con control de acceso al modificar el código fuente de los paquetes de software? | SI | X | | | | No tienen. |
| **A.14.2.5** | **Principios de ingeniería de sistemas seguros** | ¿Establecen procedimientos de ingeniería de sistemas de información? | NO | X | | | | No aplica. |
| **A.14.2.6** | **Entorno de desarrollo seguro** | ¿Se realiza la protección del ambiente de desarrollo para la integración de sistemas? | NO | X | | | | No aplica. |
| **A.14.2.7** | **Externalización del desarrollo de software** | ¿Se realiza monitoreo a los sistemas contratados externamente? | NO | X | | | | No aplica. |
| **A.14.2.8** | **Pruebas funcionales de la seguridad de sistemas** | ¿Se realizan las pruebas necesarias de la seguridad del sistema durante el desarrollo? | NO | X | | | | No aplica. |
| **A.14.2.9** | **Pruebas de aceptación del Sistemas** | ¿Realizan algún tipo de plan de pruebas de aceptación para los sistemas? | SI | X | | | | No tienen. |
| **A.14.3. DATOS DE PRUEBA** | | | | | | | | |
| **A.14.3.1** | **Protección de datos de prueba** | ¿Se protege los datos de prueba? | NO | X | | | | No aplica. |



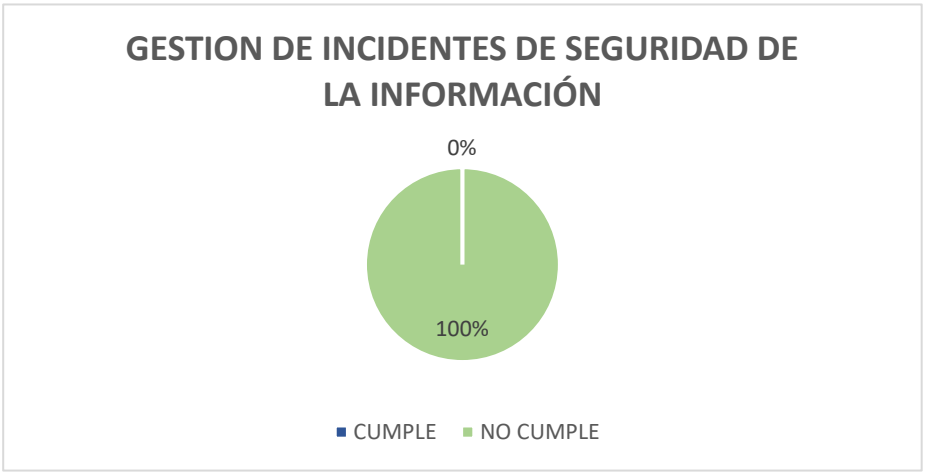

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.15. RELACION CON LOS PROVEEDORES** | | | | | | | | |
| **A.15.1. SEGURIDAD EN LAS RELACIONES CON PROVEEDORES** | | | | | | | | |
| **A.15.1.1** | **Política de seguridad de la información en las relaciones con los proveedores** | ¿Se realizan políticas de seguridad de la información por parte del proveedor hacia los activos que la organización posee? | SI | X | | | | No se realiza |
| **A.15.1.2** | **Requisitos de seguridad en contratos con terceros** | ¿Establece los requisitos de seguridad de la información con los proveedores acerca de la infraestructura de TI? | SI | X | | | | No se establecen |
| **A.15.1.3** | **Cadena de suministro de tecnología de la información y de las comunicaciones** | ¿Los acuerdos con los proveedores incluyen requisitos para abordar los riesgos de la seguridad de la información? | SI | X | | | | No se tiene acuerdos con respecto a la seguridad de la información |
| **A.15.2. GESTIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR** | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.15.2.1** | **Control y revisión de la provisión de servicios del proveedor** | ¿Se monitorea y/o audita la entrega de servicios por parte de los proveedores? | NO | | X | | | No aplica |
| **A.15.2.2** | **Gestión de cambios en la provisión del servicio del proveedor** | ¿Cuentan con un control ante la gestión de los cambios de provisión por parte de los proveedores? | NO | X | | | | No aplica |



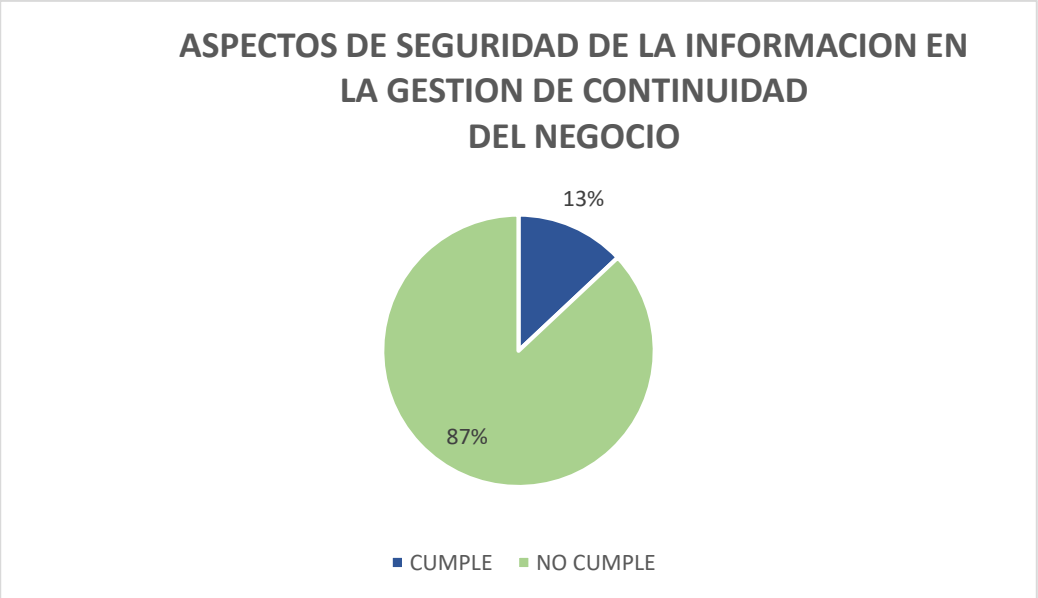

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.16. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** | | | | | | | | |
| **A.16.1. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS** | | | | | | | | |
| **A.16.1.1** | **Responsabilidades y procedimientos** | ¿Cuentan con una gestión de responsabilidades y procedimientos para los incidentes de seguridad de la información? | SI | X | | | | No cuentan |
| **A.16.1.2** | **Notificación de los eventos de seguridad de la información** | ¿Se realizan reportes sobre los eventos de seguridad de la información? | SI | X | | | | No realizan |
| **A.16.1.3** | **Notificación de puntos débiles de la seguridad** | ¿Se realizan reportes sobre las debilidades de seguridad de la información? | SI | X | | | | No realizan |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.16.1.4** | **Evaluación y decisión sobre los eventos de seguridad de la información** | ¿Realiza evaluaciones sobre incidentes de seguridad de la información? | SI | X | | | | No realizan |
| **A.16.1.5** | **Respuesta a incidentes de seguridad de la información** | ¿Se responden a los incidentes de seguridad de la información de la organización? | SI | X | | | | No se responden |
| **A.16.1.6** | **Aprendizaje de los incidentes de seguridad de la información** | ¿Resuelve los incidentes con los conocimientos adquiridos? | SI | X | | | | No se resuelven |
| **A.16.1.7** | **Recolección de evidencias** | ¿Realiza con frecuencia la recolección de evidencia y recolección de información? | SI | X | | | | No se recoleccionan |



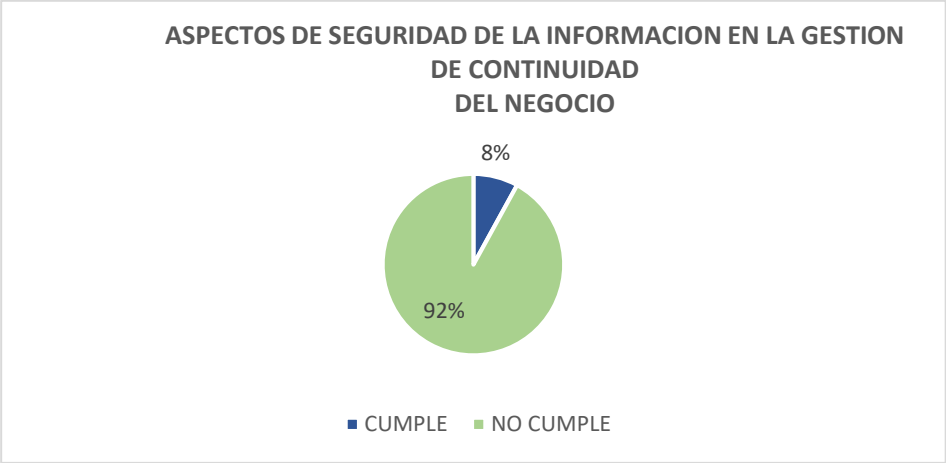

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE CONTINUIDAD DEL NEGOCIO** | | | | | | | | |
| **A.17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN** | | | | | | | | |
| **A.17.1.1** | **Planificación de continuidad de seguridad de la información** | ¿Cuentan con un plan en el cual determina los requisitos de seguridad de la información? | SI | | X | | | SÍ, está dentro de las políticas de seguridad de información. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.17.1.2** | **Implementación de continuidad de seguridad de la información** | ¿La organización cuenta con documentación, la cual busca implementar procesos, procedimientos y controles para asegurar la continuidad de la seguridad de la información? | SI | X | | | | No cuentan |
| **A.17.1.3** | **Verificación, revisión y evaluación de continuidad de seguridad de la información** | ¿Se realiza una verificación, revisión y evaluación de los controles de continuidad de seguridad de la información? | SI | X | | | | No se realizan |
| **A.17.2. REDUNDANCIAS** | | | | | | | | |
| **A.17.2.1** | **Instalación de procesamiento de la información** | ¿Existe un plan para asegurar la disponibilidad de la información? | NO | X | | | | No aplica |



| A.18. CUMPLIMIENTO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.18.1. CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES** | | | | | | | | |
| **A.18.1.1** | **Identificación de requisitos contractuales y de legislación aplicables** | ¿Cuentan con requerimientos estatutarios, regulatorios y contractuales? | SI | X | | | | No se cuentan |
| **A.18.1.2** | **Derechos de propiedad intelectual DPI** | ¿Al implementar los procedimientos cuenta con el cumplimiento de los requisitos legislativos, normativos y contractuales? | NO | X | | | | No aplica |
| | | ¿La organización tiene procedimientos para asegurar la protección de la propiedad intelectual? | NO | X | | | | No aplica |
| | | ¿Se adquiere software de fuentes conocidas y de buena reputación? | NO | | X | | | No aplica |
| **A.18.1.3** | **Protección de registros** | ¿Tienen un plan en donde protegen los registros de la organización contra pérdidas, falsificación y publicaciones no autorizadas? | SI | X | | | | No tienen |
| **A.18.1.4** | **Privacidad y protección de datos personales** | ¿Existe un control para asegurar la protección de la data y privacidad de información personal? | SI | X | | | | No existe |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.18.1.5** | **Regulación de controles criptográficos** | ¿La organización utiliza un control de cifrado de la información para verificar el cumplimiento con los acuerdos, legislación y normativas que se emplean? | NO | X | | | | No aplica |
| **A.18.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES** | | | | | | | | |
| **A.18.2.1** | **Revisión independiente de la seguridad de la información** | ¿Existen una revisión independiente de la seguridad de la información? | SI | X | | | | No realizan revisiones |
| **A.18.2.2** | **Cumplimiento de políticas y normas de seguridad** | ¿Se ha identificado las causas de incumplimiento de las políticas y normas de seguridad en la organización? | SI | | X | | | Se dio inicio debido que no se encuentran correctamente establecidas. |
| **A.18.2.3** | **Revisión del cumplimiento técnico** | ¿Se han realizadopruebas de penetración y vulnerabilidad? | NO | X | | | | No aplica |



A2. Tabla 2 – Gráfico de Cumplimiento

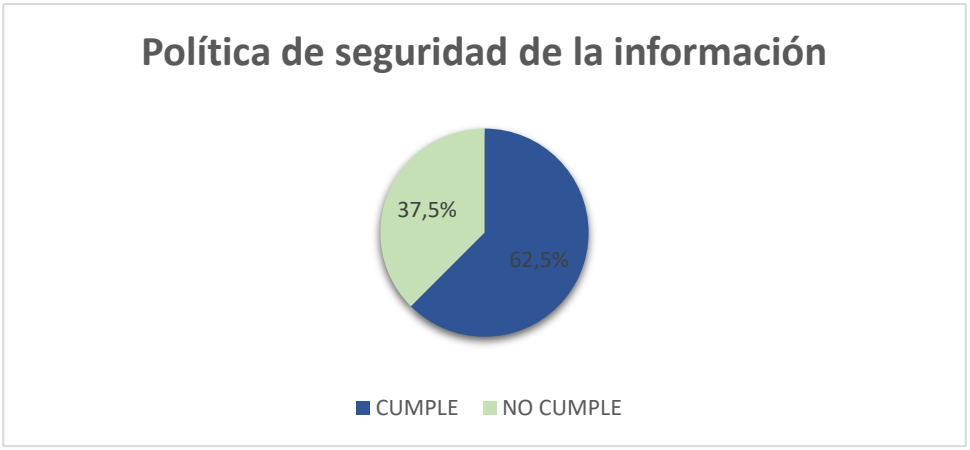
**Cuadro Porcentaje de Cumplimiento por Dominios Pre Test**

| N° | DOMINIOS EVALUDOS SEGÚN ISO 27001 | ANALISIS INICIAL | |
|---|---|---|---|
| **A.5** | Políticas de seguridad de la información | **0%** | **No existe** |
| **A.6** | Organización de la seguridad de la información | **0%** | **No existe** |
| **A.7** | Seguridad de los recursos humanos | **6.7%** | **Inicio** |
| **A.8** | Gestión de activos | **8%** | **Inicio** |
| **A.9** | Control de acceso | **8.6%** | **Inicio** |
| **A.10** | Criptografía | **0%** | **No aplica** |
| **A.11** | Seguridad física y ambiental | **7.3%** | **Inicio** |
| **A.12** | Seguridad de las operaciones | **5%** | **Inicio** |
| **A.13** | Seguridad de las comunicaciones | **26.6%** | **Inicio** |
| **A.14** | Adquisición, desarrollo y mantenimiento de sistemas | **0%** | **No existe** |
| **A.15** | Relación con los proveedores | **13.3%** | **Inicio** |
| **A.16** | Gestión de Incidentes de seguridad de la información | **0%** | **No existe** |
| **A.17** | Aspectos de seguridad de la información en la gestión de continuidad del negocio | **13%** | **Inicio** |
| **A.18** | Cumplimiento | **8%** | **Inicio** |

## A1. Tabla 1 – Resultados

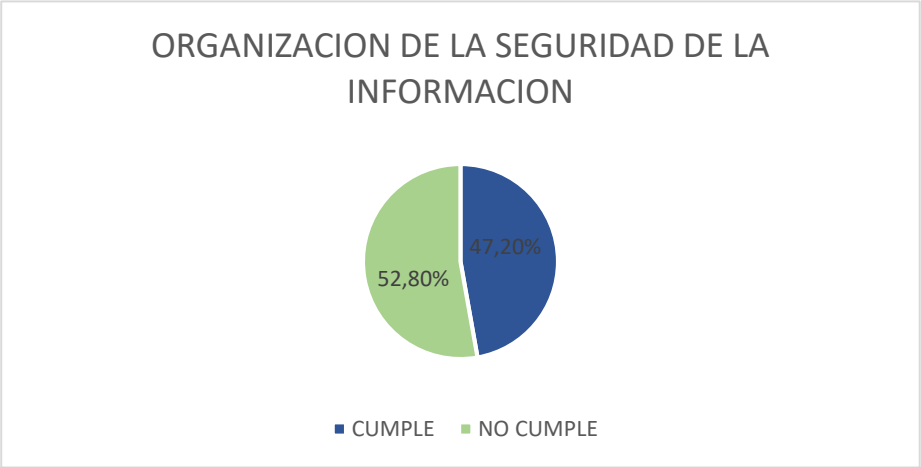
| | | | |
|---|---|---|---|
| | **FICHA DE OBSERVACION N°04: INDICADOR: NUMERO DE CONTROLES APLICADOS** | | |
| | **FASE:** POST TEST | **CODIGO:** F0-01 | **VERSION:** V1 |
| | **Fecha de recolección:** | 11/06/2022 | |
| | **Investigador:** | SANDOVAL CHERO CESAR ARTURO | |

| **TÍTULO DE CONTROL** | | **PREGUNTAS** | **¿APLICA?** | **RANGO** | | | | **COMENTARIOS** |
|---|---|---|---|---|---|---|---|---|
| | | | | **1** | **2** | **3** | **4** | |
| **A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN** | | | | | | | | |
| **A.5.1. DIRECCIÓN DE LA GERENCIA PARA LA SEGURIDAD DE LA INFORMACIÓN** | | | | | | | | |
| **A.5.1.1** | **Políticas de seguridad de la información** | ¿Existe un documento denominado Política de Seguridad de la información y que esté aprobado por la alta dirección? | SI | | | | X | Existe documento de políticade seguridad. |
| | | ¿Considera que los empleados conocen las políticas de seguridad de su organización? | SI | | | X | | Solo autorizado maneja esa información. |
| **A.5.1.2** | **Revisión de las políticas de seguridad de la información** | ¿Su organización planifica intervalos de tiempo para la revisión de las políticas de seguridad de información? | SI | | X | | | Se puso en marcha auditoría interna. |
| | | Cuando se realizaron las revisiones de las políticas de seguridad de la información, ¿se evalúa la efectividad, adecuación y conveniencia de las políticas? | SI | | X | | | Debido a que solo se enfocaron en el control de acceso de usuario y no todo engeneral. |



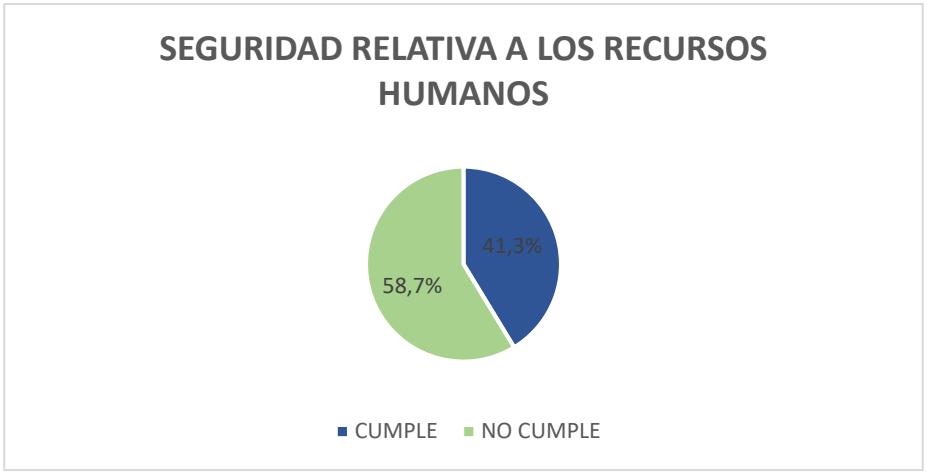

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.6 ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION** | | | | | | | | |
| **A.6.1. ORGANIZACIÓN INTERNA** | | | | | | | | |
| **A.6.1.1** | **Roles y responsabilidades para la seguridad de la información** | ¿Tienen definidos los roles que existen en la organización referentes a la seguridad de la información? | SI | | X | | | Se inició establecimiento en los roles en un organigrama. |
| | | ¿Se han asignado responsabilidades a los roles de la organización referentes a la seguridad de la información? | SI | | X | | | Se inició asignación de responsabilidades |
| **A.6.1.2** | **Segregación de funciones** | ¿La organización segregó algunas funciones a los roles en los activos de información? | SI | | X | | | Aún lasfunciones están en revisión |
| **A.6.1.3** | **Contacto con autoridades** | ¿Existe un documento que indique cuales son las autoridades por contactar al momento que exista un incidente en la seguridad de la información? | SI | | | | X | Existe ese documento. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.6.1.4** | **Contacto con grupos especiales de interés** | ¿La organización tiene algún contacto con un grupo de interés que le asesoren con problemas de seguridad de información? | SI | | X | | | Se inició a través de documentos planteados. |
| **A.6.1.5** | **Seguridad de la información en la gestión de proyectos** | ¿La seguridad de la información se está integrando dentro del método de la gestión de proyectos de la organización? | SI | | | X | | Se cuenta con un método vinculando laseguridad de la información. |
| **A.6.2 DISPOSITIVOS MOVILES Y TELETRABAJO** | | | | | | | | |
| **A.6.2.1** | **Política de dispositivos móviles** | ¿Se usan medidas de seguridad contra los riesgos en los dispositivos móviles que pertenezcan a la organización? | NO | X | | | | No Aplica. |
| **A.6.2.2** | **Teletrabajo** | ¿Se usan medidas de seguridad con respecto a la información quese envía, recibe o almacena en el teletrabajo? | SI | X | | | | No existe medidas de seguridad respecto a la información compartida. |



| A.7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.7.1. ANTES DEL EMPLEO** | | | | | | | | |
| **A.7.1.1** | **Investigación de antecedentes** | ¿Los encargados en la selección del personal verifican los antecedentes de los candidatos a empleados y contratistas para prevenir algún mal uso de la información de la organización (Ej. Referencias, DNI, comprobación del CV, etc.)? | SI | | X | | | Hace unas semanas se ha iniciado la validación de la información colocada en sus CV'S. |
| **A.7.1.2** | **Términos y condiciones del empleo** | ¿Dentro del contrato se estipulan las responsabilidades del colaborador y la organización con respecto a la seguridad de la información? | SI | X | | | | Debido a que no está correctamente detallado en las cláusulas del contrato. |
| **A.7.2. DURANTE EL EMPLEO** | | | | | | | | |
| **A.7.2.1** | **Responsabilidades de gestión** | ¿La gerencia exige a los colaboradores y contratistas aplicar de seguridad de información de acuerdo con sus políticas y procedimientos establecidos? | SI | | X | | | Se inició un documento o acuerdo que defina la aplicación de información. |
| **A.7.2.2** | **Conciencia, educación y capacitación sobre la seguridad de la información** | ¿Los colaboradores han tenido alguna capacitación sobre la conciencia de la seguridad de la información? | SI | | | | X | Se Aplicó capacitaciones respecto a la seguridad de información |

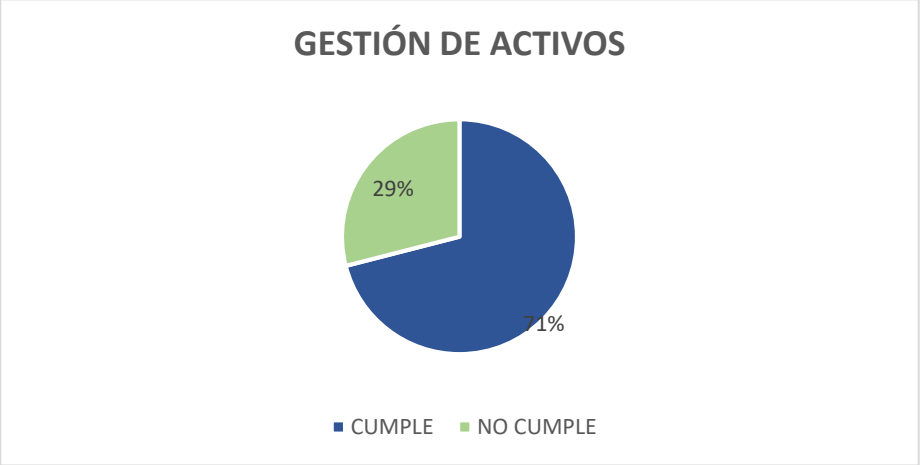
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ¿Se comunican a los colaboradores las actualizaciones sobre políticas o procedimientos de seguridad de la información, según sea relevante para la función del trabajo que cumpla? | SI | | X | | | Debido que no se encuentra formalizada la política de seguridad de información. |
| **A.7.2.3** | **Proceso disciplinario** | ¿La organización tiene algún proceso disciplinario formal para los colaboradores que hacen el mal uso de la información? | SI | | | **X** | | Se tiene un proceso disciplinario |
| | | ¿Se ha comunicado este proceso disciplinario a los colaboradores? | SI | | X | | | Se tiene un proceso disciplinario |
| **A.7.3. FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO** | | | | | | | | |
| **A.7.3.1** | **Responsabilidad antes la finalización o cambio** | ¿Se definen y comunican las responsabilidades y obligaciones sobre la seguridad de la información que siguen vigentes después del cambio o finalización del empleo? | SI | X | | | | No se tiene definido ni comunicado las responsabilidades |




| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.8. GESTIÓN DE ACTIVOS** | | | | | | | | |
| **A.8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS** | | | | | | | | |
| **A.8.1.1** | **Inventario de activos** | ¿Se tienen identificados y documentados los activos de la información relevantes? | SI | | | | X | Se tiene identificado y documentado los activos. |
| **A.8.1.2** | **Propiedad de los activos** | ¿Se tiene algún registro con los propietarios que manejan los activos de la información en la organización? | SI | | | **X** | | Se estableció a través del software los propietarios de cada información que manejen. |
| **A.8.1.3** | **Uso aceptable de los activos** | ¿Se han establecido, documentado e implantado reglas para asegurar el buen uso de los activos de información? | SI | | | | X | Se estableció procedimientos de devoluciones por parte de trabajador. |
| **A.8.1.4** | **Devolución de activos** | ¿Cuentan con algún documento en donde se especifique los activos de la información y activos que se usaron durante el trabajo? | SI | | | X | | Se estableció procedimientos de devoluciones por parte de trabajador. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ¿Tienen algún documento formal (proceso de desvinculación) que asegure la devolución del activo físico o electrónico que sea de propiedad de la organización? | SI | | X | | | Hace una semana se ha iniciado con el proceso de desvinculación del personal que implica devolución de activos. |
| **A.8.2. CLASIFICACIÓN DE LA INFORMACIÓN** | | | | | | | | |
| **A.8.2.1** | **Clasificación de la Información** | ¿La empresa tiene clasificadasu información según su importancia de revelación? | SI | | X | | | Se inició. |
| **A.8.2.2** | **Etiquetado de Información** | ¿Usan un manual de procedimientos para etiquetar la información? | SI | | | | X | Se aplicó etiquetado para los equipos. |
| **A.8.2.3** | **Manipulado de la información** | ¿Existe algún manual para manejar la información? | SI | | | X | | En proceso de ejecución del manual. |
| **A.8.3. MANIPULACIÓN DE LOS SOPORTES** | | | | | | | | |
| **A.8.3.1** | **Gestión de medios removibles** | ¿Se tiene documentado un procedimiento para la gestión de medios removibles? | SI | | X | | | Se inició procedimiento |
| **A.8.3.2** | **Disposición de medios** | ¿Tienen algún procedimiento formal en donde destruyen o eliminan la información de los medios electrónicos de la organización? | SI | | X | | | Se inició procedimiento |

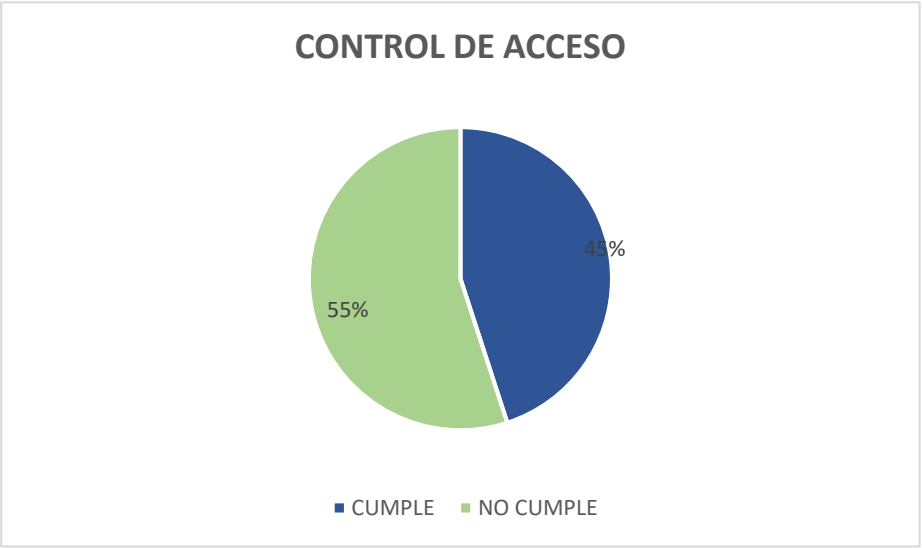
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.8.3.3** | **Transferencia de medios físicos** | ¿Existe alguna medida de seguridad para el uso de equipos físicos fuera o dentro de la empresa? | SI | | X | | | Se tiene un formato de entregas de materiales de trabajo. |




| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.9. CONTROL DE ACCESO** | | | | | | | | |
| **A.9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO** | | | | | | | | |
| **A.9.1.1** | **Política de control de acceso** | ¿Existen políticas en la organización de control de accesos con respecto a las necesidades de seguridad y negocio de la organización? | SI | | X | | | Se inició control de acceso que se tienen con los clientes. |
| **A.9.1.2** | **Acceso a redes y servicios de red** | ¿Controlan los servicios de red en los usuarios en la organización? | SI | X | | | | No tienen. |
| **A.9.2. GESTIÓN DE ACCESO DE USUARIO** | | | | | | | | |
| **A.9.2.1** | **Registro y baja de usuarios** | ¿Existe algún proceso formal que permita el registro y la baja de usuarios para permitir la asignación de accesos? | SI | | X | | | Se inicio un proceso formal, solo es actuado. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.9.2.2** | **Aprovisionamiento de acceso a usuario** | ¿Se utiliza algún sistema que permita el ingreso y eliminación de los usuarios? | SI | | | | X | Se tiene en el software que administra el gerente general. |
| **A.9.2.3** | **Gestión de privilegios de acceso** | ¿Se tiene algún control del uso de accesos privilegiados? | SI | | | X | | No tienen |
| **A.9.2.4** | **Gestión de la información secreta de autentificación de los usuarios** | ¿Se tienen políticas para la creación de las contraseñas? | SI | | X | | | No tienen |
| **A.9.2.5** | **Revisión de derechos de acceso de usuarios** | ¿El monitoreo de los accesos de los usuarios son realizados en la organización? | SI | | | X | | Se tiene un control de monitoreo respecto a los clientes. |
| **A.9.2.6** | **Retirada o reasignación de los derechos de acceso** | ¿Existe algún contrato o acuerdo que permita la exclusión al acceso de información a todos los empleados? | SI | X | | | | No tienen |
| **A.9.3. RESPONSABILIDADES DE LOS USUARIOS** | | | | | | | | |
| **A.9.3.1** | **Uso de información secreta de autentificación secreta** | ¿La organización presenta algún acuerdo que permita que el uso de la información sea secreta? | SI | | X | | | Solo se tiene un acuerdo por parte de nuestros clientes más no interno de la organización. |
| **A.9.4. CONTROL DE ACCESO A SISTEMA Y APLICACIÓN** | | | | | | | | |
| **A.9.4.1** | **Restricción de acceso a la información** | ¿La organización restringe el acceso a la información relevante? | SI | | | X | | En proceso de la restricción de acceso de información. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.9.4.2** | **Procedimientos de ingreso seguro** | ¿Existe algún procedimiento de ingreso seguro en la organización para el acceso a los sistemas de forma segura? | NO | X | | | | No aplica |
| **A.9.4.3** | **Sistema de gestión de contraseñas** | ¿Cuentan con un sistema de gestión en donde puedan establecer las contraseñas de manera segura y robustas? | SI | | | | X | se aplicó software para la gestión. |
| **A.9.4.4** | **Uso de programas utilitarios privilegiados** | ¿Se restringe o controla rigurosamente el uso de utilidades que puedan invalidar los controles del sistema? | NO | X | | | | No aplica |
| **A.9.4.5** | **Control de acceso al código fuente de los programas** | ¿Existe código fuente del cual no se permita poder manipular dentro de la organización, o sea que sea restringido? | SI | | | | X | Con las medidas de seguridad se lleva el control. |

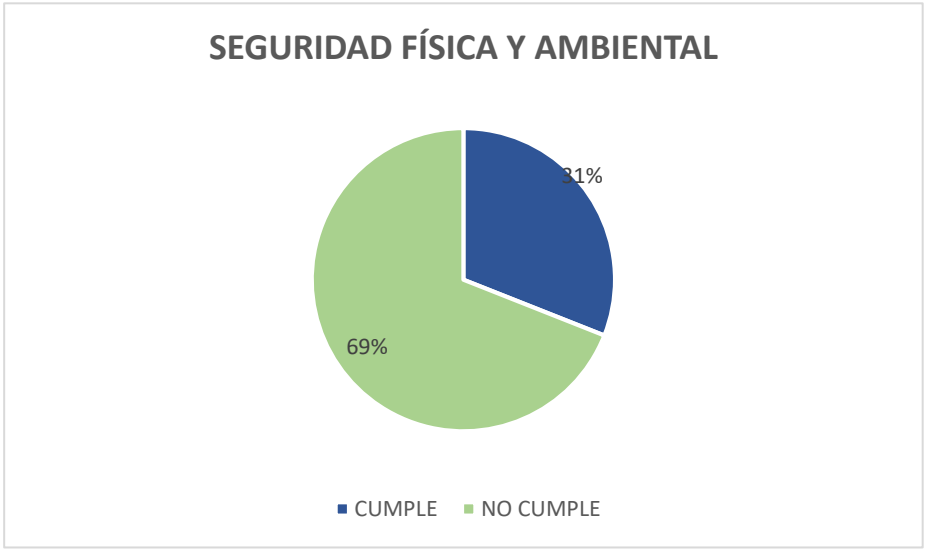



**A.10. CRIPTOGRAFÍA**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.10.1 CONTROLES CRIPTOGRÁFICOS** | | | | | | | | |
| **A.10.1.1** | **Política de uso de los controles criptográficos** | ¿La organización cuenta con una política sobre el uso de controles criptográficos para la protección de la información? | NO | X | | | | No aplica |
| **A.10.1.2** | **Gestión de claves** | ¿Se cuenta con especialistas para determinar el nivel apropiado de protección? | NO | X | | | | No aplica |
| **A.11. SEGURIDAD FISICA Y AMBIENTAL** | | | | | | | | |
| **A.11.1. ÁREAS SEGURAS** | | | | | | | | |
| **A.11.1.1** | **Perímetro de Seguridad Física** | ¿Aseguran los perímetros de seguridad en las áreas de información sensible, será suficiente para controlar el riesgo de pérdida y/robo de información? | NO | X | | | | No aplica |
| **A.11.1.2** | **Controles de Ingreso Físico** | ¿Detectan el acceso no autorizado, es decir aplicar algún medio de autenticación únicamente a personal autorizado? | SI | | **X** | | | En inicio planteado en el grupo de planes de medidas de seguridad. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.11.1.3** | **Asegurar oficinas, áreas e instalaciones** | ¿Previenen filtraciones en las oficinas, despachos y recursos, es decir se evita el acceso al público en general para prevenir cualquier pérdida y/robo de información? | SI | | X | | | Se inicio prevención. |
| **A.11.1.4** | **Protección contra amenazas externas y ambientales** | ¿Establecen las políticas contra las amenazas externas y ambientales? | SI | | X | | | Se inicio políticas contra las amenazas externas. |
| **A.11.1.5** | **Trabajo en áreas Seguras** | ¿Es seguro el área de trabajo de la organización? | NO | X | | | | No aplica |
| **A.11.1.6** | **Áreas de despacho y carga** | ¿La organización cuenta con áreas de carga y descarga? | NO | X | | | | No aplica |
| **A.11.2. SEGURIDAD DE EQUIPOS** | | | | | | | | |
| **A.11.2.1** | **Emplazamientoo y protección de los equipos** | ¿Considera importante el emplazamiento y la protección de equipos? | NO | X | | | | No aplica |
| **A.11.2.2** | **Servicio de suministro** | ¿Se inspeccionan las instalaciones de suministros para su bien funcionamiento de la organización? | SI | | X | | | Se inició en mandar a mantenimiento los equipos. |
| **A.11.2.3** | **Seguridad del cableado** | ¿Tienen disponibilidad de los servicios de cableado eléctrico y telecomunicaciones de forma segura en la organización? | SI | X | | | | Si, pero para los equipos. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.11.2.4** | **Mantenimientoo de equipos** | ¿Realizan periódicamente mantenimientos de equipos? | SI | | | X | | Se inició en mandar a mantenimiento los equipos. |
| **A.11.2.5** | **Remoción de equipos** | ¿Se realiza una buena logística en la seguridad de los equipos fuera de la organización? | SI | | X | | | En inicio. |
| **A.11.2.6** | **Seguridad de equipos y activos fuera de las instalaciones** | ¿Cuentan con un plan de seguridad con los activos que se encuentran fueras de las instalaciones? | SI | | X | | | En inicio. |
| **A.11.2.7** | **Disposición o reutilización segura de equipos** | ¿Cuenta con una reutilización o eliminación segura de equipos? | SI | | | X | | Se propuso políticas de seguridad. |
| **A.11.2.8** | **Equipos de usuario desatendidos** | ¿Hay medidas de seguridad cuando el equipo es desatendido? | SI | | X | | | Se inició en que deben bloquear los equipos cuandono estén en uso |
| **A.11.2.9** | **Política de escritorio limpio y pantalla limpia** | ¿Se cumplen políticas de puesto de trabajo despejado y pantalla limpia? | SI | | X | | | En proceso de revisión. |



| A.12 SEGURIDAD DE LAS OPERACIONES | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| A.12.1.1 | Procedimientos operativos documentados | ¿Se tienen documentado los procedimientos de operación? | SI | | X | | | Solo se tiene aún el flujo y está en proceso. |
| | | ¿Estos procedimientos se tienen a disposición de los usuarios que los necesiten? | SI | | X | | | Está en proceso. |
| A.12.1.2 | Gestión del cambio | ¿Se tiene alguna herramienta para controlar los cambios de los sistemas de procesamiento de información? | SI | | X | | | En proceso de aplicación de herramienta. |
| A.12.1.3 | Gestión de la capacidad | ¿Monitorea el uso de recursos de la organización? | NO | X | | | | Todo es manualmente. |
| A.12.1.4 | Separación de los entornos de desarrollo, pruebas y operaciones | ¿La organización tiene entornos de desarrollo, pruebas y operación? | NO | X | | | | No aplica porque no se está desarrollando software. |
| **A.12.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS** | | | | | | | | |
| A.12.2.1 | Controles contra códigos maliciosos | ¿Se tiene un software para protegerse de las amenazas cibernéticas? | SI | | X | | | Se limita el uso de licencias de antivirus solo al personal de alto uso de información. |
| **A.12.3. RESPALDO** | | | | | | | | |
| A.12.3.1 | Respaldo de la información | ¿Se realiza de forma automática o manual el back up de la información? | SI | | | | X | Se realizan el back up de información. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.12.4. REGISTROS Y MONITOREO** | | | | | | | | |
| **A.12.4.1** | **Registro de eventos** | ¿Se revisa periódicamente los registros relacionados con eventos de actividad del usuario? | NO | X | | | | No aplica |
| **A.12.4.2** | **Protección de información de registros** | ¿Cuentan con un servidor de respaldo de la información de toda la organización? | NO | X | | | | No aplica |
| **A.12.4.3** | **Registros del administrador y del operador** | ¿Se cuenta con un sistema de actividad de intrusos? | NO | X | | | | No aplica |
| **A.12.4.4** | **Sincronización de reloj** | ¿Se tiene un servidor establecido para la sincronización de relojes en los sistemas de la organización? | NO | X | | | | No aplica |
| **A.12.1. CONTROL DEL SOFTWARE OPERACIONAL** | | | | | | | | |
| **A.12.5.1** | **Instalación de software en sistemas operacionales** | ¿Tienen procedimiento que se deben implementar para controlar la instalación de software en sistemas operacionales? | SI | | | | X | Ya se cuentan con manuales de instalaciones de software. |
| **A.12.6. GESTION DE VULNERABILIDAD TECNICA** | | | | | | | | |
| **A.12.6.1** | **Gestión de vulnerabilidades técnicas** | ¿Se cuenta con un registro, control y monitoreo de vulnerabilidad de los activos de información? | SI | | X | | | En inicio |

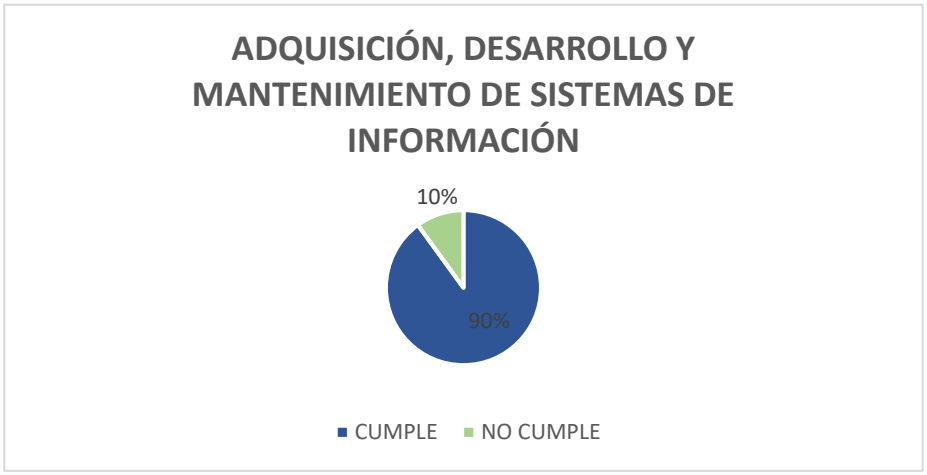
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.12.6.2** | **Restricción en la instalación de software** | ¿Se cuenta con procedimiento de control y monitoreo de uso de software instalado? | SI | | X | | | En inicio |
| **A.12.7. CONSIDERACIONES PARA LA AUDITORIA DE LOS SISTEMA DE INFORMACION** | | | | | | | | |
| **A.12.7.1** | **Controles de auditoría de sistemas de información** | ¿Se tiene un registro de auditoría de sistemas de información? | SI | | | | X | Ya se aplica auditoría. |


| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.13. SEGURIDAD DE LA COMUNICACIONES** | | | | | | | | |
| **A.13.1. GESTION DE SEGURIDAD DE LA RED** | | | | | | | | |
| **A.13.1.1** | **Controles de la red** | ¿Las redes de la organización son gestionadas y controladas? | NO | X | | | | No aplica. |
| **A.13.1.2** | **Seguridad de servicios de red** | ¿Los servicios de red se gestionan internamente o es tercerizado? | NO | X | | | | No aplica. |
| **A.13.1.3** | **Segregación en redes** | ¿Tienen segregada la red? ¿Cómo está planificado la segregación de red? | NO | X | | | | No aplica. |

| A.13.2. TRANSFERENCIA DE INFORMACIÓN | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.13.2.1** | **Políticas y procedimientos de transferencia de la información** | ¿Se tiene establecido las políticas o procedimientos para el intercambio de información? | NO | X | | | | No aplica. |
| **A.13.2.2** | **Acuerdo sobre transferencia de información** | ¿Se tienen acuerdos de intercambio de información de la organización con entidades externas? ¿Con todas las identidades se maneja el mismo procedimiento? | SI | | X | | | En inicio |
| **A.13.2.3** | **Mensajes electrónicos** | ¿Se tiene un sistema para la protección de mensajes electrónicos sospechosos? | SI | | X | | | Se tiene el antivirus Avast |
| **A.13.2.4** | **Acuerdos de confidencialidad o no divulgación** | ¿Usan algún documento de requisitos para los acuerdos de confidencialidad? | SI | | | | **X** | Se estableció documento de políticas de seguridad de la información con la empresa |

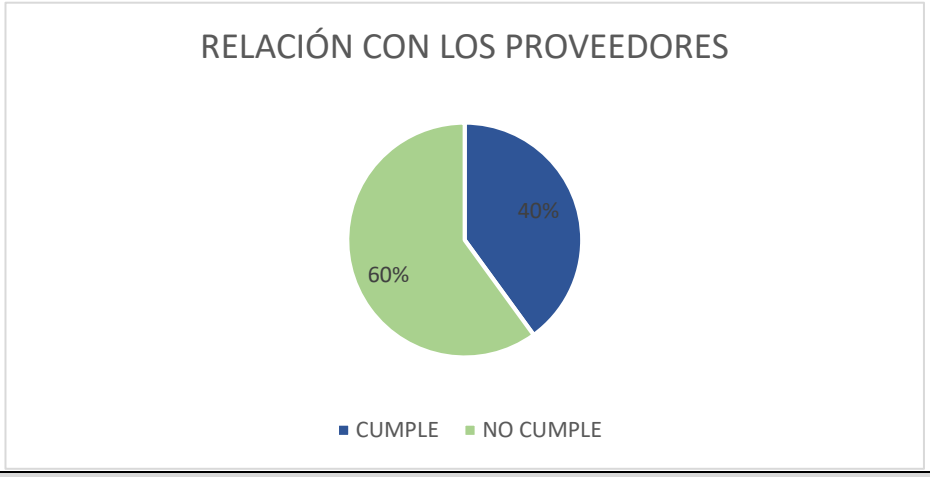
| A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.14.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN** | | | | | | | | |
| **A.14.1.1** | **Análisis de requisitos y especificaciones de seguridad de la información** | ¿Existen un análisis de los requisitos de seguridad de la información para nuevos sistemas o mejoras a los existentes? | NO | X | | | | No aplica. |
| **A.14.1.2** | **Asegurar los de servicios de aplicaciones en redes públicas** | Ante un eventual ataque a las redes, ¿poseen algún tipo de seguridad para protegerlas ante fraudes o robo de información? | NO | X | | | | No aplica. |
| **A.14.1.3** | **Protección de transacciones en servicios de aplicaciones** | Si al momento de transferir información se perdieran datos, ¿Se tiene algún plan de aseguramiento para que los datos no se pierdan? | NO | X | | | | No aplica. |
| **A.14.2. SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE** | | | | | | | | |
| **A.14.2.1** | **Política de desarrollo seguro** | ¿Cuentan con políticas la organización para el desarrollo de software / sistemas? | SI | | | | X | Con el modelo planteado y aplicado ya se cuenta con políticas para el desarrollo. |
| **A.14.2.2** | **Procedimientos de control de cambios del sistema** | ¿Toman en cuenta las políticas que tiene la organización al realizar ambos alo largo de ciclo de vida del desarrollo del software / sistemas? | NO | X | | | | No aplica. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.14.2.3** | **Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo** | ¿Se realiza la revisión técnica de aplicaciones críticas para el negocio? | NO | X | | | | No aplica. |
| **A.14.2.4** | **Restricciones sobre cambios a los paquetes de software** | ¿Cuentan con control de acceso al modificar el código fuente de los paquetes de software? | SI | | | X | | En proceso con el área de desarrollo |
| **A.14.2.5** | **Principios de ingeniería de sistemas seguros** | ¿Establecen procedimientos de ingeniería de sistemas de información? | NO | X | | | | No aplica. |
| **A.14.2.6** | **Entorno de desarrollo seguro** | ¿Se realiza la protección del ambiente de desarrollo para la integración de sistemas? | NO | X | | | | No aplica. |
| **A.14.2.7** | **Externalización del desarrollo de software** | ¿Se realiza monitoreo a los sistemas contratados externamente? | NO | X | | | | No aplica. |
| **A.14.2.8** | **Pruebas funcionales de la seguridad de sistemas** | ¿Se realizan las pruebas necesarias de la seguridad del sistema durante el desarrollo? | NO | X | | | | No aplica. |
| **A.14.2.9** | **Pruebas de aceptación del Sistemas** | ¿Realizan algún tipo de plan de pruebas de aceptación para los sistemas? | SI | | | | X | Con el plan de acción ya se aplican. |
| **A.14.3. DATOS DE PRUEBA** | | | | | | | | |
| **A.14.3.1** | **Protección de datos de prueba** | ¿Se protege los datos de prueba? | NO | X | | | | No aplica. |



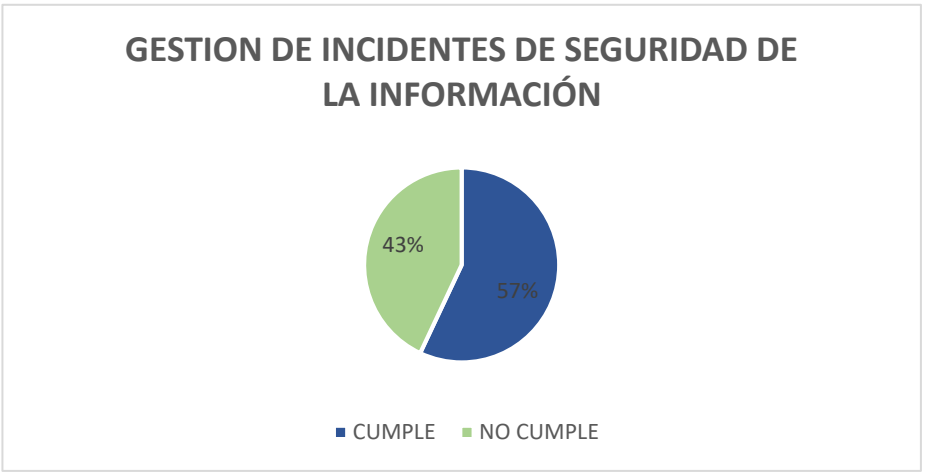

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.15. RELACION CON LOS PROVEEDORES** | | | | | | | | |
| **A.15.1. SEGURIDAD EN LAS RELACIONES CON PROVEEDORES** | | | | | | | | |
| **A.15.1.1** | **Política de seguridad de la información en las relaciones con los proveedores** | ¿Se realizan políticas de seguridad de la información por parte del proveedor hacia los activos que la organización posee? | SI | | X | | | Está en inicio con el modelo aplicado |
| **A.15.1.2** | **Requisitos de seguridad en contratos con terceros** | ¿Establece los requisitos de seguridad de la información con los proveedores acerca de la infraestructura de TI? | SI | | X | | | Está en inicio con el modelo aplicado |
| **A.15.1.3** | **Cadena de suministro de tecnología de la información y de la comunicación es** | ¿Los acuerdos con los proveedores incluyen requisitos para abordar los riesgos de la seguridad de la información? | SI | | X | | | Está en inicio con espoba la seguridad de la información |
| **A.15.2. GESTIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR** | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.15.2.1** | **Control y revisión de la provisión de servicios del proveedor** | ¿Se monitorea y/o audita la entrega de servicios por parte de los proveedores? | NO | | X | | | No aplica |
| **A.15.2.2** | **Gestión de cambios en la provisión del servicio del proveedor** | ¿Cuentan con un control ante la gestión de los cambios de provisión por parte de los proveedores? | NO | X | | | | No aplica |



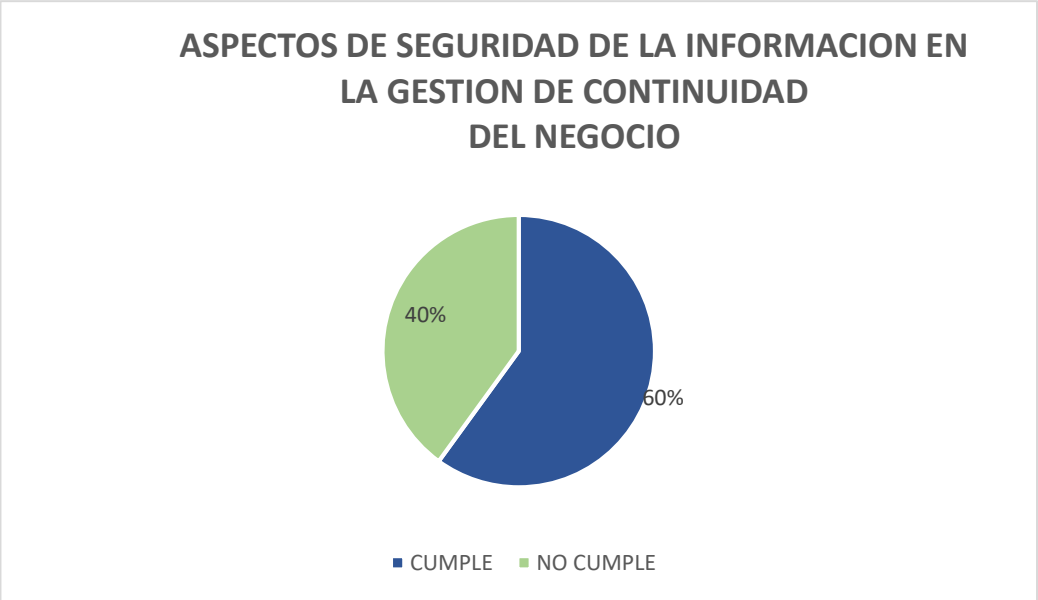

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.16. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** | | | | | | | | |
| **A.16.1. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS** | | | | | | | | |
| **A.16.1.1** | **Responsabilidades y procedimientos** | ¿Cuentan con una gestión de responsabilidades y procedimientos para los incidentes de seguridad de la información? | SI | | | | X | Ya se cuenta con gestión para los incidentes de seguridad de la información |
| **A.16.1.2** | **Notificación de los eventos de seguridad de la información** | ¿Se realizan reportes sobre los eventos de seguridad de la información? | SI | | | X | | Se aplicó auditoría |
| **A.16.1.3** | **Notificación de puntos débiles de la seguridad** | ¿Se realizan reportes sobre las debilidades de seguridad de la información? | SI | | X | | | Se aplicó auditoría |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.16.1.4** | **Evaluación y decisión sobre los eventos de seguridad de la información** | ¿Realiza evaluaciones sobre incidentes de seguridad de la información? | SI | | | X | | Se aplicó auditoría |
| **A.16.1.5** | **Respuesta a incidentes de seguridad de la información** | ¿Se responden a los incidentes de seguridad de la información de la organización? | SI | | X | | | Está en inicio |
| **A.16.1.6** | **Aprendizaje de los incidentes de seguridad de la información** | ¿Resuelve los incidentes con los conocimientos adquiridos? | SI | | X | | | Está en inicio |
| **A.16.1.7** | **Recolección de evidencias** | ¿Realiza con frecuencia la recolección de evidencia y recolección de información? | SI | | X | | | Esta en inicio del proceso seleccionado |



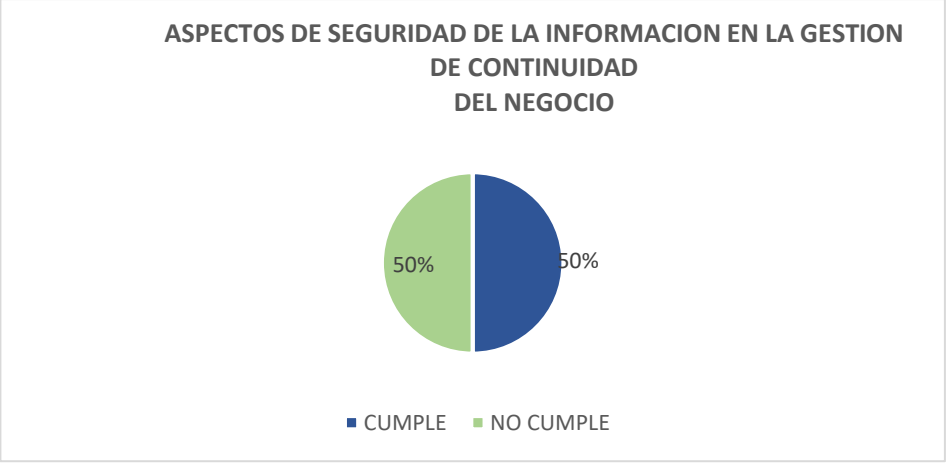

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE CONTINUIDAD DEL NEGOCIO** | | | | | | | | |
| **A.17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN** | | | | | | | | |
| **A.17.1.1** | **Planificación de continuidad de seguridad de la información** | ¿Cuentan con un plan en el cual determina los requisitos de seguridad de la información? | SI | | X | | | SÍ, está dentro de las políticas de seguridad de información. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.17.1.2** | **Implementación de continuidad de seguridad de la información** | ¿La organización cuenta con documentación, la cual busca implementar procesos, procedimientos y controles para asegurar la continuidad de la seguridad de la información? | SI | | | | X | Se aplicó medida de seguridad con respecto a la continuidad de la seguridad de la información |
| **A.17.1.3** | **Verificación, revisión y evaluación de continuidad de seguridad de la información** | ¿Se realiza una verificación, revisión y evaluación de los controles de continuidad de seguridad de la información? | SI | | | X | | Se aplico auditoría a través de un software desarrollado |
| **A.17.2. REDUNDANCIAS** | | | | | | | | |
| **A.17.2.1** | **Instalación de procesamiento de la información** | ¿Existe un plan para asegurar la disponibilidad de la información? | NO | X | | | | No aplica |



| A.18. CUMPLIMIENTO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.18.1. CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES** | | | | | | | | |
| **A.18.1.1** | **Identificación de requisitos contractuales y de legislación aplicables** | ¿Cuentan con requerimientos estatutarios, regulatorios y contractuales? | SI | X | | | | No se cuentan |
| **A.18.1.2** | **Derechos de propiedad intelectual DPI** | ¿Al implementar los procedimientos cuenta con el cumplimiento de los requisitos legislativos, normativos y contractuales? | NO | X | | | | No aplica |
| | | ¿La organización tiene procedimientos para asegurar la protección de la propiedad intelectual? | NO | X | | | | No aplica |
| | | ¿Se adquiere software de fuentes conocidas y de buena reputación? | NO | | X | | | No aplica |
| **A.18.1.3** | **Protección de registros** | ¿Tienen un plan en donde protegen los registros de la organización contra pérdidas, falsificación y publicaciones no autorizadas? | SI | | | X | | Se aplicaron planes de acciones con respecto a la seguridad de la información |
| **A.18.1.4** | **Privacidad y protección de datos personales** | ¿Existe un control para asegurar la protección de la data y privacidad de información personal? | SI | | | X | | Se aplicaron medidas de seguridad |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **A.18.1.5** | **Regulación de controles criptográficos** | ¿La organización utiliza un control de cifrado de la información para verificar el cumplimiento con los acuerdos, legislación y normativas que se emplean? | NO | X | | | | No aplica |
| **A.18.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES** | | | | | | | | |
| **A.18.2.1** | **Revisión independiente de la seguridad de la información** | ¿Existen una revisión independiente de la seguridad de la información? | SI | | X | | | Se aplico Auditoría a través de un software desarrollado |
| **A.18.2.2** | **Cumplimiento de políticas y normas de seguridad** | ¿Se ha identificado las causas de incumplimiento de las políticas y normas de seguridad en la organización? | SI | | | X | | Se dio reunión con el gerente general de la empresa para identificar el cumplimiento de las políticas de la seguridad de la información |
| **A.18.2.3** | **Revisión del cumplimiento técnico** | ¿Se han realizadopruebas de penetración y vulnerabilidad? | NO | X | | | | No aplica |



**Cuadro Porcentaje de Cumplimiento por Dominios Post Test**

| N° | DOMINIOS EVALUDOS SEGÚN ISO 27001 | ANALISIS INICIAL | |
|---|---|---|---|
| **A.5** | Políticas de seguridad de la información | **62.5%** | **Inicio** |
| **A.6** | Organización de la seguridad de la información | **47.2%** | **inicio** |
| **A.7** | Seguridad de los recursos humanos | **41.3%** | **Inicio** |
| **A.8** | Gestión de activos | **71%** | **Inicio** |
| **A.9** | Control de acceso | **45%** | **Inicio** |
| **A.10** | Criptografía | **0%** | **No aplica** |
| **A.11** | Seguridad física y ambiental | **31%** | **Inicio** |
| **A.12** | Seguridad de las operaciones | **55.6%** | **Inicio** |
| **A.13** | Seguridad de las comunicaciones | **60%** | **Inicio** |
| **A.14** | Adquisición, desarrollo y mantenimiento de sistemas | **90%** | **inicio** |
| **A.15** | Relación con los proveedores | **40%** | **Inicio** |
| **A.16** | Gestión de Incidentes de seguridad de la información | **57%** | **inicio** |
| **A.17** | Aspectos de seguridad de la información en la gestión de continuidad del negocio | **60%** | **Inicio** |
| **A.18** | Cumplimiento | **50%** | **Inicio** |

| TABLA DE RESUMEN | | | |
|---|---|---|---|
| INDICADOR: NUMERO DE CONTROLES | | | |
| N° CONTROLES TOTALES APLICAN/ EXISTEN | CONTROLES | PRE TEST (UND) | POST TEST (UND) TCA = 78 |
| 114 | NO EXISTE | 102 | 36 |
| | SI EXISTE | 12 | **78** |
| NO APLICA | | | |
| 36 | | | |

## ANEXO 12 PROCEDIMIENTO DE AUDITORIA

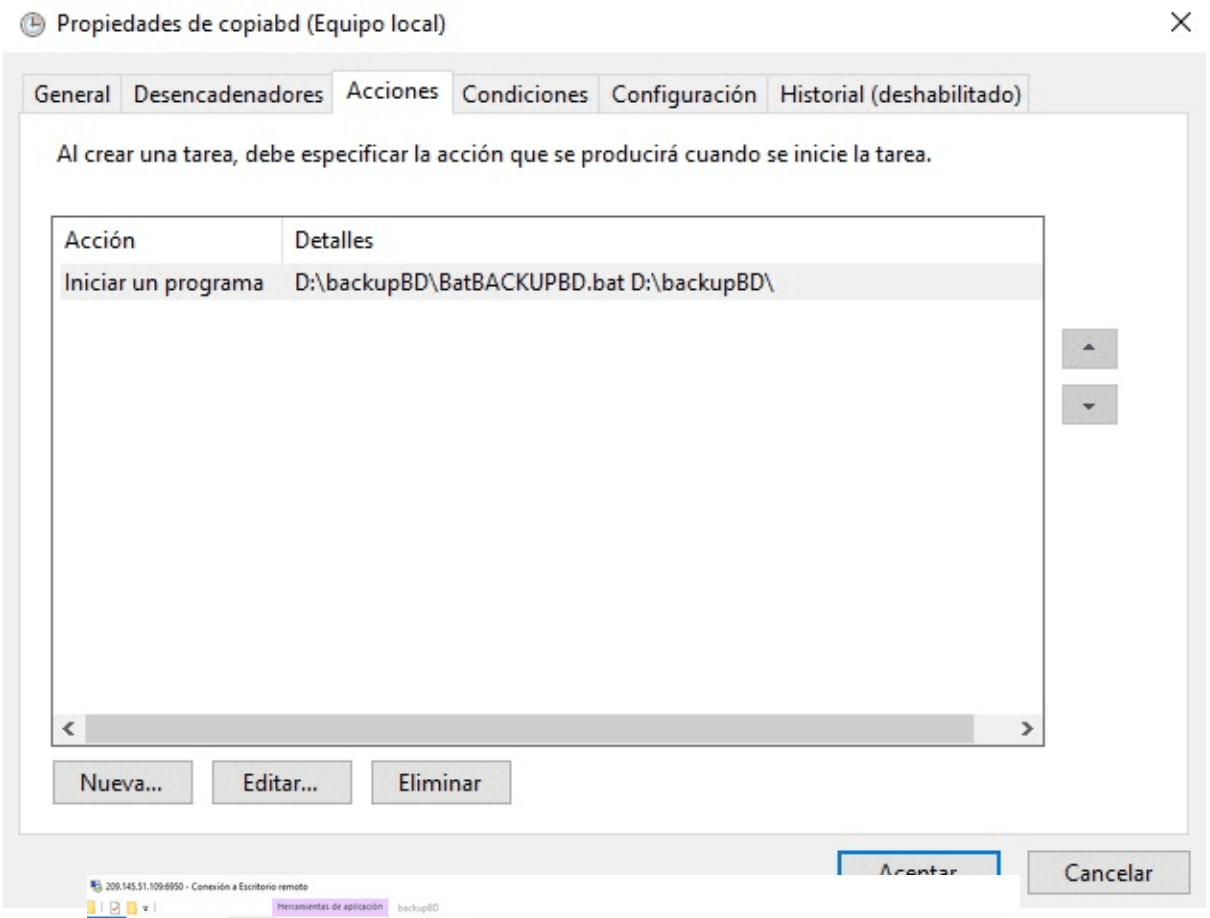
| N.º | Actividad | Descripción | Realiza | Registro |
|---|---|---|---|---|
| 1 | Planificar la auditoría | Planifica las auditorías a realizarse en el año mediante correo electrónico que se le enviará con anticipación a cada involucrado del área correspondiente | Gerente general | |
| 2 | Seleccionar Auditor | Selecciona, organiza y designa al personal que participará en la auditoría, el cual puede estar conformado por personal interno o externo que tenga calificación apropiada pararealizar auditorías y que no tengan compromiso directo con la actividad a auditar. Al seleccionarlo el gerente general asignará usuario al auditor interno para que puede ejecutar la auditoría. | Gerente general | |
| 4 | Ejecutar auditoría | El desarrollo de la auditoría contempla las siguientes etapas:<br>Reunión inicial: Antes de iniciar la auditoria, el Auditor Líder explica a los auditados el objetivo de la auditoria y en el software seleccionará las actividades que se realizarán.<br>Ejecución de la auditoría: Los Auditores proceden a recoger evidencias del proceso auditado a través de observacionesde las actividades y revisiones de registros, con la finalidad de verificar laimplementación del sistema y su eficacia. Se debe auditar teniendo en cuenta el alcance del SGSI de acuerdo a lo especificado en el Plan deAuditoría Interna.<br>Reunión de cierre: él auditor al culminar en él software tiene para poner comentarios e interactuar con los participantes a través del software, de las no conformidades y hallazgos detectados, así como las conclusiones de la auditoria. | Auditor | |
| 5 | Elaborar informe | Los auditores internos al terminar la reunión, tendrá acceso a descargar su informe en el software implementado de manera general. | Auditor | Informe de Auditoría Interna |
| 6 | Comunicar informe | El auditor tiene dos opciones, la cual la primera es imprimir su informe de su auditoría o solo a través del sistema puede ver el gerente general de lo que tema se trató y los participantes en esa reunión | Auditor | Acta de Reunión |
| 7 | Generar no conformidades, y oportunidades de mejora | Las no conformidades detectadas en la auditoría interna se pueden intercomunicar a través del software implementado. Donde se pueden hacer comentarios con respecto a lo que se observó en la auditoría | Auditor/Participantes | Monitoreo deNo Conformidades y Acciones Correctivas |

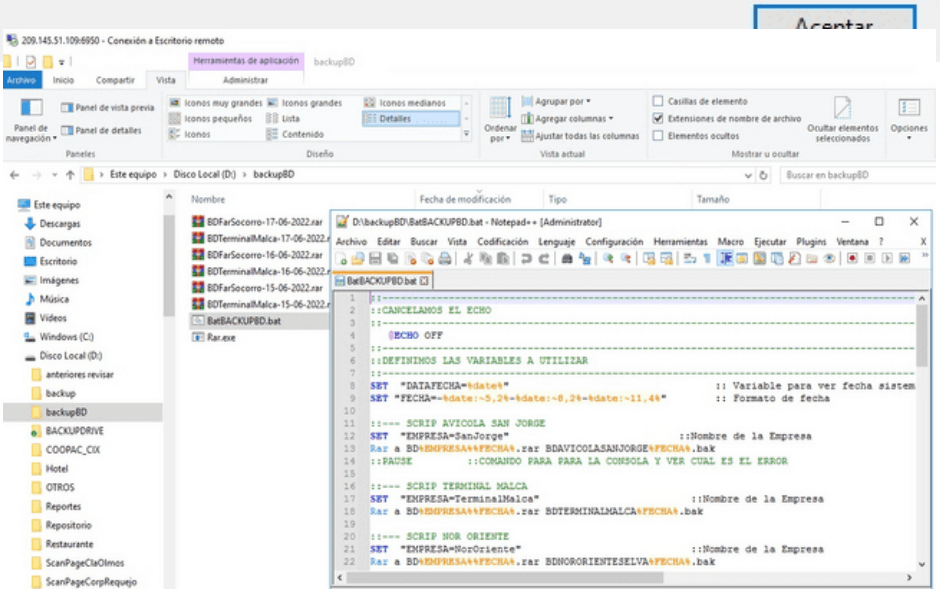
# ANEXO 13

# ETIQUETADO DE LA INFORMACION

# ANEXO 14

# SCRIPT DE COPIAS DE SEGURIDAD



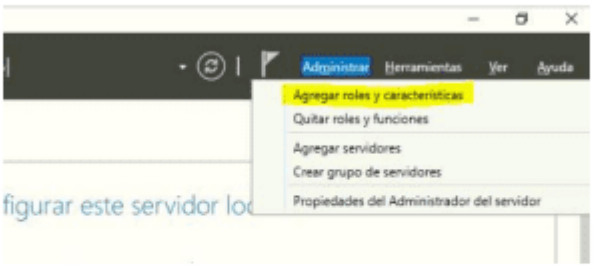



# ANEXO 15

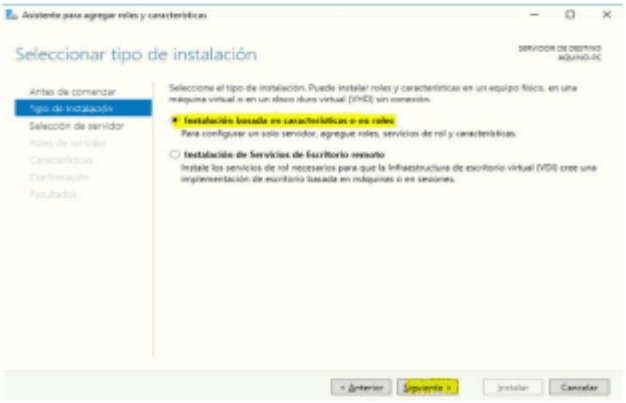
# MANUAL DE INSTALACION DEL SISTEMA

## 1. INSTALACION Y CONFIGURACION DEL IIS

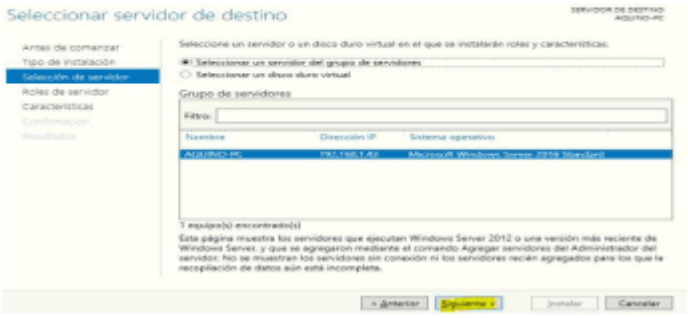
✓ **SI ESTAMOS EN WINDOWS SERVER**, vamos a panel de administrador del servidor y en administra selecionamos Agregar roles y caracteristicas



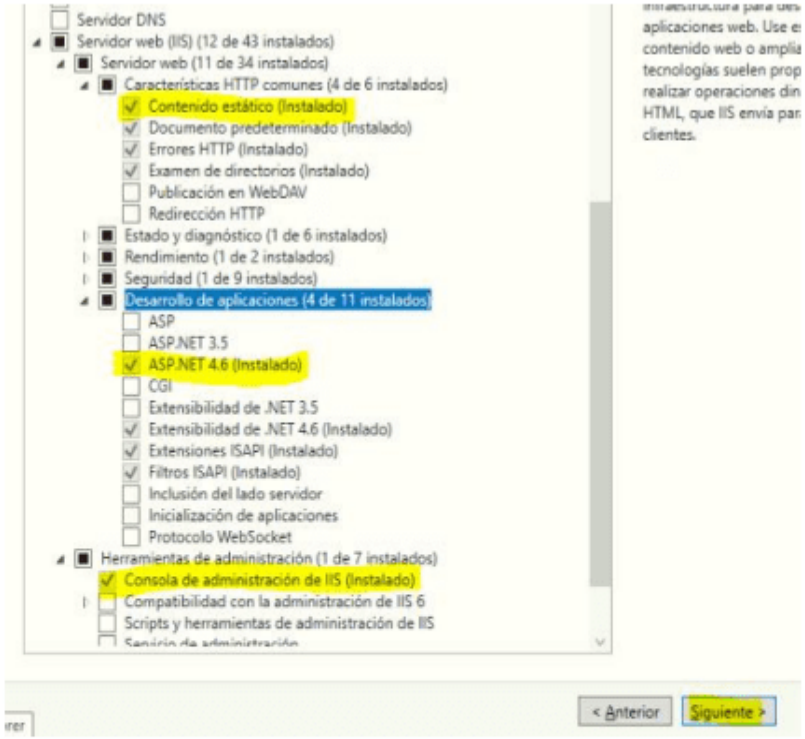

Damos click en siguiente




Damos click en siguiente

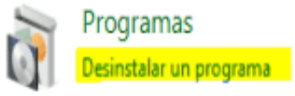


Selecionamos Servidor web(IIS) y nos aseguramos de que esten marcadas los siguientes items resaltados con amarillo sino lo estan los marcamos para que se agreguen luego click en siguiente

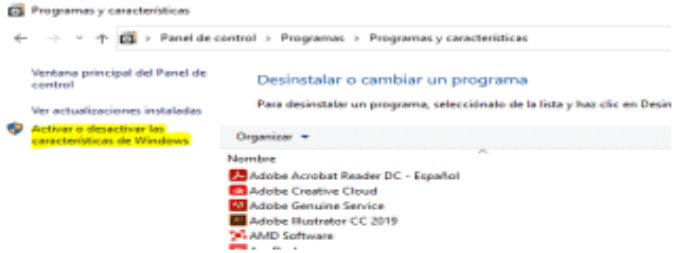



De aquí en adelate solo dar click en siguiente y cuando aparesca el boton de Instalar, **antes de dar click en instalar** asegurarte de que la casilla de reinicio automatico esta desactiva para evitar que el servidor se reinicie despues de instalar el rol ya que si estan trabajando en el sistema de escritorio podemos generar problemas, antes de reiniciar coordinar sobre ese tema, ya despues lo reiniciamos manualmente.

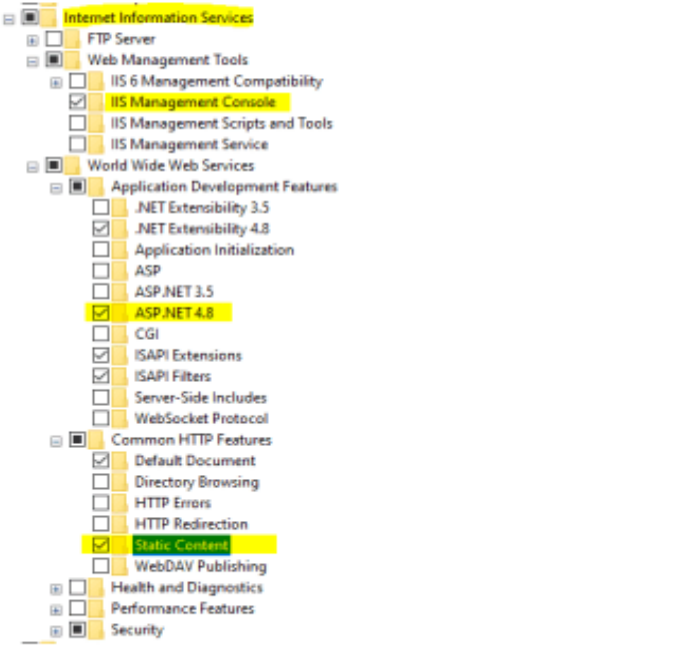
- ✓ **SI ESTAMOS EN WINDOWS DE ESCRITORIO**, vamos al panel de control en la seccion programas, desistalar un programa




Vamos a la seccion Activar o desactivar las caracteristicas de Windows




Se nos abrira una ventana , alli buscamos la **Internet Information Services** y verificamos que esten activos los siguientes items tal como se muestra en la imagen sin lo estan los activamos




Finalmente aceptamos y dejamos que termine de agregar las caracteristicas que marcamos si todo esta bien verificamos en el navegador si se instalo IIS escribimos: **localhost** y se deberia mostrar una pagina de bienvenida con informacion sobre IIS.

## 2. INSTALACION DE DEPENDENCIAS PARA EL FUNCIONAMIENTO DEL SISTEMA WEB.

Vamos a los siguientes link y descargamos los componentes y los instalamos justo en ese orde como los especifico uno a la vez no todos al mismo tiempo, si se solicita el reinicio por cada instalacion reiniciar la computadora antes de continuar para evitar errores.Consultar con adrian para guia sobre el proceso de instalacion de cada componente

**1.Descargar el .net framework 4.7.2 (la version develoment)**

https://dotnet.microsoft.com/download/dotnet-framework/net472

**2.visual studio 19 comunity**

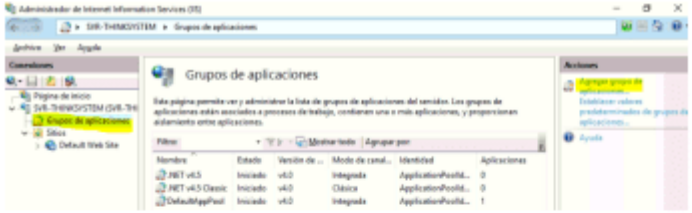
https://visualstudio.microsoft.com/es/downloads/

**cristal report version 26**

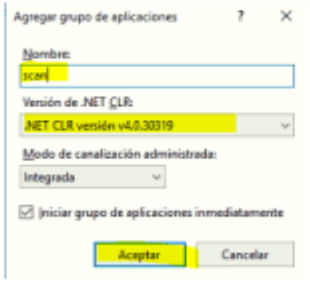
https://drive.google.com/file/d/1jw7FBzBXZlYWwRjA2N-y2Q9xvLiDRTIT/view

## 3. CREACION DEL GRUPO DE APLICACIÓN

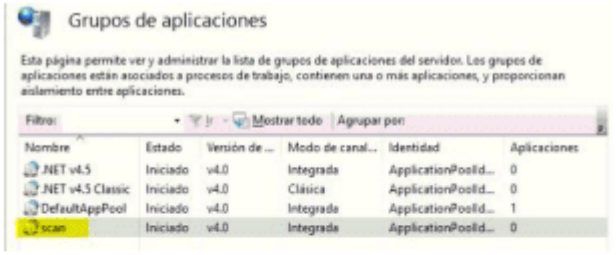
Abrimos el panel de administracion del IIS y en grupo de aplicaciones en la seccion de acciones damos click en **Agregar grupo de aplicaciones**



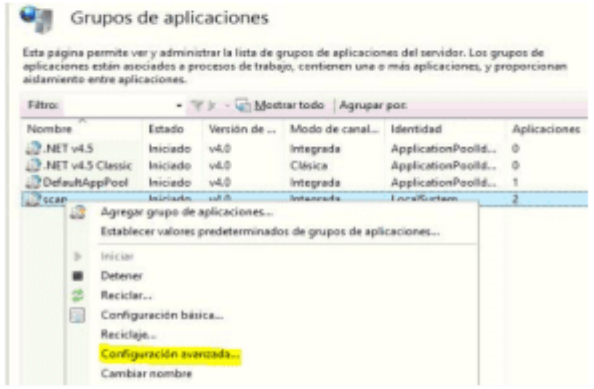

Configuramos tal y como aparece en la siguiente imagen y luego damo click en aceptar



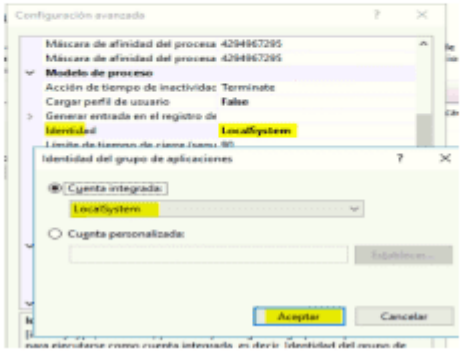

Se nos creara el grupo de aplicación llamado **scan**.



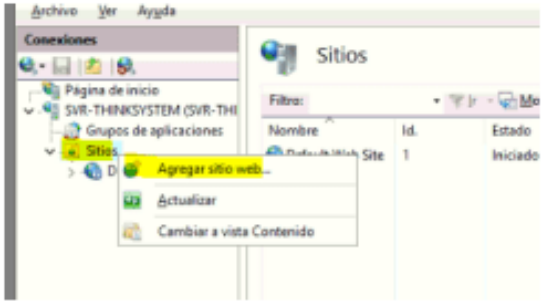

luego damos anticlick sobre él y vamos a Configuración avanzada



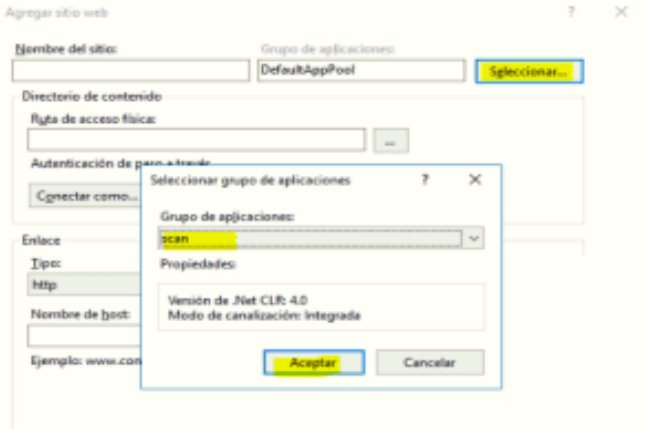

Y en el apartado identidad selecionamos LocalSystem, y luuego damos click en aceptar y aceptar



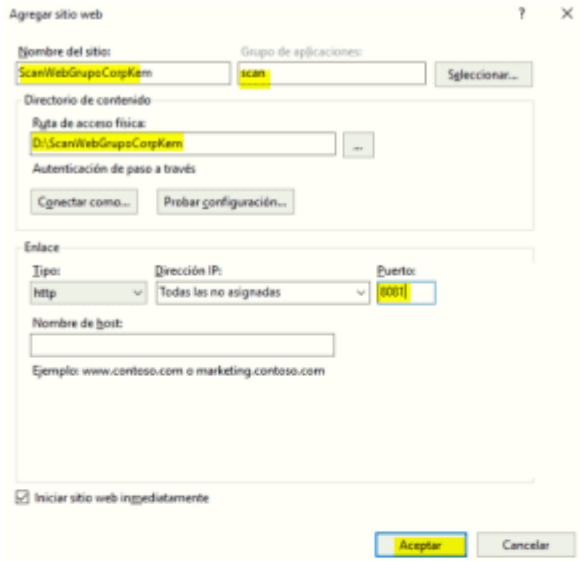
En en el apartado de Sitios damos anticlick y Agregar sitio web, previamente ya debimos haber descomprimido los archivos del sistema web en algun lugar del disco.



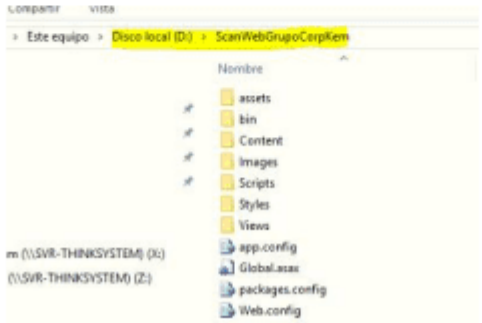

Damos click en el boton Seleccionar y selecionamos el grupo de aplicación que previamente creamos y aceptamos.



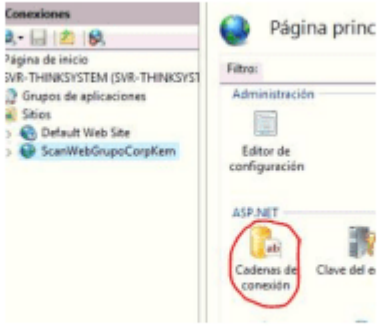

Agregamos como se va ha llamar nuestra aplicación en nombre del sitio, buscamos la ruta donde esta descomprimido los archivos del sistema web en ruta de acceso fisica definimos el puerto y por ultimo aceptamos.



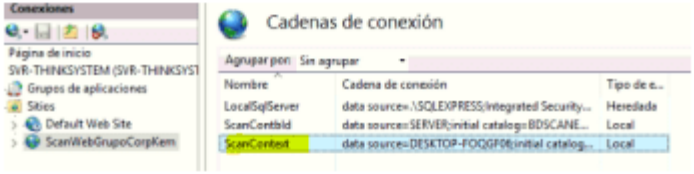

Para este ejemplo la ruta del sistema web esta en el disco D, se recomienda no descomprimir en sistema en el disco C donde se instalan los programas sino en una unidad de disco diferente



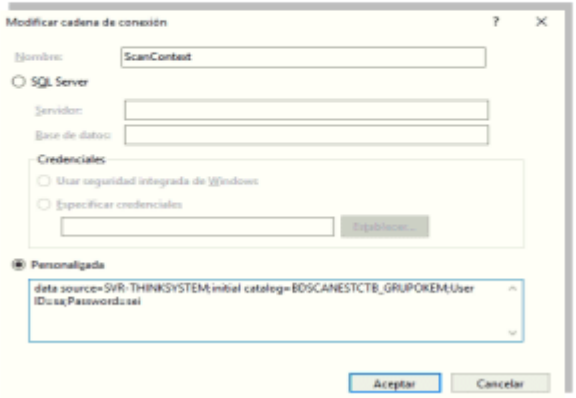
Cuando dimos aceptar se nos creara el sitio web con el nombre que le pusimos,damos click sobre él y vamos a la opcion que aparece en la imagen para configurar la cadena de conexión a la base de datos, damos doble click sobre Cadenas de conexión.



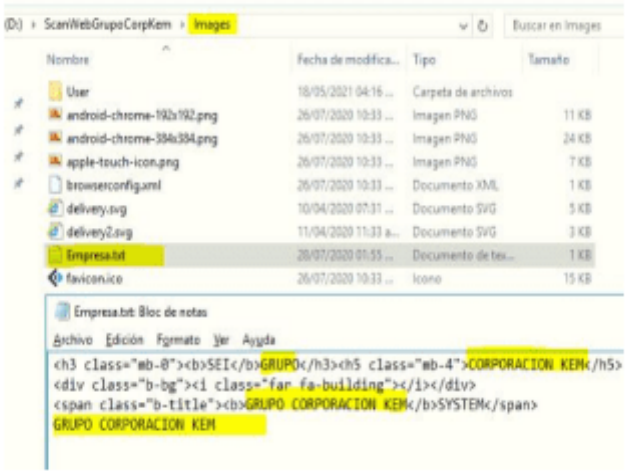

Solo en el apartado **ScanContext** , se configuran los parametros de conexión damos doble click sobre el



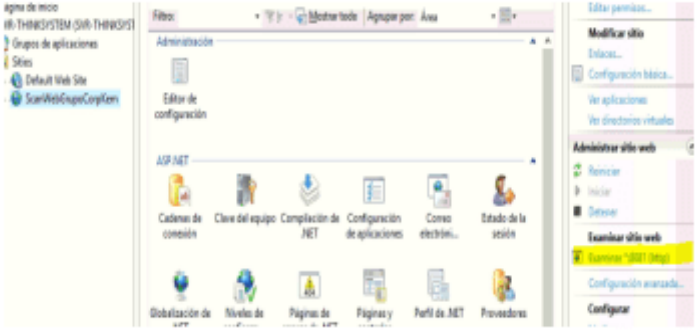

En **catalog** coloamos el nombre de la base de datos, **userID** el nombre de usuario de conexión a la BD que en este caso es sa y finalmente en **Password** la contraseña de conexión a la BD




Configuracion del Nombre de presentacion cuando iniciemos la aplicación y sepresente en el navegador web, vamos al directorio donde descomprimimos el sistema web dentro de la carpeta **Images** buscamos el archivo Empresa.txt y las secciones sobreados colocamos el nombre de la empresa




Finalmete iniciamos la aplicación desde la sección **Examinar sitio web,** si todo esta bien se nos abrira el navegado y nos mostrara la patalla de inicio de sesion.



## ANEXO 16 CONTROLES DE LA ISO/IEC 27001:2013

**A.5 Políticas de Seguridad de la Información**

**5.1** Directrices de gestión de la Seguridad de la Información

**A.5.1.1** Políticas para la Seguridad de la Información

**A.5.1.2** Revisión de las Políticas para la Seguridad de la Información

**A.6 Organización de la Seguridad de la Información**

**6.1** Organización Interna

**A.6.1.1** Roles y responsabilidades en seguridad de la información

**A.6.1.2** Segregación de tareas

**A.6.1.3** Contacto con las autoridades

**A.6.1.4** Contacto con grupos de interés especial

**A.6.1.5** Seguridad de la información en la gestión de proyectos

**6.2** Los dispositivos móviles y el teletrabajo

**A.6.2.1** Política de dispositivos móviles

**A.6.2.2** Teletrabajo

**A.7 Seguridad relativa a los recursos humanos**

**7.1** Antes del empleo

**A.7.1.1** Investigación de antecedentes

**A.7.1.2** Términos y condiciones del empleo

**7.2** Durante el empleo

**A.7.2.1** Responsabilidades de gestión

**A.7.2.2** Concienciación, educación y capacitación en seguridad de la información

**A.7.2.3** Proceso disciplinario

**7.3** Finalización del empleo o cambio en el puesto de trabajo

**A.7.3.1** Responsabilidades ante la finalización o cambio

**A.8 Gestión de Activos**

**8.1** Responsabilidad sobre los activos

**A.8.1.1** Inventario de activos

**A.8.1.2** Propiedad de los activos

**A.8.1.3** Uso aceptable de los activos

**A.8.1.4** Devolución de activos

**8.2** Clasificación de la Información

**A.8.2.1** Clasificación de la información

**A.8.2.2** Etiquetado de la información

**A.8.2.3** Manipulado de la información

**8.3** Manipulación de los soportes

**A.8.3.1** Gestión de soportes extraíbles

**A.8.3.2** Eliminación de soportes

**A.8.3.3** Soportes físicos en tránsito

**A.9 Control de Acceso**

**9.1** Requisitos del negocio para el control de acceso

**A.9.1.1** Política de control de acceso

**A.9.1.2** Acceso a las redes y a los servicios de red

**9.2** Gestión de acceso de usuario

**A.9.2.1** Registro y baja de usuarios

**A.9.2.2** Provisión de acceso de usuario

**A.9.2.3** Gestión de privilegios de acceso

**A.9.2.4** Gestión de la información de secreta de autenticación de los usuarios
**A.9.2.5** Revisión de los derechos de acceso de usuario
**A.9.2.6** Retirada o reasignación de los derechos de acceso
**9.3** Responsabilidades del usuario
**A.9.3.1** Uso de la información secreta de autenticación
**9.4** Control de acceso a sistemas y aplicaciones
**A.9.4.1** Restricción del acceso a la información
**A.9.4.2** Procedimientos seguros de inicio de sesión
**A.9.4.3** Sistema de gestión de contraseñas
**A.9.4.4** Uso de utilidades con privilegiados del sistema
**A.9.4.5** Control de acceso al código fuente de los programas

**A.10 Criptografía**
**10.1** Controles Criptográficos
**A.10.1.1** Política de uso de los controles criptográficos
**A.10.1.2** Gestión de claves
**A.11 Seguridad Física y del entorno**
**A.11.1** Áreas seguras
**A.11.1.1** Perímetro de seguridad física
**A.11.1.2** Controles de físicos de entrada
**A.11.1.3** Seguridad de oficinas, despachos y recursos
**A.11.1.4** Protección contra las amenazas externas y ambientales
**A.11.1.5** El trabajo en áreas seguras
**A.11.1.6** Áreas de carga y descarga
**A.11.2 Seguridad de los equipos**
**A.**11.**2.1** Emplazamiento y protección de equipos
**A.11.2.2** Instalaciones de suministro
**A.11.2.3** Seguridad del cableado
**A.11.2.4** Mantenimiento de los equipos
**A.11.2.5** Retirada de materiales propiedad de la empresa
**A.11.2.6** Seguridad de los equipos fuera de las instalaciones.
**A.11.2.7** Reutilización o eliminación segura de equipos
**A.11.2.8** Equipo de usuario desatendido
**A.11.2.9** Política de puesto de trabajo despejado pantalla limpia
**A.12 Seguridad de las Operaciones**
**A.12.1** Procedimientos y responsabilidades operacionales
**A.12.1.1** Documentación de procedimientos de operación.
**A.12.1.2** Gestión de cambios
**A.12.1.3** Gestión de capacidades
**A.12.1.4** Separación de los recursos de desarrollo, prueba y operación
**A.12.2** Protección contra el software malicioso (malware)
**A.12.2.1** Controles contra el código malicioso
**A.12.3 Copias de seguridad**
**A.12.3.1** Copias de seguridad de la información
**A.12.4 Registros y supervisión**
**A.12.4.1** Registro de Eventos
**A.12.4.2** Protección de la información de registro
**A.12.4.3** Registros de administración y operación

**A.12.4.4** Sincronización del Reloj

**A.12.5 Control del software en explotación**

**A.12.5.1** Instalación de software en explotación

**A.12.6 Gestión de la vulnerabilidad técnica**

**A.12.6.1** Gestión de las vulnerabilidades técnicas

**A.12.6.2** Restricciones en la instalación de software

**A.12.7 Consideraciones sobre la auditoría de sistemas de información**

**A.12.7.1** Controles de auditoría de sistemas de información

**A.13 Seguridad de las Comunicaciones**

**A.13.1** Gestión de la seguridad de redes

**A.13.1.1** Controles de red

**A.13.1.2** Seguridad de los servicios de red

**A.13.1.3** Segregación en redes

**A.13.2** Intercambio de información

**A.13.2.1** Políticas y procedimientos de intercambio de información

**A.13.2.2** Acuerdos de intercambio de información

**A.13.2.3** Mensajería electrónico

**A.13.2.4** Acuerdos de confidencialidad o no revelación

**A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información**

**A.14.1** Requisitos de seguridad en sistemas de informacion

**A.14.1.1** Análisis de requisitos y especificaciones de Seguridad de la información

**A.14.1.2** Asegurar los servicios de aplicaciones en redes públicas

**A.14.1.3** Protección de las transacciones de servicios de aplicaciones

**A.14.2** Seguridad en el desarrollo y en los procesos de soporte

**A.14.2.1** Política de desarrollo seguro

**A.14.2.2** Procedimiento de control de cambios en sistema

**A.14.2.3** Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

**A.14.2.4** Restricciones a los cambios en los paquetes de software

**A.14.2.5** Principios de ingeniería de sistemas de seguros

**A.14.2.6** Entorno de desarrollo seguro

**A.14.2.7** Externalización del desarrollo de software

**A.14.2.8** Pruebas funcionales de seguridad del sistema

**A.14.2.9** Pruebas aceptación de sistema

**A.14.3** Datos de prueba

**A.14.3.1** Protección de los datos de prueba

**A.15 Relación con Proveedores**

**15.1** Seguridad en las relaciones con los proveedores

**A.15.1.1** Política de seguridad de la información en las relaciones con los proveedores

**A.15.1.2** Requisitos de seguridad en contratos con terceros

**A.15.1.3** Cadena de suministro de tecnología de la información y de las comunicaciones

**15.2** Gestión de la provisión de servicios del proveedor

**A.15.2.1** Control y revisión de la provisión de servicios del proveedor

**A.15.2.2** Gestión cambios en la provisión del servicio del proveedor

**A.16 Gestión de Incidentes de Seguridad de la Información**

**A.16.1** Gestión de incidentes de seguridad de la información y mejoras

**A.16.1.1** Responsabilidades y procedimientos

**A.16.1.2** Notificación de los eventos de seguridad de la información

**A.16.1.3** Notificación de puntos débiles de seguridad

**A.16.1.4** Evaluación y decisión sobre los eventos de seguridad de información

**A.16.1.5** Respuesta a incidentes de seguridad de la información

**A.16.1.6** Aprendizaje de los incidentes de seguridad de la información

**A.16.1.7** Recopilación de evidencias

**A.17 Aspectos de Seguridad de la Información para la gestión de la continuidad del negocio**

**A.17.1** Continuidad de la seguridad de la Información

**A.17.1.1** Planificación de la continuidad de la seguridad de la información

**A.17.1.2** Implementar la continuidad de la seguridad de la información

**A.17.1.3** Verificación, revisión y evaluación de la continuidad de la seguridad de la información

**A.17.2** Redundancias

**A.17.2.1** Disponibilidad de los recursos de tratamiento de la información

**A.18 Cumplimiento**

**A.18.1** Cumplimiento de los requisitos legales y contractuales

**A.18.1.1** Identificación de la legislación aplicable y de los requisitos contractuales

**A.18.1.2** Derechos de propiedad intelectual (DPI)

**A.18.1.3** Protección de los registros de la organización

**A.18.1.4** Protección y privacidad de la información de carácter personal

**A.18.1.5** Regulación de los controles criptográficos

**18.2 Revisiones de seguridad de información**

**A.18.2.1** Revisión independiente de la seguridad de la información

**A.18.2.2** Cumplimiento con las políticas y normas de seguridad

**A.18.2.3** Comprobación del cumplimiento técnico

## ANEXO 17 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

SEISYSTEM
CONSULTORES
DE: SECLEN ENEQUE LUIS FERNANDO

Alfonso Ugarte 633 Dpto 205
Lambayeque - Chiclayo - Chiclayo
(074) 476790 - 978815887
www.seisystemperu.com
ventas@seisystemperu.com

**Venta de computadoras, impresoras, suminitros y accesorios.**
**Asesoramiento e instalación de redes - Soporte técnico - Desarrollo de sistemas**

**POLITICA DE SEGURIDAD DE INFORMACION**

En SEISYSTEM COSULTORES. nos dedicamos a ofrecer servicios especializados a empresas, brindando soluciones integrales de alto nivel en Tecnologías de Información y en el ámbito Empresarial, consideramos que la información es un activo de vital importancia, por esto su confidencialidad, disponible e integridad es primordial para realizar nuestras actividades organizacionales.

Demostramos nuestro compromiso con nuestros clientes implementando, manteniendo y mejorando continuamente un sistema de gestión de seguridad de la información, cumpliendo a cabalidad cada uno de sus requisitos con el fin de alcanzar un buen nivel de satisfacción con el cliente.

Esta política incluye los siguientes objetivos de seguridad de la información:

- Fortalecer la confianza de nuestros clientes y trabajadores mediante medidas de seguridad apropiadas.
- Reducir los incidentes de la seguridad de la información reportados a niveles aceptables.
- Mantener la política de seguridad actualizada en la organización, con el objetivo de garantizar su vigencia y nivel de eficiencia.

Estamos comprometidos a asegurar el éxito de nuestra política y el logro de nuestros objetivos, comprendiendo que la participación y el compromiso de nuestros colaboradores son de alta relevancia por lo que se delegan y disponen de recursos necesarios para la difusión y comprensión de esta política como parte fundamental en nuestros servicios.

GERENTE GENERAL

Luis Fernando Seclen Eneque
Sei System Consultores
GERENTE GENERAL