UNIVERSIDAD CÉSAR VALLEJO

# FACULTAD DE INGENIERÍA Y ARQUITECTURA

## ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de un sistema de gestión de seguridad basada en la ISO 27001 para reducir el riesgo ante ataques cibernéticos en la empresa System Arq S.R.L, Lima 2023

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:**

Ingeniero de Sistemas


**AUTORES:**

Huamani Rubio, Angel Jony (orcid.org/0000-0002-3814-2499)

Liza Velásquez, Johnny Pablo (orcid.org/0000-0002-1706-5471)

**ASESOR:**

Mg. Galvez Tapia, Orleans Moisés (orcid.org/0000-0002-4352-9495)


**LÍNEA DE INVESTIGACIÓN:**

Auditoria de Sistemas y Seguridad de la Información

**LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:**

Desarrollo económico, empleo y emprendimiento

**LIMA – PERÚ**

**2023**

## DEDICATORIA

Dedicamos este trabajo a nuestras familias por estar siempre presentes, acompañándonos y por el apoyo moral, que nos brindaron a lo largo de esta etapa de nuestras vidas.

A todas las personas que nos han apoyado y han hecho que el trabajo se realice con éxito, en especial a aquellos que nos abrieron las puertas y compartieron sus conocimientos.

**AGRADECIMIENTO**

Queremos agradecer principalmente a Dios, por ser el inspirador de nuestras vidas y ayudarnos para conseguir nuestros más grandes anhelos.

# ÍNDICE DE CONTENIDOS

## ÍNDICE DE TABLAS

## ÍNDICE DE FIGURAS

RESUMEN

El avance de las tecnologías de la información se ha visto incrementado de manera continua y a gran escala a nivel mundial, junto a ello surgen múltiples riesgos de seguridad a través de intentos de ataques cibernéticos y a ello se suma las vulnerabilidades en los datos, principalmente en empresas que no invierten en sistemas de protección. La empresa System Arq, presentó inconsistencias en el resguardo de datos, integridad y confiabilidad de la información, por lo que se volvió vulnerable ante cualquier ataque cibernético. Ante esta situación, mediante este trabajo investigativo se demostró como la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el riesgo ante ataques cibernéticos.

En la presente investigación el diseño es el experimental de tipo pre experimental con un enfoque cuantitativo y relacionada al tipo aplicado, donde se buscó obtener resultados referentes a la implementación de un sistema de gestión de seguridad basada en la norma ISO 27001 para reducir el riesgo ante ataques cibernéticos en la empresa system Arq S.R.L. Se trabajó con una muestra de 30 activos de información en la organización. Respecto a la recolección de los datos, se utilizó la guía de observación y fichas de registro los cuales fueron validadas y donde se determinó si la hipótesis de la investigación es aceptada o denegada.

Palabras clave: Ataques cibernéticos, ISO 27001, Tecnologías de la información

ABSTRACT

The advancement of information technologies has increased continuously and on a large scale worldwide, along with this multiple security risks arise through attempted cyber attacks and to this are added vulnerabilities in data, mainly in companies. that do not invest in protection systems. The company System Arq presented inconsistencies in data protection, integrity and reliability of information, making it vulnerable to any cyber attack. Given this situation, through this investigative work it was demonstrated how the implementation of an information security system based on the ISO 27001 standard reduces the risk of cyber attacks.

In this research, the design is the experimental pre-experimental type with a quantitative approach and related to the type applied, where we sought to obtain results referring to the implementation of a security management system based on the ISO 27001 standard to reduce the risk of cyber attacks on the company system Arq S.R.L. We worked with a sample of 30 attacks that occurred in the organization. Regarding data collection, the observation guide was used, which was validated by experts where it was determined whether the research hypothesis is accepted or denied.

Keywords: Cyber attacks, ISO 27001, Information technologies

# I. INTRODUCCIÓN

A nivel mundial, la norma ISO 27001 ha permitido grandes éxitos en gestión de seguridad de la información por lo que se recomienda el uso de esta norma. Se considera que la información es el máximo valor, la cual es muy importante que sea protegido para evitar ataques cibernéticos, por lo que se deben cumplir principios básicos para la seguridad de la información y evitar que la organización sea perjudicada y calificada con malos comentarios por sus vulnerabilidades de seguridad. Para establecer un alto estándar de seguridad en la empresa, se debe realizar diversos análisis y auditorías que permitan obtener información de cómo realmente se encuentra la organización para posteriormente con ayuda de la norma ISO 27001 blindar la información y aprovechar sus recomendaciones para elevar la seguridad y confidencialidad en la empresa (Razikin y Soewito, 2022, p. 383).

Se puede indicar que desde la aparición del Reglamento General de Protección de Datos, las entidades que certifican el nivel de seguridad han presentado un aumento significativo, ello se debe a que las empresas se encuentran prácticamente obligadas de potenciar su sistema de seguridad de privacidad, por lo que aplican estándares internacionales que se enfoque en Seguridad de la información como lo es la ISO 27001, demostrando de esta manera que son una organización confiable e íntegra para proteger la data que la organización tenga de sus clientes (Viguri, 2021, p. 6).

Por consiguiente, cuando una empresa privada o pública presenta vulnerabilidades de seguridad es un incentivo para actuar y proceder ante el ataque cibernético, de esta manera elevar los niveles de seguridad que permitan proteger la información. Para identificar el comportamiento de las vulnerabilidades que suceden dentro de una organización, se recomienda utilizar buenas prácticas de seguridad como los estándares de la ISO 27001 (Tasa, Maquera, Rojas, Delgado, 2022, p. 13).

Asimismo, cualquier empresa que su rubro sea el de tecnología, se encuentra expuesto a diferentes ataques por parte de los ciberdelincuentes que están en búsqueda de secuestrar datos e información almacenada en los servidores para posteriormente solicitar dinero a cambio de devolver la data, es por ello que se plantea implementar los estándares de la norma ISO 27001. Ello

ayudará a disminuir los riesgos de ataques y evitar la filtración de datos e información que se encuentra en los servidores (Rizky, Guntur y Oktaria, 2023, p. 1).

Por otra parte, Togu y Kalamullah (2022) indicaron que toda entidad debe manejar un máximo nivel de protección de información y evitar el manejo inadecuado de datos, inapropiado funcionamiento de los equipos informáticos, burlas a la seguridad privada, entre otras vulnerabilidades que se puedan presentar. Por lo que se considera desarrollar mediante estándares internacionales como la ISO 27001, una barrera de seguridad para resguardar la información, sirviendo de gran ayuda para la imagen de la organización, además en lo que respecta a la seguridad, logre reducir riesgos o ataques cibernéticos que actualmente son comunes, asimismo buscar que las conexiones de punto a punto sean seguras (p. 380).

En la actualidad una de las cuestiones más relevantes para las organizaciones es determinar de qué manera proteger toda la información confidencial, ello debido a la creciente cantidad de ataques cibernéticos y filtraciones de datos que los amenazan. Proteger la información digital se refiere a la capacidad de mantener las operaciones de una organización frente a múltiples ataques y situaciones inesperadas, por lo que es esencial para enfrentar estas amenazas de seguridad. Los estándares y certificaciones de ciberseguridad están disponibles para garantizar que los proveedores de tecnología de la información y la comunicación (TIC) desarrollen y fabriquen productos seguros. Además, estas normas pueden proporcionar a los consumidores garantías de seguridad de sus sistemas informáticos (Sun *et al.,* 2022, p. 71749).

Últimamente, se han dado innumerables ataques cibernéticos en la industria de la salud, causando enormes pérdidas de información bastante sensible para los pacientes, luego de identificar las vulnerabilidades en cada etapa del flujo de datos, se clasifican los ciberataques y se exponen diversas metodologías de ciberseguridad (Razaque *et al.,* 2019, p. 168774). También se ha demostrado que las pequeñas y medianas empresas son una base importante para la economía de muchos países, sin embargo, dichas actividades no están

implementadas de manera eficiente desde una perspectiva de ciberseguridad, lo que los pone en el blanco de los ataques cibernético (Chidukwani, Zander y Koutsakis, 2022, p. 85701).

En los últimos años en el Perú, se produjeron muchos errores de ciberseguridad. Ante este problema se realizó un escaneo de red utilizando diversas herramientas lo cual permite detectar e identificar vulnerabilidades para mitigarlas y evitar intrusiones maliciosas y averiguar posibles soluciones para evitar pérdidas de información y ataques al sistema (Serna, Montoya, Quintero, Henao y Castro, 2022, p. 135).

Actualmente, el incremento de ataques cibernéticos se encuentra en auge y las brechas de seguridad nos plantean preocupaciones y exige nuevas herramientas para sostener y reducir el riesgo. Esto se ha traducido en nuevas regulaciones y diversos protocolos y normas de derecho indicativo que buscan establecer mecanismos de control para un uso más seguro de este tipo de medios (Íscar y Barriga, 2022, p. 87).

Asimismo, los ataques cibernéticos a personas y empresas se han multiplicado de manera exponencial, produciendo miles de dólares en pérdidas y afectando incluso a organismos estatales. Debido al incremento de fraudes es indispensable buscar alternativas de seguridad para reducir el riesgo ante esta amenaza. En el Perú miles de personas y empresas no cuentan con un departamento de ciberseguridad o se encuentran apenas en proceso de implementación (Cando y Medina, 2021, p. 18).

System Arq. Inició funciones el 13 de enero de 1994, brinda el servicio de actividades de arquitectura e ingeniería, consultoría y gestión de instalaciones informáticas, rastreo satelital a vehículos mediante equipos GPS. Ubicada en Av. Grau N°1123 – Barranco. (Ver anexo 7). La Empresa presenta inconsistencias en el resguardo de datos, integridad y confiabilidad de la información, tal es el caso que se detectó a ex trabajadores los cuales seguían manteniendo acceso remoto al servidor, además de ello el data center no cuenta con el ambiente adecuado para el funcionamiento ni control del registro del personal autorizado al área de servidores, por lo que se vuelve vulnerable ante cualquier ataque cibernético.

La cantidad de ataques cibernéticos dirigidos a individuos y empresas ha crecido de manera exponencial, causando pérdidas financieras significativas y afectando incluso a entidades gubernamentales. Con el aumento de estas prácticas fraudulentas, se hace necesario encontrar soluciones de seguridad para minimizar el riesgo frente a esta amenaza.

La justificación teórica se lleva a cabo con el fin de contribuir al conocimiento actual acerca de la utilización de la norma ISO 27001 como técnica de protección ante ataques cibernéticos, cuyas conclusiones podrán sistematizarse en una propuesta, para ser incorporado en los sistemas de seguridad, ya que se estaría demostrando que el uso de la norma mejora el nivel de protección de la seguridad informática.

La justificación práctica se fundamenta en la relevancia de adoptar un sistema de gestión de seguridad basado en la ISO 27001, el cual permitirá reducir el riesgo ante las de amenazas cibernéticas sin la necesidad de invertir elevadas sumas de dinero en mantener la información a buen recaudo o crear una planilla excesivamente grande.

La justificación metodológica posibilita el fortalecimiento de la auditoría de los controles mediante la utilización de técnicas y ejercicios aplicados con determinadas metodologías para el tratamiento de riesgos, mediante la aplicación de las mejores prácticas establecidas en la norma ISO 27001, que evidencian su efectividad y confiabilidad.

El problema general de la investigación es: ¿De qué manera la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el riesgo ante ataques cibernéticos en la empresa System Arq, Lima-2023? Los problemas específicos planteados son:

- PE1: ¿De qué manera la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 determina el porcentaje de ataques malware como parte de los ataques cibernéticos en la empresa System Arq, Lima 2023?
- PE2: ¿De qué manera la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 determina el porcentaje de

vulnerabilidades en los activos de información ante ataques cibernéticos en la empresa System Arq, Lima 2023?

El objetivo general es: Demostrar que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el riesgo ante ataques cibernéticos en la empresa System Arq, Lima-2023. Los problemas específicos planteados son:

- OE1: Demostrar que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 influye en el porcentaje de ataques malware como parte de los ataques cibernéticos en la empresa System Arq, Lima 2023.
- OE2: Demostrar que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 influye en el porcentaje de vulnerabilidades en los activos de información ante ataques cibernéticos en la empresa System Arq, Lima 2023.

Por ello, la hipótesis que se ha planteado es: La implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el riesgo ante ataques cibernéticos en la empresa System Arq, Lima-2023.

- HE1: La implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de ataques malware como parte de los ataques cibernéticos en la empresa System Arq, Lima 2023.
- HE2: La implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de vulnerabilidades en los activos de información ante ataques cibernéticos en la empresa System Arq, Lima 2023.

# II. MARCO TEÓRICO

Referente al actual trabajo de investigación se pretende mostrar conocimientos sintetizados de diferentes bases de datos, donde tomamos artículos, tesis, libros entre otros con temas que guarden relación al desarrollo, se seleccionaron antecedentes internacionales y nacionales con temas de gran aporte referente a la implementación de Sistemas de Gestión de Seguridad basada en la ISO 27001 y ciberataques, considerando sus objetivos, metodologías aplicadas, instrumentos, herramientas y resultados. Además, se consideraron temas como confidencialidad, integridad, disponibilidad de datos, ataques malware, ataques a redes LAN y suplantación de identidad, los cuales aportan significativamente a la investigación.

Los **antecedentes internacionales** considerados para esta investigación son:

Šikman, Latinovic y Paspalj (2019) tuvieron como objetivo planificar e implementar sistemas de gestión de seguridad basados en la norma ISO 27001. Esta norma internacional fue propuesta para usarlo como guía de seguridad, cumpliendo con cada requisito solicitado. El tipo de instrumento utilizado para recolectar información son las auditorías internas. Se aplica la metodología de análisis y evaluación de riesgos que se hayan encontrado durante la auditoría. En los resultados se evidencia que el sector que mayor aplica los estándares de seguridad dentro de sus organizaciones son los del sector de tecnología. La conclusión del estudio recomienda que toda empresa debe brindar protección, seguridad y confidencialidad de los datos.

Morales, Toapanta y Toasa (2020) el objetivo que plantearon fue implementar un sistema de seguridad que se basa en barreras de protección, aumentando los niveles de confidencialidad, integridad y disponibilidad, permitiendo de esta manera no ser vulnerables ante amenazas que puedan suscitar, realizados por hackers o los mismos trabajadores. En cuanto a la población estudiada se refieren a cualquier entidad que dentro de sus instalaciones tengan equipos tecnológicos donde se almacena información. El tipo de investigación aplicado fue práctico – experimental. Se obtuvo como resultados la reducción de tiempo de respuesta ante ataques en tiempo real, realizando bloqueos a usuarios desconocidos, permitiendo mejorar el estándar de seguridad. Los autores concluyen la necesidad de implementar reglas y

políticas de seguridad en los firewalls, para proteger toda información que se encuentre en los equipos tecnológicos.

Aguinaga (2021), tiene como objetivo primordial crear un SGSI acorde a la ISO 27001 y estimar el nivel de influencia en la protección de la información financiera. Trabajó con una población de 24 registros para cada indicador propuesto. El instrumento que le permitió recolectar los datos fue la ficha de información y como metodología planteada fue la aplicada, la cual le permitirá investigar la problemática. Los resultados obtenidos se reflejaron en que los indicadores confidencialidad, integridad y disponibilidad presentan un rendimiento favorable en la seguridad de los datos al aplicar la ISO 27001. Asimismo, concluyó el logro de elevar el nivel de seguridad en la entidad financiera generando confianza a sus clientes.

Poma (2021), se destaca el objetivo que se propone el cual es determinar el impacto de un SGSI aplicada a una empresa de tecnología de información. La población investigada fueron 22 fichas de incidencias. Utilizaron instrumento para recolectar datos las cuales fueron las fichas de registro. La metodología planteada fue la aplicada. Los resultados que obtuvo fue la mejora significativa de las incidencias y soluciones en un menor tiempo. Concluyó que la implementación de un SGSI generó un elevado nivel de seguridad de los datos permitiendo disminuir las vulnerabilidades.

Antunes, Maximo, Gomes y Pinto (2021) el objetivo propuesto por los autores es que las organizaciones deben evitar que su información se encuentre expuesta ante cualquier ataque o robo cibernético, por ello inducen a que la privacidad de los sistemas de información y el área relacionados con el data center deben ser protegidos. La población estudiada fueron las Pymes, ubicados en el centro de Portugal. El instrumento que se empleó para recabar información fueron las auditorías, las cuales se aplicaron a empresas con el uso de la metodología análisis – práctico. Los resultados que surgieron de la investigación fue elevar los niveles de seguridad generando una mayor percepción de mejoramiento de privacidad. Asimismo, concluyeron que para tener una empresa sólida respecto a la gestión de seguridad de datos se deben de realizar conferencias informativas y capacitación respecto a la concientización de la seguridad y mejoramiento de infraestructura de redes.

Ipanama (2022), su objetivo fue aplicar eficientemente las políticas de seguridad de un SGSI, la cual permita conocer las vulnerabilidades para dar seguimiento y poder controlarlos o mitigarlos. Los componentes utilizados en la investigación fueron los activos de información pertenecientes a la organización. El instrumento utilizado para la recolección de datos fueron la guía de observación, lista de chequeos y fichas de registros. La metodología aplicada fue el ciclo de Deming o PDCA. Respecto a los resultados fueron favorables para cada uno de sus cuatro indicadores, permitiendo la implementación en la empresa investigada. Se comprobó la eficiencia de seguridad que reciben los activos de información aplicando un SGSI.

Togu y Kalamullah (2022) su finalidad clave del estudio era desarrollar un plan de estructuras de redes y análisis para identificar cuáles son los datos que se transmiten entre equipos informáticos dentro del ambiente laboral utilizando normas internacionales de protección de la información. Los estándares de seguridad que utilizaron fueron las normas ISO 27001, NIST SP800-161 y ITU-T X.805. Además, el instrumento utilizado fue la comparación de estándares. Se aplicaron diferentes metodologías las cuales son análisis comparativo de requisito y análisis de contenido. El resultado indica que para obtener un aseguramiento en el marco de la ciberseguridad se debe emplear estos 3 estándares de seguridad. En conclusión, se aspira que el plan propuesto de dimensiones, amenazas y propuestas de mitigación ayuden a proteger el sistema de seguridad de transferencia de datos en las comunicaciones de equipos informático.

Kitsios, Chatzidimitriou y Kamariotou (2023) la propuesta del objetivo fue desarrollar un marco de etapas de evaluación de riesgos dentro de una organización del sector tecnología, la cual permita cumplir con los estándares de seguridad de la ISO 27001. La población utilizada para el estudio fueron las empresas multinacionales que se dedican al servicio de consultorías de TI. Además, como instrumento de captación de información fue mediante auditorías a las áreas de TI y personal encargado. Se utilizaron metodologías para analizar y evaluar riesgos. Obteniendo como resultado implementar un proyecto de hallazgos de los riegos, donde se pueda recurrir y encontrar soluciones para mitigar el riesgo. Los autores llegan a la conclusión que toda empresa certificada

con ISO 27001 debe realizar prácticas de seguridad para prevenir ataques, además toda acción debe ser documentada y actualizada ante un mismo posible ataque.

En cuanto a los **antecedentes nacionales** se tiene:

Poma y Vargas (2019) trataron de demostrar en su investigación como la ciberseguridad protege los sistemas informáticos y redes sociales a nivel global, a través de una investigación cuantitativa, de diseño no experimental y descriptivo usando un análisis documentario. Los resultados arrojaron que, a través de la implementación de medidas rígidas, las redes y los sistemas informáticos se vuelven seguros en un 70%. Llegando a la conclusión que la Ciberseguridad implementada en los sistemas informáticos aumenta las buenas prácticas en las empresas y protege la información.

Zevallos (2019) busca identificar la fragilidad de seguridad informática de una red empresarial, nos permite evidenciar los diferentes tipos de vulnerabilidades y clasificarlas según su riesgo, empleando auditorias e investigaciones descriptivas, y correcto análisis de la infraestructura, con herramientas, metodologías y conocimientos de seguridad informática, se detectaron vulnerabilidades de las cuales se ignoraban por falta de conocimientos por parte de los empleados y el departamento de TI , por ello, se debe implementar medidas correctivas.

Según Medina y Rivas (2019) un ataque informático se define como la acción de un individuo que, mediante el uso de un sistema informático, trata de obtener el dominio, perturbar o provocar daños en otro sistema, abarcando desde un host hasta un red privada. El resultado de estos ataques, se pueden experimentar pérdidas de información y/o daños económicos dentro de una organización. Por lo tanto, la seguridad de la información es más importante que simplemente proteger la información acumulada en los equipos informáticos; debe dirigirse a la preservación de la propiedad intelectual y la información crucial, tanto para las empresas como para los usuarios. Las redes inalámbricas basadas en 802.11 están experimentando un crecimiento graduable en la actualidad. Aunque ofrecen la ventaja de ser flexibles y adaptables a las estructuras organizativas, también presentan el inconveniente de ser vulnerables

a una amplia diversidad de ataques informáticos. Asimismo, se analiza el desempeño de un software de detección de intrusiones que se implementará en el contexto de una red inalámbrica basadas en 802.11. Este sistema estará diseñado para identificar cualquier flujo de datos anormales dentro de la red. Con el fin de lograr el propósito, se instalarán software de detección de intrusiones en el S.O. Kali Linux, que se selecciona debido a su naturaleza de código abierto y su especialización en seguridad informática. A continuación, se llevarán a cabo una serie de ataques informáticos con el fin de evaluar el funcionamiento de estos sistemas de seguimiento de intrusiones en el entorno de una red wifi 802.11. Finalmente, se analizarán las conclusiones alcanzadas para determinar cuál de los software de detección ofrece efectividad en este tipo de escenario.

Ormachea (2020) plantea enfoques formales de ciberseguridad y también robustecer la seguridad nacional, tomando como modelo los mecanismos y políticas actuales empleadas en el medio internacional y enfrentar las ciber amenazas mediante la observación y el análisis documental. Se determinó que, los aspectos relacionados a colaboración a nivel regional, bilateral y multilateral, el Perú muestra deficiencias; además, el Estado aún está en desarrollo en cuanto a la concientización de capacidades cibernéticas militares, como medidas fundamentales de las políticas nacionales de ciberseguridad. Concluyó que la ciberseguridad debe ser un compromiso social que requiere compromiso entre el sector público y privado, Por consiguiente, propone que la estrategia nacional de seguridad cibernética de Perú se debe implementar.

Fernández, Hierro y Araque (2020) propone implantar protocolos, mecanismos, reglas o costumbres para proteger la confidencialidad y violaciones en la seguridad de arbitrajes internacionales, de esta manera evitar graves problemas. Los procesos de digitalización, análisis documentario e investigaciones descriptivas, dan como resultado nuevas normas, así como distintos protocolos para establecer mecanismos de control que revistan mayor defensa y privacidad en la utilización de los protocolos. La tendencia es favorecer la utilización de servicios electrónicos en el desarrollo de los procedimientos arbitrales.

Para Núñez Moran (2021), en su trabajo de investigación, desarrolló una metodología destinada a la detección y mitigación del Ransomware, centrándose

en el análisis del comportamiento de esta categoría de malware. Dividiéndolo en cuatro fases, y creó un software específico para implementarla y llevar a cabo las pruebas correspondientes. Como resultado, se logró detectar 5 de los 8 casos de malware evaluados, mientras que los otros 3 no llegaron a ejecutarse y, además, no cifraron ningún archivo, en contraste con otros programas anti-malware disponibles. La metodología propuesta en esta investigación se revela efectiva para detectar nuevas amenazas de malware, siempre y cuando estos amenacen con cifrar archivos. Esta estrategia protege un conjunto de datos críticos. Además, la incapacidad de los ransomware para cifrar archivos bajo esta metodología demuestra su eficacia en comparación con las herramientas anti-malware tradicionales, las cuales no son capaces de reconocer amenazas desconocidas.

Según (Pérez Díaz, Chinchay Maldonado, 2021) En su estudio de tesis, plantean la ejecución de Cuckoo Sandbox, una herramienta de código abierto utilizada para analizar malware. Esta implementación se llevó a cabo en un servidor tipo torre con un procesador Core i5 y 16 GB de RAM, utilizando Ubuntu 20.04 LTS como sistema operativo. Se configuraron varios archivos de configuración esenciales, como cuckoo.conf, donde se asignó la dirección IP del servidor; VirtualBox.conf, para definir la dirección IP y el nombre del cliente; y reporting.conf, para generar informes en formato HTML. Posteriormente, se estableció un laboratorio de pruebas virtualizado que constaba de 5 máquinas virtuales con Windows 10. Este entorno se configuró para que fuera similar a la red informática local de la Coopac Norandino Ltda. En el marco de la ejecución de las pruebas, se introdujo un malware en cada una de las máquinas virtuales. Los resultados revelaron que todos los malware inyectados, es decir, el 100%, se detectaron y aislaron de manera efectiva. Además, el proceso de análisis promedió un consumo de memoria RAM de 0.89 GB y un tiempo promedio de 123.6 segundos. Estos resultados demuestran la efectividad de Cuckoo Sandbox como una herramienta valiosa para fortalecer la seguridad en los límites de la red informática.

Para (Ochoa Díaz y Ticse López, 2022), el progr tecnológico experimentado en los últimos años ha brindado a las empresas diversas oportunidades para respaldar sus operaciones comerciales y adquirir

herramientas que les ayuden a generar valor para sus organizaciones. Sin embargo, es importante reconocer que este progreso no solo ha tenido un impacto positivo en las empresas, sino que también ha beneficiado a los actores del cibercrimen. Los delincuentes cibernéticos disponen de diversas herramientas, una de las cuales pertenece a la categoría de malware, conocida como ransomware. Estos ataques, como resultado, provocan consecuencias económicas y legales significativas, así como un deterioro de la reputación de las organizaciones afectadas. Estos efectos incluyen la interrupción de los servicios, la retención de datos como rehenes, el acceso no permitido a información reservada, sanciones económicas y otros impactos adversos. Los ataques malware han dejado una huella significativa en el sector, obteniendo un 48% de ataques de este tipo durante el año 2020. Sin embargo su propósito es ofrecer a las instituciones financieras un marco que les posibilite realizar evaliaciones cuantificables de los impactos financieros derivados de un ataque de malware.

Ortiz, Guevara y Mendoza (2022) introducen mecanismos de seguridad al uso de aplicaciones de mensajería instantánea, recopilando información confiable de bases de datos de la última década y se han revisado diversas publicaciones nacionales e internacionales. Tras un análisis exhaustivo, se identificaron cinco aspectos clave que contribuirán a una gestión más efectiva de la seguridad: aprendizaje del personal sobre seguridad informática, fomento de buenas prácticas, cumplimiento de estándares de seguridad, uso de aplicaciones con cifrado de datos y establecimiento de políticas de ciberseguridad.

Para Cieza y Ojeda (2022) la utilización de conexiones de Internet inalámbrico es una práctica extendida en empresas de todos los niveles. En consecuencia, es crucial prevenir posibles amenazas derivadas de eventos de de intrusiones cibernéticas. La Wi-Fi Alliance, ha introducido varios métodos destinados a garantizar la seguridad de las redes inalámbricas de forma local, mediante protocolos tales como WEP, WPA, entre otros. A lo largo de los años, estos protocolos han experimentado múltiples cambios y mejoras con el fin de fortalecer su seguridad y eficacia. Estas modificaciones han abarcado aspectos como el cifrado y los componentes, y se han implementado actualizaciones para hacer frente a las vulnerabilidades y ataques que se han presentado en el

camino. Se puede afirmar que el protocolo WPA3 se presenta como la opción más eficaz para hacer frente a los ataques informáticos en este contexto. Además, es esencial complementar su uso con mecanismos adicionales, como firewalls, sistemas de identificación maliciosa, vlans, herramientas de nivel superior, como RPV y servidores Radius. Estos elementos permiten eliminar, aplicar filtros y supervisar cualquier actividad inapropiada en la WLAN, lo que facilita la corrección inmediata de posibles amenazas.

Según Curay Calucho, María Fabiola, (2023) los avances tecnológicos actuales, como la proliferación de la conectividad inalámbrica, han ganado una creciente popularidad. Cada vez más individuos tienen la capacidad de acceder a la red utilizando sus dispositivos móviles o computadoras portátiles. Sin embargo, tanto las redes empresariales como las domésticas son vulnerables a ataques, por lo que es esencial configurarlas adecuadamente para prevenir la entrada de personas no autorizadas, lo que podría poner en riesgo información tanto personal como corporativa. Este estudio involucró la realización de pruebas de de intrusión en una red doméstica utilizando diversas herramientas como Airgeddon, Aircrack-ng y Wifite, con el propósito de identificar posibles vulnerabilidades. Además, se utilizó la herramienta Nessus para realizar un escaneo en busca de vulnerabilidades en los dispositivos conectados a la red. Prantearon el objetivo de analizar y mejorar el nivel de seguridad de estos dispositivos y la configuración de acceso a la red inalámbrica doméstica, con el fin de fortalecer su protección contra amenazas potenciales.

Respecto a la **fundamentación teórica**, la presente investigación se centra en los contenidos relevantes de:

Según Lopes, Guarda y Oliveira (2019) indican que la norma internacional sobre la seguridad de la información referente a la ISO 27001, ayuda a prevenir riesgos cibernéticos mediante la aplicación de técnicas y diversos criterios de seguridad establecidos en el estándar de seguridad. Toda organización que cuenta con la certificación ISO 27001 son reconocidos por el alto nivel de privacidad de información y compromiso que mantienen con la protección de los datos (p. 3).

Para Phirke y Ajit (2019) Advierten que la norma ISO 27001 mediante sus requisitos y criterios permite implementar un adecuado SGSI, a través de controles de seguridad para mitigar algún suceso sospechoso o riesgo relacionado con los recursos de información de la empresa, además busca que cada área involucrada a la gestión de información se encuentre protegido en todo momento (p. 692).

Para Zapata Moran, Diana Stefany (2021), define a un SGSI como un plan de protección de datos, la cual se encuentran almacenados en una organización y que deben ser protegidos a todo costo, cumpliendo con principios primordiales y esenciales de la seguridad de los datos, demostrando fiabilidad, confiabilidad ante cualquier incidente de seguridad.

Además, Arina (2021) menciona que la norma ISO/IEC 27001 mediante sus especificaciones pretende implementar un SGSI, donde se estipula proteger los recursos de la empresa, mediante diferentes procesos estructurados, procesos tecnológicos y procesos de recursos humanos, a través de una evaluación de riesgos, además indica que cada área debe contar con objetivos y controles de seguridad generando credibilidad hacia sus clientes (p. 86). La norma internacional referente al Sistema de Gestión de Seguridad, permite monitorear, controlar, analizar, resguardar y proteger toda información alojada en la empresa (Fonseca, Rojas y Florez, 2021. p. 2).

Sin embargo, (Tonysé, 2021) da a conocer que al implementar la norma ISO 27001 en una organización, permite elevar los niveles de seguridad de información, reducir cualquier ataque cibernético que suceda mediante la red o por el mismo personal, evitando pérdida de la información, los beneficios que nos ofrece el estándar de seguridad es identificar riegos para luego poder corregirlos, confidencialidad, flexibilidad, confianza y conformidad, alcanzando las expectativas de privacidad de la información (p. 495).

El efecto de implementar la ISO 27001 ayuda a identifica amenazas y mitigarlos rápidamente, además corrige vulnerabilidades expuestas a ataques cibernéticos, contribuye con la seguridad y privacidad del negocio, mejora los procesos relacionados a la protección de los datos (Fonseca, Rojas y Florez, 2021, p. 1).

Según Ponce Cruz, Ángel Sabino (2022) un Sistema de Seguridad de la Información son una seria de directrices integradas, normas o procedimientos que, mediante el cumplimiento de estos, permite aumentar el nivel de confiabilidad, integridad y disposición de la información, garantizando privacidad de los datos.

Asimismo, Limache Ynquilla, Anuar Mauro (2022), indica que implementar un SGSI garantiza una completa protección de los datos, usando procesos y controles con estándares internacionales en seguridad. Por consiguiente, permitirá corregir vulnerabilidades que arriesguen la perdida de información permitiendo mitigarlos rápida y efectivamente.

Además, De la Cruz Mejía, Cristhian Paul (2023), expresan que un SGSI es una agrupación de métodos, procedimientos y pautas preparados para resguardar las redes, dispositivos, software y datos contra ataques cibernéticos, intrusiones no autorizadas, piratería y accesos no autorizados, donde deben primar características como la confidencialidad, autenticidad, integridad, residencia, seguridad en capas, disponibilidad y actualización continua, este último permitirá una evolución y aseguramiento informático previniendo amenazas.

Asimismo, Ramos, Cahuaya y Llanqui (2023) pronuncian que la ISO 27001 es una norma internacional la cual mediante buenas prácticas permite aplicarlo en la Gestión de Seguridad de la Información, puede ser implementado en cualquier entidad, principalmente al área de tecnología de información. Esta norma permite establecer e implementar niveles de seguridad, actuar ante alguna situación de ciberataque, monitorear en todo momento el contenido de la data, mantener seguro la privacidad de la información y mejorar constantemente el sistema de seguridad (p. 65).

Según García (2019) en el Perú, las organizaciones enfrentan el desafío de la transformación digital, lo que implica considerar las amenazas que se susciten referente a la seguridad de los sistemas informáticos. Es importante reconocer el riesgo de sufrir un ciberataque no es algo que deba ser prevenido, controlado y minimizado únicamente por los departamentos de seguridad

informática, sino que es un riesgo del negocio en sí mismo y debe ser abordado en el nivel más alto de cualquier organización (p. 176).

Los ataques cibernéticos son acciones delictivas llevadas a cabo por individuos o grupos con conocimientos técnicos especializados, que buscan obtener información valiosa de la empresa. Estos ataques pueden ser ejecutados de varias formas, como infectar los equipos informáticos con virus, hackear servidores a través de la red o robar las credenciales de acceso al sistema, entre otras. El objetivo principal es apoderarse de la información y luego extorsionar o exigir dinero para recuperarla (Poma y Vargas, 2019, p. 275).

El efecto de los ataques cibernéticos es de infiltración, daño, manipulación, robo o comprometer sistemas informáticos, redes, dispositivos electrónicos u otros recursos digitales. Estos pueden incluir actividades como el acceso no permitido, robo de información, interrupción de servicios, propagación de malware, secuestro de cuentas, la suplantación de identidad, entre otros métodos, con el fin de obtener beneficios económicos, políticos, sociales o causar perjuicio a individuos, organizaciones o incluso a nivel global (Poma y Vargas, 2019, p. 275).

Además, Armas (2020) manifiesta que la adopción de nuevas tendencias y el aumento de la digitalización, el almacenamiento de grandes y robustas cantidades de datos, son un gran atractivo para los ciberdelincuentes. Por lo tanto, las organizaciones deben replantear y proteger sus procesos tecnológicos desde una perspectiva de ciberseguridad. Es fundamental comprender las amenazas y tomar medidas básicas para reducir el riesgo de sufrir un delito cibernético (p. 21).

Núñez y Carhuancho (2020) exponen que la propagación y uso de internet ha permitido que una nueva modalidad de delincuencia conocida como cibercriminalidad crezca a gran escala. Por tanto, se han creado herramientas tanto a nivel nacional como internacional para evitar la impunidad y sancionar este tipo de conductas. Referente a lo sucedido durante la pandemia de COVID-19, se evidencia claramente que nuestras actividades diarias aún dependen en gran medida de la tecnología, lo que ha generado nuevas formas de cibercriminalidad (p. 94).

Según, Quiroga (2021) los ataques cibernéticos son actos delincuenciales por parte de hackers o trabajadores que se inclinan por hurtar información importante para la empresa, estos ataques se pueden realizar de diversas maneras, infectando de virus a los equipos informáticos, hackeos a servidores mediante la red, robo del usuario de acceso al sistema, entre otros, buscando como propósito adueñarse de los datos privados y extorsionar o solicitar dinero para recuperar toda la información (pp. 16-17).

Para De la Cruz y Méndez (2023) la seguridad cibernética, es la capacidad de reaccionar ante la avalancha de ataques cibernéticos y otras contingencias, y fundamental para las organizaciones que enfrentan amenazas de seguridad masivas todos los días. Las organizaciones suelen emplear múltiples estrategias de gestión de riesgos para lograr la seguridad. Sin embargo, la aplicación de estándares y certificaciones de seguridad cibernética puede brindar orientación a los proveedores en el desarrollo seguro y la producción de productos TIC, así como brindarles a los clientes y consumidores cierta confianza en las capacidades de seguridad del producto (p. 234).

**Dimensiones** consideradas para la variable dependiente:

Primera dimensión:

- **Ataques malware** (Cando y Medina, 2021, p. 28).

Indicador seleccionado:

- Porcentaje de ataques malware (Cando y Medina, 2021, p. 32).

$$\text{PAM} = \left(\frac{CME - CMS}{CME}\right) * 100$$

Dónde:

PAM= Porcentaje de ataques malware

CME = Cantidad de malware encontrados

CMS= Cantidad de malware suprimidos

Segunda dimensión:

- **Vulnerabilidades en los activos de información** (Cando y Medina, 2021, p. 29).

Indicador seleccionado:

- Porcentaje de vulnerabilidades en los activos de información (Rincon, 2021, p. 80).

$$\text{PVAI} = \left(\frac{CVI - CVC}{CVI}\right) * 100$$

Dónde:

PVAI= Porcentaje de vulnerabilidades en los activos de información

CVI= Cantidad vulnerabilidades identificadas

CVC= Cantidad de vulnerabilidades corregidas

# III. METODOLOGÍA

En la actual investigación el diseño identificado es el experimental de tipo pre experimental con un enfoque cuantitativo y relacionada al tipo aplicada, donde se busca obtener resultados referentes a la implementación de un sistema de gestión de seguridad basada en la ISO 27001 para reducir el riesgo ante ataques cibernéticos en la empresa System Arq S.R.L. Se trabajará con una muestra de 30 activos de información en la organización. Respecto a la recolección de los datos, se utilizará la guía de observación y fichas de registro los cuales serán validadas donde se determinará si la hipótesis de la investigación es aceptada o denegada.

## 3.1 Tipo y diseño de la investigación

### 3.1.1 Tipo de Investigación

Referente al tipo de investigación, se desarrollará como un estudio aplicado. A juicio de Sanchez, Reyes y Mejía (2018) indican que este tipo de investigación utiliza la información adquirida mediante la investigación los cuales se consideran básicas o teóricas, mediante ello permitirá solucionar de una manera eficaz los problemas que se presenten (p. 79). Asimismo, la investigación aplicada se enfoca en las oportunidades tangibles de implementar las directrices generales y dedica su trabajo a abordar los requerimientos que enfrenta la comunidad (Baena, 2017, p. 18).

### 3.1.2 Diseño de Investigación

Respecto al diseño de investigación se desarrollará de manera experimental de tipo preexperimental, debido a la manipulación de variables que se dará en el estudio. Según Baena (2017) el diseño experimental se refiere a una técnica científica que posibilita establecer conexiones basadas en evidencias que existen entre las variables o permita corroborar la autenticidad y veracidad de una hipótesis mediante la realización de un experimento controlado (p. 40). Los diseños preexperimentales reciben su nombre debido a que su nivel de control es mínimo. Se caracterizan por utilizar un único grupo en el estudio (Hernández *et al.*, 2014, p. 163).

El enfoque que se usará en la investigación es cuantitativo, debido a que se trata de la descripción esencialmente en la naturaleza expresada mediante

números (Rodriguez, Breña y Esenarro, 2021, p. 223). Además, Hernández et. al (2018) indican que la investigación cuantitativa tiene como objetivo reconocer y comprender la envergadura del problema, que puede ser parcial o imprecisamente conocido o supuesto, como una forma de obtener retroalimentación sobre los cambios o transformaciones ocurridas (p. 117).

$$G = O_1 \; X \; O_2$$

Dónde:

- G: Grupo experimental
- X: Implementación del Sistema de Gestión de Seguridad basada en la ISO 27001.
- $O_1$ : Expresión del resultado obtenido antes de la implementación del Sistema de Gestión de Seguridad basada en la ISO 27001 (Pre test).
- $O_2$ : Expresión del resultado obtenido después de la implementación del Sistema de Gestión de Seguridad basada en la ISO 27001 (Post test).

### 3.2 Variables y operacionalización

Según su función, la variable Sistema de Gestión de Seguridad basada en la ISO 27001 es independiente, debido a que puede producir variación en la variable dependiente. Por su naturaleza, la variable expuesta es cualitativa, este tipo de variables corresponden a características o cualidades que no se pueden expresar en términos numéricos (Salazar y Del Castillo, 2018, p.16).

Respecto a la variable Ataques Cibernéticos, por su función se categoriza como dependiente y por su naturaleza se determina como cuantitativa. Asimismo, Arias (2020) define a la variable cuantitativa a las características del individuo o del objeto que pueden ser cuantificadas utilizando valores numéricos (p. 34).

Como contribución a este estudio, se incluye en el anexo 2 y 3, matriz que establece la operacionalización de las variables, donde se definen a continuación sus aspectos principales:

**Variable Independiente: Sistema de Gestión de Seguridad basada en la ISO 27001.**

- **Definición conceptual**

Norma internacional referente al SGSI, la cual permite monitorear, controlar, analizar, resguardar, proteger toda información que es alojado en la empresa. (Fonseca, Rojas y Florez, 2021, p. 2).

- **Definición operacional**

El efecto de implementar la ISO 27001 ayuda a identifica amenazas y mitigarlos rápidamente, además corrige vulnerabilidades expuestas a ataques cibernéticos, contribuye con la seguridad y privacidad del negocio, mejora los procesos relacionados a la protección de los datos (Fonseca, Rojas y Florez, 2021, p. 1).

**Variable dependiente: Ataques Cibernéticos.**

- **Definición conceptual**

Los ataques cibernéticos son acciones delictivas llevadas a cabo por individuos o grupos con conocimientos técnicos especializados, que buscan obtener información valiosa de la empresa. Estos ataques pueden ser ejecutados de varias formas, como infectar los equipos informáticos con virus, hackear servidores a través de la red o robar las credenciales de acceso al sistema, entre otras. El objetivo principal es apoderarse de la información y luego extorsionar o exigir dinero para recuperarla (Poma y Vargas, 2019, p. 275).

- **Definición operacional**

El efecto de los ataques cibernéticos es de infiltración, daño, manipulación, robo o comprometer sistemas informáticos, redes, dispositivos electrónicos u otros recursos digitales. Estos pueden incluir actividades como el acceso no permitido, robo de datos, interrupción de servicios, propagación de malware, secuestro de cuentas, la suplantación de identidad, entre otros métodos, con el fin de obtener beneficios económicos, políticos, sociales o causar perjuicio a individuos, organizaciones (Poma y Vargas, 2019, p. 275).

- **Dimensiones**

**Ataques malware**, programa malicioso con la capacidad cifrar archivos (Cando y Medina, 2021, p. 28).

**Vulnerabilidades en los activos de información,** (Cando y Medina, 2021, p. 29).

- **Indicadores**

Porcentaje de ataques malware (Cando y Medina, 2021, p. 32).

Porcentaje de vulnerabilidades en los activos de información (Rincon, 2021, p. 80).

- **Instrumento**

Guía de observación

Ficha de registro

- **Escala de medición**

Ordinal

### 3.3 Población, muestra y muestreo

#### 3.3.1 Población

Se refiere a un grupo, compuestos por objetos, individuos u otros, que comparten características específicas o cumplen con un criterio establecido. Estos se pueden identificar en un área de interés y serán objeto de estudio en relación con la hipótesis relacionada a la investigación (Sánchez, Reyes y Mejía, 2018, p. 102).

En esta investigación se estudiará como población a 30 activos de información identificadas pertenecientes a la empresa System Arq (Ver Tabla 4).

**Tabla 1:** *Población en las dimensiones*

| INDICADOR | |
|---|---|
| Ataques malware | 280 reporte de malware escaneados |
| vulnerabilidades | 41 reporte de vulnerabilidades encontradas |

*Fuente: Elaboración Propia*

### 3.3.2 Muestra

La muestra se puede describir como un subnivel de casos destacados de una población, a partir del cual se recopilan los datos. Trabajar con una muestra presenta beneficios como el ahorro de tiempo, la reducción de costos y, si está correctamente seleccionada, puede contribuir a mejorar la precisión y exactitud de los datos. (Arispe *et al.*, 2020, p. 74).

**Reporte de malware escaneados**

$$n = \frac{280 * 1.96^2 * 0.5 * 0.5}{0.05^2(280 - 1) + 1.96^2 * 0.5 * 0.5} = 162$$

**Reporte de vulnerabilidades encontrados**

$$n = \frac{41 * 1.96^2 * 0.5 * 0.5}{0.05^2(41 - 1) + 1.96^2 * 0.5 * 0.5} = 37$$

### 3.3.3 Muestreo

Los muestreos probabilísticos son una técnica empleada en estadística e investigación para escoger muestras que sean representativas de una población en particular. En estos procedimientos, se asigna a cada miembro de la población una probabilidad establecida y no nula de ser utilizado en la muestra. Esto asegura que la muestra sea imparcial y que se puedan realizar conclusiones precisas acerca de la población en su conjunto. Esta metodología se apoya en el concepto de probabilidad, donde la probabilidad de elección es idéntica para cada integrante de la población, además cada elección es independiente de selecciones previas (Velázquez, 2019, p. 4).

### 3.3.4 Unidad de Análisis

Referente a la unidad de análisis realizada en la investigación, menciona que trata sobre la entidad o elemento objeto de estudio sobre la cual se recopila información y se realizan análisis. Elegir la unidad de análisis es crucial proceso en el que se recolectan, analizan y presentan los datos.

## 3.4 Técnicas e instrumentos de recolección de datos

### 3.4.1 Técnica

#### Observación

Se aplicará la técnica mencionada para recopila información directa sobre un hecho o fenómeno observable los cuales pueden ser eventos o sucesos, características, entre otros, sin necesidad de realizar preguntas (Ríos, 2017, p. 102).

### 3.4.2 Instrumentos

Los instrumentos son recursos que se utilizan como ayuda para alcanzar el objetivo del estudio, para el presente estudio se utilizará el instrumento guía de observación que permitirán registrar acciones, registros u observaciones. Según Hernández et. al (2018) el instrumento es la herramienta que el investigador utiliza con el propósito de recopilar y registrar la información, incluyendo guías de observación, entre otros métodos que serán validados y confiables (p. 94).

Además, la confiabilidad trata sobre los resultados que se obtienen; por consiguiente, deben presentar consistencia interna. La interpretación del coeficiente de confiabilidad se determina utilizando un coeficiente de correlación conocido como alfa de Cronbach, (Arispe *et al.,* 2020, p. 81).

Asimismo, la validez se refiere al nivel que define la investigación o la característica del instrumento utilizado para recopilar la información de investigación (Rodriguez, Breña y Esenarro, 2021, p. 227).

## 3.5 Procedimientos

En la siguiente etapa se procederá a realizar un exhaustivo análisis de información la cual fue recolectada y procesada, ello implica una serie de actividades que incluyen la creación de categorías, codificación, tabulación de resultados y evaluación estadística (Hernández *et al.,* 2018, p. 131).

Mediante la observación, referente a los ataques cibernéticos ocurridos en la empresa durante el último año, se podrá apreciar los peligros a las que está expuesta y requieren prioridad en la atención. Ello implica elaborar una guía de

observación y fichas de registro, los cuales nos permitirán llevar un control de los sucesos ocurridos en el sistema, además nos facilitará el análisis de los resultados arrojados por el software SPSS los cuales sirven para tomar las mejores decisiones, mejorar los procesos de seguridad y reducir el riesgo ante cualquier ataque cibernético.

**Tabla 2:** *Procedimiento de recaudación de información*

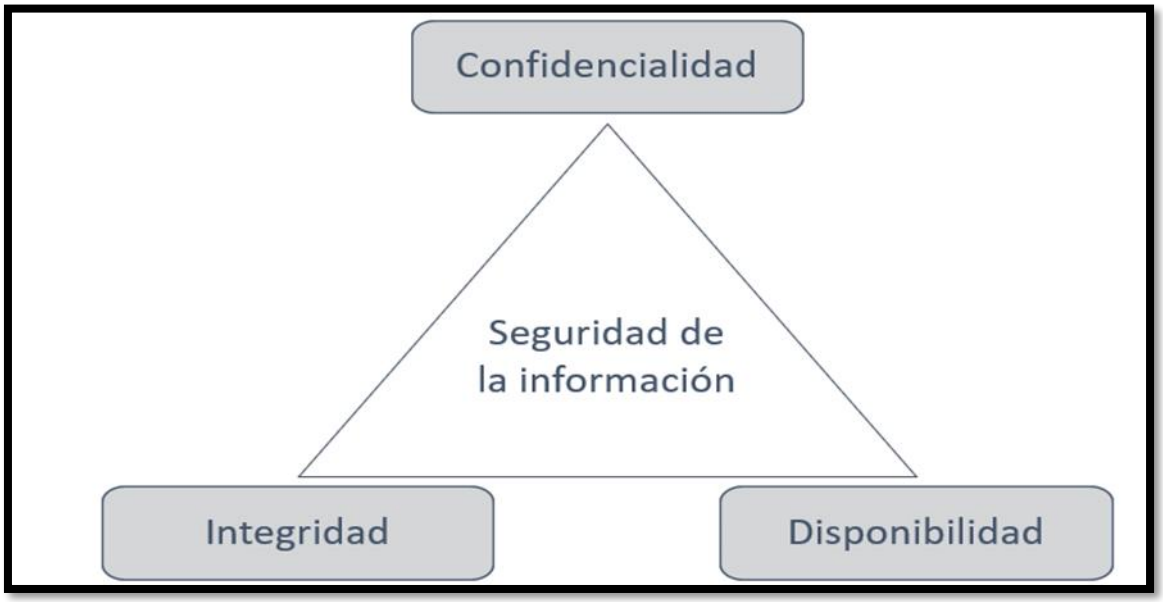
| **Generalidades** | | | | |
|---|---|---|---|---|
| Ubicación | | System Arq S.R.L. | | |
| Área responsable | | Gerencia de Tecnología e Información | | |
| Datos obtenidos por | | Oficina de Seguridad de la Información | | |
| Indicador | Instrumento | Técnica | Fuente | Dirigido a: |
| Porcentaje de ataques malware | Guía de Observación Ficha de Registro | Observación | Datos recaudados por ataques cibernéticos | Gerencia de Tecnología e Información |
| Porcentaje de vulnerabilidades en los activos de información | Guía de Observación Ficha de Registro | Observación | Datos recaudados por ataques cibernéticos | Gerencia de Tecnología e Información |

*Fuente: Elaboración Propia.*

### Implementación de un Sistema de Gestión de Seguridad basada en la ISO 27001

La norma ISO 27001 es un estándar global que establece directrices para instaurar, conservar y perfeccionar de forma continua un SGSI. Este sistema tiene como finalidad salvaguardar la confidencialidad, integridad y disponibilidad de los datos. Además, permite mantener el equilibrio adecuado entre estos tres factores es la razón de ser de la seguridad (Ver figura 1).

**Figura 1:** *Pilares de un SGSI*




*Fuente: https://cardenas9876.files.wordpress.com/2014/11/dadsdf.jpg*

Esta normativa ofrece un marco de trabajo en materia de seguridad de la información que auxilia a las entidades a detectar y gestionar eficazmente sus riesgos relacionados a la protección de datos.

La norma ISO 27001 es factible para diversas clases de organizaciones, englobando tanto a pequeñas y medianas empresas como a grandes corporaciones y organizaciones sin ánimo de lucro. Además, es adaptable a múltiples sectores, abarcando a tecnología de la información, salud, finanzas, servicios públicos y otros ámbitos.

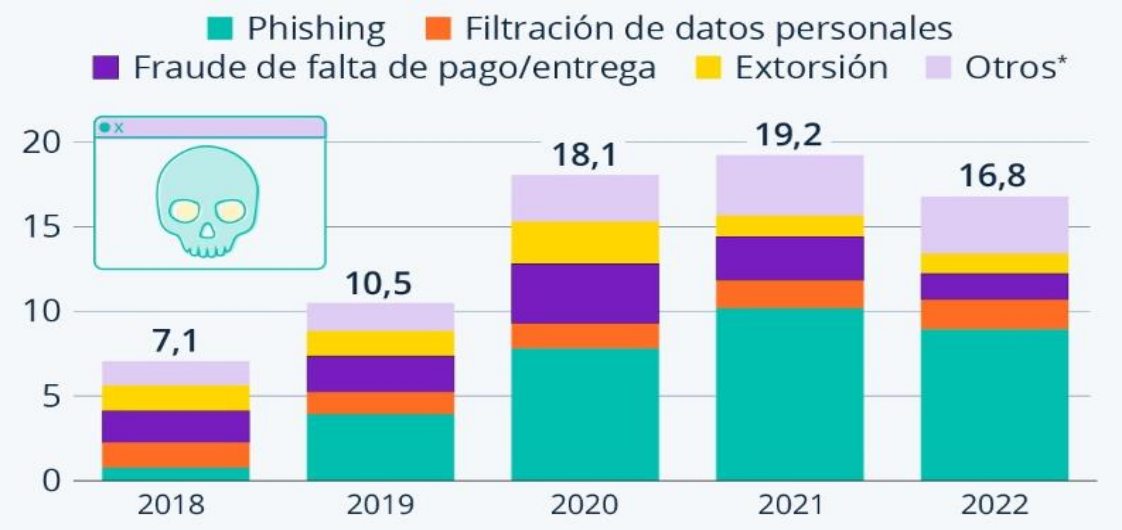
Para asegurar y preservar la integridad de la información, es fundamental contar con medidas de seguridad y directrices. Al hacerlo, adoptamos un enfoque de mejora continua, aplicando el ciclo Deming a cada proceso dentro de la organización.

Además, conocer el estado actual de la ciberseguridad es primordial para proteger la información ante las amenazas en línea. Las estadísticas arrojan datos actuales relacionados a los ciberataques registrados a nivel mundial (Ver figura 2).

Por lo que se debe tomar medidas para salvaguardar los activos. Es indispensable estar bien informado y mantenerse al tanto de las últimas

amenazas cibernéticas. Esto implica invertir en la seguridad de los dispositivos, proteger los datos y estar un paso por delante de los ciberdelincuentes.

**Figura 2**: *Número estimado de ciberataques registrados a nivel mundial (en millones)*




*Fuente: Investigación Statista, FMI, FBI*

El último cambio que se realizó a la norma ISO 27001 fue el 25 de octubre de 2022. Aunque no presenta modificaciones significativas en comparación con la versión anterior, es esencial examinar los ajustes que se han implementado.

Considerando la constante transformación del entorno digital, resulta algo asombroso que la ISO 27001 haya perdurado durante 9 años desde la versión anterior, manteniéndose como un referente destacado en cuanto a estándares de seguridad de la información. Esto resalta la estabilidad y solidez de este estándar internacional.

La reciente estructura de esta norma, sigue el modelo de otras normativas de gestión contemporáneas, como ISO 9000, ISO 20000 e ISO 22301, facilitando a las organizaciones la adaptación a múltiples estándares. La norma está compuesta por cláusulas coherentes con las últimas normativas emitidas por la ISO (Ver tabla 3)

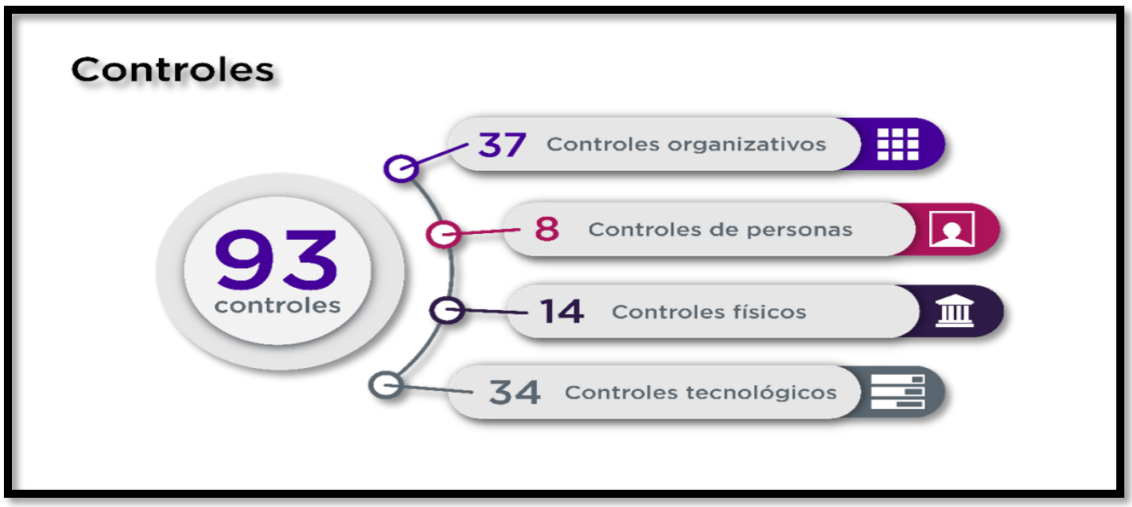
**Tabla 3:** *Estructura de la Norma ISO  27001*

| Ítem | Cláusulas de la ISO 27001 |
|---|---|
| 1 | Introducción |
| 2 | Alcance |
| 3 | Referencias Normativas |
| 4 | Términos y definiciones |
| 5 | Contexto de la Organización |
| 6 | Liderazgo |
| 7 | Planificación |
| 8 | Soporte |
| 9 | Operación |
| 10 | Evaluación de desempeño |
| 11 | Mejora |

Fuente: Elaboración Propia

Esta norma contiene en su estructura un total de 93 controles, clasificados en 4 grupos, según los criterios establecidos en la normativa de la ISO 27001 (Ver figura 3). Estos elementos se consideran adecuados para reducir al mínimo las amenazas.

**Figura 3:** *Controles de la ISO 27001:2022*




*Fuente:  https://www.cynthus.com.mx/wp-content/uploads/Esquematizacion-de-agrupacion-de-controles-del-estandar-ISO-27001-1024x559.png*

**Objetivo**

Establecer políticas de seguridad para proteger los activos de información de la Empresa System Arq S.R.L.

Establecer controles de seguridad para mitigar los riesgos de ataques cibernéticos en la Empresa System Arq S.R.L.

**Alcance**

La Empresa System Arq S.R.L. pretende establecer el diseño de un SGSI tal como lo propone la norma ISO 27001, definiendo todos los límites posibles mencionados en dicho diseño, lo que implica determinar qué información se busca proteger. La clasificación de los activos informáticos indicará qué información debe ser segura, independientemente de si se encuentra almacenada, procesada, transmitida o transferida dentro o fuera de sus instalaciones.

**Documentos de Referencia**

• Estándar ISO 27001:2022

• Documentos que establecen los requisitos mínimos para la elaboración e implantación de la norma ISO 27001 en el contexto de System Arq S.R.L.

• Exigencias de naturaleza normativa, contractual y otras que garanticen la adecuada configuración de la norma ISO 27001:2022 para System Arq S.R.L.

**Situación Actual de la Empresa**

Desde su fundación hasta la presentación del trabajo de investigación, la empresa System Arq S.R.L. cuenta con lo siguiente:

**Tabla 4:** *Situación actual de la empresa System Arq S.R.L.*

| Unidad de Análisis | Cantidad |
|---|---|
| Activos de información | 30 |
| Políticas de Seguridad de la Información | 0 |
| Controles de Seguridad de la Información | 44 |
| Roles y Responsables | 2 |

*Fuente: Elaboración Propia*

## Activos de Información

Actualmente existen 30 activos de información en la empresa (Ver Tabla 5), las cuales se encuentran divididas por categorías y valoradas según las amenazas y vulnerabilidades con las que cuentan.

***Tabla 5:*** *Relación de los Activos de Información*

| Ítem | Código | Nombre de Activo |
|---|---|---|
| 1 | [ES0001] | Datos del negocio |
| 2 | [ES0002] | Servicio |
| 3 | [ES0003] | Procesos del negocio |
| 4 | [SW0001] | BD Mysql |
| 5 | [SW0002] | Aplicaciones propias |
| 6 | [SW0003] | Aplicaciones a terceros |
| 7 | [SW0004] | Antivirus |
| 8 | [SW0005] | Servidor www |
| 9 | [SW0006] | Ofimática |
| 10 | [SW0007] | SO Windows |
| 11 | [HW0001] | Servidor |
| 12 | [HW0002] | Laptop, pc |
| 13 | [HW0003] | Celulares |
| 14 | [HW0004] | Equipo respaldo |
| 15 | [HW0005] | Impresora |
| 16 | [HW0006] | Módem |
| 17 | [HW0007] | access point |
| 18 | [COM0001] | Red de Datos |
| 19 | [COM0002] | Red Inalámbrica |
| 20 | [COM0003] | Wifi |
| 21 | [COM0004] | Red local |
| 22 | [COM0005] | WAN |
| 23 | [COM0006] | VPN |
| 24 | [AUX0001] | Fuente de poder |
| 25 | [AUX0002] | Ups |
| 26 | [AUX0003] | Generador eléctrico |
| 27 | [AUX0004] | Aire acondicionado |

| | | |
|---|---|---|
| 28 | [AUX0005] | Fibra óptica |
| 29 | [Media0001] | CD-ROM |
| 30 | [Media0002] | Memoria USB |

*Fuente: Elaboración Propia*

En lo que concierne a la parte práctica del proyecto, se implementará 3 Políticas de Seguridad de la Información, 5 Controles de Seguridad de la Información y se propondrá adicionar 3 roles y responsables a los existentes.

## 1. Políticas de Seguridad

Relación de las políticas de seguridad de la información que serán aplicadas en la empresa son:

**Tabla 6:** *Relación de Políticas de Seguridad de la información a implementar en la empresa System Arq S.R.L.*

| N° | Políticas |
|---|---|
| 01 | Análisis y gestión de riesgos |
| 02 | Políticas de gestión de vulnerabilidades |
| 03 | Políticas de protección contra software malicioso |

*Fuente: Elaboración Propia*

### 1.1. Análisis y gestión de riesgos

Es un enfoque que se emplea para reconocer y valorar las potenciales amenazas y debilidades que una empresa puede enfrentar en cuanto a su seguridad. Este procedimiento posibilita la identificación de las acciones requeridas para reducir los peligros y asegurar la seguridad de la organización y sus recursos.

### 1.2. Políticas de gestión de vulnerabilidades

La administración de vulnerabilidades es un procedimiento constante en tecnología de la información que se encarga de detectar, valorar, abordar y notificar las debilidades de seguridad presentes en los sistemas y el software que operan en ellos. La gestión de vulnerabilidades, en conjunto con otras estrategias de seguridad, desempeña un papel crucial en ayudar a las

organizaciones a dar prioridad a las amenazas potenciales y a reducir al máximo su efecto.

### 1.3. Políticas de protección contra software malicioso

Hace referencia a un conjunto de pautas y principios registrados que una entidad establece con el fin de administrar de forma eficaz los riesgos relacionados con el software malicioso. Su finalidad es salvaguardar la información, asegurar la continuidad de acceso, datos íntegros y mantener su confidencialidad.

## 2. Controles de Seguridad de la Información

Relación de los controles de seguridad de la información que serán aplicadas en la empresa son:

**Tabla 7:** *Controles de Seguridad de la Información a Implementar en la Empresa System Arq S.R.L.*

| N° | Clausula | Controles |
|---|---|---|
| 01 | 5.2 | Roles de seguridad de la información y Responsables de control |
| 02 | 6.8 | Reporte de eventos de seguridad de la información |
| 03 | 7.13 | Mantenimiento de equipos |
| 04 | 8.7 | Protección contra malware |
| 05 | 8.8 | Gestión de vulnerabilidades técnicas |

*Fuente: Elaboración Propia*

### 2.1. Roles de seguridad de la información y Responsables de control

Se definen diversos roles y responsabilidades relacionados con la seguridad de la información entre ellos tenemos director ejecutivo, Chief Information Security Office, responsable del SGSI, responsable de riesgos de seguridad de la información, entre otros. Estos roles son fundamentales para garantizar que la organización implemente y mantenga un adecuado sistema de protección y seguridad de datos.

### 2.2. Reporte de eventos de seguridad de la información

Implica la generación y mantenimiento de un registro de sucesos vinculados con la protección de la información. Estos registros de eventos son esenciales para la gestión efectiva y posterior mejora continua.

### 2.3. Mantenimiento de equipos

Aunque no se detallan los procedimientos específicos para el mantenimiento de equipos de tecnología, es fundamental que las organizaciones apliquen prácticas de mantenimiento adecuadas en su infraestructura de TI para priorizar la confidencialidad, integridad y disponibilidad de la información.

### 2.4. Protección contra malware

La protección contra malware es parte importante asegurar y proteger la información según la norma ISO 27001. La norma no proporciona detalles específicos sobre cómo protegerse contra el malware, pero dictamina un plan general para para dicha gestión que incluye la protección contra amenazas entre ellos están los malware.

### 2.5. Gestión de vulnerabilidades técnicas

Respecto a la gestión de vulnerabilidades, se trata de un componente crítico de la seguridad y establece una perspectiva global para gestionar los riesgos de seguridad de la información, que incluye la identificación, evaluación y tratamiento de vulnerabilidades técnicas mediante Inventario de Activos de TI, Identificación de Vulnerabilidades, Evaluación de Riesgos y otros, La gestión de vulnerabilidades técnicas es esencial para blindar los activos de información de organizaciones contra amenazas cibernéticas.

## 3. Roles y Responsables

En el contexto de ISO 27001, se definen varios roles y responsabilidades clave para garantizar la implementación exitosa del SGSI y la protección de la información confidencial. Estos roles y responsabilidades pueden variar según el tamaño y estructura de la organización, pero algunos de los roles comunes incluyen:

**Tabla 8:** *Roles y responsables a implementar*

| N° | Responsables |
|---|---|
| 01 | Responsable de Cumplimiento |
| 02 | Responsable de la Tecnología de la Información |
| 03 | Usuarios Finales |

*Fuente: Elaboración Propia*

**3.1. Responsable de Cumplimiento (RC):** El RC se encarga de garantizar que la organización cumple con las regulaciones y estándares de seguridad de la información aplicables. Esto puede incluir la preparación para auditorías y la gestión de las políticas de cumplimiento.

**3.2. Responsable de Tecnología de la Información (TI):** El responsable de TI es responsable de la seguridad de los sistemas de información y la infraestructura tecnológica. Deben garantizar que los controles de seguridad se implementen de manera efectiva en sistemas y aplicaciones.

**3.3. Usuarios Finales:** Todos los empleados de la organización tienen la responsabilidad de cumplir con las políticas y procedimientos de seguridad de la información y de informar posibles incidentes de seguridad.

**4. Brechas**

Se refiere a una falta de protección o una vulnerabilidad en un sistema, proceso o política que podría ser explotada por amenazas o atacantes para acceder, comprometer o dañar la información o los activos de una organización. Las brechas de seguridad pueden tener diversas causas y pueden ser perjudiciales para la confidencialidad, integridad y disponibilidad de la información.

En base a nuestros indicadores se ha logrado identificar diversos géneros de amenazas y vulnerabilidades que impactan en los activos de información estudiados (ver anexo 5).

A continuación, se ha identificado los controles de seguridad de la información de la norma ISO 27001 aplicados en la empresa System Arq S.R.L., la cual permitirá identificar qué controles de seguridad deben ser implementados en la organización (ver anexo 6).

Con el uso del Software PILAR BASIC EAR, nos permitió realizar un análisis de riesgos o vulnerabilidades en los sistemas de información, mediante la metodología Margerit la cual consta de cinco fases, empezando por la identificación de los activos relevantes, determinación de las amenazas a los que están expuestos, determinación de las medidas preventivas, medición del impacto residual y finalmente estimar el riesgo residual.

La herramienta es compatible con todas las etapas del método Margerit:

- Caracterización de los activos: identificación, clasificación, dependencias y valoración
- Caracterización de las amenazas
- Evaluación de las salvaguardas

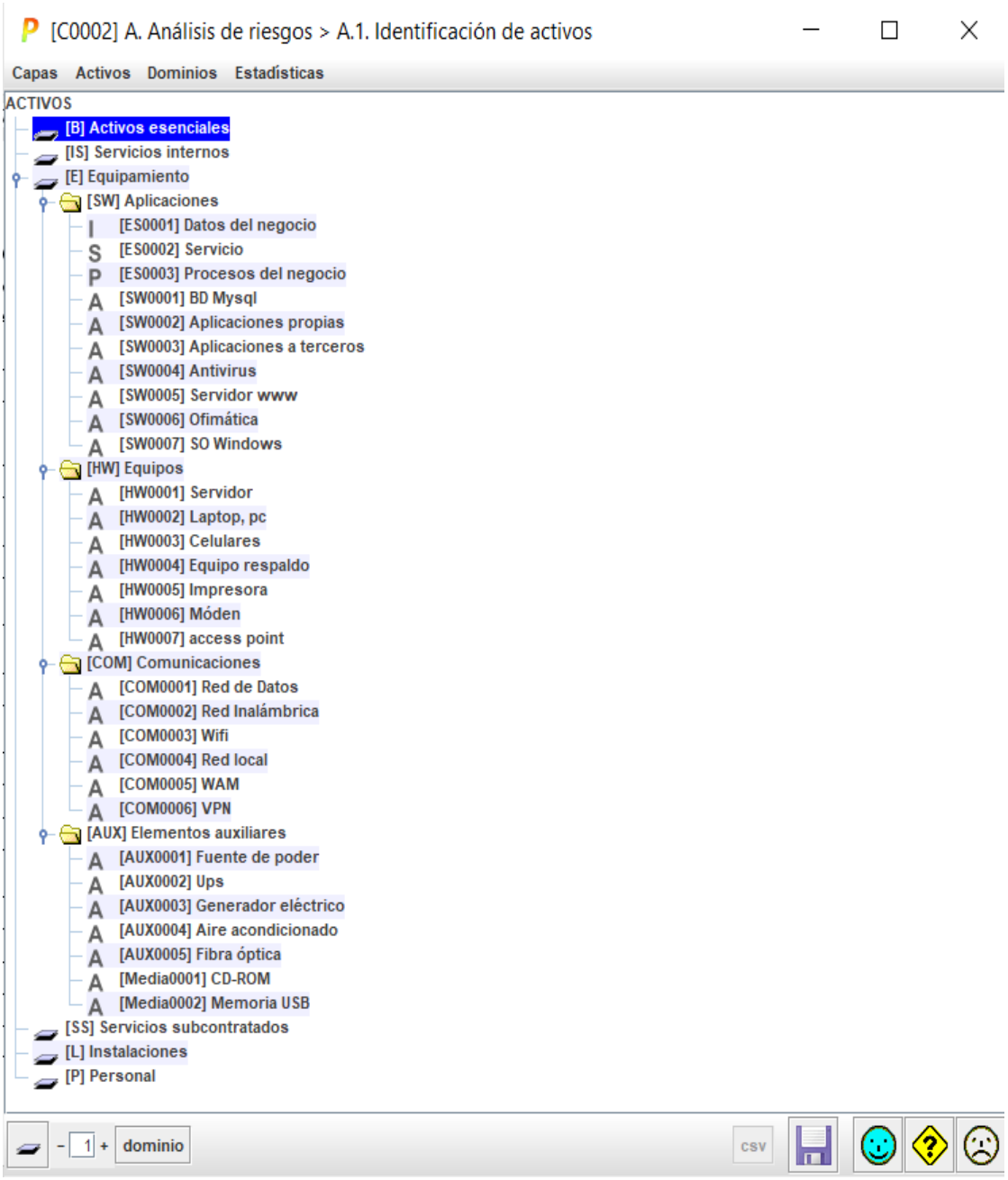
La herramienta aprovecha la lista de elementos categorizados, logrando una consistencia en los resultados de la evaluación, entre ellos encontramos:

- tipos de activos
- dimensiones de valoración
- criterios de valoración
- lista de amenazas

**Identificación de los activos de información en la empresa System Arq S.R.L.**

Mediante la herramienta PILAR se identificó 30 activos de información, categorizándolos y mostrando resultados que nos indicarían los valores mínimos que debería cumplir cada activo (Ver figura 4).

**Figura 4:** *Identificación de activos de información en el software PILAR EAR*




*Fuente: Elaboración Propia*

### Identificación de vulnerabilidades

En esta fase el software PILAR nos facilita relacionar las vulnerabilidades encontradas para cada activo de información, las cuales deberán ser tratadas para corrección de las mismas (Ver figura 5).

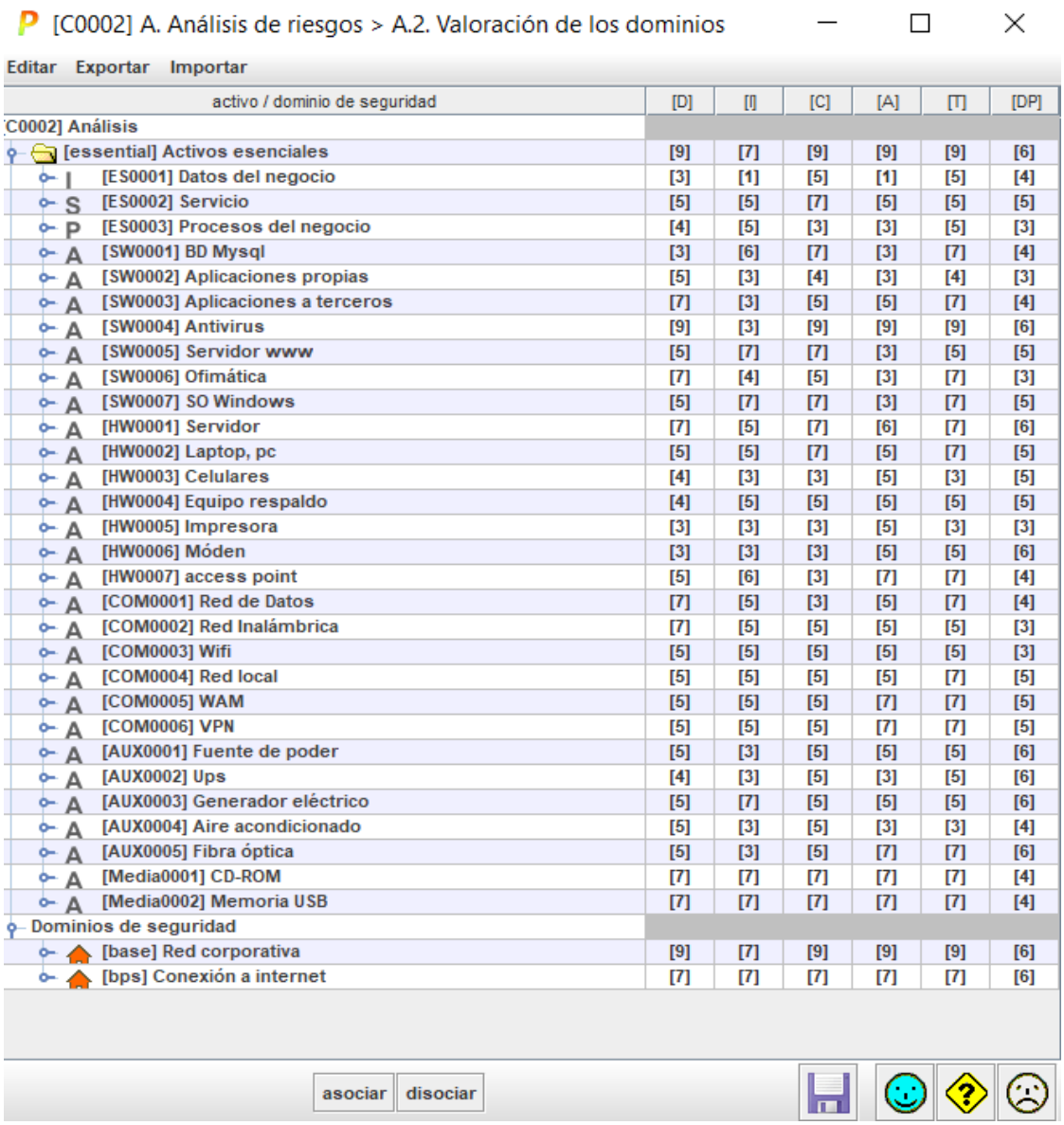
**Figura 5:** *Identificación de vulnerabilidades en los activos de información*


*Fuente: Elaboración Propia*

**Valorización de activos según su nivel de vulnerabilidad**

Determina el valor de los activos de información que posee y pretende proteger. La valorización de activos es esencial para decidir con conocimiento sobre la asignación de recursos destinados a la seguridad de la información y la gestión de riesgos, los criterios evaluados según las dimensiones del SGSI son disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y datos personales (Ver figura 6).

**Figura 6:** *Valorización a los activos de información según criterios de la ISO 27001*



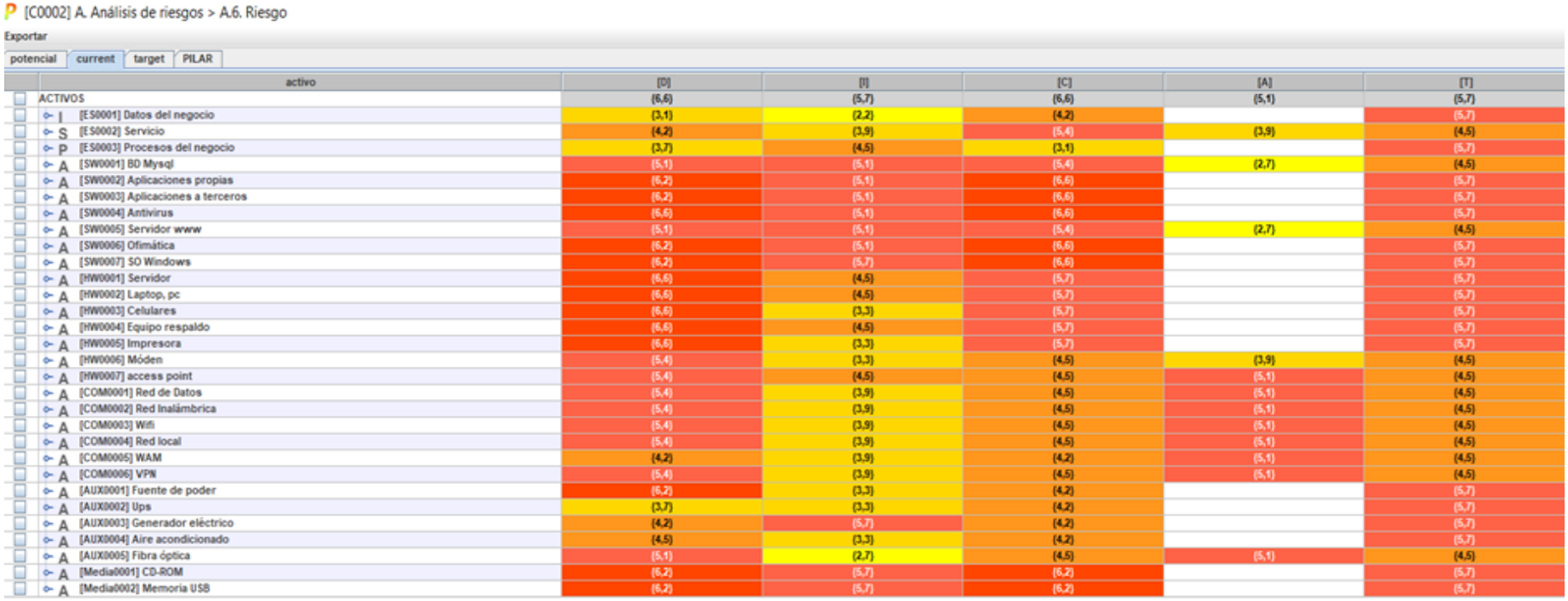

| activo / dominio de seguridad | [D] | [I] | [C] | [A] | [T] | [DP] |
|---|---|---|---|---|---|---|
| C0002] Análisis | | | | | | |
| [essential] Activos esenciales | [9] | [7] | [9] | [9] | [9] | [6] |
| I [ES0001] Datos del negocio | [3] | [1] | [5] | [1] | [5] | [4] |
| S [ES0002] Servicio | [5] | [5] | [7] | [5] | [5] | [5] |
| P [ES0003] Procesos del negocio | [4] | [5] | [3] | [3] | [5] | [3] |
| A [SW0001] BD Mysql | [3] | [6] | [7] | [3] | [7] | [4] |
| A [SW0002] Aplicaciones propias | [5] | [3] | [4] | [3] | [4] | [3] |
| A [SW0003] Aplicaciones a terceros | [7] | [3] | [5] | [5] | [7] | [4] |
| A [SW0004] Antivirus | [9] | [3] | [9] | [9] | [9] | [6] |
| A [SW0005] Servidor www | [5] | [7] | [7] | [3] | [5] | [5] |
| A [SW0006] Ofimática | [7] | [4] | [5] | [3] | [7] | [3] |
| A [SW0007] SO Windows | [5] | [7] | [7] | [3] | [7] | [5] |
| A [HW0001] Servidor | [7] | [5] | [7] | [6] | [7] | [6] |
| A [HW0002] Laptop, pc | [5] | [5] | [7] | [5] | [7] | [5] |
| A [HW0003] Celulares | [4] | [3] | [3] | [5] | [3] | [5] |
| A [HW0004] Equipo respaldo | [4] | [5] | [5] | [5] | [5] | [5] |
| A [HW0005] Impresora | [3] | [3] | [3] | [5] | [3] | [3] |
| A [HW0006] Móden | [3] | [3] | [3] | [5] | [5] | [6] |
| A [HW0007] access point | [5] | [6] | [3] | [7] | [7] | [4] |
| A [COM0001] Red de Datos | [7] | [5] | [3] | [5] | [7] | [4] |
| A [COM0002] Red Inalámbrica | [7] | [5] | [5] | [5] | [5] | [3] |
| A [COM0003] Wifi | [5] | [5] | [5] | [5] | [5] | [3] |
| A [COM0004] Red local | [5] | [5] | [5] | [5] | [7] | [5] |
| A [COM0005] WAM | [5] | [5] | [5] | [7] | [7] | [5] |
| A [COM0006] VPN | [5] | [5] | [5] | [7] | [7] | [5] |
| A [AUX0001] Fuente de poder | [5] | [3] | [5] | [5] | [5] | [6] |
| A [AUX0002] Ups | [4] | [3] | [5] | [3] | [5] | [6] |
| A [AUX0003] Generador eléctrico | [5] | [7] | [5] | [5] | [5] | [6] |
| A [AUX0004] Aire acondicionado | [5] | [3] | [5] | [3] | [3] | [4] |
| A [AUX0005] Fibra óptica | [5] | [3] | [5] | [7] | [7] | [6] |
| A [Media0001] CD-ROM | [7] | [7] | [7] | [7] | [7] | [4] |
| A [Media0002] Memoria USB | [7] | [7] | [7] | [7] | [7] | [4] |
| Dominios de seguridad | | | | | | |
| [base] Red corporativa | [9] | [7] | [9] | [9] | [9] | [6] |
| [bps] Conexión a internet | [7] | [7] | [7] | [7] | [7] | [6] |

*Fuente: Elaboración Propia*

**Nivel de Vulnerabilidades**

Se refiere al grado o la magnitud de las vulnerabilidades presentes en un sistema, aplicación, red o entorno de tecnología de la información. En el contexto de la seguridad de la información, se utiliza para evaluar el riesgo y la exposición potencial a amenazas y ataques cibernéticos. Los niveles de vulnerabilidades pueden variar desde bajos hasta altos, y se pueden clasificar de diferentes maneras, como se detalla a continuación.

**Figura 7:** *Nivel de criticidad de vulnerabilidades en los activos de información*



[C0002] A. Análisis de riesgos > A.6. Riesgo

Exportar

potencial | current | target | PILAR

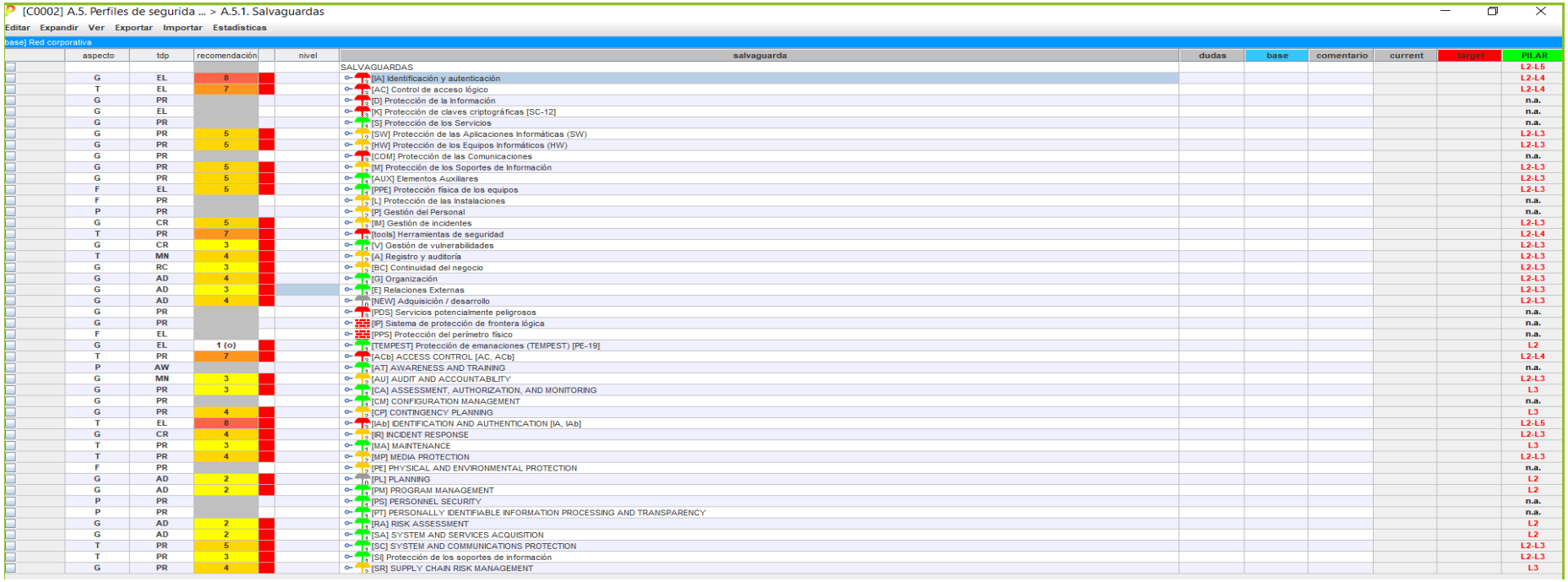
| activo | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|
| ACTIVOS | (6,6) | (5,7) | (6,6) | (5,1) | (5,7) |
| I [ES0001] Datos del negocio | (3,1) | (2,2) | (4,2) | | (5,7) |
| S [ES0002] Servicio | (4,2) | (3,9) | (5,4) | (3,9) | (4,5) |
| P [ES0003] Procesos del negocio | (3,7) | (4,5) | (3,1) | | (5,7) |
| A [SW0001] BD Mysql | (5,1) | (5,1) | (5,4) | (2,7) | (4,5) |
| A [SW0002] Aplicaciones propias | (6,2) | (5,1) | (6,6) | | (5,7) |
| A [SW0003] Aplicaciones a terceros | (6,2) | (5,1) | (6,6) | | (5,7) |
| A [SW0004] Antivirus | (6,6) | (5,1) | (6,6) | | (5,7) |
| A [SW0005] Servidor www | (5,1) | (5,1) | (5,4) | (2,7) | (4,5) |
| A [SW0006] Ofimática | (6,2) | (5,1) | (6,6) | | (5,7) |
| A [SW0007] SO Windows | (6,2) | (5,7) | (6,6) | | (5,7) |
| A [HW0001] Servidor | (6,6) | (4,5) | (5,7) | | (5,7) |
| A [HW0002] Laptop, pc | (6,6) | (4,5) | (5,7) | | (5,7) |
| A [HW0003] Celulares | (6,6) | (3,3) | (5,7) | | (5,7) |
| A [HW0004] Equipo respaldo | (6,6) | (4,5) | (5,7) | | (5,7) |
| A [HW0005] Impresora | (6,6) | (3,3) | (5,7) | | (5,7) |
| A [HW0006] Módem | (5,4) | (3,3) | (4,5) | (3,9) | (4,5) |
| A [HW0007] access point | (5,4) | (4,5) | (4,5) | (5,1) | (4,5) |
| A [COM0001] Red de Datos | (5,4) | (3,9) | (4,5) | (5,1) | (4,5) |
| A [COM0002] Red Inalámbrica | (5,4) | (3,9) | (4,5) | (5,1) | (4,5) |
| A [COM0003] Wifi | (5,4) | (3,9) | (4,5) | (5,1) | (4,5) |
| A [COM0004] Red local | (5,4) | (3,9) | (4,5) | (5,1) | (4,5) |
| A [COM0005] WAM | (4,2) | (3,9) | (4,2) | (5,1) | (4,5) |
| A [COM0006] VPN | (5,4) | (3,9) | (4,5) | (5,1) | (4,5) |
| A [AUX0001] Fuente de poder | (6,2) | (3,3) | (4,2) | | (5,7) |
| A [AUX0002] Ups | (3,7) | (3,3) | (4,2) | | (5,7) |
| A [AUX0003] Generador eléctrico | (4,2) | (5,7) | (4,2) | | (5,7) |
| A [AUX0004] Aire acondicionado | (4,5) | (3,3) | (4,2) | | (5,7) |
| A [AUX0005] Fibra óptica | (5,1) | (2,7) | (4,5) | (5,1) | (4,5) |
| A [Media0001] CD-ROM | (6,2) | (5,7) | (6,2) | | (5,7) |
| A [Media0002] Memoria USB | (6,2) | (5,7) | (6,2) | | (5,7) |

*Fuente: Elaboración Propia*

## Evaluación de Salvaguardas

La evaluación de salvaguardas es un proceso mediante el cual se analizan y evalúan las medidas de seguridad implementadas para proteger activos, información o sistemas de posibles amenazas o riesgos. Este proceso se implementó en diversas áreas de la empresa, como la seguridad de la información, la seguridad de la tecnología de la información (TI), la seguridad física y la seguridad en general obteniendo los siguientes resultados.

**Figura 8:** *Identificación de salvaguardas en los activos de información*



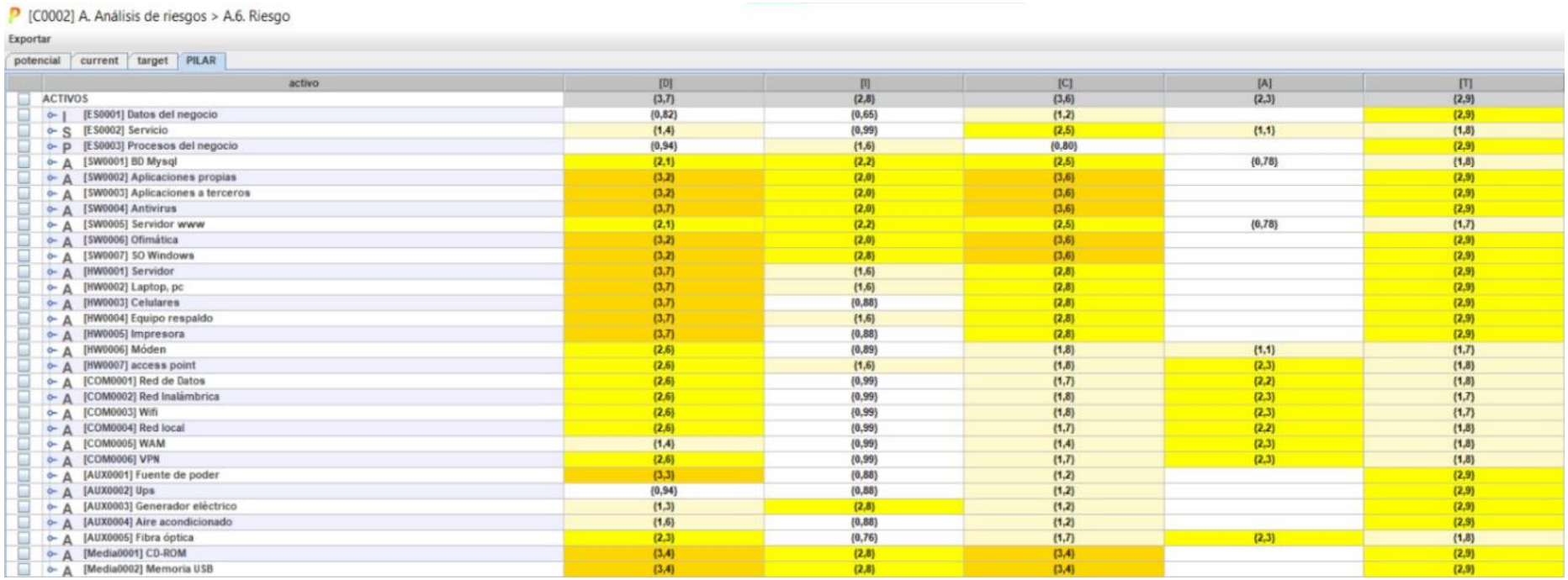

| | aspecto | tdp | recomendación | | nivel | salvaguarda | dudas | base | comentario | current | target | PILAR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | SALVAGUARDAS | | | | | | L2-L5 |
| | G | EL | 8 | | | [IA] Identificación y autenticación | | | | | | L2-L4 |
| | T | EL | 7 | | | [AC] Control de acceso lógico | | | | | | L2-L4 |
| | G | PR | | | | [D] Protección de la Información | | | | | | n.a. |
| | G | EL | | | | [K] Protección de claves criptográficas [SC-12] | | | | | | n.a. |
| | G | PR | | | | [S] Protección de los Servicios | | | | | | n.a. |
| | G | PR | 5 | | | [SW] Protección de las Aplicaciones Informáticas (SW) | | | | | | L2-L3 |
| | G | PR | 5 | | | [HW] Protección de los Equipos Informáticos (HW) | | | | | | L2-L3 |
| | G | PR | | | | [COM] Protección de las Comunicaciones | | | | | | n.a. |
| | G | PR | 5 | | | [M] Protección de los Soportes de Información | | | | | | L2-L3 |
| | G | PR | 5 | | | [AUX] Elementos Auxiliares | | | | | | L2-L3 |
| | F | EL | 5 | | | [PPE] Protección física de los equipos | | | | | | L2-L3 |
| | F | PR | | | | [L] Protección de las Instalaciones | | | | | | n.a. |
| | P | PR | | | | [P] Gestión del Personal | | | | | | n.a. |
| | G | CR | 5 | | | [IM] Gestión de incidentes | | | | | | L2-L3 |
| | T | PR | 7 | | | [tools] Herramientas de seguridad | | | | | | L2-L4 |
| | G | CR | 3 | | | [V] Gestión de vulnerabilidades | | | | | | L2-L3 |
| | T | MN | 4 | | | [A] Registro y auditoría | | | | | | L2-L3 |
| | G | RC | 3 | | | [BC] Continuidad del negocio | | | | | | L2-L3 |
| | G | AD | 4 | | | [G] Organización | | | | | | L2-L3 |
| | G | AD | 3 | | | [E] Relaciones Externas | | | | | | L2-L3 |
| | G | AD | 4 | | | [NEW] Adquisición / desarrollo | | | | | | L2-L3 |
| | G | PR | | | | [PDS] Servicios potencialmente peligrosos | | | | | | n.a. |
| | G | PR | | | | [IP] Sistema de protección de frontera lógica | | | | | | n.a. |
| | F | EL | | | | [PPS] Protección del perímetro físico | | | | | | n.a. |
| | G | EL | 1 (o) | | | [TEMPEST] Protección de emanaciones (TEMPEST) [PE-19] | | | | | | L2 |
| | T | PR | 7 | | | [ACb] ACCESS CONTROL [AC, ACb] | | | | | | L2-L4 |
| | P | AW | | | | [AT] AWARENESS AND TRAINING | | | | | | n.a. |
| | G | MN | 3 | | | [AU] AUDIT AND ACCOUNTABILITY | | | | | | L2-L3 |
| | G | PR | 3 | | | [CA] ASSESSMENT, AUTHORIZATION, AND MONITORING | | | | | | L3 |
| | G | PR | | | | [CM] CONFIGURATION MANAGEMENT | | | | | | n.a. |
| | G | PR | 4 | | | [CP] CONTINGENCY PLANNING | | | | | | L3 |
| | T | EL | 8 | | | [IAb] IDENTIFICATION AND AUTHENTICATION [IA, IAb] | | | | | | L2-L5 |
| | G | CR | 4 | | | [IR] INCIDENT RESPONSE | | | | | | L2-L3 |
| | T | PR | 3 | | | [MA] MAINTENANCE | | | | | | L3 |
| | T | PR | 4 | | | [MP] MEDIA PROTECTION | | | | | | L2-L3 |
| | F | PR | | | | [PE] PHYSICAL AND ENVIRONMENTAL PROTECTION | | | | | | n.a. |
| | G | AD | 2 | | | [PL] PLANNING | | | | | | L2 |
| | G | AD | 2 | | | [PM] PROGRAM MANAGEMENT | | | | | | L2 |
| | P | PR | | | | [PS] PERSONNEL SECURITY | | | | | | n.a. |
| | P | PR | | | | [PT] PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY | | | | | | n.a. |
| | G | AD | 2 | | | [RA] RISK ASSESSMENT | | | | | | L2 |
| | G | AD | 2 | | | [SA] SYSTEM AND SERVICES ACQUISITION | | | | | | L2 |
| | T | PR | 5 | | | [SC] SYSTEM AND COMMUNICATIONS PROTECTION | | | | | | L2-L3 |
| | T | PR | 3 | | | [SI] Protección de los soportes de información | | | | | | L2-L3 |
| | G | PR | 4 | | | [SR] SUPPLY CHAIN RISK MANAGEMENT | | | | | | L3 |

*Fuente: Elaboración Propia*

**Impacto**

Una vez que se han ajustado las configuraciones de los límites en todos los activos de información de la empresa, el software lleva a cabo de manera automática la evaluación del grado de impacto de cada categoría en función de los niveles definidos por la metodología Magerit, además luego de aplicar la norma ISO 27001 en los activos de información, estos deberían estar dentro de los valores mostrados.

**Figura 9:** *Valores permitidos para cumplir los estándares de la ISO 27001*



[C0002] A. Análisis de riesgos > A.6. Riesgo

Exportar

potencial | current | target | PILAR

| | activo | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|---|
| | ACTIVOS | (3,7) | (2,8) | (3,6) | (2,3) | (2,9) |
| I | [ES0001] Datos del negocio | (0,82) | (0,65) | (1,2) | | (2,9) |
| S | [ES0002] Servicio | (1,4) | (0,99) | (2,5) | (1,1) | (1,8) |
| P | [ES0003] Procesos del negocio | (0,94) | (1,6) | (0,80) | | (2,9) |
| A | [SW0001] BD Mysql | (2,1) | (2,2) | (2,5) | (0,78) | (1,8) |
| A | [SW0002] Aplicaciones propias | (3,2) | (2,0) | (3,6) | | (2,9) |
| A | [SW0003] Aplicaciones a terceros | (3,2) | (2,0) | (3,6) | | (2,9) |
| A | [SW0004] Antivirus | (3,7) | (2,0) | (3,6) | | (2,9) |
| A | [SW0005] Servidor www | (2,1) | (2,2) | (2,5) | (0,78) | (1,7) |
| A | [SW0006] Ofimática | (3,2) | (2,0) | (3,6) | | (2,9) |
| A | [SW0007] SO Windows | (3,2) | (2,8) | (3,6) | | (2,9) |
| A | [HW0001] Servidor | (3,7) | (1,6) | (2,8) | | (2,9) |
| A | [HW0002] Laptop, pc | (3,7) | (1,6) | (2,8) | | (2,9) |
| A | [HW0003] Celulares | (3,7) | (0,88) | (2,8) | | (2,9) |
| A | [HW0004] Equipo respaldo | (3,7) | (1,6) | (2,8) | | (2,9) |
| A | [HW0005] Impresora | (3,7) | (0,88) | (2,8) | | (2,9) |
| A | [HW0006] Móden | (2,6) | (0,89) | (1,8) | (1,1) | (1,7) |
| A | [HW0007] access point | (2,6) | (1,6) | (1,8) | (2,3) | (1,8) |
| A | [COM0001] Red de Datos | (2,6) | (0,99) | (1,7) | (2,2) | (1,8) |
| A | [COM0002] Red Inalámbrica | (2,6) | (0,99) | (1,8) | (2,3) | (1,7) |
| A | [COM0003] Wifi | (2,6) | (0,99) | (1,8) | (2,3) | (1,7) |
| A | [COM0004] Red local | (2,6) | (0,99) | (1,7) | (2,2) | (1,8) |
| A | [COM0005] WAM | (1,4) | (0,99) | (1,4) | (2,3) | (1,8) |
| A | [COM0006] VPN | (2,6) | (0,99) | (1,7) | (2,3) | (1,8) |
| A | [AUX0001] Fuente de poder | (3,3) | (0,88) | (1,2) | | (2,9) |
| A | [AUX0002] Ups | (0,94) | (0,88) | (1,2) | | (2,9) |
| A | [AUX0003] Generador eléctrico | (1,3) | (2,8) | (1,2) | | (2,9) |
| A | [AUX0004] Aire acondicionado | (1,6) | (0,88) | (1,2) | | (2,9) |
| A | [AUX0005] Fibra óptica | (2,3) | (0,76) | (1,7) | (2,3) | (1,8) |
| A | [Media0001] CD-ROM | (3,4) | (2,8) | (3,4) | | (2,9) |
| A | [Media0002] Memoria USB | (3,4) | (2,8) | (3,4) | | (2,9) |

*Fuente: Elaboración Propia*

**Niveles de criticidad**

Son los valores en la escala de 0 a 9 determinados para evaluar el nivel de criticidad de las vulnerabilidades, de la misma manera verificar el nivel permitido para el cumplimiento de la ISO 27001.

***Figura 10:*** *escala de valores del nivel de criticidad*

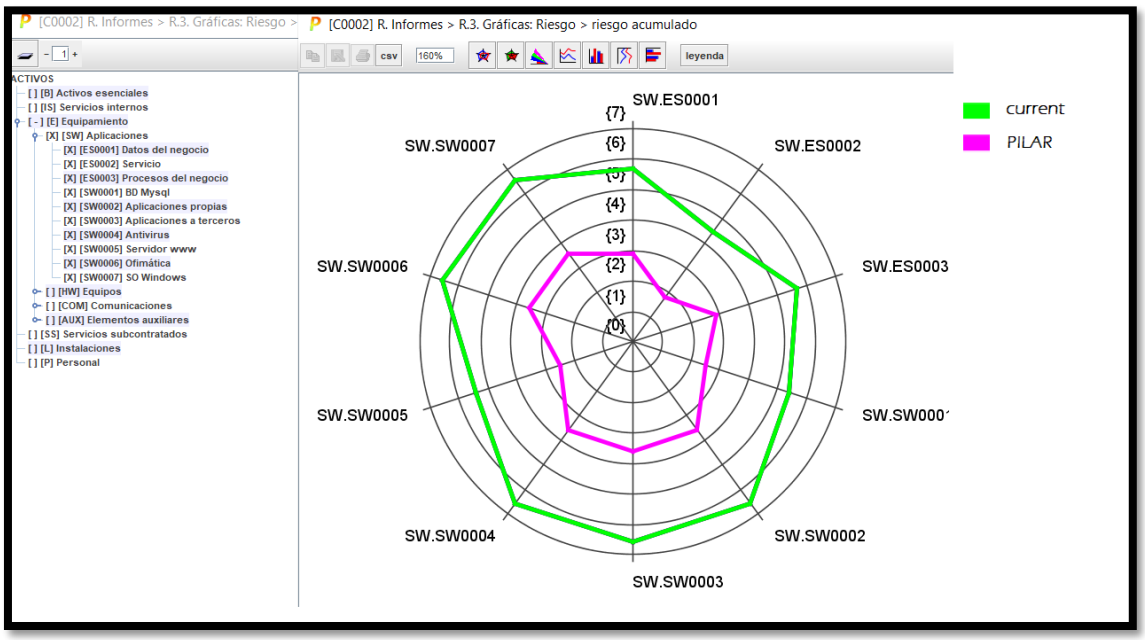

*Fuente: Elaboración Propia*

**Informes del software PILAR**

**Riesgos acumulados de los activos de información de la categoría Aplicaciones**

Resultado actual del nivel de criticidad y proyección sugerida por el software PILAR realizado en la categoría Aplicaciones, donde propone aumentar la seguridad en las aplicaciones evaluadas (Ver figura 11).

**Figura 11:** *Nivel de riesgos acumulados actual y nivel propuesto por el software PILAR en la categoría aplicaciones*

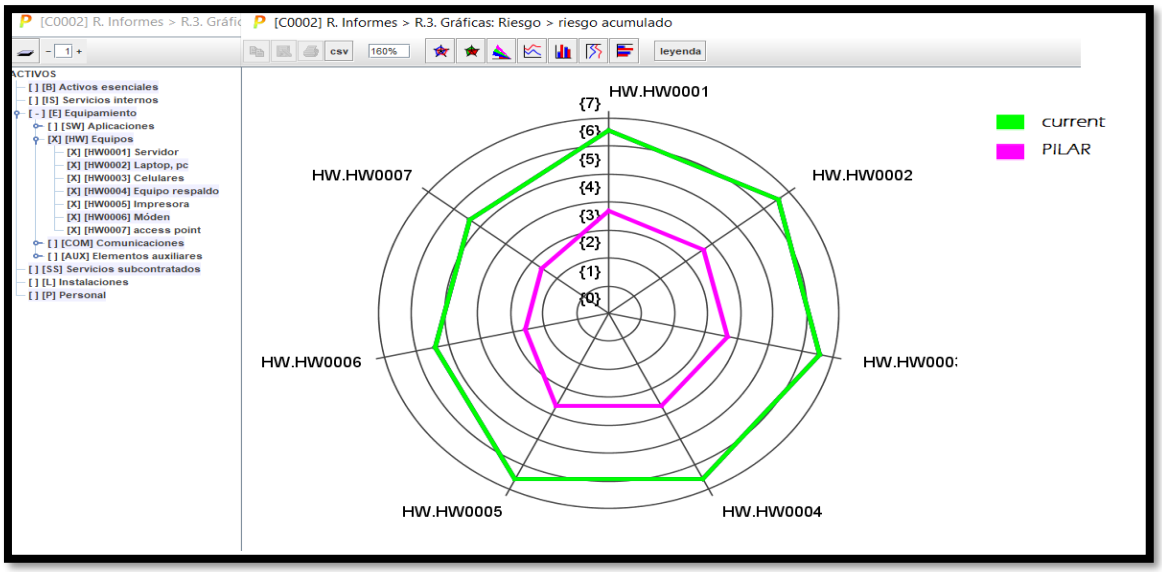



*Fuente: Elaboración Propia*

## Riesgos acumulados de los activos de información de la categoría Equipos

Resultado actual del nivel de criticidad y proyección sugerida por el software PILAR realizado en la categoría Equipos, donde propone mejorar el nivel de privacidad, integridad y disponibilidad de los hardware (Ver figura 12).

**Figura 12:** *Nivel de riesgos acumulados actual y nivel propuesto por el software PILAR en la categoría equipos*

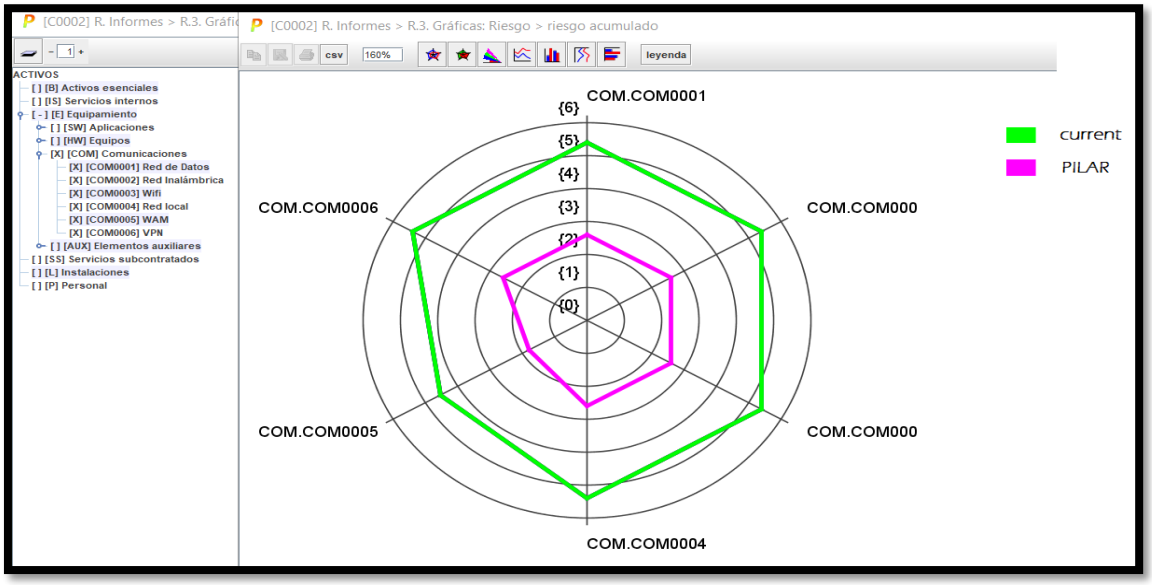



*Fuente: Elaboración Propia*

**Riesgos acumulados de los activos de información de la categoría Comunicaciones**

Resultado actual del nivel de criticidad y proyección sugerida por el software PILAR realizado en la categoría Comunicaciones, donde propone mejorar el nivel de conectividad, y seguridad de redes (Ver figura 13).

**Figura 13:** *Nivel de riesgos acumulados actual y nivel propuesto por el software PILAR en la categoría comunicaciones*

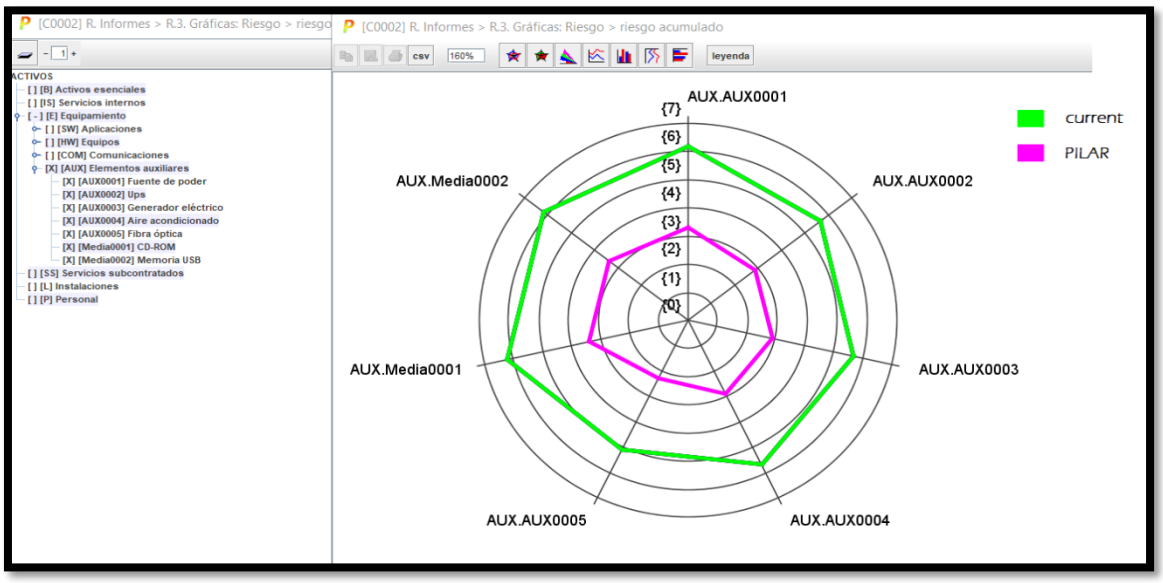



*Fuente: Elaboración Propia*

**Riesgos acumulados de los activos de información de la categoría Elementos auxiliares**

Resultado actual del nivel de criticidad y proyección sugerida por el software PILAR realizado en la categoría Elementos auxiliares, donde propone implementar el área de informática con equipos básicos para el buen funcionamiento y disponibilidad (Ver figura 14).

**Figura 14:** *Nivel de riesgos acumulados actual y nivel propuesto por el software PILAR en la categoría elementos auxiliares*

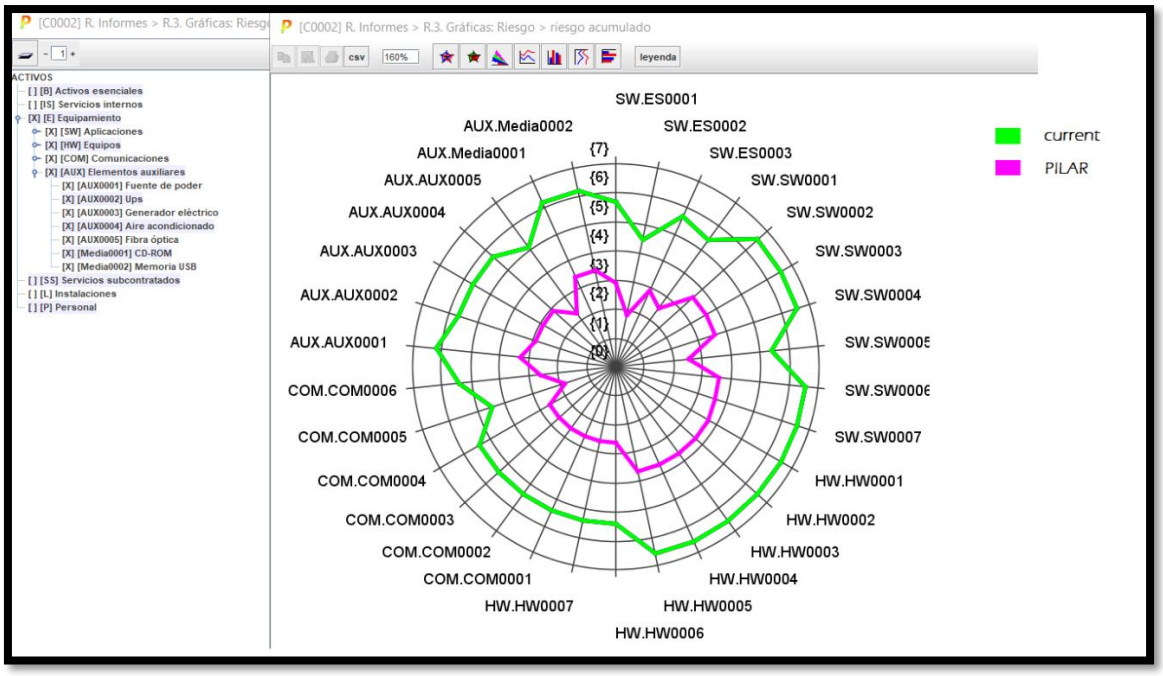



*Fuente: Elaboración Propia*

**Riesgos acumulados de los activos de información General**

Resumen de los riesgos acumulados en todas las categorías evaluadas (Ver figura 15).

**Figura 15:** *Nivel de riesgos acumulados - general*




*Fuente: Elaboración Propia*

**Identificación de malware en los activos de información**

Para la identicación de malware en los 30 equipos informáticos se utilizó diferentes software, para el pre test se aplicó un antivirus no licenciado, detectando una total de 280 posibles malware, para el postest se aplicó un software licenciado llamado “SpyHunter”, donde nos permitió identificar 260 posibles malware encontrados. Esta información se podrá visualizar con mayor detalle en la fichas de registros (Ver anexo 09 y 10)

**Tabla 9:** *Cantidad de malware identificados pre test y post test - general*

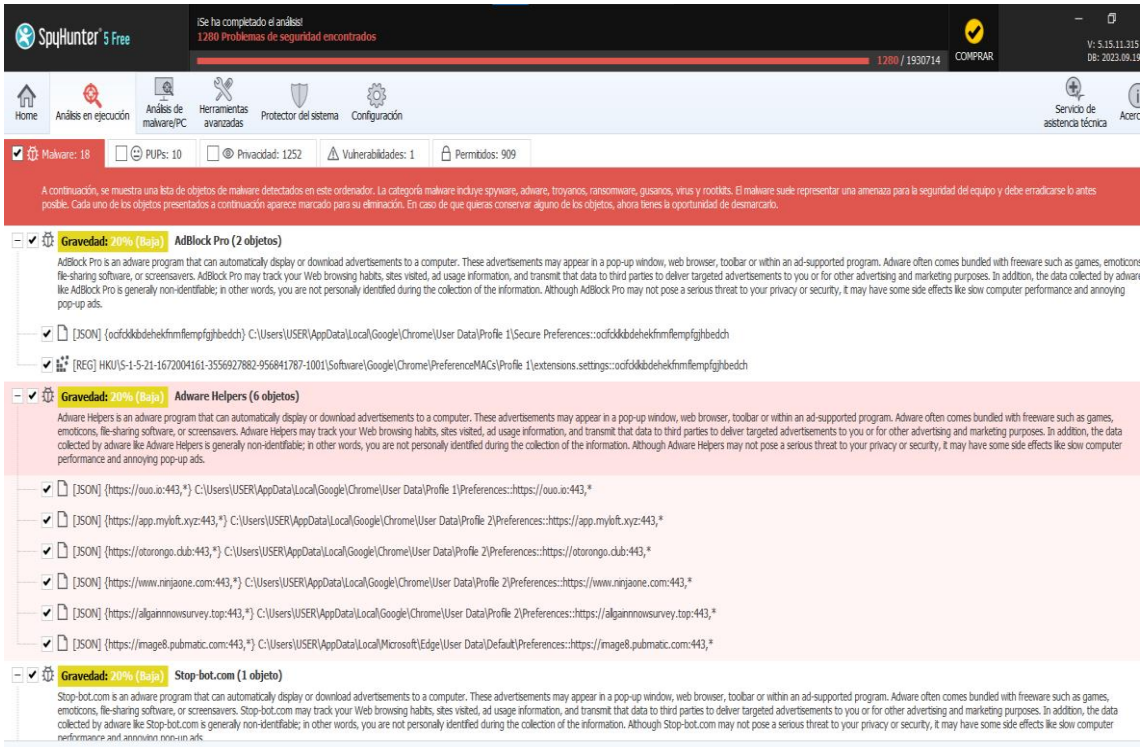
| Ítem | Código | Nombre de Activo | Malware | |
|---|---|---|---|---|
| | | | pre | post |
| 1 | EI001 | SERVIDOR-01 | 18 | 12 |
| 2 | EI002 | SERVIDOR-02 | 07 | 8 |
| 3 | EI003 | SERVIDOR-03 | 04 | 6 |
| 4 | EI004 | PC-01 MONITOREO | 08 | 7 |
| 5 | EI005 | PC-02 MONITOREO | 10 | 8 |
| 6 | EI006 | PC-03 MONITOREO | 05 | 6 |
| 7 | EI007 | PC-04 MONITOREO | 08 | 8 |
| 8 | EI008 | PC-05 MONITOREO | 07 | 9 |
| 9 | EI009 | PC-06 MONITOREO | 05 | 6 |
| 10 | EI010 | PC-07 MONITOREO | 09 | 5 |
| 11 | EI011 | PC-08 MONITOREO | 10 | 11 |
| 12 | EI012 | PC-09 ADMINISTRACIÓN | 08 | 9 |
| 13 | EI013 | PC-10 SECRETARIA | 09 | 9 |
| 14 | EI014 | PC-11 CONTABILIDAD | 06 | 7 |
| 15 | EI015 | PC-12 PROGRAMACIÓN | 12 | 10 |
| 16 | EI016 | PC-13 PROGRAMACIÓN | 10 | 9 |
| 17 | EI017 | PC-14 PROGRAMACIÓN | 08 | 7 |
| 18 | EI018 | PC-15 PROGRAMACIÓN | 06 | 7 |
| 19 | EI019 | Laptop-01 Gerencia General | 11 | 9 |
| 20 | EI020 | Laptop-02 Gerencia TI | 12 | 12 |
| 21 | EI021 | Laptop-03 Gerencia de Proyectos | 09 | 8 |
| 22 | EI022 | Laptop-04 Conf. De GPS | 12 | 11 |
| 23 | EI023 | Memorias USB 01 | 09 | 7 |

| | | | | |
|---|---|---|---|---|
| 24 | EI024 | Memorias USB 02 | 10 | 12 |
| 25 | EI025 | Router 01 | 08 | 8 |
| 26 | EI026 | Router 02 | 11 | 10 |
| 27 | EI027 | Celular 01 | 11 | 9 |
| 28 | EI028 | Celular 02 | 15 | 11 |
| 29 | EI029 | Celular 03 | 09 | 8 |
| 30 | EI030 | Celular 04 | 13 | 11 |
| **TOTAL** | | | **280** | **260** |

*Fuente: Elaboración Propia*

Identificación de malware en los activo de información, detectando un total de 260 malware utilizando el software SpyHunter, luego de ello realizar su posterior mitigación de malware y mostrando efectividad en la acción de eliminación.

**Figura 16:** *Ejemplo de malware encontrado en un activo de información - SpyHunter*




*Fuente: Elaboración Propia*

## 3.6 Método de análisis de datos

Respecto a la estadística descriptiva, es un método de análisis de datos el cual será aplicada en el presente trabajo de investigación. Según Salazar y Del Castillo (2018), este método permite tener un análisis real de una gran cantidad de información, donde se extrae principalmente conclusiones valiosas que aporten al proyecto investigativo (p. 14).

En esta investigación y en relación a los resultados obtenidos en la fase inicial (pretest) y después de la implementación del sistema de gestión de seguridad de la información (postest), procederemos a comparar las hipótesis y evaluar si son confirmadas o refutadas. Para llevar a cabo esta evaluación, utilizamos la Prueba Z para muestras con más de 30 elementos. En este análisis estadístico, nos apoyamos en el software SPSS para determinar los resultados del pretest y postest de manera instantánea. Finalmente, realizamos un análisis de normalidad y, en el caso de muestras grandes (superiores a 50 elementos), empleamos la prueba de Kolmogórov-Smirnov, siguiendo las recomendaciones del autor (Thomas Viehmann, 2021).

Por consiguiente, IBM SPSS es un programa estadístico que mediante sus herramientas permite realizar análisis de datos para luego brindar resultados según la necesidad del usuario.

## 3.7 Aspectos éticos

Los aspectos éticos son fundamentales en cualquier investigación y se refieren a los principios morales y valores que guían el comportamiento ético de los investigadores. Algunos de los aspectos éticos clave que se consideraron en nuestra investigación son:

Consentimiento informado: Los participantes otorgaron su consentimiento libre y consciente para participar en la investigación. Han estado plenamente informados sobre la finalidad, métodos, los riesgos posibles y bondades, así como su libertad a renunciar en el momento que lo consideren oportuno, sin que sufran ninguna consecuencia.

Privacidad y confidencialidad: Se protegió la privacidad y confidencialidad de los participantes, asegurando que su identidad y datos personales se

mantengan en secreto y solo se utilicen con fines de investigación específicos. Esto implica garantizar la seguridad de la información y utilizarlos de manera que no se pueda identificar a los individuos.

Beneficio y no maleficencia: La investigación se diseñó de manera que favorezca a toda la sociedad y los participantes, al tiempo que se minimizan los posibles riesgos y daños. Se tuvo en cuenta el principio de no causar daño intencional o innecesario a los participantes.

Equidad y justicia: Los integrantes fueron considerados de una manera justa y correcta, evitando la discriminación o maltrato de los integrantes. También se consideró la distribución justa de los beneficios y la equidad a la hora de tomar decisiones sobre la investigación.

Integridad científica: La investigación se realizó con integridad científica, evitando el plagio, la fabricación o falsificación de datos y la mala conducta científica en general. Citando adecuadamente las fuentes y respetando los derechos de autor.

Revisión ética: Es importante someter los proyectos de investigación a una revisión ética por parte de comités de ética o instituciones relevantes para garantizar la correcta aplicación de los principios éticos y la protección de los participantes.

Siguiendo las normas establecidas por el código de ética de investigación de la UCV, que fueron aprobadas a través de la RCU N° 470-2022 / UCV (2022). Por ejemplo, el artículo 4º establece la necesidad de obtener el consentimiento de información de los que participen en la investigación, además ofrecer una información veraz y transparente. Según lo expresado y en obediencia a artículo se obtuvo el consentimiento de los directivos de la empresa System Arq. SRL para llevar a cabo este estudio.

Asimismo, se ha cumplido con el "Artículo 9º. 'De la Política anti plagio"', que enfatiza la importancia de realizar una investigación original basada en información veraz. Además, se ha respetado el artículo 10º, que se refiere a los derechos de autor. Se ha proporcionado la información recopilada con las diferentes fuentes bibliográficas y se han citado a los autores de acuerdo con las

normas establecidas en la norma ISO 690. Además, se ha cumplido con el artículo 37 y 44 del Código de Ética del Colegio de Ingenieros del Perú, los cuales hacen referencia al respeto hacia los autores que conforman las investigaciones y la inclusión adecuada de coautores en un trabajo investigativo.

# IV. RESULTADOS

## 4.1. Análisis Descriptivo

En el transcurso de la investigación, se puso en marcha la aplicación de un SGSI, conforme a la norma ISO 27001, con la finalidad de disminuir tanto el porcentaje de ataque malware como el porcentaje de vulnerabilidades en los activos de información frente a los ataques cibernéticos. Para la obtención de los datos iniciales requeridos en el estudio, fue necesario realizar un pre test donde los datos recaudados trataban sobre cada indicador, porcentaje de ataques malware y porcentaje de vulnerabilidades en los activos de información. Posteriormente a ello se implementó el SGSI basado en la ISO 27001 y para medir los resultados se recabó la información mediante un post test donde se registró un cambio eficiente con la aplicación del SGSI nombrado. Los resultados descriptivos de ambos test se presentan en las tablas 10 y 11.

- **INDICADOR: Porcentaje de Ataques Malware**

Los valores descriptivos mostrados proporcionan información detallada sobre las características clave del porcentaje de ataques malware suprimidos, la información incluye la media, minimo, máximo y la desviación estándar del indicador (Ver Tabla 10).

**Tabla 10:** *Valores estadísticos descriptivos del indicador porcentaje de ataques malware*

| Estadísticos descriptivos | | | | | |
|---|---|---|---|---|---|
| | N | Mínimo | Máximo | Media | Desv. estándar |
| PAM_pre_test | 30 | 33.33 | 83.33 | 65.1980 | 11.47220 |
| PAM_post_test | 30 | 12.50 | 53.00 | 34.3403 | 10.98389 |
| N válido (por lista) | 30 | | | | |

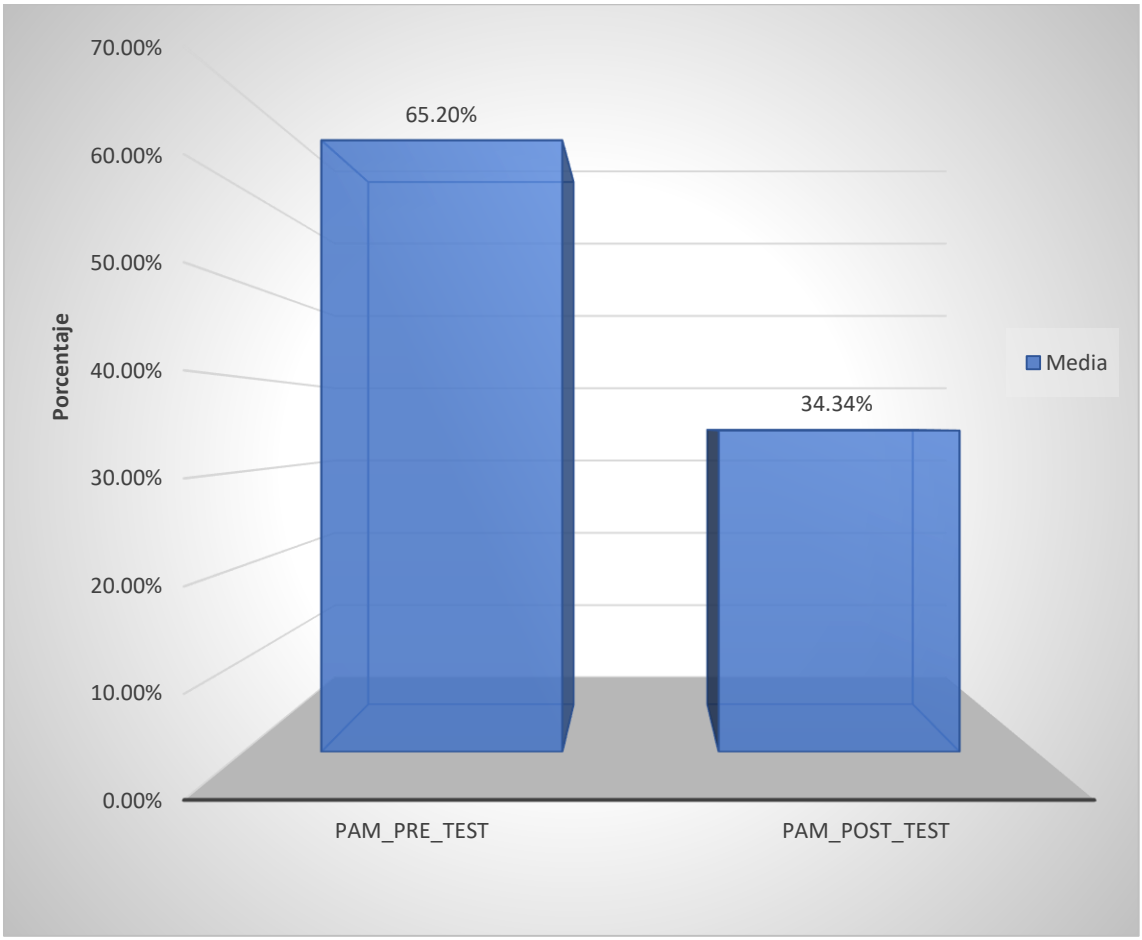
*Fuente: Elaboración Propia*

En lo que respecta al porcentaje de ataques malvare en los activos de información, el valor del porcentaje obtenido en la ficha de registro del pre-test se registró un porcentaje de 65.19%. Asimismo, el porcentaje alcanzado en el post test fue un porcentaje de 34.34%, ambos valores pertenecen a la media del indicador (Ver figura 17). Esto indica una notable disparidad en ambas líneas de tiempo de la implementación de un SGSI basada en la norma ISO 27001;

Además, el porcentaje mínimo de ataques malware fue de 33.33% antes de la implementación y del 12.50% después de adopción del SGSI basada en la norma ISO 27001(ver Tabla 10).

En lo que respecta a la desviación estándar, el porcentaje de ataques malware en el pre test se observó una dispersión del 11.47% y en lo concerniente al post test el porcentaje disminuyó a un 10.98%.

**Figura 17:** *Porcentaje de ataques malware antes y después de implementar el SGSI*




*Fuente: Elaboración Propia*

- **INDICADOR: Porcentaje de Vulnerabilidades en los Activos de Información**

Los valores descriptivos mostrados proporcionan información detallada sobre las características clave del porcentaje de vulnerabilidades en los activos de información. Los datos obtenidos incluyen la media, mínimo, máximo y la desviación estándar del indicador (Ver Tabla 11).

**Tabla 11:** *Valores estadísticos descriptivos del indicador porcentaje de vulnerabilidades en los activos de información*

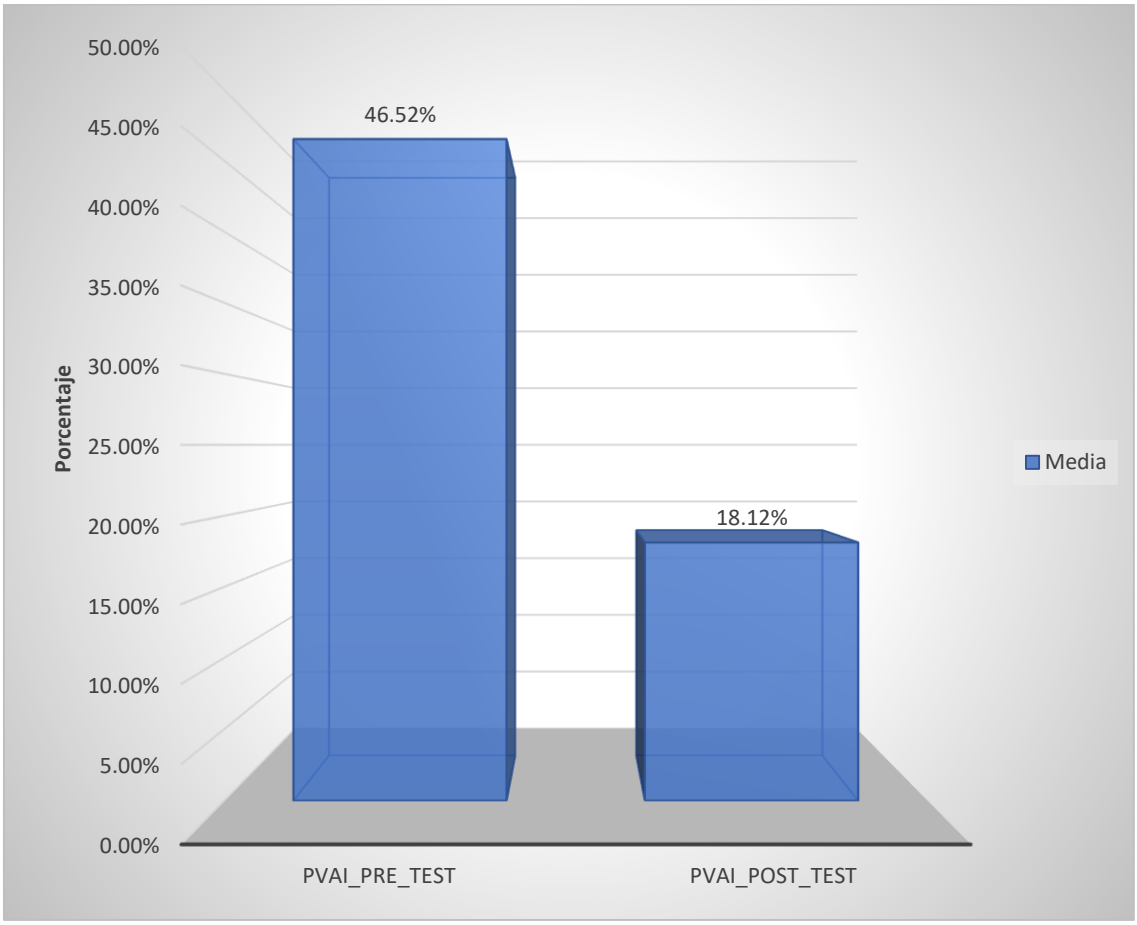
| Estadísticos descriptivos | | | | | |
|---|---|---|---|---|---|
| | N | Mínimo | Máximo | Media | Desv. estándar |
| PVAI_pre_test | 30 | 14.29 | 81.25 | 46.5169 | 17.31681 |
| PVAI_post_test | 30 | 12.50 | 24.14 | 18.1239 | 2.84379 |
| N válido (por lista) | 30 | | | | |

*Fuente: Elaboración Propia*

En lo que concierne al porcentaje de vulnerabilidades en los activos de información frente a los ataques cibernéticos, se aprecia una notable disparidad entre el pre test y el post test. Durante el pre test, el porcentaje obtenido es de 46.51%, mientras que en el post test este valor se redujo significativamente a un 18.12%, demostrado efectividad en la corrección de vulnerabilidades como se evidencia en la figura 18. Esta variación señala una mejora considerable antes y después de la implementación del SGSI basado en la norma ISO 27001. Además, el porcentaje de vulnerabilidades en los activos de información en respuesta a los ataques cibernéticos se mantuvo en un 14.29% antes de la implementación, en contraste con el 12.50% registrado después de la adopción del SGSI basado en la norma ISO 27001 (ver Tabla 11).

En lo que respecta a la variabilidad en el porcentaje de vulnerabilidades en los activos de información, los resultados obtenidos en el pre test se observó una variación de 17.31%. Asimismo, en el post test, esta variabilidad disminuyó de manera significativa, alcanzando un valor de 2.84%.

**Figura 18:** *Porcentaje de vulnerabilidades en los activos de información antes y después de la implementación del SGSI basada en la ISO 27001*




*Fuente: Elaboración Propia*

## 4.2. Análisis Inferencial

### Prueba de Normalidad

Se ejecutaron pruebas de normalidad para evaluar la distribución de ambos indicadores relacionados con el porcentaje de ataques malware y el porcentaje de vulnerabilidades en los activos de información. Se optó por el método de Shapiro-Wilk para realizar el análisis, ya que la muestra fue estratificada y consta con 30 activos, considerado un tamaño de muestra pequeño, de acuerdo con la referencia de los autores Hernández, Fernández y Baptista (2014, p. 376).

Las pruebas se llevaron a cabo utilizando la información de cada indicador e ingresando estos mismos al software estadístico SPSS Statistics 29.0.1, con un nivel de confiabilidad del 95%, sobre los términos siguientes:

Si:

Sig. < 0.05 adopta una distribución no normal

Sig. ≥ 0.05 adopta una distribución normal

Donde:

Sig. P-valor o nivel crítico

A continuación, se muestran los resultados obtenidos:

- **INDICADOR: Porcentaje de Ataques Malware**

Para seleccionar la prueba de hipótesis adecuada, se realizó una revisión de la distribución de los datos, centrándose en determinar si los datos asociados con el porcentaje de ataques cibernéticos exhibían con distribución norma (Ver tabla 12).

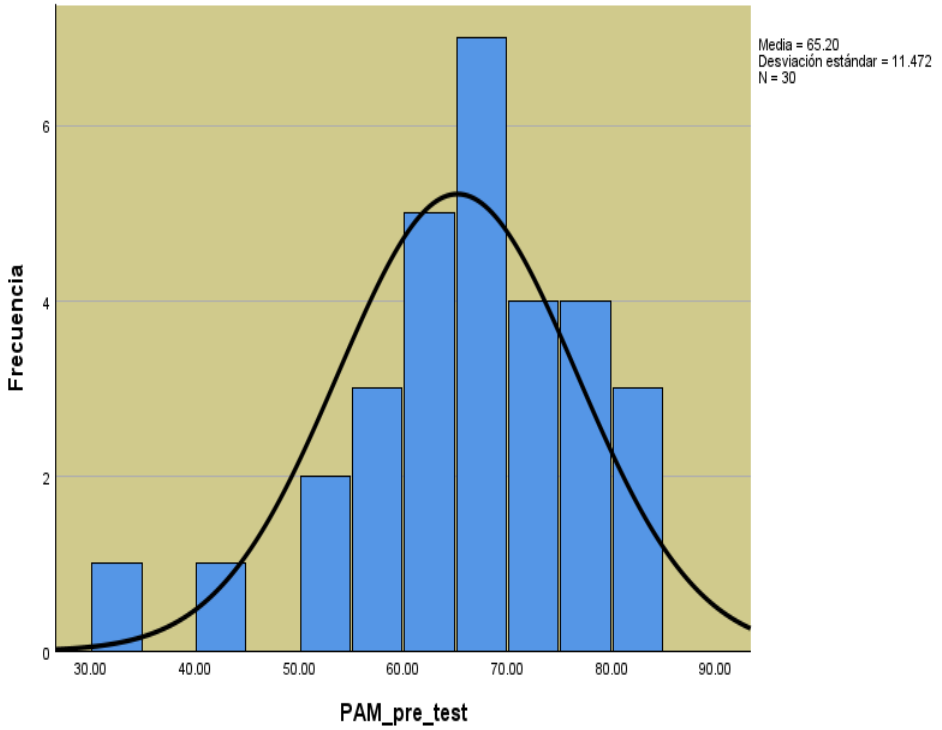
**Tabla 12:** *Prueba de normalidad del indicador porcentaje de ataques malware antes y después de la implementación de SGSI*

| | *Shapiro-Wilk* | | |
|---|---|---|---|
| | *Estadístico* | *gl* | *Sig.* |
| *PAM_pre_test* | *.940* | *30* | *.092* |
| *PAM_post_test* | *.931* | *30* | *.051* |

a. Corrección de significación de Lilliefors
*Fuente: Elaboración Propia*

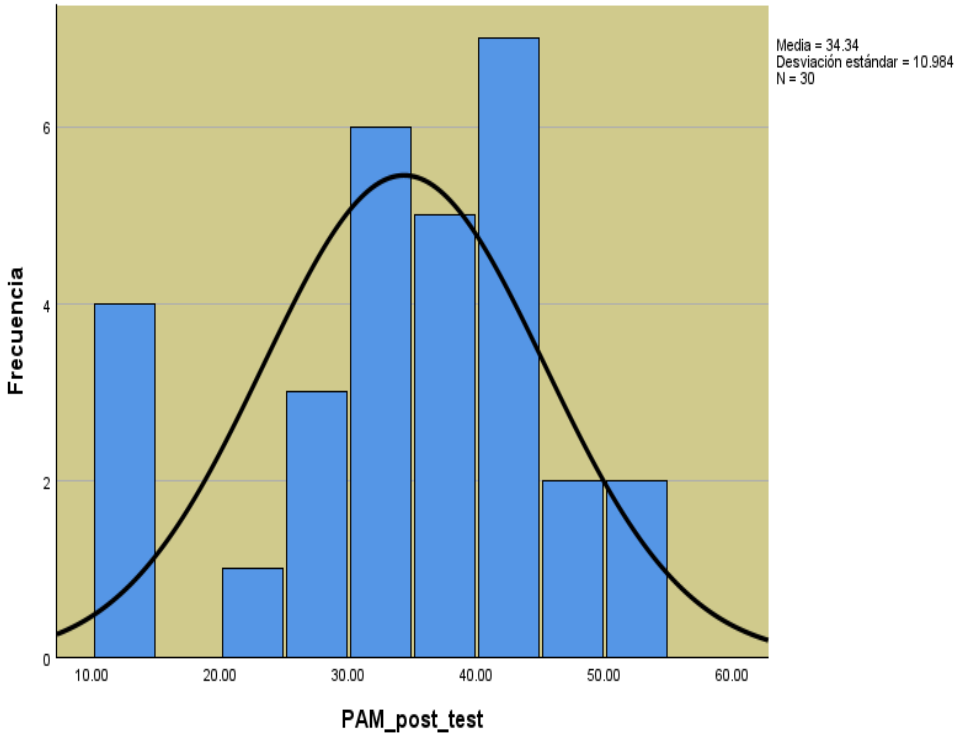
La Tabla 12 y 13, muestran claramente los datos del análisis que revelan el valor de significancia para el porcentaje de ataques de malware en el proceso de ataques cibernéticos durante el pre test fue de 0.092, superando el umbral de 0.05. Esto sugiere que el porcentaje de ataques de malware sigue una distribución normal. De manera similar, las observaciones obtenidas del post test señalan que el valor de significancia relacionado con el porcentaje de ataques de malware fue de 0.051, nuevamente superando 0.05, indicando una distribución normal del indicador. La confirmación de esta distribución normal se puede observar en la figura 19 y 20

**Figura 19:** *Prueba de normalidad del porcentaje de ataques malware antes de implementar el SGSI basado en la ISO 27001*




*Fuente: Elaboración Propia*

**Figura 20:** *Prueba de normalidad del porcentaje de ataques malware después de implementar el SGSI basado en la ISO 27001*




*Fuente: Elaboración Propia*

- **INDICADOR: Porcentaje de Vulnerabilidades en los Activos de Información**

Con el fin de seleccionar la prueba de hipótesis adecuada, se procedió a verificar la distribución de los datos, específicamente para determinar si la información relacionada con la categoría de porcentaje de vulnerabilidades en los activos de información seguía una distribución normal.

**Tabla 13:** *Prueba de Normalidad del indicador porcentaje de vulnerabilidades en los activos de información generados antes y después de la implementación de SGSI*

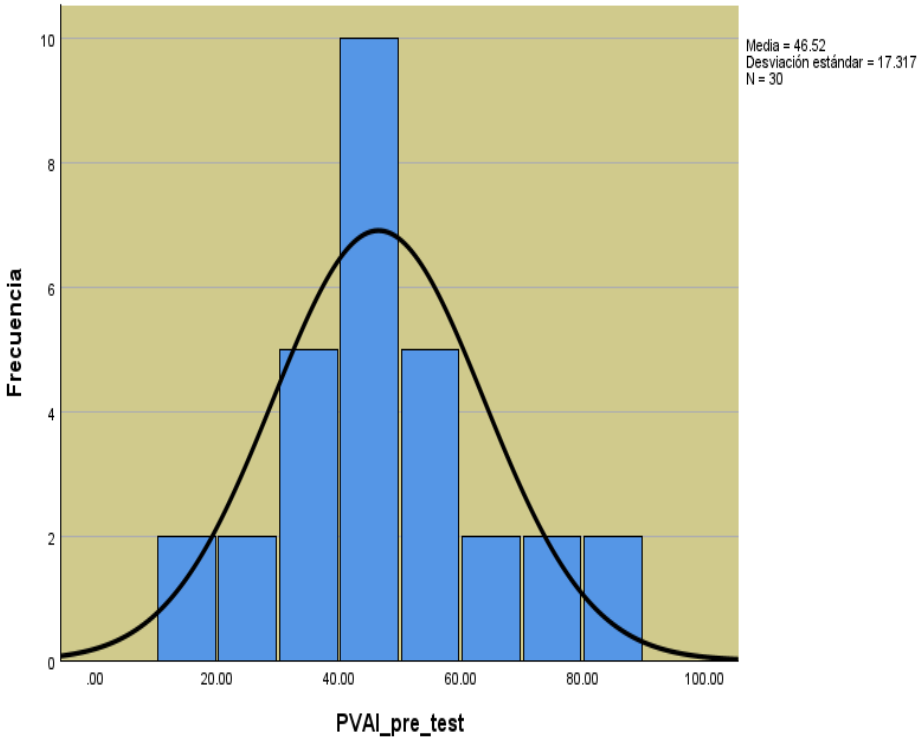
| | Shapiro-Wilk | | |
|---|---|---|---|
| | Estadístico | gl | Sig. |
| PVAI_pre_test | .967 | 30 | .461 |
| PVAI_post_test | .977 | 30 | .736 |

a. Corrección de significación de Lilliefors

*Fuente: Elaboración Propia*

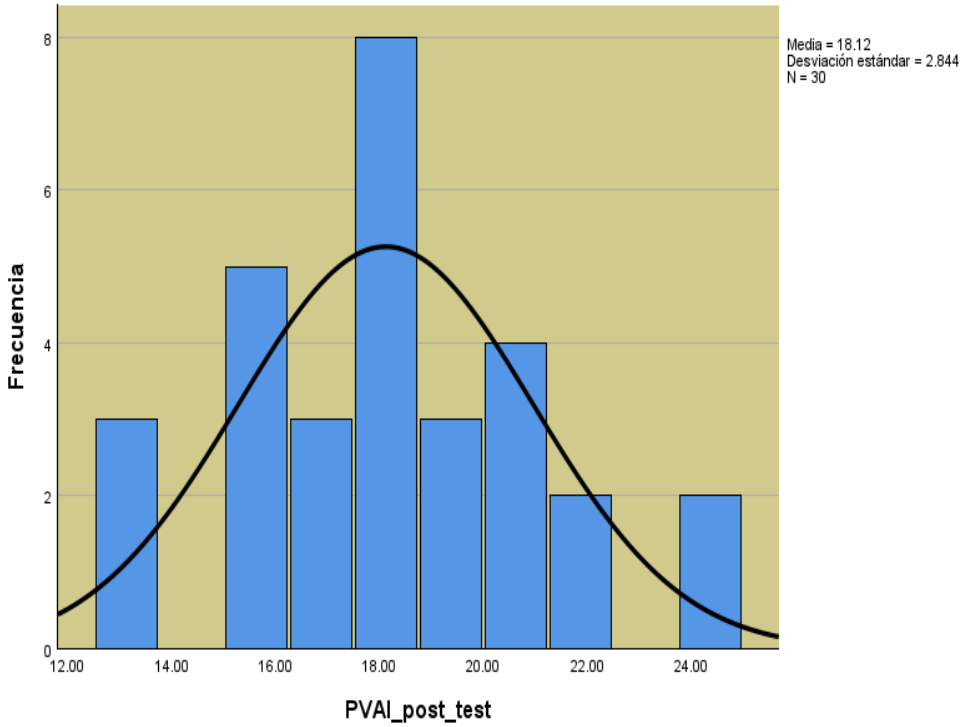
La Tabla 13 muestra claramente los resultados que indican el valor de significancia para la variable “porcentaje de vulnerabilidades en los activos de información” respecto a los ataques cibernéticos en el Pre Test fue de 0.461, lo que excede al umbral de 0.05. Esto sugiere que la distribución de porcentaje de vulnerabilidades en los activos de información sigue en distribución normal. De manera similar, los hallazgos alcanzados en el Post Test concluyen que el nivel de significancia para el porcentaje de vulnerabilidades en los activos de información fue de 0.736, nuevamente superando al valor 0.05, confirmando que la distribución es normal. Esta confirmación normal se puede apreciar en la figura 21 y 22.

**Figura 21:** *Prueba de normalidad del porcentaje de vulnerabilidades en los activos de información antes de implementar el SGSI basado en la ISO 27001*




*Fuente: Elaboración Propia*

**Figura 22:** *Prueba de normalidad del porcentaje de vulnerabilidades en los activos de información después de implementar el SGSI basado en la ISO 27001*




*Fuente: Elaboración Propia*

### 4.3. Prueba de Hipótesis

**Hipótesis de Investigación 1:**

- **H1:** La implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de ataques malware como parte de los ataques cibernéticos en la empresa System Arq S.R.L.
- **Indicador: Porcentaje de ataques malware**

**Hipótesis Estadísticas**

**Definiciones de Variable:**

**PAMa:** Porcentaje de ataques malware antes de utilizar el sistema de seguridad de la información basada en la norma ISO 27001.

**PAMd:** Porcentaje de ataques malware después de utilizar el sistema de seguridad de la información basada en la norma ISO 27001.

- **H0:** La implementación de un sistema de seguridad de la información basada en la norma ISO 27001 no reduce el porcentaje de ataques malware como parte de los ataques cibernéticos en la empresa System Arq S.R.L.

Ho: PAMa >= PAMd

El indicador sin el SGSI basada en la ISO 27001 es mejor que el indicador con el SGSI basada en la ISO 27001.

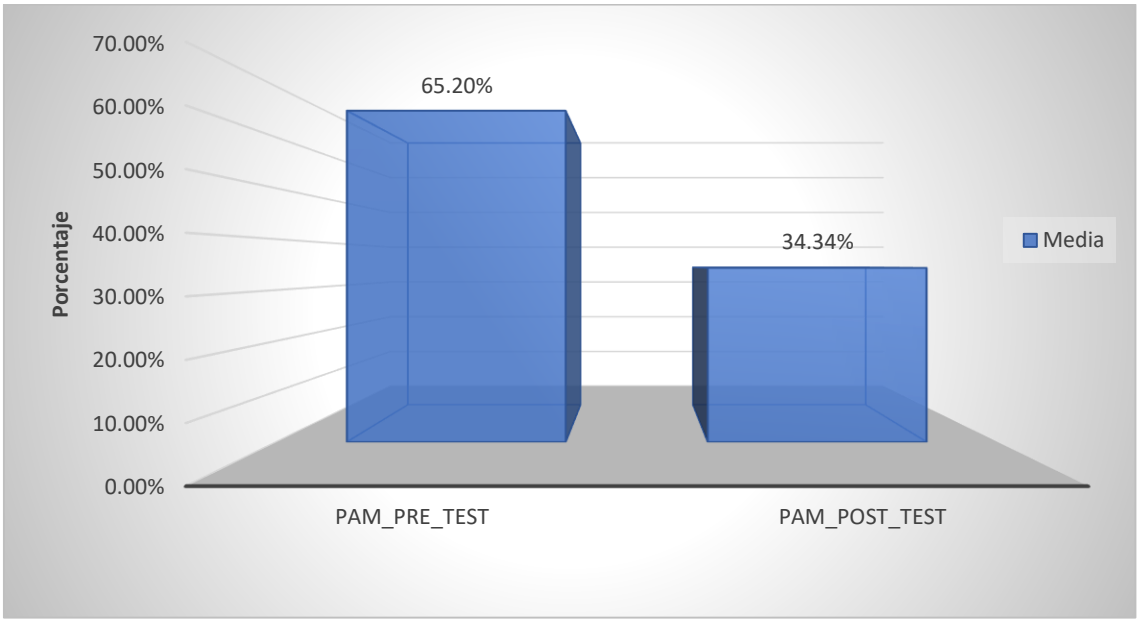
- **HA:** La implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de ataques malware como parte de los ataques cibernéticos en la empresa System Arq S.R.L.

HA: PAMa < PAMd

El indicador con el SGSI basada en la ISO 27001 es mejor que el indicador sin el SGSI basada en la ISO 27001.

En la figura 23, se logra apreciar el porcentaje ataques malware en ambos test, en el Pre Test el porcentaje equivale a 65.20% mientras tanto en lo que respecta al Post Test el resultado del porcentaje es de 34.34%.

**Figura 23:** *Porcentaje de ataques malware – Comparativa General*




*Fuente: Elaboración Propia*

Según la figura 23 se evidencia que existe una reducción de porcentaje de ataques malware, ello se logra validar al comparar el resultados de las medias de ambos test, que desciende de 65.20% al valor 34.34%.

En lo que respecta al resultado de análisis de hipótesis, se utilizó la Prueba T de Student, ya que los datos recopilados durante la investigación (Pre-Test y Post-Test) siguen en distribución normal. El valor de la prueba T es 13.784, lo cual es significativamente inferior a 1.6991 (Ver tabla 14).

**Tabla 14:** *Prueba de T-Student del porcentaje de ataques malware ante los ataques cibernéticos antes y después de implementar el SGSI basada en la ISO 27001.*

| | Media | Prueba de T-Student | | |
|---|---|---|---|---|
| | | T | gl | Sig. (bilateral) |
| PAM_Pretest | 65.1980 | 13.784 | 29 | .001 |
| PAM_Postest | 34.3403 | | | |

*Fuente: Elaboración Propia*

En consecuencia, se refuta la hipótesis nula y se adopta la hipótesis alternativa con un nivel de confianza del 95%. Adicionalmente, el valor T obtenido, de acuerdo como se ilustra en la Figura 24, se coloca en la región de

rechazo. Por ende, se respalda que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de ataques malware como parte de los ataques cibernéticos en la empresa System Arq S.R.L.

**Aplicando la fórmula T Student:**

$$Tc = \frac{X - u}{S / \sqrt{n}}$$

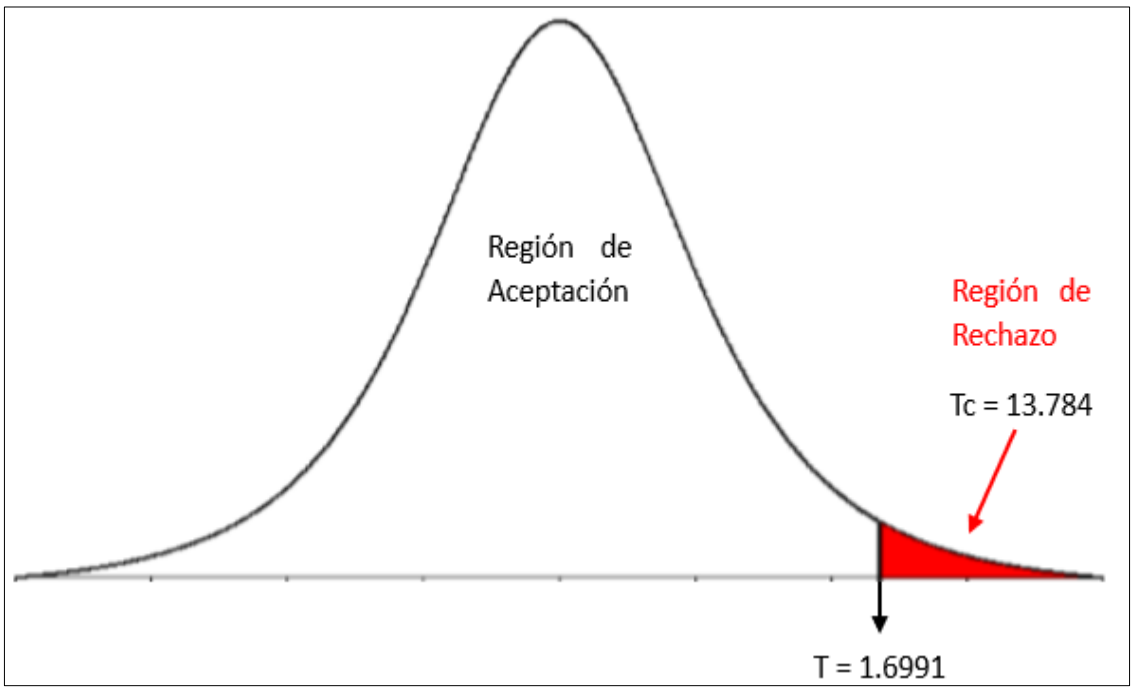
$$Tc = \frac{6520 - 3434}{12.26156 / \sqrt{30}}$$

$$Tc = \frac{-3085}{12.26156 / 5.4772}$$

$$Tc = \frac{3086}{2.2387}$$

$$Tc = 13.784$$

**Figura 24***: Prueba T-Student – Porcentaje de ataques malware*




*Fuente: Elaboración Propia*

**Hipótesis de Investigación 2:**

- **H1:** La implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de vulnerabilidades en los activos de información ante ataques cibernéticos en la empresa System Arq S.R.L.

- **Indicador: Porcentaje de Vulnerabilidades en los Activos de Información**

**Hipótesis Estadísticas**

**Definiciones de Variable:**

**PVAIa:** Porcentaje de vulnerabilidades en los activos de información antes de utilizar el sistema de seguridad de la información basada en la norma ISO 27001.

**PVAId:** Porcentaje de vulnerabilidades en los activos de información después de utilizar el sistema de seguridad de la información basada en la norma ISO 27001.

- **H0:** La Implementación de un sistema de seguridad de la información basada en la norma ISO 27001 no reduce el porcentaje de vulnerabilidades en los activos de información ante ataques cibernéticos en la empresa System Arq S.R.L.

HO: PVAIa >= PVAId

El indicador sin el SGSI basada en la ISO 27001 es mejor que el indicador con el SGSI basada en la ISO 27001.

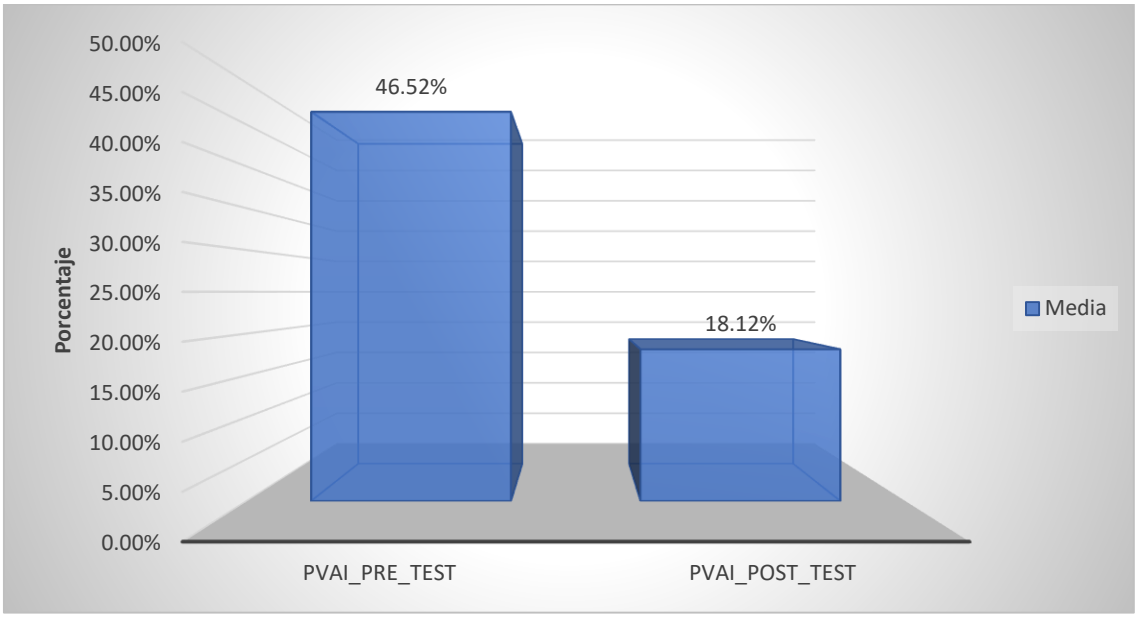
- **HA:** La implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de vulnerabilidades en los activos de información ante ataques cibernéticos en la empresa System Arq S.R.L.

HA: PVAIa < PVAId

El indicador con el SGSI basada en la ISO 27001 es mejor que el indicador sin el SGSI basada en la ISO 27001.

En la figura 25, se logra apreciar el porcentaje vulnerabilidades en los activos de información en ambos test, en el Pre Test el porcentaje equivale a 46.52% mientras que en el Post Test el resultado del porcentaje es de 18.12%.

**Figura 25:** *Porcentaje de vulnerabilidades en los activos de información – Comparativa General*




*Fuente: Elaboración Propia*

Se deduce de la figura 25 que hay una reducción de porcentaje de vulnerabilidades en los activos de información, el cual se puede validar al comparar las medias de ambos test, que asciende de 46.52% al valor 18.12%.

Respecto a la Prueba T-Student fue empleada para analizar el contraste de hipótesis, dada la naturaleza de los datos recolectados durante el estudio (Pre-Test y Post-Test) muestran una distribución normal. Asimismo, el valor del estadístico T resultó ser 8.680, lo cual es significativamente inferior a 1.6991 (consulte la Tabla 15).

**Tabla 15:** *Prueba de T-Student del porcentaje de vulnerabilidades en activos de información ante los ataques cibernéticos antes y después de implementar el SGSI basada en la ISO 27001*

| | Media | Prueba de T-Student | | |
|---|---|---|---|---|
| | | T | gl | Sig. (bilateral) |
| PVAI_Pretest | 46.5169 | 8.680 | 29 | .001 |
| PVAI_Postest | 18.1239 | | | |

Fuente: Elaboración Propia

En consecuencia, se objeta la hipótesis nula, ratificando la hipótesis alterna con un nivel de confiabilidad del 95%. Además, se evidencia en la Figura 26, el valor-T obtenido se sitúa en la región de rechazo. Por ende, la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de vulnerabilidades en los activos de información como parte de los ataques cibernéticos en la empresa System Arq S.R.L.

**Aplicando la fórmula T Student:**

$$Tc = \frac{X - u}{S / \sqrt{n}}$$

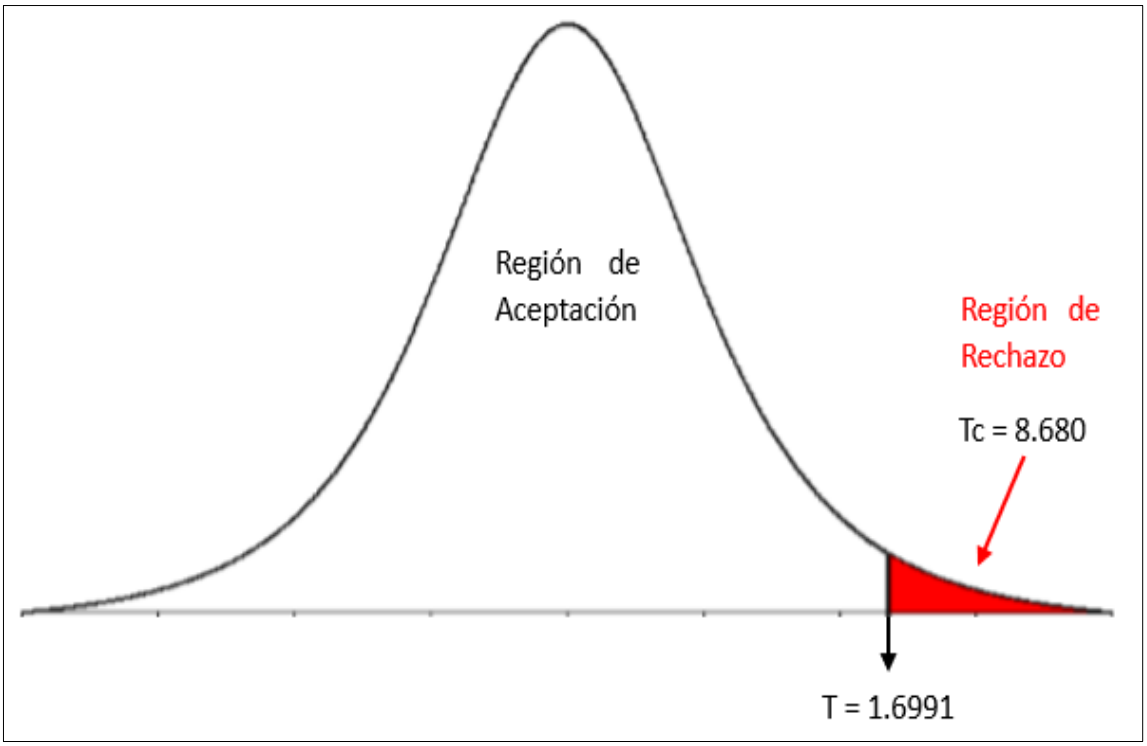
$$Tc = \frac{4652 - 1812}{17.91562 / \sqrt{30}}$$

$$Tc = \frac{2840}{17.91562 / 5.4772}$$

$$Tc = \frac{2738}{3.27095}$$

$$Tc = 8.680$$

**Figura 26:** *Prueba T-Student – Porcentaje de Vulnerabilidades en los Activos de Información*




*Fuente: Elaboración Propia*

# V. DISCUSIÓN

En la presente investigación, tuvo como resultados que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de ataques malware de un 65.20% a un 34.34%.

Asimismo, Fotis Kitsios, Elpiniki Chatzidimitriou y María Kamariotou en el artículo que trata sobre la creación de un enfoque estratégico para la evaluación de riesgos y el impacto en los SGSI y tomando como estudio a industrias de consultoría de tecnología de información, llegaron a la conclusión que es esencial instaurar un SGSI conforme a la norma ISO 27001. Este proceso implica llevar a cabo evaluaciones de riesgos y abordar amenazas o vulnerabilidades identificadas. Además, observaron que los resultados obtenidos de la evaluación de riesgos después de la implementación de la ISO 27001 fueron adecuados, estableciendo un orden de prioridad para los riesgos de seguridad de la información.

Del mismo modo, Huamán Espinoza, Frederick y Ipanama Mendoza Ryder en su investigación, mencionan Técnicas de seguridad de la información centrada en la norma ISO 27001 para supervisar y gestionar vulnerabilidades en pequeñas y medianas empresas, concluyeron que la implementación de un SGSI basado en la norma ISO 27001 demuestra eficacia al aplicar controles y políticas de seguridad en todas las áreas de la empresa. Experimentaron un aumento significativo en la eficiencia del cumplimiento de controles del 31.50% al 88.07% después de la implementación.

La interpretación de los resultados indica que la implementación de un Sistema de Gestión de Seguridad basada en la ISO 27001 reduce el riesgo ante ataques cibernéticos en la Empresa System Arq S.R.L.

# VI.CONCLUSIONES

A continuación, se presenta las conclusiones obtenidas de la investigación:

**PRIMERO:** Se concluye que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de ataques malware en un 30.86%. Por lo que se afirma que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de ataques malware como parte de los ataques cibernéticos.

**SEGUNDO:** Se concluye que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de vulnerabilidades en los activos de información en un 28.4%. Por lo tanto, se afirma que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de vulnerabilidades en los activos de información ante ataques cibernéticos.

**TERCERO:** Se concluye que la implementación de un Sistema de Gestión de Seguridad basada en la ISO 27001 reduce el riesgo ante ataques cibernéticos en la Empresa System Arq S.R.L, lo cual permitió cumplir con los objetivos trazados en esta investigación.

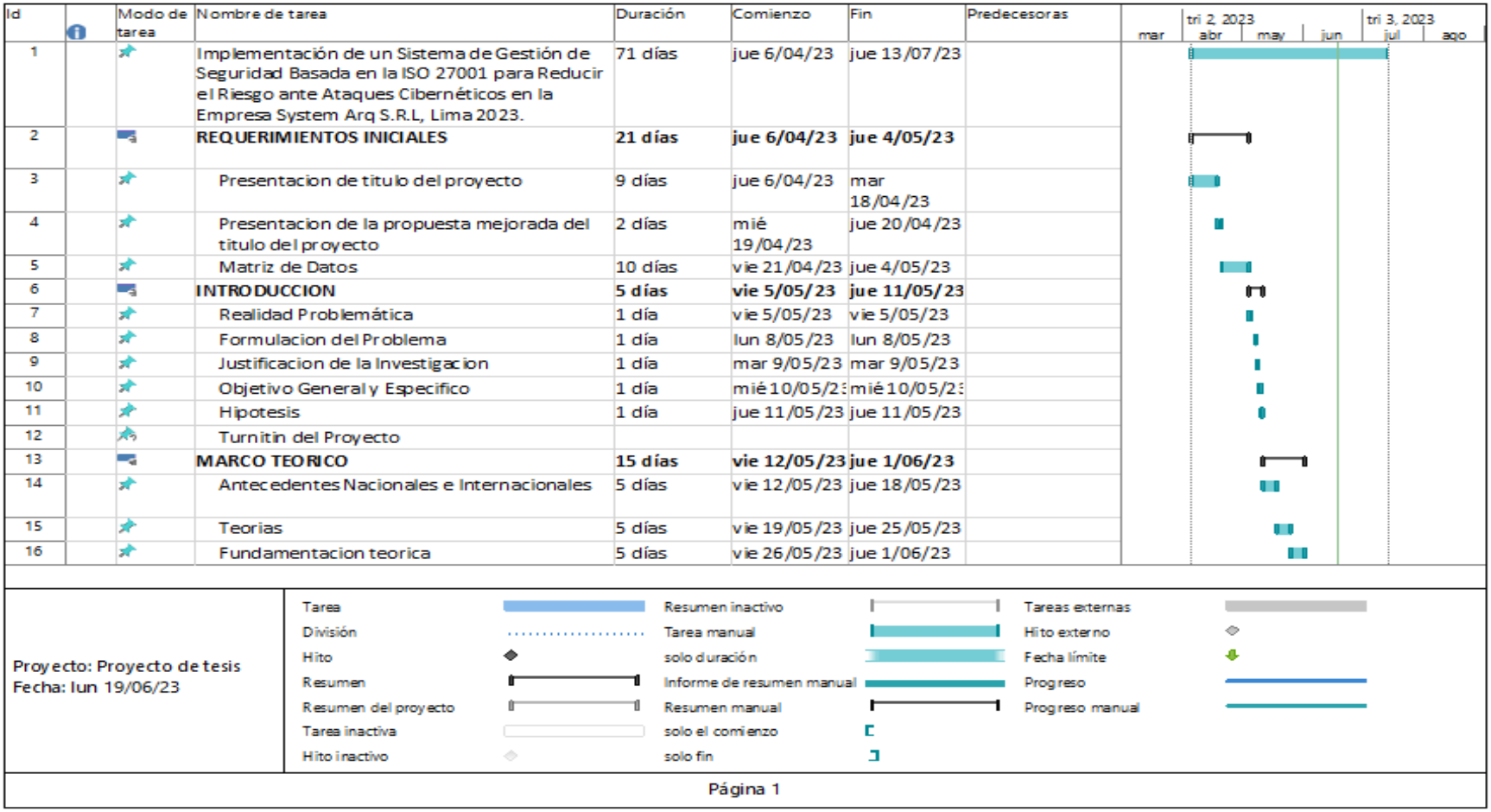
# VII. RECOMENDACIONES

Proteger una empresa contra ataques cibernéticos es un desafío constante en el entorno digital actual. Aquí tienes algunas recomendaciones generales para fortalecer la seguridad de una empresa:

- Implementación de la norma ISO 27001 especialmente a empresas que cuenten con área de tecnología de información.
- Realiza auditorías regulares de seguridad para evaluar el cumplimiento de las políticas de seguridad e identificar posibles mejoras.
- Desarrollar y aplicar políticas de seguridad cibernética claras. Estas políticas deben abordar el uso de contraseñas seguras, el acceso a sistemas, el manejo de dispositivos móviles y otras prácticas de seguridad.
- Mantener todos los sistemas, aplicaciones y dispositivos equipados con las versiones de seguridad más recientes y parches de seguridad.
- Implementar controles de acceso sólidos. Limitar el acceso a sistemas y datos solo a empleados autorizados y emplear autenticación multifactorial como una capa adicional de seguridad.
- Utiliza firewalls y software antivirus actualizados para proteger contra malware y amenazas en línea.
- Realiza copias de seguridad regulares de datos críticos y asegúrate de que las copias de seguridad se almacenen de forma segura y se puedan restaurar eficientemente.

Además, para el manejo de análisis y gestión de riesgos, se recomienda el uso del Software PILAR BASIC, ya que nos permite realizar evaluaciones de vulnerabilidades en la infraestructura y sistemas de la empresa, abordando las debilidades identificadas y siguiendo las mejores prácticas de gestión de vulnerabilidades, asimismo PILAR BASIC permite ahorrar tiempo en la evaluación de las vulnerabilidades aportando de esta manera en la efectividad de la obtención de los resultados y su posterior ejecución.

**Figura 27:** *Cronograma de actividades (1)*

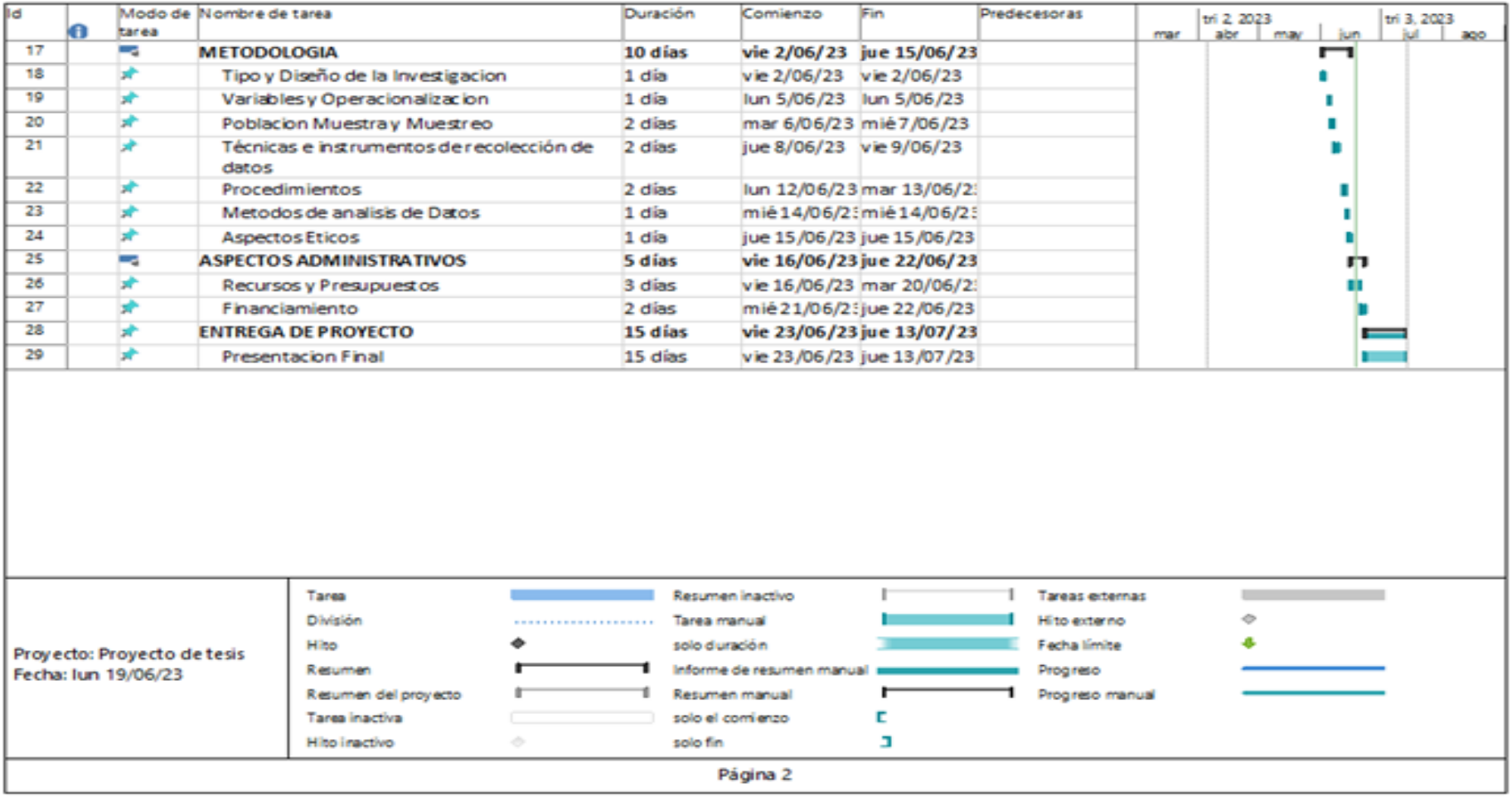


| Id | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin | Predecesoras |
|---|---|---|---|---|---|---|
| 1 | | Implementación de un Sistema de Gestión de Seguridad Basada en la ISO 27001 para Reducir el Riesgo ante Ataques Cibernéticos en la Empresa System Arq S.R.L, Lima 2023. | 71 días | jue 6/04/23 | jue 13/07/23 | |
| 2 | | **REQUERIMIENTOS INICIALES** | **21 días** | **jue 6/04/23** | **jue 4/05/23** | |
| 3 | | Presentacion de titulo del proyecto | 9 días | jue 6/04/23 | mar 18/04/23 | |
| 4 | | Presentacion de la propuesta mejorada del titulo del proyecto | 2 días | mié 19/04/23 | jue 20/04/23 | |
| 5 | | Matriz de Datos | 10 días | vie 21/04/23 | jue 4/05/23 | |
| 6 | | **INTRODUCCION** | **5 días** | **vie 5/05/23** | **jue 11/05/23** | |
| 7 | | Realidad Problemática | 1 día | vie 5/05/23 | vie 5/05/23 | |
| 8 | | Formulacion del Problema | 1 día | lun 8/05/23 | lun 8/05/23 | |
| 9 | | Justificacion de la Investigacion | 1 día | mar 9/05/23 | mar 9/05/23 | |
| 10 | | Objetivo General y Especifico | 1 día | mié 10/05/23 | mié 10/05/23 | |
| 11 | | Hipotesis | 1 día | jue 11/05/23 | jue 11/05/23 | |
| 12 | | Turnitin del Proyecto | | | | |
| 13 | | **MARCO TEORICO** | **15 días** | **vie 12/05/23** | **jue 1/06/23** | |
| 14 | | Antecedentes Nacionales e Internacionales | 5 días | vie 12/05/23 | jue 18/05/23 | |
| 15 | | Teorias | 5 días | vie 19/05/23 | jue 25/05/23 | |
| 16 | | Fundamentacion teorica | 5 días | vie 26/05/23 | jue 1/06/23 | |



*Fuente: Elaboración Propia*

**Figura 28:** *Cronograma de actividades (2)*



| Id | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin | Predecesoras |
|---|---|---|---|---|---|---|
| 17 | | **METODOLOGIA** | **10 días** | **vie 2/06/23** | **jue 15/06/23** | |
| 18 | | Tipo y Diseño de la Investigacion | 1 día | vie 2/06/23 | vie 2/06/23 | |
| 19 | | Variables y Operacionalizacion | 1 día | lun 5/06/23 | lun 5/06/23 | |
| 20 | | Poblacion Muestra y Muestreo | 2 días | mar 6/06/23 | mié 7/06/23 | |
| 21 | | Técnicas e instrumentos de recolección de datos | 2 días | jue 8/06/23 | vie 9/06/23 | |
| 22 | | Procedimientos | 2 días | lun 12/06/23 | mar 13/06/2 | |
| 23 | | Metodos de analisis de Datos | 1 día | mié 14/06/2 | mié 14/06/2 | |
| 24 | | Aspectos Eticos | 1 día | jue 15/06/23 | jue 15/06/23 | |
| 25 | | **ASPECTOS ADMINISTRATIVOS** | **5 días** | **vie 16/06/23** | **jue 22/06/23** | |
| 26 | | Recursos y Presupuestos | 3 días | vie 16/06/23 | mar 20/06/2 | |
| 27 | | Financiamiento | 2 días | mié 21/06/2 | jue 22/06/23 | |
| 28 | | **ENTREGA DE PROYECTO** | **15 días** | **vie 23/06/23** | **jue 13/07/23** | |
| 29 | | Presentacion Final | 15 días | vie 23/06/23 | jue 13/07/23 | |



*Fuente: Elaboración Propia*

## REFERENCIAS


**ANTUNES, Mário, MAXIMIANO, Marisa, GOMES, Ricardo y PINTO, Daniel.**Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. Portugal : Journal of Cybersecurity and Privacy, 2021. Vol. 1, 2.

**ARIAS, José.** Proyecto de Tesis, Guía para la Elaboración. Perú : Hecho el Depósito Legal en la Biblioteca Nacional del Perú, 2020. Vol. 1, p.60.
ISSN: 978-612-00-5416-1.

**ARINA, Alexei.** Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard. Moldavia : Journal of Social Sciences, 2021. Vol. 1, 4. p.86.
ISSN: 2587-3490.

**ARISPE, Claudia, YANGALI, Judith, GUERRERO, María, LOZADA, Oriana, ACUÑA, Luis y ARELLANO, César.** La Investigación Científica. Ecuador : Universidad Internacional del Ecuador, 2020. Vol. 1, p.74.
ISSN: 978-9942-38-578-9.

**ARMAS, Jimmy.** Ciberseguridad: Cómo tomar medidas para proteger sus activos de información. Perú : Review of Global Management, 2020. Vol. 4, 2. p.21.

**BAENA, Guillermina.** Metodología de la investigación. México : Grupo Editorial Patria, 2017. Vol. 3, p 18.
ISSN-e: 978-607-744-748-1.

**CANDO, Mauricio y MEDINA, Ricardo.** Prevención en Ciberseguridad: Enfocada a Los Procesos De Infraestructura Tecnológica. Ecuador : s.n., 2021. Vol. 10, 17-40. p.18.
ISSN-e: 2254-6529.

**CHIDUKWANI, Alladean, ZANDER, Sebastian y KOUTSAKIS, Polychronis.** A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. Australia : IEEE Access, 2022. Vol. 10. p.85701.

**CIEZA CELIS, Jesús Abelardo; OJEDA ROMERO, Anthony Jhonatan,** 2022. *Evaluación del desempeño de protocolos de seguridad para combatir ataques en redes inalámbricas wi-fi* [en línea]. Tesis grado. Chiclayo: UNIVERSIDAD Señor de Sipán [consulta: setiembre 2023]. Disponible en: https://hdl.handle.net/20.500.12802/10055

**CURAY CALUCHO, María Fabiola**, 2023. *Análisis de vulnerabilidades de redes inalámbricas Domésticas utilizando pentesting en tungurahua*. [en línea]. Tesis grado. Ecuador: Universidad Técnica de Ambato [consulta: setiembre 2023]. Disponible en: https://repositorio.uta.edu.ec/bitstream/123456789/38304/1/t2197ti.pdf

**DE LA CRUZ, Gerson, MÉNDEZ, Ronny y MÉNDEZ, Alberto.** Seguridad de la Información en el Comercio Electrónico Basado en ISO 27001: Una Revisión Sistemática. Perú : Revista Innovación y Software, 2023. Vol. 4,1.
ISSN: 2708-0935

**FERNÁNDEZ, Javier, HIERRO, Gonzalo y AREQUE, Yaiza.** Ciberseguridad y Arbitraje Internacional: El Protocolo de Ciberseguridad en Arbitraje Internacional del ICCA, el NYC Bar y el CPR. Perú: Themis, 2020. N° 77.
ISSN: 1810-9934

**FLORES, Carlos y FLORES, Karla.** Pruebas para Comprobar la Normalidad de Datos en Procesos Productivos: Anderson-Darling, Ryan-Joiner, Shapiro-Wilk y Kolmogórov-Smirnov. Ecuador: Societas. Revista de Ciencias Sociales y humanísticas, 2021. Vol. 23,2. p.87.
ISSN: 1560-0408

**FONSECA, Omar, ROJAS, Alix y FLOREZ, Hector.** A Model of an Information Security Manegement System Based on NTC-ISO/IEC 27001 Standard, International Journal of Computer Science, 2022. Vol. 48,2. p.2

**GARCÍA, Viviana.** ¿Cómo Está Avanzando La Ciberseguridad en El Perú? Breve Aproximación Al Marco Normativo. Perú : Actualidad Juridica, 2019. 52.
ISSN: 1578-956X.

**HERNANDEZ, Arturo, RAMOS, Marcos, PLACENCIA, Barbara, INDACOCHEA, Blanca, QUIMIS, Alex y MORENO, Luis.** Metodología de la Investigación Científica. Editorial Científica 3Ciencias, 2018.
ISSN: 978-84-948257-0-5.

**HERNANDEZ, Roberto, FERNANDEZ, Carlos y BAPTISTA, Pilar.** Metodología de la Investigación. McGRAW-HILL / INTERAMERICANA EDITORES, S.A, 2014.
ISSN: 978-1-4562-2396-0

**ÍSCAR, Javier y BARRIGA, Ana.** Ciberseguridad. Desde la perspectiva del Arbitraje Internacional. Perú : Revista de Derecho YACHAQ, 2022. Vol. 13. p.87.
ISSN: 2707-1197.

**JARA, Natalia y JORQUERA, Antonia.** Liability of the state administration for cybersecurity breaches. Chile : Revista Chilena de Derecho y Tecnología, 2021. Vol. 10,1. p.206.

**KITSIOS, Fotis, CHATZIDIMITRIOU, Elpiniki y KAMARIOTOU, María.** The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Suiza : s.n., 2023. Vol. 15, 7.

**LOPES, Isabel, GUARDA, Teresa y OLIVEIRA, Pedro.** Implementation of ISO 27001 standards as GDPR compliance facilitator. Portugal : Journal of Information Systems Engineering and Management, 2019. Vol. 4, 2. p.3.
ISSN: 2468-4376.

**MORALES, Flavio, TOAPANTA, Sergio y TOASA, Renato.** Implementación De Un Sistema De Seguridad Perimetral Como Estrategia De Seguridad De La Información. Ecuador : Revista Ibérica De Sistemas e Tecnologias De Informação, 2020. Vol. 3. 16469895.

**NÚÑEZ MORÁN, Esteban George**, 2021. Metodología para la detección y reducción de Ransomware [en línea]. Tesis grado. Piura: Universidad Nacional de Piura [consulta: setiembre de 2023]. Disponible en: http://repositorio.unp.edu.pe/handle/20.500.12676/3291

**NÚÑEZ, Fernando y CARHUANCHO, Brendalis** Ciberdelincuencia en tiempos de Covid-19: ¿La vulneración a derechos constitucionales? Perú : Lumen, 2020. Vol. 16, 1. p.94.

**OCHOA DÍAZ, Ricardo Andrés; TICSE LÓPEZ Diego Alonso,** 2022. *Modelo de cuantificación financiera para escenarios de ransomware para el sector financiero* [en línea]. Tesis grado. Lima: Universidad Peruana de Ciencias Aplicadas (UPC) [consulta: setiembre 2023]. Disponible en: http://hdl.handle.net/10757/668246

**ORMACHEA, Juan.** Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional. Perú: Revista De Ciencia e Investigación en Defensa - CAEN, 2020. Vol. 1, 4. ISSN: 2709-1422.

**ORTIZ, Keyly, GUEVARA, Jair y MENDOZA, Alberto.** Seguridad en el uso de aplicaciones de mensajería instantánea de comunicación interna. Perú : Sciéndo, 2022. Vol. 25, 2.

**PEREZ DIAZ, Neiler Wilter, CHINCHAY MALDONADO, Jorge Obed,** 2021. *Implementación de tecnología sandbox para proteger de ataques ransomware en una red informática local de una entidad financiera* [en línea]. Tesis grado. Chiclayo: Universidad Señor de Sipán [consulta: setiembre 2023]. Disponible en: https://repositorio.uss.edu.pe//handle/20.500.12802/9896

**PHIRKE, Amogh y AJIT, Jayshree.** Best practices of auditing in an organization using ISO 27001 standard. India : International Journal of Recent Technology Engineering, 2019. Vol. 8, 2. p.692. ISSN: 2277-3878.

**POMA, Alexis y VARGAS, Raquel.** Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. Perú : s.n., 2019. Vol. 22, 4. p.275.

**QUINTERO, Jesús, JOVEN, Jesús y BRAVO, Martín.** Design and Assembly of a Topological Network Diagram that Provides Security, Confidentiality, Integrity and Availability in the Data Network of the Company Controles Empresariales S.A.S. Neiva. Colombia: Journal of Engineering and Applied Sciences, 2021. Vol. 16,23. p.2594.
ISSN: 1819-6608

**QUIROGA, José.** Ciberseguridad y Protección de Datos Personales en el Perú. Perú: Advocatus, 2021. N°. 39. p.16-17.
ISSN: 1996-4773

**RAMOS, Roy, CAHUAYA, Rogelio y LLANQUI, Roberto.** Política Informática y la Gestión de la Seguridad de la Información en Base a la Norma ISO 27001. Perú : Revista Innovación y Software, 2023. Vol. 4,1. p.65.
ISSN: 2708-0935

**RAZAQUE, Abdul, AMSAAD, Fathi, JARO, Meer, HARIRI, Salim, CHEN, Shujing y JI, Xingchen.** Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. China : IEEE Access, 2019. Vol. 7. p.168774.

**RAZIKIN, Khairur y SOEWITO, Benfano.** Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. Indonesia : Egyptian Informatics Journal, 2022. Vol. 23, 3.
ISSN 1110-8665.

**RIOS, Roger.** Metodología para la Investigación y Redacción. España : eumed.net de la Universidad de Málaga, 2017. Vol. 1. p.102.
ISSN: 978-84-17211-23-3

**RISKY, Junior, GUNTUR, Utomo y OKTARIA, Dita.** Information Security Analysis in PT. XYZ Using ISO/IEC 27001:2013. Indonesia : Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi, 2023. Vol. 12, 1.
ISSN: 2089-3787.

**RINCON, Luis.** Test de Penetración para el Estudio de Vulnerabilidades a los Ciberataques mediante Técnicas de Hacking Ético en Redes IPV4. Venezuela : Revista Electrónica de Estudios Telemáticos, 2021. Vol. 20, 2. p.80.
ISSN 1856-4194.

**RODRIGUEZ, Ciro, BREÑA, Jorge y ESENARRO, Doris.** Las variables en la metodología de la investigación científica. Editorial Científica 3Ciencias, 2021.
ISSN 978-84-123872-2-3.

**SALAZAR, Cecilia y DEL CASTILLO, Santiago.** FUNDAMENTOS BÁSICOS DE ESTADÍSTICA. 2018. Vol. 1
ISSN 978-9942-30-616-6

**SÁNCHEZ, Hugo, REYES, Carlos y MEJÍA, Katia.** MANUAL DE TÉRMINOS EN INVESTIGACIÓN CIENTÍFICA, TECNOLÓGICA Y HUMANÍSTICA. Perú : Revista Universidad Ricardo Palma, 2018. Vol. 1. p.79
ISSN 978-612-47351-4-1.

**SERNA, Santiago, MONTOYA, Alvaro, QUINTERO, Yeiler, Henao, Cesar y Castro, Frey.** Desarrollo de un sistema de seguridad informática a partir de una auditoría sobre una red empresarial. Perú : Rev. INGENIERÍA: Ciencia, Tecnología e Innovación, 2022. Vol. 9. p.135.
ISSN: 2313-1926.

**ŠIKMAN, Lilja, LATINOVIĆ, Tihomir y PASPALJ, Darko.** Information Systems Security, Development, Trends, Technical and Economic Challenges. Annals of the Faculty of Engineering Hunedoara. Rumanía : International Journal of Engineering, 2019. Vol. 17, 4. p.45.

**SUN, Nan, LI, Chang-Tsun, CHAN, Hin, ZAHIDUL, M, RAFIQUL, M y ARMSTRONG, Warren.** How Do Organizations Seek Cyber Assurance? Investigations on the Adoption of the Common Criteria and Beyond. Australia : IEEE, 2022. Vol. 10. p.71749.

**SYREYSHCHIKOVA, Nelli, PIMENOV, Danil, MIKOLAJCZYK, Tadeusz y MOLDOVAN, Liviu.** Information Safety Process Development According to ISO 27001 for an Industrial Enterprise. Procedia Manufacturing. 2019. Vol. 32. p.285.
ISSN: 2351-9789

**TASA, María, MAQUERA, Henry, ROJAS, John y DELGADO, Marjorie.** Análisis de información de la gestión de incidentes de seguridad en organizaciones. Perú : Puriq, 2022. Vol. 4.
ISSN 2664-4029.

**TOGU, Sianturi y KALAMULLAH, Ramli.** A Security Framework for Secure Host to Host Environments. Indonesia : Rekayasa Sistem Dan Teknologi Informasi, 2022. Vol. 6, 3. p.380.
ISSN 2580-0760.

**TONYSÉ, Martín.** Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. Ecuador : s.n., 2021. Vol. 13, 5. p.495.
ISSN: 2218-3620.

**VIGURI, Jorge.** Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos. España : Revista de Internet, Derecho y Política, 2021. Vol. 33.
ISSN: 1699-8154.

**ZEVALLOS, Mauro.** Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. Perú: Revista Peruana de Computación y Sistemas, 2019. Vol. 2,2. ISSN 2627-2003.

# ANEXOS

**Anexo 1:** *Matriz de Consistencia*

<table>
<tr><th>PROBLEMA</th><th>HIPÓTESIS</th><th>OBJETIVOS</th><th colspan="4">VARIABLE</th><th>METODOLOGÍA</th></tr>
<tr><td>GENERAL</td><td>GENERAL</td><td>GENERAL</td><td colspan="4">INDEPENDIENTE:</td><td rowspan="3">TIPO DE INVESTIGACIÓN:<br>• Aplicada<br><br>DISEÑO:<br>• Experimental – Preexperimental<br><br>• POBLACIÓN: 30 activos de información en la empresa System Arq.<br><br>• MUESTRA: 30 activos de información en la empresa System Arq.<br><br>ENFOQUE:<br>• Cuantitativo<br><br>TÉCNICA:<br>• Observación.<br><br>INSTRUMENTO:</td></tr>
<tr><td>¿De qué manera la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el riesgo ante ataques cibernéticos en la empresa System Arq, Lima-2023?</td><td>Implementar un sistema de seguridad de la información basada en la norma ISO 27001 reduce el riesgo ante ataques cibernéticos en la empresa System Arq, Lima-2023.</td><td>Demostrar que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el riesgo ante ataques cibernéticos en la empresa System Arq, Lima-2023.</td><td colspan="4">Sistema de Gestión de Seguridad basada en la Norma ISO 27001</td></tr>
<tr><td>ESPECÍFICOS</td><td>ESPECÍFICOS</td><td>ESPECÍFICOS</td><td>DEPENDIENTE</td><td>DIMENSIÓN</td><td>INDICADOR</td><td>FÓRMULA</td></tr>
<tr><td>PE1: ¿De qué manera la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 determina el porcentaje de ataques malware como parte de los ataques cibernéticos en la</td><td>HE1: La implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de ataques malware como parte de los ataques cibernéticos en la empresa System Arq, Lima 2023.</td><td>OE1: Demostrar que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 influye en el porcentaje de ataques malware como parte de los ataques cibernéticos en la empresa System Arq, Lima 2023.</td><td>Ataques cibernéticos</td><td>Ataques Malware</td><td>Porcentaje de ataques malware</td><td></td></tr>
</table>

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| empresa System Arq, Lima 2023? | | | | | | | • Guía de observación<br>• Fichas de registro |
| PE2: ¿De qué manera la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 determina el porcentaje de vulnerabilidades en los activos de información ante ataques cibernéticos en la empresa System Arq, Lima 2023? | HE2: La implementación de un sistema de seguridad de la información basada en la norma ISO 27001 reduce el porcentaje de vulnerabilidades en los activos de información ante ataques cibernéticos en la empresa System Arq, Lima 2023. | OE2: Demostrar que la implementación de un sistema de seguridad de la información basada en la norma ISO 27001 influye en el porcentaje de vulnerabilidades en los activos de información ante ataques cibernéticos en la empresa System Arq, Lima 2023. | | vulnerabilidades en los activos de información | Porcentaje de vulnerabilidades en los activos de información | | |

Fuente: elaboración propia.

**Anexo 2:** *Matriz de Operacionalización de la Variables*

| Variable | Definición Conceptual | Definición Operacional | Dimensión | Indicador |
|---|---|---|---|---|
| V.I: Sistema de Gestión de Seguridad basada en la ISO 27001 | Norma internacional referente al Sistema de Gestión de Seguridad, la cual permite monitorear, controlar, analizar, resguardar, proteger toda información que alojado en la empresa. (Fonseca, Rojas y Florez, 2021, p.2). | El efecto de implementar la ISO 27001 ayuda a identifica amenazas y mitigarlos rápidamente, además corrige vulnerabilidades expuestas a ataques cibernéticos, contribuye con la seguridad y privacidad del negocio, mejora los procesos relacionados a la protección de los datos (Fonseca, Rojas y Florez, 2021, p.1). | | |
| V.D: Ataques Cibernéticos | Los ataques cibernéticos son acciones delictivas llevadas a cabo por individuos o grupos con conocimientos técnicos especializados, que buscan obtener información valiosa de la empresa. Estos ataques pueden ser ejecutados de varias formas, como infectar los equipos informáticos con virus, hackear servidores a través de la red o robar las credenciales de acceso al sistema, entre otras. El objetivo principal es apoderarse de la información y luego extorsionar o exigir dinero para recuperarla (Poma y Vargas, 2019, p.275). | El efecto de los ataques cibernéticos es de infiltración, daño, manipulación, robo o comprometer sistemas informáticos, redes, dispositivos electrónicos u otros recursos digitales. Estos pueden incluir actividades como el acceso no autorizado, robo de información, interrupción de servicios, propagación de malware, secuestro de cuentas, la suplantación de identidad, entre otros métodos, con el fin de obtener beneficios económicos, políticos, sociales o causar perjuicio a individuos, organizaciones o incluso a nivel global (Poma y Vargas, 2019, p.275). | **Ataques Malware**, programa malicioso con la capacidad cifrar archivos (Cando y Medina, 2021, p.28). | Porcentaje de ataques malware (Cando y Medina, 2021, p.32). |
| | | | **Vulnerabilidades en los activos de información** (Cando y Medina, 2021, p.29). | Porcentaje de vulnerabilidades en los activos de información (Rincon, 2021). |

Fuente: elaboración propia.

**Anexo 3:** *Indicadores del proceso académico*

| INDICADOR | DESCRIPCIÓN | OBJETIVO | TÉCNICA | INSTRUMENTO | FÓRMULA |
|---|---|---|---|---|---|
| Porcentaje de ataques malware | Es la cantidad de acciones maliciosas que comprometen la seguridad de los sistemas informáticos. | Reducir el nivel ocasionado por los ataques malware con la implementación de un Sistema de Gestión de Seguridad basada en la ISO 27001 | Observación | Guía de observación | PAM = ((CME-CMS) /CME) *100<br>Donde:<br>PAM= Porcentaje ataques malware<br>CME = Cantidad de malware encontrados<br>CMS= Cantidad de malware suprimidos |
| Porcentaje de vulnerabilidades en los activos de información | Identificar las vulnerabilidades en la empresa System Arq. | Elevar el nivel de seguridad ante las vulnerabilidades identificadas con la implementación de un Sistema de Gestión de Seguridad basada en la ISO 27001 | Observación | Guía de observación | PVAI = ((CVI-CVC) /CVI) *100<br>Donde:<br>PVAI= Porcentaje de vulnerabilidades en los activos de información<br>CVI= Cantidad vulnerabilidades identificadas<br>CVC= Cantidad de vulnerabilidades corregidas |

Fuente: elaboración propia

**Anexo 4:** *Análisis de Riesgo en los Activos de Información*

# Análisis de Riesgos en los Activos de Información

## [A0001] Análisis de riesgo

13.10.2023

### 1. Introducción

Documento para anexar a la documentación de seguridad del sistema que se presenta para conseguir la aprobación o autorización de la autoridad responsable del sistema de información.

### Datos del sistema sujeto a análisis:

Código: A0002
Nombre: Análisis de riesgos
Datos administrativos:

- Organización: System Arq
- Descripción: Ingeniería y arquitectura
- Autor: Ángel Jony Huamaní Rubio
  Johnny Pablo Liza Velásquez
- Versión: 1
- Fecha: 24/09/2023
- responsable del sistema: Johnny Pablo Liza Velásquez
- Responsable de la Seguridad de la Información: Ángel Jony Huamaní Rubio

### Dimensiones de valoración

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos
- [DP] Datos personales

### 2. Dominios de seguridad

Dominios de seguridad

- [base] Red corporativa
- [bps] Conexión a internet

### Agravantes y atenuantes

## Valoración de los activos capa: [E] Equipamiento

| activo | [D] | [I] | [C] | [A] | [T] | [DP] |
|---|---|---|---|---|---|---|
| [ES0001] Datos del negocio | [3](1) | [1](2) | [5](3) | [1](4) | [5](5) | [4](6) |
| [ES0002] Servicio | [5](7) | [5](7) | [7](8) | [5](9) | [5](10) | [5](3) |
| [ES0003] Procesos del negocio | [4](11) | [5](9) | [3](12) | [3](1) | [5](13) | [3](14) |
| [SW0001] BD Mysql | [3](15) | [6](16) | [7](17) | [3](1) | [7](18) | [4](19) |
| [SW0002] Aplicaciones propias | [5](20) | [3](21) | [4](22) | [3](23) | [4](24) | [3](14) |
| [SW0003] Aplicaciones a terceros | [7](25) | [3](12) | [5](13) | [5](9) | [7](26) | [4](22) |
| [SW0004] Antivirus | [9](27) | [3](15) | [9](27) | [9](27) | [9](27) | [6](28) |
| [SW0005] Servidor www | [5](10) | [7](17) | [7](17) | [3](23) | [5](10) | [5](29) |
| [SW0006] Ofimática | [7](26) | [4](22) | [5](30) | [3](23) | [7](17) | [3](14) |
| [SW0007] SO Windows | [5](10) | [7](17) | [7](17) | [3](23) | [7](17) | [5](29) |
| [HW0001] Servidor | [7](31) | [5](32) | [7](17) | [6](33) | [7](34) | [6](28) |
| [HW0002] Laptop, pc | [5](20) | [5](32) | [7](17) | [5](3) | [7](17) | [5](30) |
| [HW0003] Celulares | [4](6) | [3](1) | [3](15) | [5](3) | [3](15) | [5](30) |
| [HW0004] Equipo respaldo | [4](24) | [5](7) | [5](13) | [5](13) | [5](13) | [5](29) |
| [HW0005] Impresora | [3](1) | [3](35) | [3](15) | [5](9) | [3](1) | [3](14) |
| [HW0006] Módem | [3](1) | [3](15) | [3](15) | [5](13) | [5](10) | [6](28) |
| [HW0007] access point | [5](32) | [6](33) | [3](36) | [7](17) | [7](18) | [4](6) |
| [COM0001] Red de Datos | [7](34) | [5](32) | [3](1) | [5](13) | [7](34) | [4](6) |
| [COM0002] Red Inalámbrica | [7](34) | [5](32) | [5](32) | [5](7) | [5](10) | [3](14) |
| [COM0003] Wifi | [5](10) | [5](10) | [5](13) | [5](7) | [5](10) | [3](14) |
| [COM0004] Red local | [5](10) | [5](10) | [5](13) | [5](10) | [7](34) | [5](30) |
| [COM0005] WAM | [5](10) | [5](7) | [5](7) | [7](34) | [7](34) | [5](30) |
| [COM0006] VPN | [5](3) | [5](10) | [5](7) | [7](17) | [7](17) | [5](30) |
| [AUX0001] Fuente de poder | [5](7) | [3](15) | [5](13) | [5](10) | [5](10) | [6](37) |
| [AUX0002] Ups | [4](24) | [3](15) | [5](13) | [3](35) | [5](10) | [6](37) |
| [AUX0003] Generador eléctrico | [5](7) | [7](17) | [5](13) | [5](10) | [5](32) | [6](37) |
| [AUX0004] Aire acondicionado | [5](7) | [3](15) | [5](13) | [3](1) | [3](36) | [4](6) |
| [AUX0005] Fibra óptica | [5](7) | [3](15) | [5](7) | [7](26) | [7](34) | [6](37) |
| [Media0001] CD-ROM | [7](38) | [7](17) | [7](17) | [7](17) | [7](17) | [4](6) |
| [Media0002] Memoria USB | [7](17) | [7](17) | [7](17) | [7](17) | [7](17) | [4](6) |

(1) [3] probablemente impediría la operación efectiva de una parte de la Organización
(2) [1] pudiera causar el incumplimiento leve o técnico de una ley o regulación
(3) [5] Difusión Limitada
(4) [1] Pudiera causar una pérdida menor de la confianza dentro de la Organización
(5) Obligaciones legales:
[5] probablemente sea causa de incumplimiento de una ley o regulación
(6) [4] probablemente afecte a un grupo de individuos
(7) [5] Probablemente cause un cierto impacto en otras organizaciones
(8) [7] podría lesionar gravemente a varios individuos
(9) [5] probablemente sea causa de incumplimiento de una ley o regulación
(10) [5] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones

(11) [4] Puede causar malestar público
(12) [3] Probablemente afecte negativamente a las relaciones internas de la Organización
(13) [5] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
(14) [3] probablemente afecte a un individuo
(15) [3] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
(16) [6] podría lesionar gravemente a un individuo
(17) [7] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
(18) [7] Probablemente tenga un gran impacto en otras organizaciones
(19) [4] probablemente quebrante leyes o regulaciones
(20) [5] Nivel 5
(21) [3] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
[3] Probablemente afecte negativamente a las relaciones internas de la Organización
(22) [4] Difusión Limitada
(23) [3] probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
(24) [4] 4 horas < RTO < 1 día
(25) [7] Nivel 7
(26) [7] probablemente impediría la operación efectiva de la Organización
(27) [9] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
(28) [6] probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
(29) [5] probablemente quebrante seriamente leyes o regulaciones
(30) [5] probablemente afecte gravemente a un individuo
(31) [7] RTO < 4 horas
(32) [5] probablemente impediría la operación efectiva de más de una parte de la Organización
(33) [6] Difusión Limitada
(34) [7] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
(35) [3] Probablemente cause la interrupción de actividades propias de la Organización
(36) [3] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
(37) [6] probablemente afecte gravemente a un grupo de individuos
(38) [7] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[3] probablemente impediría la operación efectiva de una parte de la Organización

### Valoración de los dominios

| dominio de seguridad | [D] | [I] | [C] | [A] | [T] | [DP] |
|---|---|---|---|---|---|---|
| [base] Red corporativa | [9] | [7] | [9] | [9] | [9] | [6] |
| [bps] Conexión a internet | [7] | [7] | [7] | [7] | [7] | [6] |

## 3. Riesgo acumulado

Se presentan los principales riesgos en cada dominio de seguridad del sistema en las diferentes fases de trabajo.

**amenaza**
: presenta la amenaza dentro del catálogo de PILAR. Una amenaza aparece cuando algún activo del sistema está expuesto a ella

**D – dimensión**
: se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

**I – impacto**
: se muestra el máximo impacto causado por esta amenaza en algún activo del sistema

**R – riesgo**
: se muestra el máximo riesgo al que está expuesto el sistema por causa de esta amenaza

[potencial]
[base] Red corporativa

| amenaza | D | I | R |
|---|---|---|---|
| [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [A.24] Denegación de servicio | D | [9] | {6,5} |
| [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [A.26] Ataque destructivo | D | [9] | {6,2} |
| [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |

[bps] Conexión a internet

| amenaza | D | I | R |
|---|---|---|---|
| [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [A.24] Denegación de servicio | D | [7] | {5,4} |
| [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [A.22] Manipulación de programas | I, C | [7] | {5,1} |
| [A.11] Acceso no autorizado | A | [7] | {5,1} |
| [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |

| | | | |
|---|---|---|---|
| [A.8] Difusión de software dañino | D, I, C | [7] | {5,1} |

Fase: [current] situación actual
[base] Red corporativa

| amenaza | D | I | R |
|---|---|---|---|
| [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [A.24] Denegación de servicio | D | [9] | {6,5} |
| [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [A.26] Ataque destructivo | D | [9] | {6,2} |
| [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |

[bps] Conexión a internet

| amenaza | D | I | R |
|---|---|---|---|
| [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [A.24] Denegación de servicio | D | [7] | {5,4} |
| [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [A.22] Manipulación de programas | I, C | [7] | {5,1} |
| [A.11] Acceso no autorizado | A | [7] | {5,1} |
| [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [A.8] Difusión de software dañino | D, I, C | [7] | {5,1} |

Fase: [target] situación objetivo
[base] Red corporativa

| amenaza | D | I | R |
|---|---|---|---|
| [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [A.24] Denegación de servicio | D | [9] | {6,5} |
| [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [A.26] Ataque destructivo | D | [9] | {6,2} |
| [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |

[bps] Conexión a internet

| amenaza | D | I | R |
|---|---|---|---|

| | | | |
|---|---|---|---|
| [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [A.24] Denegación de servicio | D | [7] | {5,4} |
| [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [A.22] Manipulación de programas | I, C | [7] | {5,1} |
| [A.11] Acceso no autorizado | A | [7] | {5,1} |
| [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [A.8] Difusión de software dañino | D, I, C | [7] | {5,1} |

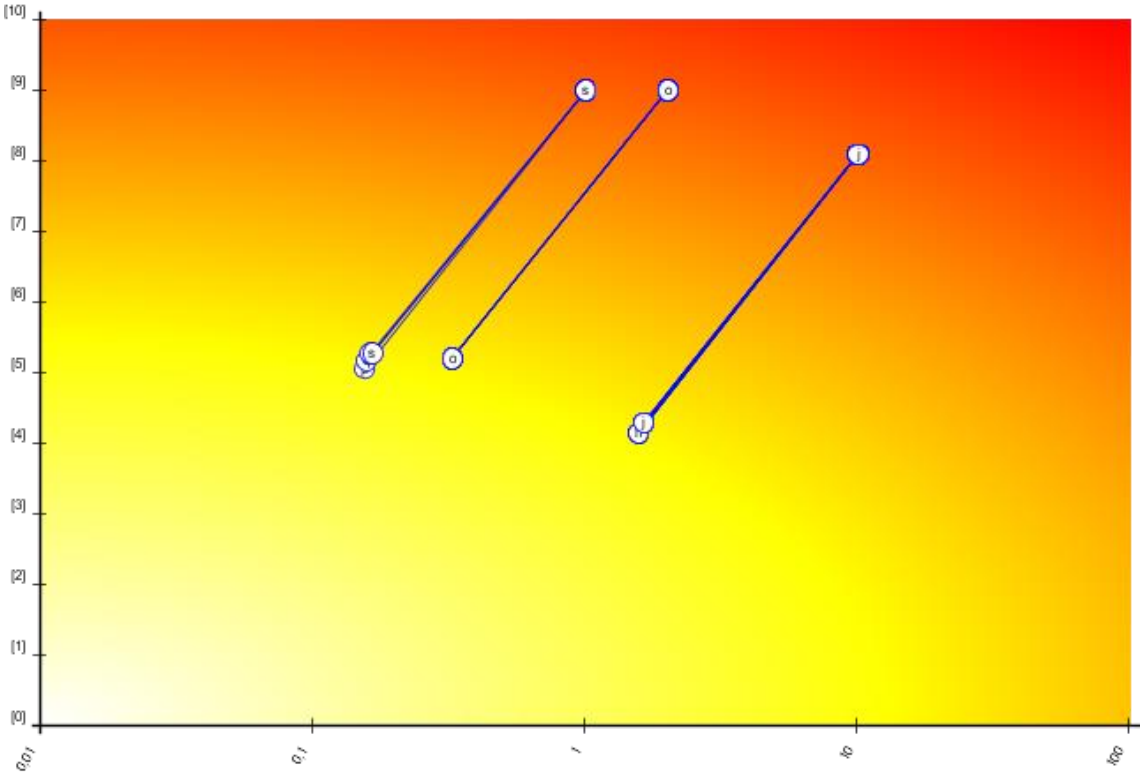
Fase: [PILAR] recomendación
[base] Red corporativa

| amenaza | D | I | R |
|---|---|---|---|
| [E.24] Caída del sistema por agotamiento de recursos | D | [4] | {3,7} |
| [A.24] Denegación de servicio | D | [5] | {3,6} |
| [E.21] Errores de mantenimiento / actualización de programas (software) | C | [4] | {3,6} |
| [A.26] Ataque destructivo | D | [5] | {3,4} |
| [I.6] Corte del suministro eléctrico | D | [5] | {3,4} |
| [A.25] Robo de equipos | C | [5] | {3,4} |
| [I.10] Degradación de los soportes de almacenamiento de la información | D | [5] | {3,4} |

[bps] Conexión a internet

| amenaza | D | I | R |
|---|---|---|---|
| [A.24] Denegación de servicio | D | [3] | {2,6} |
| [E.24] Caída del sistema por agotamiento de recursos | D | [2] | {2,6} |
| [E.21] Errores de mantenimiento / actualización de programas (software) | C | [2] | {2,5} |
| [I.6] Corte del suministro eléctrico | D | [3] | {2,3} |
| [A.26] Ataque destructivo | D | [3] | {2,3} |
| [A.5] Suplantación de la identidad | A | [3] | {2,3} |
| [A.22] Manipulación de programas | C | [3] | {2,2} |
| [A.11] Acceso no autorizado | A | [3] | {2,2} |

### Evolución del riesgo




- a. C: SW0004 * E.21
- b. D: HW0003 * E.24
- c. D: HW0001 * E.24
- d. C: SW0003 * E.21
- e. C: SW0006 * E.21
- f. D: HW0005 * E.24
- g. C: SW0002 * E.21
- h. C: SW0007 * E.21
- i. D: HW0002 * E.24
- j. D: HW0004 * E.24
- k. D: HW0004 * A.24
- l. D: HW0005 * A.24
- m. D: HW0003 * A.24
- n. D: HW0002 * A.24
- o. D: HW0001 * A.24
- p. D, C: SW0002 * A.8
- q. D: HW0004 * I.7
- r. D: HW0002 * A.26
- s. D: Media0001 * I.6

## 4. Riesgo repercutido

Se presentan los máximos riesgos a los que están expuestos los activos esenciales del sistema en cada fase de trabajo.

**activo**

presenta el activo esencial que está en riesgo; es decir, sobre el que repercute indirectamente la amenaza

**amenaza**
presenta la amenaza dentro del catálogo de PILAR.

**D – dimensión**
se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

**I – impacto**
se muestra el máximo impacto causado por esta amenaza sobre el activo esencial

**R – riesgo**
se muestra el máximo riesgo al que está expuesto el activo esencial por causa de esta amenaza

[potencial]
[base] Red corporativa

| activo | amenaza | D | I | R |
|---|---|---|---|---|
| [SW0002] Aplicaciones propias | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0003] Aplicaciones a terceros | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0004] Antivirus | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [SW0004] Antivirus | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0006] Ofimática | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0007] SO Windows | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [HW0001] Servidor | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [HW0002] Laptop, pc | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [HW0003] Celulares | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [HW0004] Equipo respaldo | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [HW0005] Impresora | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [SW0004] Antivirus | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0001] Servidor | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0002] Laptop, pc | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0003] Celulares | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0004] Equipo respaldo | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0005] Impresora | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [SW0002] Aplicaciones propias | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0002] Aplicaciones propias | [A.22] Manipulación de programas | D, C | [9] | {6,2} |

| | | | | |
|---|---|---|---|---|
| [SW0003] Aplicaciones a terceros | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0003] Aplicaciones a terceros | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [SW0004] Antivirus | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [SW0004] Antivirus | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [SW0004] Antivirus | [I.10] Degradación de los soportes de almacenamiento de la información | D | [9] | {6,2} |
| [SW0004] Antivirus | [A.18] Destrucción de la información | D | [9] | {6,2} |
| [SW0004] Antivirus | [E.25] Pérdida de equipos | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [E.18] Destrucción de la información | D | [9] | {6,2} |
| [SW0004] Antivirus | [A.25] Robo de equipos | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [SW0006] Ofimática | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0006] Ofimática | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [SW0007] SO Windows | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0007] SO Windows | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [HW0001] Servidor | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0001] Servidor | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0001] Servidor | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0002] Laptop, pc | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0002] Laptop, pc | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0002] Laptop, pc | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0003] Celulares | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0003] Celulares | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0003] Celulares | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0004] Equipo respaldo | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0004] Equipo respaldo | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0004] Equipo respaldo | [E.25] Pérdida de equipos | D, C | [9] | {6,2} |

| | | | | |
|---|---|---|---|---|
| [HW0004] Equipo respaldo | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0005] Impresora | [E.25] Pérdida de equipos | D, C | [9] | {6,2} |
| [HW0005] Impresora | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0005] Impresora | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0005] Impresora | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [AUX0001] Fuente de poder | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [Media0001] CD-ROM | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [Media0001] CD-ROM | [I.10] Degradación de los soportes de almacenamiento de la información | D | [9] | {6,2} |
| [Media0001] CD-ROM | [A.18] Destrucción de la información | D | [9] | {6,2} |
| [Media0001] CD-ROM | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [Media0001] CD-ROM | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D, C | [9] | {6,2} |
| [Media0001] CD-ROM | [E.18] Destrucción de la información | D | [9] | {6,2} |
| [Media0001] CD-ROM | [A.25] Robo de equipos | C | [9] | {6,2} |
| [Media0002] Memoria USB | [A.18] Destrucción de la información | D | [9] | {6,2} |
| [Media0002] Memoria USB | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [Media0002] Memoria USB | [I.10] Degradación de los soportes de almacenamiento de la información | D | [9] | {6,2} |
| [Media0002] Memoria USB | [E.18] Destrucción de la información | D | [9] | {6,2} |
| [Media0002] Memoria USB | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D, C | [9] | {6,2} |
| [Media0002] Memoria USB | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [Media0002] Memoria USB | [A.25] Robo de equipos | C | [9] | {6,2} |
| [SW0004] Antivirus | [I.*] Desastres industriales | D | [9] | {6,0} |
| [SW0004] Antivirus | [I.1] Fuego | D | [9] | {6,0} |
| [HW0001] Servidor | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0001] Servidor | [I.1] Fuego | D | [9] | {6,0} |
| [HW0002] Laptop, pc | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0002] Laptop, pc | [I.1] Fuego | D | [9] | {6,0} |
| [HW0003] Celulares | [I.1] Fuego | D | [9] | {6,0} |
| [HW0003] Celulares | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0004] Equipo respaldo | [A.25] Robo de equipos | D, C | [9] | {6,0} |

| | | | | |
|---|---|---|---|---|
| [HW0004] Equipo respaldo | [I.1] Fuego | D | [9] | {6,0} |
| [HW0004] Equipo respaldo | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0005] Impresora | [A.25] Robo de equipos | D, C | [9] | {6,0} |
| [HW0005] Impresora | [I.1] Fuego | D | [9] | {6,0} |
| [HW0005] Impresora | [I.*] Desastres industriales | D | [9] | {6,0} |
| [AUX0001] Fuente de poder | [I.*] Desastres industriales | D | [9] | {6,0} |
| [AUX0001] Fuente de poder | [I.1] Fuego | D | [9] | {6,0} |
| [AUX0001] Fuente de poder | [A.25] Robo de equipos | D | [9] | {6,0} |
| [Media0001] CD-ROM | [I.1] Fuego | D | [9] | {6,0} |
| [Media0001] CD-ROM | [I.*] Desastres industriales | D | [9] | {6,0} |
| [Media0002] Memoria USB | [I.1] Fuego | D | [9] | {6,0} |
| [Media0002] Memoria USB | [I.*] Desastres industriales | D | [9] | {6,0} |
| [ES0001] Datos del negocio | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [ES0003] Procesos del negocio | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0002] Aplicaciones propias | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0002] Aplicaciones propias | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0003] Aplicaciones a terceros | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0003] Aplicaciones a terceros | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0004] Antivirus | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0004] Antivirus | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [SW0004] Antivirus | [I.3] Contaminación medioambiental | D | [8] | {5,7} |
| [SW0004] Antivirus | [A.7] Uso no previsto | D | [8] | {5,7} |
| [SW0004] Antivirus | [A.23] Manipulación del hardware | D, C | [8] | {5,7} |
| [SW0004] Antivirus | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [SW0004] Antivirus | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0006] Ofimática | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0006] Ofimática | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0007] SO Windows | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |

| | | | | |
|---|---|---|---|---|
| [SW0007] SO Windows | [A.15] Modificación de la información | I | [7] | {5,7} |
| [SW0007] SO Windows | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0001] Servidor | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0001] Servidor | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0001] Servidor | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0002] Laptop, pc | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0002] Laptop, pc | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0002] Laptop, pc | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0003] Celulares | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0003] Celulares | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0003] Celulares | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0004] Equipo respaldo | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0004] Equipo respaldo | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0004] Equipo respaldo | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0005] Impresora | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0005] Impresora | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0005] Impresora | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0001] Fuente de poder | [A.7] Uso no previsto | D | [8] | {5,7} |
| [AUX0001] Fuente de poder | [A.23] Manipulación del hardware | D | [8] | {5,7} |
| [AUX0001] Fuente de poder | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0002] Ups | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0003] Generador eléctrico | [A.15] Modificación de la información | I | [7] | {5,7} |
| [AUX0003] Generador eléctrico | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0004] Aire acondicionado | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [Media0001] CD-ROM | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [Media0001] CD-ROM | [I.3] Contaminación medioambiental | D | [8] | {5,7} |
| [Media0001] CD-ROM | [A.15] Modificación de la información | I | [7] | {5,7} |
| [Media0001] CD-ROM | [E.25] Pérdida de equipos | C | [8] | {5,7} |

| | | | | |
|---|---|---|---|---|
| [Media0001] CD-ROM | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [Media0001] CD-ROM | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [Media0002] Memoria USB | [I.3] Contaminación medioambiental | D | [8] | {5,7} |
| [Media0002] Memoria USB | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [Media0002] Memoria USB | [A.15] Modificación de la información | I | [7] | {5,7} |
| [Media0002] Memoria USB | [E.25] Pérdida de equipos | C | [8] | {5,7} |
| [Media0002] Memoria USB | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [Media0002] Memoria USB | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0003] Celulares | [A.25] Robo de equipos | C | [6] | {5,6} |
| [HW0003] Celulares | [E.25] Pérdida de equipos | C | [6] | {5,6} |
| [SW0003] Aplicaciones a terceros | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [SW0004] Antivirus | [N.*] Desastres naturales | D | [9] | {5,4} |
| [SW0004] Antivirus | [N.1] Fuego | D | [9] | {5,4} |
| [SW0004] Antivirus | [I.2] Daños por agua | D | [8] | {5,4} |
| [SW0006] Ofimática | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [HW0001] Servidor | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0001] Servidor | [A.25] Robo de equipos | D, C | [9] | {5,4} |
| [HW0001] Servidor | [E.25] Pérdida de equipos | D, C | [9] | {5,4} |
| [HW0001] Servidor | [N.1] Fuego | D | [9] | {5,4} |
| [HW0001] Servidor | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0001] Servidor | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0001] Servidor | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [HW0002] Laptop, pc | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0002] Laptop, pc | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0002] Laptop, pc | [N.1] Fuego | D | [9] | {5,4} |
| [HW0002] Laptop, pc | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0002] Laptop, pc | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [HW0003] Celulares | [N.1] Fuego | D | [9] | {5,4} |
| [HW0003] Celulares | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0003] Celulares | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0003] Celulares | [I.2] Daños por agua | D | [8] | {5,4} |

| | | | | |
|---|---|---|---|---|
| [HW0004] Equipo respaldo | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0004] Equipo respaldo | [N.1] Fuego | D | [9] | {5,4} |
| [HW0004] Equipo respaldo | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0004] Equipo respaldo | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0005] Impresora | [N.1] Fuego | D | [9] | {5,4} |
| [HW0005] Impresora | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0005] Impresora | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0005] Impresora | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [AUX0001] Fuente de poder | [N.*] Desastres naturales | D | [9] | {5,4} |
| [AUX0001] Fuente de poder | [N.1] Fuego | D | [9] | {5,4} |
| [AUX0001] Fuente de poder | [I.2] Daños por agua | D | [8] | {5,4} |
| [Media0001] CD-ROM | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [Media0001] CD-ROM | [N.*] Desastres naturales | D | [9] | {5,4} |
| [Media0001] CD-ROM | [N.1] Fuego | D | [9] | {5,4} |
| [Media0001] CD-ROM | [I.2] Daños por agua | D | [8] | {5,4} |
| [Media0001] CD-ROM | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [Media0002] Memoria USB | [N.*] Desastres naturales | D | [9] | {5,4} |
| [Media0002] Memoria USB | [N.1] Fuego | D | [9] | {5,4} |
| [Media0002] Memoria USB | [I.2] Daños por agua | D | [8] | {5,4} |
| [Media0002] Memoria USB | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [Media0002] Memoria USB | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [SW0003] Aplicaciones a terceros | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [SW0006] Ofimática | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [Media0001] CD-ROM | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [Media0002] Memoria USB | [A.24] Denegación de servicio | D | [7] | {5,3} |

[bps] Conexión a internet

| activo | amenaza | D | I | R |
|---|---|---|---|---|
| [ES0002] Servicio | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [SW0001] BD Mysql | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [SW0005] Servidor www | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [HW0006] Móden | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [HW0007] access point | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [COM0001] Red de Datos | [A.24] Denegación de servicio | D | [7] | {5,4} |
| [COM0001] Red de Datos | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [COM0002] Red Inalámbrica | [A.24] Denegación de servicio | D | [7] | {5,4} |
| [COM0002] Red Inalámbrica | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [COM0003] Wifi | [A.24] Denegación de servicio | D | [6] | {5,4} |
| [COM0004] Red local | [A.24] Denegación de servicio | D | [6] | {5,4} |
| [COM0006] VPN | [A.24] Denegación de servicio | D | [6] | {5,4} |
| [HW0006] Móden | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [HW0007] access point | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [ES0002] Servicio | [A.22] Manipulación de programas | C | [7] | {5,1} |
| [ES0002] Servicio | [A.8] Difusión de software dañino | C | [7] | {5,1} |
| [SW0001] BD Mysql | [A.8] Difusión de software dañino | D, I, C | [7] | {5,1} |
| [SW0001] BD Mysql | [A.22] Manipulación de programas | D, I, C | [7] | {5,1} |
| [SW0005] Servidor www | [A.8] Difusión de software dañino | D, I, C | [7] | {5,1} |
| [SW0005] Servidor www | [A.22] Manipulación de programas | D, I, C | [7] | {5,1} |
| [HW0006] Móden | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [HW0006] Móden | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [HW0006] Móden | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [HW0007] access point | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [HW0007] access point | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [HW0007] access point | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [HW0007] access point | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |

| | | | | |
|---|---|---|---|---|
| [HW0007] access point | [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [COM0001] Red de Datos | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [COM0001] Red de Datos | [A.8] Difusión de software dañino | D | [7] | {5,1} |
| [COM0001] Red de Datos | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [COM0001] Red de Datos | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [COM0001] Red de Datos | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0001] Red de Datos | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [A.8] Difusión de software dañino | D | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [COM0003] Wifi | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0003] Wifi | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [COM0004] Red local | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [COM0004] Red local | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0005] WAM | [A.11] Acceso no autorizado | A | [7] | {5,1} |
| [COM0005] WAM | [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [COM0006] VPN | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0006] VPN | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [AUX0005] Fibra óptica | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [AUX0005] Fibra óptica | [A.11] Acceso no autorizado | A | [7] | {5,1} |
| [AUX0005] Fibra óptica | [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [COM0001] Red de Datos | [A.25] Robo de equipos | D | [7] | {5,0} |

| | | | | |
|---|---|---|---|---|
| [COM0002] Red Inalámbrica | [A.25] Robo de equipos | D | [7] | {5,0} |
| [AUX0005] Fibra óptica | [A.25] Robo de equipos | D | [7] | {5,0} |
| [HW0006] Móden | [I.*] Desastres industriales | D | [7] | {4,8} |
| [HW0006] Móden | [A.23] Manipulación del hardware | D | [7] | {4,8} |
| [HW0006] Móden | [I.1] Fuego | D | [7] | {4,8} |
| [HW0007] access point | [I.1] Fuego | D | [7] | {4,8} |
| [HW0007] access point | [A.23] Manipulación del hardware | D | [7] | {4,8} |
| [HW0007] access point | [I.*] Desastres industriales | D | [7] | {4,8} |
| [COM0001] Red de Datos | [I.*] Desastres industriales | D | [7] | {4,8} |
| [COM0001] Red de Datos | [I.1] Fuego | D | [7] | {4,8} |
| [COM0001] Red de Datos | [A.23] Manipulación del hardware | D | [7] | {4,8} |
| [COM0002] Red Inalámbrica | [I.*] Desastres industriales | D | [7] | {4,8} |
| [COM0002] Red Inalámbrica | [I.1] Fuego | D | [7] | {4,8} |
| [COM0002] Red Inalámbrica | [A.23] Manipulación del hardware | D | [7] | {4,8} |
| [AUX0005] Fibra óptica | [I.1] Fuego | D | [7] | {4,8} |
| [AUX0005] Fibra óptica | [I.*] Desastres industriales | D | [7] | {4,8} |
| [ES0002] Servicio | [A.5] Suplantación de la identidad | C | [6] | {4,5} |
| [ES0002] Servicio | [A.11] Acceso no autorizado | C | [6] | {4,5} |
| [ES0002] Servicio | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [ES0002] Servicio | [A.23] Manipulación del hardware | C | [6] | {4,5} |
| [ES0002] Servicio | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [SW0001] BD Mysql | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |
| [SW0001] BD Mysql | [A.5] Suplantación de la identidad | C | [6] | {4,5} |
| [SW0001] BD Mysql | [A.11] Acceso no autorizado | C | [6] | {4,5} |
| [SW0001] BD Mysql | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [SW0001] BD Mysql | [A.23] Manipulación del hardware | C | [6] | {4,5} |
| [SW0001] BD Mysql | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [SW0005] Servidor www | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |

| | | | | |
|---|---|---|---|---|
| [SW0005] Servidor www | [A.5] Suplantación de la identidad | C | [6] | {4,5} |
| [SW0005] Servidor www | [A.11] Acceso no autorizado | C | [6] | {4,5} |
| [SW0005] Servidor www | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [SW0005] Servidor www | [A.23] Manipulación del hardware | C | [6] | {4,5} |
| [SW0005] Servidor www | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [HW0006] Móden | [I.5.2] Avería de origen físico | D | [6] | {4,5} |
| [HW0006] Módem | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [HW0006] Móden | [A.11] Acceso no autorizado | C | [6] | {4,5} |
| [HW0006] Móden | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [HW0007] access point | [I.5.2] Avería de origen físico | D | [6] | {4,5} |
| [HW0007] access point | [A.22] Manipulación de programas | I | [6] | {4,5} |
| [HW0007] access point | [A.8] Difusión de software dañino | I | [6] | {4,5} |
| [HW0007] access point | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [HW0007] access point | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0001] Red de Datos | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0001] Red de Datos | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0001] Red de Datos | [A.22] Manipulación de programas | D | [6] | {4,5} |
| [COM0001] Red de Datos | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |
| [COM0001] Red de Datos | [I.5.2] Avería de origen físico | D | [6] | {4,5} |
| [COM0001] Red de Datos | [A.7] Uso no previsto | D | [6] | {4,5} |
| [COM0001] Red de Datos | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [A.22] Manipulación de programas | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [I.5.2] Avería de origen físico | D | [6] | {4,5} |

| | | | | |
|---|---|---|---|---|
| [COM0002] Red Inalámbrica | [A.7] Uso no previsto | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0003] Wifi | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {4,5} |
| [COM0003] Wifi | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0003] Wifi | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0003] Wifi | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0004] Red local | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {4,5} |
| [COM0004] Red local | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0004] Red local | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0004] Red local | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0005] WAM | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0006] VPN | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {4,5} |
| [COM0006] VPN | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0006] VPN | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0006] VPN | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [AUX0005] Fibra óptica | [A.7] Uso no previsto | D | [6] | {4,5} |
| [AUX0005] Fibra óptica | [A.23] Manipulación del hardware | D, C | [6] | {4,5} |
| [AUX0005] Fibra óptica | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |

Fase: [current] situación actual
[base] Red corporativa

| activo | amenaza | D | I | R |
|---|---|---|---|---|
| [SW0002] Aplicaciones propias | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0003] Aplicaciones a terceros | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0004] Antivirus | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [SW0004] Antivirus | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0006] Ofimática | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0007] SO Windows | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [HW0001] Servidor | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |

| | | | | |
|---|---|---|---|---|
| [HW0002] Laptop, pc | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [HW0003] Celulares | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [HW0004] Equipo respaldo | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [HW0005] Impresora | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [SW0004] Antivirus | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0001] Servidor | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0002] Laptop, pc | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0003] Celulares | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0004] Equipo respaldo | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0005] Impresora | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [SW0002] Aplicaciones propias | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0002] Aplicaciones propias | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [SW0003] Aplicaciones a terceros | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0003] Aplicaciones a terceros | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [SW0004] Antivirus | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [SW0004] Antivirus | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [SW0004] Antivirus | [I.10] Degradación de los soportes de almacenamiento de la información | D | [9] | {6,2} |
| [SW0004] Antivirus | [A.18] Destrucción de la información | D | [9] | {6,2} |
| [SW0004] Antivirus | [E.25] Pérdida de equipos | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [E.18] Destrucción de la información | D | [9] | {6,2} |
| [SW0004] Antivirus | [A.25] Robo de equipos | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [SW0006] Ofimática | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0006] Ofimática | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [SW0007] SO Windows | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0007] SO Windows | [A.22] Manipulación de programas | D, C | [9] | {6,2} |

| | | | | |
|---|---|---|---|---|
| [HW0001] Servidor | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0001] Servidor | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0001] Servidor | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0002] Laptop, pc | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0002] Laptop, pc | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0002] Laptop, pc | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0003] Celulares | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0003] Celulares | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0003] Celulares | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0004] Equipo respaldo | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0004] Equipo respaldo | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0004] Equipo respaldo | [E.25] Pérdida de equipos | D, C | [9] | {6,2} |
| [HW0004] Equipo respaldo | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0005] Impresora | [E.25] Pérdida de equipos | D, C | [9] | {6,2} |
| [HW0005] Impresora | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0005] Impresora | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0005] Impresora | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [AUX0001] Fuente de poder | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [Media0001] CD-ROM | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [Media0001] CD-ROM | [I.10] Degradación de los soportes de almacenamiento de la información | D | [9] | {6,2} |
| [Media0001] CD-ROM | [A.18] Destrucción de la información | D | [9] | {6,2} |
| [Media0001] CD-ROM | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [Media0001] CD-ROM | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D, C | [9] | {6,2} |
| [Media0001] CD-ROM | [E.18] Destrucción de la información | D | [9] | {6,2} |
| [Media0001] CD-ROM | [A.25] Robo de equipos | C | [9] | {6,2} |
| [Media0002] Memoria USB | [A.18] Destrucción de la información | D | [9] | {6,2} |
| [Media0002] Memoria USB | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [Media0002] Memoria USB | [I.10] Degradación de los soportes de almacenamiento de la información | D | [9] | {6,2} |

| | | | | |
|---|---|---|---|---|
| [Media0002] Memoria USB | [E.18] Destrucción de la información | D | [9] | {6,2} |
| [Media0002] Memoria USB | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D, C | [9] | {6,2} |
| [Media0002] Memoria USB | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [Media0002] Memoria USB | [A.25] Robo de equipos | C | [9] | {6,2} |
| [SW0004] Antivirus | [I.*] Desastres industriales | D | [9] | {6,0} |
| [SW0004] Antivirus | [I.1] Fuego | D | [9] | {6,0} |
| [HW0001] Servidor | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0001] Servidor | [I.1] Fuego | D | [9] | {6,0} |
| [HW0002] Laptop, pc | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0002] Laptop, pc | [I.1] Fuego | D | [9] | {6,0} |
| [HW0003] Celulares | [I.1] Fuego | D | [9] | {6,0} |
| [HW0003] Celulares | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0004] Equipo respaldo | [A.25] Robo de equipos | D, C | [9] | {6,0} |
| [HW0004] Equipo respaldo | [I.1] Fuego | D | [9] | {6,0} |
| [HW0004] Equipo respaldo | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0005] Impresora | [A.25] Robo de equipos | D, C | [9] | {6,0} |
| [HW0005] Impresora | [I.1] Fuego | D | [9] | {6,0} |
| [HW0005] Impresora | [I.*] Desastres industriales | D | [9] | {6,0} |
| [AUX0001] Fuente de poder | [I.*] Desastres industriales | D | [9] | {6,0} |
| [AUX0001] Fuente de poder | [I.1] Fuego | D | [9] | {6,0} |
| [AUX0001] Fuente de poder | [A.25] Robo de equipos | D | [9] | {6,0} |
| [Media0001] CD-ROM | [I.1] Fuego | D | [9] | {6,0} |
| [Media0001] CD-ROM | [I.*] Desastres industriales | D | [9] | {6,0} |
| [Media0002] Memoria USB | [I.1] Fuego | D | [9] | {6,0} |
| [Media0002] Memoria USB | [I.*] Desastres industriales | D | [9] | {6,0} |
| [ES0001] Datos del negocio | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [ES0003] Procesos del negocio | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0002] Aplicaciones propias | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0002] Aplicaciones propias | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |

| | | | | |
|---|---|---|---|---|
| [SW0003] Aplicaciones a terceros | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0003] Aplicaciones a terceros | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0004] Antivirus | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0004] Antivirus | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [SW0004] Antivirus | [I.3] Contaminación medioambiental | D | [8] | {5,7} |
| [SW0004] Antivirus | [A.7] Uso no previsto | D | [8] | {5,7} |
| [SW0004] Antivirus | [A.23] Manipulación del hardware | D, C | [8] | {5,7} |
| [SW0004] Antivirus | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [SW0004] Antivirus | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0006] Ofimática | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0006] Ofimática | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0007] SO Windows | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0007] SO Windows | [A.15] Modificación de la información | I | [7] | {5,7} |
| [SW0007] SO Windows | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0001] Servidor | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0001] Servidor | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0001] Servidor | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0002] Laptop, pc | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0002] Laptop, pc | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0002] Laptop, pc | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0003] Celulares | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0003] Celulares | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0003] Celulares | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0004] Equipo respaldo | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0004] Equipo respaldo | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0004] Equipo respaldo | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0005] Impresora | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0005] Impresora | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0005] Impresora | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0001] Fuente de poder | [A.7] Uso no previsto | D | [8] | {5,7} |
| [AUX0001] Fuente de poder | [A.23] Manipulación del hardware | D | [8] | {5,7} |

| | | | | |
|---|---|---|---|---|
| [AUX0001] Fuente de poder | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0002] Ups | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0003] Generador eléctrico | [A.15] Modificación de la información | I | [7] | {5,7} |
| [AUX0003] Generador eléctrico | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0004] Aire acondicionado | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [Media0001] CD-ROM | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [Media0001] CD-ROM | [I.3] Contaminación medioambiental | D | [8] | {5,7} |
| [Media0001] CD-ROM | [A.15] Modificación de la información | I | [7] | {5,7} |
| [Media0001] CD-ROM | [E.25] Pérdida de equipos | C | [8] | {5,7} |
| [Media0001] CD-ROM | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [Media0001] CD-ROM | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [Media0002] Memoria USB | [I.3] Contaminación medioambiental | D | [8] | {5,7} |
| [Media0002] Memoria USB | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [Media0002] Memoria USB | [A.15] Modificación de la información | I | [7] | {5,7} |
| [Media0002] Memoria USB | [E.25] Pérdida de equipos | C | [8] | {5,7} |
| [Media0002] Memoria USB | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [Media0002] Memoria USB | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0003] Celulares | [A.25] Robo de equipos | C | [6] | {5,6} |
| [HW0003] Celulares | [E.25] Pérdida de equipos | C | [6] | {5,6} |
| [SW0003] Aplicaciones a terceros | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [SW0004] Antivirus | [N.*] Desastres naturales | D | [9] | {5,4} |
| [SW0004] Antivirus | [N.1] Fuego | D | [9] | {5,4} |
| [SW0004] Antivirus | [I.2] Daños por agua | D | [8] | {5,4} |
| [SW0006] Ofimática | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [HW0001] Servidor | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0001] Servidor | [A.25] Robo de equipos | D, C | [9] | {5,4} |
| [HW0001] Servidor | [E.25] Pérdida de equipos | D, C | [9] | {5,4} |
| [HW0001] Servidor | [N.1] Fuego | D | [9] | {5,4} |

| | | | | |
|---|---|---|---|---|
| [HW0001] Servidor | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0001] Servidor | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0001] Servidor | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [HW0002] Laptop, pc | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0002] Laptop, pc | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0002] Laptop, pc | [N.1] Fuego | D | [9] | {5,4} |
| [HW0002] Laptop, pc | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0002] Laptop, pc | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [HW0003] Celulares | [N.1] Fuego | D | [9] | {5,4} |
| [HW0003] Celulares | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0003] Celulares | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0003] Celulares | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0004] Equipo respaldo | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0004] Equipo respaldo | [N.1] Fuego | D | [9] | {5,4} |
| [HW0004] Equipo respaldo | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0004] Equipo respaldo | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0005] Impresora | [N.1] Fuego | D | [9] | {5,4} |
| [HW0005] Impresora | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0005] Impresora | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0005] Impresora | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [AUX0001] Fuente de poder | [N.*] Desastres naturales | D | [9] | {5,4} |
| [AUX0001] Fuente de poder | [N.1] Fuego | D | [9] | {5,4} |
| [AUX0001] Fuente de poder | [I.2] Daños por agua | D | [8] | {5,4} |
| [Media0001] CD-ROM | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [Media0001] CD-ROM | [N.*] Desastres naturales | D | [9] | {5,4} |
| [Media0001] CD-ROM | [N.1] Fuego | D | [9] | {5,4} |
| [Media0001] CD-ROM | [I.2] Daños por agua | D | [8] | {5,4} |
| [Media0001] CD-ROM | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [Media0002] Memoria USB | [N.*] Desastres naturales | D | [9] | {5,4} |

| | | | | |
|---|---|---|---|---|
| [Media0002] Memoria USB | [N.1] Fuego | D | [9] | {5,4} |
| [Media0002] Memoria USB | [I.2] Daños por agua | D | [8] | {5,4} |
| [Media0002] Memoria USB | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [Media0002] Memoria USB | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [SW0003] Aplicaciones a terceros | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [SW0006] Ofimática | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [Media0001] CD-ROM | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [Media0002] Memoria USB | [A.24] Denegación de servicio | D | [7] | {5,3} |

[bps] Conexión a internet

| activo | amenaza | D | I | R |
|---|---|---|---|---|
| [ES0002] Servicio | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [SW0001] BD Mysql | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [SW0005] Servidor www | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [HW0006] Móden | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [HW0007] access point | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [COM0001] Red de Datos | [A.24] Denegación de servicio | D | [7] | {5,4} |
| [COM0001] Red de Datos | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [COM0002] Red Inalámbrica | [A.24] Denegación de servicio | D | [7] | {5,4} |
| [COM0002] Red Inalámbrica | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [COM0003] Wifi | [A.24] Denegación de servicio | D | [6] | {5,4} |
| [COM0004] Red local | [A.24] Denegación de servicio | D | [6] | {5,4} |
| [COM0006] VPN | [A.24] Denegación de servicio | D | [6] | {5,4} |
| [HW0006] Móden | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [HW0007] access point | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [ES0002] Servicio | [A.22] Manipulación de programas | C | [7] | {5,1} |
| [ES0002] Servicio | [A.8] Difusión de software dañino | C | [7] | {5,1} |
| [SW0001] BD Mysql | [A.8] Difusión de software dañino | D, I, C | [7] | {5,1} |

| | | | | |
|---|---|---|---|---|
| [SW0001] BD Mysql | [A.22] Manipulación de programas | D, I, C | [7] | {5,1} |
| [SW0005] Servidor www | [A.8] Difusión de software dañino | D, I, C | [7] | {5,1} |
| [SW0005] Servidor www | [A.22] Manipulación de programas | D, I, C | [7] | {5,1} |
| [HW0006] Móden | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [HW0006] Móden | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [HW0006] Móden | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [HW0007] access point | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [HW0007] access point | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [HW0007] access point | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [HW0007] access point | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [HW0007] access point | [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [COM0001] Red de Datos | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [COM0001] Red de Datos | [A.8] Difusión de software dañino | D | [7] | {5,1} |
| [COM0001] Red de Datos | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [COM0001] Red de Datos | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [COM0001] Red de Datos | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0001] Red de Datos | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [A.8] Difusión de software dañino | D | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [COM0003] Wifi | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0003] Wifi | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |

| | | | | |
|---|---|---|---|---|
| [COM0004] Red local | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [COM0004] Red local | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0005] WAM | [A.11] Acceso no autorizado | A | [7] | {5,1} |
| [COM0005] WAM | [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [COM0006] VPN | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0006] VPN | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [AUX0005] Fibra óptica | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [AUX0005] Fibra óptica | [A.11] Acceso no autorizado | A | [7] | {5,1} |
| [AUX0005] Fibra óptica | [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [COM0001] Red de Datos | [A.25] Robo de equipos | D | [7] | {5,0} |
| [COM0002] Red Inalámbrica | [A.25] Robo de equipos | D | [7] | {5,0} |
| [AUX0005] Fibra óptica | [A.25] Robo de equipos | D | [7] | {5,0} |
| [HW0006] Móden | [I.*] Desastres industriales | D | [7] | {4,8} |
| [HW0006] Móden | [A.23] Manipulación del hardware | D | [7] | {4,8} |
| [HW0006] Móden | [I.1] Fuego | D | [7] | {4,8} |
| [HW0007] access point | [I.1] Fuego | D | [7] | {4,8} |
| [HW0007] access point | [A.23] Manipulación del hardware | D | [7] | {4,8} |
| [HW0007] access point | [I.*] Desastres industriales | D | [7] | {4,8} |
| [COM0001] Red de Datos | [I.*] Desastres industriales | D | [7] | {4,8} |
| [COM0001] Red de Datos | [I.1] Fuego | D | [7] | {4,8} |
| [COM0001] Red de Datos | [A.23] Manipulación del hardware | D | [7] | {4,8} |
| [COM0002] Red Inalámbrica | [I.*] Desastres industriales | D | [7] | {4,8} |
| [COM0002] Red Inalámbrica | [I.1] Fuego | D | [7] | {4,8} |
| [COM0002] Red Inalámbrica | [A.23] Manipulación del hardware | D | [7] | {4,8} |
| [AUX0005] Fibra óptica | [I.1] Fuego | D | [7] | {4,8} |
| [AUX0005] Fibra óptica | [I.*] Desastres industriales | D | [7] | {4,8} |
| [ES0002] Servicio | [A.5] Suplantación de la identidad | C | [6] | {4,5} |
| [ES0002] Servicio | [A.11] Acceso no autorizado | C | [6] | {4,5} |

| | | | | |
|---|---|---|---|---|
| [ES0002] Servicio | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [ES0002] Servicio | [A.23] Manipulación del hardware | C | [6] | {4,5} |
| [ES0002] Servicio | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [SW0001] BD Mysql | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |
| [SW0001] BD Mysql | [A.5] Suplantación de la identidad | C | [6] | {4,5} |
| [SW0001] BD Mysql | [A.11] Acceso no autorizado | C | [6] | {4,5} |
| [SW0001] BD Mysql | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [SW0001] BD Mysql | [A.23] Manipulación del hardware | C | [6] | {4,5} |
| [SW0001] BD Mysql | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [SW0005] Servidor www | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |
| [SW0005] Servidor www | [A.5] Suplantación de la identidad | C | [6] | {4,5} |
| [SW0005] Servidor www | [A.11] Acceso no autorizado | C | [6] | {4,5} |
| [SW0005] Servidor www | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [SW0005] Servidor www | [A.23] Manipulación del hardware | C | [6] | {4,5} |
| [SW0005] Servidor www | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [HW0006] Móden | [I.5.2] Avería de origen físico | D | [6] | {4,5} |
| [HW0006] Móden | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [HW0006] Móden | [A.11] Acceso no autorizado | C | [6] | {4,5} |
| [HW0006] Móden | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [HW0007] access point | [I.5.2] Avería de origen físico | D | [6] | {4,5} |
| [HW0007] access point | [A.22] Manipulación de programas | I | [6] | {4,5} |
| [HW0007] access point | [A.8] Difusión de software dañino | I | [6] | {4,5} |
| [HW0007] access point | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [HW0007] access point | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0001] Red de Datos | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0001] Red de Datos | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0001] Red de Datos | [A.22] Manipulación de programas | D | [6] | {4,5} |
| [COM0001] Red de Datos | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |

| | | | | |
|---|---|---|---|---|
| [COM0001] Red de Datos | [I.5.2] Avería de origen físico | D | [6] | {4,5} |
| [COM0001] Red de Datos | [A.7] Uso no previsto | D | [6] | {4,5} |
| [COM0001] Red de Datos | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [A.22] Manipulación de programas | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [I.5.2] Avería de origen físico | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [A.7] Uso no previsto | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0003] Wifi | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {4,5} |
| [COM0003] Wifi | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0003] Wifi | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0003] Wifi | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0004] Red local | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {4,5} |
| [COM0004] Red local | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0004] Red local | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0004] Red local | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0005] WAM | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0006] VPN | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {4,5} |
| [COM0006] VPN | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0006] VPN | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0006] VPN | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [AUX0005] Fibra óptica | [A.7] Uso no previsto | D | [6] | {4,5} |
| [AUX0005] Fibra óptica | [A.23] Manipulación del hardware | D, C | [6] | {4,5} |
| [AUX0005] Fibra óptica | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |

Fase: [target] situación objetivo
[base] Red corporativa

| activo | amenaza | D | I | R |
|---|---|---|---|---|
| [SW0002] Aplicaciones propias | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0003] Aplicaciones a terceros | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0004] Antivirus | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [SW0004] Antivirus | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0006] Ofimática | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [SW0007] SO Windows | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [8] | {6,6} |
| [HW0001] Servidor | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [HW0002] Laptop, pc | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [HW0003] Celulares | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [HW0004] Equipo respaldo | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [HW0005] Impresora | [E.24] Caída del sistema por agotamiento de recursos | D | [8] | {6,6} |
| [SW0004] Antivirus | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0001] Servidor | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0002] Laptop, pc | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0003] Celulares | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0004] Equipo respaldo | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [HW0005] Impresora | [A.24] Denegación de servicio | D | [9] | {6,5} |
| [SW0002] Aplicaciones propias | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0002] Aplicaciones propias | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [SW0003] Aplicaciones a terceros | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0003] Aplicaciones a terceros | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [SW0004] Antivirus | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [SW0004] Antivirus | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [SW0004] Antivirus | [I.10] Degradación de los soportes de almacenamiento de la información | D | [9] | {6,2} |
| [SW0004] Antivirus | [A.18] Destrucción de la información | D | [9] | {6,2} |
| [SW0004] Antivirus | [E.25] Pérdida de equipos | D, C | [9] | {6,2} |

| | | | | |
|---|---|---|---|---|
| [SW0004] Antivirus | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [E.18] Destrucción de la información | D | [9] | {6,2} |
| [SW0004] Antivirus | [A.25] Robo de equipos | D, C | [9] | {6,2} |
| [SW0004] Antivirus | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [SW0006] Ofimática | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0006] Ofimática | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [SW0007] SO Windows | [A.8] Difusión de software dañino | D, C | [9] | {6,2} |
| [SW0007] SO Windows | [A.22] Manipulación de programas | D, C | [9] | {6,2} |
| [HW0001] Servidor | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0001] Servidor | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0001] Servidor | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0002] Laptop, pc | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0002] Laptop, pc | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0002] Laptop, pc | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0003] Celulares | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0003] Celulares | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0003] Celulares | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0004] Equipo respaldo | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0004] Equipo respaldo | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0004] Equipo respaldo | [E.25] Pérdida de equipos | D, C | [9] | {6,2} |
| [HW0004] Equipo respaldo | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [HW0005] Impresora | [E.25] Pérdida de equipos | D, C | [9] | {6,2} |
| [HW0005] Impresora | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [HW0005] Impresora | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [HW0005] Impresora | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [AUX0001] Fuente de poder | [A.26] Ataque destructivo | D | [9] | {6,2} |
| [Media0001] CD-ROM | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [Media0001] CD-ROM | [I.10] Degradación de los soportes de almacenamiento de la información | D | [9] | {6,2} |
| [Media0001] CD-ROM | [A.18] Destrucción de la información | D | [9] | {6,2} |

| | | | | |
|---|---|---|---|---|
| [Media0001] CD-ROM | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [Media0001] CD-ROM | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D, C | [9] | {6,2} |
| [Media0001] CD-ROM | [E.18] Destrucción de la información | D | [9] | {6,2} |
| [Media0001] CD-ROM | [A.25] Robo de equipos | C | [9] | {6,2} |
| [Media0002] Memoria USB | [A.18] Destrucción de la información | D | [9] | {6,2} |
| [Media0002] Memoria USB | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [9] | {6,2} |
| [Media0002] Memoria USB | [I.10] Degradación de los soportes de almacenamiento de la información | D | [9] | {6,2} |
| [Media0002] Memoria USB | [E.18] Destrucción de la información | D | [9] | {6,2} |
| [Media0002] Memoria USB | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D, C | [9] | {6,2} |
| [Media0002] Memoria USB | [I.6] Corte del suministro eléctrico | D | [9] | {6,2} |
| [Media0002] Memoria USB | [A.25] Robo de equipos | C | [9] | {6,2} |
| [SW0004] Antivirus | [I.*] Desastres industriales | D | [9] | {6,0} |
| [SW0004] Antivirus | [I.1] Fuego | D | [9] | {6,0} |
| [HW0001] Servidor | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0001] Servidor | [I.1] Fuego | D | [9] | {6,0} |
| [HW0002] Laptop, pc | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0002] Laptop, pc | [I.1] Fuego | D | [9] | {6,0} |
| [HW0003] Celulares | [I.1] Fuego | D | [9] | {6,0} |
| [HW0003] Celulares | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0004] Equipo respaldo | [A.25] Robo de equipos | D, C | [9] | {6,0} |
| [HW0004] Equipo respaldo | [I.1] Fuego | D | [9] | {6,0} |
| [HW0004] Equipo respaldo | [I.*] Desastres industriales | D | [9] | {6,0} |
| [HW0005] Impresora | [A.25] Robo de equipos | D, C | [9] | {6,0} |
| [HW0005] Impresora | [I.1] Fuego | D | [9] | {6,0} |
| [HW0005] Impresora | [I.*] Desastres industriales | D | [9] | {6,0} |
| [AUX0001] Fuente de poder | [I.*] Desastres industriales | D | [9] | {6,0} |
| [AUX0001] Fuente de poder | [I.1] Fuego | D | [9] | {6,0} |
| [AUX0001] Fuente de poder | [A.25] Robo de equipos | D | [9] | {6,0} |
| [Media0001] CD-ROM | [I.1] Fuego | D | [9] | {6,0} |

| | | | | |
|---|---|---|---|---|
| [Media0001] CD-ROM | [I.*] Desastres industriales | D | [9] | {6,0} |
| [Media0002] Memoria USB | [I.1] Fuego | D | [9] | {6,0} |
| [Media0002] Memoria USB | [I.*] Desastres industriales | D | [9] | {6,0} |
| [ES0001] Datos del negocio | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [ES0003] Procesos del negocio | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0002] Aplicaciones propias | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0002] Aplicaciones propias | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0003] Aplicaciones a terceros | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0003] Aplicaciones a terceros | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0004] Antivirus | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0004] Antivirus | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [SW0004] Antivirus | [I.3] Contaminación medioambiental | D | [8] | {5,7} |
| [SW0004] Antivirus | [A.7] Uso no previsto | D | [8] | {5,7} |
| [SW0004] Antivirus | [A.23] Manipulación del hardware | D, C | [8] | {5,7} |
| [SW0004] Antivirus | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [SW0004] Antivirus | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0006] Ofimática | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0006] Ofimática | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [SW0007] SO Windows | [I.5.1] Avería de origen lógico | D | [8] | {5,7} |
| [SW0007] SO Windows | [A.15] Modificación de la información | I | [7] | {5,7} |
| [SW0007] SO Windows | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0001] Servidor | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0001] Servidor | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0001] Servidor | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0002] Laptop, pc | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0002] Laptop, pc | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0002] Laptop, pc | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0003] Celulares | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0003] Celulares | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0003] Celulares | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |

| | | | | |
|---|---|---|---|---|
| [HW0004] Equipo respaldo | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0004] Equipo respaldo | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0004] Equipo respaldo | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0005] Impresora | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [HW0005] Impresora | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [HW0005] Impresora | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0001] Fuente de poder | [A.7] Uso no previsto | D | [8] | {5,7} |
| [AUX0001] Fuente de poder | [A.23] Manipulación del hardware | D | [8] | {5,7} |
| [AUX0001] Fuente de poder | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0002] Ups | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0003] Generador eléctrico | [A.15] Modificación de la información | I | [7] | {5,7} |
| [AUX0003] Generador eléctrico | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [AUX0004] Aire acondicionado | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [Media0001] CD-ROM | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [Media0001] CD-ROM | [I.3] Contaminación medioambiental | D | [8] | {5,7} |
| [Media0001] CD-ROM | [A.15] Modificación de la información | I | [7] | {5,7} |
| [Media0001] CD-ROM | [E.25] Pérdida de equipos | C | [8] | {5,7} |
| [Media0001] CD-ROM | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [Media0001] CD-ROM | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [Media0002] Memoria USB | [I.3] Contaminación medioambiental | D | [8] | {5,7} |
| [Media0002] Memoria USB | [I.5.2] Avería de origen físico | D | [8] | {5,7} |
| [Media0002] Memoria USB | [A.15] Modificación de la información | I | [7] | {5,7} |
| [Media0002] Memoria USB | [E.25] Pérdida de equipos | C | [8] | {5,7} |
| [Media0002] Memoria USB | [A.11] Acceso no autorizado | C | [8] | {5,7} |
| [Media0002] Memoria USB | [A.13] Repudio (negación de actuaciones) | T | [8] | {5,7} |
| [HW0003] Celulares | [A.25] Robo de equipos | C | [6] | {5,6} |

| | | | | |
|---|---|---|---|---|
| [HW0003] Celulares | [E.25] Pérdida de equipos | C | [6] | {5,6} |
| [SW0003] Aplicaciones a terceros | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [SW0004] Antivirus | [N.*] Desastres naturales | D | [9] | {5,4} |
| [SW0004] Antivirus | [N.1] Fuego | D | [9] | {5,4} |
| [SW0004] Antivirus | [I.2] Daños por agua | D | [8] | {5,4} |
| [SW0006] Ofimática | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [HW0001] Servidor | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0001] Servidor | [A.25] Robo de equipos | D, C | [9] | {5,4} |
| [HW0001] Servidor | [E.25] Pérdida de equipos | D, C | [9] | {5,4} |
| [HW0001] Servidor | [N.1] Fuego | D | [9] | {5,4} |
| [HW0001] Servidor | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0001] Servidor | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0001] Servidor | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [HW0002] Laptop, pc | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0002] Laptop, pc | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0002] Laptop, pc | [N.1] Fuego | D | [9] | {5,4} |
| [HW0002] Laptop, pc | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0002] Laptop, pc | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [HW0003] Celulares | [N.1] Fuego | D | [9] | {5,4} |
| [HW0003] Celulares | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0003] Celulares | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0003] Celulares | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0004] Equipo respaldo | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0004] Equipo respaldo | [N.1] Fuego | D | [9] | {5,4} |
| [HW0004] Equipo respaldo | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0004] Equipo respaldo | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [HW0005] Impresora | [N.1] Fuego | D | [9] | {5,4} |
| [HW0005] Impresora | [N.*] Desastres naturales | D | [9] | {5,4} |
| [HW0005] Impresora | [I.2] Daños por agua | D | [8] | {5,4} |
| [HW0005] Impresora | [A.23] Manipulación del hardware | D, C | [8] | {5,4} |
| [AUX0001] Fuente de poder | [N.*] Desastres naturales | D | [9] | {5,4} |
| [AUX0001] Fuente de poder | [N.1] Fuego | D | [9] | {5,4} |

| | | | | |
|---|---|---|---|---|
| [AUX0001] Fuente de poder | [I.2] Daños por agua | D | [8] | {5,4} |
| [Media0001] CD-ROM | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [Media0001] CD-ROM | [N.*] Desastres naturales | D | [9] | {5,4} |
| [Media0001] CD-ROM | [N.1] Fuego | D | [9] | {5,4} |
| [Media0001] CD-ROM | [I.2] Daños por agua | D | [8] | {5,4} |
| [Media0001] CD-ROM | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [Media0002] Memoria USB | [N.*] Desastres naturales | D | [9] | {5,4} |
| [Media0002] Memoria USB | [N.1] Fuego | D | [9] | {5,4} |
| [Media0002] Memoria USB | [I.2] Daños por agua | D | [8] | {5,4} |
| [Media0002] Memoria USB | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [Media0002] Memoria USB | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [SW0003] Aplicaciones a terceros | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [SW0006] Ofimática | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [Media0001] CD-ROM | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [Media0002] Memoria USB | [A.24] Denegación de servicio | D | [7] | {5,3} |

[bps] Conexión a internet

| activo | amenaza | D | I | R |
|---|---|---|---|---|
| [ES0002] Servicio | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [SW0001] BD Mysql | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [SW0005] Servidor www | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [6] | {5,4} |
| [HW0006] Móden | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [HW0007] access point | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [COM0001] Red de Datos | [A.24] Denegación de servicio | D | [7] | {5,4} |
| [COM0001] Red de Datos | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [COM0002] Red Inalámbrica | [A.24] Denegación de servicio | D | [7] | {5,4} |

| | | | | |
|---|---|---|---|---|
| [COM0002] Red Inalámbrica | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {5,4} |
| [COM0003] Wifi | [A.24] Denegación de servicio | D | [6] | {5,4} |
| [COM0004] Red local | [A.24] Denegación de servicio | D | [6] | {5,4} |
| [COM0006] VPN | [A.24] Denegación de servicio | D | [6] | {5,4} |
| [HW0006] Móden | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [HW0007] access point | [A.24] Denegación de servicio | D | [7] | {5,3} |
| [ES0002] Servicio | [A.22] Manipulación de programas | C | [7] | {5,1} |
| [ES0002] Servicio | [A.8] Difusión de software dañino | C | [7] | {5,1} |
| [SW0001] BD Mysql | [A.8] Difusión de software dañino | D, I, C | [7] | {5,1} |
| [SW0001] BD Mysql | [A.22] Manipulación de programas | D, I, C | [7] | {5,1} |
| [SW0005] Servidor www | [A.8] Difusión de software dañino | D, I, C | [7] | {5,1} |
| [SW0005] Servidor www | [A.22] Manipulación de programas | D, I, C | [7] | {5,1} |
| [HW0006] Móden | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [HW0006] Móden | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [HW0006] Móden | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [HW0007] access point | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [HW0007] access point | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [HW0007] access point | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [HW0007] access point | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [HW0007] access point | [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [COM0001] Red de Datos | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [COM0001] Red de Datos | [A.8] Difusión de software dañino | D | [7] | {5,1} |
| [COM0001] Red de Datos | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [COM0001] Red de Datos | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [COM0001] Red de Datos | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0001] Red de Datos | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [I.6] Corte del suministro eléctrico | D | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [A.8] Difusión de software dañino | D | [7] | {5,1} |

| | | | | |
|---|---|---|---|---|
| [COM0002] Red Inalámbrica | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0002] Red Inalámbrica | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [COM0003] Wifi | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0003] Wifi | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [COM0004] Red local | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [COM0004] Red local | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0005] WAM | [A.11] Acceso no autorizado | A | [7] | {5,1} |
| [COM0005] WAM | [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [COM0006] VPN | [A.11] Acceso no autorizado | C, A | [7] | {5,1} |
| [COM0006] VPN | [A.5] Suplantación de la identidad | C, A | [7] | {5,1} |
| [AUX0005] Fibra óptica | [A.26] Ataque destructivo | D | [7] | {5,1} |
| [AUX0005] Fibra óptica | [A.11] Acceso no autorizado | A | [7] | {5,1} |
| [AUX0005] Fibra óptica | [A.5] Suplantación de la identidad | A | [7] | {5,1} |
| [COM0001] Red de Datos | [A.25] Robo de equipos | D | [7] | {5,0} |
| [COM0002] Red Inalámbrica | [A.25] Robo de equipos | D | [7] | {5,0} |
| [AUX0005] Fibra óptica | [A.25] Robo de equipos | D | [7] | {5,0} |
| [HW0006] Móden | [I.*] Desastres industriales | D | [7] | {4,8} |
| [HW0006] Móden | [A.23] Manipulación del hardware | D | [7] | {4,8} |
| [HW0006] Móden | [I.1] Fuego | D | [7] | {4,8} |
| [HW0007] access point | [I.1] Fuego | D | [7] | {4,8} |
| [HW0007] access point | [A.23] Manipulación del hardware | D | [7] | {4,8} |
| [HW0007] access point | [I.*] Desastres industriales | D | [7] | {4,8} |
| [COM0001] Red de Datos | [I.*] Desastres industriales | D | [7] | {4,8} |
| [COM0001] Red de Datos | [I.1] Fuego | D | [7] | {4,8} |
| [COM0001] Red de Datos | [A.23] Manipulación del hardware | D | [7] | {4,8} |

| | | | | |
|---|---|---|---|---|
| [COM0002] Red Inalámbrica | [I.*] Desastres industriales | D | [7] | {4,8} |
| [COM0002] Red Inalámbrica | [I.1] Fuego | D | [7] | {4,8} |
| [COM0002] Red Inalámbrica | [A.23] Manipulación del hardware | D | [7] | {4,8} |
| [AUX0005] Fibra óptica | [I.1] Fuego | D | [7] | {4,8} |
| [AUX0005] Fibra óptica | [I.*] Desastres industriales | D | [7] | {4,8} |
| [ES0002] Servicio | [A.5] Suplantación de la identidad | C | [6] | {4,5} |
| [ES0002] Servicio | [A.11] Acceso no autorizado | C | [6] | {4,5} |
| [ES0002] Servicio | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [ES0002] Servicio | [A.23] Manipulación del hardware | C | [6] | {4,5} |
| [ES0002] Servicio | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [SW0001] BD Mysql | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |
| [SW0001] BD Mysql | [A.5] Suplantación de la identidad | C | [6] | {4,5} |
| [SW0001] BD Mysql | [A.11] Acceso no autorizado | C | [6] | {4,5} |
| [SW0001] BD Mysql | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [SW0001] BD Mysql | [A.23] Manipulación del hardware | C | [6] | {4,5} |
| [SW0001] BD Mysql | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [SW0005] Servidor www | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |
| [SW0005] Servidor www | [A.5] Suplantación de la identidad | C | [6] | {4,5} |
| [SW0005] Servidor www | [A.11] Acceso no autorizado | C | [6] | {4,5} |
| [SW0005] Servidor www | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [SW0005] Servidor www | [A.23] Manipulación del hardware | C | [6] | {4,5} |
| [SW0005] Servidor www | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [HW0006] Móden | [I.5.2] Avería de origen físico | D | [6] | {4,5} |
| [HW0006] Móden | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [HW0006] Móden | [A.11] Acceso no autorizado | C | [6] | {4,5} |
| [HW0006] Móden | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [HW0007] access point | [I.5.2] Avería de origen físico | D | [6] | {4,5} |
| [HW0007] access point | [A.22] Manipulación de programas | I | [6] | {4,5} |
| [HW0007] access point | [A.8] Difusión de software dañino | I | [6] | {4,5} |

| | | | | |
|---|---|---|---|---|
| [HW0007] access point | [E.25] Pérdida de equipos | C | [6] | {4,5} |
| [HW0007] access point | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0001] Red de Datos | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0001] Red de Datos | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0001] Red de Datos | [A.22] Manipulación de programas | D | [6] | {4,5} |
| [COM0001] Red de Datos | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |
| [COM0001] Red de Datos | [I.5.2] Avería de origen físico | D | [6] | {4,5} |
| [COM0001] Red de Datos | [A.7] Uso no previsto | D | [6] | {4,5} |
| [COM0001] Red de Datos | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [A.22] Manipulación de programas | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [I.5.1] Avería de origen lógico | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [I.5.2] Avería de origen físico | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [A.7] Uso no previsto | D | [6] | {4,5} |
| [COM0002] Red Inalámbrica | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0003] Wifi | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {4,5} |
| [COM0003] Wifi | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0003] Wifi | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0003] Wifi | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0004] Red local | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {4,5} |
| [COM0004] Red local | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |
| [COM0004] Red local | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0004] Red local | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0005] WAM | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [COM0006] VPN | [E.24] Caída del sistema por agotamiento de recursos | D | [6] | {4,5} |
| [COM0006] VPN | [I.8] Fallo de servicios de comunicaciones | D | [6] | {4,5} |

| | | | | |
|---|---|---|---|---|
| [COM0006] VPN | [A.18] Destrucción de la información | D | [6] | {4,5} |
| [COM0006] VPN | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |
| [AUX0005] Fibra óptica | [A.7] Uso no previsto | D | [6] | {4,5} |
| [AUX0005] Fibra óptica | [A.23] Manipulación del hardware | D, C | [6] | {4,5} |
| [AUX0005] Fibra óptica | [A.13] Repudio (negación de actuaciones) | T | [6] | {4,5} |

Fase: [PILAR] recomendación
[base] Red corporativa

| activo | amenaza | D | I | R |
|---|---|---|---|---|
| [SW0004] Antivirus | [E.24] Caída del sistema por agotamiento de recursos | D | [4] | {3,7} |
| [HW0001] Servidor | [E.24] Caída del sistema por agotamiento de recursos | D | [4] | {3,7} |
| [HW0002] Laptop, pc | [E.24] Caída del sistema por agotamiento de recursos | D | [4] | {3,7} |
| [HW0003] Celulares | [E.24] Caída del sistema por agotamiento de recursos | D | [4] | {3,7} |
| [HW0004] Equipo respaldo | [E.24] Caída del sistema por agotamiento de recursos | D | [4] | {3,7} |
| [HW0005] Impresora | [E.24] Caída del sistema por agotamiento de recursos | D | [4] | {3,7} |
| [SW0002] Aplicaciones propias | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [4] | {3,6} |
| [SW0003] Aplicaciones a terceros | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [4] | {3,6} |
| [SW0004] Antivirus | [A.24] Denegación de servicio | D | [5] | {3,6} |
| [SW0004] Antivirus | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [4] | {3,6} |
| [SW0006] Ofimática | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [4] | {3,6} |
| [SW0007] SO Windows | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [4] | {3,6} |
| [HW0001] Servidor | [A.24] Denegación de servicio | D | [5] | {3,6} |
| [HW0002] Laptop, pc | [A.24] Denegación de servicio | D | [5] | {3,6} |
| [HW0003] Celulares | [A.24] Denegación de servicio | D | [5] | {3,6} |
| [HW0004] Equipo respaldo | [A.24] Denegación de servicio | D | [5] | {3,6} |
| [HW0005] Impresora | [A.24] Denegación de servicio | D | [5] | {3,6} |
| [SW0004] Antivirus | [A.26] Ataque destructivo | D | [5] | {3,4} |
| [SW0004] Antivirus | [I.6] Corte del suministro eléctrico | D | [5] | {3,4} |
| [SW0004] Antivirus | [I.10] Degradación de los soportes de almacenamiento de la información | D | [5] | {3,4} |
| [SW0004] Antivirus | [E.25] Pérdida de equipos | D | [5] | {3,4} |

| | | | | |
|---|---|---|---|---|
| [SW0004] Antivirus | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [5] | {3,4} |
| [SW0004] Antivirus | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D | [5] | {3,4} |
| [SW0004] Antivirus | [E.18] Destrucción de la información | D | [5] | {3,4} |
| [SW0004] Antivirus | [A.25] Robo de equipos | D, C | [5] | {3,4} |
| [HW0001] Servidor | [A.26] Ataque destructivo | D | [5] | {3,4} |
| [HW0002] Laptop, pc | [A.26] Ataque destructivo | D | [5] | {3,4} |
| [HW0003] Celulares | [A.26] Ataque destructivo | D | [5] | {3,4} |
| [HW0004] Equipo respaldo | [A.26] Ataque destructivo | D | [5] | {3,4} |
| [HW0004] Equipo respaldo | [E.25] Pérdida de equipos | D | [5] | {3,4} |
| [HW0005] Impresora | [E.25] Pérdida de equipos | D | [5] | {3,4} |
| [HW0005] Impresora | [A.26] Ataque destructivo | D | [5] | {3,4} |
| [Media0001] CD-ROM | [I.6] Corte del suministro eléctrico | D | [5] | {3,4} |
| [Media0001] CD-ROM | [I.10] Degradación de los soportes de almacenamiento de la información | D | [5] | {3,4} |
| [Media0001] CD-ROM | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [5] | {3,4} |
| [Media0001] CD-ROM | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D | [5] | {3,4} |
| [Media0001] CD-ROM | [E.18] Destrucción de la información | D | [5] | {3,4} |
| [Media0001] CD-ROM | [A.25] Robo de equipos | C | [5] | {3,4} |
| [Media0002] Memoria USB | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [5] | {3,4} |
| [Media0002] Memoria USB | [I.10] Degradación de los soportes de almacenamiento de la información | D | [5] | {3,4} |
| [Media0002] Memoria USB | [E.18] Destrucción de la información | D | [5] | {3,4} |
| [Media0002] Memoria USB | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | D | [5] | {3,4} |
| [Media0002] Memoria USB | [I.6] Corte del suministro eléctrico | D | [5] | {3,4} |
| [Media0002] Memoria USB | [A.25] Robo de equipos | C | [5] | {3,4} |
| [SW0004] Antivirus | [A.18] Destrucción de la información | D | [5] | {3,3} |
| [HW0001] Servidor | [I.6] Corte del suministro eléctrico | D | [5] | {3,3} |
| [HW0001] Servidor | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [5] | {3,3} |
| [HW0002] Laptop, pc | [I.6] Corte del suministro eléctrico | D | [5] | {3,3} |
| [HW0002] Laptop, pc | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [5] | {3,3} |
| [HW0003] Celulares | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [5] | {3,3} |

| | | | | |
|---|---|---|---|---|
| [HW0003] Celulares | [I.6] Corte del suministro eléctrico | D | [5] | {3,3} |
| [HW0004] Equipo respaldo | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [5] | {3,3} |
| [HW0004] Equipo respaldo | [I.6] Corte del suministro eléctrico | D | [5] | {3,3} |
| [HW0005] Impresora | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [5] | {3,3} |
| [HW0005] Impresora | [I.6] Corte del suministro eléctrico | D | [5] | {3,3} |
| [AUX0001] Fuente de poder | [A.26] Ataque destructivo | D | [5] | {3,3} |
| [Media0001] CD-ROM | [A.18] Destrucción de la información | D | [5] | {3,3} |
| [Media0002] Memoria USB | [A.18] Destrucción de la información | D | [5] | {3,3} |
| [SW0002] Aplicaciones propias | [A.8] Difusión de software dañino | D, C | [5] | {3,2} |
| [SW0002] Aplicaciones propias | [A.22] Manipulación de programas | C | [5] | {3,2} |
| [SW0003] Aplicaciones a terceros | [A.8] Difusión de software dañino | D, C | [5] | {3,2} |
| [SW0003] Aplicaciones a terceros | [A.22] Manipulación de programas | C | [5] | {3,2} |
| [SW0004] Antivirus | [A.8] Difusión de software dañino | D, C | [5] | {3,2} |
| [SW0004] Antivirus | [A.22] Manipulación de programas | C | [5] | {3,2} |
| [SW0006] Ofimática | [A.8] Difusión de software dañino | D, C | [5] | {3,2} |
| [SW0006] Ofimática | [A.22] Manipulación de programas | C | [5] | {3,2} |
| [SW0007] SO Windows | [A.8] Difusión de software dañino | D, C | [5] | {3,2} |
| [SW0007] SO Windows | [A.22] Manipulación de programas | C | [5] | {3,2} |
| [SW0004] Antivirus | [I.*] Desastres industriales | D | [5] | {3,1} |
| [SW0004] Antivirus | [I.1] Fuego | D | [5] | {3,1} |
| [HW0001] Servidor | [I.*] Desastres industriales | D | [5] | {3,1} |
| [HW0001] Servidor | [I.1] Fuego | D | [5] | {3,1} |
| [HW0002] Laptop, pc | [I.*] Desastres industriales | D | [5] | {3,1} |
| [HW0002] Laptop, pc | [I.1] Fuego | D | [5] | {3,1} |
| [HW0003] Celulares | [I.1] Fuego | D | [5] | {3,1} |
| [HW0003] Celulares | [I.*] Desastres industriales | D | [5] | {3,1} |
| [HW0004] Equipo respaldo | [A.25] Robo de equipos | D | [5] | {3,1} |
| [HW0004] Equipo respaldo | [I.1] Fuego | D | [5] | {3,1} |
| [HW0004] Equipo respaldo | [I.*] Desastres industriales | D | [5] | {3,1} |
| [HW0005] Impresora | [A.25] Robo de equipos | D | [5] | {3,1} |

| | | | | |
|---|---|---|---|---|
| [HW0005] Impresora | [I.1] Fuego | D | [5] | {3,1} |
| [HW0005] Impresora | [I.*] Desastres industriales | D | [5] | {3,1} |
| [AUX0001] Fuente de poder | [I.*] Desastres industriales | D | [5] | {3,1} |
| [AUX0001] Fuente de poder | [I.1] Fuego | D | [5] | {3,1} |
| [Media0001] CD-ROM | [I.1] Fuego | D | [5] | {3,1} |
| [Media0001] CD-ROM | [I.*] Desastres industriales | D | [5] | {3,1} |
| [Media0002] Memoria USB | [I.1] Fuego | D | [5] | {3,1} |
| [Media0002] Memoria USB | [I.*] Desastres industriales | D | [5] | {3,1} |
| [AUX0001] Fuente de poder | [A.25] Robo de equipos | D | [5] | {3,0} |

[bps] Conexión a internet

| activo | amenaza | D | I | R |
|---|---|---|---|---|
| [HW0006] Móden | [E.24] Caída del sistema por agotamiento de recursos | D | [2] | {2,6} |
| [HW0007] access point | [E.24] Caída del sistema por agotamiento de recursos | D | [2] | {2,6} |
| [COM0001] Red de Datos | [A.24] Denegación de servicio | D | [3] | {2,6} |
| [COM0001] Red de Datos | [E.24] Caída del sistema por agotamiento de recursos | D | [2] | {2,6} |
| [COM0002] Red Inalámbrica | [A.24] Denegación de servicio | D | [3] | {2,6} |
| [COM0002] Red Inalámbrica | [E.24] Caída del sistema por agotamiento de recursos | D | [2] | {2,6} |
| [COM0003] Wifi | [A.24] Denegación de servicio | D | [2] | {2,6} |
| [COM0004] Red local | [A.24] Denegación de servicio | D | [2] | {2,6} |
| [COM0006] VPN | [A.24] Denegación de servicio | D | [2] | {2,6} |
| [ES0002] Servicio | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [2] | {2,5} |
| [SW0001] BD Mysql | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [2] | {2,5} |
| [SW0005] Servidor www | [E.21] Errores de mantenimiento / actualización de programas (software) | C | [2] | {2,5} |
| [HW0006] Móden | [A.24] Denegación de servicio | D | [3] | {2,5} |
| [HW0007] access point | [A.24] Denegación de servicio | D | [3] | {2,5} |
| [HW0006] Móden | [I.6] Corte del suministro eléctrico | D | [3] | {2,3} |
| [HW0006] Móden | [A.26] Ataque destructivo | D | [3] | {2,3} |
| [HW0007] access point | [I.6] Corte del suministro eléctrico | D | [3] | {2,3} |

| | | | | |
|---|---|---|---|---|
| [HW0007] access point | [A.26] Ataque destructivo | D | [3] | {2,3} |
| [HW0007] access point | [A.5] Suplantación de la identidad | A | [3] | {2,3} |
| [COM0001] Red de Datos | [I.6] Corte del suministro eléctrico | D | [3] | {2,3} |
| [COM0001] Red de Datos | [A.26] Ataque destructivo | D | [3] | {2,3} |
| [COM0002] Red Inalámbrica | [I.6] Corte del suministro eléctrico | D | [3] | {2,3} |
| [COM0002] Red Inalámbrica | [A.26] Ataque destructivo | D | [3] | {2,3} |
| [COM0002] Red Inalámbrica | [A.5] Suplantación de la identidad | A | [3] | {2,3} |
| [COM0003] Wifi | [A.5] Suplantación de la identidad | A | [3] | {2,3} |
| [COM0005] WAM | [A.5] Suplantación de la identidad | A | [3] | {2,3} |
| [COM0006] VPN | [A.5] Suplantación de la identidad | A | [3] | {2,3} |
| [AUX0005] Fibra óptica | [A.26] Ataque destructivo | D | [3] | {2,3} |
| [AUX0005] Fibra óptica | [A.5] Suplantación de la identidad | A | [3] | {2,3} |
| [ES0002] Servicio | [A.22] Manipulación de programas | C | [3] | {2,2} |
| [ES0002] Servicio | [A.8] Difusión de software dañino | C | [3] | {2,2} |
| [SW0001] BD Mysql | [A.22] Manipulación de programas | I, C | [3] | {2,2} |
| [SW0001] BD Mysql | [A.8] Difusión de software dañino | D, I, C | [3] | {2,2} |
| [SW0005] Servidor www | [A.22] Manipulación de programas | I, C | [3] | {2,2} |
| [SW0005] Servidor www | [A.8] Difusión de software dañino | D, I, C | [3] | {2,2} |
| [HW0006] Móden | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [3] | {2,2} |
| [HW0007] access point | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [3] | {2,2} |
| [HW0007] access point | [A.11] Acceso no autorizado | A | [3] | {2,2} |
| [COM0001] Red de Datos | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [3] | {2,2} |
| [COM0001] Red de Datos | [A.25] Robo de equipos | D | [3] | {2,2} |
| [COM0001] Red de Datos | [A.11] Acceso no autorizado | A | [3] | {2,2} |
| [COM0001] Red de Datos | [A.5] Suplantación de la identidad | A | [3] | {2,2} |
| [COM0002] Red Inalámbrica | [I.7] Condiciones inadecuadas de temperatura o humedad | D | [3] | {2,2} |
| [COM0002] Red Inalámbrica | [A.25] Robo de equipos | D | [3] | {2,2} |

| | | | | |
|---|---|---|---|---|
| [COM0002] Red Inalámbrica | [A.11] Acceso no autorizado | A | [3] | {2,2} |
| [COM0003] Wifi | [A.11] Acceso no autorizado | A | [3] | {2,2} |
| [COM0004] Red local | [A.5] Suplantación de la identidad | A | [3] | {2,2} |
| [COM0004] Red local | [A.11] Acceso no autorizado | A | [3] | {2,2} |
| [COM0005] WAM | [A.11] Acceso no autorizado | A | [3] | {2,2} |
| [COM0006] VPN | [A.11] Acceso no autorizado | A | [3] | {2,2} |
| [AUX0005] Fibra óptica | [A.25] Robo de equipos | D | [3] | {2,2} |
| [AUX0005] Fibra óptica | [A.11] Acceso no autorizado | A | [3] | {2,2} |
| [COM0001] Red de Datos | [A.8] Difusión de software dañino | D | [3] | {2,1} |
| [COM0002] Red Inalámbrica | [A.8] Difusión de software dañino | D | [3] | {2,1} |

## 5. Activos

Relación de activos identificados en el sistema de información.

dominio de seguridad: [base] Red corporativa
- Activos esenciales
  - [E] Equipamiento
    - [SW] Aplicaciones
      - [ES0001] Datos del negocio
    - [HW] Equipos
      - [HW0001] Servidor
      - [HW0002] Laptop, pc
      - [HW0003] Celulares
      - [HW0004] Equipo respaldo
      - [HW0005] Impresora

dominio de seguridad: [bps] Conexión a internet
- Activos esenciales
  - [E] Equipamiento
    - [COM] Comunicaciones
      - [COM0001] Red de Datos
      - [COM0002] Red Inalámbrica
      - [COM0003] Wifi
      - [COM0004] Red local
      - [COM0005] WAM
      - [COM0006] VPN

## Descripción

Detalle de los activos identificados en el sistema de información.

**dominio de seguridad: [base] Red corporativa**

**[SW] Aplicaciones**

Dominio de seguridad

[base] Red corporativa

Clases de activos

**[ES0001] Datos del negocio**

Dominio de seguridad

[base] Red corporativa

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información
  - [essential.info.biz] datos de interés para el negocio

**[ES0003] Procesos del negocio**

Dominio de seguridad

[base] Red corporativa

Clases de activos

- [essential] Activos esenciales
  - [essential. bp] proceso de negocio

**[SW0002] Aplicaciones propias**

Dominio de seguridad

[base] Red corporativa

Clases de activos

- [essential] Activos esenciales
- [SW] Aplicaciones (software)
  - [SW.prp] desarrollo propio (in house)

**[SW0003] Aplicaciones a terceros**

Dominio de seguridad

[base] Red corporativa

Clases de activos

- [essential] Activos esenciales
- [SW] Aplicaciones (software)
  - [SW.sub] desarrollo a medida (subcontratado)

**[SW0004] Antivirus**

Dominio de seguridad

[base] Red corporativa

Clases de activos
- [essential] Activos esenciales
- [SW] Aplicaciones (software)
  - [SW.sec] herramientas de seguridad
  - [SW.sec.av] anti virus

**[SW0006] Ofimática**

Dominio de seguridad
[base] Red corporativa

Clases de activos
- [essential] Activos esenciales
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std. Office] ofimática

**[SW0007] SO Windows**

Dominio de seguridad
[base] Red corporativa

Clases de activos
- [essential] Activos esenciales
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std. Os] sistema operativo
    - [SW.std. Os. Windows] Windows

**[HW] Equipos**

Dominio de seguridad
[base] Red corporativa

Clases de activos

**[HW0001] Servidor**

Dominio de seguridad
[base] Red corporativa

Clases de activos
- [essential] Activos esenciales
- [HW] Equipamiento informático (hardware)
  - [HW. host] grandes equipos (host)

**[HW0002] Laptop, pc**

Dominio de seguridad
[base] Red corporativa

Clases de activos
- [essential] Activos esenciales
- [HW] Equipamiento informático (hardware)
  - [HW. pc] informática personal

**[HW0003] Celulares**

Dominio de seguridad
[base] Red corporativa

Clases de activos
- [essential] Activos esenciales
- [HW] Equipamiento informático (hardware)
  - [HW. mobile] informática móvil

**[HW0004] Equipo respaldo**

Dominio de seguridad
[base] Red corporativa

Clases de activos
- [essential] Activos esenciales
- [HW] Equipamiento informático (hardware)
  - [HW. Backup] equipamiento de respaldo

**[HW0005] Impresora**

Dominio de seguridad
[base] Red corporativa

Clases de activos
- [essential] Activos esenciales
- [HW] Equipamiento informático (hardware)
  - [HW. peripheral] periféricos
  - [HW. peripheral.print] medios de impresión

**[COM] Comunicaciones**

Dominio de seguridad
[base] Red corporativa

Clases de activos

**[AUX] Elementos auxiliares**

Dominio de seguridad
[base] Red corporativa

Clases de activos

**[AUX0001] Fuente de poder**

Dominio de seguridad

[base] Red corporativa

Clases de activos

- [essential] Activos esenciales
- [AUX] Equipamiento auxiliar
  - [AUX.power] fuentes de alimentación

**[AUX0002] Ups**

Dominio de seguridad

[base] Red corporativa

Clases de activos

- [essential] Activos esenciales
- [AUX] Equipamiento auxiliar
  - [AUX. Ups] sai - sistemas de alimentación ininterrumpida

**[AUX0003] Generador eléctrico**

Dominio de seguridad

[base] Red corporativa

Clases de activos

- [essential] Activos esenciales
- [AUX] Equipamiento auxiliar
  - [AUX. Gen] generadores eléctricos

**[AUX0004] Aire acondicionado**

Dominio de seguridad

[base] Red corporativa

Clases de activos

- [essential] Activos esenciales
- [AUX] Equipamiento auxiliar
  - [AUX.ac] equipos de climatización

**[Media0001] CD-ROM**

Dominio de seguridad

[base] Red corporativa

Clases de activos

- [essential] Activos esenciales
- [Media] Soportes de información
  - [Media.electronic] electrónicos
  - [Media.electronic.cd] cederrón (CD-ROM)

**[Media0002] Memoria USB**

Dominio de seguridad

[base] Red corporativa

Clases de activos

- [essential] Activos esenciales
- [Media] Soportes de información
  - [Media.electronic] electrónicos
  - [Media.electronic.usb] memorias USB

**dominio de seguridad: [bps] Conexión a internet**

**[ES0002] Servicio**

Dominio de seguridad

[bps] Conexión a internet

Clases de activos

- [essential] Activos esenciales
  - [essential. Service] servicio
  - [essential. service. operations] operaciones
  - [essential. service. programme] programas
  - [essential. service. Project] proyecto

**[SW0001] BD Mysql**

Dominio de seguridad

[bps] Conexión a internet

Clases de activos

- [essential] Activos esenciales
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.dbms] sistema de gestión de bases de datos

**[SW0005] Servidor www**

Dominio de seguridad

[bps] Conexión a internet

Clases de activos

- [essential] Activos esenciales
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.www] servidor de presentación

**[HW0006] Móden**

Dominio de seguridad

[bps] Conexión a internet

Clases de activos
- [essential] Activos esenciales
- [HW] Equipamiento informático (hardware)
  - [HW. network] soporte de la red
  - [HW. network. modem] módem

**[HW0007] access point**

Dominio de seguridad
[bps] Conexión a internet

Clases de activos
- [essential] Activos esenciales
- [HW] Equipamiento informático (hardware)
  - [HW. network] soporte de la red
  - [HW.network.wap] punto de acceso Wireless

**[COM0001] Red de Datos**

Dominio de seguridad
[bps] Conexión a internet

Clases de activos
- [essential] Activos esenciales
- [COM] Redes de comunicaciones
  - [COM.X25] X25 (red de datos)

**[COM0002] Red Inalámbrica**

Dominio de seguridad
[bps] Conexión a internet

Clases de activos
- [essential] Activos esenciales
- [COM] Redes de comunicaciones
  - [COM.radio] red inalámbrica

**[COM0003] Wifi**

Dominio de seguridad
[bps] Conexión a internet

Clases de activos
- [essential] Activos esenciales
- [COM] Redes de comunicaciones
  - [COM.wifi] WiFi

**[COM0004] Red local**

Dominio de seguridad
[bps] Conexión a internet

Clases de activos
- [essential] Activos esenciales
- [COM] Redes de comunicaciones
  - [COM.LAN] red local

**[COM0005] WAM**

Dominio de seguridad
[bps] Conexión a internet

Clases de activos
- [essential] Activos esenciales

**[COM0006] VPN**

Dominio de seguridad
[bps] Conexión a internet

Clases de activos
- [essential] Activos esenciales
- [COM] Redes de comunicaciones
  - [COM.vpn] canal cifrado (red privada virtual)

**[AUX0005] Fibra óptica**

Dominio de seguridad
[bps] Conexión a internet

Clases de activos
- [essential] Activos esenciales
- [AUX] Equipamiento auxiliar
  - [AUX.cabling] cableado de datos
  - [AUX.cabling. fiber] fibra óptica

**Anexo 5:** *Guía de Observación de los Tipos de Vulnerabilidades en la empresa System Arq S.R.L.*

**GUÍA DE OBSERVACIÓN**

**Datos Generales**

| | |
|---|---|
| **Nombre de la Empresa** | **System Arq S.R.L.** |
| **Nombre del Observador** | **Ángel Jony Huamaní Rubio** |
| **Nombre de Ficha Observada** | **Identificación de vulnerabilidades** |
| **Fecha y hora** | **25/04/23** |

**Objetivo:**

- Determinar las vulnerabilidades en los activos de información

| N° | Tipo de Vulnerabilidades | Frecuencia |
|---|---|---|
| 01 | Repudio (negación de actuaciones) | INTERMEDIO |
| 02 | Avería de origen lógico | ALTO |
| 03 | Difusión de software dañino | ALTO |
| 04 | Vulnerabilidades de los programas (software) | ALTO |
| 05 | Errores de mantenimiento / actualización de programas (software) | ALTO |
| 06 | Manipulación de programas | ALTO |
| 07 | Fuego | INTERMEDIO |
| 08 | Daños por agua | INTERMEDIO |
| 09 | Desastres naturales | INTERMEDIO |
| 10 | Desastres industriales | INTERMEDIO |
| 11 | Contaminación medioambiental | INTERMEDIO |
| 12 | Contaminación electromagnética | INTERMEDIO |
| 13 | Avería de origen físico | ALTO |
| 14 | Corte del suministro eléctrico | INTERMEDIO |
| 15 | Condiciones inadecuadas de temperatura o humedad | ALTO |
| 16 | Emanaciones electromagnéticas (TEMPEST) | INTERMEDIO |
| 17 | Errores de mantenimiento / actualización de equipos | ALTO |
| 18 | Caída del sistema por agotamiento de recursos | ALTO |
| 19 | Pérdida de equipos | INTERMEDIO |

| | | |
|---|---|---|
| 20 | Uso no previsto | INTERMEDIO |
| 21 | Acceso no autorizado | ALTO |
| 22 | Manipulación del hardware | ALTO |
| 23 | Denegación de servicio | INTERMEDIO |
| 24 | Robo de equipos | INTERMEDIO |
| 25 | Ataque destructivo | INTERMEDIO |
| 26 | Fallo de servicios de comunicaciones | ALTO |
| 27 | Errores del administrador del sistema / de la seguridad | ALTO |
| 28 | Errores de [re-]encaminamiento | INTERMEDIO |
| 29 | Errores de secuencia | INTERMEDIO |
| 30 | Alteración de la información | INTERMEDIO |
| 31 | Fugas de información | ALTO |
| 32 | Suplantación de la identidad | ALTO |
| 33 | Uso no previsto | INTERMEDIO |
| 34 | [Re-]encaminamiento de mensajes | INTERMEDIO |
| 35 | Alteración de secuencia | INTERMEDIO |
| 36 | Acceso no autorizado | ALTO |
| 37 | Análisis de tráfico | ALTO |
| 38 | interceptación de información (escucha) | INTERMEDIO |
| 39 | Modificación de la información | ALTO |
| 40 | Destrucción de la información | ALTO |
| 41 | Denegación de servicio | INTERMEDIO |

*Fuente: Elaboración Propia*

**Anexo 6:** *Identificación de controles existentes en la empresa System Arq S.R.L.*

| CONTROLES APLICADOS SEGÚN NORMATIVA ISO 27001:2022 | | | |
|---|---|---|---|
| Clausula | Controles | Si | No |
| **5** | **Controles organizacionales** | | |
| 5.1 | Políticas de seguridad de la información | | **X** |
| 5.2 | Roles de seguridad de la información y Responsabilidades de control | | **X** |
| 5.3 | Segregación de deberes | X | |
| 5.4 | Responsabilidades de la dirección | X | |
| 5.5 | Contacto con autoridades | X | |
| 5.6 | Contacto con grupos de interés especial | X | |
| 5.7 | Inteligencia de amenazas | | X |
| 5.8 | Seguridad de la información en la gestión de proyectos | | X |
| 5.9 | Inventario de la información y otros activos asociados | | X |
| 5.10 | Uso aceptable de la información y otros activos asociados | | X |
| 5.11 | Devolución de activos | X | |
| 5.12 | Clasificación de la información | | X |
| 5.13 | Etiquetado de la información | | **X** |
| 5.14 | Transferencia de información | **X** | |
| 5.15 | Control de acceso | | **X** |
| 5.16 | Gestión de la identidad | | **X** |
| 5.17 | Información de autenticación | **X** | |
| 5.18 | Derechos de acceso | | **X** |
| 5.19 | Seguridad de la información en las relaciones con los proveedores | **X** | |
| 5.20 | Gestión de la seguridad de la información en los acuerdos con los proveedores | **X** | |
| 5.21 | Gestión de la seguridad de la información en la cadena de suministro de las TIC | | **X** |
| 5.22 | Monitoreo, revisión y gestión de cambios de los servicios de los proveedores | **X** | |

| | | | |
|---|---|---|---|
| 5.23 | Seguridad de la información para el uso de servicios en la nube | **X** | |
| 5.24 | Planificación y preparación de la gestión de incidentes de seguridad de la información | | **X** |
| 5.25 | Evaluación y decisión sobre eventos de seguridad de la información | | **X** |
| 5.26 | Respuesta a incidentes de seguridad de la información | | **X** |
| 5.27 | Aprendizaje de los incidentes de seguridad de la información | **X** | |
| 5.28 | Recogida de pruebas | | **X** |
| 5.29 | Seguridad de la información durante la interrupción | | **X** |
| 5.30 | Preparación de las TIC para la continuidad del negocio | **X** | |
| 5.31 | Identificación de los requisitos legales, reglamentarios y contractuales | | **X** |
| 5.32 | Derechos de propiedad intelectual | **X** | |
| 5.33 | Protección de registros | **X** | |
| 5.34 | Privacidad y protección de la información personal | **X** | |
| 5.35 | Revisión independiente de la seguridad de la información | **X** | |
| 5.36 | Cumplimiento de políticas y normas de seguridad de la información | | **X** |
| 5.37 | Procedimientos operativos documentados | **X** | |
| **6** | **Controles de personas** | | |
| 6.1 | Selección de personal | **X** | |
| 6.2 | Términos y condiciones de empleo | **X** | |
| 6.3 | Concienciación, educación y formación en materia de seguridad de la información | | **X** |
| 6.4 | Proceso disciplinario | **X** | |
| 6.5 | Responsabilidades después de la terminación o cambio de empleo | **X** | |
| 6.6 | Acuerdos de confidencialidad o no divulgación | **X** | |
| 6.7 | Trabajo a distancia | **X** | |

| | | | |
|---|---|---|---|
| 6.8 | Reporte de eventos de seguridad de la información | | **X** |
| **7** | **Controles físicos** | | |
| 7.1 | Perímetro de seguridad física | | **X** |
| 7.2 | Controles físicos de entrada | | **X** |
| 7.3 | Seguridad de oficinas, salas e instalaciones | | **X** |
| 7.4 | Supervisión de la seguridad física | | **X** |
| 7.5 | Protección contra amenazas físicas y ambientales | | **X** |
| 7.6 | Trabajar en áreas seguras | **X** | |
| 7.7 | Escritorio y pantalla despejados | **X** | |
| 7.8 | Ubicación y protección de los equipos | | **X** |
| 7.9 | Seguridad de los activos fuera de las instalaciones | | **X** |
| 7.10 | Medios de almacenamiento | **X** | |
| 7.11 | Servicios de apoyo | | **X** |
| 7.12 | Seguridad del cableado | | **X** |
| 7.13 | Mantenimiento de equipos | | **X** |
| 7.14 | Seguridad en la eliminación o reutilización de equipos | **X** | |
| **8** | **Controles tecnológicos** | | |
| 8.1 | Dispositivos de punto final del usuario | **X** | |
| 8.2 | Derechos de acceso con privilegios | | **X** |
| 8.3 | Restricción de acceso a la información | | **X** |
| 8.4 | Acceso al código fuente | **X** | |
| 8.5 | Autenticación segura | | **X** |
| 8.6 | Gestión de la capacidad | **X** | |
| 8.7 | Protección contra el malware | | **X** |
| 8.8 | Gestión de las vulnerabilidades técnicas | | **X** |
| 8.9 | Gestión de la configuración | **X** | |
| 8.10 | Eliminación de información | **X** | |
| 8.11 | Enmascaramiento de datos | | **X** |
| 8.12 | Prevención de la fuga de datos | | **X** |
| 8.13 | Copia de seguridad de la información | | **X** |
| 8.14 | Redundancia de las instalaciones de procesamiento de la información | **X** | |
| 8.15 | Registro de datos | **X** | |

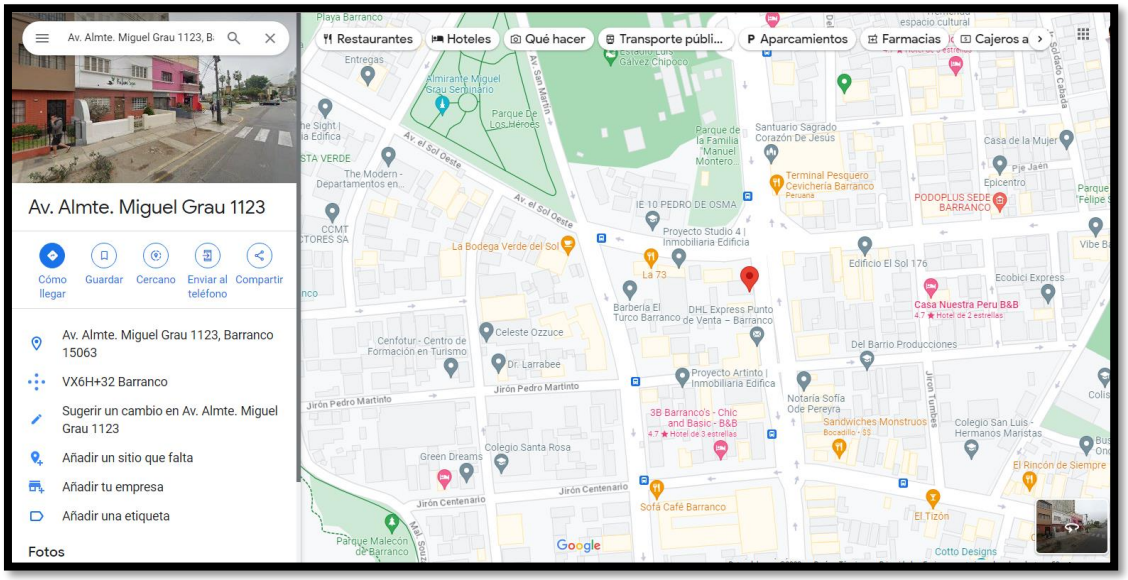
| | | | |
|---|---|---|---|
| 8.16 | Actividades de supervisión | **X** | |
| 8.17 | Sincronización de relojes | **X** | |
| 8.18 | Uso de programas de utilidad privilegiados | | **X** |
| 8.19 | Instalación de software en sistemas operativos | **X** | |
| 8.20 | Controles de red | **X** | |
| 8.21 | Seguridad de los servicios de red | | **X** |
| 8.22 | Filtrado web | | **X** |
| 8.23 | Segregación en redes | **X** | |
| 8.24 | Uso de criptografía | | **X** |
| 8.25 | Ciclo de vida de desarrollo seguro | | **X** |
| 8.26 | Requisitos de seguridad de las aplicaciones | | **X** |
| 8.27 | Arquitectura de sistemas seguros y principios de ingeniería | | **X** |
| 8.28 | Codificación segura | | **X** |
| 8.29 | Pruebas de seguridad en el desarrollo y la aceptación | | **X** |
| 8.30 | Desarrollo externalizado | **X** | |
| 8.31 | Separación de los entornos de desarrollo, prueba y producción | **X** | |
| 8.32 | Gestión del cambio | **X** | |
| 8.33 | Información de pruebas | **X** | |
| 8.34 | Protección de los sistemas de información durante la auditoría y las pruebas | | **X** |

*Fuente: Elaboración Propia*

**Anexo 7:** *Plan estratégico de la empresa System Arq S.R.L*

**Datos de la Empresa**

- Nombre de la Empresa: **System Arq. S.R.L**
- Dirección: **Av. Grau N°1123 – Barranco, Lima.**
- Nombre de Gerente o Representante legal: **David Guillermo Rayter Arnao**
- Nombre persona contacto: **Johnny Pablo Liza Velásquez**
- Cargo Persona de Contacto: **Estudiante Ingeniería de Sistemas**
- Número de Trabajadores: **25**
- Ubicación




**Breve Referencia:** Inició sus actividades el 13 de enero de 1994, brinda el servicio de actividades de arquitectura e ingeniería, consultoría de informática y gestión de instalaciones informáticas, rastreo satelital a vehículos mediante equipos GPS. System Arq. Ha obtenido permisos por el Ministerio de Transportes y Comunicaciones para brindar el servicio de rastreo satelital y comercialización de equipos GPS.

Hoy en día, el servicio principal de la empresa es el rastreo satelital mediante equipos GPS instalados en vehículos, obteniendo como principal función la

posición del vehículo y requerimientos que el cliente desee para mejorar la plataforma.

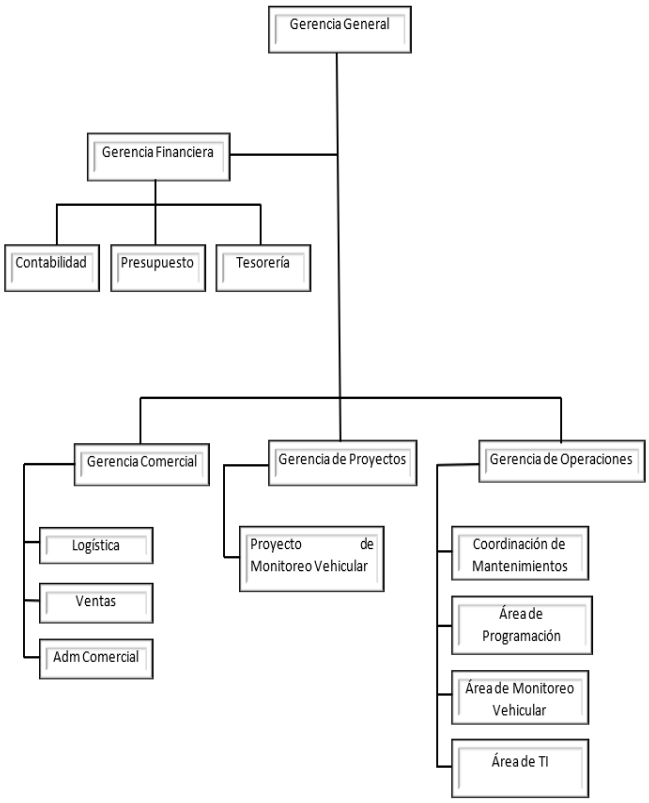
**Misión**

Proveer el servicio de rastreo satelital con equipos GPS a vehículos terrestres, que se desplacen por el territorio peruano, brindando calidad de servicio y a un precio competitivo, incorporándonos con las redes existentes.

**Visión**

Alcanzar a ser una empresa líder en el rubro de rastreo satelital y servicios de valor agregado, ofreciendo a los clientes el mejor servicio y productos para responder a todas las necesidades que requieran para la gestión de telecomunicación

**Organigrama**




*Fuente: Elaboración Propia*

**Anexo 8**: *Acta de compromiso de la alta dirección*

**SYSTEM ARQ SRL.**

**Compromiso de la Alta Dirección para el Sistema de Gestión de Seguridad de la Información (SGSI)**

Nosotros, David Guillermo Rayter Arnao y el equipo de alta dirección de SYSTEM ARQ SRL., reconocemos la importancia de la seguridad de la información para nuestra organización y sus partes interesadas. Entendemos que la gestión efectiva de la seguridad de la información es esencial para proteger la confidencialidad, integridad y disponibilidad de la información y para garantizar la continuidad de nuestras operaciones.

Declaramos nuestro compromiso con la implementación y el mantenimiento de un SGSI conforme a la norma ISO 27001. Para ello, nos comprometemos a:

Proporcionar el liderazgo y los recursos necesarios para el éxito del SGSI.

Establecer un marco de políticas y procedimientos que defina roles, responsabilidades y obligaciones en materia de seguridad de la información.

Asegurar que el SGSI se alinee con los objetivos estratégicos de la organización y que se integre en todos los procesos y funciones.

Proporcionar la capacitación y la concienciación necesarias a todos los empleados y partes interesadas para que entiendan la importancia de la seguridad de la información y cumplan con las políticas y procedimientos establecidos.

Participar en la evaluación de riesgos y en la toma de decisiones relacionadas con la implementación de controles de seguridad de la información.

Realizar revisiones periódicas del SGSI para evaluar su efectividad y tomar medidas correctivas y preventivas cuando sea necesario.

Mantenernos informados sobre las amenazas y vulnerabilidades de seguridad de la información y adaptar el SGSI de acuerdo con las nuevas circunstancias.

Promover una cultura de seguridad de la información en toda la organización.

Este compromiso con la seguridad de la información es esencial para proteger los activos de la organización y para cumplir con nuestras obligaciones legales y contractuales. Reconocemos que la seguridad de la información es un esfuerzo continuo y nos comprometemos a invertir los recursos necesarios para mantener y mejorar constantemente nuestro SGSI.

Firmado por:

David Guillermo Rayter Arnao

Gerente General

Ángel Jony Huamaní Rubio

Asistente

Johnny Pablo Liza Velasquez

Asistente

Fecha: 20/04/23

**Anexo 9:** *Ficha de registro – Pre test del indicador porcentaje de ataques malware*

| Ficha de Registro | | | |
|---|---|---|---|
| Investigador | Huamaní Rubio Ángel Jony | Tipo de prueba: | Pre Test |
| Empresa | System Arq S.R.L. | | |
| Variable | Ataques Cibernéticos | | |
| Dimensión | Ataques malware | | |
| Periodo | 01-Mayo-2023 hasta 30-Mayo-2023 | | |

| Indicador | Descripción | Técnica | Unidad de Medida | Fórmula |
|---|---|---|---|---|
| Porcentaje de ataques malware | Es la cantidad de acciones maliciosas que comprometen la seguridad de los sistemas informáticos | FICHAJE | % | {(CME-CMS)/CME)*100<br>CME= Cantidad de malware encontrados<br>CMS= Cantidad de malware suprimidos |

| Item | Fecha | Cod. De activos de información | Cantidad de malware encontrados | Cantidad de malware suprimidos | PORCENTAJE DE ATAQUES MALWARE DETECTADAS |
|---|---|---|---|---|---|
| 1 | 1-May-23 | [ES0001] | 18 | 3 | 83,33 |
| 2 | 2-May-23 | [ES0002] | 7 | 3 | 57,14 |
| 3 | 3-May-23 | [ES0003] | 4 | 2 | 50,00 |
| 4 | 4-May-23 | [SW0001] | 8 | 2 | 75,00 |
| 5 | 5-May-23 | [SW0002] | 10 | 3 | 70,00 |
| 6 | 6-May-23 | [SW0003] | 5 | 2 | 60,00 |
| 7 | 7-May-23 | [SW0004] | 8 | 3 | 62,50 |
| 8 | 8-May-23 | [SW0005] | 7 | 3 | 57,14 |
| 9 | 9-May-23 | [SW0006] | 5 | 3 | 40,00 |
| 10 | 10-May-23 | [SW0007] | 9 | 4 | 55,56 |
| 11 | 11-May-23 | [HW0001] | 10 | 3 | 70,00 |
| 12 | 12-May-23 | [HW0002] | 8 | 2 | 75,00 |
| 13 | 13-May-23 | [HW0003] | 9 | 3 | 66,67 |
| 14 | 14-May-23 | [HW0004] | 6 | 2 | 66,67 |
| 15 | 15-May-23 | [HW0005] | 12 | 4 | 66,67 |
| 16 | 16-May-23 | [HW0006] | 10 | 2 | 80,00 |
| 17 | 17-May-23 | [HW0007] | 8 | 4 | 50,00 |
| 18 | 18-May-23 | [COM0001] | 6 | 4 | 33,33 |
| 19 | 19-May-23 | [COM0002] | 11 | 4 | 63,64 |
| 20 | 20-May-23 | [COM0003] | 12 | 3 | 75,00 |
| 21 | 21-May-23 | [COM0004] | 9 | 2 | 77,78 |
| 22 | 22-May-23 | [COM0005] | 12 | 4 | 66,67 |
| 23 | 23-May-23 | [COM0006] | 9 | 3 | 66,67 |
| 24 | 24-May-23 | [AUX0001] | 10 | 3 | 70,00 |
| 25 | 25-May-23 | [AUX0002] | 8 | 3 | 62,50 |
| 26 | 26-May-23 | [AUX0003] | 11 | 2 | 81,82 |
| 27 | 27-May-23 | [AUX0004] | 11 | 4 | 63,64 |
| 28 | 28-May-23 | [AUX0005] | 15 | 4 | 73,33 |
| 29 | 29-May-23 | [Media0001] | 9 | 3 | 66,67 |
| 30 | 30-May-23 | [Media0002] | 13 | 4 | 69,23 |

Firma y sello

**Anexo 10:** *Ficha de registro – Post test del indicador porcentaje de ataques malware*

| Ficha de Registro | | | |
|---|---|---|---|
| Investigador | Huamaní Rubio Ángel Jony | Tipo de prueba: | PosTest |
| Empresa | System Arq S.R.L. | | |
| Variable | Ataques Cibernéticos | | |
| Dimensión | Ataques malware | | |
| Periodo | 01-Octubre-2023 hasta 30-Octubre-2023 | | |

| Indicador | Descripción | Técnica | Unidad de Medida | Fórmula |
|---|---|---|---|---|
| Porcentaje de ataques malware | Es la cantidad de acciones maliciosas que comprometen la seguridad de los sistemas informáticos | FICHAJE | % | ((CME-CMS)/CME)*100<br>CME= Cantidad de malware encontrados<br>CMS= Cantidad de malware suprimidos |

| Item | Fecha | Cod. De activos de información | Cantidad de malware encontrados | Cantidad de malware suprimidos | PORCENTAJE DE ATAQUES MALWARE DETECTADAS |
|---|---|---|---|---|---|
| 1 | 1-Oct-23 | [ES0001] | 12 | 7 | 41,67 |
| 2 | 2-Oct-23 | [ES0002] | 8 | 6 | 25,00 |
| 3 | 3-Oct-23 | [ES0003] | 6 | 4 | 33,33 |
| 4 | 4-Oct-23 | [SW0001] | 7 | 5 | 28,57 |
| 5 | 5-Oct-23 | [SW0002] | 8 | 6 | 31,25 |
| 6 | 6-Oct-23 | [SW0003] | 6 | 4 | 33,33 |
| 7 | 7-Oct-23 | [SW0004] | 8 | 5 | 37,50 |
| 8 | 8-Oct-23 | [SW0005] | 9 | 5 | 44,44 |
| 9 | 9-Oct-23 | [SW0006] | 6 | 4 | 33,33 |
| 10 | 10-Oct-23 | [SW0007] | 5 | 4 | 20,00 |
| 11 | 11-Oct-23 | [HW0001] | 11 | 6 | 45,45 |
| 12 | 12-Oct-23 | [HW0002] | 9 | 5 | 44,44 |
| 13 | 13-Oct-23 | [HW0003] | 9 | 6 | 38,89 |
| 14 | 14-Oct-23 | [HW0004] | 7 | 4 | 42,86 |
| 15 | 15-Oct-23 | [HW0005] | 10 | 5 | 50,00 |
| 16 | 16-Oct-23 | [HW0006] | 9 | 6 | 35,56 |
| 17 | 17-Oct-23 | [HW0007] | 7 | 6 | 14,29 |
| 18 | 18-Oct-23 | [COM0001] | 7 | 5 | 28,57 |
| 19 | 19-Oct-23 | [COM0002] | 9 | 6 | 33,33 |
| 20 | 20-Oct-23 | [COM0003] | 12 | 7 | 41,67 |
| 21 | 21-Oct-23 | [COM0004] | 8 | 5 | 41,25 |
| 22 | 22-Oct-23 | [COM0005] | 11 | 6 | 45,45 |
| 23 | 23-Oct-23 | [COM0006] | 7 | 6 | 14,29 |
| 24 | 24-Oct-23 | [AUX0001] | 12 | 7 | 41,67 |
| 25 | 25-Oct-23 | [AUX0002] | 8 | 7 | 12,50 |
| 26 | 26-Oct-23 | [AUX0003] | 10 | 5 | 53,00 |
| 27 | 27-Oct-23 | [AUX0004] | 9 | 6 | 33,33 |
| 28 | 28-Oct-23 | [AUX0005] | 11 | 7 | 36,36 |
| 29 | 29-Oct-23 | [Media0001] | 8 | 7 | 12,50 |
| 30 | 30-Oct-23 | [Media0002] | 11 | 7 | 36,36 |

Firma y sello

**Anexo 11:** *Ficha de registro – Pre test del indicador porcentaje de vulnerabilidades en los activos de información*

| Ficha de Registro | | | |
|---|---|---|---|
| Investigador | Liza Velásquez Johnny Pablo | Tipo de prueba: | Pre Test |
| Empresa | System Arq S.R.L. | | |
| Variable | Ataques Cibernéticos | | |
| Dimensión | Vulnerabilidad en los activos de información | | |
| Periodo | 01-Mayo-2023 hasta 30-Mayo-2023 | | |

| Indicador | Descripción | Técnica | Unidad de Medida | Fórmula |
|---|---|---|---|---|
| Porcentaje de vulnerabilidades en los activos de información | porcentaje de debilidades o fallas de seguridad identificadas en los recursos de información | FICHAJE | % | ((CVI-CVC)/CVI) *100<br>CVI= Cantidad vulnerabilidades identificadas<br>CVC= Cantidad de vulnerabilidades corregidas |

| Item | Fecha | Cod. De activos de información | Cantidad de vulnerabilidades identificadas | Cantidad de vulnerabilidades corregidas | PORCENTAJE DE VULNERABILIDADES DETECTADAS |
|---|---|---|---|---|---|
| 1 | 1-May-23 | [ES0001] | 19 | 10 | 47,37 |
| 2 | 2-May-23 | [ES0002] | 32 | 17 | 46,88 |
| 3 | 3-May-23 | [ES0003] | 23 | 12 | 47,83 |
| 4 | 4-May-23 | [SW0001] | 30 | 14 | 53,33 |
| 5 | 5-May-23 | [SW0002] | 22 | 12 | 45,45 |
| 6 | 6-May-23 | [SW0003] | 31 | 18 | 41,94 |
| 7 | 7-May-23 | [SW0004] | 45 | 26 | 42,22 |
| 8 | 8-May-23 | [SW0005] | 32 | 18 | 43,75 |
| 9 | 9-May-23 | [SW0006] | 29 | 17 | 41,38 |
| 10 | 10-May-23 | [SW0007] | 33 | 19 | 42,42 |
| 11 | 11-May-23 | [HW0001] | 38 | 18 | 52,63 |
| 12 | 12-May-23 | [HW0002] | 34 | 18 | 47,06 |
| 13 | 13-May-23 | [HW0003] | 23 | 12 | 47,83 |
| 14 | 14-May-23 | [HW0004] | 29 | 16 | 44,83 |
| 15 | 15-May-23 | [HW0005] | 20 | 11 | 45,00 |
| 16 | 16-May-23 | [HW0006] | 25 | 12 | 52,00 |
| 17 | 17-May-23 | [HW0007] | 32 | 17 | 46,88 |
| 18 | 18-May-23 | [COM0001] | 31 | 16 | 48,39 |
| 19 | 19-May-23 | [COM0002] | 30 | 16 | 46,67 |
| 20 | 20-May-23 | [COM0003] | 28 | 15 | 46,43 |
| 21 | 21-May-23 | [COM0004] | 32 | 18 | 43,75 |
| 22 | 22-May-23 | [COM0005] | 34 | 18 | 47,06 |
| 23 | 23-May-23 | [COM0006] | 34 | 17 | 50,00 |
| 24 | 24-May-23 | [AUX0001] | 29 | 16 | 44,83 |
| 25 | 25-May-23 | [AUX0002] | 26 | 14 | 46,15 |
| 26 | 26-May-23 | [AUX0003] | 33 | 16 | 51,52 |
| 27 | 27-May-23 | [AUX0004] | 23 | 12 | 47,83 |
| 28 | 28-May-23 | [AUX0005] | 33 | 18 | 45,45 |
| 29 | 29-May-23 | [Media0001] | 39 | 19 | 51,28 |
| 30 | 30-May-23 | [Media0002] | 39 | 21 | 46,15 |

Firma y sello

**Anexo 12:** *Ficha de registro – Post test del indicador porcentaje de vulnerabilidades en los activos de información*

| Ficha de Registro | | | |
|---|---|---|---|
| Investigador | Liza Velásquez Johnny Pablo | Tipo de prueba: | PosTest |
| Empresa | System Arq S.R.L. | | |
| Variable | Ataques Cibernéticos | | |
| Dimensión | Vulnerabilidad en los activos de información | | |
| Periodo | 01-Octubre-2023 hasta 30-Octubre-2023 | | |

| Indicador | Descripción | Técnica | Unidad de Medida | Fórmula |
|---|---|---|---|---|
| Porcentaje de vulnerabilidades en los activos de información | porcentaje de debilidades o fallas de seguridad identificadas en los recursos de información | FICHAJE | % | ((CVI-CVC)/CVI) *100<br>CVI= Cantidad vulnerabilidades identificadas<br>CVC= Cantidad de vulnerabilidades corregidas |

| Item | Fecha | Cod. De activos de información | Cantidad de vulnerabilidades identificadas | Cantidad de vulnerabilidades corregidas | PORCENTAJE DE VULNERABILIDADES DETECTADAS |
|---|---|---|---|---|---|
| 1 | 1-Oct-23 | [ES0001] | 19 | 15 | 21,05 |
| 2 | 2-Oct-23 | [ES0002] | 32 | 26 | 18,75 |
| 3 | 3-Oct-23 | [ES0003] | 23 | 19 | 17,39 |
| 4 | 4-Oct-23 | [SW0001] | 30 | 26 | 13,33 |
| 5 | 5-Oct-23 | [SW0002] | 22 | 19 | 13,64 |
| 6 | 6-Oct-23 | [SW0003] | 31 | 26 | 16,13 |
| 7 | 7-Oct-23 | [SW0004] | 45 | 38 | 15,56 |
| 8 | 8-Oct-23 | [SW0005] | 32 | 28 | 12,50 |
| 9 | 9-Oct-23 | [SW0006] | 29 | 24 | 17,24 |
| 10 | 10-Oct-23 | [SW0007] | 33 | 27 | 18,18 |
| 11 | 11-Oct-23 | [HW0001] | 38 | 31 | 18,42 |
| 12 | 12-Oct-23 | [HW0002] | 34 | 28 | 17,65 |
| 13 | 13-Oct-23 | [HW0003] | 23 | 18 | 21,74 |
| 14 | 14-Oct-23 | [HW0004] | 29 | 22 | 24,14 |
| 15 | 15-Oct-23 | [HW0005] | 20 | 16 | 20,00 |
| 16 | 16-Oct-23 | [HW0006] | 25 | 19 | 24,00 |
| 17 | 17-Oct-23 | [HW0007] | 32 | 27 | 15,63 |
| 18 | 18-Oct-23 | [COM0001] | 31 | 25 | 19,35 |
| 19 | 19-Oct-23 | [COM0002] | 30 | 25 | 16,67 |
| 20 | 20-Oct-23 | [COM0003] | 28 | 23 | 17,86 |
| 21 | 21-Oct-23 | [COM0004] | 32 | 26 | 18,75 |
| 22 | 22-Oct-23 | [COM0005] | 34 | 28 | 17,65 |
| 23 | 23-Oct-23 | [COM0006] | 34 | 27 | 20,59 |
| 24 | 24-Oct-23 | [AUX0001] | 29 | 23 | 20,69 |
| 25 | 25-Oct-23 | [AUX0002] | 26 | 22 | 15,38 |
| 26 | 26-Oct-23 | [AUX0003] | 33 | 27 | 18,18 |
| 27 | 27-Oct-23 | [AUX0004] | 23 | 18 | 21,74 |
| 28 | 28-Oct-23 | [AUX0005] | 33 | 27 | 18,18 |
| 29 | 29-Oct-23 | [Media0001] | 39 | 33 | 15,38 |
| 30 | 30-Oct-23 | [Media0002] | 39 | 32 | 17,95 |

Firma y sello

**Anexo 13**: *Proyect Chárter (1)*

## INICIO DEL PROYECTO

El **07 de abril de 2023** se dio inicio al proyecto de implementación del SGSI basada en la ISO/IEC 27001:2022, para reducir el riesgo ante ataques cibernéticos en la Empresa System Arq S.R.L, para lo cual se elaboró y aprobó el siguiente Project Chárter.

| ACTA DE CONSTITUCIÓN DEL PROYECTO | |
|---|---|
| **INFORMACIÓN GENERAL** | |
| NOMBRE DEL PROYECTO | SIGLAS DEL PROYECTO |
| IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD BASADA EN LA ISO/IEC 27001:2022 | SGSI |

**DESCRIPCIÓN DEL PROYECTO**

El proyecto: La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001.2022 es un proceso integral que ayuda a la organización a establecer un sistema de gestión efectivo para reducir los riesgos de ataques cibernéticos y proteger la confidencialidad, integridad y disponibilidad de la información.

La implementación consiste en las siguientes etapas:

1. Compromiso de la dirección
2. Establecer un equipo de proyecto
3. Alcance y objetivos
4. Evaluación de riesgos
5. Planificación
6. Implementación de controles
7. Capacitación y concientización
8. Monitoreo y medición
9. Revisión por la dirección
10. Mejora continua
11. Certificación (opcional)

**Equipo de Trabajo:**

- Liza Velásquez, Johnny Pablo --> Líder del Proyecto
- Rayter Arnao, David Guillermo --> Gerente General
- Huamani Rubio, Ángel Jony --> Asistente

El proyecto será realizado desde el 06 de abril de 2023 al 09 de diciembre de 2023.

**DEFINICION DEL PRODUCTO DEL PROYECTO**

Implementación de un Sistema de Gestión de Seguridad de la información, basada en la ISO/IEC 27001:2022 para reducir el riesgo ante ataques cibernéticos en la Empresa System Arq S.R.L, Lima 2023

**DEFINICIÓN DE REQUISITOS DEL PROYECTO**

**Anexo 14:** *Proyect Chárter (2)*

- Se entregará un informe del avance mensual del proyecto.
- Entregar un documento final con los resultados obtenidos post implementación.

| CONCEPTO | OBJETIVOS | CRITERIO DE ÉXITO |
|---|---|---|
| 1. ALCANCE | Cumplir con la elaboración de los siguientes entregables: alcance del SGSI, Metodología de riesgos, Política y objetivos de SI, y toda la documentación que evidencie el cumplimiento del SGSI | Aprobación de todos los documentos |
| 2. TIEMPO | Cumplir el proyecto en los plazos establecidos | Seguimiento del cronograma del proyecto. |
| 3. COSTO | Cumplir con el presupuesto estimado del proyecto | No exceder del presupuesto |

Contribuir al conocimiento actual acerca de la utilización de la norma ISO 27001 como técnica de protección ante ataques cibernéticos, cuyas conclusiones podrán sistematizarse en una propuesta, para ser incorporado en los sistemas de seguridad, ya que se estaría demostrando que el uso de la norma mejora el nivel de protección de la seguridad informática.

JUSTIFICACIÓN DEL PROYECTO

| JUSTIFICACIÓN PRACTICA | JUSTIFICACIÓN METODOLOGICA |
|---|---|
| Radica en la importancia de implementar un sistema de gestión de seguridad basado en la ISO 27001, el cual permitirá reducir el riesgo ante las amenazas cibernéticas sin tener que invertir fuertes cantidades de dinero en mantener la información a buen recaudo o crear una planilla excesivamente grande. | Posibilita el fortalecimiento de la auditoría de los controles mediante la utilización de técnicas y ejercicios aplicados con determinadas metodologías para el tratamiento de riesgos, mediante la aplicación de las mejores prácticas establecidas en la norma ISO 27001, que evidencian su efectividad y confiabilidad. |

DESIGNACIÓN DEL PROJECT MANAGER DEL PROYECTO

| NOMBRE | Liza Velásquez, Johnny Pablo | NIVELES DE AUTORIDAD |
|---|---|---|

**Anexo 15**: *Proyect Chárter (3)*

| | | |
|---|---|---|
| REPORTA A | Rayter Arnao, David Guillermo | Exigir el cumplimiento de los entregables del proyecto |
| SUPERVISA A | Huamani Rubio, Angel Jony | |

| HITO O EVENTO SIGNIFICATIVO | FECHA PROGRAMADA |
|---|---|
| Inicio del Proyecto | 06 de Abril 2023 |
| Compromiso de la dirección | 20 de Abril 2023 |
| Establecer un equipo de proyecto | 21 de Abril 2023 |
| Alcance y objetivos | 23 de Abril 2023 |
| Evaluación de riesgos | 03 de Mayo 2023 |
| Planificación | 01 de Julio 2023 |
| Implementación de controles | 03 de Setiembre 2023 |
| Capacitación y concientización | 01 de Octubre 2023 |
| Monitoreo y medición | 15 de Octubre 2023 |
| Revisión por la dirección | 01 de Noviembre 2023 |
| Mejora continua | 15 de Noviembre 2023 |
| Fin del Proyecto | 09 de Diciembre 2023 |

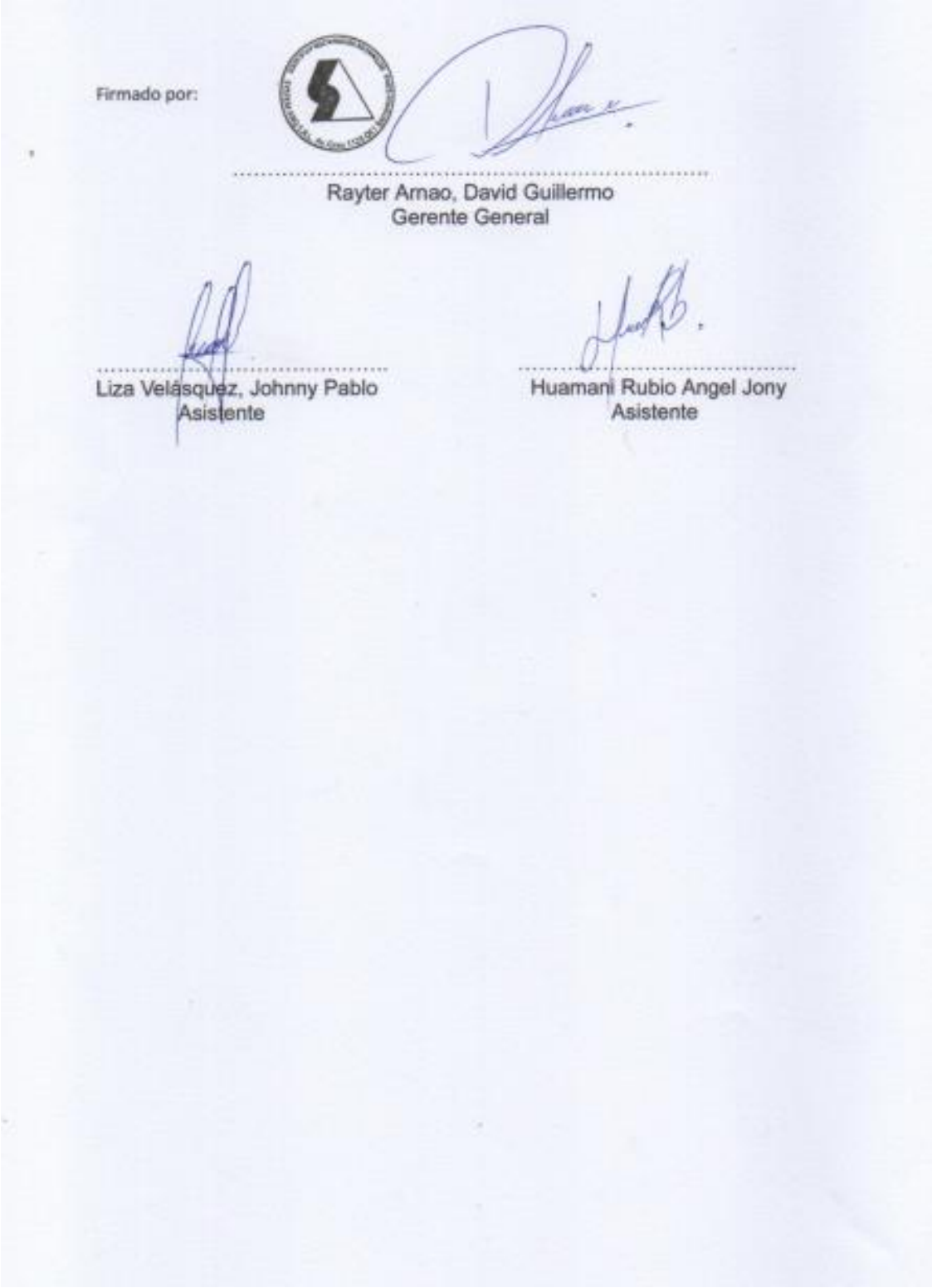
- Tiempo insuficiente para consolidar los controles y almacenar evidencias asociadas al SGSI.
- Nueva versión de la norma
- No aprobación de los documentos generados a raíz del proyecto
- No cumplimiento en el tiempo establecido de actividades o documentos del cronograma del proyecto

La implementación del SGSI permite identificar la eficacia de los controles y tecnología utilizada en el presente proyecto.

| NOMBRE | EMPRESA | CARGO | FECHA |
|---|---|---|---|
| Rayter Arnao, David Guillermo | System Arq. S.R.L. | Gerente General | 20 de abril 2023 |

Fuente: Elaboración propia

**Anexo 16:** *Proyect Chárter (4)*



Firmado por:

Rayter Arnao, David Guillermo
Gerente General

Liza Velásquez, Johnny Pablo
Asistente

Huamani Rubio Angel Jony
Asistente

UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE INGENIERÍA Y ARQUITECTURA**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

# Declaratoria de Autenticidad del Asesor

Yo, GALVEZ TAPIA ORLEANS MOISES, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, asesor de Tesis titulada: "Implementación de un Sistema de Gestión de Seguridad basada en la ISO 27001 para reducir el riesgo ante ataques cibernéticos en la Empresa System Arq S.R.L, Lima 2023", cuyos autores son HUAMANI RUBIO ANGEL JONY, LIZA VELÁSQUEZ JOHNNY PABLO, constato que la investigación tiene un índice de similitud de 18.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 14 de Diciembre del 2023

| **Apellidos y Nombres del Asesor:** | **Firma** |
|---|---|
| GALVEZ TAPIA ORLEANS MOISES<br>**DNI:** 16798332<br>**ORCID:** 0000-0002-4352-9495 | Firmado electrónicamente por: GORLEANSM el 14-12-2023 14:29:46 |

Código documento Trilce: TRI - 0696725

INVESTIGA UCV