FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA ACADÉMICA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Sistema de gestión alineado a la norma ISO/IEC 27001:2013 para la seguridad de la información en una institución financiera, Chachapoyas-Amazonas, 2021.

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

AUTOR:

Br. Aguinaga Quispe, William (ORCID: 0000-0002-1371-8359)

ASESORA:

Mgtr. Acuña Meléndez, M. Eudelia ((ORCID: 0000-0002-5188-3806)

LÍNEA DE INVESTIGACIÓN:

Autoría de Sistemas y seguridad de la Información

LIMA – PERÚ

2021

DEDICATORIA

A mi madre, por su afecto y confianza, pues ella estuvo en el momento más decisivo de mi vida, acompañándome en cada paso para ser un profesional de bien ante la sociedad.

AGRADECIMIENTO

Al Programa Nacional de Becas y créditos educativos (PRONABEC), por brindarme el apoyo económico en toda mi etapa universitaria y abrirme las puertas a un mundo con más oportunidades para servir a mi Perú.

De igual manera va un profundo y sincero agradecimiento a la Universidad Cesar Vallejo, por permitirme cristalizar este gran sueño en su prestigiosa casa de estudios.

íNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente estudio que fue desarrollado en el primer semestre del año 2021 nace en respuesta a las vulnerabilidades existentes en el proceso tecnológico crediticio donde el factor humano se aprovecha para atentar en contra del nivel de producción y por ende causar un impacto negativo en la rentabilidad de una institución financiera. También la investigación tiene como finalidad la creación de un sistema de gestión alineado en la ISO/IEC 27001:2013 para determinar la influencia en la seguridad de la información en una institución financiera. Para tal éxito se utilizó la metodología cuantitativa aplicada, bajo el enfoque de investigación experimental con tipo preexperimental. De igual forma se conformó la muestra de 24 registros en cada indicador. Para luego obtener un resultado favorable en la confidencialidad de la información de un 75.52% al 87.36%, para la integridad de la información se observó un rendimiento del 50.83% al 76.32% y a favor de la disponibilidad de la información se logró un ascenso considerable del 96.81 al 99.93%.

Finalmente, se afirma que el sistema de gestión alineado en la ISO/IEC 27001:2013 influye significativamente en la seguridad de la información en una institución financiera.

Palabras clave: Sistema de gestión, seguridad de la información, ISO/IEC 27001:2013, confidencialidad, integridad, disponibilidad.

ABSTRACT

This study, which was developed in the first semester of 2021, was born in response to the existing vulnerabilities in the technological credit process where the human factor is used to undermine the level of production and therefore causes a negative impact on the profitability of a financial institution. The research also aims to create a management system based on ISO / IEC 27001: 2013 to determine the influence on information security in a financial institution. For such success, the applied quantitative methodology was used, under the experimental research approach with a pre-experimental type. In the same way, the sample of 24 records was made up for each indicator. In order to later obtain a favorable result in the confidentiality of the information from 75.52% to 87.36%, for the integrity of the information a performance of 50.83% to 76.32% was observed and in favor of the availability of the information, a considerable rise was achieved in the 96.81 to 99.93%.

Finally, it is stated that the management system based on ISO / IEC 27001: 2013 significantly influences information security in a financial institution.

Keywords: Management system, information security, ISO / IEC 27001: 2013, confidentiality, integrity, availability.

I. INTRODUCCIÓN

A nivel mundial los procesos de negocio han sido automatizados, situación que ha conllevado a entrar en una lucha constante por salvaguardar la información como activo principal de una organización. Los factores que atentan a su seguridad son técnicos (Softwares y equipos obsoletos, redes vulnerables, ataques informáticos, virus, etc.) y organizacionales (empleados, directivos, gerentes).

Según (Figueroa; Rodriguez & Otros, 2017), refieren que las amenazas que se suscitan son debido a que el propio usuario no es consciente de las vulnerabilidades que existen producto del mal uso del sistema, ya sea en la descarga de archivos y programas maliciosos o la eliminación de archivos valiosos del sistema. Para tal efecto existes buenas prácticas de seguridad que son diversas y muchas consisten en restringir el acceso parcial o total al sistema. Ya que el acceso debe ser permitido solo a personas debidamente acreditadas.

Como sucedió: En Filipinas: “sustracción de 81 millones al Banco Central de Bangladés, Hong Kong: sustracción de 64 millones en Bitcoins a Bitfinex, México: se divulgó información personal de 93 millones de mexicanos, sustracción de 1000 millones de cuentas Yahoo, Ataque de denegación de servicio (DDoS) a Play Station y Twitter, sustracción de 400 millones de cuentas a Friend Finder Network Inc, fallo en la implementación de la pila TCP en sistemas Linux y el fallo en los procesadores Qualcomm”. (GruopoED, 2017).

De acuerdo con (Suaréz, 2015) afirma que actualmente las organizaciones junto a sus sistemas de información cada vez más están frente a riesgos informáticos que surgen de una gran variedad de fuentes, tales como: fraudes informáticos, sabotaje, espionaje y sumado a esto daños producidos por virus de negación de servicios que cada vez van en un aumento en las organizaciones.

Según (Ramirez, 2019), manifiesta que una de las actividades de quienes trabajan en el ámbito del comercio exterior, es salvaguardar la información sensible dentro de sistema aduanero ecuatoriano, más cuando se trata de información confidencial, resulta muy sensible a nivel operativo para las

transacciones comerciales. Pero suceden casos en que dicha información es filtrada hacia terceras personas.

En el ámbito nacional, según (Calderon & Hoyos, 2016), describe que, la ausencia de procesos, controles y normativas en el orden de la información que permita aplicar los niveles de accesos para su comunicación y transmisión, impacta negativamente en la seguridad de la información lo que resulta insegura al momento de ser tomada en cuenta para las decisiones estratégicas de los negocios.

(América Sistemas, 2016). Publica: “Se aprueba el uso de la NTP ISO/IEC 27001:2014 sobre Sistemas de Gestión de Seguridad de la Información en el Estado”, pese al trabajo del ONGEI por brindar asistencia a las entidades públicas, hay también empresas que desconocen el valor real que merece la información y el impacto directo que causa en las metas de negocios.

El ámbito de esta investigación alcanza a una entidad financiera donde existen relaciones jerárquicas, situación que influye en la gestión de la seguridad de la información. Pese a que se encuentran estándares como la ISO 27001:2013, las metodologías que se manejan, no son las calificadas para el nivel de infraestructura de tecnologías de la información o simplemente desconocen de herramientas que sean adaptables o peor aún implementarlas acarrea enormes gastos para el tipo de instituciones financieras.

Ante esta realidad, nace la propuesta para mejorar el grado de seguridad en la información de una entidad financiera, mediante metodologías y estándares como la ISO/IE:27001: 2013, enfocada a preservar en la información su seguridad, disponibilidad e integridad de forma más eficiente.

Lo que conlleva a formularnos el siguiente problema: ¿De qué manera un sistema de gestión alineado a la norma ISO/IEC 27001: 2013; influye en la seguridad de la información en una institución financiera? A continuación, se formulan los problemas específicos:

¿De qué manera un sistema de gestión alineado en la norma ISO/IEC 27001:2013 asegurará la confidencialidad de la información en una institución financiera?, ¿De qué manera un sistema de gestión alineado a la norma ISO/IEC

27001:2013 asegurará la integridad de la información en una institución? y ¿De qué manera un sistema de gestión basado en la norma ISO/IEC 27001:2013 asegurará la disponibilidad de la información en una institución financiera?

En seguida, se describió la justificación metodológica puesto que, a partir del - Modelo Deming, se logrará una cultura óptima en la parte organizacional respecto a temas de seguridad de la información. La justificación práctica se basa en la ISO/IEC: 27001, ya que posee los aspectos básicos y es un estándar en el cual se certifica un sistema de gestión de seguridad de la información. Por ende, se asegurará el avance de sus operaciones y negocios de la institución.

Por tanto, se expresó el objetivo general: Determinar la influencia del sistema de gestión alineado a la Norma ISO/IEC 27001:2013 en la seguridad de la información en una institución financiera.

Además, se obtuvo los siguientes objetivos específicos: Determinar la influencia del sistema de gestión alineado a la Norma ISO/IEC 27001:2013, en la confidencialidad de la información en una institución financiera. Determinar la influencia del sistema de gestión alineado a la Norma ISO/IEC 27001:2013, en la integridad de la información en una institución financiera y Determinar la influencia del sistema de gestión alineado a la Norma ISO/IEC 27001:2013, en la disponibilidad de la información en una institución financiera.

Se planteó la siguiente hipótesis, un sistema de gestión alineado a la Norma ISO/IEC 27001:2013, influye significativamente en la seguridad de la información en una institución financiera. También se listaron las siguientes hipótesis específicas:

Un sistema de gestión alineado en la Norma ISO/IEC 27001:2013, influye significativamente en la confidencialidad de la seguridad de la información en una institución financiera. Un sistema de gestión alineado a la Norma ISO/IEC 27001:2013, influye significativamente en la integridad de la seguridad de la información en una institución financiera. Y un sistema de gestión alineado a la Norma ISO/IEC 27001:2013, influye significativamente en la disponibilidad de la seguridad de la información en una institución financiera.

II. MARCO TEÓRICO

En el antecedente a nivel internacional, cuyos autores (SamPedro, Machuca & Otros, 2019), con el objetivo de obtener una percepción global acerca de las medianas y pequeñas empresas en Santo Domingo respecto a la seguridad de la información. Basado en una metodología con alcance exploratorio, descriptivo y cualicuantitativo aplicado a 106 empresas, cuyos resultados arrojaron que más del 50% de las Pymes ha evaluado el riesgo mediante políticas de seguridad de la información.

Continuando con la investigación de los autores (Rodríguez, Cruzado & Otros, 2020). Cuyo objetivo de su investigación fue analizar la influencia de la aplicación ISO 27001 en una empresa privada respecto a la seguridad de la información. Llevaron un estudio en cuya metodología cuantitativa, se empleó un estudio preexperimental. Para lo cual consideraron una muestra de 30 colaboradores, llegando a una conclusión cuantitativa donde se evidenció la influencia de la aplicación de la ISO en sus tres dimensiones: confidencialidad, integridad y disponibilidad de la información.

En la siguiente investigación de (Moreyra, 2019), consideró como objetivo la elaboración del plan de Gestión para la Seguridad de la Información y apoyándose de la metodología ANFEM (metodología de Análisis Modal de Fallos y Efectos), la misma que le permitió identificar los puntos críticos en las que se pueden producir errores, analizar sus causas por las que fueron provocadas y las consecuencias que tendrían en la seguridad el proceso, así como también fijar medidas de control para mitigarlos. Frente a ello pudo verificar que la organización perecía de procedimientos formales y guías para una buena gestión de la seguridad de la información, por ende, el mayor riesgo que existe radica en el mal uso de los activos por parte del personal interno frente a las amenazas externas.

Siguiendo con la investigación de los (Valencia y Orozco, 2017), Con la finalidad de presentar una metodología para implementar el sistema de gestión de seguridad de la información, tomando de referente a la ISO/IEC 270003:2010; la cual contiene una guía de especificaciones y diseño de un sistema de gestión de

seguridad de la información; llevó a cabo el desarrollo de su investigación. Dando por hecho un aporte metodológico a seguir al momento de implementar un SGSI en las organizaciones y cumplir con las distintas regulaciones que existen en la actualidad.

Del mismo modo la investigación de los autores (Mayorga y Zapata, 2020), con el objetivo de implementar un Sistema de Gestión de Seguridad de la Información basado en las Normas de la ISO/IEC 27001, aplicaron la metodología de investigación, análisis y resultado para su posterior análisis de la información obtenida en el área de TI. Llegándose a concluir que, dentro de las políticas definidas para los usuarios en paralelo, también es necesario aplicarlas a los sistemas de información para que relacionadas entre sí hagan frente a las múltiples vulnerabilidades y amenazas a los que se exponen los distintos activos organizacionales.

Y por último la investigación de los autores (Ramos & Urrutia, 2017), con el propósito de implementar políticas de seguridad de la información teniendo en cuenta la norma 27002:2013 en la cooperativa CODELCAUCA. Se aplicaron los controles 5.1 y 5.2 relacionada a políticas de seguridad y objetivos de la empresa, con una muestra de 23 personas incluyendo al jefe de sistemas y personal de las diferentes áreas, cuyos resultados demostraron que el 46.8% del personal conoce de seguridad de la información frente al 45.5% de ignorancia.

Se menciona el antecedente nacional, cuyo autor (Jordan, 2018), con el propósito de desarrollar el Sistema de Gestión de seguridad de la Información alineada a la Norma ISO 27001 en la Financiera Crediscotia en el área de operaciones, alineó su metodología en la guía con los fundamentos de la dirección de proyectos (PMBOK), cuyos resultados obtenidos a partir de las entrevistas realizadas al personal de operación y jefe de seguridad de la información, fue proponer objetivos de control que abarca la norma internacional, las cuales garanticen una oportuna gestión del riesgo de activos de información.

Como indica (Cherres, 2020), en su investigación la cual tuvo como objetivo el diagnóstico de la seguridad de la información, mediante la circular 140-2009-SBS, basada también en la norma ISO 27001. Proceso que le llevó a concluir

que la aplicación de directivas es vital para los usuarios de los sistemas, siendo esta la clave para lograr una cultura de seguridad.

Del mismo modo (Moscaiza, 2018), en su investigación cuya finalidad fue Diseñar un sistema de gestión de seguridad de la información alineada a la ISO 27001 2013 que gestione los riesgos y garantice un nivel óptimo el tema de seguridad, utilizo para tal fin la metodología cualitativa y cuantitativa, lo que le permitió concluir que la cooperativa mejoró la gestión de riesgos respecto a su valor inicial del 22.2% cuando aún no existían metodologías claras.

Según (Puma, 2017), con el objetivo de implantar un proceso de auditoria se seguridad de la información alineada a la norma ISO/IEC 27002 para caja los andes, utilizo la metodología cuantitativa en una población de 2 auditorías realizadas en la institución, mediante el cual pudo concluir que, la gestión riesgos aplicada a la seguridad de la información no se ajusta a la norma SBS G 140-2009.

Finalmente, (Ccesa, 2016), en su investigación la cual tuvo como objetivo fijar un método adecuado de gestión de la seguridad de la información que contribuya a la preservación de principios fundamentales como la confidencialidad, integridad y disponibilidad de la misma. Con una investigación aplicada a una muestra de seis trabajadores tomados de las áreas de Subgerencia de Sistemas y Tecnología da a conocer que en dicha entidad no cuentan con un sistema de gestión de seguridad de la información pese a ser una entidad del estado. Finalmente, el investigador concluye que concientizar al personal sobre la protección de este activo es de gran importancia, ejecutando controles que permitan minimizar los riesgos, y hacerle frente a posibles desastres o ataques que pudiesen afectar las necesidades institucionales.

En el ámbito regional, en la investigación de (Cabrera, 2018). Cuyo propósito fue diseñar un modelo de políticas basándose en la norma ISO 27001 para reforzar la gestión de seguridad de la información. Llevando a cabo el estudio con un total de 13 personas, los mismos que le permitieron obtener un resultado post test satisfactorio, concluyendo que la seguridad de la información es una responsabilidad compartida de todas las áreas. Por último, menciona que la labor

que abordan los sistemas de gestión de seguridad de la información, es de vital importancia para identificar los riesgos a los que están expuestos los activos a fin de evitar pérdidas económicas u operacionales.

Se finaliza los antecedentes con la investigación de (Ñañez, 2019) , cuyo propósito fue identificar y evaluar los escenarios de riesgo en la seguridad de la información en los procesos académicos y administrativos de la Universidad Nacional Toribio Rodríguez de Mendoza. Para la cual se ayudó de la metodología Magerit y la ISO/IEC 27005para una gestión del riesgo total.

A través de esta investigación se logró identificar que en la institución no se albergaba políticas de seguridad de la información, menos una cultura de protección de información, y luego de implementarse el modelo se alcanzó un 85% de mejoría en cuanto al conocimiento de políticas en sus colaboradores, incrementando así sus compromisos con la seguridad de los activos de la información.

Sistema: Según (Von, 1968) en su libro de la Teoría General de los Sistemas determina que: “Un sistema es el conjunto de elementos interactuantes. Lo equivalente a decir que elementos de P se relacionan con R, aun cuando sea diferente el comportamiento de un elemento P en una o varias relaciones con R.”

Gestión: Según (Rubio, 2000) en su libro describe que: “La gestión se soporta y actúa por medio de las personas en equipos de trabajo para poder alcanzar sus objetivos”.

Sistema de gestión: Según (Martinez, 2014), define que: “Dicho término está constituido por el conjunto de políticas, estándares y procedimientos, que buscan perfeccionar un proceso específico”.

Ciclo Deming: (Chacón & Nuñez, 2017), Señala que es un método de gestión que aborda la mejora continua en sus cuatro etapas y junto a la norma ISO 27001 buscan la revaluación constante de controles y políticas admitidas para garantizar la seguridad de los sistemas informáticos y la información a través del tiempo.

Plan: (Andres & Gomez, 2012)**,** señalan que en esta etapa se diseña el programa, enfatizando las políticas que se aplicarán en la organización, los fines y los medios tomados en cuenta para lograr los objetivos del negocio de modo coherente con la seguridad de la información.

Hacer: (Martinez, 2015)**,** indica que en esta fase se lleva a cabo la implementación del plan de gestión de seguridad ya estipulado en el primer ciclo.

Verificar: Para (Bustamante & Osorio, 2014)**,** en esta etapa se estudian los efectos después de ejecutar las actividades y procesos listados en el Hacer y se contrastan con los efectos del Plan para analizar sus disconformidades.

Actuar: (Nuñez & Chacon, 2017), puntualizan que en esta última etapa se desarrollan acciones correctivas y preventivas basadas en auditorias con el objetivo de mejorar el sistema de gestión de seguridad de la información, a raíz de los resultados obtenidos se proponen acciones para reiniciar las fases del ciclo PHVA.

ISO/IEC 27001:2013 Según (Goucher, 2016), This is an international standard that addresses the management of information security in order to promote adequate management in the secure handling of data as a dynamic process within organizations, constantly directing it forward strategically, in order to plan and improve the functioning of its processes in the organization, not only with those parts that seem to be at greater risk of exposure to data loss. It also argues that the holistic approach of this standard is to increase the level of "safety culture" in companies. Applying ISO / IEC 27001 is about presenting and providing evidence of operationally effective controls.

Según (Lilja Šikman, 2019) Los aspectos básicos de seguridad en ISO / IEC 27001 se listan a continuación:

a. Information**:** Defining and analyzing the characteristics of IT equipment, the rules of access to information, passwords, encryption procedures, policies from the point of occurrence of risk to the security of data and information, instructions for handling media, e-commerce services, relationships with suppliers, network security management, maintenance and development.

b. Technically**:** Control physical access, protection workspace, video monitoring, recording and control of employees.

c. Organizing**:** Security policy, organization of information security, managing information resources, security, human resources, operational procedures and responsibilities, management of security incidents, management business.

(Alcántara, 2015), afirma que seguridad es una manera de protección contra el riesgo.

(ISO 27000, 2017), señala que: la información es el orden de datos en un conjunto, que ya procesados componen un aviso que altera el estado de conocimiento del sujeto o sistema que lo recepciona, ya sea hablada, impresa o almacenada digitalmente.

(Goucher, 2016) Information security tries to protect information from unauthorized access, loss or damage. As shown in the following figure, we can see some of the elements that have an effect on the SI process. From this a potential tension is visualized, for example, between business requirements and privacy and data protection.

Organizational Culture & Legal and Regulatory Environment

a. Business Continuity and disaster recovery
b. Business Risk appetite
c. Architecture
d. Information assurance
e. Incident management
f. Business requirements
g. Information security and management system
h. Privacy and data protection
i. It operations

A continuación, según el autor (Puma, 2017), se detallan sus dimensiones principales: Confidencialidad, disponibilidad e integridad.

Según (Bonilla, 2019), describe que la confidencialidad es la dimensión encargada de garantizar la manipulación y el acceso total o parcial a los recursos por parte del personal debidamente autorizado.

Para (Olaza, 2017), la disponibilidad es un aspecto fundamental dado que la información debe estar accesible en cualquier momento para los diferentes usuarios autorizados.

Del mismo modo (Barrantes & Javier, 2012), indican que la integridad es el atributo encargado de preservar datos, libre de alteraciones sin autorización.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Se empleó la investigación cuantitativa aplicada. Según (Cardenas, 2018) es el procedimiento de formular interrogantes para luego responderlas con datos numéricos, medibles y cuantificables, enfocadas a un resultado.

Para (Carrasco, 2017), el diseño pre experimental hace mención al diagnóstico previo en un grupo de elementos, para su manipulación y experimento, luego gestionar su tratamiento, finalmente en un tiempo determinado volver aplicar otro diagnóstico.

El diseño de estudio fue experimental, del tipo pre experimental, ya que se evaluará la seguridad de información antes de su aplicación del sistema de gestión para luego comparar sus resultados.

Su grafico es el siguiente:

G O_1 X O_2

En el cual:

G: Grupo de experimento

O_1: Previa medición, de la variable dependiente ()

X: Resuelve la variable independiente

O_2: Posterior medición de la variable dependiente ()

Se emplea un pretest (antes de implantar; $O_{1)}$ a un grupo de elementos (G), tratamiento posterior (Seguridad de la información; X), concluyendo con el postest (luego de implantar; O_2)

3.2. Variables y operacionalización

- **Variable independiente:** Sistema de gestión.
- **Variable dependiente:** Seguridad de la información

Tabla 1 : Matriz de consistencia

PROBLEMA	HIPÓTESIS	OBJETIVOS	OPERACIONALIZACION DE VARIABLES					
PROBLEMA PRINCIPAL:	**HIPOTESIS PRINCIPAL:**	**OBJETIVO PRINCIPAL:**	**VARIABLE**	**DIMENSIONES**	**INDICADORES**	**INSTRUMENTO DE MEDICIÓN**	**ESCALA**	**METODO**
- ¿De qué manera un sistema de gestión alineado a la norma ISO/IEC 27001: 2013; influye en la seguridad de la información en una institución financiera? **PROBLEMA SECUNDARIOS:** - ¿De qué manera un sistema de gestión alineado a la norma ISO/IEC 27001:2013 asegurará la confidencialidad de la información en una institución financiera? - ¿De qué manera un sistema de gestión alineado a la norma ISO/IEC 27001:2013 asegurará la integridad de la información en una institución financiera? - ¿De qué manera un sistema de gestión alineado a la norma ISO/IEC 27001:2013 asegurará la disponibilidad de la información en una institución financiera?	- Un sistema de gestión alineado a la Norma ISO/IEC 27001:2013, influye significativamente en la seguridad de la información en una institución financiera. **HIPÓTESIS ESPECÍFICAS:** - Un sistema de gestión alineado a la Norma ISO/IEC 27001:2013, influye significativamente en la confidencialidad de la información en una institución financiera. - Un sistema de alineado a la Norma ISO/IEC 27001:2013, influye significativamente en la integridad de la información en una institución financiera. - Un sistema de gestión alineado a la Norma ISO/IEC 27001:2013, influye significativamente en la disponibilidad de la información en una institución financiera.	- Determinar la influencia del sistema de gestión alineado a la Norma ISO/IEC 27001:2013 en la seguridad de la información en una institución financiera. **OBJETIVOS SECUNDARIOS:** - Determinar la influencia del sistema de gestión alineado a la Norma ISO/IEC 27001:2013, en la confidencialidad de la información en una institución financiera. - Determinar la influencia del sistema de gestión alineado a la Norma ISO/IEC 27001:2013, en la integridad de la información en una institución financiera. - Determinar la influencia del sistema de gestión alineado a la Norma ISO/IEC 27001:2013, en la disponibilidad de la información en una institución financiera.	Sistema de gestión					
			Seguridad de la información	**Confidencialidad**	Accesos no autorizados $\mathrm{IC} = \frac{\mathrm{AS} - \mathrm{ANA}}{AS} x\ 100$	**Ficha de observación**	**Razón**	**Enfoque de la investigación:** Cuantitativa **Tipo de estudio:** Aplicada **Diseño de la investigación:** Experimental **Población y muestra**: 164 accesos no autorizados 72 datos manipulados 18.38h servicios denegados **Tipo de muestreo:** Probabilística aleatoria simple
				Integridad	Eliminar/manipular datos $\mathrm{INT} = \frac{\mathrm{DE} - \mathrm{EDC}}{DE} x\ 100$			
				Disponibilidad	Negación del servicio $\mathrm{ID} = \frac{\mathrm{HD} - \mathrm{HSS}}{HD} x\ 100$			

Referencia: Elaboración propia

3.3. Población, muestra y muestreo, unidad de análisis

Según (De la Cruz, 2016), Población es el total del conjunto en estudio, el cual sus elementos poseen una cualidad general, la misma que se analiza y da inicio a la investigación.

Tabla 2: Población

INDICADOR	CANTIDAD POBLACIÓN
Accesos no autorizados	164 accesos no autorizados
Eliminar/manipular datos	72 datos manipulados
Negación de servicio	18.38h servicios denegados

Referencia: Elaboración propia

Para (Gorgas, Cardiel, & Otros, 2011), afirman que aun cuando la población es finita, posee un alto número de elementos, por ello la necesidad de trabajar con tan solo una parte de la mencionada, lo que equivale a decir que la muestra es el subconjunto de elementos de una población. Empleando la fórmula para el cálculo de la muestra en poblaciones finitas, se detalla a continuación:

n: Tamaño de la muestra

Z: Nivel de confianza deseado

p: proporción de la población con la característica deseada

q: proporción de la población sin la característica deseada

e: nivel de error dispuesto a cometer

N: Tamaño de la población

$$\boldsymbol{n = \frac{Npq Z^2}{e^2(N-1) + Z^2 pq}}$$

El muestro utilizado en la presente investigación es del tipo probabilístico aleatoria simple por voluntad y criterio propio, puesto que se tomaron todos los datos de la población los cuales tienen la misma consigna de elección. La muestra será contabilizada en 24 registros.

3.4. Técnicas e instrumentos de recolección de datos

Tabla 3: Técnicas e instrumentos utilizados.

TÉCNICA	INSTRUMENTO	FUENTE	INFORMANTE
Observación	Guía de observación	Información de la gerencia	Gerente

Referencia: Elaboración propia

3.5. Procedimientos

La información sobre la entidad financiera CMAC AREQUIPA, fueron gestionados mediante solicitud formal al gerente de agencia en la ciudad de Chachapoyas. Información que se pasó a tabular en Excel, para su validación respectiva de cada uno de los indicadores a través del juicio de expertos, bajo el procedimiento de test y retest de fiabilidad, los datos obtenidos se pusieron al SPSS para su análisis.

De igual manera se siguió la investigación acoplándose a la norma ISO/IEC 27001:2013, la misma que aborda la gestión de la seguridad de la información en el manejo seguro de los datos como un proceso dinámico dentro de las organizaciones. Posteriormente se aplicaron pruebas de pre y postest y las validaciones normales. Finalmente se realizó la discusión de resultados, conclusiones y recomendaciones.

3.6. Método de análisis de datos

Según (Gomez & Cohen, 2016), escriben que, el investigador por medio de técnicas necesarias busca obtener información, para lo cual debe de seguir un proceso sucesivo de actos de medición orientados a lograr los resultados que darán respuesta al problema de la investigación.

En el presente estudio se pretende realizar la comparación de efectos que se obtuvieron con el pretest, con los efectos postest, luego de implementar el sistema que a través de la contrastación de las hipótesis fijadas se evalúa su aceptación o negación.

3.7. Aspectos éticos

El investigador asume la total responsabilidad de guardar autenticidad en el estudio y la credibilidad de la información proporcionada por la entidad financiera, del mismo modo poner a buen recaudo la identidad de las personas y materiales que formaron parte de la investigación.

IV. RESULTADOS

El análisis llevado a cabo en el presente estudio aspira comprobar que tanto contribuye un sistema de gestión basado en la Norma ISO/IEC 27001:2013 en la parte operativa de un sistema informático en temas de seguridad de la información dentro de una institución financiera, si influye de manera favorable o no la aplicación en la disponibilidad, integridad y disponibilidad de datos.

Para explicar el resultado obtenido en la investigación se hizo un análisis inferencial y descriptivo del total de datos a través de los instrumentos de recolección. (Salazar & Del Castillo, 2018) argumentan que la estadística descriptiva es el análisis completo, organizado y ordenado en forma sintetizada de un conjunto de datos para posteriormente obtener conclusiones de dicho conjunto. De la misma forma señalan que la estadística inferencial es la rama que analiza una población representada en datos y resultados extraídos de la muestra.

Análisis descriptivo

En esta parte del análisis, se presentan datos resumidos que se recolectaron y se da una vista general de los integrantes de la muestra. Como la población es igual a la muestra, con ese efecto, se analizó la conducta en el pretest y postest de cada uno de los indicadores

Indicador 1: Accesos no autorizados

Los resultados descriptivos para el primer indicador se pueden apreciar continuación:

Tabla 4: Estadísticos descriptivos del indicador 1 antes y después de la implantación.

	N	Min	Max	Media	Desviación estándar	Varianza
Pretest	24	33.33	100.00	75.52	19.40	376.38
Postest	24	66.67	100.00	87.36	12.35	152.62
N válido por lista 24						
Elaboración SPSS v26						

En la Tabla 5, se puede visualizar que la media de los accesos no autorizados en el pretest obtuvo un valor de 75.52%, mientras que en el postest obtuvo un valor de 87.36% para la muestra.

En conclusión, al realizar la comparación entre la media conseguida en el pretest y en el postest, se alcanzó un incremento del 11.84%, lo que indica que la variable independiente causo efecto positivo en la implantación.

Indicador 2: Eliminación/manipulación de datos

Los resultados descriptivos para el segundo indicador se pueden apreciar continuación:

Tabla 5: Estadísticos descriptivos del indicador 2 antes y después de la implantación

	N	Min	Max	Media	Desviación estándar	Varianza
Pretest	24	0	100.00	50.83	23.02	35.25
Postest	24	0	100.00	76.32	34.75	34.75
N válido por lista 24						
Elaboración SPSS v26						

El análisis dio como resultado una diferencia de Medias. El valor de la Media del pretest antes es de 50.83% respecto al valor de la Media del índice después que es de 76.32%. Lo que resulta decir que, al efectuar la comparación entre la media conseguida en el pretest y postest, se comprueba que la variabilidad respecto a los datos difiere en gran medida, por lo que la comparación de los valores de las medias se considera adecuada.

Indicador 3: Negación del servicio

Los resultados descriptivos para el tercer indicador se pueden apreciar continuación:

Tabla 6: Estadísticos descriptivos del indicador 3 antes y después de la implantación.

	N	Min	Max	Media	Desviación estándar	Varianza
Pretest	24	86.21	100.00	96.81	3.568	12.733
Postest	24	99.54	100.00	99.93	0.164	0.027
N válido por lista 24						
Elaboración SPSS v26						

El análisis dio como resultado una diferencia de Medias. El valor de la Media del índice antes es de 96,81 respecto al valor de la Media del índice después que es de 99,93. Esto significa que la influencia de la variable independiente causo efecto al momento de ser implantado. Se logró mejorar en un 3.12%, lo que implica un avance significativo luego de ejecutar la propuesta

Análisis inferencial

(Samavides, 2017), Argumenta que la prueba de normalidad en estadística se lleva a cabo para validar si los datos que se obtienen adoptan un carácter paramétrico o no paramétrico, enfatizando el valor de significancia para cada uno de los siguientes casos:

Significancia>0.05, es distribución normal de lo contrario la distribución es no normal, para el primer caso si es paramétrico->Tstudent de otro modo se utilizaría Wilcoxon continuando con el análisis, el autor señala que en cuanto a los estadígrafos se utilizan de acuerdo al número de muestras que según detalle es:

Para muestras > 30 se aplicará Kolmogorov- Smirnov y en caso la muestra sea

≤30 se usará Shapiro wilk.

Por otro lado, cuando las hipótesis cumplan los detalles siguientes:

Paramétrico: las 2 variables son paramétricas.

No paramétrico: solo una variable es paramétrica.

La prueba se realizó empleando el SPSS v26 como programa estadístico, el cual facilita el contraste de hipótesis a tal grado de aceptar o rechazar su nivel de significancia, las restricciones para tal efecto continuación se detalla:

Pv ≤0.05, se acepta la hipótesis alterna de lo contrario se toma la hipótesis nula.

Indicador 1: Accesos no autorizados

La prueba de normalidad para el primer indicador realizadas en el pretest y postest alcanzaron los siguientes resultados estadísticos:

Tabla 7: Prueba de normalidad del indicador 1

	Shapiro-Wilk		
	Estadístico	**gl**	**sig.**
Pretest	,897	24	,019
Postest	,801	24	,000
a. Corrección de significación de Lilliefors			

En la Tabla 7, se evidencia que la información proviene de una distribución no normal, puesto que el valor de significancia del pretest es 0,019 y para el postest es 0,000. Los dos valores son inferiores al margen de error (α = 0,05).

Indicador 2: Eliminación/manipulación de datos

La prueba de normalidad para el segundo indicador realizadas en el pretest y postest alcanzaron los siguientes resultados estadísticos:

Tabla 8: Prueba de normalidad del indicador 2

	Shapiro-Wilk		
	Estadístico	**gl**	**sig.**
Pretest	,822	24	,001
Postest	,707	24	,000
a. Corrección de significación de Lilliefors			

En la Tabla 8, se observa que la información proviene de una distribución no normal, ya que el valor de significancia del pretest es 0,001 y para el postest es 0,000. Los dos valores son inferiores al margen de error (α = 0,05).

Indicador 3: Negación del servicio

La prueba de normalidad para el segundo indicador realizadas en el pretest y postest alcanzaron los siguientes resultados estadísticos:

Tabla 9: Prueba de normalidad del indicador 3

	Shapiro-Wilk		
	Estadístico	**gl**	**sig**
Pretest	,822	24	,001
Postest	,463	24	,000
a. Corrección de significación de Lilliefors			

En la Tabla 9, se evidencia que la información proviene de una distribución no normal, ya que el valor de significancia del pretest es 0,001 y para el postest es 0,000. Los dos valores son inferiores al margen de error (α = 0,05).

Prueba de hipótesis

Hipótesis de investigación 1:

Hipótesis H_0: Un sistema de gestión basado en la Norma ISO/IEC 27001:2013, no influye significativamente en la confidencialidad de la seguridad de la información en una institución financiera.

$$H_0 = IC_d \leq IC_a$$

Hipótesis H_1: Un sistema de gestión basado en la Norma ISO/IEC 27001:2013, influye significativamente en la confidencialidad de la seguridad de la información en una institución financiera.

$$H_1 = IC_d > IC_a$$

Para la constatación de la hipótesis de investigación 1, se realizó la prueba de rangos con signo de Wilcoxon, ya que se obtuvo un resultado con sesgo atípico.

Tabla 10: Prueba de rangos de wilcoxon para el indicador de confidencialidad antes y después de la implantación.

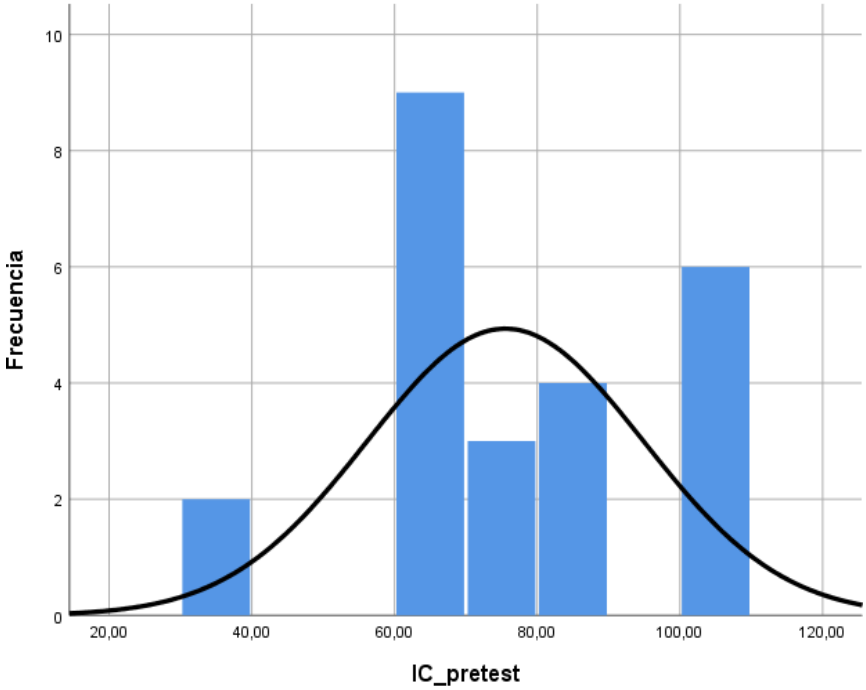
		N	Rango promedio	Suma de rasgos
IC_postest & IC_pretest	**Rangos negativos**	5	10.40	52.00
	Rangos positivos	16	10.19	179.00
	Empates	3		
	Total	24		
a. IC_postest <IC_ IC_pretest				
b. IC_postest > IC_ IC_pretest				
c. IC_postest = IC_ IC_pretest				
Elaboración: SPSS V26				

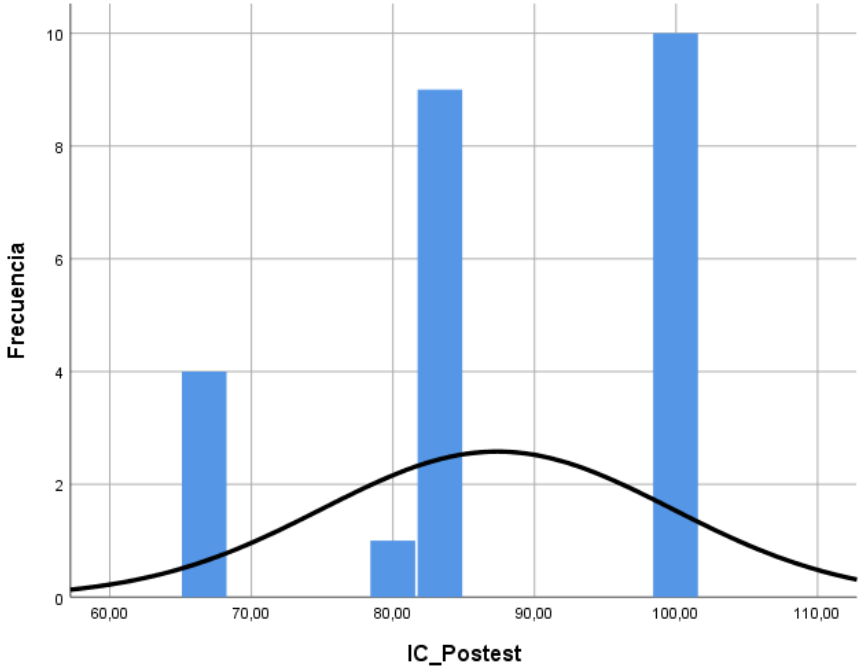
Tabla 11: Estadístico de contraste del indicador 1

	IC_postest & IC_pretest
Z	-2,210
Sig.(bilateral)	,027
a. Prueba de Wilcoxon	
b. Se basa en rangos negativos	
Elaboración: SPSS V26	

Lo indicado en la Tabla 10 y en la tabla 11, corresponde que el valor de Sig. es de 0.027, cayendo en la región conocida como rechazo, por lo que se toma como válida la hipótesis alterna(H_1), donde se señala que un sistema de gestión basado en la Norma ISO/IEC 27001:2013, influye significativamente en la confidencialidad de la seguridad de la información en una institución financiera", y se da por descartado la hipótesis nula(H_0),

Figura 1. Diagrama de normalidad de datos para el indicador 1





Los histogramas muestran una distribución no normal para los datos, en el antes y después de implantar el sistema de gestión basado en la norma ISO IEC/27001:2013

Hipótesis de investigación 2:

Hipótesis H_0: Un sistema de gestión basado en la Norma ISO/IEC 27001:2013, no influye significativamente en la integridad de la seguridad de la información en una institución financiera.

$$H_0 = INT_d \leq INT_a$$

Hipótesis H_1: Un sistema de gestión basado en la Norma ISO/IEC 27001:2013, influye significativamente en la integridad de la seguridad de la información en una institución financiera.

$$H_1 = INT_d > INT_a$$

Para la constatación de la hipótesis de investigación 2, se realizó la prueba de rangos con signo de Wilcoxon, ya que se obtuvo un resultado con sesgo atípico.

Tabla 12: Prueba de rangos de wilcoxon para el indicador de integridad antes y después de la implantación.

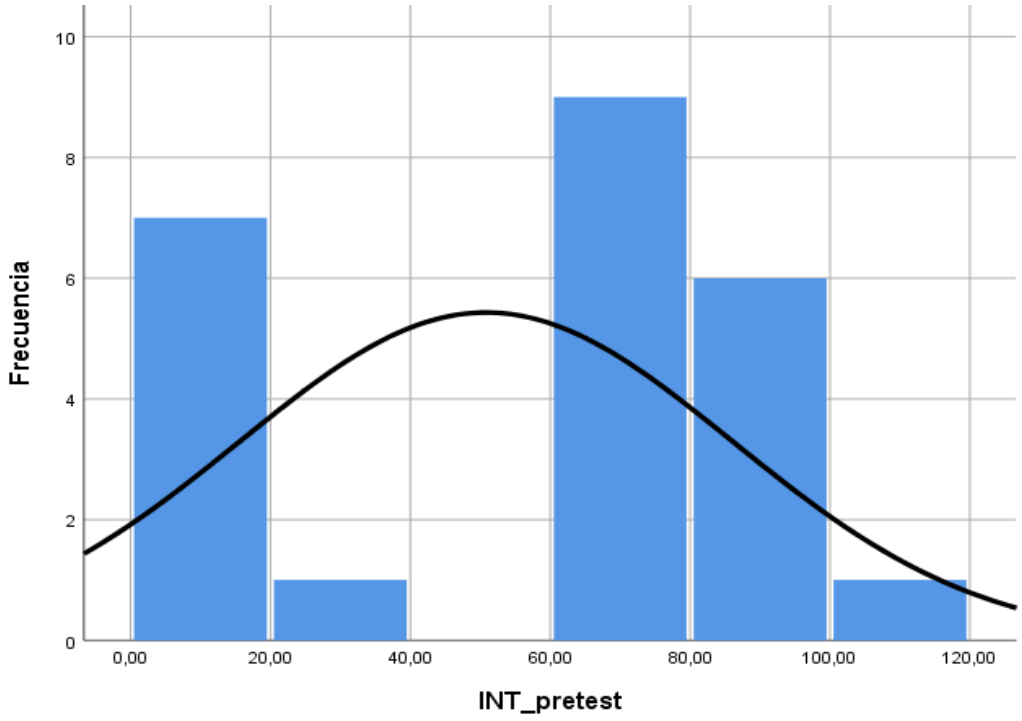
		N	Rango promedio	Suma de rasgos
IC_postest & IC_pretest	**Rangos negativos**	6	9.17	55.00
	Rangos positivos	15	11.73	176.00
	Empates	3		
	Total	24		
a. IC_postest <IC_ IC_pretest				
b. IC_postest > IC_ IC_pretest				
c. IC_postest = IC_ IC_pretest				
Elaboración: SPSS V26				

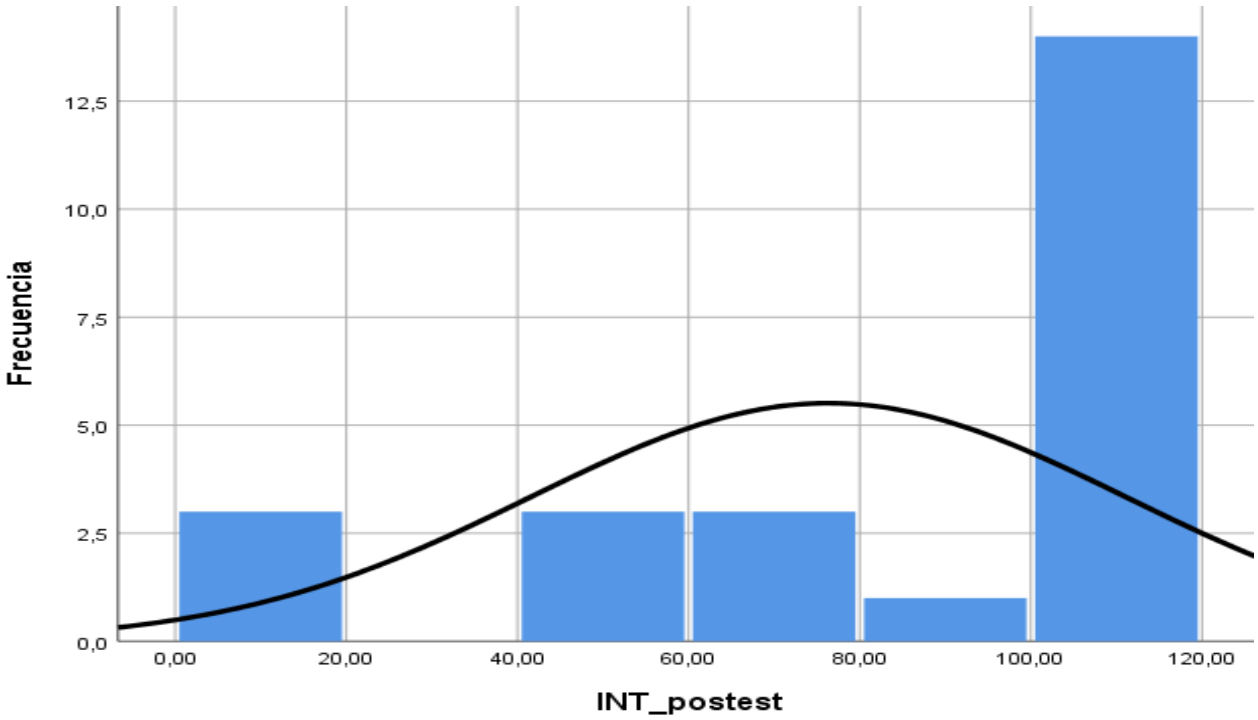
Tabla 13: Estadístico de contraste del indicador 2

	IC_postest & IC_pretest
Z	-2,111
Sig.(bilateral)	,035
a. Prueba de Wilcoxon	
b. Se basa en rangos negativos	
Elaboración: SPSS V26	

Lo indicado en la Tabla 12 y en la tabla 13, corresponde que el valor de Sig. es de 0.035, cayendo en la región conocida como rechazo, por lo que se toma como válida la hipótesis alterna(H_1), donde se señala que un sistema de gestión basado en la Norma ISO/IEC 27001:2013, influye significativamente en la integridad de la seguridad de la información en una institución financiera", y se da por descartado la hipótesis nula(H_0),

Figura 2. Diagrama de normalidad de datos para el indicador 2





Los histogramas muestran una distribución no normal para los datos, en el antes y después de implantar el sistema de gestión basado en la norma ISO IEC/27001:2013

Hipótesis de investigación 3:

Hipótesis H_0: Un sistema de gestión basado en la Norma ISO/IEC 27001:2013, no influye significativamente en la disponibilidad de la seguridad de la información en una institución financiera.

$$H_0 = INT_d \leq INT_a$$

Hipótesis H_1: Un sistema de gestión basado en la Norma ISO/IEC 27001:2013, influye significativamente en la disponibilidad de la seguridad de la información en una institución financiera.

$$H_1 = INT_d > INT_a$$

Para la constatación de la hipótesis de investigación 3, se realizó la prueba de rangos con signo de Wilcoxon, ya que se obtuvo un resultado con sesgo atípico.

Tabla 14: Prueba de rangos de wilcoxon para el indicador de disponibilidad antes y después de la implantación.

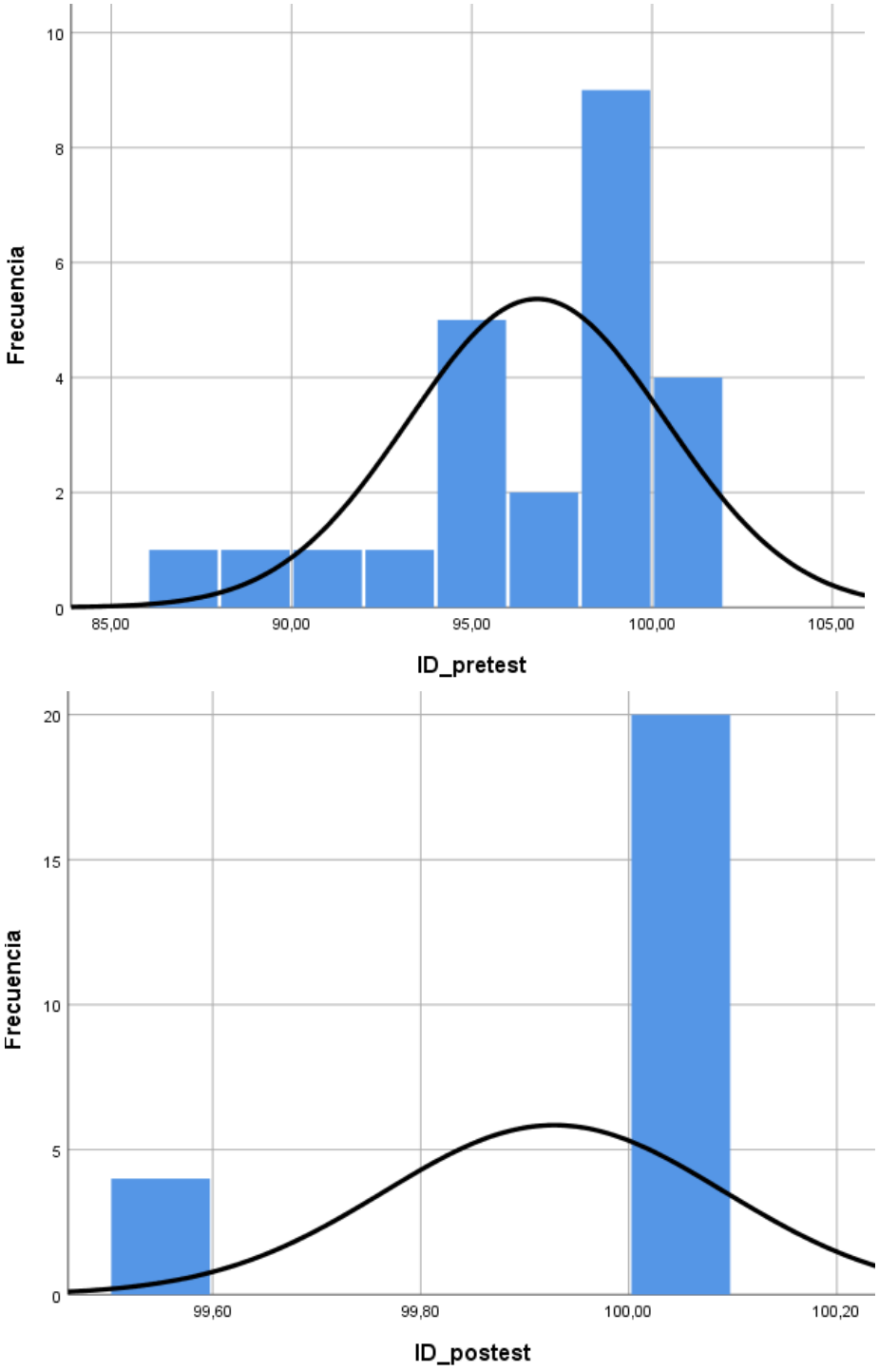
		N	Rango promedio	Suma de rasgos
INT_postest & INT_pretest	**Rangos negativos**	0	0	0.00
	Rangos positivos	20	10.50	210.00
	Empates	4		
	Total	24		
a. INT_postest <IC_ INT_pretest				
b. INT_postest > INT_pretest				
c. INT_postest = INT_pretest				
Elaboración: SPSS V26				

Tabla 15: Estadístico de contraste del indicador 3

	IC_postest & IC_pretest
Z	-3,920
Sig.(bilateral)	,000
a. Prueba de Wilcoxon	
b. Se basa en rangos negativos	
Elaboración: SPSS V26	

Lo indicado en la Tabla Nro. 14 y en la tabla Nro. 15, corresponde que el valor de Sig. es de 0.000, cayendo en la región conocida como rechazo, por lo que se toma como válida la hipótesis alterna(H_1), donde se señala que un sistema de gestión basado en la Norma ISO/IEC 27001:2013, influye significativamente en la disponibilidad de la seguridad de la información en una institución financiera", y se da por descartado la hipótesis nula(H_0).

Figura 3. Diagrama de normalidad de datos para el indicador 3



Los histogramas muestran una distribución no normal para los datos, en el antes y después de implantar el sistema de gestión basado en la norma ISO IEC/27001:2013.

V. DISCUSIÓN

En base a los resultados obtenidos en la presente investigación, se valora la hipótesis general la misma que establece que Un sistema de gestión basado en la ISO/IEC 27001:2013, influyó significativamente en la seguridad de la información en una institución financiera, ya que dicha norma técnica internacional ayuda considerablemente en los procesos importantes dentro una empresa, aportando seguridad y confiabilidad en la gestión de sus procesos.

La presente investigación obtuvo resultados para la confidencialidad, en el pretest diagnosticó un total de 75.52% y luego de la implantación del sistema de gestión, arrojó un valor mayor postest de 87.36%, en cuanto a la integridad, el pretest determinó un valor de 50.83% y posteriormente a la implantación en la etapa de postest escaló a 76.32%, y para la disponibilidad el valor pretest alcanzó un valor de 96.81% y después de la implantación en etapa postest subió a 99.93%.

En cuanto al contraste de los antecedentes citados en líneas anteriores, (SamPedro, Machuca & Otros, 2019), pudo demostrar que más del 50% de las Pymes cuentan con políticas y directrices que precautelan la seguridad de la información, sin embargo, estos no están bajo seguimiento, si bien los empresarios son conscientes del riesgo al que está expuesta la información de su empresa, la confidencialidad, integridad y disponibilidad no son parte de acciones preventivas en forma total o parcial, lo que demuestra que a medida que las Pymes implementen sus sistemas informáticos, estarán más expuestas a daños informáticos. De modo que el desarrollo de acciones preventivas y correctivas se alinea a un estándar como ISO.

En el estudio llevado a cabo por (Rodríguez, Cruzado & Otros, 2020), se obtuvieron resultados influyentes como en la presente investigación en la que se propone la ISO 27001 como una herramienta que garantiza la seguridad de la información de clientes y proveedores. Además, el autor refiere que esta norma reduce costos y tiempo. En cuanto a la confidencialidad de la información, se ve reflejada en la discreción de activos como componente primordial en la toma de decisiones, con respecto a la disponibilidad e

integridad, garantizó el fácil acceso y la credibilidad de los recursos ante la gran demanda de gestores de información.

Para (Moreyra, 2019), en su estudio llevado a cabo obtuvo un resultado con mejora del 73% para la seguridad física basado en la ISO 27001, y para el control de accesos pudo demostrar un aumento del 50%, de tal manera que la aplicación de la norma permitió tomar acciones a favor de la gestión de la seguridad de la información, evaluando riesgos y desarrollando acciones de prevención que salvaguarden el activo estratégico institucional en la infraestructura tecnológica y servicios informáticos del gobierno autónomo descentralizado municipal del Cantón Chone.

En el estudio realizado por (Mayorga y Zapata, 2020), se obtuvo un resultado predominante del 100% de aceptación de políticas de seguridad de la información, así mismo se mejoró el control de accesos en relación a la confidencialidad a un 70% de eficacia cuyo índice está en la medida esperada, entonces se vale afirmar que la implementación de políticas fue elaboradas coherentemente a fin de gestionar la seguridad de la información adecuadamente

En el estudio realizado por (Cherres, 2020), evidencio como resultado de las bases de su proyecto, donde pudo implementar alternativas innovadoras en relación a la gestión del riesgo de seguridad de la información, proceso que involucro a la alta gerencia en la búsqueda de oportunidades que mejoren la administración de controles de acceso a los sistemas en base a una comunicación constante y consensuada dispuestos a la solución de amenazas y debilidades para finalmente atravesar por un proceso de cambio.

Para (Puma, 2017), en su estudio realizado obtuvo un resultado austero para el proceso de auditoría de seguridad de la información alineada a la ISO 27002 en una institución financiera, en la que destaca la deficiente evaluación de tecnologías de la información cuando la propia organización no cuenta con una arquitectura de seguridad de la información, por lo que está expuesta a mayores riesgos y costos de respuesta. Por ello destaca en su resultado que aplicar herramientas basado en la norma internacional, mejora en gran medida

la ejecución de actividades y los resultados van acorde con las directrices y políticas institucionales.

En la investigación de (Ramos & Urrutia, 2017), se dio a conocer un resultado del 46.8 %, evidenciando un conocimiento aceptable en el manejo de activos que genera, crea y procesa información dentro de la cooperativa Condelcauca. La adopción de políticas sobre las funciones de los usuarios permitió el acceso seguro a la información y de esta forma tener un mejor control y registro de los usuarios, el investigador resaltó la implementación de directrices en la que se incluyen procedimientos, funciones de hardware y software, estructuras organizacionales y políticas que busquen asegurar los datos con un alto nivel de compromiso.

Para (Ñañez, 2019), la valoración de su estudio alcanzó el 67% de eficacia en cuanto a políticas de seguridad de la información implementadas en paralela al 13% de usuarios que dan cumplimiento al Sistema de gestión de seguridad de la información ya estandarizado, de esto ya se predice una mejora significativa de bajar el riesgo a un nivel aceptable luego de su gestión con la ayuda de la ISO/IEC 27005 y la metodología Magerit, en palabras resumidas el estudio logró incrementar el compromiso de los usuarios con la seguridad de los de información.

En la investigación de (Moscaiza, 2018), se evidenciaron resultados donde más del 22% de las políticas implementadas causaron efectos positivos como parte de mejora de la gestión de riesgos, con ello indica el autor que la entidad se halla preparada para identificar elementos críticos que merman los objetivos de la empresa. Los controles de la ISO/IEC 27001 implantados hicieron frente a diferentes riesgos y daños potenciales en base a la sensibilidad de los recursos. Dicho de otra forma, los resultados obtenidos permitieron determinar un plan correcto de seguridad de la información.

Para (Ccesa, 2016), el resultado de su estudio describe un 100% de aceptación del sistema de gestión de seguridad de la información ya que los datos obtenidos en su estudio van acorde con sus objetivos, de tal manera que su propuesta permite identificar amenazas en las que se encuentra el área de

subgerencia de sistemas y tecnología, de modo que la evaluación de riesgos y la aplicación de controles alcanzaron su objetivo el de resguardar los activos de la información, en tanto la confidencialidad predomina en este estudio al 50% de lo esperado.

En el estudio llevado a cabo por (Cabrera, 2018), obtuvo un resultado optimo donde aplicó un plan de políticas que ayuden a la seguridad de la información, haciéndola más confiable, integra y disponible, ya que, de ocurrir cualquier alteración en esos indicadores, los resultados ocasionarían grandes pérdidas económicas, por ello tal investigación favoreció considerablemente a la prevención e identificación de riesgos a los que está expuesto los activos de la Municipalidad de distrital de Florida

VI. CONCLUSIONES

Como consecuencia en el presente estudio se obtuvieron los siguientes resultados:

a) Se logró mejorar la seguridad de la información en una institución financiera, por medio de un sistema de gestión basado en la ISO/IEC 27001:2013, reflejado en la rentabilidad empresarial además de ayudar a la mejor comunicación de entre las áreas operativas de todo el proceso crediticio.

b) Se consiguió aumentar la confidencialidad de la información dentro de una institución financiera, una vez llevado a cabo la implantación del sistema de gestión, se alcanzó un incremento del 87.36%, de acuerdo al resultado obtenido en la tabla 6, de tal forma que se evidencia una mejora del 11.84%. La implantación de la propuesta ayudó potencialmente a aumentar la confidencialidad de la información.

c) Se logró incrementar la integridad de la información dentro de una institución financiera, una vez llevado a cabo la implantación del sistema de gestión, se alcanzó un incremento del 76.32%, de acuerdo al resultado obtenido en la tabla 7, de tal forma que se evidencia una mejora del 25.49%. Lo que equivale a decir que la variable independiente causó un impacto positivo en la integridad de la información.

d) Se consiguió aumentar la disponibilidad de la información dentro de una institución financiera, una vez llevado a cabo la implantación del sistema de gestión, se alcanzó un incremento del 99.93%, de acuerdo al resultado obtenido en la tabla 8, de tal forma que se evidencia una mejora del 3.12%. Lo que significa que la propuesta ayudó potencialmente a mejorar la disponibilidad de la información.

VII. RECOMENDACIONES

Se detallan en líneas siguientes los consejos para posteriores estudios:

a) Se recomienda que las investigaciones venideras se desarrollen de acuerdo a las nuevas tendencias y actualizaciones de la norma ISO 27001; las mismas que faciliten un mejor resguardo del activo sensible (la información).

b) Se sugiere en un estudio próximo mayor énfasis en antecedentes puntuales a las variables y dimensiones que acoplan de forma total o parcial a la seguridad de la información.

c) Se advierte a futuros investigadores duplicar el número de indicadores con el fin de ganar mayor fiabilidad en el estudio llevado a cabo.

d) Se recomienda adentrar la investigación en la ISO 27001 y las ISO cercanas a esta, junto con la NTP/ISO 27001, direccionadas a la gestión de la seguridad de la información dentro de una institución financiera abarcando un análisis más completo y con mejores resultados.

e) Finalmente, se sugiere la implementación de la norma ISO/27001:2013 en la totalidad de sus procesos dentro de una institución financiera para lograr su certificación internacional y ganar mayor confianza en sus clientes y proveedores en un mercado más competitivo.

REFERENCIAS

Alcántara, J. (2015). Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte p.n.p en la ciudad de Chiclayo. Recuperado el 01 de 03 de 2021, de http://tesis.usat.edu.pe/handle/usat/539

América sistemas. (enero de 2016). Iso 27001:2014 obligatorio en el estado Peruano. Recuperado el 02 de 02 de 2021,de http://www.americasistemas.com.pe/iso-27001-2014-obligatorio-en-el-estado-peruano/

Andres, A., & Gomez, I. (2012). Guía de aplicación de la norma une-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. España: aenor. Recuperado el 25 de 02 de 2021, de https://www.marcialpons.es/libros/guia-de-aplicacion-de-la-norma-une-isoiec-27001-sobre-seguridad-en-sistemas-de-informacion-para-pymes/9788481437492/

Barrantes, C, & Javier, H. (2012). Diseño e implementación de un sistema de gestion de seguridad de informacóon en procesos tecnologicós. Lima. Recuperado el 02 de 03 de 2021, de https://repositorioacademico.usmp.edu.pe/bitstream/handle/20.500.12727/609/barrantes_ce.pdf?sequence=3&isallowed=y

Bonilla, E. (2019). Propuesta de mejoramiento continúo de la seguridad informática y de la información en las instituciones de educación superior. Bogotá. Recuperado el 02 de 03 de 2021, de https://repository.usta.edu.co/bitstream/handle/11634/20824/2019erikabonilla.pdf?sequence=15

Bustamante, G., & Osorio, J. (2014). Methodology of information security as a measure ofprotection small business. Cuaderno activa. Recuperado el 25 de 02 de 2021, de https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/202/206

Cabrera. (2018). Diseño de un modelo de políticas basado en la norma iso 27001, para mejorar la gestión de la seguridad de la información en la municipalidad distrital de Florida – Bongará – Amazonas. Recuperado el 10 de 02 de 2021, de https://repositorio.upeu.edu.pe/handle/upeu/1542

Calderon & hoyos. (2016). Plan de gestión de riesgos de tecnologías de la información en los procesos críticos de créditos y captaciones para la caja de ahorro y créditos Sipan Sa de Chiclayo - 2016. Recuperado el 02 de 02 de 2021, de http://repositorio.unprg.edu.pe/handle/unprg/2879

Cardenas, J. (2018). Investigación cuantitativa. Berlin. Recuperado el 10 de 03 de 2021,de https://www.programa-trandes.net/ressources/manuales/manual_cardenas_investigacion_cuantitativa.pdf

Carrasco, S. (2017). Metodologia de la investigacion cientifica. Lima. Recuperado el 10 de 03 de 2021, de https://www.academia.edu/26909781/metodologia_de_la_investigacion_cientifica_carrasco_diaz_1_

Ccesa. (2016). "diseño de un sitema de gestión de seguridad de la información bajo la ntp iso/iec 27001:2014 para la Municipalidad Provincial de Huamanga, 2016". Recuperado el 10 de 02 de 2021, de http://repositorio.unsch.edu.pe/handle/unsch/1751

Cherres, G. (2020). Auditoría de seguridad de información y riesgos de tecnología de información en una cooperativa de ahorro y crédito. Lima. Recuperado el 15 de 02 de 2021, de http://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/7009/cherres_jgj.pdf?sequence=3&isallowed=y

De la cruz, R. (2016). Propuesta de políticas, basadas en buenas prácticas,para la gestión de la seguridad de la información en la Municipalidad Provincial de Paita,2016. Recuperado el 15 de 03 de 2021, de http://repositorio.uladech.edu.pe/handle/123456789/885

Figueroa; Rodriguez & Otros. (2017). La seguridad informática y la seguridad de la información. Polo del conocimiento. Recuperado el 26 de 01 de 2021, de https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf#

Gomez, & Cohen. (2016). Metodologia de la investigacion ¿para qué? Buenos Aires. Recuperado el 20 de 03 de 2021, de http://up-rid2.up.ac.pa:8080/xmlui/bitstream/handle/123456789/1363/metodolog%c3%ada%20de%20la%20investigaci%c3%b3n-cohen.pdf?sequence=1&isallowed=y

Gorgas, J., Cradiel & Otros(2011). Estadistica Basica para estudiantes de ciencias. Madrid. recuperado el 26 de 03 de 2021,de https://webs.ucm.es/info/astrof/users/jaz/estadistica/libro_gcz2009-pdf

Goucher, W. (2016). Information security auditor. Reino unido. Recuperado el 25 de 02 de 2021, de http://eds.a.ebscohost.com/eds/ebookviewer/ebook/bmxlymtfxzc4odkznf9fqu41?sid=3bb878fb-da7c-4463-8844-9380f6301a9f@sdc-v-sessmgr03&vid=7&format=eb

GruopoED. (2017). Edeconomíadigital. Los diez mayores ataques informáticos del 2016. Recuperado el 26 de 01 de 2021, de https://www.economiadigital.es/tecnologia-y-tendencias/los-diez-mayores-ataques-informaticos-de-2016_188964_102.html

Iso 27000. (martes de noviembre de 2017). Iso 27000.es. Obtenido de iso 27000.es: http://www.iso27000.es/sgsi.html

Jordan, J. (2018). Sistema de gestión de seguridad de la información basado en la norma iso 27001 para la financiera crediscotia sucursal Chimbote.

Recuperado el 15 de 02 de 2021, de http://repositorio.usanpedro.edu.pe/handle/usanpedro/13633?show=full

Lilja šikman, t. L. (2019). Iso 27001 – information systems security, development,trends, technical and economic challenges. Bosnia & Herzegovina. Recuperado el 25 de 02 de 2021, de http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=8&sid=3bb878fb-da7c-4463-8844-9380f6301a9f%40sdc-v-sessmgr03

Martinez. (2014). Sistema de gestión para mejorar la seguridad de la información en la institución servicios industriales de la marina. Chimbote. Recuperado el 20 de 02 de 2021, de http://repositorio.uns.edu.pe/handle/uns/1943

Martinez. (2015). Seguridad de la información en pequeñas y medianas empresas (pymes). Colombia. Recuperado el 25 de 02 de 2021, de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2860/trabajo%20de%20grado.pdf?sequence=1&isallowed=y

Mayorga y Zapata. (2020). Sistema de gestión de seguridad de la información basado en las normas iso/iec 27001, en el departamento de tecnologías de la información del gobierno autónomo descentralizado de la Municipalidad de Ambato. Ecuador. Recuperado el 15 de 02 de 2021, de https://repositorio.uta.edu.ec/jspui/handle/123456789/30694

Moreyra. (2019). Seguridad de la información de infraestructura tecnológica y sistemas informáticos del gadm del cantón chone basado en la norma iso/iec 27001. Ecuador. Recuperado el 05 de 02 de 2021, de http://repositorio.espam.edu.ec/xmlui/handle/42000/1077

Moscaiza, O. (2018). Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la cooperativa de ahorro y crédito ABC, basado en la norma ISO 27001:2013. Lima. Recuperado el 10 de 02 de 2021, de https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/623063/moscaiza_mo.pdf?sequence=5&isallowed=y

Nuñez, W., & Chacon, E. (2017). Diseño del sistema de gestión de seguridad de la información para la empresa serexcel servicios funerarios. Bogotá. Recuperado el 25 de 02 de 2021, de https://repository.udistrital.edu.co/bitstream/handle/11349/8323/edinson%20andres%20chacon%20uma%c3%b1a%20-%20william%20andres%20nu%c3%b1ez%20vergara%202017.pdf?sequence=1&isallowed=y

Ñañez. (2019). Modelo de gestión de riesgos de ti basados en la norma ISO/IEC 27005 y metodología Magerit para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez De Mendoza – Chachapoyas. Recuperado el 20 de 02 de 2021, de https://repositorio.unprg.edu.pe/handle/20.500.12893/6110

Olaza, H. (2017). “Implementación de ntp iso/iec 27001 para la seguridad de información en el área de configuración y activos del ministerio de educación – sede centromin”. Lima. Recuperado el 02 de 03 de 2021, de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/9927/olaza_ahd.pdf?sequence=1&isallowed=y

Puma. (2017). “Implantación de un proceso de auditoría de seguridad de información bajo la norma iso/iec 27002 en una entidad financiera de Puno – 2016”. Recuperado el 10 de 02 de 2021, de http://repositorio.unap.edu.pe/bitstream/handle/unap/6629/puma_arosquipa_max_yonel.pdf?sequence=1&isallowed=y

Ramirez. (2019). La protección de la información confidencial de los OCE por parte del agente afianzado de aduana en la legislación Ecuatoriana. Machala. Recuperado el 26 de 01 de 21, de http://repositorio.utmachala.edu.ec/bitstream/48000/13515/1/ecuace-2019-ci-de00270.pdf

Ramos & Urrutia. (2017). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca. Popayan. Recuperado el 15 de 02 de 2021, de https://revistas.utp.ac.pa/index.php/memoutp/article/view/1475/2121

Rodriguez, Cruzado & Otros. (2020). Aplicación de iso 27001 y su influencia en la seguridad de la información de una empresa privada peruana. Lima. Recuperado el 05 de 02 de 2021, de http://www.scielo.org.pe/pdf/pyr/v8n3/2310-4635-pyr-8-03-e786.pdf

Rubio, P. (2000). Introducción a la gestión empresarial. En p. R. Domínguez, & 2. Eumed.net (ed.), introducción a la gestión empresarial (pág. 297). España: iege-publicaciones. Recuperado el 20 de 02 de 2021, de http://www.adizesca.com/site/assets/g introduccion_a_la_gestion_empresarial-pr.pdf

Salazar & Del castillo. (2018). Fundamentos basicos de la estadistica. Quito. Recuperado el 01 de abril de 2021, de http://www.dspace.uce.edu.ec/bitstream/25000/13720/3/fundamentos%20b%c3%a1sicos%20de%20estad%c3%adstica-libro.pdf

Samavides, T. (2017). “Aplicación de la gestión de almacenes para mejorar el abastecimiento de materiales en el nivel secundaria de la I.E.P Jesús Amigo, Puente Piedra,2017. Lima. Recuperado el 20 de 03 de 2021, de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/22817/samavides_vte.pdf?sequence=1&isallowed=y

Sampedro, Machuca & Otros. (2019). Percepción de seguridad de la en las pequeñas y medianas empresas en Santo Domingo. Revista investigacion operacional. Recuperado el 05 de 02 de 2021, de https://rev-inv-ope.univ-paris1.fr/fileadmin/rev-inv-ope/files/40319/40319-12.pdf

Suaréz, S. (2015). Análisis y diseño de un sistema de gestion de seguridad informática en la empresa aseguradora Suárez Padilla & Cía.Ltda, que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Bogotá. Recuperado el 26 de 01 de 2021, de http://repository.unad.edu.co/handle/10596/3777

Valencia y Orozco. (2017). Metodología para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC27000.Risti, http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=s1646-98952017000200006. Recuperado el 05 de 02 de 2021

Von, L. (1968). Teoría general de sistemas. New york. Recuperado el 20 de 02 de 2021, de https://cienciasyparadigmas.files.wordpress.com/2012/06/teoria-general-de-los-sistemas-_-fundamentos-desarrollo-aplicacionesludwig-von-bertalanffy.pdf

ANEXOS

ANEXO A:

Tabla 16**:** Matriz Operacionalización de variables

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	INSTRUMENTOS DE MEDICIÓN	ESCALA
Sistema de gestión	Según (Martinez, 2014), define que: “Dicho término está constituido por el conjunto de políticas, estándares y procedimientos, que buscan perfeccionar un proceso específico”.	Fuente que genera valor dentro de las organizaciones mediante aspectos claves de planificación y control.				
Seguridad de la información	(SamPedro, Machuca & Otros, 2019), Explican que: La seguridad de la información es el conjunto de medidas preventivas y reactivas que las organizaciones deben aplicar: políticas, normas, procedimientos, evaluar el riesgo, planes de contingencia, entre otras medidas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de la información.	Agrupa controles y políticas en el proceso de gestión de riesgos ante posibles atentados que vulneren la seguridad de la información. Garantizando el acceso a los sistemas y aplicaciones de la organización.	Confidencialidad	Accesos no autorizados	Guía de observación	Razón
			Integridad	Eliminar/manipular datos		
			Disponibilidad	Negación del servicio		

Referencia; Elaboración propia

ANEXO B: Instrumento y población aplicados en el pretest y postest

GUIA DE OBSERVACION			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCIÓN	JR LIBERTAD NRO 667		
MES	FEBRERO	**AÑO**	2021
INDICADOR **ACCESOS NO AUTORIZADOS**		FORMULA IC= ((AS - ANA) / AS) x 100	
Dia	**Num_accesos al sistema**	**Num_accesos no autorizados**	**IC**
1	6	0	100
2	8	2	75
3	8	1	87.5
4	8	0	100
5	8	0	100
6	8	3	62.5
7	8	5	37.5
8	8	0	100
9	8	3	62.5
10	8	3	62.5
11	8	3	62.5
12	8	3	62.5
13	8	1	87.5
14	6	1	83.33
15	6	2	66.67
16	6	4	33.33
17	6	0	100
18	8	0	100
19	8	1	87.5
20	6	2	66.67
21	8	2	75
22	8	2	75
23	8	3	62.5
24	8	3	62.5
		PROMEDIO	75.52

GUIA DE OBSERVACIÓN			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCIÓN	JR LIBERTAD NRO 667		
MES	ENERO	**AÑO**	2021
INDICADOR **ACCESOS NO AUTORIZADOS**		**FORMULA** **IC= ((AS - ANA) / AS) x 100**	
Dia	**Num_accesos al sistema**	**Num_accesos no autorizados**	**IC**
1	7	1	85.71
2	7	2	71.43
3	8	0	100
4	7	0	100
5	8	3	62.5
6	7	2	71.43
7	8	5	37.5
8	7	0	100
9	8	3	62.5
10	8	3	62.5
11	7	3	57.14
12	7	2	71.43
13	7	1	85.71
14	6	1	83.33
15	6	4	33.33
16	6	0	100
17	8	0	100
18	7	1	85.71
19	8	1	87.5
20	6	2	66.67
21	8	2	75
22	5	3	40
23	8	3	62.5
24	6	1	83.33
		PROMEDIO	74.38

GUIA DE OBSERVACIÓN			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCIÓN	JR LIBERTAD NRO 667		
Mes	DICIEMBRE	**Año**	2021
INDICADOR **ACCESOS NO AUTORIZADOS**		**FORMULA** **IC= ((AS - ANA) / AS) x 100**	
Dia	**Num_accesos al sistema**	**Num_accesos no autorizados**	**IC**
1	8	3	62.5
2	8	3	62.5
3	7	1	
4	8	5	37.5
5	7	4	42.86
6	7	2	71.43
7	8	5	37.5
8	7	0	100
9	8	1	87.5
10	5	3	40
11	8	3	62.5
12	7	1	85.71
13	7	1	85.71
14	6	1	83.33
15	8	4	50
16	6	4	33.33
17	6	0	100
18	7	2	71.43
19	5	2	60
20	6	2	66.67
21	6	3	50
22	8	2	75
23	5	3	40
24	6	1	83.33
		PROMEDIO	67.68

GUIA DE OBSERVACIÓN			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCIÓN	JR LIBERTAD NRO 667		
Mes	FEBRERO	**Año**	2021
INDICADOR ELIMINACION/MANIPULACION DE DATOS		**FORMULA INT= ((DE - EDC) / DE) x 100**	
Dia	**Num_datos eliminados**	**Num_datos eliminados que alteran la data de clientes**	**INT**
1	1	1	0
2	3	2	33.33
3	3	0	100
4	6	1	83.33
5	3	1	66.67
6	6	1	83.33
7	3	1	66.67
8	5	1	80
9	5	1	80
10	3	1	66.67
11	1	1	0
12	3	1	66.67
13	1	1	0
14	1	1	0
15	1	1	0
16	3	1	66.67
17	3	1	66.67
18	3	1	66.67
19	3	1	66.67
20	1	1	0
21	3	1	66.67
22	5	1	80
23	5	1	80
24	1	1	0
		PROMEDIO	50.83

GUIA DE OBSERVACION			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCION	JR LIBERTAD NRO 667		
Mes	ENERO	**Año**	2021
INDICADOR ELIMINACION/MANIPULACION DE DATOS		**FORMULA INT= ((DE - EDC) / DE) x 100**	
Dia	**Num_datos eliminados**	**Num_datos eliminados que alteran la data de clientes**	**INT**
1	8	1	87.5
2	10	2	80
3	6	1	83.33
4	3	1	66.67
5	6	1	83.33
6	7	0	100
7	9	1	88.89
8	5	1	80
9	5	1	80
10	1	1	0
11	10	1	90
12	7	0	100
13	1	1	0
14	1	1	0
15	3	1	66.67
16	3	1	66.67
17	3	1	66.67
18	15	0	100
19	3	1	66.67
20	1	1	0
21	5	1	80
22	5	1	80
23	1	1	0
24	11	0	100
		PROMEDIO	56.93

GUIA DE OBSERVACION			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCION	JR LIBERTAD NRO 667		
Mes	DICIEMBRE	**Año**	2021
INDICADOR ELIMINACION/MANIPULACION DE DATOS		**FORMULA INT= ((DE - EDC) / DE) x 100**	
Dia	**Num_datos eliminados**	**Num_datos eliminados que alteran la data de clientes**	**INT**
1	9	3	66.67
2	8	5	37.5
3	9	2	77.78
4	10	5	50
5	8	4	50
6	8	3	62.5
7	8	3	62.5
8	8	2	75
9	11	6	45.45
10	9	8	11.11
11	9	4	55.56
12	2	2	0
13	10	4	60
14	2	0	100
15	3	1	66.67
16	5	1	80
17	5	2	60
18	7	0	100
19	7	1	85.71
20	10	2	80
21	8	0	100
22	1	0	100
23	10	1	90
24	10	4	60
		PROMEDIO	65.69

GUIA DE OBSERVACION			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCION	JR LIBERTAD NRO 667		
Mes	FEBRERO	**Año**	2021
INDICADOR DENEGACION DEL SERVICIO		**FORMULA ID= ((HD - HSS) / HD) x 100**	
Dia	**Num_horas por dia**	**Num_horas sin acceso**	**ID**
1	24	0.25	98.96
2	24	1	95.83
3	24	0	100
4	24	0.15	99.38
5	24	0.17	99.29
6	24	0.56	97.67
7	24	0	100
8	24	1	95.83
9	24	1.15	95.21
10	24	2.11	91.21
11	24	0	100
12	24	0.48	98
13	24	1	95.83
14	24	0.44	98.17
15	24	0.15	99.38
16	24	1.22	94.92
17	24	0.59	97.54
18	24	0.11	99.54
19	24	0.45	98.13
20	24	0.28	98.83
21	24	0	100
22	24	3.31	86.21
23	24	1.55	93.54
24	24	2.41	89.96
		PROMEDIO	96.81

GUIA DE OBSERVACION			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCION	JR LIBERTAD NRO 667		
Mes	ENERO	**Año**	2021
INDICADOR DENEGACION DEL SERVICIO		**FORMULA ID= ((HD - HSS) / HD) x 100**	
Dia	**Num_horas por dia**	**Num_horas sin acceso**	**ID**
1	24	0.03	99.88
2	24	0.45	98.13
3	24	3.25	86.46
4	24	1.46	93.92
5	24	0	100
6	24	0.18	99.25
7	24	3.33	86.13
8	24	1.00	95.83
9	24	2.22	90.75
10	24	1.11	95.38
11	24	1.00	95.83
12	24	0.18	99.25
13	24	0	100
14	24	1.54	93.58
15	24	1.00	95.83
16	24	0.22	99.08
17	24	0.37	98.46
18	24	0	100
19	24	0.32	98.67
20	24	1.00	95.83
21	24	0.11	99.54
22	24	1.48	93.83
23	24	1.26	94.75
24	24	0.00	100
		PROMEDIO	96.07

GUIA DE OBSERVACION			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCION	JR LIBERTAD NRO 667		
Mes	DICIEMBRE	**Año**	2021
INDICADOR DENEGACION DEL SERVICIO		**FORMULA ID= ((HD - HSS) / HD) x 100**	
Dia	**Num_horas por día**	**Num_horas sin acceso**	**ID**
1	24	0.25	98.96
2	24	0.51	97.88
3	24	1.1	95.42
4	24	0.1	99.58
5	24	4.35	81.88
6	24	2.36	90.17
7	24	0	100
8	24	1.25	94.79
9	24	1.56	93.5
10	24	0.25	98.96
11	24	0.41	98.29
12	24	0	100
13	24	0.41	98.29
14	24	1.44	94
15	24	0.15	99.38
16	24	1	95.83
17	24	1.25	94.79
18	24	0.39	98.38
19	24	0.2	99.17
20	24	2.33	90.29
21	24	0	100
22	24	0.37	98.46
23	24	0.45	98.13
24	24	0.1	99.58
		PROMEDIO	96.49

GUIA DE OBSERVACION			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCION	JR LIBERTAD NRO 667		
Mes	MARZO	**Año**	2021
INDICADOR DENEGACION DEL SERVICIO		**FORMULA ID= ((HD - HSS) / HD) x 100**	
Dia	**Num_horas por día**	**Num_horas sin acceso**	**ID**
1	24	0.15	99.38
2	24	0	100.00
3	24	0.05	99.79
4	24	0	100.00
5	24	0.17	99.29
6	24	0.25	98.96
8	24	0	100.00
9	24	0.08	99.67
10	24	0.35	98.54
11	24	0.18	99.25
12	24	0	100.00
13	24	0.35	98.54
15	24	0.55	97.71
16	24	0.22	99.08
17	24	0	100.00
18	24	0.2	99.17
19	24	0.59	97.54
20	24	0	100.00
22	24	0.15	99.38
23	24	0	100.00
24	24	0.14	99.42
25	24	0.25	98.96
26	24	0.15	99.38
27	24	0.19	99.21
		PROMEDIO	99.30

GUIA DE OBSERVACION			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCION	JR LIBERTAD NRO 667		
Mes	MARZO	**Año**	2021
INDICADOR ELIMINACION/MANIPULACION DE DATOS		**FORMULA INT= ((DE - EDC) / DE) x 100**	
Dia	**Num_datos eliminados**	**Num_datos eliminados que alteran la data de clientes**	**INT**
1	3	0	100.00
2	4	1	75.00
3	4	0	100.00
4	2	0	100.00
5	3	0	100.00
6	1	0	100.00
7	1	1	0.00
8	1	0	100.00
9	2	1	50.00
10	3	1	66.67
11	1	0	100.00
12	1	1	0.00
13	1	0	100.00
14	1	0	100.00
15	1	0	100.00
16	2	0	100.00
17	1	1	0.00
18	1	0	100.00
19	2	0	100.00
20	4	0	100.00
21	2	1	50.00
22	2	1	50.00
23	5	1	80.00
24	5	2	60.00
		PROMEDIO	76.32

GUIA DE OBSERVACION			
INVESTIGADOR	AGUINAGA QUISPE WILLIAM		
EMPRESA	CMAC AREQUIPA-AGENCIA CHACHAPOYAS		
DIRECCION	JR LIBERTAD NRO 667		
MES	MARZO	**AÑO**	2021
INDICADOR **ACCESOS NO AUTORIZADOS**		FORMULA IC= ((AS - ANA) / AS) x 100	
Dia	**Num_accesos al sistema**	**Num_accesos no autorizados**	**IC**
1	6	0.00	100.00
2	6	1.00	83.33
3	6	1.00	83.33
4	6	1.00	83.33
5	6	0.00	100.00
6	5	0.00	100.00
7	6	0.00	100.00
8	6	1.00	83.33
9	6	2.00	66.67
10	6	2.00	66.67
11	6	0.00	100.00
12	6	2.00	66.67
13	6	0.00	100.00
14	6	1.00	83.33
15	6	1.00	83.33
16	6	0.00	100.00
17	6	2.00	66.67
18	5	1.00	80.00
19	6	0.00	100.00
20	6	0.00	100.00
21	6	0.00	100.00
22	6	1.00	83.33
23	6	1.00	83.33
24	6	1.00	83.33
		PROMEDIO	87.36

ANEXO C: Ficha de juicio de expertos

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Estrada Aro Marcelino
Titulo/Grado: Ing. de Sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

DIMENSION: Integridad
FORMULA: INT= ((DE - EDC) / DE) x 100

INT : Indicador de eliminación/manipulación de datos
DE : Núm. de documentos eliminados/manipulados
EDC : Núm. de documentos que alteran la data de clientes

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, en base a una serie de interrogantes marcando un valor porcentual, del mismo modo, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

Ítems	Preguntas	Deficiente (0-20%)	Regular (21-50%)	Bueno (51-70%)	Muy Bueno (71-80%)	Excelente (81-100)
1	¿El instrumento de medición cumple con el diseño adecuado?				80%	
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?				80%	
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?				80%	
5	¿El instrumento examina los datos de la empresa?				80%	
6	Los efectos del instrumento son entendibles para ser analizado correctamente				80%	
Total					80%	

Recomendaciones:

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Estrada Aro Marcelino

Titulo/Grado: Ing. de Sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

DIMENSION: Confidencialidad
FORMULA: IC= ((AS - ANA) / AS) x 100

IC : Indicador de accesos no autorizados
AS : Núm. de accesos al sistema
ANA : Núm. de accesos no autorizados

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, en base a una serie de interrogantes marcando un valor porcentual, del mismo modo, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

Ítems	Preguntas	Deficiente (0-20%)	Regular (21-50%)	Bueno (51-70%)	Muy Bueno (71-80%)	Excelente (81-100)
1	¿El instrumento de medición cumple con el diseño adecuado?				80%	
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?				80%	
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?				80%	
5	¿El instrumento examina los datos de la empresa?				80%	
6	Los efectos del instrumento son entendibles para ser analizado correctamente				80%	
Total					80%	

Recomendaciones:

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Estrada Aro Marcelino

Titulo/Grado: Ing., de Sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÒN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

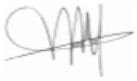
DIMENSION: Disponibilidad
FORMULA: IC= ((HD - HSS) / HD) x 100

IC : Indicador de denegación del servicio
HD : Núm. de horas por día
HSS: Núm. de horas sin acceso a la información

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, en base a una serie de interrogantes marcando un valor porcentual, del mismo modo, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

ítems	Preguntas	Deficiente (0-20%)	Regular (21-50%)	Bueno (51-70%)	Muy Bueno (71-80%)	Excelente (81-100)
1	¿El instrumento de medición cumple con el diseño adecuado?				80%	
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?				80%	
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?				80%	
5	¿El instrumento examina los datos de la empresa?				80%	
6	Los efectos del instrumento son entendibles para ser analizado correctamente				80%	
Total					80%	

Recomendaciones:



UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Estrada Aro Marcelino
Titulo/Grado: Ing. de Sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÒN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

Ítems	Preguntas	METODOLOGIAS		
		ISO 27001	COBIT	MAGERIT
1	¿El instrumento de medición cumple con el diseño adecuado?	1	2	2
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?	1	2	2
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?	1	2	2
5	¿El instrumento examina los datos de la empresa?	1	2	2
6	Los efectos del instrumento son entendibles para ser analizado correctamente	1	2	2
Total		5	10	10

Escala a evaluar es 1. Bueno 2. Regular 3. Malo

Recomendaciones::

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Rivera Crisóstomo Reneé

Titulo/Grado: Ing. de Sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

DIMENSION: Confidencialidad
FORMULA: IC= ((AS - ANA) / AS) x 100

IC : Indicador de accesos no autorizados
AS : Núm. de accesos al sistema
ANA : Núm. de accesos no autorizados

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, en base a una serie de interrogantes marcando un valor porcentual, del mismo modo, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

ítems	Preguntas	Deficiente (0-20%)	Regular (21-50%)	Bueno (51-70%)	Muy Bueno (71-80%)	Excelente (81-100)
1	¿El instrumento de medición cumple con el diseño adecuado?				80%	
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?				80%	
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?				80%	
5	¿El instrumento examina los datos de la empresa?				80%	
6	Los efectos del instrumento son entendibles para ser analizado correctamente				78%	
	Total				80%	

Recomendaciones:

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Rivera Crisóstomo Reneé

Titulo/Grado: Ing. de Sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

DIMENSION: Integridad
FORMULA: INT= ((DE - EDC) / DE) x 100

INT : Indicador de eliminación/manipulación de datos
DE : Núm. de documentos eliminados/manipulados
EDC : Núm. de documentos que alteran la data de clientes

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, en base a una serie de interrogantes marcando un valor porcentual, del mismo modo, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

Ítems	Preguntas	Deficiente (0-20%)	Regular (21-50%)	Bueno (51-70%)	Muy Bueno (71-80%)	Excelente (81-100)
1	¿El instrumento de medición cumple con el diseño adecuado?				80%	
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?				80%	
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?				78%	
5	¿El instrumento examina los datos de la empresa?				80%	
6	Los efectos del instrumento son entendibles para ser analizado correctamente				80%	
Total					80%	

Recomendaciones:

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Rivera Crisóstomo Reneé

Titulo/Grado: Ing. de Sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

DIMENSION: Disponibilidad
FORMULA: IC= ((HD - HSS) / HD) x 100

IC : Indicador de denegación del servicio
HD : Núm. de horas por día
HSS: Núm. de horas sin acceso a la información

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, en base a una serie de interrogantes marcando un valor porcentual, del mismo modo, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

Ítems	Preguntas	Deficiente (0-20%)	Regular (21-50%)	Bueno (51-70%)	Muy Bueno (71-80%)	Excelente (81-100)
1	¿El instrumento de medición cumple con el diseño adecuado?				80%	
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?				80%	
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?				80%	
5	¿El instrumento examina los datos de la empresa?				80%	
6	Los efectos del instrumento son entendibles para ser analizado correctamente				80%	
	Total				80%	

Recomendaciones:

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Rivera Crisóstomo Reneé

Titulo/Grado: Ing. de Sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

ítems	Preguntas	METODOLOGIAS		
		ISO 27001	COBIT	MAGERIT
1	¿El instrumento de medición cumple con el diseño adecuado?	1	2	2
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?	1	2	3
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?	1	2	2
5	¿El instrumento examina los datos de la empresa?	1	3	2
6	Los efectos del instrumento son entendibles para ser analizado correctamente	1	2	2
Total		5	11	11

Escala a evaluar es 1. Bueno 2. Regular 3. Malo

Recomendaciones:

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Vásquez Valencia Yesenia

Titulo/Grado: Ing. de sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

DIMENSION: Confidencialidad
FORMULA: IC= ((AS - ANA) / AS) x 100

IC : Indicador de accesos no autorizados
AS : Núm. de accesos al sistema
ANA : Núm. de accesos no autorizados

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, en base a una serie de interrogantes marcando un valor porcentual, del mismo modo, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

ítems	Preguntas	Deficiente (0-20%)	Regular (21-50%)	Bueno (51-70%)	Muy Bueno (71-80%)	Excelente (81-100)
1	¿El instrumento de medición cumple con el diseño adecuado?				80%	
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?				80%	
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?				80%	
5	¿El instrumento examina los datos de la empresa?				80%	
6	Los efectos del instrumento son entendibles para ser analizado correctamente				80%	
Total					80%	

Recomendaciones: El instrumento es aplicable

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Vásquez Valencia Yesenia

Titulo/Grado: Ing. de sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

DIMENSION: Disponibilidad
FORMULA: IC= ((HD - HSS) / HD) x 100

IC : Indicador de denegación del servicio
HD : Núm. de horas por día
HSS: Núm. de horas sin acceso a la información

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, en base a una serie de interrogantes marcando un valor porcentual, del mismo modo, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

Ítems	Preguntas	Deficiente (0-20%)	Regular (21-50%)	Bueno (51-70%)	Muy Bueno (71-80%)	Excelente (81-100)
1	¿El instrumento de medición cumple con el diseño adecuado?				80%	
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?				80%	
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?				80%	
5	¿El instrumento examina los datos de la empresa?				80%	
6	Los efectos del instrumento son entendibles para ser analizado correctamente				80%	
	Total				80%	

Recomendaciones: El instrumento es aplicable

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Vásquez Valencia Yesenia

Titulo/Grado: Ing. de sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

DIMENSION: Integridad
FORMULA: INT= ((DE - EDC) / DE) x 100

INT : Indicador de eliminación/manipulación de datos
DE : Núm. de documentos eliminados/manipulados
EDC : Núm. de documentos que alteran la data de clientes

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, en base a una serie de interrogantes marcando un valor porcentual, del mismo modo, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

Ítems	Preguntas	Deficiente (0-20%)	Regular (21-50%)	Bueno (51-70%)	Muy Bueno (71-80%)	Excelente (81-100)
1	¿El instrumento de medición cumple con el diseño adecuado?				80%	
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?				80%	
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?				80%	
5	¿El instrumento examina los datos de la empresa?				80%	
6	Los efectos del instrumento son entendibles para ser analizado correctamente				80%	
	Total				80%	

Recomendaciones: El instrumento es aplicable

UNIVERSIDAD CÉSAR VALLEJO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Vásquez Valencia Yesenia

Titulo/Grado: Ing. de sistemas

Universidad que labora: Universidad Cesar Vallejo Lima-Norte

TESIS: SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO/IEC: 27001:2013 PARA LA SEGURIDAD DE LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCION FINANCIERA, CHACHAPOYAS, AMAZONAS

Por medio de la tabla de evaluación de expertos, Ud. tiene la autoridad de calificar el instrumento que se usará, se exhorta a la corrección de los ítems puntualizando sus observaciones y/o sugerencias, cuyo fin sea mejorar la relación del instrumento.

ítems	Preguntas	METODOLOGIAS		
		ISO 27001	COBIT	MAGERIT
1	¿El instrumento de medición cumple con el diseño adecuado?	3	2	2
3	¿El instrumento de recopilación de datos, tiene concordancia con las variables del estudio?	3	2	2
4	¿El instrumento de recopilación de datos, ayudará al éxito de los objetivos del estudio?	3	2	2
5	¿El instrumento examina los datos de la empresa?	3	2	2
6	Los efectos del instrumento son entendibles para ser analizado correctamente	3	2	2
Total		15	10	10

Escala a evaluar es 1. Bueno 2. Regular 3. Malo

Recomendaciones: La metodología es aplicable

ANEXO D: DESARROLLO DEL PROYECTO SISTEMA DE GESTION BASADO EN LA NORMA ISO/IEC 27001:2013 PARA LA SEGURIDAD DE LA INFORMACION EN UNA INSTITUCIÓN FINANCIERA

La disciplina denominada seguridad de la información ha evolucionado con mayor rapidez los últimos años en el campo de las TIC, con el objetivo principal de protegerla de causas accidentales o provocadas, hacerla en sus 3 dimensiones: Disponibilidad, integridad y confidencialidad.

Como un enfoque más completo hablar del Sistema de gestión de seguridad de la información que no solo abarca problemas tecnológicos y sus debilidades, amenazas e incidencias, sino más bien amplía el campo abordando otros aspectos como: normativos, organizativos, legales concebidos desde la visión de problema de negocio.

En esta experiencia dentro de una institución financiera, en la que se plantea un enfoque de mejora continua del ciclo Deming, que la Norma internacional lo adopta como parte de implantación a sus controles, los que direccionan el logro de resultados exitosos. Esta estructura compuesta por 114 controles, 35 objetivos de control y 14 dominios se dividen en controles estratégicos, tácticos y operativos, las cuales se aprecian en la figura 4:

1. Objetivo

a. Seleccionar controles de la ISO/IEC 27001:2013 a aplicarse en base a la necesidad de la organización.
b. Establecer formatos de confidencialidad. Check list, aprobación y comunicación de los efectos de controles, políticas, procedimientos, niveles de riesgos, roles y responsabilidades al recurso humano del nivel operativo de una institución financiera.

2. Alcance

La presente propuesta se delimitará en la protección de activos lógicos, físicos y de información que pertenecen al proceso crediticio de una institución financiera en financiera. Esta investigación se adapta a la necesidad de la empresa en la cual se identificaron vulnerabilidades y amenazas que se controlaran con el sistema de gestión basándose en la norma internacional ISO 27001:2013.

3. Usuarios

MIEMBROS DE ALTA DIRECCION	
ROL	**NOMBRE**
Gerente de agencia	Armando García Montenegro
Recursos humanos	Renzo Fabricio Agurto Granda
Jefe de soporte de TI	Ricardo Moran

EQUIPO DEL PROYECTO SGSI
Usuarios (Analistas de créditos)
Oficial de seguridad de la información (jefe de soporte de TI)

a. Documentos de referencia

ISO/IEC 27001: 2013

NTP/ISO 27001:2014

Ley de protección de datos personales

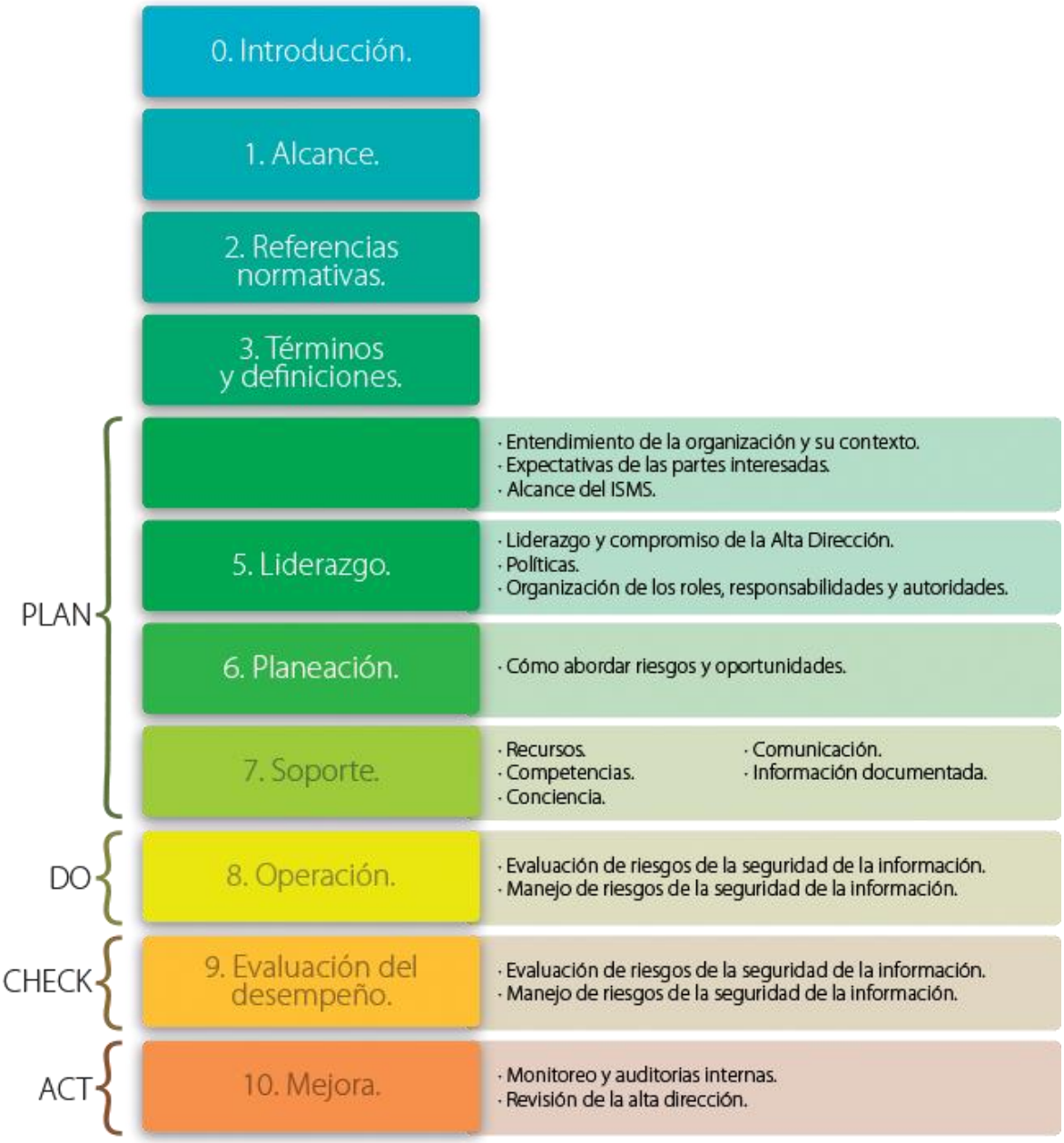


Figura 4: Estructura de la ISO/IEC 27001:2013

1. Propuesta del SGSI

a. Objetivo del proyecto

Documentar la propuesta en conformidad con la ISO/IEC 27001:2013

b. Entregables del proyecto

Durante la implementación de la propuesta, los entregables se clasificaron de la siguiente forma:

Alcance: documento que define el alcance del SGSI, tomando en cuenta procesos, funciones, activos, partes interesadas de la organización.

Política de seguridad: documento que describe la forma en como la dirección gestionará la seguridad de la información.

Guía para control de documentos y registros: describir la manera de redactar los documentos, títulos, letras, encabezado y otros detalles que lo conformen.

Identificación de amenazas y vulnerabilidades: se evalúa el nivel de riesgo y se asigna un responsable.

Plan de tratamiento del riesgo: documento que detalla controles de seguridad para cada tipo de riesgo como evidencia de su tratamiento.

2. Alcance del sistema de seguridad de la información

2.1. Naturaleza de la organización

La Caja Municipal de ahorro y crédito Arequipa, es una institución financiera inclusiva líder que viene beneficiando a mas 1, 800,000 clientes ofreciendo productos y servicios financieros para todas las necesidades de la población, y promoviendo el ahorro, lo que la ha convertido en indiscutible líder de la categoría.

Hoy en día cuenta con 160 agencias, distribuidas en todo el país y una creciente red de atención que asciende a más de 1,092 Agentes Caja Arequipa, más de 164 cajeros automáticos propios, 10,276 agentes kasnet a nivel nacional, así como 445 cajeros de la Red Unicard en Lima, Callao y el norte del país

2.2. Misión

Lograr la inclusión financiera sustentable de personas y empresarios durante su ciclo de vida, brindando una experiencia cercana, ágil e integral.

2.3. Visión

Liderar el desarrollo integral de los clientes, reconociendo su diversidad, para ser su opción preferida en soluciones financieras, fortaleciendo nuestro talento, innovando y usando tecnologías digitales.

2.4. Valores: Caja con sentido

Apasionados por la Innovación: Es la Caja más innovadora de Perú. Buscando siempre estar a la vanguardia de la industria microfinanciera. Promueve el aprendizaje y explora nuevas oportunidades. Celebra la creatividad y recibe con mente abierta ideas y propuestas innovadoras, porque nuestra apertura al cambio y a la mejora sea permanente.

Motivados por transformar vidas: facilitadores de sueños en la vida de sus clientes. Toman decisiones con responsabilidad y empatía. Reconocen que sus acciones del día a día tienen un impacto en sus clientes y comunidad.

Imparables ante las metas: Esfuerzo para triunfar y para hacer realidad sus planes. Trabajan para ser exitosos, alcanzar sueños y objetivos. El esfuerzo está entrelazado; como Caja Arequipa, es más que la suma de cada uno.

Íntegramente Humanos: honestos, sinceros y transparentes en sus interacciones entre compañeros y clientes. Toman decisiones con responsabilidad, conciencia y moralidad. Lideran con el ejemplo y valoran el potencial humano de sus colaboradores.

Profundamente Orgullosos: Portavoces más apasionados de la marca, de su historia y trayectoria. Vestir con orgullo el uniforme, y presentan siempre lo mejor en acciones e interacciones.

Figura 5 : Lineamientos estratégicos 2019-2023

3. Comprensión de las necesidades y expectativas de las partes involucradas

Las partes importantes al SGSI son:

Personal: colaboradores de la agencia chachapoyas a los cuales se le asignan responsabilidades de activos y deben cumplir estricta seguridad de los mismos en la empresa.

Clientes: personas que requieren acceso a información de productos, tasas y tarifarios, pagos anticipados y amortizaciones.

Competidores: con la seguridad de la información se adquiere ventaja competitiva y de imagen institucional.

4. Inventario de equipos

Inventario de activos físicos – Agencia Chachapoyas

	Áreas		
Activos físicos	**Créditos**	**Operaciones**	**Total**
Pc	7	3	10
Laptop	-	-	-
Impresora	1	1	2
Switch	1	1	2
Estabilizador	7	3	10
Access point	1	1	2
Tv	1	1	2
Cámara video vigilancia	1	3	4
Equipos móviles	7	1	8

Inventario de activos lógicos – Agencia Chachapoyas

Activos lógicos	Descripción
Programa informático	Microsoft office 2016 Google Chrome 90.0.4430.66 Internet Explorer 11 Adobe Reader
Sistema operativo	Windows 10 home
Sistemas	Sistema de consultas Reniec Sistema de consultas Sunat Sistema de consultas Sunarp Sistema de consultas Essalud Sistema Bantotal
Internet	Línea claro
Aplicaciones móviles	Data entry Misti

Inventario de activos lógicos – Agencia Chachapoyas

N°	**Activos de información**
1	Copias dni
2	Copias documento de propiedad
3	Copias separación matrimonial
4	Copias licencia municipal
5	Declaración jurada de servicios
6	Copias carta no adeudo
7	Copias cronograma de créditos
8	Copias baucher de cancelación
9	Contratos de trabajo
10	Boletas de pago
11	Libro de actas
12	Información de empresas (ruc, pdt, vigencia, constitución)
13	Certificados médicos
14	Convenios
15	Actas de defunción
16	Cartas poder
17	Numero de cuentas
18	Data de clientes inactivos y vigentes
19	Fotografías

5. Políticas de seguridad de la información

Política de uso de los activos físicos
a) El personal que recepciona un equipo móvil es responsable de su cuidado. b) Evitar realizar la carga en instalaciones donde hay contacto con los clientes. c) Se prohíbe el uso de los tv para cualquier uso distinto a las exposiciones gerenciales d) La revisión de cámaras ante cualquier incidente estará a cargo del gerente de agencia. e) Transpórtalo consigo durante toda la jornada laboral. f) No se alterará la configuración ya establecida. g) Se prohíbe el uso de aplicaciones que alteren su rendimiento. h) En caso de pérdida o robo, comunicarse de inmediato i) Correcto encendido y apagado en toda la jornada laboral j) Se prohíbe la ingesta de comidas y bebidas en las estaciones de trabajo k) Todos los equipos móviles e informáticos serán de uso exclusivo para actividades empresariales y no de terceros.

Política de uso de los activos lógicos
a) Los sistemas informáticos serán de uso exclusivo de la organización y no personales. b) Se prohíbe cualquier intento de configuración distinta a la establecida c) En caso de fallas u otro incidente, comunicarse vía correo institucional antes de manipular a su criterio.

Política de uso de los activos de información
a) Cada analista es responsable de la información asignada. b) No se divulgará ni se prestará a terceros, tampoco es de uso personal en actividades de jornada no laboral. c) Almacenar correctamente en los estantes asignados d) Se prohíbe circular información difamatoria ya sea de persona natural o jurídica. e) La copia de algún documento se debe solicitar por correo al analista responsable f) g) Realizar el arqueo de expedientes los primeros días de cada mes sin excepción h) En caso de pérdida comunicar a la gerencia.

Política de control de accesos
a) Definir roles de usuario en función a su área de trabajo b) Definir permisos necesarios para que cada usuario realice acciones oportunas sobre el crédito otorgado c) La clave de acceso tendrá un periodo de validez por 15 días y de uso personal estricto. d) Las claves estarán compuestas por letras y caracteres especiales, mínimo 8 dígitos que no serán escritos en ningún medio. e) El oficial de seguridad es el encargado de configurar las claves de acceso y asignarlas. El olvido de las mismas gestionar por correo su recuperación. f) Los colaboradores deben bloquear sus equipos de trabajo inmediatamente al salir del escritorio

Política de control de servicios móviles e informáticos
a) Solo se permite usar la aplicación de WhatsApp y de la organización, cualquier otra aplicación de comunicación o entretenimiento estará denegada. b) Denegar el acceso a redes sociales y juegos por los navegadores c) El wifi y blooetooth estará deshabilitado d) Esta denegado la instalación de programas por los usuarios e) Acceso restringido a descargas de programas f) Todos los programas a utilizar por los usuarios deben estar licenciados

Protección contra amenazas externas e internas
a) Se debe capacitar a los colaboradores con simulacros ante desastres naturales b) Se prohíbe la realización de cualquier evento a cargo del área comercial, para este fin solo está permitido el área de operaciones dentro de las instalaciones. c) Sensibilizar al personal sobre el cumplimiento de políticas y eventos para prevenir eventos indeseables. d) Dotar de estantes suficientes para el personal de créditos que permitan accesar a la data de clientes activos e inactivos. e) El acceso a los economatos solo está permitido a la gerencia y jefe de plataforma. f) La información impresa que no se utilice debe ser desechada en el lugar indicado

Protección de información de registros
a) Las unidades de almacenamiento para estos registros deben estar correctamente protegidas contra adulteración y el acceso no autorizado b) Los documentos deben estar agrupados por tipo de información c) Cualquier evento como falla y excepciones será derivado al oficial de seguridad de la información. d) Las carpetas con información importante deben estar almacenadas bajo el nombre de analista responsable. e) Los eventos realizados en esta sección serán registrados por el oficial de seguridad de la información.

Acuerdos de transferencia de información
a) el gerente de agencia solo está permitido para la transferencia de información. b) No se revela información de clientes y el estado de su crédito a ningún agente externo a la organización c) Esta denegado el uso de dispositivos de almacenamiento. d) No realizar copias de data de clientes vigentes e inactivos sin autorización e) El uso inapropiado de las cuentas es sancionado de acuerdo a la ley servir N° 30057

6. Gestión de incidentes de seguridad de la información

a) Responsabilidades y procedimientos
Los colaboradores de la agencia chachapoyas conocen las responsabilidades y roles de los encargados de la seguridad de la información.

b) Reporte de eventos de seguridad de la información.
Si el colaborador reconoce un ataque a los activos de la entidad, deberá reportarla al oficial de seguridad de la información por correo o en forma directa.

c) Reporte de eventos de seguridad de la información.

Se registra el incidente, precisando hora y fecha, involucrados y el contexto de lo ocurrido.

d) Evaluación y decisión sobre eventos ocurridos.

El oficial de seguridad de la información vela por la solución a los incidentes presentados.

Evaluar el tipo de evento, los activos afectados, probabilidad de expansión y los posibles daños que ocurra.

La evaluación de los eventos tomará en cuenta la clasificación de los activos.

El oficial deberá identificar el nivel de riesgo en la matriz de evaluación de riesgos

e) Respuestas a los incidentes.

Se procederá de acuerdo al plan de acción preestablecido a cada riesgo identificado

El encargado de implementar el plan debe priorizar el tiempo, recursos necesarios y herramientas existentes.

f) Recolección de evidencias

Número de incidentes presentados
Tiempo asignado para los incidentes
Daños provocados
Cantidad de activos de información involucrados
Frecuencia de incidencias
Causa de incidencias
Acciones preventivas y correctivas

g) Aspectos de seguridad de la información en la gestión de continuidad del negocio.

Identificar los activos críticos del negocio

Identificar los eventos causantes de las interrupciones en los procesos de negocio

Analizar la posibilidad de ocurrencia y el impacto de las interrupciones provocadas.

Identificar los controles preventivos y planes de acción

Determinar políticas, restricciones y buenas practicas

h) Implementación de la continuidad de la seguridad de la información

Identificar servicios y recursos de restauración

Identificar perdida aceptable de información y servicios

Fijar procedimientos a seguir para la recuperación de los procesos de negocio

Capacitar al personal en los procesos acordados

Realizar revisiones y actualizaciones periódicamente de los planes

Los efectos deben ser comunicados y documentados

i) Revisión independiente de la seguridad de la información

Revisar los objetivos de control, políticas, procedimientos de manera trimestral o cuando sucedan cambios significativos en la seguridad de la información de acuerdo al check list de la propuesta.

El oficial de la seguridad de la información esta a cargo de las revisiones del sistema de gestión de seguridad de la información.

j) Cumplimiento de políticas y normas de seguridad de la información

Se debe sensibilizar y capacitar al colaborador para el cumplimiento del SGSI

El cumplimiento de políticas aprobadas por la alta dirección tiene carácter obligatorio

El incumplimiento a estas políticas deberá ser causal de una sanción

Debe existir un incentivo para los colaboradores que cumplan y apoyen las políticas de seguridad de la información

7. Procedimiento de control de documentos

La presentación de los documentos tiene el siguiente formato:

Papel: A4

Tipo y tamaño de letra: Arial 12

Encabezado de tablas: Arial 12 en negrita

Márgenes:

Superior: 2.5 cm

Inferior: 3 cm

Derecho: 2.5 cm

Izquierdo: 3 cm

7.1. Políticas de seguridad de la información

Todas las políticas establecidas en el SGSI, deben ser aceptadas en el siguiente formato:

AGENCIA CHACHAPOYAS			
Formato de aprobación de políticas de seguridad de la información			
1. Datos generales	Fecha de solicitud: __/__/__		
Nombre completo del colaborador:			
Área de trabajo:			
Ocupación laboral:			
Descripción de política y N°:			
2. **Aprobación de la alta dirección**: ( ) Si ( ) No			
En caso de rechazo especifique:			
Rol	**Nombre**	**Fecha**	**Firma/sello**
Gerente de agencia	Armando García Montenegro		
Recursos humanos	Renzo Agurto Granda		
Jefe de soporte de TI	Ricardo moran		

En caso de modificación, se adopta el siguiente formato, el mismo que será comunicado.

AGENCIA CHACHAPOYAS			
Formato de modificación de políticas de seguridad de la información			
1. Datos generales	Fecha de solicitud: __/__/__		
Nombre completo del colaborador:			
Área de trabajo:			
Ocupación laboral:			
Descripción de política y N°: (política a actualizar), indicar el número de modificaciones.			
Motivo:			
Rol	**Nombre**	**Fecha**	**Firma/sello**
Gerente de agencia	Armando García Montenegro		
Recursos humanos	Renzo Agurto Granda		
Jefe de soporte de TI	Ricardo moran		

7.2. Organización de la seguridad de la información

a) Roles y responsabilidades

Rol	Responsabilidad
Usuario	Cualquier colaborador CMAC AREQUIPA-Agencia Chachapoyas
Oficial de seguridad de la información	Diseña, implanta y controla mecanismos de verificación y las herramientas requeridas para la medición de la efectividad de los controles implantados en el SGSI.

7.3. Responsabilidades de gerencia

El gerente de agencia debe comprometerse con el SGSI, para tal efecto lleva a cabo las siguientes funciones:

a. Designa recursos idóneos para el desarrollo del SGSI
b. Revisa periódicamente el SGSI
c. Garantiza que se realicen auditorías internas
d. Garantiza el cumplimiento de planes y objetivos del SGSI

7.4. Educación y capacitación sobre la SI

Los colaboradores de la agencia chachapoyas deben desarrollar los cursos virtuales de capacitación sobre la seguridad de la información de forma obligatoria. A continuación, se detallan las temáticas:

a. Sistema de gestión de seguridad de la información
b. Estándares
c. Clasificación de activos
d. Amenazas, vulnerabilidades y riesgos
e. Políticas de seguridad
f. Prevención

7.5. Proceso sancionador

En este apartado se ha creído conveniente tomar el articulo N° 87 al N° 98 de la ley N° 30057 “Ley del servicio civil”, el cual describe todo el procedimiento sancionador, la determinación de faltas y sanciones aplicables:

a. Artículo N° 89: Amonestación en verbal o escrita
b. Artículo N° 90: Suspensión sin goce de remuneración desde un día hasta por doce meses y destitución.
a. Artículo N° 91: graduación de las faltas, la cual menciona que las sanciones deben corresponder a la magnitud de las faltas.

b. Artículo N° 92, hace mención a las autoridades competentes, las cuales son:

   El jefe del presunto infractor

   El jefe de recursos humanos o quien haga sus veces el titular de la entidad

c. Artículo N° 93, hacen mención a todo el procesamiento disciplinario
d. Artículo N° 96, medidas cautelares
e. Artículo N° 97, medidas correctivas
f. Artículo N° 98, registro de sanciones

8. Retorno de los activos

Se propone en el contrato de trabajo, la devolución de activos de información que tienen en su posesión durante la permanencia y duración del mismo, en la siguiente acta:

Agencia Chachapoyas		Acta de devolución de activos N°	
1. Datos del colaborador		Fecha:	__/__/__
Nombre completo:			
Cargo:		Área:	
Función:			
Activos que entrega:			
2. Datos del gerente que recepciona			
Nombre completo:			
Observaciones:			
_____ Entrega conforme		_____ Recibe conforme	

9. Gestión de accesos

9.1. Registro y baja de usuarios

En este control se establece el siguiente proceso

N°	Actividad	Descripción	Encargado
1	Registro, modificación o baja de usuarios	El colaborador solicita mediante correo institucional indicando esta necesidad	Oficial de seguridad de la información
2	Registra solicitud	El oficial deberá registrarla como evidencia de su decisión en la que autoriza o rechaza	
3	Toma de decisión	Si aprueba la solicitud, este debe identificar el tipo de usuario con su permiso correspondiente	
4	Configuración correspondiente	De hacer el registro de un nuevo usuario, se asigna una clave y se conceden los permisos de acuerdo a sus funciones. Para modificar se alteran los permisos y en una baja de usuarios se deben eliminar esos permisos	
5	Comunicación de resultados	Una vez terminado el proceso se debe informar al usuario vía correo institucional	

9.2. Gestión de derechos de acceso privilegiado

<table>
<tr><td colspan="2">Agencia chachapoyas</td><td colspan="3">Revisión de accesos privilegiados</td></tr>
<tr><td colspan="2">N°:</td><td colspan="3">Fecha:</td></tr>
<tr><td colspan="5">Área:</td></tr>
<tr><td colspan="5">Usuario:</td></tr>
<tr><td colspan="5">Puesto:</td></tr>
<tr><td rowspan="2">N°</td><td rowspan="2">Lista de accesos</td><td colspan="3">Cumple</td></tr>
<tr><td>Si</td><td colspan="2">No</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="5">Observaciones:</td></tr>
<tr><td colspan="5">

_____
Responsable</td></tr>
</table>

9.3. Revisión de derechos de accesos

<table>
<tr><td colspan="2">Agencia chachapoyas</td><td colspan="3">Check list de accesos</td></tr>
<tr><td colspan="2">N°:</td><td colspan="3">Fecha:</td></tr>
<tr><td colspan="5">Área:</td></tr>
<tr><td colspan="5">Usuario:</td></tr>
<tr><td colspan="5">Puesto:</td></tr>
<tr><td rowspan="2">N°</td><td rowspan="2">Lista de accesos</td><td colspan="3">Restringido</td></tr>
<tr><td>Si</td><td colspan="2">No</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="5">Observaciones:</td></tr>
<tr><td colspan="5">

_____
Responsable</td></tr>
</table>

10. Mantenimiento de equipos

a) Preventivo

El oficial de seguridad de la información gestión el mantenimiento de equipos a través del siguiente check list:

Check list de mantenimiento preventivo de equipos informáticos			
Ordenador N°	Área:	Fecha:	
CPU			
N°	Indicaciones	Cumple	
1	Eliminar exceso de polvo		
2	Tarjetas bien conectadas		
3	Fuente poder en modo silencioso		
4	Cable bien conectado y en buen estado		
TECLADO			
N°	Indicaciones	Cumple	
1	Eliminar exceso de polvo		
2	Teclas completas y en buen estado		
4	Cable bien conectado y en buen estado		
Ratón			
N°	Indicaciones	Cumple	
1	Funciona el click izquierdo		
2	Funciona el click derecho		
5	Cables bien conectados y en buen estado		
Pantalla			
N°	Indicaciones	Cumple	
1	Pantalla limpia		
2	Presenta rayaduras		
5	Cable bien conectado y en buen estado		
_____ Responsable			

b) Correctivo

Es el procedimiento de reparación de daños encontrados por el usuario o por detención temprana, las actividades son las siguientes:

Verificar el estado físico del equipo y sus periféricos

Realizar test de diagnósticos para comprobar daños

Realizar ajustes, limpieza e inspección de los equipos que lo requieran

De requerir algún cambio en sus partes, contactar al proveedor correspondiente para su reposición inmediata

Se registran los incidentes de seguridad

El mantenimiento está a cargo del Oficial de SI, tiene consigo un check list con las características de los equipos

11. Gestión del cambio

Agencia chachapoyas	**Acta de gestión de cambios N°**		
Lugar:			fecha: __/__/___
1. Datos generales			
Nombre del solicitante:			
Cambio requerido:			
Prioridad	Alta ( )	Media ( )	Baja ( )
2. Aprobación			
Si ( ) No ( )			
En caso de rechazo, especifique:			

ROL	NOMBRE	FECHA	FIRMA
Gerente de agencia	Armando García Montenegro		
Recursos humanos	Renzo Agurto Granda		
Jefe de soporte de TI	Ricardo moran		

12. Acuerdo de confidencialidad

ACUERDO DE CONFIDENCIALIDAD
Mediante el presente documente, el suscrito declara que yo, _____identificado con DNI _____, declaro que presto servicios a la CMAC AREQUIPA. AGENCIA CHACHAPOPYAS
1. CONFIDENCIALIDAD
El colaborador se compromete ante esta entidad, no revelar, divulgar, facilitar bajo ninguna de las formas, a no utilizar para su propio beneficio o el de cualquier otro individuo toda información relacionada a sus funciones, como también las políticas y/o cualquier otra información vinculada con la dirección. También se compromete a cumplir con las siguientes pautas y acepta lo indicado por las políticas de control de accesos proporcionada por el área de soporte de T, área encargada de asegurar la confidencialidad de la información y buen uso de los recursos informáticos. a. Es responsable de las acciones que realiza su usuario b. Solo podrá utilizarla con fines relacionados de sus funciones c. Debe usar contraseñas seguras y en secreto d. No se puede eliminar, editar, registrar demás recursos solicitados e. Divulgar información a través de canales no autorizados
2. SANCIÓN
Queda expreso de su conocimiento que todo incumplimiento total o parcial en relación a las obligaciones de confidencialidad sumidas en el presente documento, CMAC AREQUIPA, podrá actuar de acuerdo a ley.
_____ Firma de Usuario Chachapoyas, _____de_____del 20___

13. Identificación de vulnerabilidades

Tipo de activo involucrado	Riesgo	Vulnerabilidades
Activos de información	Acceso no autorizado	Claves débiles de seguridad
	Divulgación de información	Carece de acuerdos de confidencialidad
	Abuso de privilegios	Cuentas sin permisos establecidos
	Fuga de información	Falta de back up
	Alteración de información	Escasos controles de seguridad
Equipos informáticos	Error de configuración de equipos	Aplicación incorrecta del manual de configuración
	Abuso de privilegios	Falta de restricción en los servicios de red
	Acceso denegado	Usuarios abiertos sin cerrar sesión Prestación de usuarios a terceros
	Manipulación de equipos	Falta de planes de acción
	Daños por agua	Ingesta de bebidas cerca de los equipos Ausencia de políticas de seguridad
Equipos de red	Saturación de la red	Infraestructura inadecuada

	Acceso no autorizado	Falta de controles de red
	Alteración en los puertos de conectividad	Falta de puertos identificados por los equipos
	Virus	Usuarios con acceso libre a internet Ausencia de controles de acceso
Software	Instalación de software no autorizado	Carencia de controles de red Abuso de privilegios
	Denegación de servicios	Saturación del servidor principal

14. Identificación de vulnerabilidades

Para evaluar el riesgo se utilizó la metodología Magerit:

Escala			
Impacto	Probabilidad	Riesgo	Valor cuantitativo
MA: Muy alto	Seguro	Critico	5
Alto: alto	Probable	Importante	4
M: Medio	posible	Apreciable	3
B: bajo	Poco probable	Bajo	2
MB: Muy bajo	Muy raro	Despreciable	1

Evaluación de riesgos

N°	Riesgo	Probabilidad	Responsable	Valor de impacto			Total de valoración	Nivel de riesgo	Acciones correctivas
				D	C	I			
1	Acceso no autorizado	5	Jefe de soporte	5	5	5	5	Critico	Mitigar
2	Divulgación de información	5	Colaborador	5	5	5	5	Critico	Mitigar
3	Abuso de privilegios	4	Jefe de soporte	3	3	4	3	Apreciable	Mitigar
4	Fuga de información	4	colaborador	5	4	5	5	Critico	Mitigar
5	Alteración de información	4	Colaborador	5	4	4	4	Importante	Mitigar
6	Error de configuración de equipos	2	Jefe de soporte	3	3	2	3	Apreciable	Mitigar
7	Abuso de privilegios	2	Jefe de soporte	2	3	3	3	Apreciable	Mitigar
8	Acceso denegado	2	Jefe de soporte	4	5	5	4	Importante	Mitigar
9	Manipulación de equipos	4	Colaborador	3	3	3	3	Apreciable	Mitigar
10	Daños por agua	3	Colaborador	4	4	3	4	Importante	Mitigar
11	Saturación de la red	3	Jefe de soporte	5	4	4	4	Importante	Mitigar
12	Acceso no autorizado a la red	3	Jefe de soporte	3	5	4	4	Importante	Mitigar
13	Alteración en los puertos de conectividad	2	Jefe de soporte	2	3	3	3	Apreciable	Mitigar
14	Virus	2	Jefe de soporte	2	1	2	2	Bajo	Aceptar

15	Instalación de software no autorizado	3	Jefe de soporte	2	1	1	1	Despreciable	Aceptar
16	Denegación de servicios	4	Gerente de agencia	4	5	5	5	Crítico	Mitigar

15. Plan de tratamiento de riesgos

N°	Nombre del riesgo	Nivel del riesgo	Controles según ISO 27001	Encargado
1	Acceso no autorizado	Critico	Política de control de accesos.	Jefe de soporte
2	Divulgación de información	Critico	Proceso disciplinario. Acuerdos de confidencialidad.	Colaborador
3	Abuso de privilegios	Apreciable	Política de control de accesos. Controles de red.	Jefe de soporte
4	Fuga de información	Critico	Respaldo de la información.	colaborador
5	Alteración de información	Importante	políticas de control de acceso	Colaborador
6	Error de configuración de equipos	Apreciable	uso aceptable de los equipos. Conciencia educación y capacitación sobre la seguridad de la información.	Jefe de soporte

7	Abuso de privilegios	Apreciable	Políticas de control de accesos. controles de red	Jefe de soporte
8	Acceso denegado	Importante	Políticas de control de accesos. Gestión de claves.	Jefe de soporte
9	Manipulación de equipos	Apreciable	Uso aceptable de los equipos. Gestión de claves.	Colaborador
10	Daños por agua	Importante	Uso aceptable de los equipos. Conciencia educación y capacitación sobre la seguridad de la información	Colaborador
11	Saturación de la red	Importante	Políticas de control de acceso	Jefe de soporte
12	Acceso no autorizado a la red	Importante	acceso a redes y a servicios de red	Jefe de soporte
13	Alteración en los puertos de conectividad	Apreciable	Políticas de control de acceso. Proceso disciplinario.	Jefe de soporte

			uso aceptable de los equipos.	
14	Virus	Bajo	Controles de red. conciencia, educación y capacitación. sobre la seguridad de la información. políticas de control de acceso	Jefe de soporte
15	Instalación de software no autorizado	Despreciable	Proceso disciplinario. Roles y responsabilidades	Jefe de soporte
16	Denegación de servicios	Crítico	Continuidad de la seguridad de la información.	Gerente de agencia

ANEXO E: DESARROLLO DEL PROYECTO PROPUESTO UTILIZANDO PILAR 7.4.7 (8.2.2021)

1. Identificación de activos

Luego de la creación del proyecto, como primer paso de esta herramienta es elegir los activos mediante código y nombre, su clasificación se aprecia en la siguiente figura:

Activos esenciales

Servicios internos

Equipamiento

Servicios Subcontratados

Instalaciones

Personal

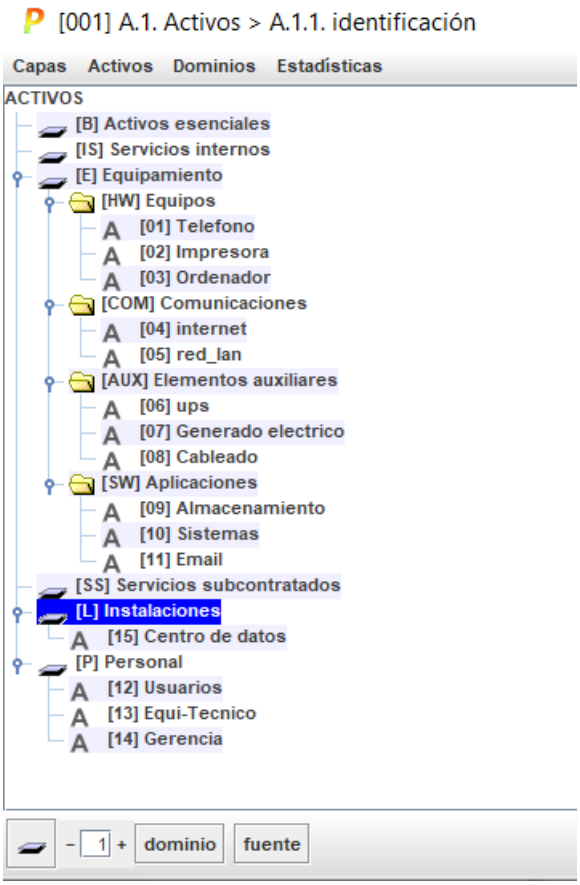


Figura 6: Identificación de activos

2. Dependencia de activos

A partir de lo anterior se estableció la dependencia entre ordenador con equipamiento informático, redes de comunicaciones, equipamiento auxiliar, personal e instalaciones. Proceso que se repite para los demás activos.

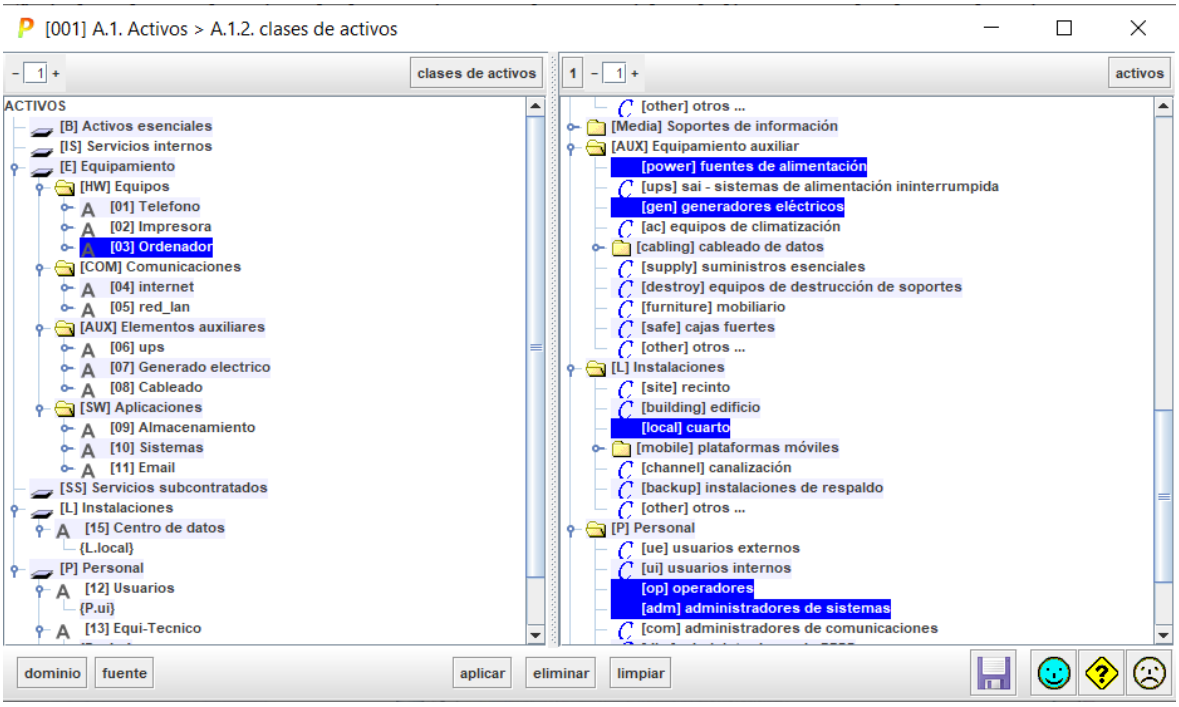


Figura 7: Dependencia de activos

3. Valoración de activos

Se realizó la evaluación de activos de acuerdo a las dimensiones de seguridad (disponibilidad, integridad y confidencialidad) en que se verían afectados al exponerse a varios tipos de amenazas que provocan la pérdida de información o daños sobre el equipo de almacenamiento de acuerdo al nivel de impacto detallado anteriormente con Magerit: 5 (Muy alto), 4 (alto), 3 (medio), 2 (bajo) y 1 (muy bajo).

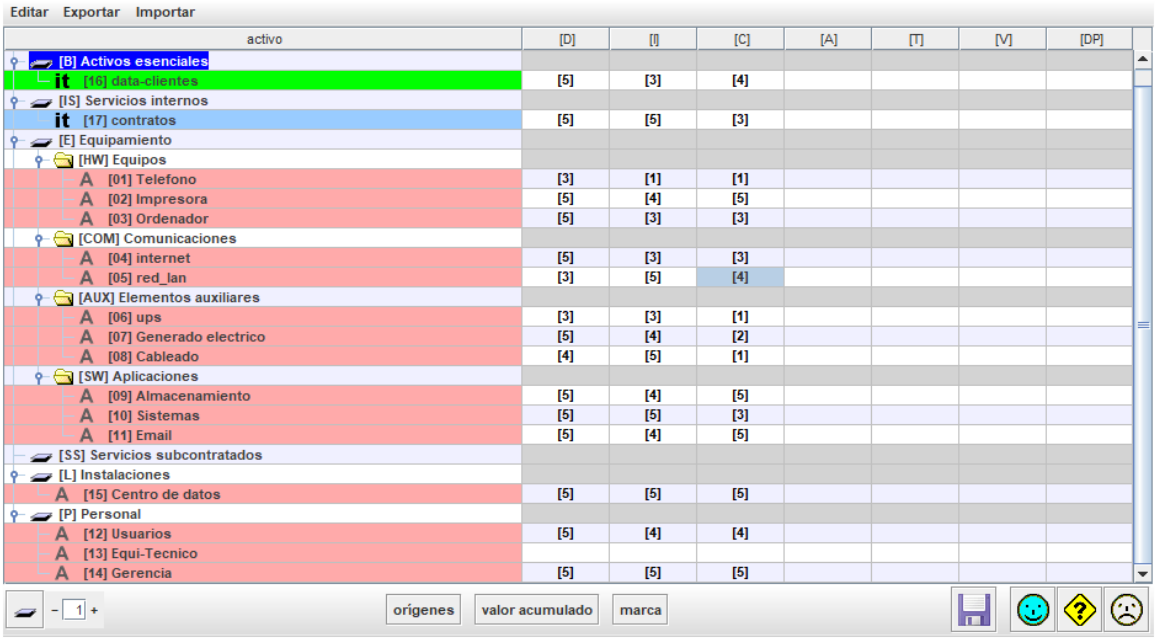


Figura 8: Valoración de activos

4. Identificación y valoración de amenazas

Se identificaron las amenazas que producen más daños para evaluar el nivel de riesgo, asimismo se obtuvo la valoración automática considerando la frecuencia de materialización y el impacto que causaría en la empresa.

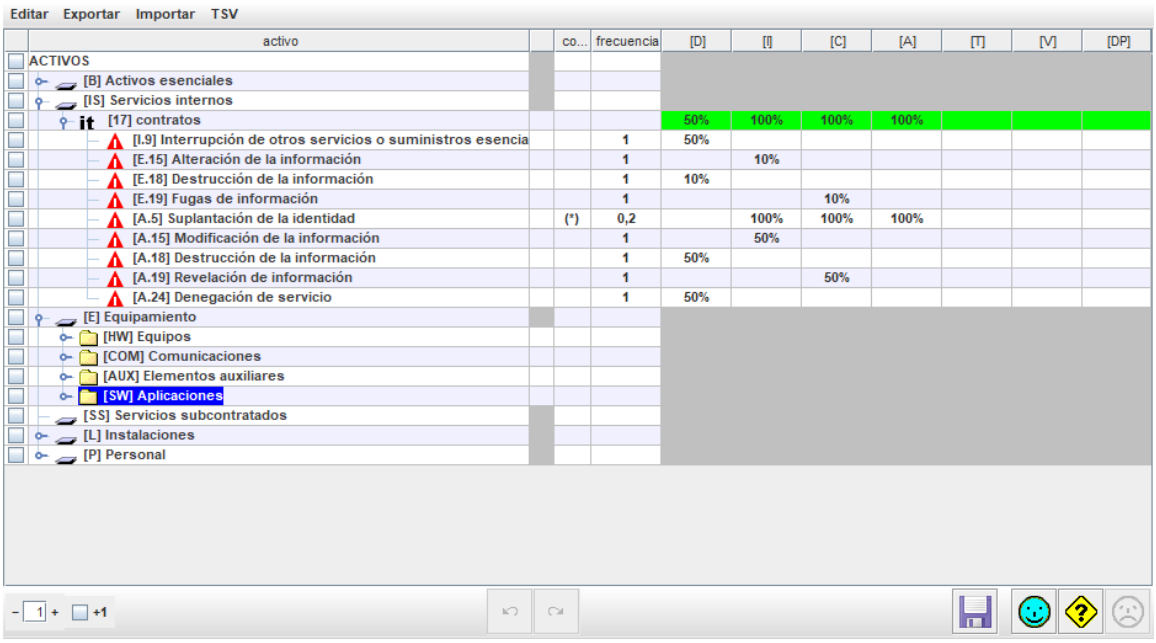


Figura 9: Identificación y valoración de amenazas

5. Evaluación de salvaguardas

Se trabajó en base a 4 aspectos:

Gestión

Técnico

Seguridad física

Gestión de personal

La columna recomendación indica la valoración aproximada de la salvaguarda en base al tipo de activo que tiene una escala de 0-10.

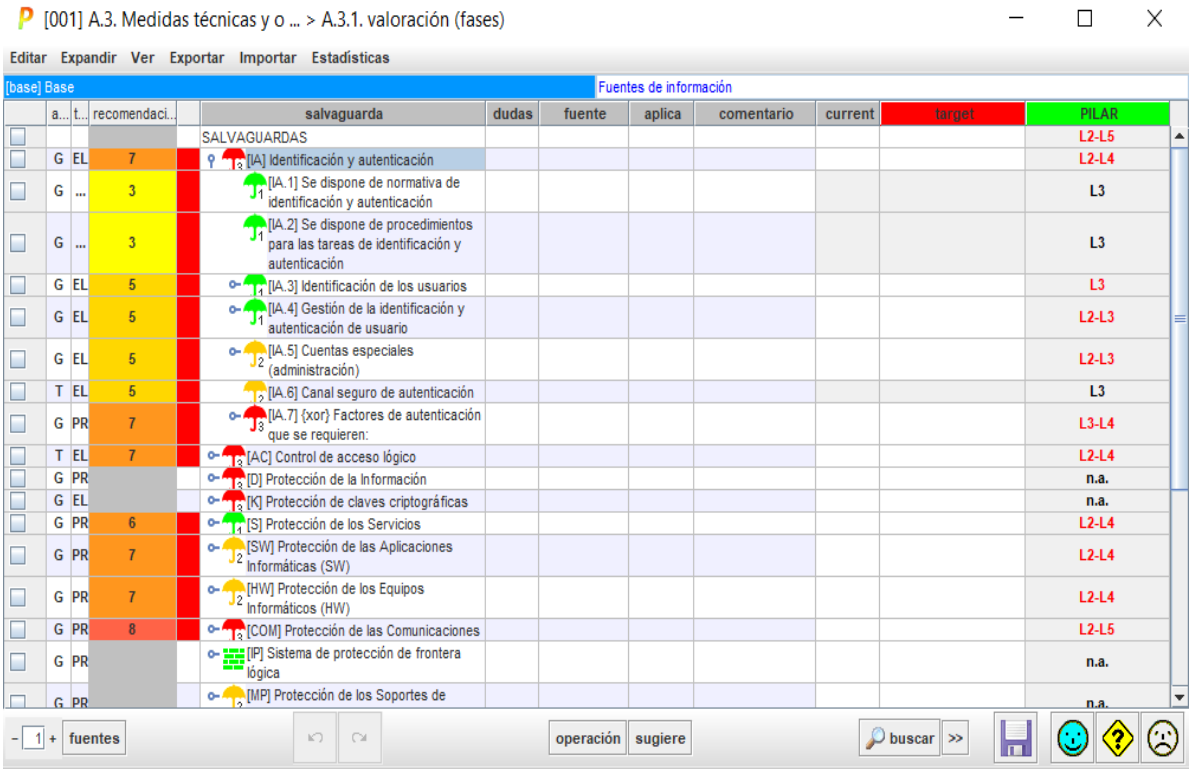


Figura 10: Evaluación de salvaguardas

Como se observa en la figura 13 el nivel de salvaguarda actualmente está entre 1 y 3, lo que nos indica que aún faltan aplicar controles para mejorar la seguridad de la información.

6. Impacto

Ver Exportar

potencial | current | target | PILAR

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	[5]	[5]	[5]				
[B] Activos esenciales							
[IS] Servicios internos	[4]	[5]	[4]				
[17] contratos	[4]	[5]	[4]				
[E] Equipamiento	[5]	[5]	[5]				
[HW] Equipos	[5]	[5]	[5]				
[01] Telefono	[5]	[5]	[4]				
[02] Impresora	[5]	[5]	[5]				
[03] Ordenador	[5]	[5]	[4]				
[COM] Comunicaciones	[5]	[5]	[4]				
[04] internet	[5]	[5]	[4]				
[05] red_lan	[5]	[5]	[4]				
[AUX] Elementos auxiliares	[5]	[5]	[4]				
[06] ups	[5]	[5]	[4]				
[07] Generado electrico	[5]	[5]	[4]				
[08] Cableado	[5]	[2]	[3]				
[SW] Aplicaciones	[5]	[5]	[5]				
[09] Almacenamiento	[5]	[5]	[5]				
[10] Sistemas	[5]	[5]	[4]				
[11] Email	[5]	[5]	[5]				
[SS] Servicios subcontratados							
[L] Instalaciones	[5]	[5]	[5]				
[P] Personal	[5]	[5]	[5]				

dominio | fuente | gestionar | leyenda

Figura 11: Impacto acumulado potencial

Ver Exportar

potencial | current | target | PILAR

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	[5]	[5]	[5]				
[B] Activos esenciales							
[IS] Servicios internos	[4]	[5]	[4]				
[17] contratos	[4]	[5]	[4]				
[E] Equipamiento	[5]	[5]	[5]				
[HW] Equipos	[4]	[4]	[4]				
[01] Telefono	[4]	[4]	[3]				
[02] Impresora	[4]	[4]	[4]				
[03] Ordenador	[4]	[4]	[3]				
[COM] Comunicaciones	[4]	[4]	[3]				
[04] internet	[4]	[4]	[3]				
[05] red_lan	[4]	[4]	[3]				
[AUX] Elementos auxiliares	[5]	[4]	[3]				
[06] ups	[4]	[4]	[3]				
[07] Generado electrico	[4]	[4]	[3]				
[08] Cableado	[5]	[2]	[3]				
[SW] Aplicaciones	[4]	[5]	[5]				
[09] Almacenamiento	[4]	[4]	[4]				
[10] Sistemas	[4]	[4]	[3]				
[11] Email	[4]	[5]	[5]				
[SS] Servicios subcontratados							
[L] Instalaciones	[4]	[4]	[4]				
[P] Personal	[4]	[4]	[4]				

dominio | fuente | gestionar | leyenda

Figura 12: Impacto cumulado Actual (current)

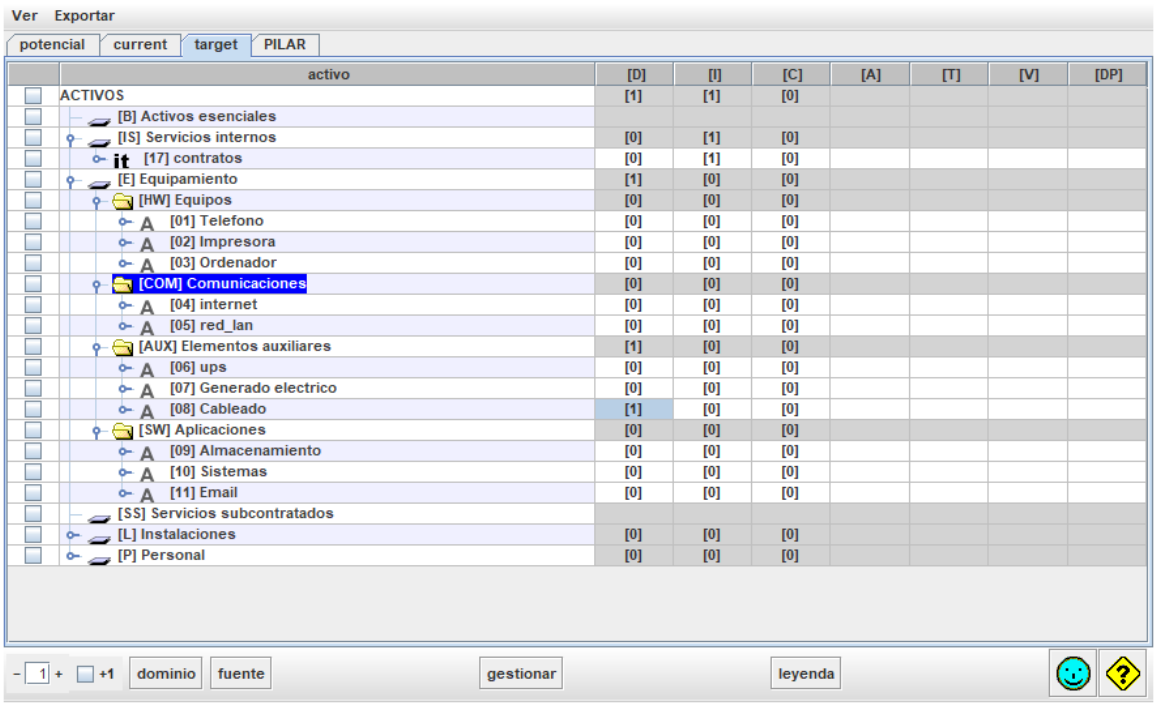


Figura 13: Impacto acumulado objetivo (target)

De las ultimas 3 figuras se puede observar la importancia de aplicar salvaguardas que disminuyeran los niveles de impacto, actualmente están en el nivel medio, y el nivel objetivo es obtener un bajo impacto (ver figura 16)

7. Riesgo

Se evaluaron los niveles de criticidad del riesgo a los cuales se exponen los activos, en la figura 17 la dimensión de disponibilidad es la que se ve gravemente afectada si no se aplicasen los salvaguardas; las figuras reflejan las disminuciones del nivel de riesgo en las tres dimensiones una vez alcanzado el objetivo.

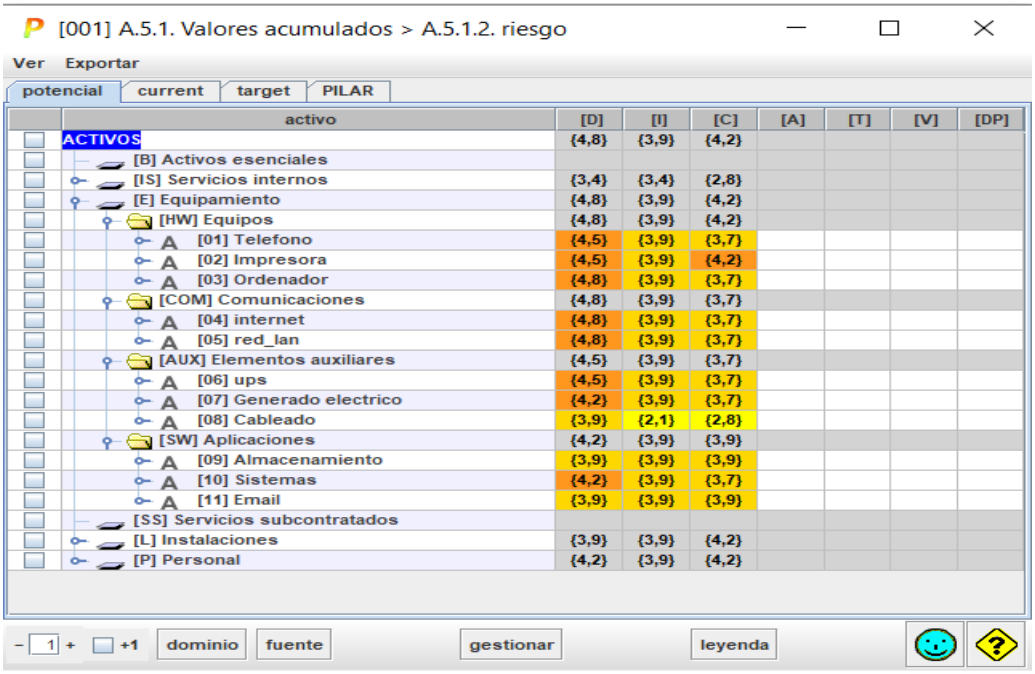


Figura 14: Riesgo acumulado potencial

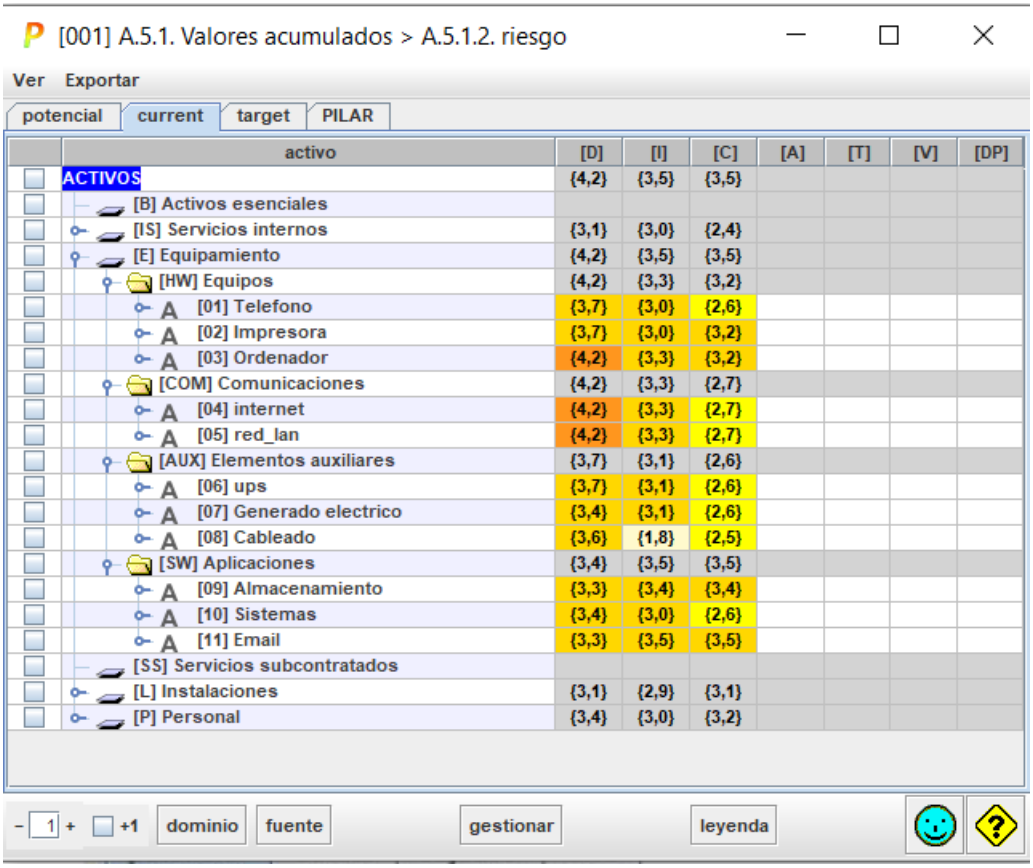
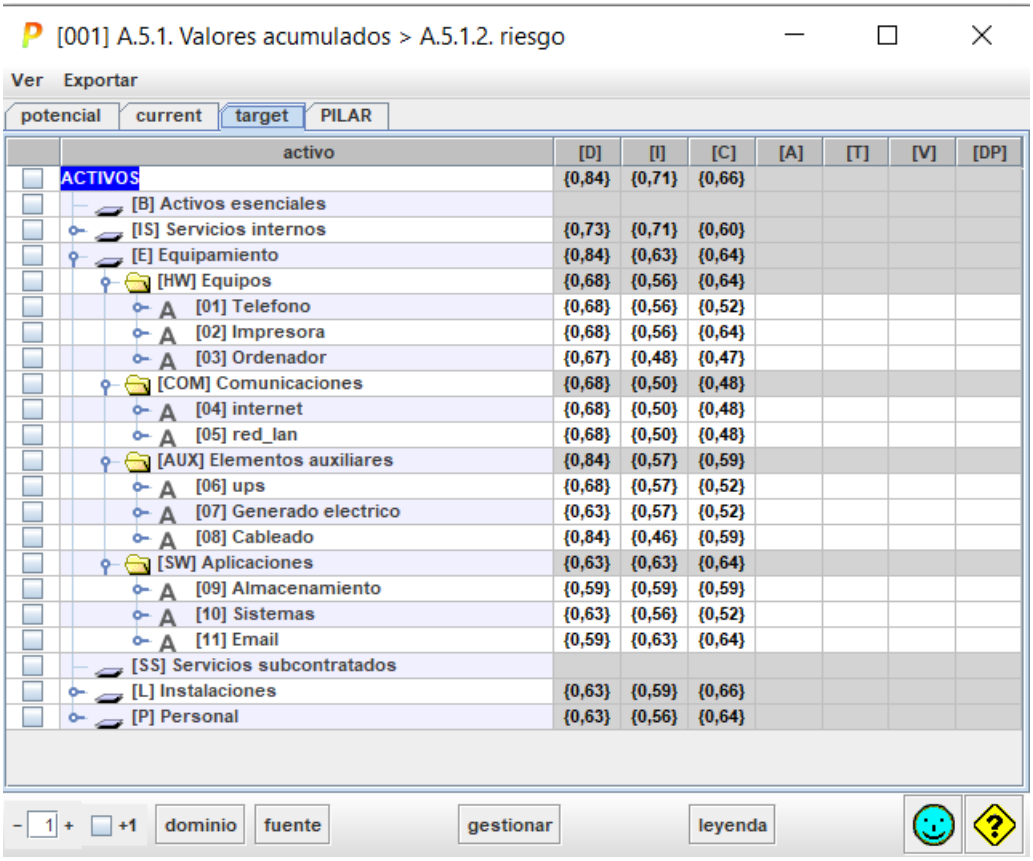


Figura 15: Riesgo acumulado actual (current)



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	{0,84}	{0,71}	{0,66}				
[B] Activos esenciales							
[IS] Servicios internos	{0,73}	{0,71}	{0,60}				
[E] Equipamiento	{0,84}	{0,63}	{0,64}				
[HW] Equipos	{0,68}	{0,56}	{0,64}				
[01] Telefono	{0,68}	{0,56}	{0,52}				
[02] Impresora	{0,68}	{0,56}	{0,64}				
[03] Ordenador	{0,67}	{0,48}	{0,47}				
[COM] Comunicaciones	{0,68}	{0,50}	{0,48}				
[04] internet	{0,68}	{0,50}	{0,48}				
[05] red_lan	{0,68}	{0,50}	{0,48}				
[AUX] Elementos auxiliares	{0,84}	{0,57}	{0,59}				
[06] ups	{0,68}	{0,57}	{0,52}				
[07] Generado electrico	{0,63}	{0,57}	{0,52}				
[08] Cableado	{0,84}	{0,46}	{0,59}				
[SW] Aplicaciones	{0,63}	{0,63}	{0,64}				
[09] Almacenamiento	{0,59}	{0,59}	{0,59}				
[10] Sistemas	{0,63}	{0,56}	{0,52}				
[11] Email	{0,59}	{0,63}	{0,64}				
[SS] Servicios subcontratados							
[L] Instalaciones	{0,63}	{0,59}	{0,66}				
[P] Personal	{0,63}	{0,56}	{0,64}				

Figura 16: Riesgo acumulado objetivo (target)

8. Informes

Finalmente se muestra el gráfico de las evaluaciones realizadas, en la figura 20 se observa a las dimensiones de seguridad de la información afectadas en cada uno de los activos, resaltando a la disponibilidad en la mayoría de activos.

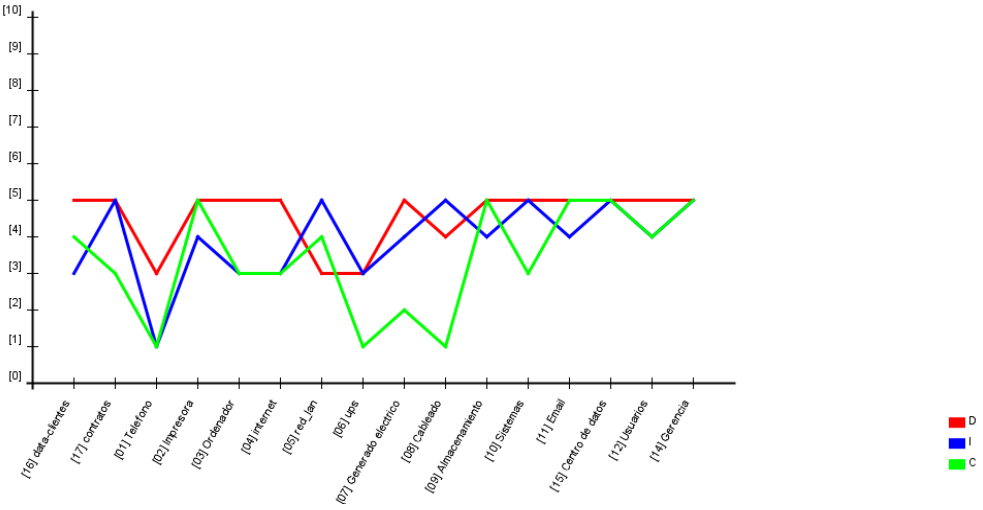


Figura 17: Valor de activos