“AÑO DEL DIÁLOGO Y LA RECONCILIACIÓN NACIONAL”

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

“IMPLEMENTACION DEL MODELO "ARSI" PARA OPTIMIZAR LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA. 289”

PARA OPTAR EL GRADO DE INGENIERO DE SISTEMAS

TESISTAS: Kathering Yajaira INGUNZA LASTRA

José Antonio VALDIVIA JAIMES

ASESORA: Mg. Heidy Velsy RIVERA VIDAL

Huánuco – Perú

2018

DEDICATORIA

El presente trabajo de investigación lo dedicamos principalmente a Dios, por ser el inspirador y darnos fuerza para continuar en este proceso de obtener uno de nuestros anhelos más deseados.

A nuestros padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes hemos logrado llegar hasta aquí y convertirnos en lo que somos.

A nuestros hermanos (as) por estar siempre presentes, acompañándonos y por el apoyo moral, que nos brindaron a lo largo de esta etapa de nuestras vidas.

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

AGRADECIMIENTO

Agradecemos a Dios por bendecirnos con la vida, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a nuestros padres: Natali y Francisco; y, Clelia, por ser los principales promotores de nuestros sueños, por confiar y creer en nuestras expectativas, por los consejos, valores y principios que nos han inculcado.

Agradecemos a nuestros docentes de la Escuela de Ingeniería de Sistemas de la Universidad Nacional Hermilio Valdizán, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión, de manera especial, al master Heidy Velsy Rivera Vidal tutora de nuestro proyecto de investigación quien ha guiado con su paciencia, y su rectitud como docente.

RESUMEN

El Análisis de Riesgos se ha diseñado para identificar los activos y las medidas de seguridad utilizadas para mitigar los riesgos a los que se encuentra expuesto un activo. A partir de los problemas más comunes las empresas, se han visto en la necesidad de desarrollar una evaluación que permita validar los elementos que forman parte de los procesos y que son utilizados por el personal de la empresa. La valoración del riesgo al que la empresa está expuesta conforme al modelo y metodología seleccionados, permiten plantear una serie de preguntas para comprender como las medidas de seguridad que su empresa ha ido implantado a lo largo del tiempo, han formado capas de defensa, lo que proporciona una mayor protección frente a los riesgos de seguridad y las vulnerabilidades específicas.

Para desarrollar la autoevaluación es esencial el desarrollo de un Plan de Seguridad, el mismo que se constituye en la herramienta que permite al Responsable de Seguridad gestionar de una forma adecuada la seguridad, al ejecutar ésta actividad no únicamente sabremos el estado de la empresa entorno a la seguridad, nos permitirá escalar a mejores prácticas y a un mejor ambiente de seguridad si nos enfocamos en estándares conocidos, en nuestro caso empleamos el conjunto de normas ISO 27001, y MAGERIT V3 como metodología para la gestión de riesgo, si éstas poderosas herramientas las fusionamos con el modelo de mejora continua conocido como Deming o PDCA(Plan-Do-Check-Act).

ABSTRACT

The Risk Analysis is designed to identify the assets and security measures used to mitigate the risks to which an asset is exposed. Based on the most common problems, the companies have found themselves in need of developing an evaluation that allows to validate the elements that are part of the processes and that are used by the personnel of the company. The assessment of the risk to which the company is exposed according to the selected model and methodology, allow raising a series of questions to understand how the security measures that your company has been implemented over time, have formed layers of defense, which It provides greater protection against security risks and specific vulnerabilities.

To develop the self-assessment is essential to develop a Security Plan, which is the tool that allows the Security Manager to properly manage security, by executing this activity we will not only know the status of the company around security will allow us to scale to better practices and a better security environment if we focus on known standards, in our case we use the set of ISO 27001 standards, and MAGERIT V3 as a methodology for risk management, if these powerful tools are merged with the continuous improvement model known as Deming or PDCA (Plan-Do-Check-Act).

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRAFICOS

INTRODUCCIÓN

El Análisis de Riesgos se ha diseñado para identificar los activos y las medidas de seguridad utilizadas para mitigar los riesgos a los que se encuentra expuesto un activo. A partir de los problemas más comunes es así que las empresas, se han visto en la necesidad de desarrollar una evaluación que permita validar los elementos que forman parte de los procesos y que son utilizados por el personal de la empresa, ya que la valoración del riesgo al que la empresa está expuesta conforme al modelo y metodología seleccionados, permiten plantear una serie de preguntas para comprender como las medidas de seguridad que su empresa ha ido implantando a lo largo del tiempo, han formado capas de defensa, lo que proporciona una mayor protección frente a los riesgos de seguridad y las vulnerabilidades específicas.

La Cooperativa de Ahorro y Crédito San Francisco consiente de la responsabilidad de entregar servicios financieros eficientes y de calidad a sus clientes; adaptándose a los innovadores y constantes cambios tecnológicos ha buscado siempre innovar, sin dejar de lado la administración correcta de la información. Hace más de una década el manejo de la seguridad estaba limitada y fácilmente administrada mediante el resguardo de documentos importantes a accesos físicos controlados, hoy es más difícil; pues la información no solo se almacena en documentos físicos, siendo de esta manera cambiante en el tiempo gracias a la introducción de sistemas informáticos que nos acercan a la información pero que también la hacen más sensible. El uso actual de servicios globales como el internet ha obligado a los sistemas de seguridad a evolucionar de tal manera que no solo se enfoquen en

la protección de la información, hoy los sistemas de seguridad deben ser capaces de gestionar y reducir incidentes para evitar delitos, que permitan cuantificar gastos y pérdidas, minimizar impactos de riesgo. Debemos ser conscientes que no son las computadoras o elementos autónomos los que atacan a las empresas; son las personas que intentan hacer que los sistemas de seguridad fallen. El análisis de riesgos de la seguridad de la información pretende mitigar los incidentes de seguridad, pretendiendo de un modo objetivo y pro-activo, constituirse en la piedra angular de la "cultura de seguridad", de tal manera que le permita sobrevivir en los escenarios más exigentes, permitiendo que sean los empleados quienes entiendan como reconocer, responder e informar un incidente.

De allí que la presente investigación se encuentra estructurada en cinco capítulos que se presentan a continuación:

El Capítulo I: Descripción del Problema de investigación, se fundamenta el problema y se formula el problema, los objetivos, hipótesis, las variables su operacionalización y definición de términos operacionales.

El Capítulo II: Contiene el marco teórico, se presenta los antecedentes, bases teóricas y conceptuales que hacen referencia histórica evolutiva del tema investigado.

El Capítulo III: Estructura la metodología, señalando el ámbito, población y muestra, se especifica el tipo y diseño utilizados, así como las técnicas de validación y confiabilidad del instrumento y procedimientos del desarrollo de la investigación.

El Capítulo IV: Modelo ARSI, implementación del modelo ARSI, teniendo en cuenta las fases de desarrollo; Fase I: caracterización de activos, Fase II: Evaluación de amenazas, Fase III: Plan de tratamiento de riesgos, Fase IV: Analizar controles, Fase V: Implementación de mejoras.

El capítulo V: Resultados, mostramos los resultados de la investigación con aplicación de la estadística como instrumento de medida. Y la discusión, en referencia con los antecedentes, bases teóricas, la prueba de hipótesis y el aporte científico de esta investigación

Finalmente, se establecen las conclusiones en relación a los objetivos de la presente investigación, para luego fijar las recomendaciones o sugerencias pertinentes, acompañando las referencias bibliográficas utilizadas en la investigación, así como los anexos correspondientes.

CAPÍTULO I

DESCRIPCIÓN DEL PROBLEMA DE INVESTIGACIÓN

1.1. Fundamentación del problema de investigación

Hoy en día la seguridad de la información debe establecer normas que minimicen los riesgos. Estas normas deben incluir horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad de la información minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas.

Pues en un reciente reporte del House Banking Committee de Estados Unidos, muestra que el sector financiero perdió 2.4 billones de dólares por ataques computarizados en 1998, más del triple que en 1996. No es sorprendente, considerando que por día se transfieren electrónicamente 2 trillones de dólares, mucho de lo cual pasa a través de líneas que según el FBI no son muy seguras. (Fortune 500, 2003).

Es más casi el 80% de los valores intelectuales de las corporaciones son electrónicos, de acuerdo a la Cámara de Comercio estadounidense, y un competidor puede subir hasta las nubes si roba secretos comerciales y listas de clientes. (Sloan Review, 2003). Asimismo, los hackers son expertos en ingeniería social, consiguiendo personas de dentro de las compañías para sacarles contraseñas y claves de invitados.

En la ciudad de Huánuco hoy en día se cuenta con varias entidades financieras dentro de los cuales una de las más representativas es la Cooperativa de Ahorro y Crédito San Francisco Ltda. Pues es una organización sin fines de lucro que brinda servicios financieros y cooperativos (principalmente de ahorro y crédito) a sus asociados de las ciudades de Huánuco, Tingo María y Pucallpa, considerando siempre una atención con calidez y eficiencia, que la diferencia de las demás instituciones micro financiero y financiero del sector, basados en los principios cooperativos de “ayuda mutua”.

La cual entiende y se preocupa por la seguridad de sus activos informáticos y de la información que esta posee de cada uno de sus clientes, por lo cual se ha visto la importancia de la implementación de un Sistema de Seguridad de los activos Informáticos.

Puesto que la Cooperativa de Ahorro y Crédito San Francisco ha identificado la necesidad de desarrollar mecanismos que les permitan asegurar la disponibilidad, integridad y confidencialidad en el manejo de la información ya que la información está sujeta a muchas amenazas, tanto de índole interna como externa. Por tanto, es necesario llevar la implementación del modelo propuesto “ARSI”, el cual contribuirá para

optimizar la Seguridad de la Información en La Cooperativa de Ahorro y Crédito San Francisco Ltda. 289 para así gestionar al análisis y seguridad de la información de la organización.

1.2. Justificación

Los sistemas de información y las tecnologías de información han cambiado la forma en que operan las organizaciones actuales. Pues la gestión y análisis de los riesgos persigue lograr un conocimiento lo más realista posible de aquellas circunstancias que podrían afectar a los procesos o servicios, causando daños o pérdidas de modo que se puedan establecer prioridades y asignar requisitos de seguridad para afrontar convenientemente dichas situaciones. Es necesario tener presente que el lugar donde se centraliza la información con frecuencia el centro de cómputo puede ser el activo más valioso y al mismo tiempo el más vulnerable.

Siendo así que al analizar los riesgos soportados por los sistemas TIC en La Cooperativa de Ahorro y Crédito San Francisco Ltda. 289 pudimos apreciar que aún existen guías informales, aproximaciones metódicas y herramientas de soporte. Todas ellas buscan objetivar el análisis de riesgos, el gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que el Modelo “ARSI” persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

1.3. Importancia o propósito

Siendo de gran importancia pues hoy en día la información en la empresa es uno de los más importantes activos que se poseen, por ello se debe de preservar y resguardar de manera segura y confiable. De esta manera las organizaciones tienen deben de desarrollar mecanismos que les permitan asegurar la disponibilidad, integridad y confidencialidad en el manejo de la información y sus activos informáticos.

La información está sujeta a muchas amenazas, tanto de índole interna como externa. Es por ello que la Cooperativa de Ahorro y Crédito San Francisco la cual hoy en día cuenta con el triple de clientes que hace dos años atrás ha visto de manera inmediata la implementación de un Sistema de Seguridad de Activos Informáticos.

1.4. Limitaciones

Siendo la principal limitante el tiempo de disponibilidad del coordinador, trabajadores, y otros actores involucrados al tema de investigación.

1.5. Formulación del problema de investigación

1.5.1. Problema general

¿De qué manera se optimizará la seguridad de la información mediante el modelo propuesto “ARSI” en la Cooperativa de Ahorro y Crédito San Francisco?

1.5.2. Problemas específicos

- ¿En qué medida las políticas de seguridad permiten minimizar los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289 – Huánuco, 2018?
- ¿Existe un software de monitoreo que permite mitigar los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289 – Huánuco, 2018?

1.6. Formulación de los objetivos

1.6.1. Objetivo general

Optimizar la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco mediante el modelo propuesto "ARSI"- Huánuco, 2018.

1.6.2. Objetivos específicos

- Establecer políticas de seguridad para minimizar los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289 – Huánuco, 2018.
- Monitorear la seguridad de la información de la Cooperativa de Ahorro San Francisco Ltda. 289, mediante la implementación de un software.

1.7. Formulación de la hipótesis

1.7.1. Hipótesis general

HO: Mediante el modelo "ARSI" no se optimizará la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco.

Ha: Mediante el modelo "ARSI" se optimizará la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco.

1.7.2. Hipótesis específicas

- **HO_1:** Mediante la implementación de políticas de seguridad no se minimizará los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289.

  Hi_1: Mediante la implementación de políticas de seguridad sí se minimizará los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289.

- **Ho_2:** Mediante la implementación del software de monitoreo no se mitigará los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289.

  Hi_2: Mediante la implementación del software de monitoreo si se mitigará los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289.

1.8. Variables

1.8.1. Variable independiente

MODELO ARSI

1.8.2. Variable dependiente

SEGURIDAD DE LA INFORMACIÓN

1.9. Operacionalización de las variables

	VARIABLES	DIMENSIONES	INDICADORES
Variable Independiente	**X:** MODELO “ARSI”	AMENAZAS	Probabilidad de ocurrencia de la amenaza
		IMPACTO	Medida de Impacto
		RIESGO	Estimación de Riesgo
Variable Dependiente	**Y:** Seguridad de la información	DISPONIBILIDAD	Riesgo en la disponibilidad de la información de los activos informáticos.
		INTEGRIDAD	Riesgo en la integridad de la información de los activos informáticos.
		CONFIDENCIALIDAD	Riesgo en la confidencialidad de la información de los activos informáticos.
		AUTENTIFICACIÓN	Riesgo en la autentificación de la información de los activos informáticos.
		NO REPUDIO	Riesgo en no repudio de la información de los activos informáticos.

Fuente: elaboración propia

1.10. Definición de términos operacionales

Tabla 1. Definición operacional

	VARIABLES	DEFINICIONES	DIMENSIONES
Variable Independiente	**X:** MODELO "ARSI"	**CONCEPTUAL:** Metodología es una ciencia del conocimiento, subordinada a la Tecnología y cuyo objeto de estudio es el cómo del conocimiento, trata una serie de conceptos y técnicas que hacen expedito el camino del descubrimiento y de la invención. **Lizardo Carbajal 2006. ISBN 978-958-30-9. 150 p.** **OPERACIONAL:** La metodología muestra una serie conceptos y técnicas con las que se identificaran las **amenazas**, **vulnerabilidades**, **impacto** y el **riesgo** de los sistemas de información con el cual se podrán crear **salvaguardas** a medida según el tipo de activo, así mismo la implementación de **políticas de seguridad** que sirvan de control y monitoreo para minimizar el impacto de los riesgos.	**AMENAZAS:** Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.
			IMPACTO: El impacto generado sobre un activo de información según la norma ISO 27001 es la consecuencia de la materialización de una amenaza.
			RIESGO: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio.
			SALVAGUARDA: Es la medida de control y monitoreo con el cual se mitiga el impacto de materialización de las amenazas en función de las vulnerabilidades que existen en los sistemas de información.
			POLÍTICAS DE SEGURIDAD: La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad.

Variable Dependiente	**Y:** Seguridad de la información	**CONCEPTUAL:** La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada. La seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Podemos entender como seguridad un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar a su funcionamiento directo o a los resultados que se obtienen. Javier Areitio Bertolín, 2008 ISBN: 8497325028 - EAN: 9788497325028. **OPERACIONAL:** La Seguridad de la Información tiene como fin la protección de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada, identificando y monitoreando cada activo perteneciente a las siguientes dimensiones como autentificación, integridad, disponibilidad, confidencialidad y no repudio.	**AUTENTIFICACIÓN:** Propiedad o característica que consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. **INTEGRIDAD:** Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización. **DISPONIBILIDAD:** Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones. **CONFIDENCIALIDAD:** Permite que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. **NO REPUDIO:** Este objetivo garantiza la participación de las partes en una comunicación. En toda comunicación, existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio: a) No repudio en origen: garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío. b) No repudio en destino: El receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES

2.1.1. A nivel Internacional

(Vásquez, 2013) **en su tesis Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial BRAVITO S.A. en la ciudad de Machala, para optar por el título de Ingeniero de Sistemas.**

Estudia estado actual en el que se encuentra la empresa “Pesquera e Industrial Bravito S.A. Encontrando de esta manera una situación alarmante ya que en sus procesos no implementa, medidas de seguridad apropiada lo cual provoca que exista inseguridad. Pues Las amenazas que existen en las instalaciones de la empresa pueden causar la pérdida de la información ya que no existen medidas de seguridad adecuadas. Luego realizo el análisis de los activos informáticos aplicando la metodología MAGERIT, al finalizar concluyo que, la empresa “Pesquera e Industrial Bravito S.A.” no tiene medidas de seguridad guiados y documentados, por lo cual este estudio será de gran beneficio para

minimizar riesgos en el futuro. Asimismo, pudo afirmar que la herramienta PILAR 5.2.9 fue de gran ayuda en este proyecto de tesis ya que ayudo en la valoración de los riesgos en diferentes etapas potencial, situación actual y objetivo. Finalmente, después de haber realizado este proyecto, la empresa obtendrá un documento encaminado a la seguridad que será punto de partida para la creación de normativas de seguridad para los recursos informáticos y para los empleados que laboran en la empresa.

(Florentino Galindo & Morales Morales, 2008) **en su tesis Aplicación de la Metodología MAGERIT en el Análisis de Riesgo del Flujo de Información en el área de Gestión de una empresa dedicada a la aplicación de exámenes de Control de Confianza, para optar por el título de ingeniero en comunicaciones y electrónica.**

En su tesis propone la aplicación de la Aplicación de la Metodología MAGERIT en el Análisis de Riesgo del Flujo de Información en el área de Gestión de una empresa dedicada a la aplicación de exámenes de Control de Confianza, una vez concluido la aplicación de la metodología concluye que, la investigación le permitió reconocer de manera sistemática las vulnerabilidades en el área de gestión de la dirección general de control de confianza. Pues la implementación de políticas de seguridad resguardo la información, difundiendo el uso de canales de comunicación seguros para el envío de los resultados de las áreas a la de gestión, que a su vez dan lugar a una base de datos dejando desfasado el uso de los archivos en Excel.

(Ramos, 2015) **Análisis de Riesgos Informáticos y Desarrollo de un Plan de Seguridad de la Información para el Gobierno Autónomo Descentralizado Municipal de Catamayo**

La presente investigación tuvo como finalidad desarrollar un Plan de la Seguridad de la Información para el Gobierno Autónomo Descentralizado Municipal de Catamayo, tomando en cuenta Norma ISO 27001 y las recomendaciones proporcionadas en la Norma ISO 27002. Tuvo como punto de partida para el diseño la identificación de los activos que contribuyen a la entrega de los servicios a los usuarios, además de las medidas de seguridad implementadas en la institución, finalmente realizó un análisis de riesgos, identificando los activos críticos, así como las amenazas a las que están expuestos dichos activos y creando perfiles de riesgo para cada activo critico incluyendo el impacto, la probabilidad de ocurrencia de amenazas y el plan para el tratamiento del riesgo. Finalmente, desarrolló el plan de seguridad para la Institución, incluyendo políticas a seguir por parte del personal y soluciones técnicas de acuerdo al equipamiento de la institución que contribuyan a garantizar la seguridad de la información.

Luego realizó la implementación y validación de las soluciones técnicas que consisten en un nuevo diseño de red lógica basado en VLANS, DHCP y ACL, optimizando los recursos que existen en la institución y garantizando la seguridad de la información, para la validación de la implementación del plan se realizaron pruebas de petición de respuesta

de eco y recolección de información de los usuarios finales, lo que permite determinar que se cumplan las reglas de acceso implementadas.

2.1.2. A nivel Nacional

(Barrantes Porras & Hugo Herrera, 2012)**. En su tesis Diseño e implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos**.

Menciona que actualmente Card Perú S.A. no cuenta con los controles, medidas, procedimientos de seguridad necesarios para resguardar sus activos de información, tales como documentos, software, dispositivos físicos, personas, imagen, reputación y servicios, están expuestos a altos niveles de riesgos, frente a las diversas amenazas físicas y lógicas existentes, por ello plantea como objetivo general reducir y mitigar los riesgos de los activos de información de los procesos que se encuentran bajo la gerencia de tecnología de Card Perú S.A. que ponen en peligro los recursos, servicios y continuidad de los procesos tecnológicos, mediante la implementación de un Sistema de gestión de seguridad de información, el cual brindará los procedimientos y lineamientos necesarios para identificar e evaluar los riesgos, las amenazas, las vulnerabilidades de los activos de información de los procesos de tecnología. Al implementar el SGSI se minimizó la interrupción en el funcionamiento de las actividades del negocio, así también ayuda a identificar los activos de información y los protege adecuadamente generando así mayor confianza en los clientes y

socios estratégicos por la garantía de calidad y confidencialidad comercial. Finalmente concluye que al diseñar e implementar una buena metodología para gestionar los riesgos y ejecutando los planes de tratamiento de riesgos planteados, se logra reducir a niveles aceptables el gran porcentaje de riesgos que afectan a los activos de información.

(Serrano, 2007), en su tesis Gestión de seguridad de la Información y los servicios críticos de las universidades.

Menciona que la preocupación de las organizaciones por la seguridad de la información no debe de estar centrada sólo en los aspectos más técnicos de la seguridad, sino es necesario proponer a las organizaciones estrategias de gestión de seguridad de la información que abarque el desarrollo, revisión y cumplimiento de las políticas de seguridad y abordar temas claves se seguridad como la identificación de riesgos críticos, capacitación y privacidad. Por todo lo mencionado anteriormente propone como objetivo principal proponer estrategias de gestión de Seguridad de la Información y sus implicancias en la calidad y eficacia en los servicios críticos de las Universidades como son los servicios de matrícula, admisión y registros, grados y títulos, tesorería e informática. Identificando a su vez como variable independiente: Gestión de seguridad de la Información y como variable independiente: Servicios críticos de las Universidades. Siendo la investigación de carácter descriptivo, y su muestra estuvo

conformada por 24 universidades de Lima, 5 públicas y 19 privadas. Utilizando como instrumento de recolección de datos el cuestionario. Llegando así a la conclusión de que las autoridades no consideran a la seguridad de la información como una prioridad alineada con la estrategia universitaria ello se refleja en las encuestas realizadas al personal de TIC donde se les formuló la pregunta si habían asistido a eventos o programas de capacitación de seguridad de la información, la cual reportó que la mayoría nunca asistió a programas de capacitación: UNMSM 20%, UNFV 100% y UPSJB 70%. Así mismo respecto a los riesgos de la información en las universidades como son: divulgación ilícita de la información por los trabajadores (UNFV 36%), no realizaron copias de seguridad (UPSJB 28%), virus informáticos (UNMSM 56%), corroboran con lo que está pasando a nivel mundial, donde el 70% de los rodos o accidentes que se producen en los sistemas informáticos de las organizaciones los causan los propios trabajadores, ya que muchas veces son resultados de errores, descuidos o desconocimiento sobre la seguridad de la organización o actos delictivos propiamente dichos.

Espinoza, (2013) Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para la empresa de producción y comercialización de productos de consumo masivo, de la Pontificia Universidad Católica del Perú.

Tuvo como objetivo: Analizar y diseñar un sistema de gestión de seguridad de información, basado en la norma ISO/IEC 271001:2005, para una empresa dedicada a la producción y comercialización de alimentos de consumo masivo, por lo tanto, la investigación llegó a la siguiente conclusión:

Debe tenerse en cuenta que el diseño de SGSI presentado se adapta a los objetivos actuales del proceso de producción, en el cual se ha basado el proyecto, y que este diseño podría variar ya que los objetivos estratégicos y de gobierno de le empresa pueden cambiar y por ello algunos sub procesos que forman parte del alcance del proyecto, también lo harán Del mismo modo, se debe establecer que los dueños de cada uno de los procesos que fueron analizados para el diseño del SGSI de este proyecto, empiecen a darle mayor importancia a la seguridad de la información, y que velen para que de alguna manera se pueda levantar los riesgos encontrados dentro de sus actividades ya que no es seguro que este diseño se logre implementar, y por ello debería ser labor de ellos el tratar de eliminar dichos riesgos.

Esta investigación es de suma importancia, porque habla de información en el ámbito profesional, es decir se refiere a uno de los activos más importantes que manejan las empresas como elemento básico sobre el que fundamentan, realizan y prestan sus servicios. Por ello la gestión de esta información, sea personal, económica, estratégica u organizativa cobra una importancia vital

para la consecución de los objetivos marcados y el buen desarrollo del negocio.

(Chumán, 2015) **en su tesis Aplicación de la Metodología MAGERIT para el Análisis y Gestión de Riesgos en los Servidores de los Sistemas de Gestión Académica de la Universidad Nacional Pedro Ruiz Gallo, para optar por el título de Ingeniero en Computación e Informática.**

Tuvo como objetivo brindar un Plan de Mitigación de riesgos basado en las medidas de seguridad ya implementadas, aplicando la metodología MAGERIT, Metodología de Análisis y Gestión de riesgos de las tecnologías de Información, la cual abarca dos procesos que son estructurados de la siguiente manera: Método de análisis de riesgos (Identificación, Dependencias y Valoración de los activos; Identificación y Valoración de las amenazas; Identificación y Valoración de las salvaguardas existentes; estimación del impacto y riesgo). Proceso De Gestión De Riesgos (Toma de decisiones y Plan de Mitigación) y la herramienta Pilar. Procedimiento Informático Lógico de Análisis de Riesgos, aplicación desarrollada en java y desarrollada a medida para la implementación de MAGERIT. Una vez aplicada la metodología concluye que, los Servidores de los sistemas de Gestión Académica tienen medidas de seguridad implementadas, pero no se encuentran ni guiadas y documentados, y no son

adecuadamente aprovechadas, por lo cual este estudio será beneficioso para reducir, minimizar o contrarrestar riesgos. Asimismo, como resultado de la aplicación de la Metodología MAGERIT y Herramienta PILAR, concluyo que los servidores están expuestos a un riesgo critico mediante amenazas como: Caída del sistema por agotamiento de recursos, Avería de origen físico o lógico, Corte del suministro eléctrico, Condiciones inadecuadas de temperatura o humedad, Robo de equipos, Perdida de equipos, errores del administrador del sistema/ seguridad, Desastres naturales, a pesar de las medidas ya tomadas por la administración del área de red-telemática. Lo cual sustenta la problemática expuesta y la importancia del desarrollo de la temática. Los servidores permiten la funcionalidad y generación del servicio de gestión académica. Presentando de esta manera un Plan de Mitigación el cual realizó tomando en cuenta factores de seguridad, la importancia de la seguridad en los activos y los servidores de los sistemas de gestión académica como principal objeto de estudio.

2.2. BASES TEÓRICAS

2.2.1. Teoría general del Riesgo

Para (Luhmann, 1998), el concepto de riesgo ser refiere a la posibilidad de daños futuros debido a decisiones particulares. Las decisiones que se toman en el presente condicionan lo que acontecerá en el futuro, aunque no se sabe de qué modo. El riesgo está caracterizado por el hecho de que, no obstante, la

posibilidad de consecuencias negativas, conviene, de cualquier modo, decidir mejor de una manera que de otra. Por lo tanto, indica (Luhmann, 1998), el riesgo depende de la atribución de los daños (posibles o efectivamente decididos) debido a una resolución que se toma en el sistema, mientras que peligro se entiende como una posibilidad de daño digna de atención, se habla de riesgo solo en el caso en que el daño se hace posible como consecuencia de una decisión tomada en el sistema y que no puede acontecer sin que hubiera mediado tal decisión.

2.2.2. Teoría general de Riesgos y Controles en Sistemas de Información

Hay riesgos inherentes, para cualquier nivel de organización o sistema. Cada organización o sistema está constituido por una serie de procesos y funciones, a su vez formados por actividades, manuales o automatizadas, que pueden estar relacionadas a un error potencial o riesgo, cada uno de los cuales tiene una causa que puede someterse a cierto nivel de control.

Los objetivos de control pueden cumplirse, o los riesgos pueden evitarse mediante una gran variedad de prácticas de control para cada actividad. El cual señala dos características fundamentales: probabilidad de ocurrencia y efecto negativo que no deseamos, directamente relacionado con la pérdida financiera (Quiroz, 1996).

2.2.3. Teoría de la Auto - Seguridad Informática

La auto-seguridad aplicada a la informática es: el correcto comportamiento de los individuos frente a las TI; comportamiento que es formado por el propio individuo, y que nos debe llevar a una conducta controlada, para evitar situaciones de riesgo que pongan en peligro la conservación de la información de la organización. La auto-seguridad es, además, una actitud, que debemos como seres inteligentes asumir con compromiso, ética y responsabilidad. La auto-seguridad podría traer beneficios a las organizaciones tales como: mejora del nivel de convivencia, regulación y optimización de resultados en los procesos, trabajo con responsabilidad, fomento de la disciplina, la organización, la excelencia y el sentido de pertenencia; calidad de vida personal y laboral, y otras tantas más. La auto-seguridad también promueve: hacer las cosas con calidad, oportunidad, transparencia y participación; mejoramiento continuo en la forma de realizar nuestra labor diaria; respeto por las normas y los demás (Moreno, 2012).

2.3. BASES CONCEPTUALES

2.3.1. ACTIVOS

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware),

comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

2.3.2. AMENAZA

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

2.3.3. DISPONIBILIDAD

Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

2.3.4. INTEGRIDAD

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada

2.3.5. CONFIDENCIALIDAD

Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados

2.3.6. AUTENTICIDAD

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

2.3.7. TRAZABILIDAD

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

2.3.8. ATAQUE

Se dice que se ha producido un ataque accidental o deliberado contra el sistema cuando se ha materializado una amenaza. En función del impacto causado a los activos atacados, los ataques se clasifican en:

- Activos. Si modifican, dañan, suprimen o agregan información, o bien bloquean o saturan los canales de comunicación.
- Pasivos. Solamente acceden sin autorización a los datos contenidos en el sistema. Son los más difíciles de detectar.

Un ataque puede ser directo o indirecto, si se produce desde el atacante al elemento “víctima” directamente, o a través de recursos o personas intermediarias.

2.3.9. APLICACIONES (SOFTWARE)

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos

permitiendo la explotación de la información para la prestación de los servicios.

2.3.10. EQUIPOS INFORMÁTICOS (HARDWARE)

Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

2.3.11. REDES DE COMUNICACIONES

Instalaciones dedicadas como servicio de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de trasporte que llevan datos de un sitio a otro.

2.3.12. EQUIPAMIENTO AUXILIAR

Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

2.3.13. INSTALACIONES

Lugares donde se hospedan los sistemas de información y comunicaciones.

2.3.14. PERSONAL

Personas relacionadas con los sistemas de información.

2.3.15. IMPACTO

Es la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado.

Los impactos pueden ser cuantitativos, si los perjuicios pueden cuantificarse económicamente, o cualitativos, si suponen daños no cuantificables, como los causados contra los derechos fundamentales de las personas.

2.3.16. VULNERABILIDAD

Es aquella debilidad que poseen los activos y que pueden ser explotados por una o más amenazas. Las vulnerabilidades en sí mismas no causan daño, el daño se produce cuando una amenaza explota la vulnerabilidad. Cuando hablamos de vulnerabilidades no solo nos referimos a aquellas que afectan a los sistemas, existen vulnerabilidades que afectan a otros recursos como a las infraestructuras, al personal, etc.

2.3.17. ANÁLISIS DE RIESGO

En un entorno de sistemas de información, existen una serie de recursos humanos, técnicos, de infraestructura, organizativos o de gestión, que están expuestos a diferentes tipos de riesgos usuales en cualquier entorno, y a otros excepcionales, que afectan, o pueden afectar a toda o a parte de una organización, como la inestabilidad política en un país o la ubicación de la empresa en una región sensible a terremotos, tornados o inundaciones.

Para tratar de minimizar los efectos de un problema de seguridad, se realiza el denominado análisis de riesgos, término que hace referencia al proceso necesario para responder a tres cuestiones básicas de la seguridad de una organización, que es:

- ¿Qué queremos proteger?
- ¿Contra quién o qué se quiere proteger?
- ¿Cómo lo vamos a hacer?

El análisis de riesgos constituye una parte clave de la gestión de éstos y están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. Es un proceso consistente en identificar los peligros que afectan a la seguridad, determinar su magnitud e identificar las áreas que necesitan salvaguardas. La valoración de riesgos es el resultado del proceso del análisis de riesgos.

2.3.18. IDENTIFICACIÓN DE AMENAZAS

MAGERIT presenta un catálogo de amenazas posibles sobre los activos de un sistema de información.

- De origen natural: Hay accidentes naturales (terremotos, inundaciones,...). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.
- Del entorno (de origen industrial): Hay desastres industriales (contaminación, fallos eléctricos) ante los cuales el sus-tema

de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

- Defectos de las aplicaciones: Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, 'vulnerabilidades'.
- Causadas por las personas de forma accidental: Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
- Causadas por las personas de forma deliberada: Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

2.3.19. SALVAGUARDA

Mecanismos, estrategias o procedimientos que nos permiten asegurar y mantener efectiva la viabilidad del funcionamiento del recurso. La función esencial de las salvaguardas consiste en proteger y resguardar los criterios de seguridad de los activos de mayor valor, son medidas, procedimientos o mecanismos que

permiten asegurar el desenvolvimiento efectivo de los mismos hasta el cumplimiento de su vida útil.

2.3.20. SEGURIDAD

La capacidad de las redes o de los sistemas de información de resistir, los accidentes o acciones ilícitas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios.

2.3.21. SEGURIDAD DE LA INFORMACIÓN

Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad: Disponibilidad, Autenticación, Confidencialidad e Integridad.

2.3.22. POLÍTICA DE SEGURIDAD

Una o más reglas de seguridad, procedimientos, prácticas o directrices impuestas por una organización sobre sus operaciones.

La evaluación de los principios de seguridad de nivel informático se efectúa con mayor énfasis y aplicación en sistemas operativos,

bases de datos, redes, etc. debido al aumento exponencial de usuarios involucrados (potenciales atacantes) en las redes informáticas, aumento de la complejidad del sistema, límites desconocidos y por los múltiples puntos de ataque a través de la red.

2.3.23. CULTURA DE SEGURIDAD

Para que la implementación de las políticas de seguridad se desarrolle de manera efectiva requiere el involucramiento del personal que labora en la organización, por lo tanto, la labor de las direcciones de la organización debe ser el fomentar una cultura y un clima de seguridad, donde todos los involucrados puedan ser conscientes de la importancia de la seguridad de los activos de mayor valor de la organización.

Reúne un conjunto de prácticas implantadas en las empresas tendentes a la eliminación o reducción de los riesgos derivados del trabajo, las cuales se han venido considerando como factores integrantes de la cultura de seguridad de la empresa.

2.3.24. ENFOQUE DE PREVENCIÓN

Un modelo organizativo que conduzca hacia una seguridad integrada, prevención participativa y prevención integral en el proceso y en todos los niveles jerárquicos de la empresa, donde la seguridad sea considerada inseparable de los procesos de fabricación y donde las funciones correspondientes a la seguridad se transfieran a la línea jerárquica.

2.4. DEFINICIÓN DE TÉRMINOS BÁSICOS

- **Declaración de aplicabilidad**

  Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

- **Evaluación de salvaguardas**

  Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

- **Análisis de riesgos**

  Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

- **Estado de riesgo**

  Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

- **Informe de insuficiencias**

  Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.

- **Confidencialidad:**

  Permite que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no

autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

- **Plan de seguridad**

  Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos.

- **Disponibilidad**

  Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

- **Integridad:**

  Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

- **Mapa de riesgos**

  Relación de las amenazas a que están expuestos los activos.

- **Autenticidad:**

  Propiedad o característica que consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener

manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

- **Riesgo**

  Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Nivel y Tipo de estudio

Nivel de estudio

Tiene 2 niveles; descriptivo - explicativo.

- Descriptivo, porque se busca especificar el riesgo que sufren los activos informáticos ante posibles amenazas. También conocida como la investigación estadística, se describen los datos y

características de la población o fenómeno en estudio. Este nivel de Investigación responde a las preguntas: quién, qué, dónde, cuándo y cómo. (Hernández, 2010).

- Explicativo, porque se enfoca en explicar las causas por qué ocurre un fenómeno y en qué condiciones se manifiesta, o por qué se relacionan dos o más variables (Morales, 1994).

Tipo de estudio

El tipo de investigación que corresponde a la presente tesis, es de tipo aplicada.

- Aplicada, porque se busca el conocer para hacer, para actuar, para construir, para modificar donde se presenta el fenómeno que quiere estudiarse (Ander-Egg, 2011). Es decir, se interesa fundamentalmente por la propuesta de solución en un contexto físico-social específico. Y destina sus esfuerzos a resolver los problemas y necesidades que se plantean los hombres en sociedad en un corto, mediano o largo plazo (Lozada, 2014, p.25).

3.2. Diseño de la Investigación

La presente Investigación se ubica en el diseño pre experimental; pues este consiste en administrar un estímulo a un grupo para luego aplicar una medición de una o más variables para observar. Con un diseño de pre prueba – pos prueba con un solo grupo. En este diseño si existe un punto de referencia inicial para ver qué nivel tenía el grupo en las variables

dependientes antes del estímulo. (Sampieri, 1994).

De esta manera se realizara el análisis de la seguridad de la información mediante el modelo propuesto ARSI; antes y después de la aplicación del software para el control y monitoreo de los riesgos de los activos informáticos, en la Cooperativa de Ahorro y crédito San Francisco LTDA.289.

El esquema es lo siguiente.

Esquema de la Investigación:

En el diseño de pre prueba – pos prueba:

G O1 --- X ----O2

Leyenda:

O1: Pre prueba - Análisis de la seguridad de la información.

X: Modelo ARSI (implementación del software para el control y monitoreo)

O2: Pos prueba- Análisis de la seguridad de la información.

3.3. Población

La población está conformada por 317 activos informáticos, pertenecientes a la Cooperativa de Ahorro y Crédito San Francisco LTDA. 289, oficina principal Huánuco, Oficina especial Plaza de armas y Oficina permanente Amarilis.

Tabla 2. Población proyectada para la investigación.

Activos	Población Total Proyectada
Oficina principal Huánuco	235
Oficina especial Plaza de armas	63
Oficina permanente Amarilis	19

Total	317

Elaboración propia

3.4. Muestra

La muestra es no probabilística, considerándose un muestreo intencional que busca ser representativa, la misma que está constituida por 140 tipos de activos informáticos, pertenecientes a la Cooperativa de Ahorro y Crédito San Francisco LTDA. 289, oficina principal Huánuco. De la misma manera que la población.

3.5. Técnicas de recolección de datos

Para analizar la información se utilizó las siguientes técnicas:

- **Documentación:** Se recolectó información de las áreas de sistemas y contabilidad de la Cooperativa San Francisco para así poder recoger las características y contenidos de los mismos.
- **Entrevista:** Se consultó a un especialista en el área de sistemas acerca de los equipos e información que nos pueda facilitar para la absorción de todas las interrogantes que esta investigación nos originó, los cuales podían ser levantados por sus conocimientos en las áreas.
- **Fichas de observación:** Estos instrumentos son muy importantes, evitan olvidar datos, personas o situaciones, por ello el investigador debe tener siempre a la mano sus fichas para completar el registro anecdótico que realiza cuando su investigación requiere trabajar directamente con ambientes o

realidades.

- **Check List:** Este instrumento se aplicó para poder para reducir los errores provocados por los potenciales límites de la memoria y la atención en la observación que se realizó de los activos.

3.6. Validación y confiabilidad del instrumento

El criterio de validez y confiabilidad del modelo ARSI tiene que ver con el contenido interno del modelo, y la validez de construcción de las actividades en relación con las bases teóricas y objetivos de la investigación respetando su consistencia y coherencia técnica.

Aplicamos el alfa de Cronbach para determinar la validez y confiabilidad:

$$\alpha = \left[\frac{K}{K-1}\right].\left[1 - \frac{\sum_{i=1}^{K} \sigma_i^2}{\sigma_t^2}\right]$$

Donde:

$\sum_{i=1}^{K} \sigma_i^2$: Es la suma de varianzas de cada ítem.

σ_t^2 : Es la varianza del total de filas (Varianza de la suma de los ítems).

K: Es el número de preguntas o ítems

$$\alpha = \left[\frac{8}{8-1}\right] * \left[1 - \frac{1.333}{6.653}\right]$$

$$\alpha = 0.9142$$

El alfa de Cronbach no es un estadístico al uso, por lo que no viene acompañado de ningún p-valor que permita rechazar la hipótesis de fiabilidad en la escala. Sin embargo, cuanto más se aproxime a su valor máximo, 1, mayor es la confiabilidad de la escala. Además, en determinados contextos y por tácito convenio, se considera que valores del alfa superiores a 0,8 o 0,9 (dependiendo de la fuente) son suficientes para garantizar la fiabilidad de la escala. Cuanto menor sea la variabilidad de respuesta por parte de los jueces, es decir haya homogeneidad en las respuestas dentro de cada ítem, mayor será el alfa de Cronbach.

Dado el siguiente cuadro con los niveles de confiabilidad para el alfa de Cronbach:

Tabla 3. Validez y confiabilidad del instrumento

CRITERIO DE CONFIABILIDAD	VALORES
Inaceptable	Menor a 0,5
Pobre	Mayor a 0,5 hasta 0,6
Cuestionable	Mayor a 0,6 hasta 0,7
Aceptable	Mayor a 0,7 hasta 0,8
Bueno	Mayor 0,8 hasta 0,9
Excelente	Mayor 0,9

Elaborado por George y Mallery (2003,p 231)

En vista a los resultados obtenidos en la confiabilidad del modelo ARSI, observamos que este reside en la escala de **EXCELENTE** lo que garantiza la validez y confiabilidad de nuestro modelo propuesto.

3.7. Procedimiento

Se realizó el siguiente procedimiento:

Recolección de los datos. Se realizó el análisis de riesgos de los sistemas de información mediante un estudio de diferentes metodologías la cual nos permitió proponer un modelo que se ajuste a la realidad de actuar de la cooperativa de Ahorro y Crédito San Francisco.

Revisión de los datos. Se examinó en forma crítica los resultados obtenidos a fin de comprobar la integridad de sus respuestas.

El ordenamiento de la Información: Este paso consistió básicamente en depurar la información revisando los datos contenidos en los instrumentos de trabajo de campo, con el propósito de ajustar los llamados datos primarios.

Procesamiento de los datos. Previa codificación de los reportes, se elaboró una plataforma de datos utilizando el programa estadístico SPSS versión 22 en español, y se registraron los datos procedentes de la aplicación del modelo; no olvidando parear los instrumentos aplicados.

Clasificación de la Información: Se llevó a cabo con la finalidad de agrupar datos mediante la distribución de frecuencias de las variables independiente y dependiente.

Tabulación

Puntualizamos las acciones realizadas con la finalidad de procesar y analizar la información obtenida para su tabulación.

La Codificación y Tabulación: La codificación es la etapa en la que se forma un cuerpo o grupo de símbolos o valores de tal manera que los datos serán tabulados, generalmente se efectúa con números o letras. La tabulación manual se realizó ubicando cada uno de las variables en los grupos establecidos en la clasificación de datos, o sea en la distribución de frecuencias. También se utilizó la tabulación mecánica, aplicando programas o paquetes estadísticos de sistema computarizado.

Análisis descriptivo e Interpretación de datos:

En cuanto al análisis descriptivo de cada una de las variables se tuvo en cuenta las medidas de tendencia central, de dispersión para las variables y de porcentaje para las variables categóricas.

Análisis inferencial e Interpretación de datos:

Asimismo, en el análisis inferencial de los datos se utilizó el coeficiente de correlación de Rho de Spearman con el fin de medir la relación entre las variables en estudio. Se tuvo en cuenta una significación de 0,05.

Para el procesamiento de los datos se utilizó el paquete estadístico SPSS versión 22 en español, Minitab.

CAPÍTULO IV

CONSTRUCCIÓN DEL MODELO ARSI

Para la construcción del Modelo ARSI, se estudió diferentes metodologías orientadas al análisis de riesgo de los sistemas de información.

Para ello el Instituto Nacional de Normas y Tecnología que administra la de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida. (NIST, s.f.)

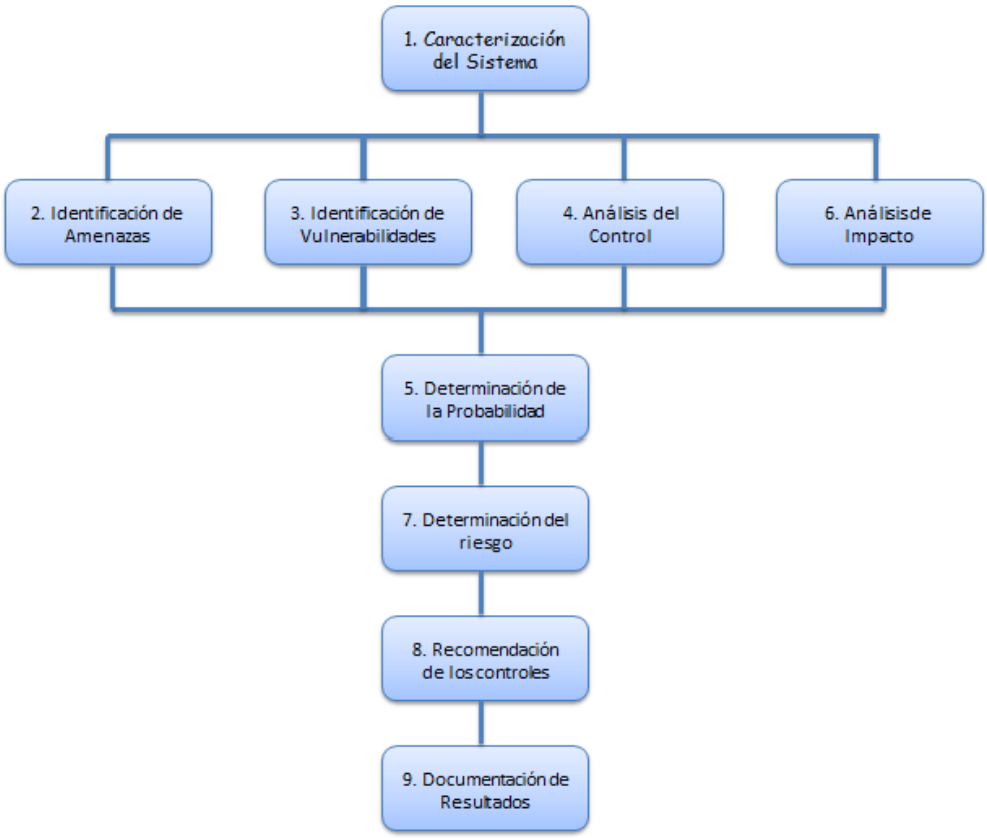
Evaluación de riesgos

La evaluación de riesgos es el primer proceso en la metodología de gestión de riesgos. Las organizaciones utilizan la evaluación de riesgos para determinar el alcance de la amenaza potencial y el riesgo asociado con un sistema de tecnología de la información a través del desarrollo del ciclo de vida del sistema. El resultado de este proceso ayuda a identificar los controles adecuados para reducir o eliminar los riesgos durante el proceso de mitigación de los mismos. La metodología de evaluación de riesgos trabaja bajo nueve pasos principales, que se describen a continuación:

1. Caracterización del Sistema
2. Identificación de amenazas
3. Identificación de vulnerabilidades
4. Análisis de Control
5. Determinación de la probabilidad
6. Análisis de Impacto
7. Determinación de Riesgos
8. Recomendaciones de los controles
9. Documentación de Resultados

Los pasos 2, 3, 4 y 6 se pueden realizar en paralelo después de terminar el 1er paso. La siguiente figura describe los pasos y las entradas y salidas de cada etapa.

Gráfico 1. Propuesta para el análisis de riesgos



Caracterización del sistema

En la evaluación de los riesgos de un sistema informático, el primer paso es definir el alcance del esfuerzo. En este paso, los límites del sistema de tecnología de la información son identificados, junto con los recursos y la información que conforman el sistema. En la caracterización de un sistema de tecnología de información se establece el alcance del esfuerzo de la evaluación del riesgo, se delinea la autorización operacional de los límites, y ofrece información (por ejemplo, hardware, software, la conectividad del sistema, y responsable de la división o el apoyo personal), esencial para definir el riesgo. Es importante que todas las interfaces y las dependencias estén bien definidas antes de aplicar la

metodología. La información relacionada al sistema se puede clasificar de la siguiente manera:

- Hardware:
- Software
- Las interfaces del sistema (por ejemplo, la conectividad interna y externa)
- Los datos y la información
- Las personas que apoyan y utilizan el sistema de TI
- Misión del Sistema (por ejemplo, los procesos realizados por el sistema informático)
- Criticidad en el Sistema y en los datos
- Sensibilidad del Sistema y los datos
- Los requisitos funcionales del sistema de TI
- Los usuarios del sistema
- Sistema de seguridad de la arquitectura
- Diagrama de la red
- Las políticas de seguridad del sistema que rigen el sistema informático (políticas de la organización, requisitos federales, leyes, prácticas de la industria)
- Protección de la información almacenada, la disponibilidad de datos, la integridad y la confidencialidad
- Flujo de información relacionada con el sistema informático
- Los controles técnicos utilizados en el sistema
- Gestión de los controles utilizados para el sistema de TI

- Las políticas de funcionamiento utilizados para el sistema informático.
- Entorno de seguridad física del sistema informático
- La seguridad ambiental

Identificación de las vulnerabilidades

El análisis de la amenaza a un sistema informático debe incluir un análisis de las vulnerabilidades asociadas con el sistema de medio ambiente. El objetivo de este paso es elaborar una lista de las vulnerabilidades del sistema (defectos o puntos débiles) que podrían ser explotados por la amenaza potencial de fuentes. Los métodos recomendados para la identificación de las vulnerabilidades del sistema son:

- Uso de las fuentes de la vulnerabilidad
- Mejoramiento de las pruebas de seguridad del sistema
- Desarrollo de una lista de requerimientos de seguridad.

Las fuentes de la vulnerabilidad que deben ser considerados en un análisis de vulnerabilidades incluyen:

- Una previa documentación de análisis de riesgos de los sistemas TI evaluados
- Los informes de auditoría del sistema de TI, los informes de anomalías del sistema, los informes de revisión de seguridad, y los informes de prueba y evaluación del sistema
- Las listas de vulnerabilidad, como la base de datos de vulnerabilidad NIST NVD (http://nvd.nist.gov/)
- Avisos de seguridad

- Avisos de proveedores
- Comercial equipo de incidentes / equipos de emergencia de respuesta.
- Información de alertas y boletines de Garantía de la vulnerabilidad a los sistemas militares
- Sistema de análisis de software de seguridad.

Análisis del control

El objetivo de este paso es analizar los controles que se han implementado o están a punto de implementarse por la organización para minimizar o eliminarla la probabilidad de una amenaza del sistema. Para obtener una calificación de riesgo global que indica la probabilidad de que una vulnerabilidad potencial puede ser ejercida dentro de la construcción del entorno de las amenazas asociadas, la aplicación de los controles actuales o previstos que deben ser considerados. Hay dos tipos principales de controles:

- Controles técnicos: Son incorporados en hardware, software o firmware (por ejemplo, el acceso mecanismos de control, identificación y autenticación de los mecanismos, métodos de encriptación, la intrusión de software de detección).
- Controles no técnicos: Son los controles operacionales y de gestión, tales como las políticas de seguridad, los procedimientos operacionales y de personal, físico y ambiental.

Determinación de la probabilidad

Para obtener una calificación de riesgo global que indica la probabilidad de que una vulnerabilidad potencial puede materializarse dentro de la construcción del entorno de las amenazas asociadas, los siguientes factores deben ser considerados:

- Fuente de amenaza
- Naturaleza de la vulnerabilidad
- Existencia y eficacia de los controles actuales.

Tabla 4. La probabilidad de que una vulnerabilidad potencial pueda suceder por una fuente de amenaza

Nivel de Probabilidad	Definición de la probabilidad
Alta	La fuente de amenaza es altamente motivada y suficientemente capaz. Los controles para prevenir que la vulnerabilidad suceda son ineficientes.
Media	La fuente de amenaza es motivada y capaz. Los controles pueden impedir el éxito de que la vulnerabilidad suceda.
Baja	La fuente de amenaza carece de motivación. Los controles están listos para prevenir o para impedir significativamente que la vulnerabilidad suceda.

Determinación del riesgo

El propósito de este paso es evaluar el nivel de riesgo para el sistema de TI. La determinación del riesgo para una determinada amenaza / vulnerabilidad se puede expresar en función de:

- La probabilidad de una determinada amenaza
- La magnitud del impacto de una amenaza materializada
- La adecuación de los controles de seguridad existentes o previstos para reducir o eliminar el riesgo.

La determinación final de la misión de riesgo se obtiene multiplicando las calificaciones asignadas por la probabilidad de la amenaza y el impacto de la amenaza.

Escala de riesgo:

- Alto: 50 – 100
- Medio: 10 – 50
- Bajo: 1 – 10

Tabla 5. Escala de riesgos

Probabilidad de amenaza	Impacto		
Bajo (10)	Medio (50)		Alto (100)
Alto (1.0)	Bajo 10 x 1.0 = 10	Bajo 50 x 1.0 = 50	Bajo 100 x 1.0 = 100
Medio (0.5)	Bajo 10 x 0.5 = 5	Bajo 50 x 0.5 = 25	Bajo 100 x 0.5 = 50

Recomendaciones de los controles

Inicialmente se deciden que controles se van a utilizar ya sea para mitigar (reducir el nivel de riesgo para el sistema informático y sus datos a un nivel aceptable) o eliminar los riesgos identificados. Los siguientes factores se deben considerar a la hora de recomendar los controles y las alternativas de solución o las alternativas para minimizar o eliminar los riesgos identificados:

- Efectividad de las opciones recomendadas (por ejemplo, la compatibilidad con el sistema)

- Legislación y regulación
- La política de la organización
- El impacto operacional
- Seguridad y fiabilidad.

Documentación de resultados.

Una vez que la evaluación del riesgo se ha completado, los resultados deben ser documentados en un documento oficial.

Un informe de evaluación de riesgos es un informe de gestión que ayuda a la gerencia a tomar decisiones sobre la política, el presupuesto de procedimiento y la gestión de cambios que se deben tener en cuenta con el sistema operativo.

Salida: Reporte de la evaluación del riesgo que describe las amenazas y vulnerabilidades, medidas del riesgo y provee recomendaciones para la implementación de los controles.

4.2. OCTAVE

Hay cuatro áreas de actividad que se lleva a cabo a través de ocho pasos de la Metodología de Octava Allegro. Las áreas de actividad son:

- Establecer los controladores, donde la organización desarrolla los criterios de medición de riesgos que son consistentes con los conductores de la organización.
- Los activos perfil, donde los bienes que son el foco de la evaluación de riesgos se identifican y se perfila y los contenedores de los activos se identifican.

- Identificar las amenazas, donde las amenazas a los activos-en el contexto de sus envases se identifican y documentado a través de un proceso estructurado.
- Identificar y mitigar los riesgos, donde los riesgos se identifican y analizan sobre la base de información sobre amenazas, y estrategias de mitigación que hagan frente a esos riesgos.

Los resultados de cada paso en el proceso son capturados en una serie de hojas de trabajo que luego se utilizan como insumos para el siguiente paso en el proceso. Los distintos pasos de la metodología se describen con más detalle a continuación. Establecer criterios de medición del riesgo.

Se establecen los controladores de la organización que evalúan los efectos de un riesgo de la misión de una organización y los objetivos de negocio. Estos conductores se reflejan en un conjunto de criterios de medición de riesgo que se crea y se registra como parte de este primer paso.

El método OCTAVE Allegro proporciona un conjunto estándar de plantillas de hoja de trabajo para crear estos criterios en varias áreas de impacto y establecer prioridades. Las áreas de impacto que se consideran son:

- Confidencialidad, Reputación/cliente
- Financiero
- Productividad
- Salud y seguridad
- Penalidades Legales

- Definición de áreas de impacto del usuario

Se debe priorizar las áreas de impacto de la más importante a la menos importante

✓ **Desarrollar un perfil de Activos de Información.**

La metodología OCTAVE Allegro se centra en los activos de información de la organización para lo cual se realiza el proceso de creación de un perfil de esos activos. Un perfil es una representación de una información de los activos que describe sus características únicas, cualidades, características y valor. Para desarrollar el perfil se debe tener en cuenta las siguientes actividades:

- Identificar el grupo de activos de información al cual se le va a realizar el perfil
- Enfocarse en los activos de información más críticos
- Obtener información necesaria para empezar a estructurar el proceso de análisis de riesgos del activo.

✓ **Identificar los contenedores de los activos de la información.**

Los contenedores describen los lugares en los que la información es almacenada, transportada y procesada. Los activos de información residen no sólo en los contenedores dentro de los límites de una organización, sino también a menudo en envases que no están bajo el control directo de la organización. Los diferentes tipos de contenedores se describen a continuación:

- Contenedores técnicos: Están bajo el control directo de la organización o los que son administrados fuera de la organización.

- Contenedores físicos: La información pues estar de dentro o fuera de la empresa.
- Contenedor persona: Persona interna o externa de la organización que tiene el conocimiento detallado del activo.

✓ **Identificar las áreas de interés**

En este paso se realiza el proceso de identificación de riesgos con lluvia de ideas acerca de las condiciones o situaciones que pueden poner en peligro los activos de información de la organización. Estos escenarios del mundo real se refieren a las áreas de preocupación y pueden representar amenazas y sus correspondientes resultados no deseados.

✓ **Identificar las situaciones de amenaza**

En la primera mitad de la etapa 5, las áreas de interés identificadas en el paso anterior se expanden en escenarios de amenaza. Una serie de escenarios de amenaza pueden ser representados visualmente en una estructura de árbol comúnmente conocido como un árbol de amenaza.

✓ **Identificar los riesgos**

En el anterior paso se identificaron las amenazas, y en este se identificarán las consecuencias en una organización. Una amenaza puede tener múltiples impactos potenciales sobre una organización. Por ejemplo, la interrupción de sistema de comercio electrónico de una organización puede afectar la reputación de la organización con sus clientes, así como su posición financiera.

✓ **Analizar los riesgos**

Se calcula una medida cuantitativa en que la organización se ve afectada por una amenaza. Esto se realiza teniendo en cuenta el escenario de amenaza y su consecuencia. Luego se determinar un valor de impacto (bajo, medio, moderado) para cada área de impacto. Por último se computa los valores de impacto de cada área para analizar el riesgo y así ayudar a la organización a determinar la mejor estrategia para manejar ese riesgo.

- ✓ **Seleccione enfoque de mitigación.**

La organización determina cuál de los riesgos que han identificado requieren mitigación desarrollando una estrategia para esto. La organización debe ordenar cada uno de los riesgos que ha identificado por su calificación ayudándole de manera ordenada a tomar decisiones sobre su estado de mitigación. A continuación se debe asignar un enfoque de mitigación para cada uno de esos riesgos y por último desarrollar la estrategia de mitigación que se decida para mitigar el riesgo. Las hojas de trabajo han sido diseñadas para que puedan ser traducibles fácilmente a otros formatos electrónicos.

4.3. METODOLOGÍA MAGERIT

1. Determinar los activos

Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.

Se denominan activos los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

El activo esencial es la información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

Tipos de activos

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes.

Si el sistema maneja datos de carácter personal, estos suelen ser importantes por sí mismos y requerir una serie de salvaguardas frecuentemente reguladas por ley. En estos activos interesa determinar qué tratamiento hay que imponerles. El hecho de que un dato sea de carácter personal impacta sobre todos los activos involucrados en su tratamiento y custodia.

Algo similar ocurre con los datos sometidos a una clasificación de confidencialidad. Cuando se dice que un cierto informe está clasificado como “reservado”, de forma que las copias están numeradas, sólo pueden llegar a |ciertas personas, no deben salir del recinto y deben ser destruidas concienzudamente, etc. se están imponiendo una serie de salvaguardas porque lo ordena el reglamento, sectorial o específico de la Organización.

Dependencias

Los activos más llamativos suelen ser los datos y los servicios; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones o las frecuentemente olvidadas personas que trabajan con aquellos. Por ello aparece como importante el concepto de “dependencias entre activos” o la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior.

Se dice que un “activo superior” depende de otro “activo inferior” cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores. Aunque en cada caso hay que adaptarse a la Organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

- capa 1: el entorno: activos que se precisan para garantizar las siguientes capas
    - equipamiento y suministros: energía, climatización, comunicaciones
    - personal: de dirección, de operación, de desarrollo, etc.
    - otros: edificios, mobiliario, etc.
- capa 2: el sistema de información propiamente dicho
    - equipos informáticos (hardware)
    - aplicaciones (software)
    - comunicaciones
    - soportes de información: discos, cintas, etc.
- capa 3: la información
    - datos
    - meta-datos: estructuras, índices, claves de cifra, etc.
- capa 4: las funciones de la Organización, que justifican la existencia del sistema de información y le dan finalidad
    - objetivos y misión
    - bienes y servicios producidos
- capa 5: otros activos
    - credibilidad o buena imagen
    - conocimiento acumulado
    - independencia de criterio o actuación
    - intimidad de las personas
    - integridad física de las personas

Valoración

No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

1. Determinar a qué amenazas están expuestos aquellos activos

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

Hay accidentes naturales (terremotos, inundaciones,...) y desastres industriales (contaminación, fallos eléctricos,...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos. Hay amenazas causadas por las personas, bien errores, bien ataques intencionados.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

- Degradación: cuán perjudicado resultaría el activo
- Frecuencia: cada cuánto se materializa la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

Tabla 6. Frecuencia causada por el daño

La frecuencia se modela como una tasa anual de ocurrencia, siendo	Muy frecuente	A diario

valores típicos 100		
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco frecuente	Cada varios años

Agregación de riesgos

Los párrafos anteriores determinan el riesgo que sobre un activo tendría una amenaza en una cierta dimensión. Estos riesgos singulares pueden agregarse bajo ciertas condiciones:

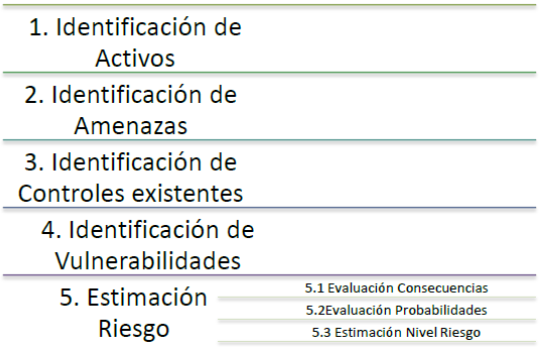
- Puede agregarse el riesgo repercutido sobre diferentes activos,
- Puede agregarse el riesgo acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún activo superior común,
- No debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores,
- Puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,
- Puede agregarse el riesgo de una amenaza en diferentes dimensiones.

Con el objeto de organizar la presentación, se tratan primero los pasos 1, 2, 4 y 5, obviando el paso 3, de forma que las estimaciones de impacto y riesgo sean “potenciales”: caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las

salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

4.4. ISO 27005

Es el mayor desarrollador mundial y editor de Normas Internacionales. ISO es una red de los institutos de normas nacionales de 162 países, un miembro por país, con una Secretaría Central en Ginebra, Suiza, que coordina el sistema.



Tecnologías de la información – Técnicas de seguridad – Gestión de riesgo de seguridad de la información.

La norma ISO 27005 dentro de la evaluación de los riesgos de la seguridad de la información tiene como actividades el análisis de riesgos y la evaluación del mismo. A continuación se encuentran las actividades que se llevan a cabo para el análisis de riesgos:

Pasos Análisis de Riesgo.

 Identificación del riesgo:

El propósito de esta actividad es determinar qué cosas pueden pasar que cause pérdidas potenciales, al igual que saber cómo, dónde y por qué pueden suceder esas pérdidas. A continuación se explicarán los pasos que se llevan a cabo en esta actividad.

1. Identificación de activos

- ***Entrada:*** Alcance y límites para la evaluación de los riesgos. Lista de constituyentes con sus propietarios, localización, función, etc.

- ***Acción:*** El activo dentro del alcance establecido debe ser identificado.

- Un activo es algo que la organización valora y considera que necesita protección. Se debe realizar esta identificación en un nivel de detalle que provea suficiente información para la evaluación de los riesgos.

- Cada activo debe tener un propietario para tener a algún responsable

- ***Salida:*** Lista de activos a ser administrado por los riesgos y una lista de procesos de negocio relacionados con los activos y su relevancia.

2. Identificación de amenazas

- ***Entrada:*** Información sobre amenazas obtenida de la revisión de incidentes, propietario de los activos, los usuarios y de otras fuentes, incluidos los catálogos de las amenazas externas

- ***Acción:*** Las amenazas y sus fuentes deben ser identificadas.

- Las amenazas pueden ser accidentales (A), deliberadas (D) o ambientales (E).

- D se utiliza para todas las acciones deliberadas dirigidas a los activos de información.

- A se utiliza para todas las acciones humanas que accidentalmente puede dañas los activos de información.

- E se utiliza para todos los incidentes que no están basados en acciones humanas.

- Hay diferentes tipos de amenazas, ejemplo: acciones no autorizadas, daños físicos, fallos técnicos.

- Algunas amenazas pueden afectar varios activos pero con diferente tipo de impacto.

- La identificación de las amenazas y de la probabilidad de ocurrencia debe ser obtenido de los propietarios o usuarios del activo, personal de recursos humanos, gestión de instalaciones, especialistas en la seguridad de la información, expertos en seguridad física, departamento legal, autoridades meteorológicas, compañías de seguros y autoridades de gobierno nacional. No se debe olvidar considerar los aspectos de ambiente y cultura.

- ***Salida:*** Una lista de amenazas con la identificación del tipo de amenaza y su fuente.

3. Identificación de controles existentes

- Entrada: Documentación de controles y el plan de implementación del tratamiento de los riesgos

- Acción: Controles existentes y planeados deben ser identificados

- Es importante identificar los controles existentes para evitar trabajo y costo innecesario. También es importante revisar que esos controles están funcionando correctamente.

- Se debe tener una medida de eficacia del control para poder identificar el control efectivamente. Se puede mirar como ése control reduce la probabilidad y facilita la explosión de la vulnerabilidad o el impacto del incidente.

- Los siguientes son actividades que ayudan a la identificación de controles existentes y planeados:

- Revisar documentos que tengan información acerca de controles. Si se cuenta con los procesos de la administración de la seguridad de la información bien documentados, los controles y su estado de implementación debe estar disponible.
- Revisar con las personas responsables de la seguridad de la información y los usuarios que los controles están implementados para los procesos de información.
- Llevar a cabo una revisión en el lugar de los controles físicos, comparando los implementados con la lista de los controles que deberían estar ahí y revisar que los implementados estén funcionando correctamente y efectivamente
- Revisar resultados de auditorías internas
- Salida: Una lista de todos los controles existentes y planeados, su implementación y estado de uso

4. Identificación de vulnerabilidades

- Entrada: Lista de amenazas identificadas, lista de activos y controles existentes.

- Acción: Vulnerabilidades que pueden ser explotadas por una amenaza que cause daño a un activo o sencillamente que deben ser identificados por la organización.
- Las vulnerabilidades se pueden identificar en diferentes áreas como organización, procesos y procedimientos, adm. de rutinas, personal, ambiente físico, configuración de sistemas de información, hardware, software o equipos de comunicación y dependencias o partes externas.
- Una vulnerabilidad como tal no causa daño si no se presenta una amenaza. Por esta razón, si existe una vulnerabilidad que no tenga ninguna amenaza no necesitará ningún control, sin embargo se debe monitorear por si un cambio ocurre.
- Salida: Una lista de vulnerabilidades en relación con los activos, amenazas y controles; una lista de vulnerabilidades que no se relaciones con ninguna amenaza identificada para revisión.

5. Identificación de consecuencias

- Entrada: Lista de activos, lista de procesos de negocio y lista de amenazas y vulnerabilidades propiamente relacionada con los activos y su relevancia.
- Acción: Identificar las consecuencias que la pérdida de confidencialidad, integridad y disponibilidad pueden tener sobre los activos Las consecuencias pueden ser pérdida de efectividad, condiciones de operaciones adversas, pérdida del negocio, reputación, daños, etc.
- Salida: Lista de escenarios de incidentes con sus consecuencias relacionadas a los activos y procesos del negocio.

- **Estimación del riesgo:**

Para la realización de la estimación del riesgo se deben tener en cuenta las siguientes metodologías que son estimación cualitativa y estimación cuantitativa.

- Estimación cualitativa: Se utiliza una escala de atributos calificados para describir la magnitud de consecuencias potenciales (bajo, medio, alto) y la probabilidad de que esas consecuencias puedan ocurrir. Una de las ventajas de utilizar esta estimación es la facilidad de entendimiento por todo el personal dentro de la organización. La desventaja es la dependencia de la elección de la escala por alguien. Esta estimación se debe tener en cuenta:

  Como una proyección de la actividad inicial para identificar los riesgos que requieran un análisis más detallado.

  Donde ese tipo de análisis es apropiado para las decisiones.

  Donde el dato numérico o fuentes están inadecuadas para una estimación cuantitativa.

- Estimación cuantitativa: Usa una escala con valores numéricos tanto para las consecuencias como para la probabilidad, usando datos de diferentes fuentes. La calidad de este análisis depende en la precisión y completitud de los valores numéricos y la valides del modelo utilizado. Generalmente utiliza datos de incidentes históricos. La ventaja es que se puede relacionar directamente con los objetivos de seguridad de la información y los objetivos concernientes a la

organización. La desventaja es la falta de datos sobre los nuevos riesgos o debilidades de seguridad de la información

Los pasos que se deben realizar para la estimación del riesgo se explican a continuación.

1. **Evaluación de las consecuencias**

- Entrada: Lista de escenarios de incidentes relevantes que hayan sido identificados, las amenazas identificadas, vulnerabilidades, activos afectados, consecuencias de los activos y los procesos de negocio

- Acción: Evaluar el impacto del negocio sobre la organización que sucedió por un incidente, teniendo en cuenta las consecuencias del incumplimiento de la seguridad de la información (pérdida de confidencialidad, integridad o disponibilidad de los activos).

- Las consecuencias o el impacto del negocio puede ser determinado al modelar los resultados de un evento o de un conjunto de eventos, o también por la investigación de estudios experimentales o datos pasados.

- Salida: Lista de consecuencias evaluadas de un incidente en un escenario expresado con respecto a los activos y los criterios de impacto.

2. Evaluación de la probabilidad de incidentes

- Entrada: Lista de escenarios de incidentes relevantes identificados incluidos amenazas identificadas, activos afectados, vulnerabilidades explotadas y consecuencias de los activos y procesos del negocio. Lista de todos los controles existentes y planeados, la efectividad de cada uno, implementación y estado de uso.

- Acción: Evaluar la probabilidad de un incidente en un escenario.

- Después de identificar los escenarios de incidentes es necesario evaluar la probabilidad para cada uno y el impacto ocurrido. Se debe tener en cuenta que tan seguido ocurre la amenaza y que tan fácil la vulnerabilidad puede explotar, considerando

- Experiencias y estadísticas aplicadas para la probabilidad de las amenazas
- Para fuentes de amenazas deliberadas: motivación, capacidades y recursos disponibles para posibles atacantes, al igual que la percepción del atractivo y vulnerabilidades de los activos para un posible atacante
- Para fuentes de amenazas accidentales: factores geográficos, la posibilidad de condiciones extremas en el clima y factores que puedan influenciar errores humanos y el mal funcionamiento de los equipos
- Vulnerabilidades (individuales y de agregación)
- Controles existentes y cómo efectivamente se reduce la vulnerabilidad

- Salida: Probabilidad de un incidente en un escenario. (Cuantitativo o cualitativo)

3. Nivel de la estimación del riesgo

- Entrada: Lista de escenarios incidentes con sus respectivas consecuencias relacionadas con los activos y procesos del negocio y su probabilidad.

- Acción: Estimación del nivel de riesgo para todos los escenarios de incidentes relevantes

- Salida: Lista de riesgos con el valor del nivel asignado

Metodologías seleccionadas

Las metodologías que se van a proponer en la guía metodológica son:

 Guía de gestión de riesgo para los sistemas de Tecnologías de la Información. NIST: El propósito es proveer una guía que desarrolle un programa de administración de riesgos efectivo y que ayude a las organizaciones a manejar mejor las tecnologías de información relacionadas con la gestión de los riesgos

Se eligieron estas metodologías por su reconocimiento a nivel mundial que lograron al encargarse de cubrir aspectos relacionados con la seguridad de la información y que sirven de apoyo para desarrollar políticas, controles y procedimientos. Otra de las razones fueron las organizaciones responsables de esas metodologías, ya que son organizaciones con experiencia en lo que hacen.

El valor nuclear suele estar en la información (o datos) que el sistema maneja, quedando los demás activos subordinados a las necesidades de explotación y protección de la información. Por otra parte, los sistemas de información explotan los datos para proporcionar servicios, internos a la Organización o destinados a terceros, apareciendo una serie de datos necesarios para prestar un servicio. Sin entrar en detalles técnicos de cómo se hacen las cosas, el conjunto de datos y servicios finales permite caracterizar funcionalmente una organización. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios.

Dimensiones

De un activo puede interesar calibrar diferentes dimensiones:

- Autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa? Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)
- Confidencialidad: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- Integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
- Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

En sistemas dedicados a la administración electrónica o al comercio electrónico, el conocimiento de los actores es fundamental para poder prestar el servicio correctamente y poder perseguir los fallos (accidentales o deliberados) que pudieran darse. En estos activos, además de la autenticidad, interesa calibrar la:

- Trazabilidad del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?
- Trazabilidad del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Los aspectos de autenticidad y trazabilidad de los datos son críticos para satisfacer medidas reglamentarias sobre ficheros que contengan datos de carácter personal.

¿Cuánto vale la "salud" de los activos?

Una vez determinadas qué dimensiones (de seguridad) interesan de un activo hay que proceder a valorarlo. La valoración es la determinación del coste que supondría salir de una incidencia que destrozara el activo. Hay muchos factores a considerar:

- Coste de reposición: adquisición e instalación
- Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo
- Lucro cesante: pérdida de ingresos
- Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- Sanciones por incumplimiento de la ley u obligaciones contractuales
- Daño a otros activos, propios o ajenos
- Daño a personas
- Daños medioambientales

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes a respetar son:

- Homogeneidad: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores

acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra

- Relatividad: es importante poder relativizar el valor de un activo en comparación con otros activos

Todos estos criterios se satisfacen con valoraciones económicas (coste dinerario requerido para "curar" el activo) y es frecuente la tentación de ponerle precio a todo. Si se consigue, excelente. Incluso es fácil ponerle precio a los aspectos más tangibles (equipamiento, horas de trabajo, etc.); pero al entrar en valoraciones más abstractas (intangibles como la credibilidad de la Organización) la valoración económica exacta puede ser escurridiza y motivo de agrias disputas entre expertos.

Valoración cualitativa

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como "órdenes de magnitud" y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo. La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

4.5. EVALUACIÓN DE METODOLOGÍAS PARA EVALUACIÓN DEL RIESGO

Tabla 7. Evaluación de metodologías para evaluación del riesgo

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
OCTAVE	Pymes, organizaciones públicas y privadas	Es auto dirigible. Se puede desarrollar por empleados de la misma organización, utilizando un equipo multidisciplinario. Involucra a todo el personal Construcción de los perfiles de amenazas basados en activos. Identificación de la infraestructura de vulnerabilidades. Desarrollo de planes y estrategias de seguridad Comprende las etapas de análisis y gestión de riesgos Involucra procesos, activos, dependencias, recursos, vulnerabilidades, amenazas y salvaguardas. Relaciona amenazas y vulnerabilidades. Uso interno: gratuito. Posee tres métodos Octave, Octave-s y Octave allegro, adaptables a una organización	No tiene en cuenta el principio de no repudio de la información. Utiliza muchos documentos en el proceso de análisis de riesgos. Se requiere de amplios conocimientos técnicos No define claramente los activos de información. Uso externo: se debe comprar la licencia al SEI si se quiere implementar la metodología a un tercero.
MAGERIT	Gobierno, compañías grandes comerciales y no comerciales, Pymes	Alcance completo en el análisis y gestión de riesgos. Esté bien documentada en cuanto a recursos de información, amenazas y tipos de activos. Utiliza un completo análisis de riesgos cuantitativo. Es libre y no requiere autorización en diferentes grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier riesgo. Se centra en tres objetivos: Concientizar sobre la existencia de los riesgos y de la necesidad de atajarlos a tiempo, ofrecer un método	En su modelo no involucra los procesos, recursos, ni vulnerabilidades. Posee falencias en el inventario de políticas. Se considera una metodología costosa en su aplicación.

		sistemático para analizar tales riesgos, ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación. Permite que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión de riesgos efectiva. Posee una buena base documental.	
ISO 27005	Utilizada por organizaciones gubernamentales y no gubernamentales.	Bajo costo relacionado con el riesgo analizado y solventado. Proporciona una guía para evaluación de riesgos de seguridad en las infraestructuras de TI. Presenta un resumen de los elementos clave de las pruebas de seguridad técnica y la evaluación con el énfasis en técnicas específicas, sus beneficios, limitaciones y recomendaciones para su uso. La guía provee herramientas para la valoración y mitigación de riesgos. Asegura los sistemas informáticos que almacenan, procesan y transmiten información. Mejora la administración a partir de los resultados del análisis y la gestión de los riesgos	En su modelo no tiene contemplados elementos como los procesos, los activos ni las dependencias.

En este punto de desarrollo, se procedió a diseñar el modelo en base a los estudio anteriormente modificando e incorporando nuevos elementos y valores que nos proporcionen una metodología nueva y consistente y que a su vez nos permita aplicarla a la realidad organizacional en cuanto a riesgos informáticos se trate en la Cooperativa de Ahorro y Crédito San francisco.

El procedimiento se llevó a cabo a través de unificar etapas de las metodologías propuestas con similitudes y características propias de cada una de ellas, logrando obtener como resultado cinco fases y con procedimientos implementados en cada uno de ellos.

A continuación se detalla una breve descripción del modelo ARSI en referencia a las cinco propuestas:

Tabla 8. Etapas propuestas para el modelo ARSI

1. Caracterización de activos	**Etapas del modelo "ARSI"**
2. Evaluación de Amenazas	
3. Plan de tratamiento de riesgos	
4. Analizar controles	
5. Implantar Mejoras	

De las etapas anteriores se obtiene la Fase I de la siguiente manera:

Fase I: Caracterización de activos

Esta fase contempla 3 procesos:

1. Identificación de los activos de la Organización.
2. Identificación de dependencias entre activos
3. Valoración de activos y establecimiento de dimensiones.

Fase II: Evaluación de amenazas

Esta fase contempla 4 procesos:

1. Identificación de las amenazas y vulnerabilidades.

    - De origen natural
    - De origen industrial
    - Errores y fallos no intencionados
    - Ataques intencionados

2. Caracterización de la probabilidad de ocurrencia del impacto.
3. Análisis y evaluación del impacto potencial.
4. Análisis y evaluación del riesgo potencial.

Fase III: Plan de tratamiento de riesgos

Esta fase contempla 2 procesos:

1. Definir plan de tratamiento de riesgos.
2. Operar el sistema ARSI.

Fase IV: Analizar controles

Esta fase contempla 2 procesos:

1. Implementación de controles.
2. Seguimiento y control mediante el software propuesto por el modelo ARSI.

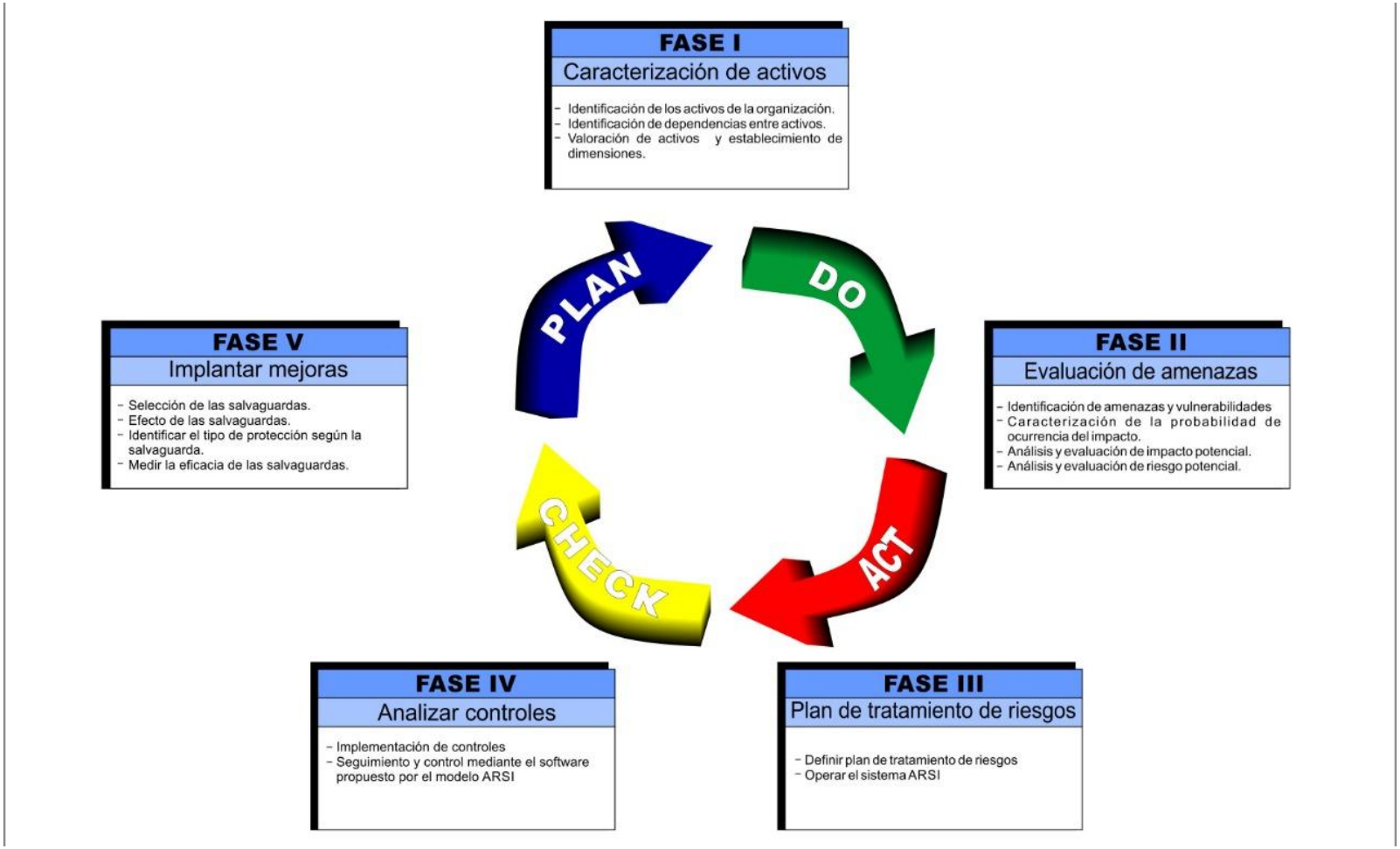
Fase V: Implantar mejoras

Esta fase contempla 4 procesos:

1. Selección de las salvaguardas, identificar salvaguardas especificas ante la presencia del amplio abanico de posibilidades.
2. Efecto de las salvaguardas, se analiza la reducción de la probabilidad de las amenazas y limitando el daño causado.
3. Identificar el Tipo de protección según la salvaguarda
4. Medir la Eficacia de protección frente al riesgo identificado

Planteado las cinco fases identificadas construimos el modelo de análisis de riesgos modelo ARSI, presentado a continuación.

Gráfico 2. Modelo ARSI - Análisis de los Riesgos de la Seguridad de la Información



CAPÍTULO V.

MODELO ARSI

Para la ejecución del modelo ARSI, utilizaremos el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

La implementación del modelo ARSI se aplicará en una primera etapa a los datos, sistemas de información, medios de enlace y redes de comunicación, infraestructura tecnológica, soportes de información, infraestructura física y funcionarios que apoyan la ejecución, de la sede Huánuco, hasta obtener un grado de madurez que luego nos permita gestionar de una manera adecuada para la sede de Tingo María y Pucallpa. Siendo en esta oportunidad aplicado a la sede Huánuco, los usuarios que tendrán acceso son:

- Gerente General.
- Gerente de Administración y finanzas.
- Gerente de Sistemas.
- Gerente de Riesgos.
- Gerente de Créditos
- Los miembros para la ejecución del proyecto, que serán debidamente identificados y notificados por el Jefe del área de Sistemas.

Gráfico 3. Cuadro pictórico de la Cooperativa de Ahorro y Crédito San Francisco

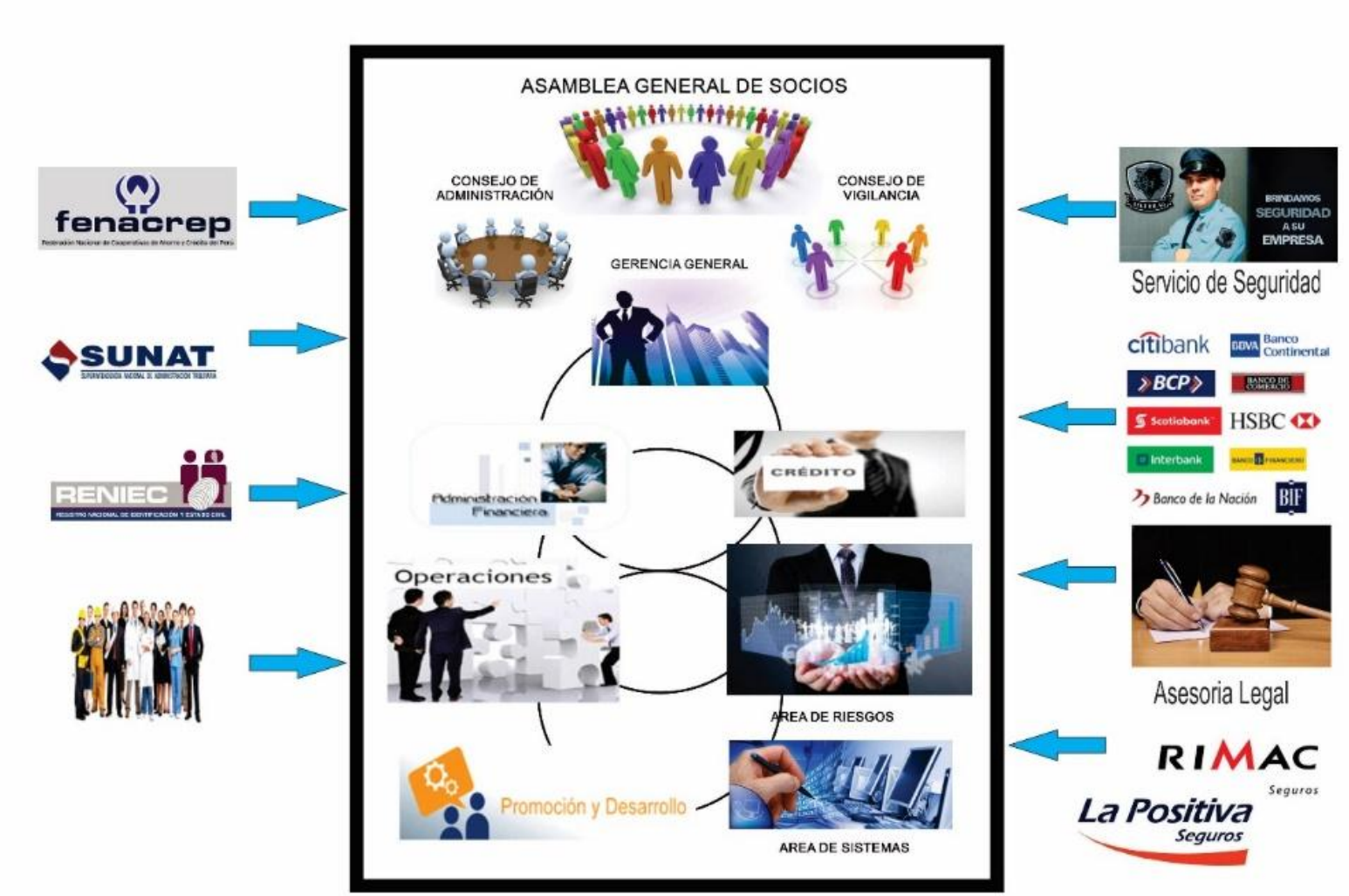
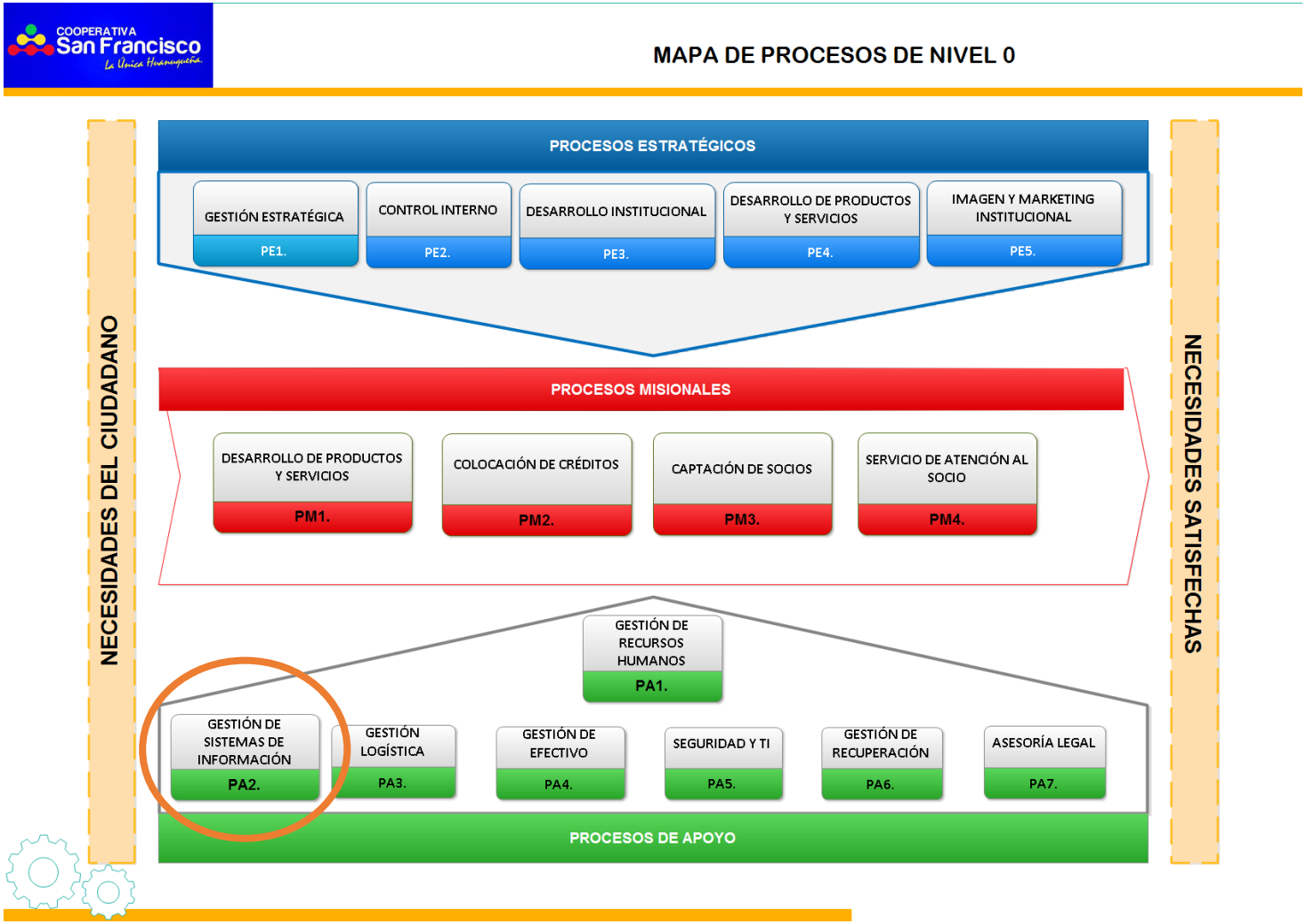
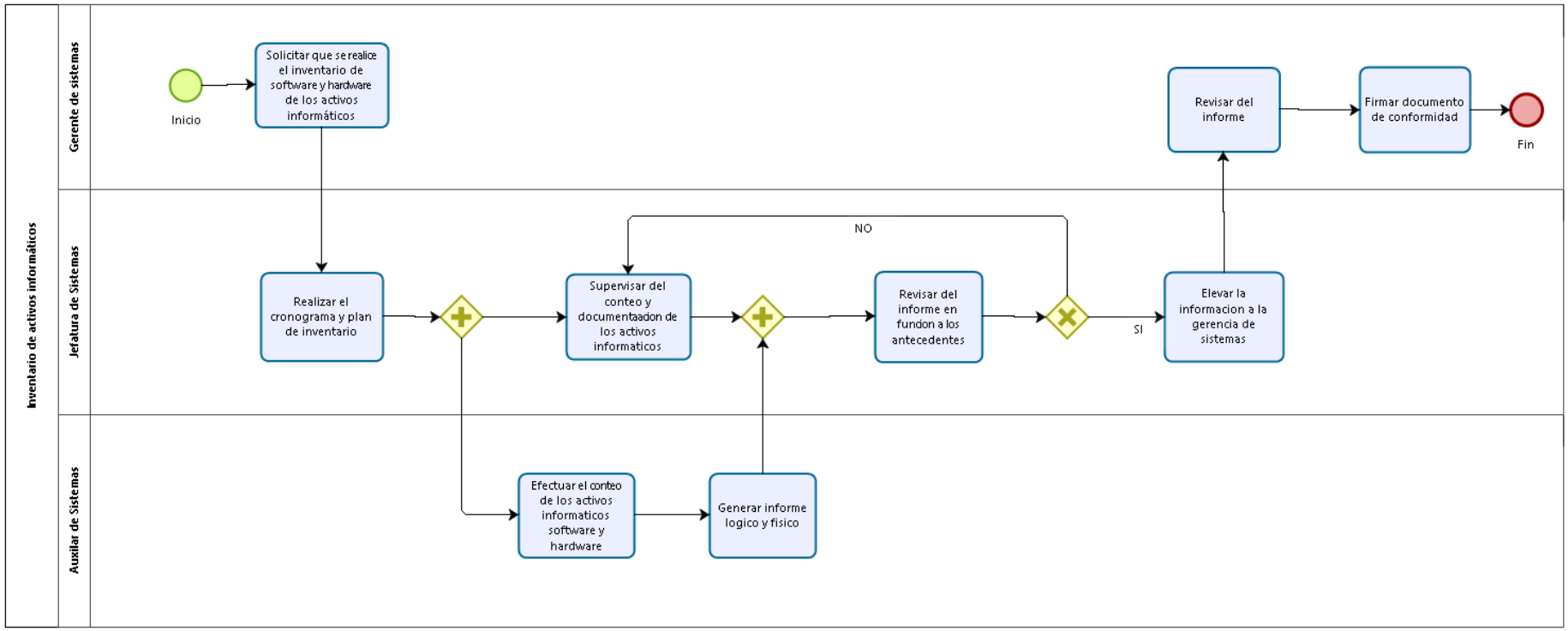


Gráfico 4. Mapa de procesos de nivel 0 de la Cooperativa de Ahorro y Crédito San Francisco



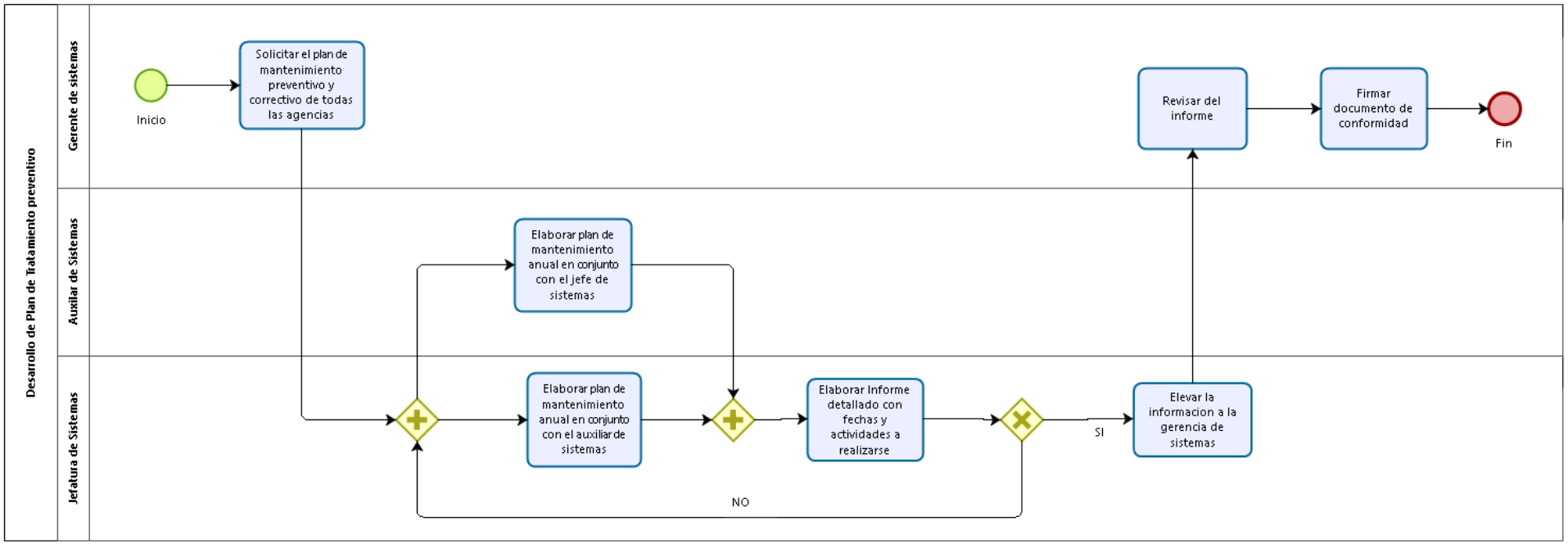
- **PA2.1. Inventario de activos informáticos**

Gráfico 5. Inventario de activos informáticos



- **PA2.2. Desarrollo de Plan de tratamiento preventivo**

Gráfico 6. Desarrollo de Plan de tratamiento preventivo



5.1. FASE I: CARACTERIZACIÓN DE ACTIVOS

a. Identificación de los activos de la organización

Entre los activos más relevantes tenemos:

- UTM FIREWALL - Gestión Unificada de Amenazas
- Cajero Multifuncional NCR
- Cajero DIEBOLD
- Servidor Base de Datos
- Servidor de Dominio/Archivos
- Servidor Switch Transaccional ATM
- Servidor de Aplicaciones 1
- Servidor de Aplicaciones 2
- Servidor Balanceador

Siendo estos algunos de los activos con un coste alto y de gran importancia para la correcta administración y función operativa del servicio y negocio de todas las agencias de la Cooperativa de Ahorro y Crédito San Francisco.

b. Identificación de dependencias entre activos

Existe dependencia alta entre los principales activos identificados previamente.

Tabla 9. Dependencias entre activos

ACTIVOS	DEPENDENCIA CON OTROS ACTIVOS
UTM FIREWALL - Gestión Unificada de Amenazas	Servidores y redes de conectividad
Cajero Multifuncional NCR	Sistema Financiero integrado SFI Base de datos Switch transaccional
Cajero DIEBOLD	Sistema Financiero integrado SFI Switch transaccional Base de datos
Servidor Base de Datos	Con todos los servidores
Servidor de Dominio/Archivos	Con todas las computadoras de usuario comunes
Servidor Switch Transaccional ATM	Cajero Multifuncional NCR Cajero DIEBOLD
Servidor de Aplicaciones 1	Servidor Balanceador Base de datos
Servidor de Aplicaciones 2	Servidor Balanceador Base de datos
Servidor Balanceador	Servidor de aplicaciones 1 Servidor de aplicaciones 2

Fuente elaboración propia

c. Valoración de activos y establecimiento de dimensiones

VALOR			CRITERIO
10		Muy alto	Daño muy grave a la ORG.
7	**9**	Alto	Daño grave a la ORG.
4	**6**	Medio	Daño importante a la ORG.
1	**3**	Bajo	Daño menor a la ORG.
0		Despreciable	Irrelevante a efectos prácticos

CATEGORÍA	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTIFICACIÓN	NO REPUDIO
ACTIVOS ESENCIALES	7	7	6	6	5
APLICACIONES INFORMÁTICAS	5	4	5	4	4
EQUIPOS INFORMÁTICOS	6	6	6	5	5
COMUNICACIONES	6	3	4	3	3
SOPORTES DE INFORMACIÓN	3	4	3	3	4
EQUIPAMIENTO AUXILIAR	7	6	4	3	3
INSTALACIONES	6	5	4	4	3
PERSONAL	6	5	5	3	3
TOTAL	6	5	5	4	4

En la Cooperativa de ahorro y crédito San Francisco LTDA. 289, se identificó que para la categoría de activos esenciales ante la existencia de alguna amenaza para la dimensión disponibilidad e integridad causaría un daño grave para la organización, para la dimensión confidencialidad, autentificación y no repudio, causarían un daño importante. Para la categoría de aplicativos informáticos y equipos informáticos, comunicación, soporte de información, equipamiento auxiliar, instalaciones y personal ante la existencia de alguna amenaza para la dimensión disponibilidad, integridad, confidencialidad, autentificación y no repudio, causarían un daño importante para la organización. Para la categoría de equipos informáticos ante la existencia de alguna amenaza para la dimensión disponibilidad, integridad, confidencialidad, autentificación y no repudio, causarían un daño importante para la organización.

Tabla 10. Identificación de activos del área de sistemas

	N°	CAPA	CÓDIGO	ACTIVO	UN	COSTO UNITARIO	COSTO TOTAL	DIMENSIONES				
								[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	AED1	DATOS (Date)	[ivp]	Inventario de IPs	-	-	-	7	5	7	6	4
	AED2		[odt]	Ordenes de trabajo	-	-	-	9	7	8	8	6
	AED3		[dgi]	Datos de gestión interna	-	-	-	8	9	9	8	7
	AED4		[mlt]	Multimedia	-	-	-	4		3	5	
	AED5	INFORMACION (Info)	[rbc]	Respaldos BACKUP	-	-	-	7	8	7	7	6
	AED6		[dal]	Dato almacenados	-	-	-	7	6	5	6	4
	AED7		[dfi]	Datos físicos	-	-	-	7	7	4	5	3
	AED8	SERVICIO [service]	[shd]	Servicio de Host-Dominio	-	-	-	7	8	7	6	6
	AED9		[sin]	Servicio de Internet	-	-	-	8	7	7	3	3
	AED10		[spt]	Servicio de mantenimiento de Pozo Tierra	-	-	-	7		6		3
	AED11		[sfo]	Servicio de Fibra Óptica	-	-	-	7	7	8	3	
APLICACIONES INFORMÁTICAS [apps]	APS1	SOFTWARE [sw]	[ocl]	ORACLE 11 GR2	-	-	-	8	9	8	7	7
	APS2		[jbe]	JBOOS Enterprise	-	-	-	7	7	8		7
	APS3		[sql]	Pl/sqls Developer	-	-	-	4	5	3	3	3
	APS4		[sfi]	Sistema financiero integrado (SFI) WEB	-	-	-	9	8	8	7	7
	APS5		[apc]	Ap_Cobradiario	-	-	-	8	7	8	7	6
	APS6		[vnc]	VNC Enterprise Edition E4.4.3	-	-	-	4	2	3		2
	APS7		[dwv]	Dvr_WebOcx Versión 5.1.7.3	-	-	-	3	2	3	1	1
	APS8		[sps]	SmartPSS 2.00.1	-	-	-	3	2	3	1	1
	APS9		[lmh]	LogMeIn Hamachi	-	-	-	3	2	3	1	1
	APS10		[wsp]	WinSCP 5.9.5	-	-	-	4	3	4		3
	APS11		[vmc]	VMware vSphere Cliente 5.5	-	-	-	5	3	5	3	3
	APS12		[put]	Putty	-	-	-	5	5	5	3	3
	APS13		[sow]	Sistema Operativo Windows	-	-	-	6	6	5	3	4
	APS14		[sol]	Sistema Operativo Linux				8	7	8	6	6
	APS15		[nwb]	Navegador Web	-	-	-	7	1	3	5	4
	APS16		[mpp]	Microsoft Office Professional Plus 2010	-	-	-	5	1	3	2	3
	APS17		[sdd]	Software de documentación (Open Office)	-	-	-	5	1	3	2	3
	APS18		[afp]	Adobe flash player	-	-	-	2	3		4	
	APS19		[vis]	Visio	-	-	-	2		3		2

	APS20		[sdb]	Sistema de Backup (Batch)	-	-	-	3	3		4		
	APS21		[adr]	Adobe Reader 11	-	-	-	2	3		4		
	APS22		[cco]	Correo corporativo	-	-	-	3	3	5	4	6	
	APS23		[jav]	Java ™ 6 Update 45	-	-	-	6		7		7	
	APS24		[aen]	Antivirus ESED NOD 32	100	S/. 35.00	S/. 3,500.00	9	7	9	8	6	
EQUIPOS INFORMÁTICOS [einf]	EIH1	HARDWARE [SW]	[utm]	UTM FIREWALL - Gestión Unificada de Amenazas	1	S/. 20,816.40	S/. 20,816.40	10	10	10	10	10	
	EIH2		[aac]	Aire Acondicionado	2	S/. 2,064.61	S/. 4,129.22	4		5		3	
	EIH3		[asg]	Alarma de seguridad	5	S/. 610.00	S/. 3,050.00	8	7	8	7	6	
	EIH4		[apu]	Access Point (Unify Ubiquity)	5	S/. 560.00	S/. 2,800.00	5	7	8	8	7	
	EIH5		[apt]	Access Point (TP-LINK)	4	S/. 248.00	S/. 992.00	5	7	8	8	7	
	EIH6		[bdr]	BLUE-RAY DISK	1	S/. 320.00	S/. 320.00	1		0		1	
	EIH7		[cdb]	Cajero DIEBOLD	1	S/. 69,720.00	S/. 69,720.00	9	10	10	10	9	
	EIH8		[cmt]	Cajero Multifuncional NCR	2	S/. 283,793.60	S/. 567,587.20	9	10	10	10	9	
	EIH9		[csf]	Cámara de Seguridad Fija	21	S/. 288.84	S/. 6,065.64	7	7	5	3	3	
	EIH10		[csm]	Cámara de Seguridad Móvil (PTZ)	15	S/. 1,250.00	S/. 18,750.00	8	8	6	3	4	
	EIH11		[csi]	Cámara de Seguridad (IP)	8	S/. 270.00	S/. 2,160.00	7	7	5	3	3	
	EIH12		[cas]	Case	20	S/. 75.00	S/. 1,500.00	2	2	2			
	EIH13		[cpu]	Computadoras (CPU)	97	S/. 1,720.00	S/. 166,840.00	7	6	6	5	4	
	EIH14		[cdb]	Contador de Billete	9	S/. 2,850.00	S/. 25,650.00	5		5		4	
	EIH15		[cdm]	Contador de Moneda	2	S/. 2,100.00	S/. 4,200.00	5		4		3	
	EIH16		[cpt]	Controller PTZ	1	S/. 328.68	S/. 328.68	4	4	4	4	3	
	EIH17		[dvr]	DVR (Grabadora de Video Digital)	6	S/. 890.00	S/. 5,340.00	7	8	7	8	8	
	EIH18		[ede]	Estabilizador de energía	108	S/. 55.00	S/. 5,940.00	4		4			
	EIH19		[etd]	Etiquetadora	1	S/. 2,822.00	S/. 2,822.00	2				1	
	EIH20		[ext]	Extintores	5	S/. 95.00	S/. 475.00	4		4	3	2	
	EIH21		[fdp]	Fuente de poder	12	S/. 50.00	S/. 600.00	4		4		3	
	EIH22		[fff]	Firewall Fortinet FAP 220B-N	1	S/. 1,643.40	S/. 1,643.40	6	6	6	6	5	
	EIH23		[ffa]	Firewall Fortinet Analyzer	1	S/. 8,300.00	S/. 8,300.00	9	10	10	9	9	

	EIH24		[gsa]	Gabinete Satra	7	S/. 780.00	S/.	5,460.00	8		8		6
	EIH25		[imr]	Impresoras en RED	15	S/. 2,373.80	S/.	35,607.00	6	3	3	4	3
	EIH26		[iml]	Impresoras Locales	15	S/. 720.00	S/.	10,800.00	6	3	3	3	3
	EIH27		[imt]	Impresoras Térmicas	12	S/. 1,050.00	S/.	12,600.00	6	4	4	4	4
	EIH28		[scn]	Scanner	3	S/. 292.00	S/.	876.00	3	2	2		
	EIH29		[jac]	Jack Modular	58	S/. 24.90	S/.	1,444.20	2		3		
	EIH30		[ros]	Rosetas	50	S/. 16.60	S/.	830.00	2		3		
	EIH31		[cri]	Kit Satra (Crimping)	2	S/. 420.00	S/.	840.00	3				2
	EIH32		[lap]	Laptops	9	S/. 2,250.00	S/.	20,250.00	7	7		7	6
	EIH33		[lin]	Lectoras internas	9	S/. 150.00	S/.	1,350.00	2		1		2
	EIH34		[lex]	Lectora Externas	2	S/. 268.00	S/.	536.00	2		1		2
	EIH35		[lem]	Luz de Emergencia	22	S/. 65.00	S/.	1,430.00	4	2			
	EIH36		[mcg]	Media converter trendnet Gigabit	4	S/. 557.76	S/.	2,231.04	10	7	9	8	7
	EIH37		[mcf]	Media converter TP-LINK Ethernet	4	S/. 341.96	S/.	1,367.84	10	7	9	8	7
	EIH38		[mer]	Memoria RAM	8	S/. 120.00	S/.	960.00	3	3			2
	EIH39		[mod]	Modem	6	S/. 2,500.00	S/.	15,000.00	9	9	8	7	8
	EIH40		[mon]	Monitores	114	S/. 485.00	S/.	55,290.00	5	4			3
	EIH41		[kvm]	Monitor Satra 16 PORT - KVM SWITCH LCD-05D	1	S/. 4,946.80	S/.	4,946.80	5	5			4
	EIH42		[mou]	Mouse	145	S/. 35.00	S/.	5,075.00	3	2	3	2	2
	EIH43		[hdm]	Multi HDMI	1	S/. 260.00	S/.	260.00	2	1	3	1	
	EIH44		[pdc]	Panel de Conexiones	9	S/. 320.00	S/.	2,880.00	6	6	7		6
	EIH45		[prt]	Parlantes	9	S/. 25.00	S/.	225.00	3	1	3	3	1
	EIH46		[pty]	Parlantes Yamaha	2	S/. 4,906.96	S/.	9,813.92	3	1	3	3	1
	EIH47		[prc]	Procesadores	7	S/. 820.00	S/.	5,740.00	3	3	4	3	2
	EIH48		[pzt]	Pozo a tierra	3		S/.	-	9	5	8	3	3
	EIH49		[pwr]	Power Rack x 8 tomas	8	S/. 90.00	S/.	720.00	5	3	5	3	3
	EIH50		[seh]	Sensor de humo	2	S/. 120.00	S/.	240.00	5	2	3	1	3

	EIH51		[sem]	Sensor de movimiento	11	S/. 90.00	S/. 990.00	5	2	3	1	3
	EIH52		[sbd]	Servidor Base de Datos	1	S/. 58,697.60	S/. 58,697.60	9	10	9	9	10
	EIH53		[sda]	Servidor de Dominio/Archivos	1	S/. 14,110.00	S/. 14,110.00	8	8	7	8	8
	EIH54		[sst]	Servidor Switch Transaccional ATM	1	S/. 18,027.60	S/. 18,027.60	8	8	8	8	8
	EIH55		[sbl]	Servidor Balanceador	1	S/. 13,877.60	S/. 13,877.60	9	8	9	8	8
	EIH56		[sa1]	Servidor de Aplicaciones 1	1	S/. 42,695.20	S/. 42,695.20	10	10	10	10	10
	EIH57		[sa2]	Servidor de Aplicaciones 2	1	S/. 15,537.60	S/. 15,537.60	10	10	10	10	10
	EIH58		[eqb]	Equipo Biométrico	5	S/. 420.00	S/. 2,100.00	5	4	2	3	2
	EIH59		[sdp]	Supresor de picos	1	S/. 18.00	S/. 18.00	4	2	2	2	2
	EIH60		[sws]	Switch SATRA	3	S/. 3,220.40	S/. 9,661.20	8	7	8	8	8
	EIH61		[swd]	Switch D-LINK	9	S/. 2,124.80	S/. 19,123.20	8	7	8	8	8
	EIH62		[swt]	Switch TP-LINK	4	S/. 1,958.80	S/. 7,835.20	8	7	8	8	8
	EIH63		[tah]	Tablets Huawey	12	S/. 580.00	S/. 6,960.00	6	5	4	4	4
	EIH64		[tal]	Tablets Lenovo	7	S/. 400.00	S/. 2,800.00	6	5	4	4	4
	EIH65		[tbo]	Taladro Kit BOSCH	1	S/. 320.00	S/. 320.00	3	3	2	2	2
	EIH66		[tec]	Teclados USB/PS2	142	S/. 30.00	S/. 4,260.00	4	3	4	3	3
	EIH67		[tv5]	Televisor Samsung de 55	3	S/. 2,850.00	S/. 8,550.00	6	4	5	2	3
	EIH68		[tv9]	Televisor Samsung de 49	6	S/. 2,180.00	S/. 13,080.00	6	4	5	2	3
	EIH69		[tv3]	Televisor Samsung de 43	1	S/. 1,850.00	S/. 1,850.00	6	4	5	2	3
	EIH70		[tra]	Transformador XFMR (ATM)	2	S/. 5,146.00	S/. 10,292.00	10	9	9	9	9
	EIH71		[ups]	UPS SMART 3000 (ATM)	2	S/. 3,984.00	S/. 7,968.00	10	9	9	9	9
	EIH72		[tdr]	Tarjeta de red	21	S/. 50.00	S/. 1,050.00	7	6	7	6	6
	EIH73		[rot]	Router	10	S/. 3,253.60	S/. 32,536.00	10	9	10	8	7
COMUNICACIONES [ccm]	CRC1	**REDES DE COMUNICACIÓN [COM]**	[lan]	Red LAN	-	-	-	6	4	4	3	3
	CRC2		[wan]	Red WAN	-	-	-	6	4	4	3	3
	CRC3		[int]	Internet	-	-	-	8	3	4	3	4
	CRC4		[pgw]	Página web	-	-	-	8		3	4	3
	CRC5		[pap]	Punto a punto	-	-	-	5	2		2	

	CRC6		[vpn]	Red privada Virtual	-	-	-	8	3	6	1	4
	CRC7		[adsl]	ADSL	-	-	-	7		5	2	3
	CRC8		[rin]	Red inalámbrica	-	-	-	5	3		3	2
	CRC9		[tmo]	Telefonía móvil	-	-	-	4	4	3	2	4
SOPORTES DE INFORMACIÓN [spi]	SIS1	SOPORTE [media]	[pdv]	Pendrive	5	-	-	2	2	2	3	
	SIS2		[cdb]	CD/DVD /BLUE-RAY	100	-	-	2	3	3	4	
	SIS3		[prm]	Proyector multimedia	2	S/. 2,200.00	S/. 4,400.00	3	4			4
	SIS4		[dex]	Discos externos	2	S/. 250.00	S/. 500.00	3	4	3	3	4
	SIS5		[tdm]	Lector de memorias	1	S/. 230.00	S/. 230.00	3	4	3	3	3
	SIS6		[hdv]	Hard Drive	10	S/. 235.00	S/. 2,350.00	3	4	3	3	4
EQUIPAMIENTO AUXILIAR [eax]	EAE1	EQUIPAMIENTO [aux]	[sai]	Sistema de Alimentación Interrumpida	5	S/. 2,700.00	S/. 13,500.00	8	6		2	3
	EAE2		[gpe]	Grupo Electrógeno	1	S/. 59,096.00	S/. 59,096.00	9	7		4	4
	EAE3		[cab]	Cableado Contingencia	-	-	-	6	6	5	4	4
	EAE4		[mvl]	Mobiliario	-	-	-	5		4		3
	EAE5		[edc]	Equipo de Climatización	-	-	-	6	7		1	3
	EAE6		[cel]	Cable Eléctrico	-	-	-	6	5	2	1	3
	EAE7		[fop]	Fibra Óptica	-	-	-	7	4		3	4
INSTALACIONES [ins]	INI1	INSTALACIONES [L]	[ofi]	Oficina	4	-	-	6	5	3	3	
	INI2		[sco]	Sala de Comunicaciones	1	-	-	6	5	5	4	3
	INI3		[adm]	Área de mantenimiento	2	-	-	6	5	5		3
PERSONAL [per]	PSP1	PERSONAL [per]	[ger]	Gerencia de Sistemas	-	-	-	7	5	5	3	3
	PSP2		[aux]	Auxiliarles de área	-	-	-	7	4	5	3	3
	PSP3		[use]	Usuarios Externos	-	-	-	6	3	3	2	3
	PSP4		[pea]	Personal Administrativo	-	-	-	5		4	3	2
	PSP5		[tin]	TI	-	-	-	7	6	8	5	5
	PSP6		[sfi]	Seguridad Física	-	-	-	7	8	4	3	
	PSP7		[pat]	Recorredor de pozos	-	-	-	5	5	4		

5.2. FASE II: EVALUACION DE AMENAZAS

a. Identificación de amenazas y vulnerabilidades

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. La metodología nos ofrece un catálogo de elementos de las amenazas más típicas para la evaluación de la afección que puede ocasionar a nuestros activos identificados. Se ha procedido con el despliegue del catálogo de amenazas más comunes que generan consecuencias entre nuestros activos de valor identificados con anterioridad.

Tabla 11. Catálogo de amenazas

DESASTRES NATURALES [I]	**DN1**	Fuego (incendios) **[N1]**	Posibilidad de que el fuego acabe con recursos del sistema
	DN2	Daños por agua (Inundaciones) **[N2]**	Posibilidad de que el agua acabe con recursos del sistema
DE ORIGEN INDUSTRIAL [N]	**OI1**	Avería de origen físico o lógico **[I1]**	Fallos en los equipos (hardware) o falla en los programas (software)
	OI2	Corte del suministro eléctrico **[I2]**	Pérdida o cese del fluido eléctrico
	OI3	Falla en los equipos de climatización **[3]**	Dejando en condiciones inadecuadas a los servidores y otros equipos de telecomunicaciones.
	OI4	Fallo en los servicios de comunicaciones **[I4]**	Daño o destrucción de los medios físicos, y caída del enlace de las redes y telecomunicaciones.
	OI5	Perdida o fallo de servicios terceros **[I5]**	Servicios o recursos de los que depende la operación de los equipos y de las redes (Movistar, Claro)
	OI6	Degradación de los soportes de almacenamiento de la información **[I6]**	Avería o falla de los mismos como consecuencia del paso del tiempo o uso inadecuado
ERRORES Y FALLOS NO INTENCIONADOS [E]	**EF1**	Errores de los usuarios **[F1]**	Error de uso de los servicios o datos
	EF2	Errores del administrador **[F2]**	Error de configuración y uso de los responsables de instalación y operación
	EF3	Errores de monitorización (log) **[F3]**	Registros de actividades fallidos, incompletos, faltantes
	EF4	Deficiencias en el área **[F4]**	Acciones del personal descoordinadas, errores por omisión

	EF5	Difusión de software dañino **[F5]**	Visita frecuente de páginas con alto contenido de virus, spyware, gusanos, troyanos, etc.
	EF6	Errores de re - encaminamiento **[F6]**	Envío de información a través de una ruta, sistema o red incorrecta
	EF7	Fugas de información **[F7]**	Transferencia o revelación accidental de información almacenada en algún soporte informático
	EF8	Destrucción de información **[F8]**	Eliminación accidental de información almacenada en algún soporte informático o medio físico
	EF9	Error en el uso de programas de uso gratuito o libre (software) **[F9]**	Defectos en el código o funcionalidad de los programas
	EF10	Errores de actualización de software **[F10]**	Defectos en los procedimientos o controles de actualización
	EF11	Errores en el mantenimiento preventivo o correctivo **[F11]**	Errores u omisiones en los procedimientos preventivos del software y hardware, perjuicio a la mantenibilidad del sistema de información
	EF12	Pérdida de equipos **[F12]**	Pérdida de equipos (hardware) y soportes de información
ATAQUES INTENCIONADOS [A]	**AI1**	Indisponibilidad del personal **[A1]**	Ausencia del puesto de trabajo
	AI2	Manipulación de la configuración **[A2]**	Configuración del software o hardware por personal no responsable del mismo
	AI3	Suplantación de la identidad del usuario **[A3]**	Intención de actuar con impunidad, usurpación de derechos y privilegios de acceso
	AI4	Abuso de privilegios de acceso **[A4]**	Abuso de derecho y nivel de privilegios ajenos a su competencia
	AI5	Uso no previsto **[A5]**	Utilización de los recursos del sistema para fines no previstos
	AI6	Difusión de software dañino **[A6]**	Propagación intencionada de virus, spyware, gusanos, troyanos, etc.
	AI7	Acceso no permitido a la información **[A7]**	Intención de acceder a los datos.
	AI8	Monitorización de tráfico de red **[A8]**	Extrae contenido de las comunicaciones: destino, volumen, frecuencia de los intercambios
	AI9	Repudio **[A9]**	Negación de acciones: de origen, de recepción o de entrega
	AI10	Interceptación de información **[A10]**	Extracción o escucha pasiva de información que no le corresponde
	AI11	Modificación malintencionada de la información [**A11]**	Dañar la información de la empresa, alteración intencional de la información
	AI12	Destrucción de información **[A12]**	Eliminación intencional de información
	AI13	Divulgación de información **[A13]**	Divulgación, geolocalización y copia ilegal de software
	AI14	Manipulación de programas **[A14]**	Alteración intencionada del funcionamiento de los programas

	AI15	Manipulación de los equipos **[A15]**	Sabotaje del hardware
	AI16	Robo **[A16]**	Sustracción de hardware
	AI17	Ataque destructivo **[A17]**	Destrucción de hardware o de soportes
	AI18	Ingeniería social **[A18]**	Abuso de la buena fe de las personas para que realicen actividades que interesan a terceros

Siendo entre ellos los más influyentes, consecuentes y con un impacto claramente dañino para los sistemas de información del área de sistemas.

- Corte del suministro eléctrico [I2]
- Fallo en los servicios de comunicaciones [I4]
- Errores de monitorización (log) [F3]
- Acceso no permitido a la información [A7]
- Avería de origen físico o lógico [I1]
- Ingeniería social [A19]
- Fuego (incendios) [N1]
- Errores del administrador [F2]
- Errores en el mantenimiento preventivo o correctivo [F11]
- Modificación malintencionada de la información [A11]
- Abuso de privilegios de acceso [A4]

b. Caracterización de la probabilidad de ocurrencia del impacto

El modelo ARSI nos ofrece la siguiente valoración con respecto a la probabilidad de ocurrencia y el porcentaje de degradación que ocasiona al activo, basado en lo propuesto por la metodología MAGERIT V3.

Tabla 12. Probabilidad de ocurrencia

PROBABILIDAD DE OCURRENCIA	
1	Muy Raro
2	Improbable
3	Posible
4	Probable
5	Prácticamente segura

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

- Degradación: cuán perjudicado resultaría el [valor del] activo.
- Probabilidad: cuán probable o improbable es que se materialice la amenaza.

Según ello se ha identificado las amenazas más comunes y recurrentes por activo de valor de la organización, asignándole la valoración correspondiente.

Tabla 13. Valores cuantitativos de la Degradación

DEGRADACIÓN		
Despreciable	**0**	**10**
Bajo	**20**	**30**
Medio	**40**	**60**
Alto	**70**	**80**
Muy Alto	**90**	**100**

CATEGORÍAS	PROBABILIDAD DE OCURRENCIA	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	ATENTIFICACIÓN	NO REPUDIO
ACTIVOS ESENCIALES	3	35%	37%	36%	34%	35%
APLICACIONES INFORMÁTICAS	3	36%	36%	37%	29%	30%
EQUIPOS INFORMÁTICOS	3	40%	38%	37%	32%	32%
COMUNICACIONES	3	44%	47%	51%	32%	39%
SOPORTES DE INFORMACIÓN	4	37%	38%	37%	28%	30%
EQUIPAMIENTO AUXILIAR	3	40%	39%	36%	29%	27%
INSTALACIONES	3	37%	47%	47%	30%	27%
PERSONAL	3	36%	43%	33%	21%	27%
	3	38%	41%	39%	29%	31%

Se puede evidenciar que la probabilidad de ocurrencia mayor se manifiesta en la categoría de soporte de información.

Tabla 14. Caracterización de los activos del área de sistemas

	N°	CÓDIGO	ACTIVO	PROBABILIDAD	DIMENSIONES				
					[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	**AED1**	**[ivp]**	**Inventario de IPs**	**3**	**40%**	**40%**	**40%**	**30%**	**20%**
		OI6	Degradación de los soportes de almacenamiento de la información [I6]	3	40%	30%			
		EF10	Destrucción de información [F10]	2	40%	40%	40%	30%	20%
		EF14	Pérdida de equipos [F14]	3	30%		30%		
	AED2	**[odt]**	**Ordenes de trabajo**	**3**	**30%**	**30%**	**40%**	**40%**	**40%**
		AI1	Indisponibilidad del personal [A1]	2				40%	40%
		AI4	Abuso de privilegios de acceso [A4]	4		30%	30%		40%
		AI5	Uso no previsto [A5]	3	30%		40%	40%	
		OI2	Corte del suministro eléctrico [I2]	3	20%			20%	30%
	AED3	**[dgi]**	**Datos de gestión interna**	**3**	**30%**	**50%**	**50%**	**40%**	**50%**
		AI14	Divulgación de información [A14]	3			50%	30%	40%
		AI13	Destrucción de información [A13]	2	30%	50%	40%		
		AI4	Abuso de privilegios de acceso [A4]	3		50%	40%		30%
		AI11	Modificación malintencionada de la información [A11]	3		40%		40%	50%
	AED4	**[mlt]**	**Multimedia**	**3**	**20%**	40%	30%	30%	20%
		OI6	Degradación de los soportes de almacenamiento de la información [I6]	4	20%	40%			
		EF2	Errores del administrador [F2]	3	20%			30%	
		AI5	Uso no previsto [A5]	3		20%	30%		20%
	AED5	**[rbc]**	**Respaldos BACKUP**	**3**	**30%**	**40%**	**30%**	**40%**	**40%**
		OI6	Degradación de los soportes de almacenamiento de la información [I6]	4	30%		30%		
		EF10	Destrucción de información [F10]	2	20%	30%			
		AI2	Manipulación de la configuración [A2]	3		40%	30%		
		AI14	Divulgación de información [A14]	3			30%	40%	40%
		AI11	Modificación malintencionada de la información [A11]	2		40%		40%	40%
	AED6	**[dal]**	**Datos almacenados**	**3**	**40%**	**40%**	**50%**	**30%**	**50%**
		OI6	Degradación de los soportes de almacenamiento de la información [I6]	4	40%	20%	20%		
		EF10	Destrucción de información [F10]	2	40%	40%		30%	30%
		AI2	Manipulación de la configuración [A2]	3		40%	50%		
		AI14	Divulgación de información [A14]	3			40%	30%	50%
		AI11	Modificación malintencionada de la información [A11]	4		40%	30%	30%	
	AED7	**[dfi]**	**Datos físicos**	**2**	**50%**	**30%**	**20%**	**40%**	**40%**
		EF10	Destrucción de información [F10]	3		30%	20%	40%	40%
		DN1	Fuego [N.1]	2	50%			20%	40%
		DN2	Daños por agua [N.2]	2	50%			20%	40%
	AED8	**[shd]**	**Servicio de Host-Dominio**	**2**	**40%**	**40%**	**40%**	**40%**	**30%**
		OI4	Fallo en los servicios de comunicaciones [I4]	2	40%		40%		30%
		EF3	Errores de monitorización (log) [F3]	2		30%		40%	30%
		EF2	Errores del administrador [F2]	2		40%		20%	20%
	AED9	**[sin]**	**Servicio de Internet**	**4**	**40%**	**30%**	**40%**	**30%**	**30%**

		OI4	Fallo en los servicios de comunicaciones [I4]	4	40%		40%		30%
		OI5	Perdida o fallo de servicios terceros [I5]	4			20%	30%	30%
		EF3	Errores de monitorización (log) [F3]	3		30%	30%	30%	
	AED10	**[spt]**	**Servicio de mantenimiento de Pozo Tierra**	**3**	**30%**	**30%**	**30%**	**20%**	**30%**
		OI5	Perdida o fallo de servicios terceros [I5]	4					30%
		EF3	Errores de monitorización (log) [F3]	3		20%	30%	20%	
		AI18	Ataque destructivo [A18]	2	30%	30%			20%
	AED11	**[sfo]**	**Servicio de Fibra Óptica**	**4**	**40%**	**40%**	**30%**	**30%**	**30%**
		OI5	Perdida o fallo de servicios terceros [I5]	5	40%	40%			30%
		EF3	Errores de monitorización (log) [F3]	3		20%	30%	30%	
		AI18	Ataque destructivo [A18]	3				20%	20%
APLICACIONES INFORMÁTICAS [apps]	**APS1**	**[ocl]**	**ORACLE 11 GR2**	**3**	**40%**	**40%**	**30%**	**30%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	3	20%				20%
		EF2	Errores del administrador [F2]	3		40%	30%	30%	
		AI4	Abuso de privilegios de acceso [A4]	4	40%	40%			
	APS2	**[jbe]**	**JBOOS Enterprise**	**4**	**30%**	**40%**	**50%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	30%	50%		
		EF2	Errores del administrador [F2]	4	20%			20%	30%
		AI4	Abuso de privilegios de acceso [A4]	4		40%	30%	30%	
	APS3	**[sql]**	**PI/sqls Developer**	**3**	**30%**	**40%**	**50%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	30%	30%	50%		
		EF2	Errores del administrador [F2]	3	20%			20%	30%
		AI15	Manipulación de programas [A15]	4		40%	30%	30%	
	APS4	**[sfi]**	**Sistema financiero integrado (SFI) WEB**	**4**	**70%**	**50%**	**50%**	**30%**	**40%**
		OI4	Fallo en los servicios de comunicaciones [I4]	4	70%		50%	30%	30%
		OI1	Avería de origen físico o lógico [I1]	4	60%	40%	30%	30%	
		OI5	Perdida o fallo de servicios terceros [I5]	4			40%		40%
		EF2	Errores del administrador [F2]	4	30%	40%		30%	30%
		EF1	Errores de los usuarios [F1]	5	40%	50%	40%	30%	40%
		EF7	Errores de re – encaminamiento [F7]	4	40%	40%	30%		40%
	APS5	**[apc]**	**Ap_Cobradiario**	**4**	**40%**	**40%**	**40%**	**60%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	40%	40%			30%
		OI4	Fallo en los servicios de comunicaciones [I4]	3		30%		20%	20%
		EF1	Errores de los usuarios [F1]	4	30%		30%		30%
		EF2	Errores del administrador [F2]	3		30%		50%	20%
		EF9	Fugas de información [F9]	4		40%	40%	60%	
		EF10	Errores de actualización de software [F10]	4	40%	40%	30%		
	APS6	**[vnc]**	**VNC Enterprise Edition E4.4.3**	**3**	**30%**	**30%**	**20%**	**30%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	3	30%		20%		20%
		OI4	Fallo en los servicios de comunicaciones [I4]	3	20%		20%	30%	
		EF2	Errores del administrador [F2]	2	30%	30%			
	APS7	**[dwv]**	**Dvr_WebOcx Versión 5.1.7.3**	**3**	**30%**	**20%**	**30%**	**20%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	30%				30%
		OI4	Fallo en los servicios de comunicaciones [I4]	4		20%	30%	20%	
		EF2	Errores del administrador [F2]	2	20%	20%			20%
	APS8	**[sps]**	**SmartPSS 2.00.1**	**3**	**30%**	**20%**	**30%**	**20%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	30%				30%

	OI4	Fallo en los servicios de comunicaciones [I4]	4		20%	30%	20%	
	EF2	Errores del administrador [F2]	2	20%	20%			20%
APS9	**[lmh]**	**LogMeIn Hamachi**	**3**	**30%**	**20%**	**30%**	**20%**	**30%**
	OI1	Avería de origen físico o lógico [I1]	3	30%				30%
	OI4	Fallo en los servicios de comunicaciones [I4]	4		20%	30%	20%	
	EF2	Errores del administrador [F2]	3	20%	20%			20%
APS10	**[wsp]**	**WinSCP 5.9.5**	**3**	**30%**	**20%**	**30%**	**20%**	**30%**
	OI1	Avería de origen físico o lógico [I1]	3	30%				30%
	OI4	Fallo en los servicios de comunicaciones [I4]	4		20%	30%	20%	
	EF2	Errores del administrador [F2]	3	20%	20%			20%
APS11	**[vmc]**	**VMware vSphere Cliente 5.5**	**3**	**30%**	**30%**	**30%**	**20%**	**40%**
	OI1	Avería de origen físico o lógico [I1]	3	30%				40%
	EF2	Errores del administrador [F2]	3	30%	30%	20%		
	EF3	Errores de monitorización (log) [F3]	3		30%	30%	20%	
APS12	**[put]**	**Putty**	**3**	**20%**	**30%**	**20%**	**30%**	**20%**
	OI1	Avería de origen físico o lógico [I1]	3			20%	30%	20%
	EF2	Errores del administrador [F2]	2	20%	30%			
APS13	**[sow]**	**Sistema Operativo Windows**	**4**	**40%**	**40%**	**40%**	**30%**	**30%**
	AI7	Acceso no permitido a la información [A7]	4	40%	40%	40%		20%
	AI4	Abuso de privilegios de acceso [A4]	3		40%		30%	
	AI5	Uso no previsto [A5]	4				20%	
	EF2	Errores del administrador [F2]	3		30%			30%
APS14	**[sol]**	**Sistema Operativo Linux**	**3**	**40%**	**50%**	**50%**	**30%**	**30%**
	AI7	Acceso no permitido a la información [A7]	4	40%	50%	50%		20%
	AI4	Abuso de privilegios de acceso [A4]	3		40%	40%	30%	
	AI5	Uso no previsto [A5]	3				20%	
	EF2	Errores del administrador [F2]	3		30%	30%		30%
APS15	**[nwb]**	**Navegador Web**	**4**	**40%**	**40%**	**50%**	**30%**	**30%**
	OI5	Perdida o fallo de servicios terceros [I5]	4	40%	40%	50%	30%	30%
	OI1	Avería de origen físico o lógico [I1]	5	40%		30%		20%
	EF2	Errores del administrador [F2]	3	30%	30%			
APS16	**[mpp]**	**Microsoft Office Professional Plus 2010**	**4**	**40%**	**40%**	**30%**	**30%**	**30%**
	EF10	Errores de actualización de software [F10]	4	40%	30%			30%
	AI2	Manipulación de la configuración [A2]	4		40%	30%	30%	
	EF1	Errores de los usuarios [F1]	5	40%		20%		
APS17	**[sdd]**	**Software de documentación (Open Office)**	**4**	**40%**	**40%**	**30%**	**30%**	**30%**
	EF10	Errores de actualización de software [F10]	4	40%	30%			30%
	AI2	Manipulación de la configuración [A2]	4		40%	30%	30%	
	EF1	Errores de los usuarios [F1]	5	40%		20%		
APS18	**[afp]**	**Adobe flash player**	**4**	**40%**	**40%**	**30%**	**30%**	**20%**
	EF10	Errores de actualización de software [F10]	4	40%		30%	30%	
	AI2	Manipulación de la configuración [A2]	3		40%	30%		20%
APS19	**[vis]**	**Visio**	**4**	**40%**	**40%**	**30%**	**30%**	**30%**
	EF10	Errores de actualización de software [F10]	4	40%	30%			30%
	AI2	Manipulación de la configuración [A2]	3		40%	30%	30%	
	EF1	Errores de los usuarios [F1]	4	40%		20%		
APS20	**[sdb]**	**Sistema de Backup (Batch)**	**3**	**30%**	**40%**	**40%**	**30%**	**30%**

		EF2	Errores del administrador [F2]	3		40%	40%		30%
		EF3	Errores de monitorización (log) [F3]	3	30%			30%	
	APS21	**[adr]**	**Adobe Reader 11**	**3**	**30%**	**40%**	**30%**	**30%**	**30%**
		AI2	Manipulación de la configuración [A2]	3	30%	30%			30%
		AI4	Abuso de privilegios de acceso [A4]	3		40%	30%	30%	
		EF1	Errores de los usuarios [F1]	3	30%				20%
	APS22	**[cco]**	**Correo corporativo**	**4**	**30%**	**40%**	**50%**	**40%**	**50%**
		EF1	Errores de los usuarios [F1]	5	30%				30%
		AI6	Difusión de software dañino [A6]	4		40%	40%	40%	50%
		AI11	Interceptación de información [A11]	4		30%	40%		40%
		AI19	Ingeniería social [A19]	4		40%	50%		
	APS23	**[jav]**	**Java ™ 6 Update 45**	**3**	**20%**	**30%**	**30%**	**20%**	**20%**
		AI2	Manipulación de la configuración [A2]	3	20%	30%			
		EF1	Errores de los usuarios [F1]	3			30%	20%	20%
	APS24	**[aen]**	**Antivirus ESED NOD 32**	**3**	**40%**	**40%**	**40%**	**30%**	**30%**
		EF2	Errores del administrador [F2]	2		40%	40%		30%
		EF3	Errores de monitorización (log) [F3]	3		30%		30%	30%
		EF6	Difusión de software dañino [F6]	3	40%	40%	40%		
		EF10	Errores de actualización de software [F10]	4		30%	30%	30%	
EQUIPOS INFORMÁTICOS [einf]	**EIH1**	**[utm]**	**UTM FIREWALL - Gestión Unificada de Amenazas**	**3**	**70%**	**70%**	**70%**	**60%**	**60%**
		DN1	Fuego (incendios) [N1]	1	50%				30%
		OI1	Avería de origen físico o lógico [I1]	2	30%	40%			
		OI2	Corte del suministro eléctrico [I2]	4			30%	30%	
		OI3	Falla en los equipos de climatización [3]	3	60%	60%	70%	60%	60%
		OI4	Fallo en los servicios de comunicaciones [I4]	4	50%	50%	60%		40%
		EF3	Errores de monitorización (log) [F3]	4	50%	50%	60%		50%
		EF2	Errores del administrador [F2]	3		30%	30%		
		AI3	Suplantación de la identidad del usuario [A3]	2		50%		30%	50%
		AI7	Acceso no permitido a la información [A7]	4	60%	70%			60%
		AI18	Ataque destructivo [A18]	3	70%	70%	70%	60%	6%
		AI19	Ingeniería social [A19]	4		70%	70%		
	EIH2	**[aac]**	**Aire Acondicionado**	**3**	**30%**	**40%**	**40%**	**40%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	3	30%		40%		30%
		OI5	Perdida o fallo de servicios terceros [I5]	3		30%			
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	3		40%	40%	40%	30%
		AI17	Robo [A17]	2		40%		30%	40%
	EIH3	**[asg]**	**Alarma de seguridad**	**3**	**20%**	**40%**	**40%**	**30%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	20%	40%	40%		
		AI17	Robo [A17]	2		30%		30%	20%
		AI18	Ataque destructivo [A18]	2		20%	30%	20%	
	EIH4	**[apu]**	**Access Point (Unify Ubiquity)**	**3**	**40%**	**40%**	**50%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	4	40%	30%	40%		
		OI4	Fallo en los servicios de comunicaciones [I4]	3		30%	40%		30%
		EF2	Errores del administrador [F2]	2		30%		20%	

		AI19	Ingeniería social [A19]	3		40%	50%	30%	
	EIH5	**[apt]**	**Access Point (TP-LINK)**	**3**	**40%**	**40%**	**50%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	4	40%	30%	40%		
		OI4	Fallo en los servicios de comunicaciones [I4]	3		30%	40%		30%
		EF2	Errores del administrador [F2]	2		30%		20%	
		AI19	Ingeniería social [A19]	3		40%	50%	30%	
	EIH6	**[bdr]**	**BLUE-RAY DISK**	**3**	**20%**	**30%**	**10%**	**20%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	20%			20%	20%
		AI17	Robo [A17]	2		30%			
		AI18	Ataque destructivo [A18]	2	20%	30%	10%		
	EIH7	**[cdb]**	**Cajero DIEBOLD**	**4**	**60%**	**60%**	**60%**	**50%**	**50%**
		AI10	Repudio [A10]	3		50%			50%
		OI1	Avería de origen físico o lógico [I1]	3	50%	50%	60%	40%	
		OI4	Fallo en los servicios de comunicaciones [I4]	4	40%	40%	40%		
		OI5	Perdida o fallo de servicios terceros [I5]	4	40%		50%		40%
		EF1	Errores de los usuarios [F1]	4	40%	40%			40%
		EF3	Errores de monitorización (log) [F3]	4		50%	50%		40%
		AI2	Manipulación de la configuración [A2]	3		50%		50%	50%
		AI3	Suplantación de la identidad del usuario [A3]	4	30%	60%	60%		
		AI18	Ataque destructivo [A18]	4	60%	50%		50%	40%
	EIH8	**[cmt]**	**Cajero Multifuncional NCR**	**4**	**60%**	**60%**	**60%**	**50%**	**50%**
		AI10	Repudio [A10]	3		50%			50%
		OI1	Avería de origen físico o lógico [I1]	3	50%	50%	60%	40%	
		OI4	Fallo en los servicios de comunicaciones [I4]	4	40%	40%	40%		
		OI5	Perdida o fallo de servicios terceros [I5]	4	40%		50%		40%
		EF1	Errores de los usuarios [F1]	4	40%	40%			40%
		EF3	Errores de monitorización (log) [F3]	4		50%	50%		40%
		AI2	Manipulación de la configuración [A2]	3		50%		50%	50%
		AI3	Suplantación de la identidad del usuario [A3]	4	30%	60%	60%		
		AI18	Ataque destructivo [A18]	4	60%	50%		50%	40%
	EIH9	**[csf]**	**Cámara de Seguridad Fija**	**3**	**40%**	**50%**	**50%**	**50%**	**50%**
		OI1	Avería de origen físico o lógico [I1]	4	40%		50%		40%
		EF12	Pérdida de equipos [F12]	2	40%	50%		50%	
		AI5	Uso no previsto [A5]	3	40%			40%	
		AI17	Ataque destructivo [A17]	4	40%	50%	50%		50%
	EIH10	**[csm]**	**Cámara de Seguridad Móvil (PTZ)**	**3**	**40%**	**50%**	**50%**	**50%**	**50%**
		OI1	Avería de origen físico o lógico [I1]	4	40%		50%		40%
		EF12	Pérdida de equipos [F12]	2	40%	50%		50%	
		AI5	Uso no previsto [A5]	3	40%			40%	
		AI17	Ataque destructivo [A17]	4	40%	50%	50%		50%
	EIH11	**[csi]**	**Cámara de Seguridad (IP)**	**3**	**40%**	**50%**	**50%**	**50%**	**50%**
		OI1	Avería de origen físico o lógico [I1]	4	40%		50%		40%
		EF12	Pérdida de equipos [F12]	2	40%	50%		50%	
		AI5	Uso no previsto [A5]	3	40%			40%	
		AI17	Ataque destructivo [A17]	4	40%	50%	50%		50%
	EIH12	**[cas]**	**Case**	**4**	**30%**	**30%**	**10%**	**20%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	5	30%	20%	10%		30%
		AI16	Robo [A16]	2		30%		20%	20%

	EIH13	**[cpu]**	**Computadoras (CPU)**	**3**	**50%**	**50%**	**50%**	**50%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	3	50%	40%			30%
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4	50%	50%	50%	30%	
		EF12	Pérdida de equipos [F12]	2		50%		50%	40%
		OI2	Corte del suministro eléctrico [I2]	4	50%				
		AI16	Robo [A16]	2		50%		50%	40%
		AI17	Ataque destructivo [A17]	2		50%	40%		40%
	EIH14	**[cdb]**	**Contador de Billete**	**4**	**50%**	**50%**	**40%**	**30%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	3	50%	40%			
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4	40%	50%	40%	20%	30%
		AI2	Manipulación de la configuración [A2]	4		40%			40%
		OI2	Corte del suministro eléctrico [I2]	4				30%	
	EIH15	**[cdm]**	**Contador de Moneda**	**4**	**50%**	**50%**	**40%**	**30%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	3	50%	40%			
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4	40%	50%	40%	20%	30%
		AI2	Manipulación de la configuración [A2]	4		40%			40%
		OI2	Corte del suministro eléctrico [I2]	4				30%	
	EIH16	**[cpt]**	**Controller PTZ**	**2**	**40%**	**40%**	**40%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	2	40%		40%		30%
		EF2	Errores del administrador [F2]	2		40%	20%	30%	
	EIH17	**[dvr]**	**DVR (Grabadora de Video Digital)**	**3**	**40%**	**40%**	**40%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	40%		40%		30%
		EF2	Errores del administrador [F2]	2		40%		30%	
	EIH18	**[ede]**	**Estabilizador de energía**	**3**	**30%**	**0%**	**0%**	**0%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	3	30%				20%
	EIH19	**[etd]**	**Etiquetadora**	**3**	**30%**	**0%**	**20%**	**0%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	3	30%		20%		20%
	EIH20	**[ext]**	**Extintores**	**3**	**30%**	**30%**	**10%**	**30%**	**20%**
		EF3	Errores de monitorización (log) [F3]	3	20%	30%		30%	20%
		OI1	Avería de origen físico o lógico [I1]	3	30%		10%		
	EIH21	**[fdp]**	**Fuente de poder**	**3**	**30%**	**0%**	**20%**	**20%**	**10%**
		OI1	Avería de origen físico o lógico [I1]	3	30%		20%	20%	10%
	EIH22	**[fff]**	**Firewall Fortinet FAP 220B-N**	**3**	**40%**	**40%**	**50%**	**30%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	4	40%	30%		30%	20%
		OI4	Fallo en los servicios de comunicaciones [I4]	3		30%	50%		
		OI5	Perdida o fallo de servicios terceros [I5]	3		40%	40%	30%	
		EF2	Errores del administrador [F2]	3		40%	40%		
		AI11	Modificación malintencionada de la información [A11]	3		20%		30%	40%
		AI13	Divulgación de información [A13]	4		40%	50%		30%
	EIH23	**[ffa]**	**Firewall Fortinet Analyzer**	**3**	**30%**	**40%**	**40%**	**40%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	4		40%	40%	30%	20%
		OI4	Fallo en los servicios de comunicaciones [I4]	3		40%	40%		
		EF2	Errores del administrador [F2]	3	30%	30%			
		AI11	Modificación malintencionada de la información [A11]	3		40%		40%	40%
	EIH24	**[gsa]**	**Gabinete Satra**	**3**	**40%**	**40%**	**30%**	**40%**	**40%**
		DN1	Fuego (incendios) [N1]	3			30%	20%	30%
		OI3	Falla en los equipos de climatización [3]	3	40%	40%			

		AI17	Ataque destructivo [A17]	3		40%		40%	40%
	EIH25	**[imr]**	**Impresoras en RED**	**4**	**40%**	**40%**	**40%**	**40%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	40%	20%	40%		20%
		OI2	Corte del suministro eléctrico [I2]	4			30%	20%	
		EF1	Errores de los usuarios [F1]	4	30%	20%			20%
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	3		40%		40%	
	EIH26	**[iml]**	**Impresoras Locales**	**4**	**40%**	**40%**	**40%**	**40%**	**20%**
		EF1	Errores de los usuarios [F1]	4	40%	20%	40%		20%
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4			30%	20%	
		OI1	Avería de origen físico o lógico [I1]	4	40%	30%			20%
		OI2	Corte del suministro eléctrico [I2]	4		40%		40%	
	EIH27	**[imt]**	**Impresoras Térmicas**	**4**	**50%**	**40%**	**40%**	**40%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	40%	20%	40%		20%
		OI2	Corte del suministro eléctrico [I2]	4			30%	20%	
		EF1	Errores de los usuarios [F1]	4	50%	40%			20%
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	3		40%		40%	
	EIH28	**[scn]**	**Scanner**	**4**	**30%**	**20%**	**10%**	**30%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	30%			30%	20%
		EF1	Errores de los usuarios [F1]	4	20%	20%	10%		
	EIH29	**[jac]**	**Jack Modular**	**4**	**30%**	**20%**	**20%**	**30%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	20%	20%	30%	20%
	EIH30	**[ros]**	**Rosetas**	**4**	**30%**	**20%**	**10%**	**20%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	20%	10%	20%	20%
	EIH31	**[cri]**	**Kit Satra (Crimping)**	**4**	**30%**	**20%**	**10%**	**20%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	20%	10%	20%	20%
	EIH32	**[lap]**	**Laptops**	**3**	**50%**	**50%**	**50%**	**50%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	4	50%	40%			30%
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	3	50%	50%	50%	30%	
		EF12	Pérdida de equipos [F12]	2		50%		50%	40%
		OI2	Corte del suministro eléctrico [I2]	4	50%				
		AI16	Robo [A16]	1		50%		50%	40%
		AI17	Ataque destructivo [A17]	2		50%	40%		40%
	EIH33	**[lin]**	**Lectoras internas**	**4**	**30%**	**20%**	**10%**	**20%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	20%	10%	20%	20%
	EIH34	**[lex]**	**Lectora Externas**	**4**	**30%**	**20%**	**10%**	**20%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	20%	10%	20%	20%
	EIH35	**[lem]**	**Luz de Emergencia**	**4**	**30%**	**20%**	**10%**	**20%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	20%	10%	20%	20%
	EIH36	**[mcg]**	**Media converter trendnet Gigabit**	**4**	**30%**	**40%**	**50%**	**40%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	40%	50%	40%	40%
		OI4	Fallo en los servicios de comunicaciones [I4]	3			50%	40%	
		OI5	Perdida o fallo de servicios terceros [I5]	5			40%		
		AI16	Robo [A16]	2		40%	40%		
	EIH37	**[mcf]**	**Media converter TP-LINK Ethernet**	**4**	**30%**	**40%**	**50%**	**40%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	40%	50%	40%	40%
		OI4	Fallo en los servicios de comunicaciones [I4]	3			50%	40%	
		OI5	Perdida o fallo de servicios terceros [I5]	5			40%		
		AI16	Robo [A16]	2		40%	40%		
	EIH38	**[mer]**	**Memoria RAM**	**3**	**20%**	**40%**	**30%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	4			30%	20%	20%
		AI16	Robo [A16]	3	20%	40%			30%
		AI17	Ataque destructivo [A17]	3		30%		30%	30%
	EIH39	**[mod]**	**Modem**	**4**	**50%**	**40%**	**50%**	**30%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	3	40%	40%	50%	20%	30%

		OI4	Fallo en los servicios de comunicaciones [I4]	4	50%	40%	50%		
		OI5	Perdida o fallo de servicios terceros [I5]	4			40%		30%
		EF2	Errores del administrador [F2]	3		40%	30%	30%	
		AI8	Monitorización de tráfico de red [A8]	4		40%	40%		
		AI11	Modificación malintencionada de la información [A11]	4		40%	40%	30%	40%
	EIH40	**[mon]**	**Monitores**	**3**	**40%**	**40%**	**30%**	**30%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	3	40%	30%	30%		30%
		EF1	Errores de los usuarios [F1]	3	40%			30%	
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4		40%		30%	30%
		AI17	Ataque destructivo [A17]	3		40%			40%
	EIH41	**[kvm]**	**Monitor Satra 16 PORT - KVM SWITCH LCD-05D**	**2**	**40%**	**40%**	**30%**	**30%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	3	40%	30%	30%		30%
		EF1	Errores de los usuarios [F1]	2	40%			30%	
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	2		40%		30%	30%
		AI17	Ataque destructivo [A17]	1		40%			40%
	EIH42	**[mou]**	**Mouse**	**4**	**40%**	**30%**	**30%**	**40%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	4	40%			40%	30%
		EF1	Errores de los usuarios [F1]	4		30%	30%		
	EIH43	**[hdm]**	**Multi HDMI**	**4**	**40%**	**20%**	**30%**	**0%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	40%		20%		20%
		EF1	Errores de los usuarios [F1]	4		20%	30%		
	EIH44	**[pdc]**	**Panel de Conexiones**	**3**	**40%**	**40%**	**40%**	**50%**	**40%**
		EF2	Errores del administrador [F2]	3		40%	40%	30%	30%
		DN1	Fuego (incendios) [N1]	3	40%			30%	30%
		AI17	Ataque destructivo [A17]	2	40%	40%		50%	40%
	EIH45	**[prt]**	**Parlantes**	**4**	**30%**	**20%**	**20%**	**10%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	20%		10%	20%
		EF1	Errores de los usuarios [F1]	4	30%	20%	20%		
	EIH46	**[pty]**	**Parlantes Yamaha**	**3**	**30%**	**20%**	**20%**	**10%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	3	30%	20%		10%	20%
		EF1	Errores de los usuarios [F1]	3	30%	20%	20%		
	EIH47	**[prc]**	**Procesadores**	**3**	**40%**	**40%**	**20%**	**20%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	4	40%	30%		20%	20%
		AI16	Robo [A16]	3		40%	20%		30%
		AI17	Ataque destructivo [A17]	2		30%			40%
	EIH48	**[pzt]**	**Pozo a tierra**	**4**	**30%**	**40%**	**40%**	**20%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	5	30%	40%	40%	20%	30%
		AI17	Ataque destructivo [A17]	3		40%	30%		
	EIH49	**[pwr]**	**Power Rack x 8 tomas**	**3**	**40%**	**40%**	**40%**	**30%**	**30%**
		DN1	Fuego (incendios) [N1]	4	40%		40%		30%
		OI2	Corte del suministro eléctrico [I2]	4	20%				20%
		AI17	Ataque destructivo [A17]	2		40%		30%	
	EIH50	**[seh]**	**Sensor de humo**	**3**	**30%**	**40%**	**30%**	**20%**	**30%**
		DN1	Fuego (incendios) [N1]	4	30%		30%	20%	20%
		AI17	Ataque destructivo [A17]	2		40%			30%
		AI16	Robo [A16]	2		30%			30%
	EIH51	**[sem]**	**Sensor de movimiento**	**2**	**30%**	**40%**	**30%**	**20%**	**30%**
		DN1	Fuego (incendios) [N1]	3	30%		30%	20%	20%
		AI17	Ataque destructivo [A17]	2		40%			30%
		AI16	Robo [A16]	2		30%			30%

	EIH52	**[sbd]**	**Servidor Base de Datos**	**3**	**70%**	**70%**	**80%**	**60%**	**60%**
		DN1	Fuego (incendios) [N1]	2	70%	70%	80%	60%	50%
		OI1	Avería de origen físico o lógico [I1]	3	60%	60%	50%		40%
		OI3	Falla en los equipos de climatización [3]	2	50%		60%		
		OI4	Fallo en los servicios de comunicaciones [I4]	4	70%	70%	70%		50%
		EF2	Errores del administrador [F2]	3		60%	60%		60%
		EF4	Deficiencias en el área [F4]	3		50%	50%	50%	
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4		50%	40%	50%	40%
		AI9	Repudio [A9]	2	40%	40%			40%
		AI11	Modificación malintencionada de la información [A11]	2		60%	60%	50%	50%
	EIH53	**[sda]**	**Servidor de Dominio/Archivos**	**3**	**70%**	**70%**	**80%**	**60%**	**60%**
		DN1	Fuego (incendios) [N1]	2	70%	70%	80%	60%	50%
		OI1	Avería de origen físico o lógico [I1]	3	60%	60%	50%		40%
		OI3	Falla en los equipos de climatización [3]	2	50%		60%		
		OI4	Fallo en los servicios de comunicaciones [I4]	4	70%	70%	70%		50%
		EF2	Errores del administrador [F2]	3		60%	60%		60%
		EF4	Deficiencias en el área [F4]	3		50%	50%	50%	
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4		50%	40%	50%	40%
		AI9	Repudio [A9]	2	40%	40%			40%
		AI11	Modificación malintencionada de la información [A11]	2		60%	60%	50%	50%
	EIH54	**[sst]**	**Servidor Switch Transaccional ATM**	**3**	**70%**	**70%**	**80%**	**60%**	**60%**
		DN1	Fuego (incendios) [N1]	2	70%	70%	80%	60%	50%
		OI1	Avería de origen físico o lógico [I1]	3	60%	60%	50%		40%
		OI3	Falla en los equipos de climatización [3]	2	50%		60%		
		OI4	Fallo en los servicios de comunicaciones [I4]	4	70%	70%	70%		50%
		EF2	Errores del administrador [F2]	3		60%	60%		60%
		EF4	Deficiencias en el área [F4]	3		50%	50%	50%	
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4		50%	40%	50%	40%
		AI9	Repudio [A9]	2	40%	40%			40%
		AI11	Modificación malintencionada de la información [A11]	2		60%	60%	50%	50%
	EIH55	**[sbl]**	**Servidor Balanceador**	**3**	**70%**	**70%**	**80%**	**60%**	**60%**
		DN1	Fuego (incendios) [N1]	2	70%	70%	80%	60%	50%
		OI1	Avería de origen físico o lógico [I1]	3	60%	60%	50%		40%
		OI3	Falla en los equipos de climatización [3]	2	50%		60%		
		OI4	Fallo en los servicios de comunicaciones [I4]	4	70%	70%	70%		50%
		EF2	Errores del administrador [F2]	3		60%	60%		60%
		EF4	Deficiencias en el área [F4]	3		50%	50%	50%	
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4		50%	40%	50%	40%
		OI2	Corte del suministro eléctrico [I2]	2	40%	40%			40%
		AI11	Modificación malintencionada de la información [A11]	2		60%	60%	50%	50%
	EIH56	**[sa1]**	**Servidor de Aplicaciones 1**	**3**	**70%**	**70%**	**80%**	**60%**	**60%**
		DN1	Fuego (incendios) [N1]	2	70%	70%	80%	60%	50%
		OI1	Avería de origen físico o lógico [I1]	3	60%	60%	50%		40%
		OI3	Falla en los equipos de climatización [3]	2	50%		60%		
		OI4	Fallo en los servicios de comunicaciones [I4]	4	70%	70%	70%		50%
		EF2	Errores del administrador [F2]	3		60%	60%		60%
		EF4	Deficiencias en el área [F4]	3		50%	50%	50%	
		EF11	Errores en el mantenimiento preventivo o	4		50%	40%	50%	40%

			correctivo [F11]						
		OI2	Corte del suministro eléctrico [I2]	2	40%	40%			40%
		AI11	Modificación malintencionada de la información [A11]	2		60%	60%	50%	50%
	EIH57	**[sa2]**	**Servidor de Aplicaciones 2**	**3**	**70%**	**70%**	**80%**	**60%**	**60%**
		DN1	Fuego (incendios) [N1]	2	70%	70%	80%	60%	50%
		OI1	Avería de origen físico o lógico [I1]	3	60%	60%	50%		40%
		OI3	Falla en los equipos de climatización [3]	2	50%		60%		
		OI4	Fallo en los servicios de comunicaciones [I4]	4	70%	70%	70%		50%
		EF2	Errores del administrador [F2]	3		60%	60%		60%
		EF4	Deficiencias en el área [F4]	3		50%	50%	50%	
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4		50%	40%	50%	40%
		OI2	Corte del suministro eléctrico [I2]	2	40%	40%			40%
		AI11	Modificación malintencionada de la información [A11]	2		60%	60%	50%	50%
	EIH58	**[eqb]**	**Equipo Biométrico**	**3**	**50%**	**50%**	**20%**	**30%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	3	50%	50%			20%
		EF1	Errores de los usuarios [F1]	4	20%	30%	20%	30%	
		AI16	Robo [A16]	1		30%			20%
	EIH59	**[sdp]**	**Supresor de picos**	**4**	**30%**	**0%**	**0%**	**20%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	30%			20%	20%
	EIH60	**[sws]**	**Switch SATRA**	**3**	**50%**	**40%**	**50%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	50%	40%	50%		30%
		EF2	Errores del administrador [F2]	2		40%	40%	30%	
		AI2	Manipulación de la configuración [A2]	3		30%		30%	30%
		AI4	Abuso de privilegios de acceso [A4]	3	30%	40%	40%		
	EIH61	**[swd]**	**Switch D-LINK**	**3**	**50%**	**40%**	**50%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	50%	40%	50%		30%
		EF2	Errores del administrador [F2]	2		40%	40%	30%	
		AI2	Manipulación de la configuración [A2]	3		30%		30%	30%
		AI4	Abuso de privilegios de acceso [A4]	3	30%	40%	40%		
	EIH62	**[swt]**	**Switch TP-LINK**	**3**	**50%**	**40%**	**50%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	50%	40%	50%		30%
		EF2	Errores del administrador [F2]	2		40%	40%	30%	
		AI2	Manipulación de la configuración [A2]	3		30%		30%	30%
		AI4	Abuso de privilegios de acceso [A4]	3	30%	40%	40%		
	EIH63	**[tah]**	**Tablets Huawey**	**4**	**30%**	**30%**	**30%**	**30%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	3	30%		30%		20%
		EF1	Errores de los usuarios [F1]	5	20%	30%		30%	
	EIH64	**[tal]**	**Tablets Lenovo**	**4**	**30%**	**30%**	**30%**	**30%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	3	30%		30%		20%
		EF1	Errores de los usuarios [F1]	5	20%	30%		30%	
	EIH65	**[tbo]**	**Taladro Kit BOSCH**	**4**	**20%**	**0%**	**0%**	**0%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	20%				20%
	EIH66	**[tec]**	**Teclados USB/PS2**	**4**	**40%**	**20%**	**20%**	**0%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	40%	20%	20%		20%
	EIH67	**[tv5]**	**Televisor Samsung de 55**	**4**	**30%**	**50%**	**30%**	**20%**	**20%**
		OI2	Corte del suministro eléctrico [I2]	4	30%	50%	30%	20%	20%
		OI1	Avería de origen físico o lógico [I1]	4	30%		20%		
	EIH68	**[tv9]**	**Televisor Samsung de 49**	**4**	**30%**	**40%**	**30%**	**20%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	40%	30%	20%	20%
		OI2	Corte del suministro eléctrico [I2]	4	30%		20%		
	EIH69	**[tv3]**	**Televisor Samsung de 43**	**4**	**30%**	**30%**	**30%**	**20%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	4	30%	30%	30%	20%	20%

		OI2	Corte del suministro eléctrico [I2]	4	30%		20%		
	EIH70	**[tra]**	**Transformador XFMR (ATM)**	**3**	**50%**	**50%**	**50%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	2	50%	50%	50%		30%
		OI2	Corte del suministro eléctrico [I2]	4	20%	10%	10%		10%
		DN1	Fuego (incendios) [N1]	2	40%		30%	30%	20%
		DN2	Daños por agua (Inundaciones) [N2]	3	30%		20%		20%
		AI5	Uso no previsto [A5]	3		30%	20%		
		AI15	Manipulación de los equipos [A15]	4		40%	30%		30%
	EIH71	**[ups]**	**UPS SMART 3000 (ATM)**	**3**	**50%**	**40%**	**50%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	2	40%		50%		30%
		OI2	Corte del suministro eléctrico [I2]	4					30%
		DN1	Fuego (incendios) [N1]	2	40%	30%	40%	30%	
		DN2	Daños por agua (Inundaciones) [N2]	3	40%	30%	30%	20%	
		AI5	Uso no previsto [A5]	3	50%	30%	40%		30%
		AI15	Manipulación de los equipos [A15]	4		40%	40%		
	EIH72	**[tdr]**	**Tarjeta de red**	**2**	**30%**	**40%**	**30%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	30%		30%	30%	20%
		OI4	Fallo en los servicios de comunicaciones [I4]	3	20%	30%	30%		
		AI16	Robo [A16]	1		40%	30%		30%
	EIH73	**[rot]**	**Router**	**3**	**50%**	**50%**	**50%**	**40%**	**40%**
		OI1	Avería de origen físico o lógico [I1]	3	40%	40%	50%		30%
		OI4	Fallo en los servicios de comunicaciones [I4]	4	50%		50%		
		OI5	Perdida o fallo de servicios terceros [I5]	4		40%	50%		
		EF2	Errores del administrador [F2]	3		50%	40%	40%	20%
		EF6	Errores de re - encaminamiento [F6]	3	30%	40%	50%		
		AI2	Manipulación de la configuración [A2]	3	30%	50%		40%	40%
		AI4	Abuso de privilegios de acceso [A4]	4		50%	50%	40%	
COMUNICACIONES [ccm]	**CRC1**	**[lan]**	**Red LAN**	**3**	**60%**	**60%**	**60%**	**50%**	**50%**
		OI1	Avería de origen físico o lógico [I1]	4	60%	60%	60%		40%
		OI4	Fallo en los servicios de comunicaciones [I4]	3	50%	40%	50%	50%	
		OI5	Perdida o fallo de servicios terceros [I5]	3	50%		60%	40%	
		EF2	Errores del administrador [F2]	4		50%	40%	30%	30%
		AI8	Monitorización de tráfico de red [A8]	3		50%	50%		
		AI17	Ataque destructivo [A17]	3		60%	60%		50%
	CRC2	**[wan]**	**Red WAN**	**3**	**50%**	**60%**	**60%**	**50%**	**50%**
		AI18	Ingeniería social [A18]	4		60%	60%		50%
		OI4	Fallo en los servicios de comunicaciones [I4]	3	50%	50%	50%		
		OI5	Perdida o fallo de servicios terceros [I5]	3	40%		50%		
		EF2	Errores del administrador [F2]	2		50%		50%	40%
		EF6	Errores de re - encaminamiento [F6]	2	40%	40%	50%	30%	
	CRC3	**[int]**	**Internet**	**4**	**50%**	**60%**	**60%**	**30%**	**50%**
		OI4	Fallo en los servicios de comunicaciones [I4]	4	50%	50%	50%		40%
		EF2	Errores del administrador [F2]	2	40%	50%		30%	40%
		AI18	Ingeniería social [A18]	4		60%	60%		40%
		EF5	Difusión de software dañino [F5]	4	50%	50%	60%		50%
	CRC4	**[pgw]**	**Pagina web**	**4**	**40%**	**40%**	**40%**	**30%**	**30%**
		OI4	Fallo en los servicios de comunicaciones [I4]	3	40%	40%	40%		
		EF2	Errores del administrador [F2]	4		40%		30%	30%
	CRC5	**[pap]**	**Punto a punto**	**4**	**50%**	**40%**	**50%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	50%	40%	50%		
		OI4	Fallo en los servicios de comunicaciones [I4]	4			40%	30%	30%
		OI5	Perdida o fallo de servicios terceros [I5]	4		40%	40%		
	CRC6	**[vpn]**	**Red Privada Virtual**	**3**	**40%**	**40%**	**50%**	**30%**	**30%**
		OI4	Fallo en los servicios de comunicaciones [I4]	3	40%		50%		

		OI5	Perdida o fallo de servicios terceros [I5]	4	40%	40%	50%		
		EF2	Errores del administrador [F2]	3		40%		30%	30%
		EF6	Errores de re - encaminamiento [F6]	3		40%	50%		
	CRC7	**[adsl]**	**ADSL**	**2**	**40%**	**30%**	**50%**	**20%**	**30%**
		OI4	Fallo en los servicios de comunicaciones [I4]	2	40%	30%	50%		
		OI5	Perdida o fallo de servicios terceros [I5]	2			40%	20%	30%
	CRC8	**[rin]**	**Red inalámbrica**	**3**	**40%**	**50%**	**50%**	**30%**	**50%**
		OI1	Avería de origen físico o lógico [I1]	3	40%	30%	40%		
		OI4	Fallo en los servicios de comunicaciones [I4]	3	30%	40%	50%		
		EF2	Errores del administrador [F2]	3		40%	50%	30%	30%
		AI18	Ingeniería social [A18]	3		50%	50%		50%
		AI13	Divulgación de información [A13]	3		50%	50%		40%
	CRC9	**[tmo]**	**Telefonía móvil**	**3**	**30%**	**40%**	**40%**	**20%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	30%	30%	40%		30%
		OI4	Fallo en los servicios de comunicaciones [I4]	3		40%	40%	20%	
SOPORTES DE INFORMACIÓN [spi]	**SIS1**	**[pdv]**	**Pendrive**	**4**	**40%**	**40%**	**40%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	4	30%			20%	20%
		EF1	Errores de los usuarios [F1]	4	20%	20%			20%
		EF8	Destrucción de información [F8]	4		30%	40%		
		EF12	Pérdida de equipos [F12]	5	40%	40%			30%
		AI7	Acceso no permitido a la información [A7]	5		40%	40%	30%	
		AI13	Divulgación de información [A13]	4		40%	40%	20%	
	SIS2	**[cdb]**	**CD/DVD /BLUE-RAY**	**4**	**40%**	**40%**	**40%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	5	30%			20%	20%
		EF8	Destrucción de información [F8]	4		30%	40%		
		EF12	Pérdida de equipos [F12]	5	40%	40%			30%
		AI7	Acceso no permitido a la información [A7]	2		40%	40%	30%	
		AI13	Divulgación de información [A13]	4		40%	40%	20%	
	SIS3	**[prm]**	**Proyector multimedia**	**3**	**40%**	**40%**	**30%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	30%			20%	20%
		EF1	Errores de los usuarios [F1]	3	20%	20%			20%
		OI3	Falla en los equipos de climatización [3]	3	40%			30%	
		AI15	Manipulación de los equipos [A15]	3		40%	30%		
		AI17	Ataque destructivo [A17]	2		30%		30%	30%
	SIS4	**[dex]**	**Discos externos**	**5**	**30%**	**40%**	**40%**	**20%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	4	30%			20%	20%
		EF8	Destrucción de información [F8]	5		30%	40%		
		AI7	Acceso no permitido a la información [A7]	5		40%			30%
		AI13	Divulgación de información [A13]	4		40%	40%	20%	
	SIS5	**[tdm]**	**Lector de memorias**	**3**	**30%**	**30%**	**30%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	30%			20%	20%
		EF1	Errores de los usuarios [F1]	3	30%	30%	30%		
		EF12	Pérdida de equipos [F12]	3	30%			30%	30%
	SIS6	**[hdv]**	**Hard Drive (hard drive internal)**	**4**	**40%**	**40%**	**40%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	4	30%			20%	20%
		EF8	Destrucción de información [F8]	4		30%	40%		
		EF12	Pérdida de equipos [F12]	3	40%	40%			30%

		AI7	Acceso no permitido a la información [A7]	3		40%	40%	30%	
		AI13	Divulgación de información [A13]	4		40%	40%	20%	
EQUIPAMIENTO AUXILIAR [eax]	**EAE1**	**[sai]**	**Sistema de Alimentación Interrumpida**	**3**	**30%**	**30%**	**40%**	**30%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	3	30%		40%		20%
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	3		30%	30%	30%	
	EAE2	**[gpe]**	**Grupo Electrógeno**	**3**	**60%**	**50%**	**50%**	**50%**	**50%**
		DN1	Fuego (incendios) [N1]	3	50%	50%			30%
		DN2	Daños por agua (Inundaciones) [N2]	3	50%	50%			30%
		OI1	Avería de origen físico o lógico [I1]	4	60%		50%	50%	50%
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	3		40%		40%	
	EAE3	**[cab]**	**Cableado Contingencia**	**3**	**30%**	**30%**	**40%**	**30%**	**20%**
		OI1	Avería de origen físico o lógico [I1]	3	30%		40%		20%
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	3		30%	30%	30%	
	EAE4	**[mvl]**	**Mobiliario**	**2**	**40%**	**40%**	**30%**	**20%**	**20%**
		DN1	Fuego (incendios) [N1]	2	40%		20%	20%	20%
		DN2	Daños por agua (Inundaciones) [N2]	2	30%		30%		
		OI1	Avería de origen físico o lógico [I1]	3	30%	40%			
	EAE5	**[edc]**	**Equipo de Climatización**	**3**	**40%**	**40%**	**30%**	**20%**	**20%**
		DN1	Fuego (incendios) [N1]	3	40%		30%	20%	20%
		DN2	Daños por agua (Inundaciones) [N2]	2	30%		20%		
		OI1	Avería de origen físico o lógico [I1]	3	30%	40%			
	EAE6	**[cel]**	**Cable Eléctrico**	**4**	**40%**	**40%**	**20%**	**20%**	**30%**
		DN1	Fuego (incendios) [N1]	3	40%		20%	20%	30%
		DN2	Daños por agua (Inundaciones) [N2]	4	30%		20%		
		OI1	Avería de origen físico o lógico [I1]	4	30%	40%			
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4	40%	40%			30%
	EAE7	**[fop]**	**Fibra Óptica**	**3**	**40%**	**40%**	**40%**	**30%**	**30%**
		OI1	Avería de origen físico o lógico [I1]	3	40%		40%		30%
		OI5	Perdida o fallo de servicios terceros [I5]	4		40%	40%		
		AI17	Ataque destructivo [A17]	3		30%		30%	30%
INSTALACIONES [ins]	**INI1**	**[ofi]**	**Oficina**	**2**	**30%**	**40%**	**40%**	**30%**	**20%**
		DN1	Fuego (incendios) [N1]	2	30%			30%	
		DN2	Daños por agua (Inundaciones) [N2]	2	30%			30%	
		AI17	Ataque destructivo [A17]	2		40%	40%		20%
	INI2	**[sco]**	**Sala de Comunicaciones**	**3**	**40%**	**50%**	**50%**	**30%**	**30%**
		DN2	Daños por agua (Inundaciones) [N2]	4	40%	40%	50%	30%	30%
		OI3	Falla en los equipos de climatización [3]	3	40%		40%		
		DN1	Fuego (incendios) [N1]	4	40%	40%	50%	20%	20%
		AI17	Ataque destructivo [A17]	2		40%	40%		30%
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4	40%	50%	30%		
	INI3	**[adm]**	**Área de mantenimiento**	**3**	**40%**	**50%**	**50%**	**30%**	**30%**
		DN2	Daños por agua (Inundaciones) [N2]	4	40%	40%	50%	30%	30%

		OI3	Falla en los equipos de climatización [3]	3	40%		40%		
		DN1	Fuego (incendios) [N1]	4	40%	40%	50%	20%	20%
		AI17	Ataque destructivo [A17]	2		30%	40%		30%
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4	40%	50%	30%		20%
PERSONAL [per]	**PSP1**	**[ger]**	**Gerencia de Sistemas**	**3**	**40%**	**50%**	**40%**	**30%**	**40%**
		EF2	Errores del administrador [F2]	3		40%	40%	30%	30%
		AI2	Manipulación de la configuración [A2]	4	40%	50%	40%		
		AI4	Abuso de privilegios de acceso [A4]	4		40%	30%		
		AI11	Modificación malintencionada de la información [A11]	3		40%	40%		
		AI13	Divulgación de información [A13]	3		50%		30%	40%
		AI15	Manipulación de los equipos [A15]	3	40%	40%	30%		
	PSP2	**[aux]**	**Auxiliares de área**	**4**	**40%**	**50%**	**40%**	**0%**	**0%**
		AI2	Manipulación de la configuración [A2]	4	40%	50%	40%		
		AI4	Abuso de privilegios de acceso [A4]	4		40%	30%		
		AI11	Modificación malintencionada de la información [A11]	3		40%	40%		
	PSP3	**[use]**	**Usuarios Externos**	**4**	**30%**	**40%**	**30%**	**30%**	**30%**
		AI4	Abuso de privilegios de acceso [A4]	4		40%	30%		30%
		AI7	Acceso no permitido a la información [A7]	4		40%		30%	
		AI13	Divulgación de información [A13]	5		30%	30%		
		AI16	Robo [A16]	4	30%	40%			
	PSP4	**[pea]**	**Personal Administrativo**	**4**	**20%**	**40%**	**20%**	**20%**	**30%**
		AI4	Abuso de privilegios de acceso [A4]	4	20%	30%		20%	30%
		AI13	Divulgación de información [A13]	3		40%	20%		
	PSP5	**[tin]**	**TI**	**3**	**40%**	**40%**	**40%**	**30%**	**30%**
		AI2	Manipulación de la configuración [A2]	4	40%	40%	30%	30%	30%
		AI4	Abuso de privilegios de acceso [A4]	4		30%	30%		
		AI12	Destrucción de información [A12]	2	40%	40%	40%		
		AI17	Ataque destructivo [A17]	2		30%			30%
	PSP6	**[sfi]**	**Seguridad Física**	**2**	**40%**	**40%**	**30%**	**20%**	**30%**
		AI7	Acceso no permitido a la información [A7]	3	40%	40%			30%
		AI10	Interceptación de información [A10]	3		30%	30%		
		AI17	Ataque destructivo [A17]	2		30%	30%	20%	30%
		AI3	Suplantación de la identidad del usuario [A3]	1		20%			
	PSP7	**[pat]**	**Recorredor de pozos**	**4**	**40%**	**40%**	**30%**	**20%**	**30%**
		AI4	Abuso de privilegios de acceso [A4]	4		30%		20%	30%
		AI15	Manipulación de los equipos [A15]	4	30%	30%	20%		
		AI17	Ataque destructivo [A17]	3		40%	30%		30%
		EF11	Errores en el mantenimiento preventivo o correctivo [F11]	4	40%	30%			

c. Análisis y evaluación del impacto potencial

Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

Tabla 15. Escala de la degradación del valor

VALOR		
10		Muy alto
7	**9**	Alto
4	**6**	Medio
1	**3**	Bajo
0		Despreciable

El impacto es el resultado del producto del valor de cada activo por el valor de degradación de cada amenaza:

$$\boldsymbol{I = Va * d}$$

Dónde:

I: Impacto **Va**: Valor de Activo

d: Degradación de Activo

Tabla 16. Escala de la degradación del Impacto

IMPACTO		
9	**10**	Desastroso
7	**8**	Mayor
4	**6**	Moderado
2	**3**	Menor
0	**1**	Insignificante

Según ello se ha determinado el impacto potencial por activo de valor de la organización, asignándole la valoración correspondiente.

Tabla 17. Valoración según el impacto potencial

		Despreciable		Bajo		Medio			Alto		Muy Alto	
		0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
Muy Alto	**10**	0	1	2	3	4	5	6	7	8	9	10
Alto	**9**	0	1	2	3	4	5	5	6	7	8	9
	8	0	1	2	2	3	4	5	6	6	7	8
	7	0	1	1	2	3	4	4	5	6	6	7
Medio	**6**	0	1	1	2	2	3	4	4	5	5	6
	5	0	1	1	2	2	3	3	4	4	5	5
	4	0	0	1	1	2	2	2	3	3	4	4
Bajo	**3**	0	0	1	1	1	2	2	2	2	3	3
	2	0	0	0	1	1	1	1	1	2	2	2
	1	0	0	0	0	0	1	1	1	1	1	1
Despreciable	**0**	0	0	0	0	0	0	0	0	0	0	0

Los activos cuyo impacto potencial se encuentran de color amarillo y ámbar son aquellos que podrían estar expuestos a una materialización de degradación significativa para la organización. Entre ellos tenemos a:

ACTIVOS CON IMPACTO MAYOR

- UTM FIREWALL - Gestión Unificada de Amenazas
- Servidor Base de Datos
- Servidor Balanceador
- Servidor de Aplicaciones 1
- Servidor de Aplicaciones 2

ACTIVOS CON IMPACTO MODERADO

- Datos de gestión interna
- Datos físicos
- ORACLE 11 GR2
- Sistema financiero integrado (SFI) WEB
- Sistema Operativo Linux

- Antivirus ESED NOD 32
- Cajero DIEBOLD
- Cajero Multifuncional NCR
- Computadoras (CPU)
- Firewall Fortinet Analyzer
- Laptops
- Media converter trendnet Gigabit
- Media converter TP-LINK Ethernet
- Modem
- Servidor de Dominio/Archivos
- Servidor Switch Transaccional ATM
- Router

	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTIFICACIÓN	NO REPUDIO
ACTIVOS ESENCIALES	3	2	3	2	2
APLICACIONES INFORMÁTICAS	2	1	2	1	1
EQUIPOS INFORMÁTICOS	3	2	2	2	2
COMUNICACIONES	3	2	2	1	1
SOPORTES DE INFORMACIÓN	1	2	1	1	1
EQUIPAMIENTO AUXILIAR	2	2	1	1	1
INSTALACIONES	2	2	1	1	1
PERSONAL	2	2	2	1	1
	2	2	2	1	1

Tabla 18 Impacto de los activos del área de sistemas de la "COOPAC San Francisco"

	N°	CAPA	CÓDIGO	ACTIVO	PROBABILIDAD	DIMENSIONES				
						[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	AED1	DATOS (Date)	[ivp]	Inventario de Ips	3	3	2	3	2	1
	AED2		[odt]	Ordenes de trabajo	3	3	2	3	3	2
	AED3		[dgi]	Datos de gestión interna	3	2	5	5	3	4
	AED4		[mlt]	Multimedia	3	1	0	1	2	0
	AED5	INFORMACION (Info)	[rbc]	Respaldos BACKUP	3	2	3	2	3	2
	AED6		[dal]	Datos almacenados	3	3	2	3	2	2
	AED7		[dfi]	Datos físicos	2	4	2	1	2	1
	AED8		[shd]	Servicio de Host-Dominio	2	3	3	3	2	2
	AED9	SERVICIO [service]	[sin]	Servicio de Internet	4	3	2	3	1	1
	AED10		[spt]	Servicio de mantenimiento de Pozo Tierra	3	2	0	2	0	1
	AED11		[sfo]	Servicio de Fibra Óptica	4	3	3	2	1	0
APLICACIONES INFORMÁTICAS [apps]	APS1	SOFTWARE [sw]	[ocl]	ORACLE 11 GR2	3	3	4	2	2	1
	APS2		[jbe]	JBOOS Enterprise	4	2	3	4	0	2
	APS3		[sql]	PI/sqls Developer	3	1	2	2	1	1
	APS4		[sfi]	Sistema financiero integrado (SFI) WEB	4	6	4	4	2	3
	APS5		[apc]	Ap_Cobradiario	4	3	3	3	4	2
	APS6		[vnc]	VNC Enterprise Edition E4.4.3	3	1	1	1	0	0
	APS7		[dwv]	Dvr_WebOcx Versión 5.1.7.3	3	1	0	1	0	0
	APS8		[sps]	SmartPSS 2.00.1	3	1	0	1	0	0
	APS9		[lmh]	LogMeIn Hamachi	3	1	0	1	0	0
	APS10		[wsp]	WinSCP 5.9.5	3	1	1	1	0	1
	APS11		[vmc]	VMware vSphere Cliente 5.5	3	2	1	2	1	1
	APS12		[put]	Putty	3	1	2	1	1	1
	APS13		[sow]	Sistema Operativo Windows	4	2	2	2	1	1
	APS14		[sol]	Sistema Operativo Linux	3	3	4	4	2	2
	APS15		[nwb]	Navegador Web	4	3	0	2	2	1
	APS16		[mpp]	Microsoft Office Professional Plus 2010	4	2	0	1	1	1
	APS17		[sdd]	Software de documentación (Open Office)	4	2	0	1	1	1
	APS18		[afp]	Adobe flash player	4	1	1	0	1	0
	APS19		[vis]	Visio	4	1	0	1	0	1
	APS20		[sdb]	Sistema de Backup (Batch)	3	1	1	0	1	0
	APS21		[adr]	Adobe Reader 11	3	1	1	0	1	0
	APS22		[cco]	Correo corporativo	4	1	1	3	2	3
	APS23		[jav]	Java ™ 6 Update 45	3	1	0	2	0	1
	APS24		[aen]	Antivirus ESED NOD 32	3	4	3	4	2	2
EQUIPOS INFORMÁTICOS [einf]	EIH1	HARDWARE [SW]	[utm]	UTM FIREWALL - Gestión Unificada de Amenazas	3	7	7	7	6	6
	EIH2		[aac]	Aire Acondicionado	3	1	0	2	0	1
	EIH3		[asg]	Alarma de seguridad	3	2	3	3	2	1
	EIH4		[apu]	Access Point (Unify Ubiquity)	3	2	3	4	2	2
	EIH5		[apt]	Access Point (TP-LINK)	3	2	3	4	2	2

	EIH6		[bdr]	BLUE-RAY DISK	3	0	0	0	0	0
	EIH7		[cdb]	Cajero DIEBOLD	4	5	6	6	5	5
	EIH8		[cmt]	Cajero Multifuncional NCR	4	5	6	6	5	5
	EIH9		[csf]	Cámara de Seguridad Fija	3	3	4	3	2	2
	EIH10		[csm]	Cámara de Seguridad Móvil (PTZ)	3	3	4	3	2	2
	EIH11		[csi]	Cámara de Seguridad (IP)	3	3	4	3	2	2
	EIH12		[cas]	Case	4	1	1	0	0	0
	EIH13		[cpu]	Computadoras (CPU)	3	4	3	3	3	2
	EIH14		[cdb]	Contador de Billete	4	3	0	2	0	2
	EIH15		[cdm]	Contador de Moneda	4	3	0	2	0	1
	EIH16		[cpt]	Controller PTZ	2	2	2	2	1	1
	EIH17		[dvr]	DVR (Grabadora de Video Digital)	3	3	3	3	2	2
	EIH18		[ede]	Estabilizador de energía	3	1	0	0	0	0
	EIH19		[etd]	Etiquetadora	3	1	0	0	0	0
	EIH20		[ext]	Extintores	3	1	0	0	1	0
	EIH21		[fdp]	Fuente de poder	3	1	0	1	0	0
	EIH22		[fff]	Firewall Fortinet FAP 220B-N	3	2	2	3	2	2
	EIH23		[ffa]	Firewall Fortinet Analyzer	3	3	4	4	4	4
	EIH24		[gsa]	Gabinete Satra	3	3	0	2	0	2
	EIH25		[imr]	Impresoras en RED	4	2	1	1	2	1
	EIH26		[iml]	Impresoras Locales	4	2	1	1	1	1
	EIH27		[imt]	Impresoras Térmicas	4	3	2	2	2	1
	EIH28		[scn]	Scanner	4	1	0	0	0	0
	EIH29		[jac]	Jack Modular	4	1	0	1	0	0
	EIH30		[ros]	Rosetas	4	1	0	0	0	0
	EIH31		[cri]	Kit Satra (Crimping)	4	1	0	0	0	0
	EIH32		[lap]	Laptops	3	4	4	0	4	2
	EIH33		[lin]	Lectoras internas	4	1	0	0	0	0
	EIH34		[lex]	Lectora Externas	4	1	0	0	0	0
	EIH35		[lem]	Luz de Emergencia	4	1	0	0	0	0
	EIH36		[mcg]	Media converter trendnet Gigabit	4	3	3	5	3	3
	EIH37		[mcf]	Media converter TP-LINK Ethernet	4	3	3	5	3	3
	EIH38		[mer]	Memoria RAM	3	1	1	0	0	1
	EIH39		[mod]	Modem	4	5	4	4	2	3
	EIH40		[mon]	Monitores	3	2	2	0	0	1
	EIH41		[kvm]	Monitor Satra 16 PORT - KVM SWITCH LCD-05D	2	2	2	0	0	2
	EIH42		[mou]	Mouse	4	1	1	1	1	1
	EIH43		[hdm]	Multi HDMI	4	1	0	1	0	0
	EIH44		[pdc]	Panel de Conexiones	3	2	2	3	0	2
	EIH45		[prt]	Parlantes	4	1	0	1	0	0
	EIH46		[pty]	Parlantes Yamaha	3	1	0	1	0	0
	EIH47		[prc]	Procesadores	3	1	1	1	1	1
	EIH48		[pzt]	Pozo a tierra	4	3	2	3	1	1
	EIH49		[pwr]	Power Rack x 8 tomas	3	2	1	2	1	1
	EIH50		[seh]	Sensor de humo	3	2	1	1	0	1

	EIH51		[sem]	Sensor de movimiento	2	2	1	1	0	1
	EIH52		[sbd]	Servidor Base de Datos	3	6	7	7	5	6
	EIH53		[sda]	Servidor de Dominio/Archivos	3	6	6	6	5	5
	EIH54		[sst]	Servidor Switch Transaccional ATM	3	6	6	6	5	5
	EIH55		[sbl]	Servidor Balanceador	3	6	6	7	5	5
	EIH56		[sa1]	Servidor de Aplicaciones 1	3	7	7	8	6	6
	EIH57		[sa2]	Servidor de Aplicaciones 2	3	7	7	8	6	6
	EIH58		[eqb]	Equipo Biométrico	3	3	2	0	1	0
	EIH59		[sdp]	Supresor de picos	4	1	0	0	0	0
	EIH60		[sws]	Switch SATRA	3	4	3	4	2	2
	EIH61		[swd]	Switch D-LINK	3	4	3	4	2	2
	EIH62		[swt]	Switch TP-LINK	3	4	3	4	2	2
	EIH63		[tah]	Tablets Huawey	4	2	2	1	1	1
	EIH64		[tal]	Tablets Lenovo	4	2	2	1	1	1
	EIH65		[tbo]	Taladro Kit BOSCH	4	1	0	0	0	0
	EIH66		[tec]	Teclados USB/PS2	4	2	1	1	0	1
	EIH67		[tv5]	Televisor Samsung de 55	4	2	2	2	0	1
	EIH68		[tv9]	Televisor Samsung de 49	4	2	2	2	0	1
	EIH69		[tv3]	Televisor Samsung de 43	4	2	1	2	0	1
	EIH70		[tra]	Transformador XFMR (ATM)	3	5	5	5	3	3
	EIH71		[ups]	UPS SMART 3000 (ATM)	3	5	4	5	3	3
	EIH72		[tdr]	Tarjeta de red	2	2	2	2	2	2
	EIH73		[rot]	Router	3	5	5	5	3	3
COMUNICACIONES [ccm]	CRC1	REDES DE COMUNICACIÓN [COM]	[lan]	Red LAN	3	4	2	2	2	2
	CRC2		[wan]	Red WAN	3	3	2	2	2	2
	CRC3		[int]	Internet	4	4	2	2	1	2
	CRC4		[pgw]	Página web	4	3	0	1	1	1
	CRC5		[pap]	Punto a punto	4	3	1	0	1	0
	CRC6		[vpn]	Red privada Virtual	3	3	1	3	0	1
	CRC7		[adsl]	ADSL	2	3	0	3	0	1
	CRC8		[rin]	Red inalámbrica	3	2	2	0	1	1
	CRC9		[tmo]	Telefonía móvil	3	1	2	1	0	1
SOPORTES DE INFORMACIÓN [spi]	SIS1	SOPORTE [media]	[pdv]	Pendrive	4	1	1	1	1	0
	SIS2		[cdb]	CD/DVD /BLUE-RAY	4	1	1	1	1	0
	SIS3		[prm]	Proyector multimedia	3	1	2	0	0	1
	SIS4		[dex]	Discos externos	5	1	2	1	1	1
	SIS5		[tdm]	Lector de memorias	3	1	1	1	1	1
	SIS6		[hdv]	Hard Drive	4	1	2	1	1	1
EQUIPAMIENTO AUXILIAR [eax]	EAE1	EQUIPAMIENTO [aux]	[sai]	Sistema de Alimentación Interrumpida	3	2	2	0	1	1
	EAE2		[gpe]	Grupo Electrógeno	3	5	4	0	2	2
	EAE3		[cab]	Cableado Contingencia	3	2	2	2	1	1
	EAE4		[mvl]	Mobiliario	2	2	0	1	0	1
	EAE5		[edc]	Equipo de Climatización	3	2	3	0	0	1
	EAE6		[cel]	Cable Eléctrico	4	2	2	0	0	1

	EAE7		[fop]	Fibra Óptica	3	3	2	0	1	1
INSTALACIONES [ins]	INI1	INSTALACIONES [L]	[ofi]	Oficina	2	2	2	1	1	0
	INI2		[sco]	Sala de Comunicaciones	3	2	3	3	1	1
	INI3		[adm]	Área de mantenimiento	3	2	3	3	0	1
PERSONAL [per]	PSP1	PERSONAL [per]	[ger]	Gerencia de Sistemas	3	3	3	2	1	1
	PSP2		[aux]	Auxiliares de área	4	3	2	2	0	0
	PSP3		[use]	Usuarios Externos	4	2	1	1	1	1
	PSP4		[pea]	Personal Administrativo	4	1	0	1	1	1
	PSP5		[tin]	TI	3	3	2	3	2	2
	PSP6		[sfi]	Seguridad Física	2	3	3	1	1	0
	PSP7		[pat]	Recorredor de pozos	4	2	2	1	0	0

d. Análisis y evaluación del riesgo potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

Tabla 19. Probabilidad de ocurrencia del mapa de riesgo

PROBABILIDAD DE OCURRENCIA	
1	*Muy Raro*
2	*Improbable*
3	*Posible*
4	*Probable*
5	*Prácticamente segura*

El riesgo crece con el impacto y con la probabilidad.

$$\boldsymbol{R = I * Prob}$$

Dónde: **R:** Riesgo **I:** Impacto **Prob:** Probabilidad

Tabla 20. Riesgo

RIESGO		
0	***1***	*Controlable*
2	***5***	*Aceptable*
6	***16***	*Tolerable*
17	***30***	*Intolerable*
31	***50***	*Extremo*

Tabla 21. Valoración del riesgo potencial

Muy Alto	**10**	10	20	30	40	50
Alto	**9**	9	18	27	36	45
	8	8	16	24	32	40
	7	7	14	21	28	35
Medio	**6**	6	12	18	24	30
	5	5	10	15	20	25
	4	4	8	12	16	20
Bajo	**3**	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
Despreciable	**0**	0	0	0	0	0
		1	**2**	**3**	**4**	**5**
		Muy raro	**Improbable**	**Posible**	**Probable**	**Prácticamente segura**

Los activos cuyo riesgo se encuentran de color amarillo (15, 16) y ámbar son aquellos que podrían estar expuestos al daño probable con mayor ocurrencia. Entre ellos tenemos a:

ACTIVOS CON RIESGO INTOLERABLE

- Sistema Financiero Integrado (SFI)
- UTM FIREWALL - Gestión Unificada de Amenazas
- Cajero DIEBOLD
- Cajero Multifuncional NCR
- Modem
- Servidor de Dominio/Archivos
- Servidor Switch Transaccional ATM
- Media converter trendnet Gigabit
- Media converter TP-LINK Ethernet
- Servidor Base de Datos
- Servidor Balanceador

- Servidor de Aplicaciones 1
- Servidor de Aplicaciones 2

ACTIVOS CON RIESGO TOLERABLE

- Datos de gestión interna
- Ap_Cobradiario
- Antivirus ESED NOD 32
- Internet
- Transformador XFMR (ATM)
- UPS SMART 3000 (ATM)
- Router
- Grupo Electrógeno
- Sistema Operativo Linux

	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTIFICACIÓN	NO REPUDIO
ACTIVOS ESENCIALES	7	6	8	6	5
APLICACIONES INFORMÁTICAS	7	5	6	4	4
EQUIPOS INFORMÁTICOS	9	7	8	5	6
COMUNICACIONES	11	5	6	4	5
SOPORTES DE INFORMACIÓN	4	6	3	3	2
EQUIPAMIENTO AUXILIAR	7	7	2	2	4
INSTALACIONES	6	6	4	3	2
PERSONAL	8	6	6	3	3
	7	6	5	4	4

Tabla 22. Mapa de riesgo de la "COOPAC San Francisco"

	N°	CAPA	CÓDIGO	ACTIVO	PROBABILIDAD	DIMENSIONES				
						[D]	[I]	[C]	[A]	[N_R]
ACTIVOS ESENCIALES [essential]	AED1	DATOS (Date)	[ivp]	Inventario de Ips	3	9	6	9	6	3
	AED2		[odt]	Ordenes de trabajo	3	9	6	9	9	6
	AED3		[dgi]	Datos de gestión interna	3	6	15	15	9	12
	AED4		[mlt]	Multimedia	3	3	0	3	6	0
	AED5	INFORMACION (Info)	[rbc]	Respaldos BACKUP	3	6	9	6	9	6
	AED6		[dal]	Datos almacenados	3	9	6	9	6	6
	AED7		[dfi]	Datos físicos	2	8	4	2	4	2
	AED8		[shd]	Servicio de Host-Dominio	2	6	6	6	4	4
	AED9	SERVICIO [service]	[sin]	Servicio de Internet	4	12	8	12	4	4
	AED10		[spt]	Servicio de mantenimiento de Pozo Tierra	3	6	0	6	0	3
	AED11		[sfo]	Servicio de Fibra Óptica	4	12	12	8	4	0
APLICACIONES INFORMÁTICAS [apps]	APS1	SOFTWARE [sw]	[ocl]	ORACLE 11 GR2	3	9	12	6	6	3
	APS2		[jbe]	JBOOS Enterprise	4	8	12	16	0	8
	APS3		[sql]	Pl/sqls Developer	3	3	6	6	3	3
	APS4		[sfi]	Sistema financiero integrado (SFI) WEB	4	24	16	16	8	12
	APS5		[apc]	Ap_Cobradiario	4	12	12	12	16	8
	APS6		[vnc]	VNC Enterprise Edition E4.4.3	3	3	3	3	0	0
	APS7		[dwv]	Dvr_WebOcx Versión 5.1.7.3	3	3	0	3	0	0
	APS8		[sps]	SmartPSS 2.00.1	3	3	0	3	0	0
	APS9		[lmh]	LogMeIn Hamachi	3	3	0	3	0	0
	APS10		[wsp]	WinSCP 5.9.5	3	3	3	3	0	3
	APS11		[vmc]	VMware vSphere Cliente 5.5	3	6	3	6	3	3
	APS12		[put]	Putty	3	3	6	3	3	3
	APS13		[sow]	Sistema Operativo Windows	4	8	8	8	4	4
	APS14		[sol]	Sistema Operativo Linux	3	9	12	12	6	6
	APS15		[nwb]	Navegador Web	4	12	0	8	8	4
	APS16		[mpp]	Microsoft Office Professional Plus 2010	4	8	0	4	4	4
	APS17		[sdd]	Software de documentación (Open Office)	4	8	0	4	4	4
	APS18		[afp]	Adobe flash player	4	4	4	0	4	0
	APS19		[vis]	Visio	4	4	0	4	0	4
	APS20		[sdb]	Sistema de Backup (Batch)	3	3	3	0	3	0
	APS21		[adr]	Adobe Reader 11	3	3	3	0	3	0
	APS22		[cco]	Correo corporativo	4	4	4	12	8	12
	APS23		[jav]	Java ™ 6 Update 45	3	3	0	6	0	3
	APS24		[aen]	Antivirus ESED NOD 32	3	12	9	12	6	6
EQUIPOS INFORMÁTICOS [einf]	EIH1	HARDWARE [SW]	[utm]	UTM FIREWALL - Gestión Unificada de Amenazas	3	21	21	21	18	18
	EIH2		[aac]	Aire Acondicionado	3	3	0	6	0	3
	EIH3		[asg]	Alarma de seguridad	3	6	9	9	6	3
	EIH4		[apu]	Access Point (Unify Ubiquity)	3	6	9	12	6	6
	EIH5		[apt]	Access Point (TP-LINK)	3	6	9	12	6	6

	EIH6		[bdr]	BLUE-RAY DISK	3	0	0	0	0	0
	EIH7		[cdb]	Cajero DIEBOLD	4	20	24	24	20	20
	EIH8		[cmt]	Cajero Multifuncional NCR	4	20	24	24	20	20
	EIH9		[csf]	Cámara de Seguridad Fija	3	9	12	9	6	6
	EIH10		[csm]	Cámara de Seguridad Móvil (PTZ)	3	9	12	9	6	6
	EIH11		[csi]	Cámara de Seguridad (IP)	3	9	12	9	6	6
	EIH12		[cas]	Case	4	4	4	0	0	0
	EIH13		[cpu]	Computadoras (CPU)	3	12	9	9	9	6
	EIH14		[cdb]	Contador de Billete	4	12	0	8	0	8
	EIH15		[cdm]	Contador de Moneda	4	12	0	8	0	4
	EIH16		[cpt]	Controller PTZ	2	4	4	4	2	2
	EIH17		[dvr]	DVR (Grabadora de Video Digital)	3	9	9	9	6	6
	EIH18		[ede]	Estabilizador de energía	3	3	0	0	0	0
	EIH19		[etd]	Etiquetadora	3	3	0	0	0	0
	EIH20		[ext]	Extintores	3	3	0	0	3	0
	EIH21		[fdp]	Fuente de poder	3	3	0	3	0	0
	EIH22		[fff]	Firewall Fortinet FAP 220B-N	3	6	6	9	6	6
	EIH23		[ffa]	Firewall Fortinet Analyzer	3	9	12	12	12	12
	EIH24		[gsa]	Gabinete Satra	3	9	0	6	0	6
	EIH25		[imr]	Impresoras en RED	4	8	4	4	8	4
	EIH26		[iml]	Impresoras Locales	4	8	4	4	4	4
	EIH27		[imt]	Impresoras Térmicas	4	12	8	8	8	4
	EIH28		[scn]	Scanner	4	4	0	0	0	0
	EIH29		[jac]	Jack Modular	4	4	0	4	0	0
	EIH30		[ros]	Rosetas	4	4	0	0	0	0
	EIH31		[cri]	Kit Satra (Crimping)	4	4	0	0	0	0
	EIH32		[lap]	Laptops	3	12	12	0	12	6
	EIH33		[lin]	Lectoras internas	4	4	0	0	0	0
	EIH34		[lex]	Lectora Externas	4	4	0	0	0	0
	EIH35		[lem]	Luz de Emergencia	4	4	0	0	0	0
	EIH36		[mcg]	Media converter trendnet Gigabit	4	12	12	20	12	12
	EIH37		[mcf]	Media converter TP-LINK Ethernet	4	12	12	20	12	12
	EIH38		[mer]	Memoria RAM	3	3	3	0	0	3
	EIH39		[mod]	Modem	4	20	16	16	8	12
	EIH40		[mon]	Monitores	3	6	6	0	0	3
	EIH41		[kvm]	Monitor Satra 16 PORT - KVM SWITCH LCD-05D	2	4	4	0	0	4
	EIH42		[mou]	Mouse	4	4	4	4	4	4
	EIH43		[hdm]	Multi HDMI	4	4	0	4	0	0
	EIH44		[pdc]	Panel de Conexiones	3	6	6	9	0	6
	EIH45		[prt]	Parlantes	4	4	0	4	0	0
	EIH46		[pty]	Parlantes Yamaha	3	3	0	3	0	0
	EIH47		[prc]	Procesadores	3	3	3	3	3	3
	EIH48		[pzt]	Pozo a tierra	4	12	8	12	4	4
	EIH49		[pwr]	Power Rack x 8 tomas	3	6	3	6	3	3
	EIH50		[seh]	Sensor de humo	3	6	3	3	0	3

	EIH51		[sem]	Sensor de movimiento	2	4	2	2	0	2
	EIH52		[sbd]	Servidor Base de Datos	3	18	21	21	15	18
	EIH53		[sda]	Servidor de Dominio/Archivos	3	18	18	18	15	15
	EIH54		[sst]	Servidor Switch Transaccional ATM	3	18	18	18	15	15
	EIH55		[sbl]	Servidor Balanceador	3	18	18	21	15	15
	EIH56		[sa1]	Servidor de Aplicaciones 1	3	21	21	24	18	18
	EIH57		[sa2]	Servidor de Aplicaciones 2	3	21	21	24	18	18
	EIH58		[eqb]	Equipo Biométrico	3	9	6	0	3	0
	EIH59		[sdp]	Supresor de picos	4	4	0	0	0	0
	EIH60		[sws]	Switch SATRA	3	12	9	12	6	6
	EIH61		[swd]	Switch D-LINK	3	12	9	12	6	6
	EIH62		[swt]	Switch TP-LINK	3	12	9	12	6	6
	EIH63		[tah]	Tablets Huawey	4	8	8	4	4	4
	EIH64		[tal]	Tablets Lenovo	4	8	8	4	4	4
	EIH65		[tbo]	Taladro Kit BOSCH	4	4	0	0	0	0
	EIH66		[tec]	Teclados USB/PS2	4	8	4	4	0	4
	EIH67		[tv5]	Televisor Samsung de 55	4	8	8	8	0	4
	EIH68		[tv9]	Televisor Samsung de 49	4	8	8	8	0	4
	EIH69		[tv3]	Televisor Samsung de 43	4	8	4	8	0	4
	EIH70		[tra]	Transformador XFMR (ATM)	3	15	15	15	9	9
	EIH71		[ups]	UPS SMART 3000 (ATM)	3	15	12	15	9	9
	EIH72		[tdr]	Tarjeta de red	2	4	4	4	4	4
	EIH73		[rot]	Router	3	15	15	15	9	9
COMUNICACIONES [ccm]	CRC1	REDES DE COMUNICACIÓN [COM]	[lan]	Red LAN	3	12	6	6	6	6
	CRC2		[wan]	Red WAN	3	9	6	6	6	6
	CRC3		[int]	Internet	4	16	8	8	4	8
	CRC4		[pgw]	Página web	4	12	0	4	4	4
	CRC5		[pap]	Punto a punto	4	12	4	0	4	0
	CRC6		[vpn]	Red privada Virtual	3	9	3	9	0	3
	CRC7		[adsl]	ADSL	2	6	0	6	0	2
	CRC8		[rin]	Red inalámbrica	3	6	6	0	3	3
	CRC9		[tmo]	Telefonía móvil	3	3	6	3	0	3
SOPORTES DE INFORMACIÓN [spi]	SIS1	SOPORTE [media]	[pdv]	Pendrive	4	4	4	4	4	0
	SIS2		[cdb]	CD/DVD /BLUE-RAY	4	4	4	4	4	0
	SIS3		[prm]	Proyector multimedia	3	3	6	0	0	3
	SIS4		[dex]	Discos externos	5	5	10	5	5	5
	SIS5		[tdm]	Lector de memorias	3	3	3	3	3	3
	SIS6		[hdv]	Hard Drive	4	4	8	4	4	4
EQUIPAMIENTO AUXILIAR [eax]	EAE1	EQUIPAMIENTO [aux]	[sai]	Sistema de Alimentación Interrumpida	3	6	6	0	3	3
	EAE2		[gpe]	Grupo Electrógeno	3	15	12	0	6	6
	EAE3		[cab]	Cableado Contingencia	3	6	6	6	3	3
	EAE4		[mvl]	Mobiliario	2	4	0	2	0	2
	EAE5		[edc]	Equipo de Climatización	3	6	9	0	0	3
	EAE6		[cel]	Cable Eléctrico	4	8	8	0	0	4
	EAE7		[fop]	Fibra Óptica	3	9	6	0	3	3

INSTALACIONES [ins]	INI1	INSTALACIONES [L]	[ofi]	Oficina	2	4	4	2	2	0
	INI2		[sco]	Sala de Comunicaciones	3	6	9	9	3	3
	INI3		[adm]	Área de mantenimiento	3	6	9	9	0	3
PERSONAL [per]	PSP1	PERSONAL [per]	[ger]	Gerencia de Sistemas	3	9	9	6	3	3
	PSP2		[aux]	Auxiliares de área	4	12	8	8	0	0
	PSP3		[use]	Usuarios Externos	4	8	4	4	4	4
	PSP4		[pea]	Personal Administrativo	4	4	0	4	4	4
	PSP5		[tin]	TI	3	9	6	9	6	6
	PSP6		[sfi]	Seguridad Física	2	6	6	2	2	0
	PSP7		[pat]	Recorredor de pozos	4	8	8	4	0	0

5.3. FASE III: PLAN DE TRAMIENTO DE RIESGOS

Una vez calificados los controles y evaluado su nivel de incidencia en la mitigación de los riesgos, si el riesgo residual se ubica en una zona de riesgo que requiera tratamiento, éste se deberá realizar en función de las cuatro opciones de tratamiento de riesgos que se describen a continuación:

Tabla 23. Opciones de tratamiento de riesgo

OPCIONES DE TRATAMIENTO DE RIESGO	
Evitar el riesgo	Implica tomar medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.
Reducir el riesgo	Implica tomar medidas encaminadas a disminuir tanto la probabilidad, como el impacto, a través de la optimización de los procedimientos y la implementación de controles eficientes, eficaces y efectivos.
Compartir o transferir el riesgo	Implica reducir su efecto a través del traspaso de posibles impactos a otras organizaciones, como el caso de los seguros o a través de otros medios que permitan distribuir una porción del riesgo con otra entidad.
Asumir el	Una vez que el riesgo ha sido reducido o transferido puede quedar un

riesgo	riesgo residual que se mantiene, en este caso se puede aceptar el riesgo residual.

(Seguridad de la Información TGE, 2016)

a. Definir Plan de tratamiento de riesgos

Tabla 24. Plan de tratamiento de riesgos

IDENTIFICACIÓN		EVALUACIÓN DEL RIESGO			
ACTIVO	**ID RIESGO**	**TIPO DE RIESGO**	**RIESGO - SITUACIÓN OBSERVADA**	**ACCIÓN CORRECTIVA**	**RESPONSABLE**
Sistema financiero integrado (SFI) WEB	**RSI-01**	Riesgo Intolerable	El sistema financiero integrado es manejado por un servicio tercer izado	• Actualización del código periódicamente.	Área de Sistemas
				• Realizar Backus de la información	Área de Sistemas
UTM FIREWALL - Gestión Unificada de Amenazas	**RSI-02**	Riesgo Intolerable	No existe monitoreo constante	• Plan de control y monitoreo, reajustando reglas y políticas institucionales, dando prioridad a la seguridad y la operatividad	Área de Sistemas
Cajero DIEBOLD	**RSI-03**	Riesgo Intolerable	Los cajeros ATM, se maneja mediante un servicio tercer izado	• Realizar soporte a los cajeros	Área de Sistemas
Cajero Multifuncional NCR		Riesgo Intolerable		• Monitoreo constante	Área de Sistemas
Modem	**RSI-04**	Riesgo Intolerable	No cuenta con un sistema de enlace de contingencia, puesto que la caída de la red, generara la inoperatividad de la sede	• Contar con un enlace de contingencia	Área de Sistemas
Router		Riesgo Tolerable			Área de Sistemas
Servidor Switch Transaccional ATM	**RSI-05**	Riesgo Intolerable	No cuenta con un sistema de control y monitoreo	• Monitoreo constante	Área de Sistemas

Servidor de Base de datos	**RSI-06**	Riesgo Intolerable	Propenso a daños físicos por caídas de tensión	• Implementar medidas de contingencia	Área de Sistemas
Servidor Balanceador					
Servidor de Aplicaciones 1					
Servidor de Aplicaciones 2					
Ap_Cobradiario	**RSI-07**	Riesgo Tolerable	El cobro no es registrado en el sistema	• Implementar un sistema en línea en tiempo real para realizar los cobros	Área de Sistemas
Internet	**RSI-08**	Riesgo Tolerable	Si se cae la red se suspende las labores	• Plan de contingencia manuales	Área de Sistemas
UPS SMART 3000 (ATM)	**RSI-09**	Riesgo Tolerable	Una falla del UPS deja expuesto a daños a los equipos del Data Center	• Contar con un UPS se reserva.	Área de Sistemas
Grupo Electrógeno	**RSI-10**	Riesgo Tolerable	En una caída de energía eléctrica, no permitiría la operatividad de la agencia	• Revisión periódica de los grupos electrógenos	Área de Sistemas

Fuente: elaboración propia

b. Operar el Sistema "ARSI"

El software tiene por objetivo hacer el seguimiento, monitoreo y control de los activos informáticos con los que cuenta la Cooperativa de Ahorro y Crédito San Francisco LTDA. 289:

- Oficina especial permanente amarilis.
- Oficina principal Huánuco
- Oficina Plaza de armas.

Se tomó en consideración las siguientes características para el desarrollo del software:

Lenguajes	PHP, JavaScript y Java
Maquetado y estilos	HTML y CSS
Framework	Laravel 5.7
Gestor de base de Datos	Mysql

El cual cuenta con cuatro módulos:

Usuarios: En el cual se podrá crear, eliminar y editar usuarios que hacen uso del modelo ARSI.

Oficinas: Se crean las dependencias de cada activo.

Activos: Lista de activos y la identificación de las amenazas, caracterización y mapa de riesgos.

- **Diseño de la Interfaz Gráfica**

A continuación se muestran los prototipos de las pantallas de inicio de sesión, sistema de control de asistencia, y el registro de los servicios brindados, entre otros.

Gráfico 7. Interfaz de usuario

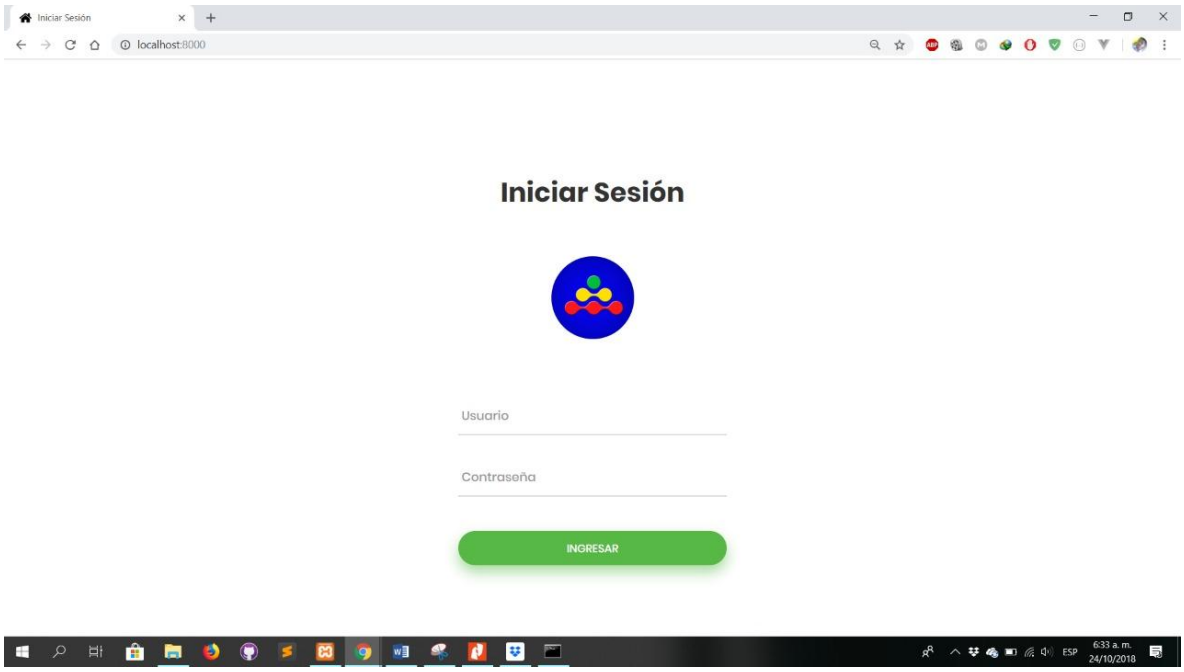
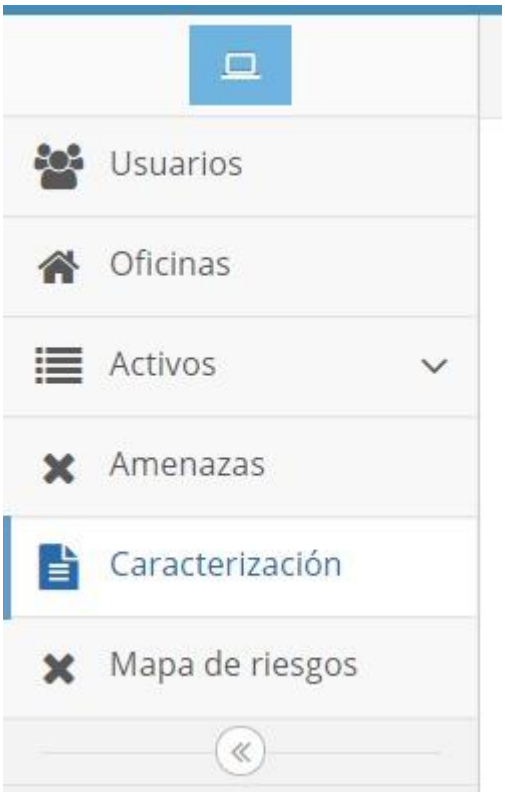
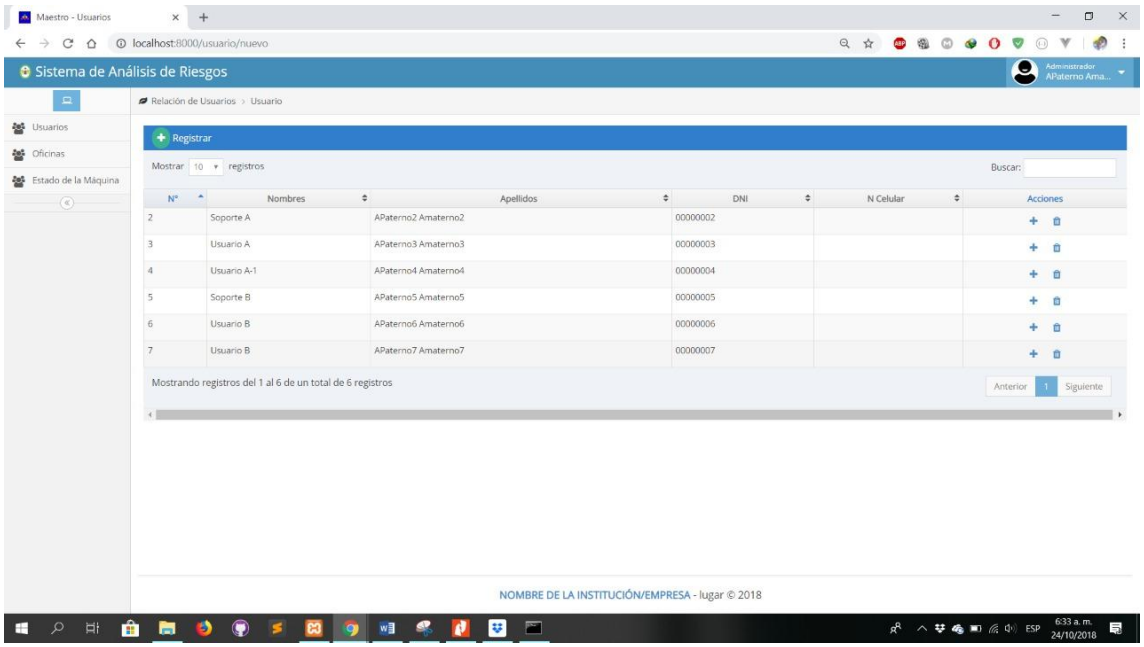


Gráfico 8. Módulos para la admiración del modelo ARSI





5.4. FASE IV: ANALIZAR CONTROLES

a. Implementación de controles

Se muestra la organización de los controles por categoría identificados.

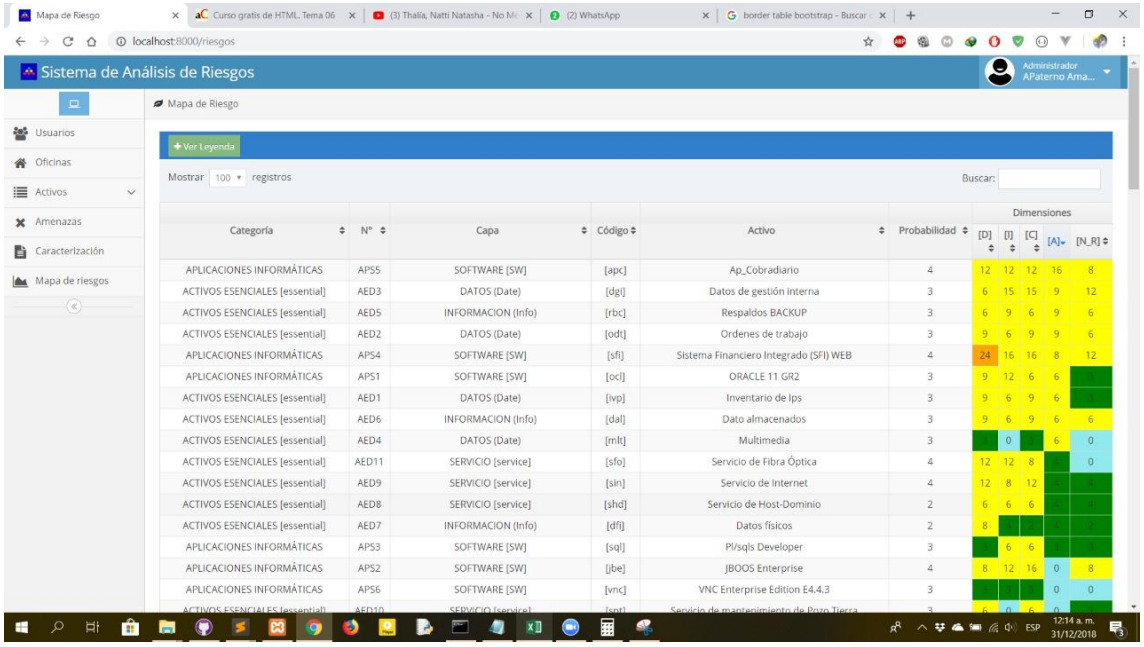
Tabla 25. Implementación de controles

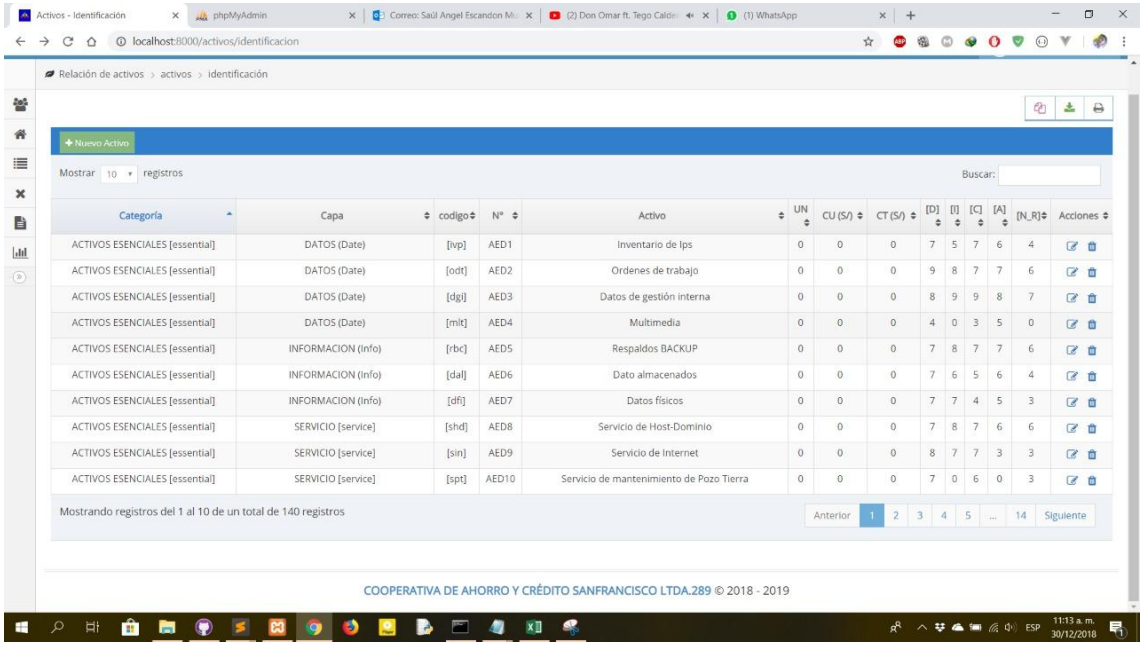
Código	Nombre	Descripción
ACTIVOS ESENCIALES [essential]		
AE1	Políticas para la seguridad de la información	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
AE2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
APLICACIONES INFORMÁTICAS [apps]		
AIN1	Política de control de acceso	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
AIN2	Política sobre el uso de los servicios de red	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

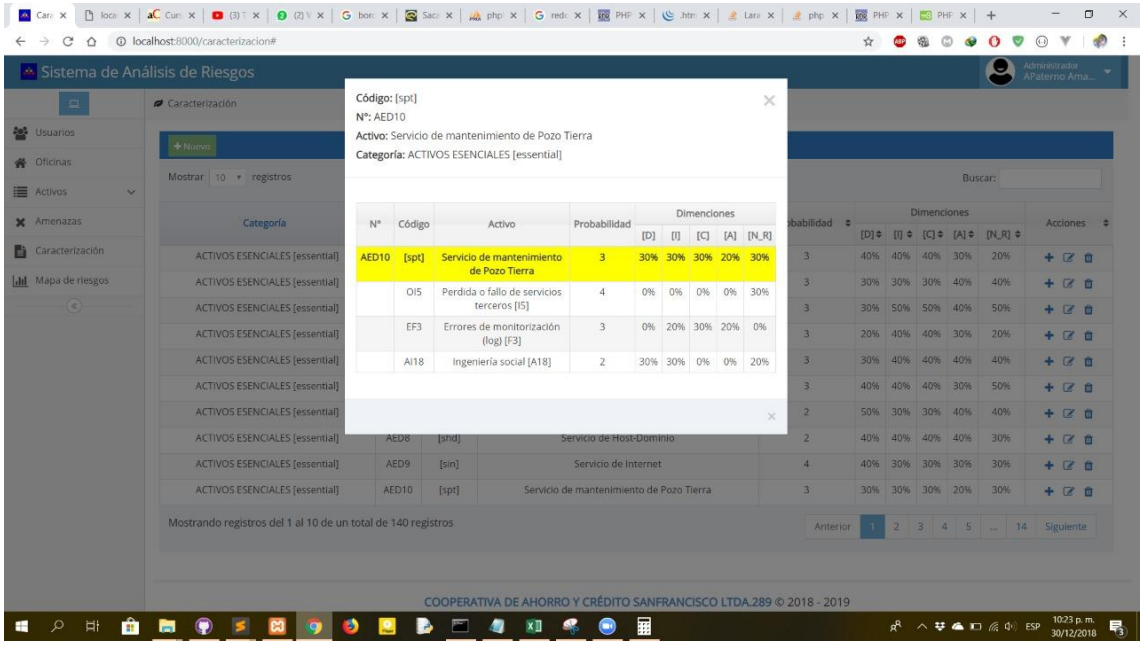
AIN3	Registro y cancelación del registro de usuarios	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
EQUIPOS INFORMÁTICOS [einf]		
EIN1	Inventario de activos	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
EIN2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deberían tener un propietario
EIN3	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo
COMUNICACIONES [ccm]		
COM1	Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
SOPORTES DE INFORMACIÓN [spi]		
EIN4	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
EIN5	Uso de programas utilitarios privilegiados	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
INSTALACIONES [ins]		
INT1	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
PERSONAL [per]		
PER1	Contacto con grupos de interés especial	Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad
PER2	Contacto con las autoridades	Se deberían mantener los contactos apropiados con las autoridades pertinentes.
PER3	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

b. Seguimiento y control mediante el software propuesto por el modelo ARSI.

El monitoreo de la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco LTDA. 289. Se realizará de manera constante mediante el software de análisis de riesgos de la seguridad de la información (ARSI)

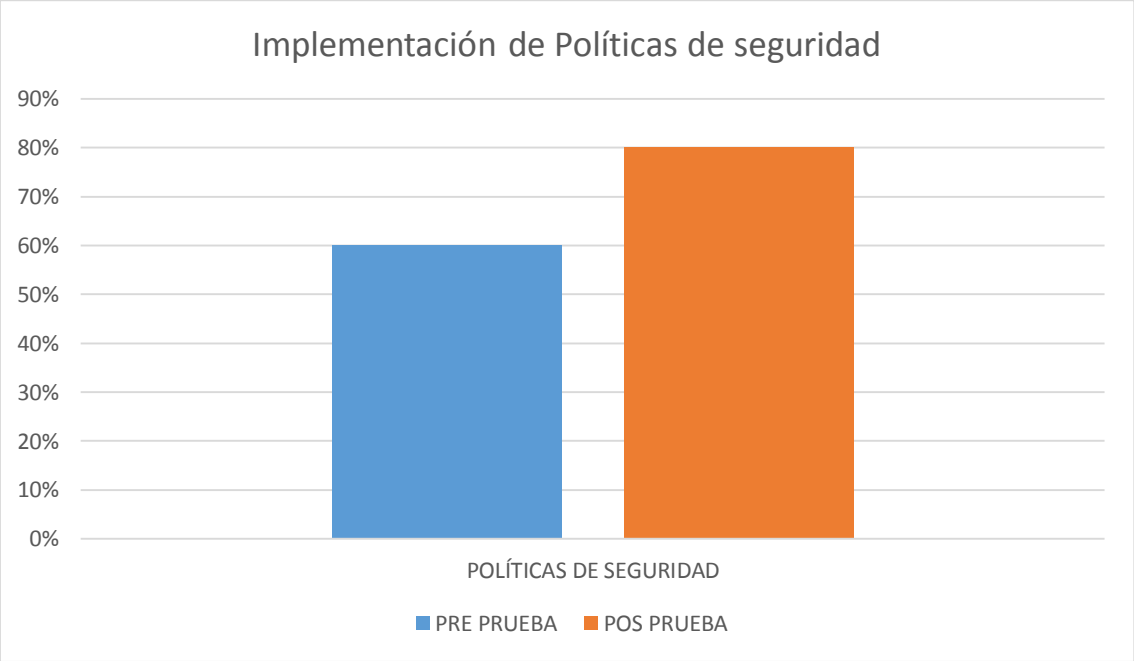






Propuesta de indicadores para evaluación de políticas de seguridad

INDICADOR – VERIFICACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		
DEFINICIÓN		
Porcentaje de políticas de seguridad institucionalizadas en la Cooperativa de Ahorro y Crédito San Francisco		
OBJETIVO		
Busca identificar el nivel de implementación de políticas de seguridad en la organización		
TIPO DE INDICADOR		
Indicador de cumplimiento		
FORMULA		**FUENTE DE INFORMACIÓN**
Número de actividades cumplidas propuestas en las políticas de seguridad de la información de la entidad / Número de políticas de la seguridad de la información totales		Usuarios internos
META		
META PROPUESTA	80%	META REAL: 75%


Implementación de Políticas de seguridad
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
POLÍTICAS DE SEGURIDAD
PRE PRUEBA
POS PRUEBA

5.5. FASE V: IMPLANTAR MEJORAS

a. Selección de las salvaguardas

En el siguiente cuadro se muestra todos los activos simplificados en su respectiva categoría y a la seguridad de la información a las cuales pertenecen.

Tabla 26. Propuestas de salvaguardas

	ORGANIZANDO LA SEGURIDAD DE LA INFORMACIÓN							
CATEGORÍA DE LOS ACTIVOS	Gestión de activos	Seguridad en RRHH	Seguridad física y ambiental	Gestión de comunicaciones y operaciones	Control de acceso	Adquisición, desarrollo y mantenimiento de SI	Gestión de incidentes de los SI	Gestión de la continuidad del negocio
ACTIVOS ESENCIALES			X	X			X	
APLICACIONES INFORMATICAS								X
EQUIPOS INFORMATICOS					X	X		X
COMUNICACIONES			X	X				X
SOPORTES DE INFORMACION			X		X	X	X	
EQUIPAMIENTO AUXILIAR		X						X
INSTALACIONES	X	X			X		X	X
PERSONAL		X	X					

b. Identificar el tipo de protección según la salvaguarda

En la tabla se muestra el listado de salvaguardas y al tipo de protección que pertenece cada uno de ellos.

Tabla 27. Tipo de protección según la salvaguarda

TIPO DE PROTECCIÓN	N°	SALVAGUARDAS
PROTECCIONES GENERALES U HORIZONTALES	**PGH1**	Identificación y autenticación
	PGH2	Control de acceso lógico
	PGH3	Gestión de incidencias
	PGH4	Herramientas de seguridad
	PGH5	Herramientas contra código dañino
	PGH6	Herramienta de detección / prevención de intrusión
	PGH7	Herramienta de chequeo de configuración
	PGH8	Herramienta de análisis de vulnerabilidades
	PGH9	Herramienta de monitorización de tráfico
	PGH10	DLP: Herramienta de monitorización de contenidos
	PGH11	Gestión de vulnerabilidades
	PGH12	Registro y auditoría
PROTECCIÓN DE LOS DATOS / INFORMACIÓN	**PDI1**	Copias de seguridad (backup)
	PDI2	Aseguramiento de la integridad
	PDI3	Cifrado de la información
	PDI4	Tercerizar el backup de los servidores
	PDI5	Protección de la información
PROTECCIÓN DE LAS CLAVES	**PCC1**	Gestión de claves de comunicaciones
	PCC2	Control y monitoreo de las claves de los principales aplicativos
PROTECCIÓN DE LOS SERVICIOS	**PPS1**	Aseguramiento de la disponibilidad
	PPS2	Cumplimiento de los proyectos tercerizado
	PPS3	Perfiles de seguridad

	PPS4	Protección de servicios y aplicaciones web
	PPS5	Protección del correo electrónico
	PPS6	Protección del directorio
	PPS7	Protección de nombres de dominio (DNS)
PROTECCIÓN DE LAS APLICACIONES (SOFTWARE)	**PPA1**	Copias de seguridad (backup)
	PPA2	Capacitaciones en TI
	PPA3	Puesta en producción
	PPA4	Actualizaciones y mantenimiento
	PPA5	Protección de las aplicaciones informáticas
PROTECCIÓN DE LOS EQUIPOS (HARDWARE)	**PPH1**	Aseguramiento de la disponibilidad
	PPH2	Mantenimiento preventivo/correctivo
	PPH3	Cambios (Actualizaciones y mantenimiento)
	PPH4	Reproducción de documentos
	PPH5	Protección de los equipos informáticos
PROTECCIÓN DE LAS COMUNICACIONES	**PPC1**	Monitoreo de las VPN
	PPC2	Autenticación de canal
	PPC3	Configuración de re-encaminamiento
	PPC4	Protección de la integridad de los datos intercambiados
	PPC5	Perfiles de seguridad
	PPC6	Telefonía móvil
	PPC7	Seguridad Wireless
	PPC8	Protección de las comunicaciones
PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN	**PSI1**	Aseguramiento de la disponibilidad
	PSI2	Limpieza de contenidos
	PSI3	Destrucción de soportes
	PSI4	Protección de los soportes de información
PROTECCIÓN DE LAS INSTALACIONES	**PEA1**	Protección del cableado
	PEA2	Climatización
	PEA3	Suministro eléctrico
	PEA4	Aseguramiento de la disponibilidad

	PEA5	Control de acceso físico
	PEA6	Aseguramiento de la disponibilidad
	PEA7	Protección de las instalaciones
SALVAGUARDAS RELATIVAS AL PERSONAL	**SRP1**	Gestión del personal
	SRP2	Capacitaciones en sistemas de información
	SRP3	Desarrollo de cronogramas de actividades trimestrales
	SRP4	Formación y concienciación
	SRP5	Aseguramiento de la disponibilidad
EXTERNALIZACIÓN	**EXT1**	Compromiso de confidencialidad
	EXT2	Identificación y calificación del personal encargado
	EXT3	Procedimiento de escalado y resolución de incidencias
ADQUISICIÓN Y DESARROLLO	**AYD1**	Servicios
	AYD2	Aplicaciones
	AYD3	Equipos
	AYD4	Comunicaciones
	AYD5	Soportes de información

CAPÍTULO VI

RESULTADOS

6.1. Análisis descriptivo

Se describe mediante figuras y tablas cada dato general, durante la aplicación del modelo ARSI, para el análisis de riesgos de los activos según los objetivos formulados en las variables investigadas, donde se han elaborado figuras y tablas de porcentajes y frecuencias utilizando un procedimiento de categorización que permita su clasificación para la variable.

VARIABLE INDEPENDIENTE X: MODELO "ARSI"

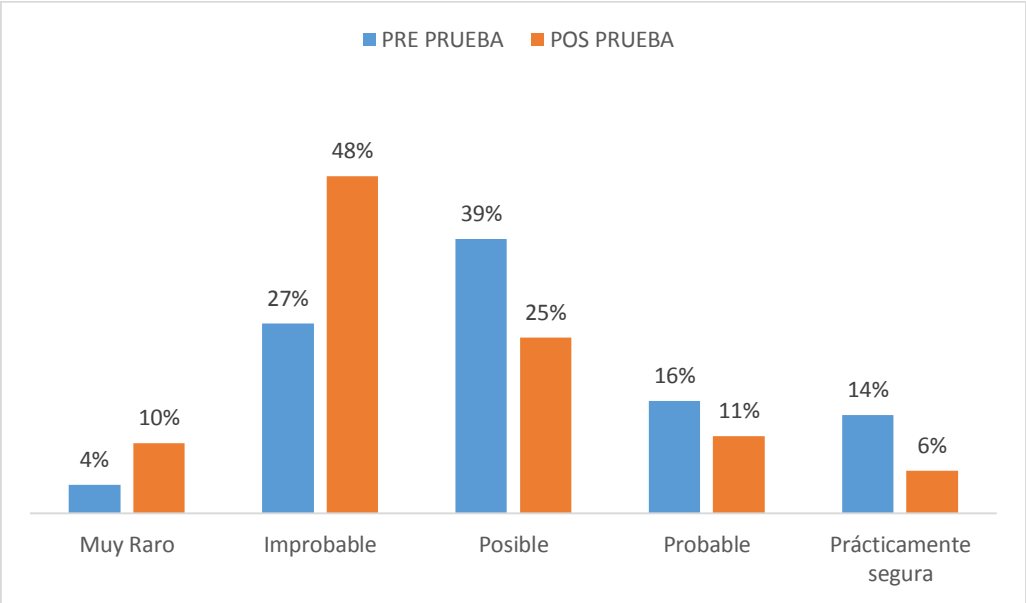
DIMENSIÓN: AMENAZAS

INDICADOR: PROBABILIDAD DE OCURRENCIA DE LA AMENAZA

Tabla 28. Resultado del indicador "Probabilidad de ocurrencia de la amenaza"

		Pre prueba "Análisis de los activos antes de la implementación del Modelo ARSI"		**Pos prueba** "Análisis de los activos después de la implementación del Modelo ARSI"	
Escala numérica	**Nivel o categoría**	**ACTIVOS**		**ACTIVOS**	
		fi	**hi%**	**fi**	**hi%**
1	Muy Raro	6	4	15	10
2	Improbable	37	27	67	48
3	Posible	54	39	33	25
4	Probable	23	16	16	11
5	Prácticamente segura	20	14	9	6
		140	100	140	100

Gráfico 9. Resultado del indicador "Probabilidad de ocurrencia de la amenaza" para los activos informáticos



La tabla N°28 muestra los resultados del indicador "probabilidad de ocurrencia" para el análisis de los activos informáticos antes de la implementación del modelo ARSI; se observa que de los 140 activos informáticos evaluados, 54 activos, que representan al 39% del total, se encuentran en la categoría de probabilidad de la amenaza POSIBLE, solo 37 se encuentran la categoría de IMPROBABLE, indicando que es muy improbable que se materialice la amenaza, la cual está representada por 27%. En cuanto a la pos prueba para el análisis de los activos después de la implementación del modelo ARSI, se observa que a comparación de la pre prueba ahora solo 33 activos informáticos, que representan el 25%, se ubican en la categoría de POSIBLE, así mismo ahora 67 activos se encuentran en la categoría de IMPROBABLE, que representan el 48%.

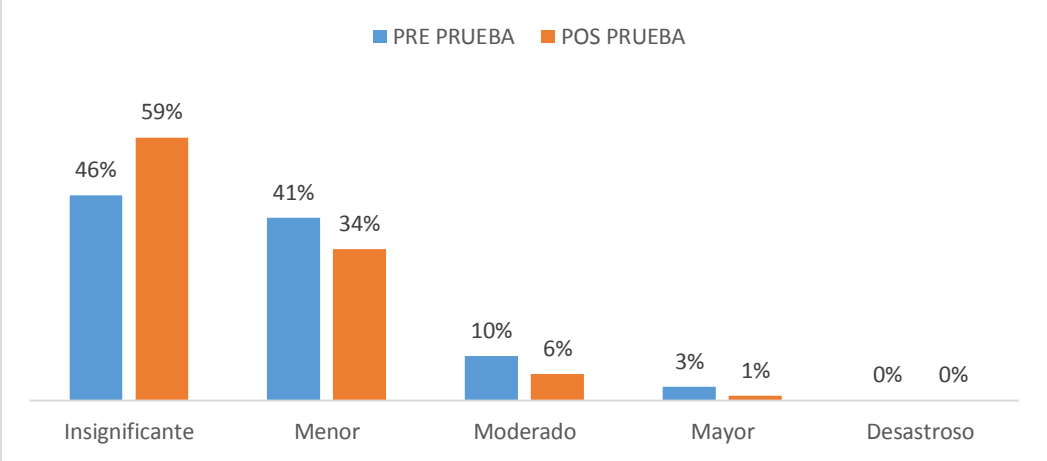
DIMENSIÓN: IMPACTO

INDICADOR: MEDIDA DE IMPACTO

Tabla 29. Resultado del indicador "Medida de Impacto"

		Pre prueba "Análisis de los activos antes de la implementación del Modelo ARSI"		**Pos prueba** "Análisis de los activos después de la implementación del Modelo ARSI"	
Rango de impacto	**Nivel o categoría**	**ACTIVOS**		**ACTIVOS**	
		fi	**hi%**	**Fi**	**hi%**
0 - 1	Insignificante	64	46	83	59
2 - 3	Menor	58	41	47	34
4 - 6	Moderado	14	10	9	6
7 - 8	Mayor	3	3	1	1
9 - 10	Desastroso	0	0	0	0
		140	100	140	100

Gráfico 10. Resultado del indicador "Medida de Impacto" para los activos informáticos



La tabla N°29 muestra los resultados del indicador "medida de impacto" para el análisis de los activos informáticos antes de la implementación del modelo ARSI; se observa que de los 140 tipos de activos informáticos evaluados, 58 activos, que representan al 41% del total, se encuentran en la categoría para la medida del impacto se encuentra en la categoría MENOR, 14 activos se encuentran la categoría de MODERADO,

indicando que si dicho activo tuviese la materialización de la amenaza, el impacto que sufriría la entidad sería un daño moderado. En cuanto a la pos prueba para el análisis de los activos después de la implementación del modelo ARSI, se observa que a comparación de la pre prueba ahora solo 47 activos informáticos, que representan el 34%, se ubican en la categoría de MENOR, así mismo ahora únicamente 9 activos se encuentran en la categoría de MODERADO, que representan el 6%.

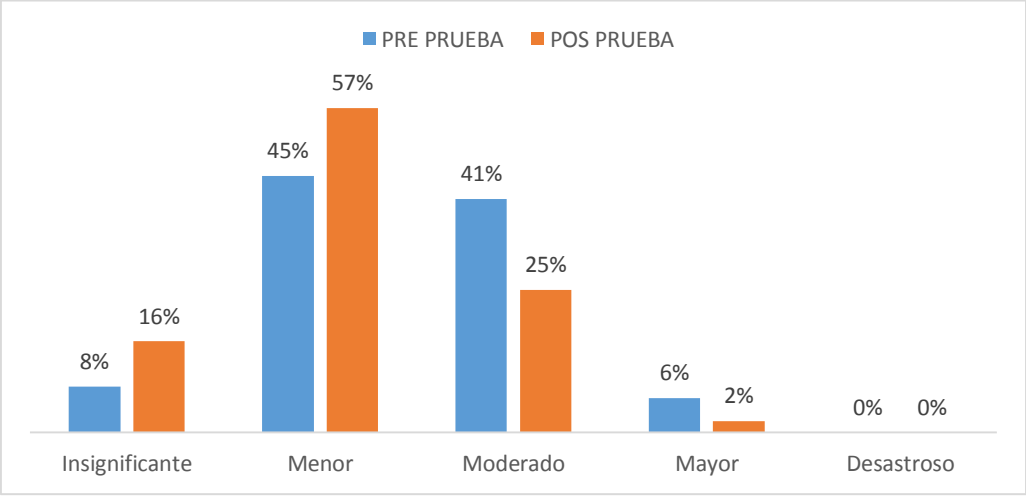
DIMENSIÓN: RIESGO

INDICADOR: ESTIMACIÓN DE RIESGO

Tabla 30. Resultado del indicador "Estimación de riesgo" para los activos informáticos

		Pre prueba "Análisis de los activos antes de la implementación del Modelo ARSI"		**Pos prueba** "Análisis de los activos después de la implementación del Modelo ARSI"	
Escala numérica	**Nivel o categoría**	**ACTIVOS**		**ACTIVOS**	
		fi	**hi%**	**fi**	**hi%**
1	Controlable	11	8	23	16
2	Aceptable	63	45	79	57
3	Tolerable	57	41	35	25
4	Intolerable	9	6	3	2
5	Extremo	0	0	0	0
		140	100	140	100

Gráfico 11. Resultado del indicador "Estimación de riesgos" para los activos informáticos



La tabla N°30 muestra los resultados del indicador “estimación de riesgo” para el análisis de los activos informáticos antes de la implementación del modelo ARSI; se observa que de los 140 tipos de activos informáticos evaluados,9 activos, que representan al 6% del total, se encuentran en la categoría para la estimación de riesgo se encuentra en la categoría de INTOLERABLE, 57 activos, que representan al 41% se encuentran la categoría de TOLERABLE, indicando que si dicho activo tuviese la materialización de la amenaza. En cuanto a la pos prueba para el análisis de los activos después de la implementación del modelo ARSI, se observa que a comparación de la pre prueba ahora solo 3 activos informáticos, que representan el 2%, se ubican en la categoría de INTOLERABLE, así mismo ahora únicamente 35 activos se encuentran en la categoría de TOLERABLE, que representan el 25%.

VARIABLE DEPENDIENTE Y: SEGURIDAD DE LA INFORMACIÓN

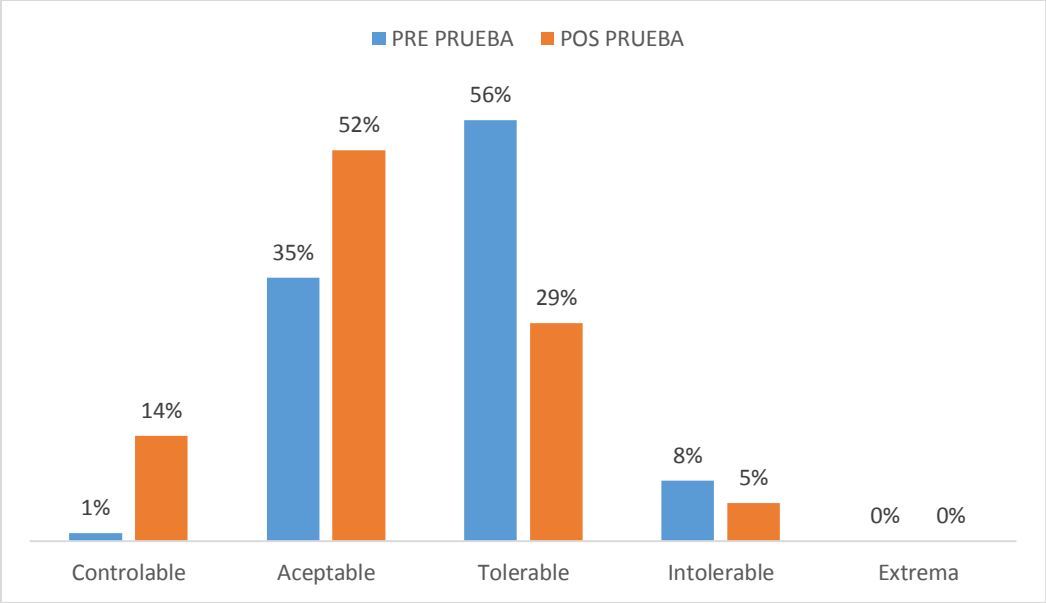
DIMENSIÓN: DISPONIBILIDAD

INDICADOR: RIESGO EN LA DISPONIBILIDAD DE LA INFORMACIÓN DE LOS ACTIVOS INFORMÁTICOS

Tabla 31. Resultado del indicador “Riesgo en la disponibilidad de la información de los activos informáticos”

		Pre prueba “Análisis de los activos antes de la implementación del Modelo ARSI”		**Pos prueba** “Análisis de los activos después de la implementación del Modelo ARSI”	
Escala numérica	**Nivel o categoría**	**ACTIVOS**		**ACTIVOS**	
		fi	**hi%**	**fi**	**hi%**
1	Controlable	1	1	19	14
2	Aceptable	49	35	73	52
3	Tolerable	79	56	41	29
4	Intolerable	11	8	7	5
5	Extrema	0	0	0	0
		140	100	140	100

Gráfico 12. Resultado del indicador "Riesgo en la disponibilidad de la información de los activos informáticos"



La tabla N°31 muestra los resultados del indicador "Riesgo en la disponibilidad de la información de los activos informáticos" para el análisis de los activos informáticos antes de la implementación del modelo ARSI; se observa que de los 140 tipos de activos informáticos evaluados, 11 activos, que representan al 8% del total, se encuentran en la categoría para la estimación de riesgo se encuentra en la categoría de INTOLERABLE, 79 activos, que representan al 56% se encuentran la categoría de TOLERABLE, indicando que si dicho activo tuviese la materialización de la amenaza para la disponibilidad de la información, podría causar un daño tolerable para la empresa. En cuanto a la pos prueba para el análisis de los activos después de la implementación del modelo ARSI, se observa que a comparación de la pre prueba ahora solo 7 activos informáticos, que representan el 5%, se ubican en la categoría de INTOLERABLE, así mismo ahora únicamente 41 activos se encuentran en la categoría de TOLERABLE, que representan el 29%.

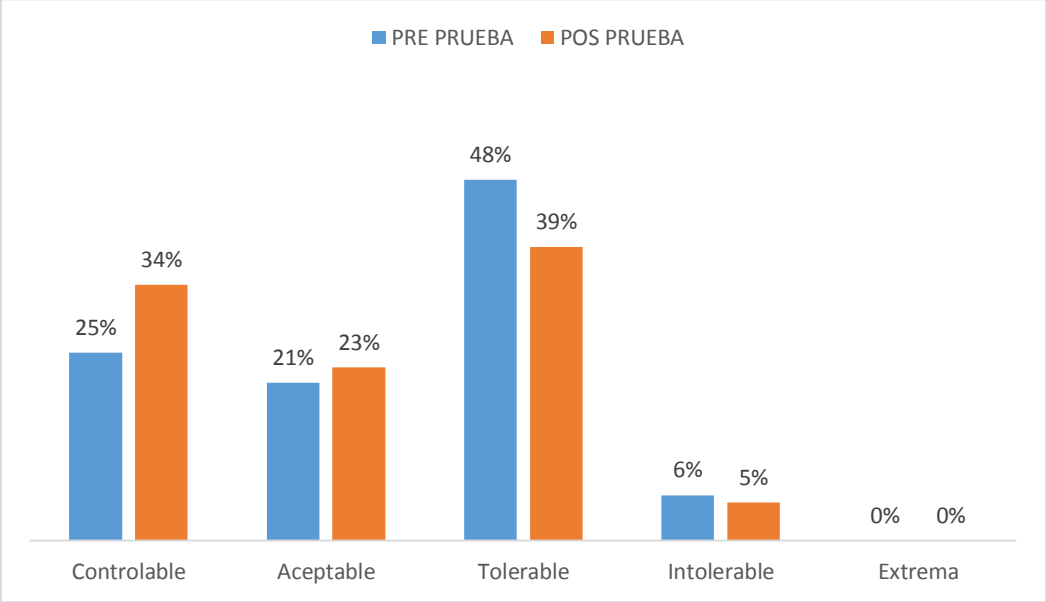
DIMENSIÓN: INTEGRIDAD

INDICADOR: RIESGO EN LA INTEGRIDAD DE LA INFORMACIÓN DE LOS ACTIVOS INFORMÁTICOS

Tabla 32. Resultado del indicador "Riesgo en la Integridad de la información de los activos informáticos"

		Pre prueba "Análisis de los activos antes de la implementación del Modelo ARSI"		**Pos prueba** "Análisis de los activos después de la implementación del Modelo ARSI"	
Escala numérica	**Nivel o categoría**	**ACTIVOS**		**ACTIVOS**	
		fi	**hi%**	**fi**	**hi%**
1	Controlable	35	25	48	34
2	Aceptable	29	21	31	23
3	Tolerable	67	48	55	39
4	Intolerable	9	6	6	4
5	Extrema	0	0	0	0
		140	100	140	100

Gráfico 13. Resultado del indicador "Riesgo en la Integridad de la información de los activos informáticos"



La tabla N°32 muestra los resultados del indicador "Riesgo en la integridad de la información de los activos informáticos" para el análisis de los activos informáticos antes de la implementación del modelo ARSI; se

observa que de los 140 tipos de activos informáticos evaluados, 9 activos, que representan al 6% del total, se encuentran en la categoría para la estimación de riesgo se encuentra en la categoría de INTOLERABLE, 67 activos, que representan al 48% se encuentran la categoría de TOLERABLE, indicando que si dicho activo tuviese la materialización de la amenaza para la integridad de la información, podría causar un daño tolerable para la empresa. En cuanto a la pos prueba para el análisis de los activos después de la implementación del modelo ARSI, se observa que a comparación de la pre prueba ahora solo 6 activos informáticos, que representan el 4%, se ubican en la categoría de INTOLERABLE, así mismo ahora únicamente 55 activos se encuentran en la categoría de TOLERABLE, que representan el 39%.

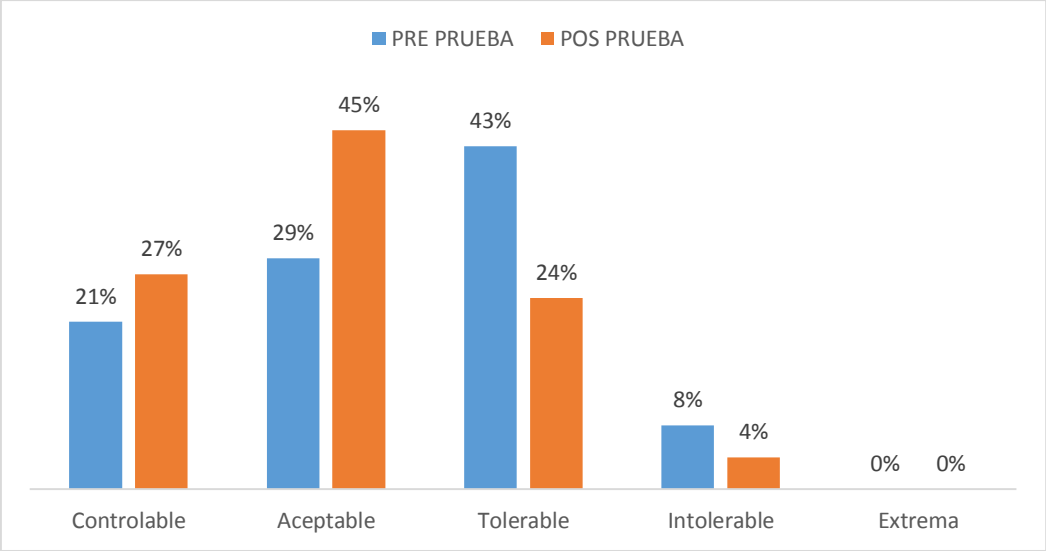
DIMENSIÓN: CONFIDENCIALIDAD

INDICADOR: RIESGO EN LA CONFIDENCIALIDAD DE LA INFORMACIÓN DE LOS ACTIVOS INFORMÁTICOS

Tabla 33. Resultado del indicador "Riesgo en la confidencialidad de la información de los activos informáticos"

		Pre prueba "Análisis de los activos antes de la implementación del Modelo ARSI"		**Pos prueba** "Análisis de los activos después de la implementación del Modelo ARSI"	
Escala numérica	**Nivel o categoría**	**ACTIVOS**		**ACTIVOS**	
		fi	**hi%**	**fi**	**hi%**
1	Controlable	29	21	38	27
2	Aceptable	40	29	63	45
3	Tolerable	60	43	34	24
4	Intolerable	11	8	5	4
5	Extrema	0	0	0	0
		140	100	140	100

Gráfico 14. Resultado del indicador "Riesgo en la confidencialidad de la información de los activos informáticos"



La tabla N°33 muestra los resultados del indicador "Riesgo en la confidencialidad de la información de los activos informáticos" para el análisis de los activos informáticos antes de la implementación del modelo ARSI; se observa que de los 140 tipos de activos informáticos evaluados, 11 activos, que representan al 8% del total, se encuentran en la categoría para la estimación de riesgo se encuentra en la categoría de INTOLERABLE, 60 activos, que representan al 43% se encuentran la categoría de TOLERABLE, indicando que si dicho activo tuviese la materialización de la amenaza para la confidencialidad de la información, podría causar un daño tolerable para la empresa. En cuanto a la pos prueba para el análisis de los activos después de la implementación del modelo ARSI, se observa que a comparación de la pre prueba ahora solo 5 activos informáticos, que representan el 4%, se ubican en la categoría de INTOLERABLE, así mismo ahora únicamente 34 activos se encuentran en la categoría de TOLERABLE, que representan el 24%.

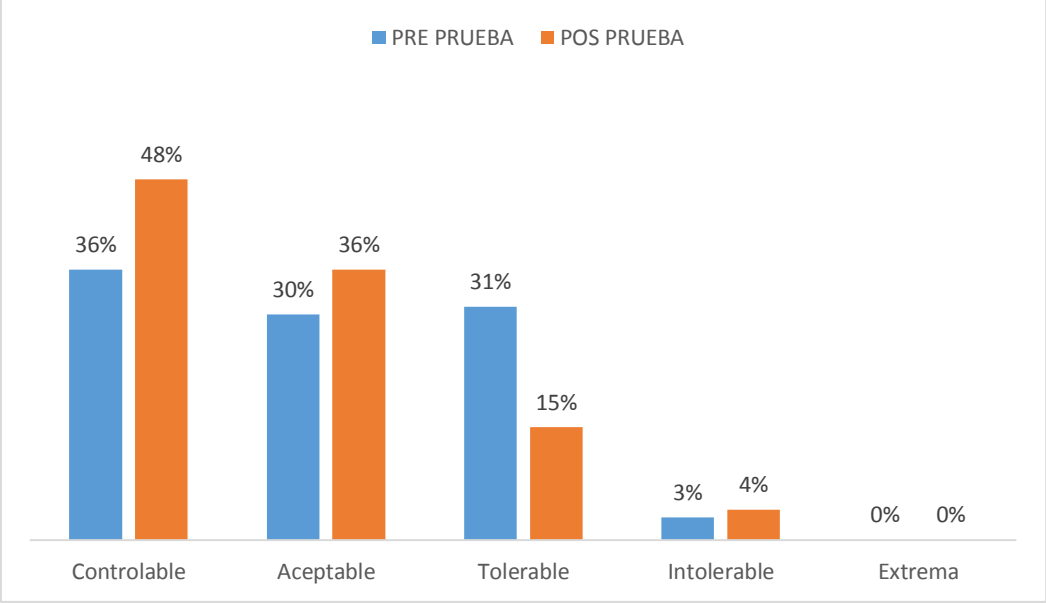
DIMENSIÓN: AUTENTIFICACIÓN

INDICADOR: RIESGO EN LA AUTENTIFICACIÓN DE LA INFORMACIÓN DE LOS ACTIVOS INFORMÁTICOS

Tabla 34. Resultado del indicador "Riesgo en la autentificación de la información de los activos informáticos"

		Pre prueba "Análisis de los activos antes de la implementación del Modelo ARSI"		**Pos prueba** "Análisis de los activos después de la implementación del Modelo ARSI"	
Escala numérica	**Nivel o categoría**	**ACTIVOS**		**ACTIVOS**	
		fi	**hi%**	**fi**	**hi%**
1	Controlable	50	36	68	48
2	Aceptable	42	30	50	36
3	Tolerable	43	31	21	15
4	Intolerable	5	3	1	1
5	Extrema	0	0	0	0
		140	100	140	100

Gráfico 15. Resultado del indicador "Riesgo en la autentificación de la información de los activos informáticos"



La tabla N°34 muestra los resultados del indicador "Riesgo en la autentificación de la información de los activos informáticos" para el análisis de los activos informáticos antes de la implementación del modelo ARSI; se observa que de los 140 tipos de activos informáticos evaluados,

5 activos, que representan al 3% del total, se encuentran en la categoría para la estimación de riesgo se encuentra en la categoría de INTOLERABLE, 43 activos, que representan al 31% se encuentran la categoría de TOLERABLE, indicando que si dicho activo tuviese la materialización de la amenaza para la autentificación de la información, podría causar un daño tolerable para la empresa. En cuanto a la pos prueba para el análisis de los activos después de la implementación del modelo ARSI, se observa que a comparación de la pre prueba ahora solo 1 activos informáticos, que representan el 1%, se ubican en la categoría de INTOLERABLE, así mismo ahora únicamente 21 activos se encuentran en la categoría de TOLERABLE, que representan el 15%.

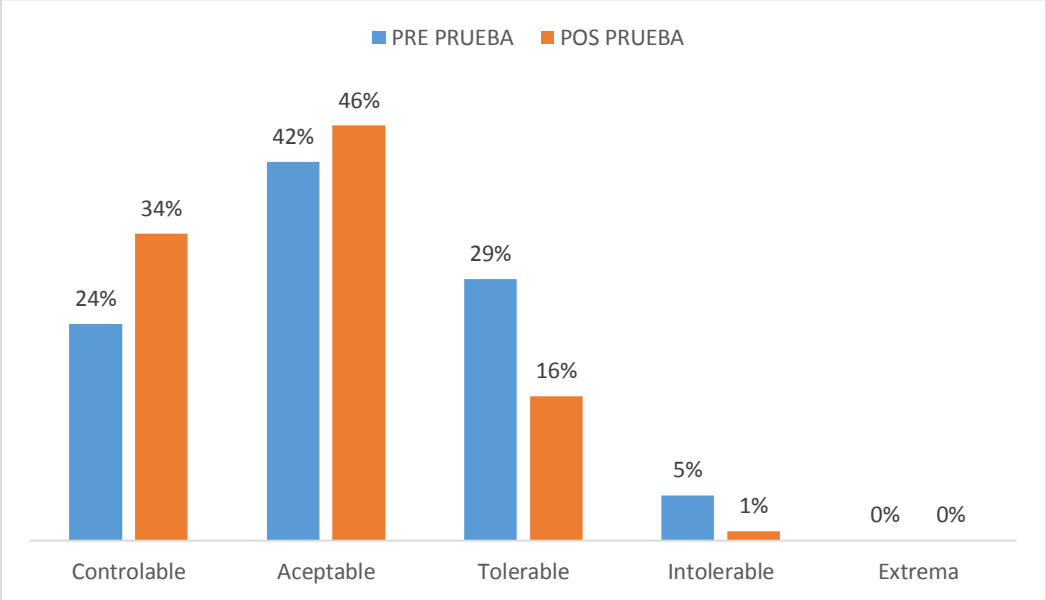
DIMENSIÓN: NO REPUDIO

INDICADOR: RIESGO EN NO REPUDIO DE LA INFORMACIÓN DE LOS ACTIVOS INFORMÁTICOS

Tabla 35. Resultado del indicador "Riesgo en no repudio de la información de los activos informáticos"

		Pre prueba "Análisis de los activos antes de la implementación del Modelo ARSI"		**Pos prueba** "Análisis de los activos después de la implementación del Modelo ARSI"	
Escala numérica	**Nivel o categoría**	**ACTIVOS**		**ACTIVOS**	
		fi	**hi%**	**fi**	**hi%**
1	Controlable	35	24	48	34
2	Aceptable	59	42	64	46
3	Tolerable	40	29	23	16
4	Intolerable	6	5	5	4
5	Extrema	0	0	0	0
		140	100	140	100

Gráfico 16. Resultado del indicador "Riesgo en no repudio de la información de los activos informáticos"



La tabla N°35 muestra los resultados del indicador "Riesgo en no repudio de la información de los activos informáticos" para el análisis de los activos informáticos antes de la implementación del modelo ARSI; se observa que de los 140 tipos de activos informáticos evaluados, 6 activos, que representan al 5% del total, se encuentran en la categoría para la estimación de riesgo se encuentra en la categoría de INTOLERABLE, 40 activos, que representan al 29% se encuentran la categoría de TOLERABLE, indicando que si dicho activo tuviese la materialización de la amenaza para el no repudio de la información, podría causar un daño tolerable para la empresa. En cuanto a la pos prueba para el análisis de los activos después de la implementación del modelo ARSI, se observa que a comparación de la pre prueba ahora solo 5 activos informáticos, que representan el 4%, se ubican en la categoría de INTOLERABLE, así mismo ahora únicamente 23 activos se encuentran en la categoría de TOLERABLE, que representan el 16%.

INTERPRETACIÓN GENERAL

De acuerdo a los resultados obtenidos mediante el análisis de riesgo de los activos informáticos, se pudo evidenciar la variación del riesgo de los activos, antes y después de la aplicación del modelo propuesto “ARSI”; dado que, en la variable dependiente, seguridad de la información; tanto para el riesgo en la disponibilidad, integridad, confidencialidad y no repudio se observa que para la pre prueba la mayoría de los activos se centra en un riesgo TOLERABLE, representados por 56%, 48%, 43%, 31% y 29% respectivamente; una vez que se aplicó la pos prueba la mayoría de los activos se centraron dentro de un riesgo ACEPTABLE; 52%, 23%, 45%, 36 y 46% respectivamente, lo cual es evidencia para afirmar que mediante la implementación del modelo ARSI, se optimizó la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco.

6.2. Análisis inferencial y contrastación de la hipótesis

6.2.1. Contrastación de la hipótesis general

Variables:

V. I.: MODELO ARSI

V. D.: SEGURIDAD DE LA INFORMACIÓN

1. Planeamiento de hipótesis:

H0: Mediante el modelo "ARSI" no se optimizará la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco.

Hi: Mediante el modelo "ARSI" se optimizará la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco.

Tabla 36. Diferencia de medias para el análisis de la pre y pos prueba aplicada a los activos informáticos

Diferencia de medias			
Activos informáticos	**Pre prueba** "Análisis de riesgo los activos antes de la implementación del Modelo ARSI"	Media	2,46
		Desviación estándar	1,18
		N	140
	Pos prueba "Análisis de riesgo de los activos después de la implementación del Modelo ARSI"	Media	1,57
		Desviación estándar	1,20
		N	140

Ho: $\boldsymbol{\mu_1 = \mu_2}$

H1: $\boldsymbol{\mu_1 \neq \mu_2}$

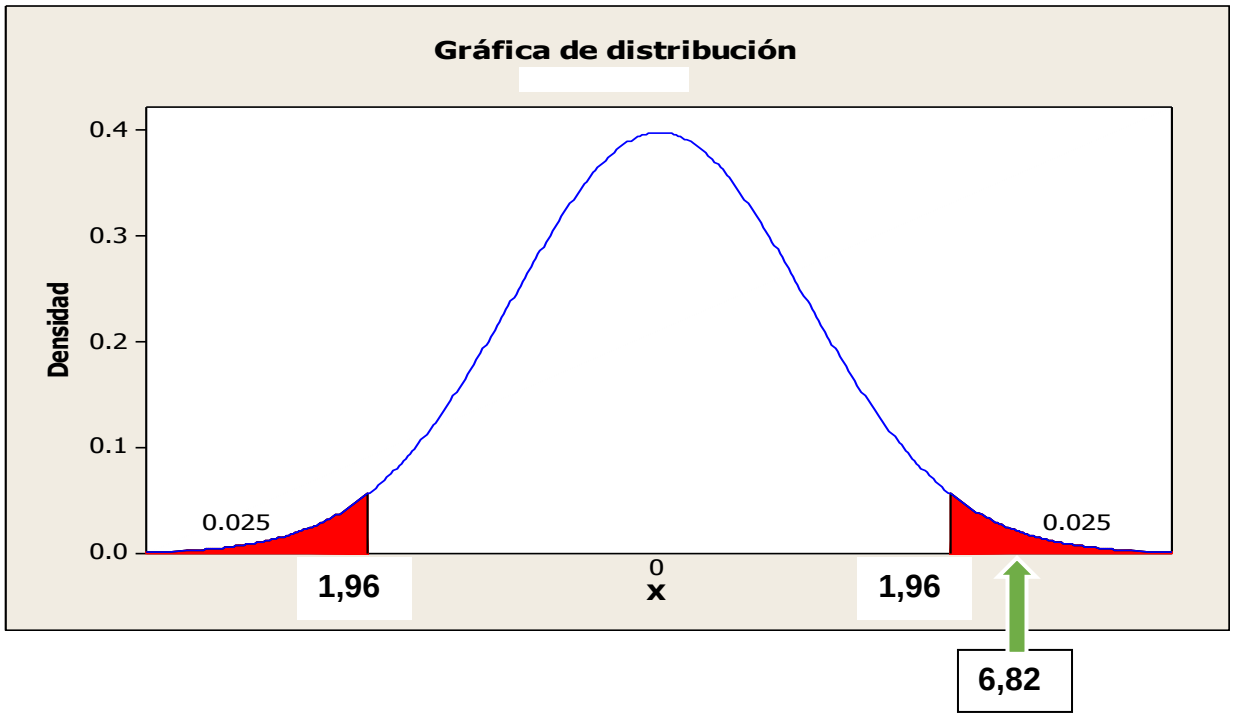
A partir de los resultados obtenidos mediante el SPSS en la tabla N°29 se obtiene:

$$Z = \frac{(\bar{X}_1 - \bar{X}_2)}{\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}}$$

$$Z = \frac{(2.46 - 1,57)}{\sqrt{\frac{1,18}{140} + \frac{1,20}{140}}}$$

$$Z = 6,82$$

Nivel de significancia: α = 0.05 **α /2 = 0.025** **Z = 1,96**



Conclusión:

En los resultados que se muestran en la tabla N°29, se puede apreciar la diferencia de medias al evaluar el pre y pos análisis de riesgo de los activos informáticos, obteniendo como media para la pre prueba = 2,46; con una

desviación estándar de 1,18 y para el pos análisis, es de 1,57; y una desviación estándar de 1,12; evaluados a un nivel de significancia **α** /2 = 0.025; entre un valor critico de (-1,96 < Z >1,96), una vez evaluado la distribución normal se obtuvo como valor de Z = 6,82; por lo cual **se rechaza la hipótesis nula y se acepta la hipótesis alterna**; es decir, “Mediante el modelo "ARSI" se optimizará la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco”.

6.2.2. Contrastación de las hipótesis secundarias

Mediante la utilización del software informático SPSS el cual nos permite procesar la información se han obtenido las siguientes tablas donde se detalla los resultados obtenidos para cada uno.

a. Prueba de hipótesis para el Análisis de las políticas de seguridad para los activos informáticos mediante diferencia de medias.

Tabla 37.Análisis de las políticas de seguridad para los activos informáticos mediante diferencia de medias

Diferencia de medias			
Activos informáticos	**Pre prueba** “Análisis de riesgo los activos antes de la implementación del Modelo ARSI”	Media	3,22
		Desviación estándar	1,19
		N	140
	Pos prueba “Análisis de riesgo de los activos después de la implementación del Modelo ARSI”	Media	2,30
		Desviación estándar	1,14
		N	140

- HO_2: Mediante la implementación de políticas de seguridad no se minimizará los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289.

  Hi_2: Mediante la implementación de políticas de seguridad sí se minimizará los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289.

Ho: $\boldsymbol{\mu_1 = \mu_2}$

H1: $\boldsymbol{\mu_1 \neq \mu_2}$

A partir de los resultados obtenidos mediante el SPSS en la tabla N°30 se obtiene:

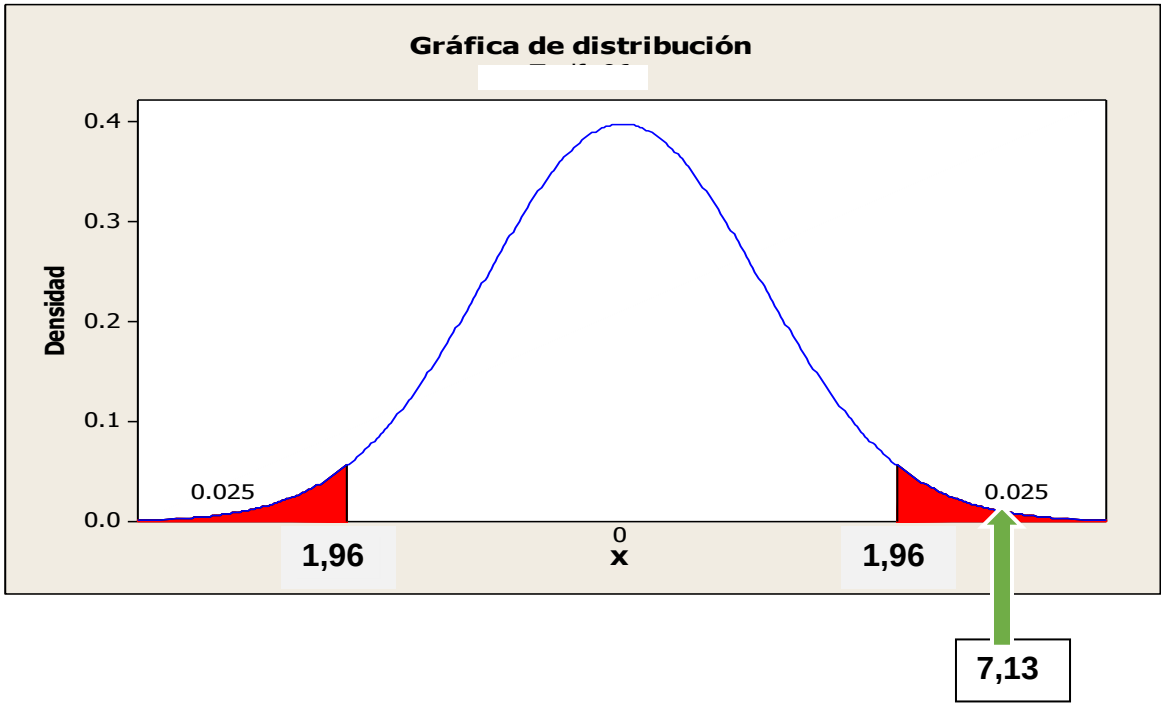
$$\boldsymbol{Z = \frac{(\bar{X}_1 - \bar{X}_2)}{\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}}}$$

$$\boldsymbol{Z = \frac{(3,22 - 2,30)}{\sqrt{\frac{1,19}{140} + \frac{1,14}{140}}}}$$

$$\boldsymbol{Z = 7,13}$$

Nivel de significancia: α = 0.05

α /2 = 0.025 **Z = 1,96**



Conclusión:

En los resultados que se muestran en la tabla N°30, se puede apreciar la diferencia de medias al evaluar el pre y pos análisis de riesgo de los activos informáticos, obteniendo como media para la pre prueba = 3,22; con una desviación estándar de 1,19 y para la pos prueba, la cual se aplicó después de la llegada de los supermercados es 2,30; y una desviación estándar de 1,14; evaluados a un nivel de significancia α /2 = 0.025; entre un valor critico de (-1,96 < Z >1,96), una vez evaluado la distribución normal se obtuvo como valor de Z = 7,13; por lo cual se **Se rechaza la hipótesis nula y se acepta la hipótesis alterna**; es decir, “Mediante la implementación de políticas de seguridad sí se minimizará los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289”.

a. Prueba de hipótesis para la implementación del software de monitoreo mediante diferencia de medias.

Tabla 38. Prueba de hipótesis para la implementación del software de monitoreo mediante diferencia de medias.

Diferencia de medias			
Activos informáticos	**Pre prueba** "Análisis de riesgo los activos antes de la implementación del Modelo ARSI"	Media	3,70
		Desviación estándar	1,17
		N	140
	Pos prueba "Análisis de riesgo de los activos después de la implementación del Modelo ARSI"	Media	2,83
		Desviación estándar	1,13
		N	140

- Ho_2: Mediante la implementación del software de monitoreo no se mitigará los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289.

  Hi_2: Mediante la implementación del software de monitoreo si se mitigará los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289.

A partir de los resultados obtenidos mediante el SPSS en la tabla N°16 se obtiene:

Ho: $\boldsymbol{\mu_1 = \mu_2}$

Hi: $\boldsymbol{\mu_1 \neq \mu_2}$

A partir de los resultados obtenidos mediante el SPSS en la tabla N° 16 se obtiene:

$$Z = \frac{(\bar{X}_1 - \bar{X}_2)}{\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}}$$

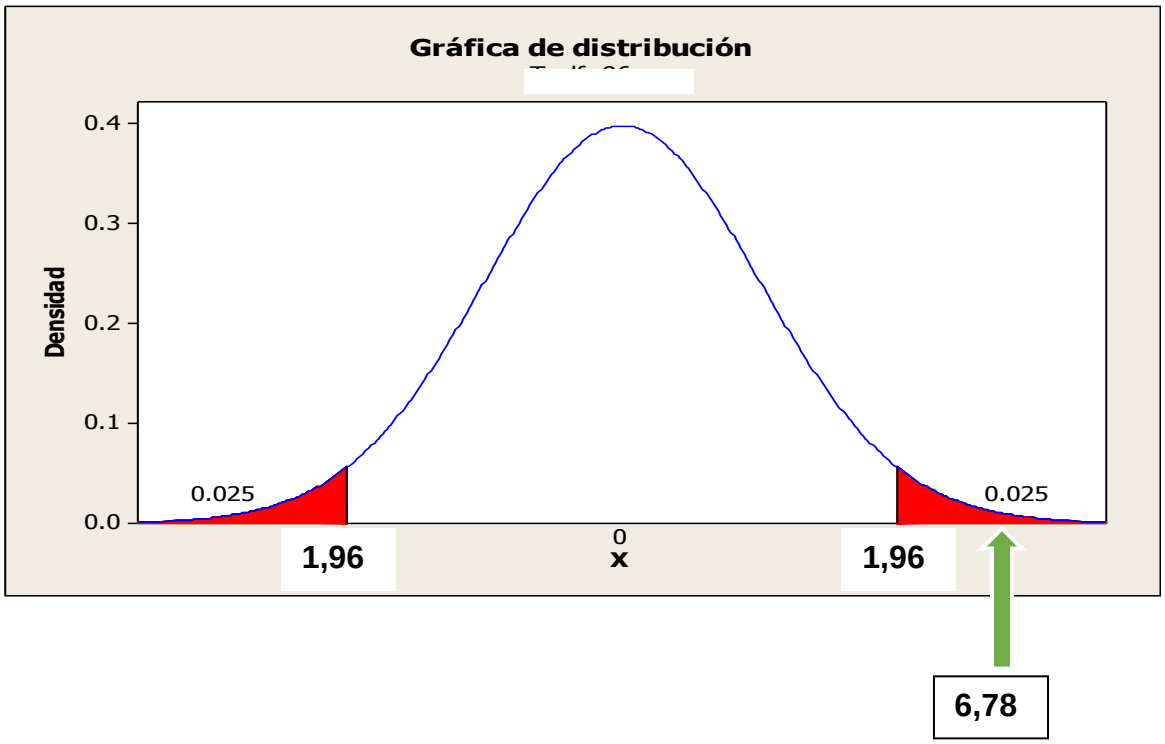
$$Z = \frac{(3,70 - 2,83)}{\sqrt{\frac{1,17}{140} + \frac{1,13}{140}}}$$

$$Z = 6,78$$

Nivel de significancia: α = 0.05

α /2 = 0.025

Z = 1,96



Conclusión:

En los resultados que se muestran en la tabla N°31, se puede apreciar la diferencia de medias al evaluar el pre y pos análisis de riesgo de los activos informáticos, obteniendo como media para la pre prueba = 3,70; con una desviación estándar de 1,17 y para la pos prueba, la media es de 2,83; y una desviación estándar de 1,13; evaluados a un nivel de significancia **α** /2 = 0.025; entre un valor critico de (-1,96 < Z >1,96), una vez evaluado la distribución normal se obtuvo como valor de Z = 6,78; por lo cual se **Se rechaza la hipótesis nula y se acepta la hipótesis alterna**; es decir, “Mediante la implementación del software de monitoreo si se mitigará los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289”.

6.3. Discusión de resultados

En este apartado se presenta la confrontación de la situación problemática formulada con los referentes bibliográficos de las bases teóricas, la hipótesis general y el aporte científico de la investigación.

Las teorías planteadas constituyen una base sólida para las variables de estudio en la cual se contrasta nuestros resultados.

El resultado de la hipótesis general; se obtuvo el valor de Z obtiene el valor de 6,82 por lo cual se **rechaza la hipótesis nula y se acepta la hipótesis alterna** concluyendo que, “mediante el modelo "ARSI" se optimizará la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco; evidenciados que la implementación del modelo ARSI, contribuyo de manera positiva

en la mitigación de los riesgos a los que estaban expuestos los activos informáticos. En la cual nuestros resultados guardan relación con la investigación realizada por Serrano (2007); en su tesis Gestión de seguridad de la información y los servicios críticos de las universidades, quien concluye que los riesgos de la información en las universidades como son: divulgación ilícita de la información por los trabajadores (UNFV 36%), no realizaron copias de seguridad (UPSJB 28%), virus informáticos (UNMSM 56%), corroboran con lo que está pasando a nivel mundial, donde el 70% de los rodos o accidentes que se producen en los sistemas informáticos de las organizaciones los causan los propios trabajadores, ya que muchas veces son resultados de errores, descuidos o desconocimiento sobre la seguridad de la organización o actos delictivos propiamente dichos, los cuales fueron mitigados mediante la implementación de un sistema de control y monitoreo de riesgos.

CONCLUSIONES

Del análisis de los resultados obtenidos en la investigación y contrastándolos con los objetivos planteados, podemos concluir en lo siguiente:

1. En relación a la prueba de hipótesis general se obtuvo un valor de Z = 6,82 por lo cual **se rechaza la hipótesis nula y se acepta la hipótesis alterna**; es decir, “Mediante el modelo "ARSI" se optimizará la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco”.
2. Se propuso y ejecuto las políticas se seguridad aprobadas en la Cooperativa de Ahorro y Crédito San Francisco LTDA. 289, permitiendo conocer que el antes de la implementación del modelo ARSI, únicamente se hacían efectivos el 60% de las políticas de seguridad, una vez que se implementó el modelo ARSI, se puede afirmar que se hacen uso del 80% de las políticas aprobadas por la institución.
3. Mediante la implementación de los controles para realizar el seguimiento y monitoreo de la seguridad de los activos mediante la implementación del software se puede afirmar de los resultados obtenidos donde Z obtiene el valor de 6,78 por lo cual se **rechaza la hipótesis nula y se acepta la hipótesis alterna** concluyendo que, “Mediante la implementación del software de monitoreo si se mitigará los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289”.

RECOMENDACIONES O SUGERENCIAS

De acuerdo a las conclusiones de la investigación realizada se sugiere lo siguiente:

1. A los encargados del área de sistemas realizar una evaluación periódica de las políticas de seguridad aprobadas, puesto que la tecnología está en constante evolución y con ello existen nuevas amenazas que las aquejan.
2. A los encargados del seguimiento de monitoreo y control de la seguridad de los activos informáticos continuar con el plan de tratamiento propuesto para la mitigación de los riesgos identificados.

REFERENCIAS BIBLIOGRAFICAS

Barrantes Porras, C. E., & Hugo Herrera, J. R. (2012). *Diseño e implementación de un sistema de Gestión de Seguridad de Información en procesos tecnológicos.* Lima: Escuela Profesional de Ingeniería de Computación y Sistemas-USMP.

Canales, F., De Alvarado, E., & Pineda, E. (1994). *Metodología de la investigacion.* T. ed México: Limusa.

Chumán, J. G. (2015). *Aplicación de la Metodología MAGERIT para el Análisis y Gestión de Riesgos en los Servidores de los Sistemas de Gestión Académica de la Universidad Nacional Pedro Ruiz Gallo.* Lambayeque: Universidad Nacional Pedro Ruiz Gallo.

Florentino Galindo , E., & Morales Morales, J. (2008). *Aplicación de la Metodología MAGERIT en el Análisis de Riesgo del Flujo de Información en el área de Gestión de una empresa dedicada a la aplicación de exámenes de Control de Confianza.* México, D.F.: Instituto Politécnico Nacional.

Luhmann, N. (1998). *"Sociología del riesgo".* México: Triana Editores; Universidad Iberoamericana.

Morales, V. (1994). *Planeamiento y análisis de investigaciones.* Caracas, Venezuela: El dorado Ediciones.

Moreno, D. A. (2012). *Gestión del Riesgo en la Seguridad Informática: "Cultura de la Auto-seguridad Informática".* Bogotá: Universidad Militar Nueva Granada, especialización en Control Interno.

NIST. (s.f.). *National Institute of Standards and Technology*. Obtenido de https://www.nist.gov/

Quiroz, L. G. (1996). Teoría General de Riesgos y controles en Sistemas de Información. En L. G. Quiroz, *Informática y Auditoría para las ciencias empresariales* (pág. 51). Bucaramanga: ISBN 958-96064-1-5.

Ramos, V. P. (2015). *Análisis de Riesgos Informáticos y Desarrollo de un Plan de Seguridad de la Información para el Gobierno Autónomo Descentralizado Municipal de Catamayo.* Catamayo: Universidad Nacional de Loja.

Sampieri, H. (1994). Metodología de la Investigación. En H. Sampieri, *Definición del Tipo de Investigación a realizar: Básicamente exploratoria, descriptiva, correlacional o explicativa* (pág. Cap.4 y5). México: Mc Graw Hill.

SEI. (s.f.). *Software Engineering Institute*. Obtenido de https://www.sei.cmu.edu/

Serrano, R. A. (2007). *Gestión de seguridad de la información y los servicios críticos de las universidades.* Lima: Universidad Nacional Mayor de San Marcos.

Vásquez, K. d. (2013). *Aplicación de la Metodología Magerit para el Análisis y Gestión de Riesgos de la Seguridad de la Información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala.* Cuenca: Universidad Politécnica Salesiana Sede Cuenca.

ANEXOS

ANEXO N°01: MATRIZ DE CONCISTENCIA

Objetivo general	Objetivos específicos	Variables		Dimensiones	Indicadores
Optimizar la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco mediante la metodología "ARSI"- Huánuco, 2018.	Gestionar los mecanismos de salvaguardas de la seguridad de la información, en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289, mediante la Metodología ARSI	VARIABLE INDEPENDIENTE	METODOLOGIA MAGERIT	Riesgos	Porcentaje de activos relacionados a la seguridad de la información
					Porcentaje de degradación según el nivel de la caracterización de la amenaza
					Vulnerabilidades reportadas adecuadamente
					Porcentaje de activos según el valor de impacto por dimensión
					Porcentaje de probabilidad de ocurrencia del riesgo por dimensión
	Establecer políticas de seguridad para minimizar los riesgos en la seguridad de la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. 289 – Huánuco, 2018			Políticas de Seguridad	Porcentaje de colaboradores que conocen las políticas de seguridad de la información
					Porcentaje de activos respaldados adecuadamente
					Administración de comunicaciones y operaciones
					Porcentaje de registros fallidos de acceso al sistema
	Monitorear la seguridad de la información de la Cooperativa de Ahorro San Francisco Ltda. 289, mediante la implementación de un software			Software	Portabilidad: Porcentaje de activos que soportan el software
					Eficiencia: Porcentaje de riesgos mitigamos con la implementación del software
					Satisfacción: Porcentaje de usuarios satisfechos
					Funcionabilidad: Porcentaje de necesidades cubiertas
					Usabilidad: Tiempo promedio de aprendizaje del software

ANEXO N°02: VALIDACIÓN DEL MODELO

			CONOCIMIENTO Y EXPERIENCIA				
N°	COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA. 289		Kc	Ka	K	Promedio	
1	Gerente de sistemas	Ing. Fernando Augusto Calderón Juárez	0.8	0.7	0.95	0.82	SE ACEPTA COMO EXPERTO
2	Gerente de riesgos	CPC. Jocelyn Sánchez Herrera	1	1	0.8	0.93	SE ACEPTA COMO EXPERTO
3	Gerente de créditos	CPC. Stella Angulo Jaime	0.9	0.8	0.85	0.85	SE ACEPTA COMO EXPERTO
4	Jefatura de cobranzas	Dr. Judith Martell Yacolca	1	0.9	0.95	0.95	SE ACEPTA COMO EXPERTO
5	Gerente de Administración y finanzas	Adm. Cirilo Esteban Maylle	0.8	0.9	0.85	0.85	SE ACEPTA COMO EXPERTO
6	Auxiliar del área de riesgos	CPC. Yanina Dennise Campos Retiz	1	1	0.65	0.88	SE ACEPTA COMO EXPERTO
7	Jefatura del área de contabilidad	CPC. Mercedes Bermúdez Lombardi	0.95	0.6	0.8	0.78	SE ACEPTA COMO EXPERTO
8	Analista de créditos	Ing. Sandra Clarisa Rumaldo Martel	0.95	0.6	1	0.85	SE ACEPTA COMO EXPERTO
9	Sub gerencia de créditos	Adm. Yovana María Pajuelo Garay	0.75	0.75	0.9	0.80	SE ACEPTA COMO EXPERTO
10	Jefatura de Operaciones	CPC. Omayra Cachay Suarez	0.95	0.95	0.55	0.82	SE ACEPTA COMO EXPERTO
11	Analista de créditos	Ing. Luis Antonio Fuster Quispe	0.8	0.83	0.8	0.81	SE ACEPTA COMO EXPERTO
12	Jefatura de créditos	CPC. Llery Luz Alanya Ollero	0.8	0.95	0.75	0.83	SE ACEPTA COMO EXPERTO

Características		Su características	
Atributo	**Peso**	**Atributo**	**Peso**
Caracterización de Activos	**30**	Identificación de activos	**10**
		Dependencias	**7**
		Valoración	**9**
		Dimensiones	**9**
Evaluación de Amenazas	**20**	Identificación de las amenazas	**10**
		Valoración de las amenazas	**9**
		Determinación del impacto potencial	**9**
		Determinación del riesgo potencial	**9**
Determinación y valoración del daño causado	**15**	Magnitud de la degradación	**7**
		Cálculo del impacto	**8**
Estimación del nivel del riesgo	**15**	Probabilidad de las amenazas	**7**
		Cálculo del riesgo	**8**
Determinación Salvaguardas	**20**	Selección de las salvaguardas	**9**
		Efecto de las salvaguardas	**9**
		Tipo de protección	**9**
		Eficacia de la protección	**8**
		Recomendaciones de control	**9**

		MODELO ARSI												
	EXPERTOS	1	2	7	9	8	6	7	8	9	10	11	12	
		8.25	8.50	8.50	8.25	8.00	8.75	7.75	8.00	8.00	8.50	7.75	8.25	0.73
1.1	Identificación de activos	8.00	9.00	9.00	8.00	8.00	9.00	8.00	8.00	8.00	9.00	8.00	9.00	0.51
1.2	Dependencias	7.00	7.00	7.00	9.00	9.00	9.00	7.00	7.00	7.00	9.00	7.00	7.00	0.98
1.7	Valoración	9.00	9.00	9.00	8.00	7.00	9.00	7.00	9.00	9.00	8.00	7.00	9.00	0.89
1.9	Dimensiones	9.00	9.00	9.00	8.00	8.00	8.00	9.00	8.00	8.00	8.00	9.00	8.00	0.51
		8.50	8.39	8.44	8.50	8.22	8.33	8.33	8.33	8.39	7.83	8.33	8.33	0.72
2.1	Identificación de las amenazas	8.00	8.00	9.00	8.00	9.00	9.00	8.00	9.00	9.00	8.00	9.00	9.00	0.51
2.2	Valoración de las amenazas	9.00	9.00	8.00	9.00	9.00	8.00	8.00	8.00	9.00	9.00	8.00	8.00	0.52
2.7	Determinación del impacto potencial	9.00	9.00	7.00	7.00	8.00	7.00	9.00	9.00	8.00	9.00	7.00	8.00	0.90
2.9	Determinación del riesgo potencial	7.00	8.00	9.00	9.00	7.00	9.00	7.00	7.00	7.00	8.00	9.00	7.00	0.94
		8.50	8.00	8.50	8.50	8.00	8.00	8.50	8.00	8.50	7.50	8.00	9.00	0.66
7.1	Magnitud de la degradación	9.00	8.00	9.00	8.00	9.00	9.00	9.00	9.00	8.00	8.00	9.00	9.00	0.49
7.2	Cálculo del impacto	8.00	8.00	8.00	9.00	7.00	7.00	8.00	7.00	9.00	7.00	7.00	9.00	0.83
		9.00	8.50	8.50	9.00	8.00	9.00	8.50	9.00	8.00	7.00	9.00	8.00	0.73
7.1	Probabilidad de las amenazas	9.00	9.00	9.00	9.00	9.00	9.00	9.00	9.00	9.00	7.00	9.00	8.00	0.62
7.2	Cálculo del riesgo	9.00	8.00	8.00	9.00	7.00	9.00	8.00	9.00	7.00	7.00	9.00	8.00	0.83
		8.60	8.40	8.60	8.40	8.40	8.40	8.60	8.40	8.40	8.60	8.20	8.40	0.68
7.1	Selección de las salvaguardas	9.00	9.00	9.00	7.00	9.00	7.00	9.00	7.00	8.00	8.00	9.00	7.00	0.94
7.2	Efecto de las salvaguardas	9.00	8.00	9.00	8.00	8.00	8.00	8.00	9.00	8.00	9.00	8.00	9.00	0.51
7.2	Tipo de protección	7.00	9.00	7.00	9.00	9.00	9.00	9.00	8.00	9.00	9.00	7.00	9.00	0.90
7.2	Eficacia de la protección	9.00	8.00	9.00	9.00	7.00	9.00	8.00	9.00	8.00	9.00	8.00	8.00	0.67
7.2	Recomendaciones de control	9.00	8.00	9.00	9.00	9.00	9.00	9.00	9.00	9.00	8.00	9.00	9.00	0.39
														0.70

ANEXO N°04: FICHA DE EQUIPOS

San Francisco Ltda. La Única Huanuqueña	**FICHA TECNICA DE COMPUTADORAS COOPAC**

INFORMACIÓN GENERAL Fecha de Actualización: 06/07/2017

COOPERATIVA	"San Francisco" Ltda.
ÁREA Y AGENCIAACTUAL	Cobranza – Huánuco
NOMBRE DE EQUIPO	
CÓDIGO DE EQUIPO	
IP	
MAC	

Agencia: 101= Central

DESCRIPCIÓN DE ACCESORIOS	NOMBRE DE ACCESORIOS
DESTINADO A:	
Mainboard – Placa Base	
Procesador	
Total Memoria RAM	
Total Capacidad Disco Duro	
CPU (Case)	
Monitor	
Estabilizador	
Mouse Tipo/Marca	
Teclado Tipo/Marca	
Lectora CD/DVD	
impresora	
Parlantes (Equipo de sonido)	

HISTORIAL

AREA	IP	MAC	RESPONSABE	FECHA

ANEXO N°05: FICHA DE TRASLADO DE EQUIPOS

San Francisco Ltda. La Única Huanuqueña	**FICHA TÉCNICA DE TRASLADO DE EQUIPO DE CÓMPUTO**	**FICHA TÉCNICA DE TRASLADO N° - 0001**

1. Información del Usuario Anterior

RESPONSABLE ANTERIOR	
ÁREA Y AGENCIA	
NOMBRE DE EQUIPO	
CÓDIGO DE EQUIPO	
IP	
MAC	

2. Información del Usuario Asignado Actualmente

DESTINADO A:	
AREA Y AGENCIA:	
NOMBRE DE EQUIPO	
IP :	
MAC:	
FECHA DE ENTREGA DEL EQUIPO	**16 – 09 - 2016**

3. Información del Hardware Actual, con fecha _____

NONBRE Y TIPO DE ACCESORIO	DESCRIPCION DEL ACCESORIO
Mainboard – Placa Base	
Procesador	
Total Memoria RAM	

Total Capacidad Disco Duro	
CPU (Case)	
Tarjeta de video Dedicada	
Fuente de Poder	
Lectora CD/DVD	

4. Información del Software Instalado Actual, con fecha _____

It	SOFTWARE	TIPO	ULTIMA ACTUALIZACIÓN
1	**Windows 7 SP1 x64bits**	Sistema Operativo	16/09/2016
2	**Microsoft Office 2013**	Aplicativo	16/09/2016
3	**SFI**	Sistema Financiero	16/09/2016
4	**Adobe Reader 11**	Aplicativo	16/09/2016
5	**Winrar 4.0**	Aplicativo	16/09/2016
6	**VNC**	Aplicativo	16/09/2016
7	**ESET NOD32 8**	Antivirus	16/09/2016
8	**Java Jre 6 y 8**	Otro	16/09/2016

- **Tipo : Base Datos / Sistema Operativo / Aplicativo / Otro**

OBSERVACIONES.

Jefatura del área de Promoción y Desarrollo	Usuario Asignado del área de Promoción y Desarrollo	Asistente responsable del área de Sistemas

ANEXO N°06: FICHA DE CREACIÓN DE USUARIOS

San Francisco Ltda. La Única Yuanuqueña	FORMULARIO DE CREACIÓN Y/O DESACTIVACIÓN DE USUARIO SFI "COOPAC SAN FRANCISCO"	Código	FS-FCU-0001	Página 1
		Revisión	0	De 1
	Jefatura de Sistemas	Fecha	03/10/2016	

1.- DATOS DE LA ENTIDAD						
NOMBRE DE LA ENTIDAD						
ABREVIATURA (Si corresponde)		R.U.C.		TELÉFONO		
DOMICILIO LEGAL						
Av./Jr./Calle/Psje. :		Nro.:	Of.:	Int.:	Mza:	Lote:
Urbanización:	Distrito:	Provincia:		Departamento:		

2.- DATOS DEL SOLICITANTE (JEFATURAS, SUBGERENCIAS O GERENCIA GENERAL DE LA INSTITUCIÓN)					
APELLIDOS Y NOMBRES COMPLETOS		CARGO QUE DESEMPEÑA EN LA INSTITUCIÓN		D.N.I	
TELÉFONO/ANEXO:		FAX:		FECHA DE SOLICITUD:	

3.- DATOS DEL NUEVO USUARIO SFI			
APELLIDOS Y NOMBRES COMPLETOS			D.N.I
CARGO O FUNCIÓN QUE DESEMPEÑA	ÁREA	AGENCIA/CÓDIGO	TELÉFONO
USUARIO SFI	CONTRASEÑA POR DEFECTO	FECHA DE ACTIVACIÓN	FECHA DE EXPIRACIÓN

4.- DATOS DE LA PERSONA ENCARGADA A CREAR LOS USUARIOS			
APELLIDOS Y NOMBRES COMPLETOS		CARGO QUE DESEMPEÑA EN LA INSTITUCIÓN	D.N.I
ÁREA	AGENCIA/CÓDIGO	TELÉFONO	CORREO

5.- DATOS DEL USUARIO FUNCIONARIO A DESACTIVAR
APELLIDOS Y NOMBRES COMPLETOS
USUARIO SFI
RAZÓN/MOTIVO DE LA DESACTIVACIÓN

TÉRMINOS DE RESPONSABILIDADES:

El Responsable de la Solicitud para la creación del Usuario SFI:

- Es único autorizado a solicitar la habilitación y cancelación de las cuentas de usuarios del sistema
- Estará obligado comunicar a la Gerencia General y al área de Sistemas, siempre que se sucedan cambios en las cuentas de los usuarios habilitados.

El usuario será el único responsable:

- Por todas las operaciones que queden registradas a consecuencias de las operaciones realizadas con el sistema.
- Por el mantenimiento de la confidencialidad de la contraseña a él concedida, debiendo abstenerse de cederla o divulgarla en todos los casos.
- Por el mantenimiento de la confidencialidad acerca de los datos e información que obtenga del sistema;
- Por desconectarse de la aplicación en uso de forma completa cada vez que se aleje de su puesto de trabajo.

_____	_____	_____
SOLICITANTE DEL USUARIO	**RESPONSABLE DEL USUARIO**	**AUTORIZADOR POR**

ANEXO N°07: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA. 2018.