UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIO DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Sistema de gestión de seguridad de la información basada en la Norma ISO 27001 para la Caja Sullana**.**

Tesis para optar el Título Profesional de Ingeniero en Informática y de Sistemas.

Autores

Tavara Reyes, Crhistian Jhoao

Navarro Chumacero, Maryury Mirella

Asesor

Valle Peláez, Miguel Arturo.

0000-0003-2255-0938

PIURA – PERÚ

2021

Palabras clave

Tema	:	Seguridad de la información.
Especialidad	:	Gestión.

Key words

Topic	:	Security of the Information.
Specialty	:	Management

Línea de investigación - OCDE

Línea	:	Ingeniería de Software
Área	:	Ingeniería y Tecnología
Sub Área	:	Ingeniería Eléctrica, Electrónica e Informática
Disciplina	:	Ingeniería de Sistemas y Comunicaciones

“Sistema de gestión de seguridad de la información basada en la Norma ISO 27001 para la Caja Sullana.”

Resumen

La presente investigación tiene por objetivo el desarrollo de un Sistema de gestión de seguridad de la información basada en la Norma ISO 27001 para la Caja Sullana. en el área de Operaciones.

En el desarrollo de la tesis se utilizó el marco de referencia de la Guía de los fundamentos para la dirección de Proyectos (PMBOK) de la Quinta edición, el cual es un marco de trabajo que contiene el estándar reconocido a nivel mundial y la guía para la profesión de la dirección de proyectos, el cual cuenta con la suficiente flexibilidad para adaptarse a cualquier empresa, pudiendo seleccionar los procesos a aplicar, modo y técnicas concretas, por lo que facilita el periodo de adaptación de nuevas incorporaciones al equipo de trabajo.

Esta iniciática partió de la experiencia de las circunstancias de eventos que desarrollaron ex-trabajadores y compañeros del área, que atentaron contra los controles del Sistema de Seguridad de la información del área de operaciones de la empresa que laboramos.

Se llevó a cabo entrevistas y encuestas al jefe del área de seguridad de la información y al personal del área de operaciones, la interpretación de sus resultados nos sirvió de apoyo para el desarrollo de los controles del ISO 27001:2013.

Concluida la tesis se plantearon las recomendaciones basadas en los objetivos de control de los dominios de la norma ISO 27001: 2013, respecto a lo que se debe implementar para la seguridad de trabajadores y sobre todo de sus clientes, lo cual garantizaría que los riesgos de los activos de información sean identificados, gestionados, minimizados y documentados.

Abstract

This research aims to develop an Information Security Management System based on ISO – International Organization for Standardization 27001 for Caja Sullana entity in the area of operations.

The framework of the guide to the basics of project management (PMBOK) Fifth edition, which is a framework that contains the globally recognized standard and the guide which was used in the development of the thesis and the guide the profession of project management; which, it has sufficient flexibility to adapt to any business and can select the processes to be applied, method and specific techniques for facilitating the adaptation period of new inclusions to the teamwork.

This initiation was based on the experience of the circumstances of events that developed ex-workers and partners in the area, who attacked the controls from area of operations of the Information Security System of the company where we work.

It conducted interviews and surveys to information security chief and to operations personnel, the interpretation of the results helped us to develop the controls ISO 27001: 2013.
Completed the thesis, the recommendations were based on control objectives of the domains of the ISO 27001:2013,in relation on what must be implemented for the safety of workers and especially their customers, which would ensure that the risks of information assets are identified, managed, minimized and documented.

Índice

Palabras claves ..... **i**

Resumen ..... **iii**

Abstract ..... **iv**

Introducción **1**

Metodología **20**

Resultados **70**

Análisis y discusión **79**

Conclusiones y recomendaciones **81**

Referencias bibliográficas **83**

Apéndices y anexos **86**

Introducción

En el estudio se han considerado los trabajos relevantes que guardan relación con esta investigación:

Montoya Pachas, N. K. (2012), En lima se presentó la tesis "Diseño de un sistemade gestión de seguridad de información para un centro cultural binacional", su propósito fue proteger los activos de la información ante las amenazas a las cuales estánexpuestas, y de esta manera dar un tratamiento a los riesgos de información en los procesos de la institución , este proyecto se realizó siguiendo lo propuesto en la Norma ISO/IEC 27001:2005 para elaborar el diseño de un SGSI donde se establezcan una política , objetivos , procesos y procedimientos ,concluyendo así que el Centro Cultural , y las organizaciones en general deben tomar en cuenta la seguridad de la información de la empresa y de esa forma proteger su activo más valioso que es la información.

La presente investigación nos brindó de apoyo en la consideración del diseño del Sistema de Gestión de Seguridad de la Información el cuál se basó bajo la misma Norma ISO 27001 de nuestra investigación, por lo que les permitió gestionar la seguridad de sus activos con el objetivo de darles un tratamiento adecuado.

Villena Aguilar, M. A. (2006), En Lima se presentó la tesis "Sistema de gestión de seguridad de información para una institución financiera*",* el objetivo de esta tesis fue establecer los principales lineamientos de manera exitosa, un adecuado modelo de sistema de gestión de la información (SGSI) en una institución financiera del Perú, el cual apuntó a asegurar que la tecnología de información usada estaba alineada con la estrategia de negocio y que los activos de información tenían el nivel de protección acorde con el valor y riesgo que representaba para la organización, utilizando como referencia el modelo de seguridad de información de Mc Cumber, por ser uno de los más influyentes, dado que abarca los principales estados de la información, características y medidas de seguridad y así se implanto una adecuada gestión de seguridad de la información en una institución financiera.

Debido a que la siguiente investigación desarrolla un sistema de Gestión de Seguridad de la Información y va dirigida específicamente a una entidad financiera fue el motivo

de su selección brindándonos el soporte en relación a los 3 pilares en la seguridad de la información como son la; confidencialidad, integridad y disponibilidad de sus activos de información.

De la Cruz Guerrero, C. W. (2009),en Chiclayo se presentó la tesis "Elaboración y Aplicación de un Sistema de gestión de la Seguridad de La Información (SGSI) para la realidad tecnológica de la USAT", su propósito fue garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados; de esta manera se buscó proteger la información de un amplio rango de amenazas para mejorar la seguridad de las tecnologías de información y las comunicaciones en la Universidad Católica Santo Toribio de Mogrovejo, utilizando el modelo PDCA (Metodología análisis de riesgos COBIT – Metodología análisis de riesgosMAGERIT), concluyó que se recomienda capacitar a los Alumnos como a Docentes y/o administrativos de manera que se conozca un poco más acerca del tema deseguridad de la información, con la finalidad de minimizar los inconvenientes que se muestran, pero no solo son los usuarios quienes debían recibir dicha capacitación, debía ser difundida desde las áreas que se encuentran directamente comprometidas conel tema, con la finalidad de mejorar en algún aspectos en los que se flaquea y/o desconoce.
La presente investigación nos brindó apoyo en relación de su marco teórico la cual destaca la base de sus antecedentes con investigaciones en Sistemas de Gestión de la Información, además de su análisis en riesgos y del apoyo en la elaboración de las encuestas.

Barragán, I., Góngora I., & Martínez, E. (2013), En Guayaquil se presentó la tesis "Implementación de políticas de seguridad informática para la M.I. municipalidad de Guayaquil aplicando la norma ISO/IEC 27002",su objetivo fue formular un modelo de política de seguridad de la información que sirva de punto de partida para la elaboración de políticas correspondientes tomando como base estándares internacionales, se decidió basar el modelo en la norma ISO/IEC 27002 , como un marco de referencias para la gestión de la seguridad de la información , concluyendo que la forma de conseguir el mayor beneficio en seguridad de la información es contar con una

adecuada evaluación de riesgos, que oriente las inversiones, que minimicen el impacto en caso de incidentes , dando a conocer que la seguridad de la información no es una responsabilidad únicamente del área de tecnología , debe fluir desde la alta gerencia hacia todos los procesos de negocios.

La presente tesis nos apoyó en el alcance del objetivo de sus políticas generales en relación a la consideración de los accesos de los usuarios y de las condiciones del uso de las claves de acceso.

Aguirre Cardona, J. D., & Aristizabal Betancourt, C. (2013), en Pereira se presentó la tesis "Diseño del sistema de gestión de seguridad de la información para el Grupo Empresarial La Ofrenda", su propósito fue diseñar el sistema de gestión de seguridad de la información para el grupo Empresarial La ofrenda ya que dicha organización no contaba con un SGSI, para así poder determinar los riegos que se presentan con la información que se maneja en la empresa, utilizando herramientas tecnológicas y de desarrollo que permitan la gestión de los procesos que avalen la SI, aplicar los controles de la Norma ISO 27001 que permitan administrar el funcionamiento de un sistema de detección de intrusos dentro de un SGSI, se aplicó el modelo COBIT que se basa en un conjunto de herramientas de soporte del gobierno TI que les permitió a los gerentes cubrir la brecha entre los requerimientos de control , los aspectos técnicos y riesgos del negocio, concluyo que actualmente se vive en una época en que la información y los datos poseen una importancia decisiva en la gran mayoría de las organizaciones, convirtiéndose así en su activo más importante, se debe tener en cuenta que hay que recalcar que de nada sirve contar con un SGSI, que consideren todos los posibles riesgos y controles para mitigarlos o contar con toda la tecnología posible para asegurar la información de la compañía si no se da una debida importancia a la seguridad de la información por parte de la alta gerencia y no se cumplen las políticasy procedimientos establecidos por parte del personal de la empresa.

La presente investigación nos sirvió como orientación en el diseño del Sistema de Gestión de Seguridad de la Información; el cual considera a la Norma ISO 2001:2005 para salvaguardar la Información.

EL Sistema de Gestión de Seguridad de la información basada en el ISO 27001:2013 permite a Caja Sullana dar fiel cumplimiento a la Norma según la exigencia de la Superintendencia de Banca y Seguros, garantizar los activos de información de la empresa, minimizar y documentar los riesgos o eventos que atenten en contra de la seguridad de la Información de la empresa y además brindar el respaldo y seguridad de la información y de los activos de sus clientes.
El ISO 27001:2013, permite el desarrollo de la gestión de los activos de información de la institución, lo cual destaca la evolución de la gestión de sus activos a un nivel de servicio de calidad, siendo funcional, de fácil uso y auditable en todos sus dominios por lo que minimiza los costos a la organización por su adaptabilidad y mejora.

La empresa diariamente genera diferentes activos de información el cual sólo debe de ser de importancia para quien es destinada o usada. Estos activos de información son almacenados o custodiados por diferentes medios, ya sea físico o electrónico.
Considerando que esta información esté disponible para diferentes usuarios e interacciones, ya sea para la toma de decisiones, realización de reportes, inventarios, planeamientos, estadísticas y operaciones, sin embargo; ¿Qué sucede si los activos de información no son utilizados según su objetivo y son usados para otros fines no autorizados y malintencionados? ¿Qué medidas asumir si nuestros usuarios son ajenos a las políticas de la institución?

La experiencia ante ciertas eventualidades trascendentales que atentaron en contra de la seguridad de la información, involucradas a esta área y del respaldo del desarrollo de las encuestas al personal de operaciones es porque nació el motivo al desarrollo de esta investigación.
El área de operaciones no cuenta con los controles necesarios en seguridad de información y ello se manifiesta en los eventos ocurridos.

El uso, cambio, incremento o traslados de los perfiles de los usuarios y sus niveles de acceso al sistema son interacciones del día a día, sin embargo, muchos de los perfiles

o accesos que solían ser solicitados temporalmente permanecían por un periodo indeterminado sin autorización.
Existen usuarios a los cuales a sus perfiles se les otorga ciertas claves o passwords a lo que permiten validar o aprobar determinadas operaciones según procedimiento; sin embargo, la ausencia de control y el uso malintencionado e irresponsable de estos accesos jugaban un papel en contra del sistema de gestión de seguridad de la información de Caja Sullana y sobre todo de los riesgos y amenazas que conlleva.

Según la determinación de la SBS los documentos resultados de operaciones de los clientes son guardados en custodia por varios años, cabe a mencionar según el proceso de custodia de la garantía prendaria generado de la venta de un lote adjudicado se procede a custodiar dicho documento después de haberse entregado al cliente su garantía pignoraticia. Su tiempo de custodia es de 10 años; sin embargo sucedía que el cliente solicitaba la verificación de dicho documento, o se traspapelaba o perdía, ello generaba una inadecuada gestión ya que obligaba a la búsqueda física y no inmediata del mismo, generando malestar ante una posible consulta o reclamo ya sea del cliente o del mismo personal de caja Sullana, es por ello que se consideró la existencia de un medio informático que alivie o minimice los riesgos mencionados líneas atrás y evite el riesgo reputacional en contra de la entidad.

Por lo antes expuesto surge la necesidad de desarrollar la mejora e implementación de los puntos débiles de los controles del Sistema de Gestión de Seguridad de la Información basada en la Norma ISO 27001 para el área de operaciones de la Caja Sullana; Entonces nos planteamos la siguiente interrogante: ¿Cómo desarrollar un sistema de gestión de seguridad de la información basada en el ISO 27001- 2013 para la Caja Sullana en el área de Operaciones?

A fin de describir la esencia y características de la variable de estudio se ha conceptualizado y operacionalizado, de la siguiente manera:

Activo de Información

Los activos de información son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad, los cuales son necesarios para que la organización funcione y alcance los objetivos que propone su dirección. (Aguirre, 2014)

Los activos de información se pueden clasificar en las siguientes categorías:

- ✓ Activos de información (Datos, manuales del usuario)
- ✓ Documentos de papel (contratos)
- ✓ Activos de software (aplicación, software de sistemas)
- ✓ Personal (clientes, trabajadores)
- ✓ Imagen de la empresa y reputación
- ✓ Servicios (comunicaciones)

Seguridad de Información

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información.

Está caracterizada por la preservación de los siguientes aspectos *(Villena, 2006)*

- ✓ **Confidencialidad:** Asegurando que la información seas accesible solo por aquellos que están autorizados.
- ✓ **Integridad:** Salvaguardando la exactitud de la información en su procesamiento, así como su modificación autorizada.
- ✓ **Disponibilidad:** asegurando que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando sea requerido.

Figura 1. Pilares de Seguridad de la Información

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos saber que puede ser confidencial. Puede ser divulgada, mal utilizada, robada, borrada, saboteada, etc. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, esta se clasifica como:

- ✓ **Critica**: Es indispensable para la operación de la empresa.
- ✓ **Valiosa**: Es un activo de la empresa y muy valioso.
- ✓ **Sensible**: Debe ser conocida por las personas autorizadas.

Sistema de Gestión de Seguridad de Información (SGSI)

Es una forma sistemática de administrar la información sensible de una institución, para que permanezca segura. Abarca a las personas, los procesos y las tecnologías de información. La forma total de la Seguridad de la Información, y la integración de diferentes iniciativas de seguridad necesitan ser administradas para que cada elemento sea completamente efectivo. Aquí es donde entra el Sistema de Gestión de Seguridad de la Información que permite coordinar esfuerzos de seguridad con mayor efectividad *(Villena ,2006)*

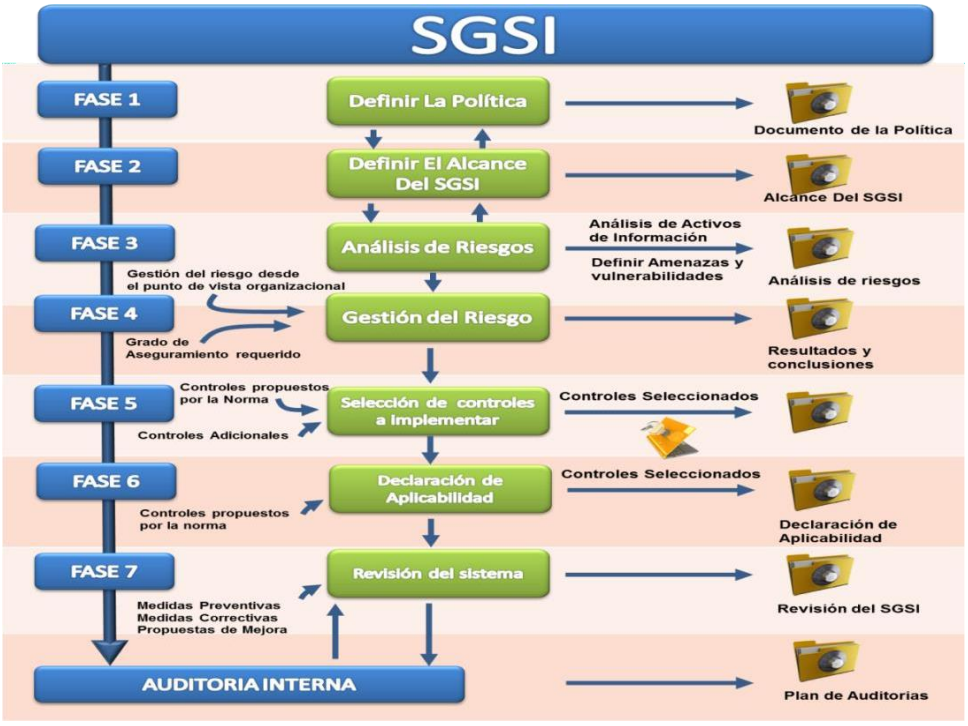


Figura 2. Sistema de Gestión de Seguridad de la Información

Para qué sirve un Sistema de Gestión de seguridad de la Información

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Figura 3. Riesgos – SGSI

Definición del riesgo

Estimación de 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 puede que 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.

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de causalidad y probabilidad de ocurrencia.

Figura 4. Elementos del riesgo

- **Identificar los riesgos**
  - ✓ Identificar todos aquellos activos de información que tienen algún valor para la organización que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.
  - ✓ Identificar las amenazas relevantes asociadas a los activos identificados.
  - ✓ Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.

- ✓ Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

- **Análisis del Riesgo**

  Para analizar el riesgo se debe establecer la probabilidad de ocurrencia del mismo, así como sus consecuencias, esto finalmente orientará a la clasificación del riesgo. Esta fase depende de la información obtenida en la etapa de identificación. Existen dos aspectos principales que determinarán el análisis de riesgo:

  - ✓ **Probabilidad:** posibilidad de ocurrencia del riesgo, la cual se puede medir con criterios de frecuencia.
  - ✓ **Impacto:** consecuencias que pueden ocasionar la materialización del riesgo en la organización

- **Evaluación del riesgo**

  La evaluación involucra comparar niveles de riesgo con criterios definidos en el contexto. El objetivo de esta evaluación es la de identificar y evaluar los riesgos, los cuales son calculados por una combinación de valores de activos y niveles de requerimiento de seguridad. Con base en esta comparación, se puede considerar la necesidad de tratamiento; además las decisiones se deben tomar de acuerdo con los requisitos legales, reglamentarios y otros.

  La evaluación de riesgos también puede tener como resultado la decisión de no tratar el riesgo de ninguna manera diferente de los controles existentes.

- **Tratamiento del riesgo**

  El tratamiento del riesgo se define como el conjunto de decisiones tomadas con cada activo de información.

  Las decisiones para tratar el riesgo pueden incluir las siguientes opciones:

  Evitar el riesgo: La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión

comercial del negocio, se modifican, para así poder evitar la ocurrencia del riesgo. Las maneras tradicionales para implementar esta opción son:

- ✓ Dejar de conducir ciertas actividades.
- ✓ Desplazar activos de información de un área riesgosa a otra.
- ✓ Decidir no procesar cierto tipo de información y no se consigue la protección adecuada.

La decisión por la opción de "evitar el riesgo" debe ser balanceada contra las necesidades financieras y comerciales de la empresa.

Aceptar el riesgo cuando no es posible mitigarlo y se debe continuar la actividad que lo originó.

- ✓ En muchas ocasiones a la empresa se le presentan circunstancias donde no se pueden encontrar controles ni tampoco es factible diseñarlos o el costo de implantar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.
- ✓ Cuando la situación se presenta donde es muy costoso para la empresa mitigar el riesgo a través de los controles o las consecuencias del riesgo son devastadoras para la organización, se deben visualizar las opciones de "transferencia de riesgo" o la de "evitar el riesgo".

Reducir el riesgo

Para los riesgos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente indefinidos por la empresa. Los controles deben obtenerse del anexo "A" del ISO 270001:2013. Al identificar el nivel de los controles es importante considerar los requerimientos de seguridad relacionados con el riesgo, así como la vulnerabilidad y las amenazas previamente identificadas.

Los controles pueden reducir los riesgos valorados en varias maneras:

- ✓ Reduciendo la posibilidad que la vulnerabilidad sea explotada por las amenazas.
- ✓ Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionado y recuperándose de ellos.

Transferir el riesgo fuera del apetito de riesgo, el riesgo se comparte con una o varias partes, pueden ser agentes externos.

Figura 5. Gestión de Riesgos

Controles

Son las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza de que se alcanzarán los objetivos del negocio.

Existen varias formas de establecer controles sobre riesgos organizacionales. La siguiente es:

- ✓ Disuasivos: su presencia disuade de la comisión de acciones en contra de alguna política o procedimiento establecido y considerado correcto. Por ejemplo: cámaras de vigilancia.

- ✓ Preventivos: detectan problemas antes que ocurran por medio de monitoreo constante. Por ejemplo: políticas de contratación.
- ✓ Detectivos: detectan y reportan los problemas suscitados por errores u omisiones, en el momento en que éstos ocurren. Por ejemplo: Uso de antivirus.
- ✓ Correctivos: minimizan el impacto de una amenaza ya consumada. Por ejemplo: Planes de contingencia. Propios de cada área administrativa y operativa de las organizaciones. (Espinoza, 2013)

Circular G140-2009-SBS

La circular G-140-2009-SBS, elaborada en abril del 2009 por la Superintendencia de Banca y Seguros, obliga a las entidades financieras que son reguladas por este organismo a establecer, mantener y documentar un Sistema de Gestión de Seguridad de la Información (SGSI) tomando como referencia la ISO 17799 e ISO 27001. El objetivo de implementar el SGSI es de brindar seguridad a los activos de información más importantes como resultado del análisis de riesgo y sobre todo cumpliendo con las expectativas de todos los interesados del sistema, clientes, comunidad, estado, proveedores, y la misma entidad financiera entre otros. (Superintendencia de Banca, Seguros Y AFP, 2009)

PMBOK (Quinta versión)

La Guía del PMBOK es el estándar, reconocido a nivel global y la guía para la Administración de Proyectos y cuyas siglas significan en inglés Project Management Body of Knowledge (el Compendio del Saber de la Gestión de Proyectos en español). Es un estándar reconocido internacionalmente (IEEE Std 1490-2003) que provee los fundamentos de la gestión de proyectos que son aplicables a un amplio rango de proyectos, incluyendo construcción, software, ingeniería, etc.

PMBOK reconoce 5 grupos de procesos básicos y 10 áreas de conocimiento comunes a casi todos los proyectos.

Los procesos se trasladan e interactúan a través de un proyecto o fase. Los procesos son descritos en términos de: Entradas (documentos, planes, diseños, etc.), herramientas y Técnicas (mecanismos aplicados a las entradas) y Salidas (documentos, productos, etc.).

Tabla 1

Resumen de los 5 procesos de la dirección de proyectos y las diez áreas de conocimientos.

Área de Conocimiento	Grupos de Procesos de Gestión de Proyectos				
	Procesos de Iniciación	**Procesos de Planificación**	**Procesos de Ejecución**	**Procesos de Motorización y Control**	**Procesos de Cierre**
Gestión de la Integración del Proyecto (1)	Desarrollar el Acta de Constitución del Proyecto (1.1)	Desarrollar el Plan de Gestión del Proyecto (1.2)	Dirigir y Gestionar la Ejecución del Proyecto (1.3)	Supervisar y Controlar el Trabajo del Proyecto (1.4) Control Integrado de Cambios (1.5)	Cerrar Proyecto (1.6)
Gestión del Alcance del Proyecto (2)		Planificar la Gestión del Alcance (2.1) Identificar los Requisitos (2.2) Definir el Alcance (2.3) Crear EDT (2.4)		Validar el Alcance (2.5) Controlar el Alcance (2.6)	
Gestión del Tiempo del Proyecto (3)		Planificar la Gestión del Cronograma (3.1) Definir las Actividades(3.2) Establecimiento de la Secuenciar las Actividades (3.3) Estimar los Recursos de Actividades (3.4) Estimar la Duración de Actividades (3.5) Desarrollar el Cronograma (3.6)		Controlar el Cronograma (3.7)	

Gestión de los Costes del Proyecto (4)		Planificar la Gestión de Costes (4.1) Estimar Costes (4.2) Definir el Presupuesto (4.3)		Control de Costes (4.4)	
Gestión de la Calidad del Proyecto (5)		Planificar la Gestión de Calidad (5.1)	Realizar Aseguramiento de Calidad (5.2	Controlar la Calidad (5.3)	
Gestión de los Recursos Humanos del Proyecto (6)		Planificar la Gestión de Recursos Humanos (6.1)	Adquirir el Equipo del Proyecto (6.2) Desarrollar el Equipo del Proyecto (6.3) Gestionar el Equipo del Proyecto (6.4)		
Gestión de las Comunicaciones del Proyecto (7)		Planificar las Comunicaciones (7.1)	Gestionar las Comunicaciones (7.2)	Controlar las Comunicaciones (7.3)	
Gestión de los Riesgos del Proyecto (8)		Planificar la Gestión de Riesgos (8.1) Identificar los Riesgos (8.2) Realizar el Análisis Cualitativo de Riesgos (8.3) Realizar el Análisis Cuantitativo de Riesgos (8.4) Planificar la Respuesta a los riesgos (8.5)		Controlar los Riesgos (8.6)	
Gestión de las Adquisiciones del Proyecto (9)		Planificar las Adquisiciones (9.1)	Realizar las Adquisiciones (9.2)	Controlar las Adquisiciones (9.3)	Cerrar las Adquisiciones (9.4)
Gestión de los Grupos de Interés del Proyecto (10)	Identificar a los Grupos de Interés (10.1)	Planificar la Gestión de los Grupos de Interés (10.2)	Gestionar los Grupos de Interés (10.3)	Controlar los Grupos de Interés (10.4)	

International Organization for Standardization (ISO)

ISO, sus siglas en inglés proviene de los términos (International Standarization Organization) la cual es una entidad internacional que se encarga de la normalización a nivel mundial, las cuales desarrollan bajo diferentes grupos o comités especializados las normativas, modelos o patrones a seguir con el objetivo de definir ciertas características que debe poseer un objeto o producto. Su finalidad es orientar, coordinar, simplificar y unificar los usos para conseguir menores costes y efectividad.

ISO 27001: 2013

El ISO/ IEC 27001: 2013, es un modelo de gestión de seguridad de la información, el cual se define como un conjunto de lineamientos el cual especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Estos requisitos describen cual es el comportamiento esperado del sistema de Gestión una vez que esté en funcionamiento; por lo tanto para el desarrollo del proyecto se tomó a la Norma ISO 27001:2013 como marco de referencia en la implementación del Sistema de Gestión de Seguridad de la información.

Evolución de la Estructura ISO 27001:2013

Figura 6. (Fuente Presentación Manuel Collazos)

La ISO 27001:2013 cuenta con 114 controles, 14 Dominios de Seguridad y 130 Requisitos de Gestión.

Los dominios del ISO 27001.

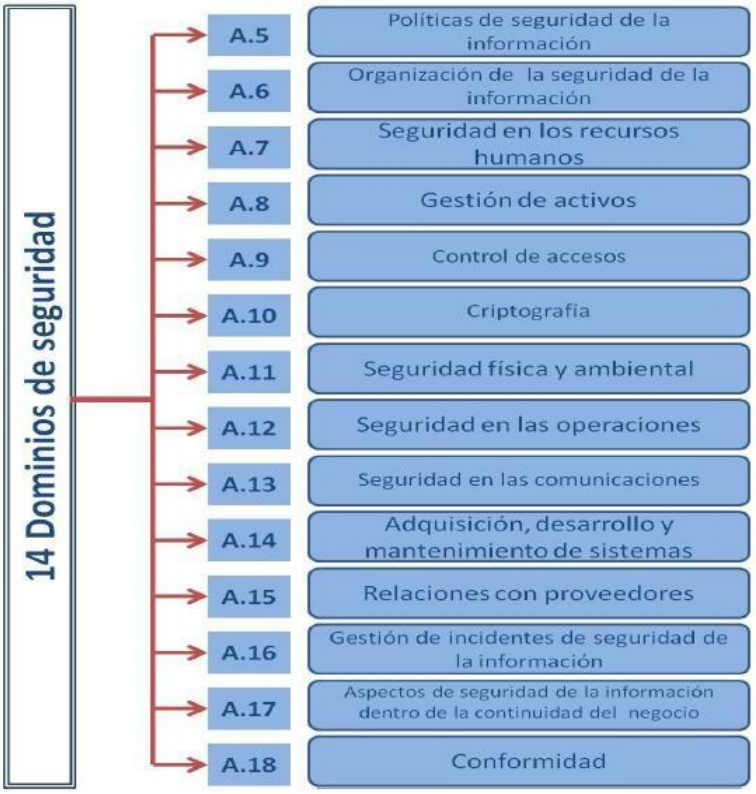


Figura 7. Dominios de Seguridad de la Información

En vista de que la investigación tiene un alcance de carácter Descriptivo, no fue posible plantear una hipótesis debido a que no se intentó correlacionar o explicar casualidad de variables, debido a ello es que la hipótesis es Implícita.

El objetivo general de la investigación es: Desarrollar un Sistema de gestión de seguridad de la información basada en la norma iso 27001-2013; en la Caja Sullana para el área de Operaciones. Como objetivos especifico: Analizar y Diagnosticar la situación actual del área de operaciones de Caja Sullana considerando los antecedentes de violación de los controles del sistema de Gestión de Seguridad de la Información, desarrollar la guía de las buenas prácticas para la Gestión de proyectos PMBOK, el cual permite el obtener los entregables tales como; el Acta de Constitución del proyecto y la EDT (Estructura Desagregada de Trabajo), documentos fundamentales en la formalización e inicio del proyecto y desarrollar la guía de buenas prácticas de la Norma ISO 27001:2013 del sistema de Gestión de

Seguridad de la Información para Caja Sullana, así como seleccionar los controles de Seguridad de Información para el apoyo de salvaguardar los activos de información de Caja Sullana.

Metodología

La investigación se enmarca en una orientación aplicada, considerando que se trata de dar una solución practica a la entidad financiera. Así mismo, respecto al nivel de investigación es un estudio descriptivo. Por otra parte, en lo concerniente al diseño de la investigación, considerando la toma de datos mediante la técnicas e instrumentos, es no experimental

Tabla 2.

Técnicas e instrumentos empleados para el presente informe de investigación fueron:

TECNICA / METODO	JUSTIFICACION	INSTRUMENTO	APLICACIÓN
Entrevista Presencial	Basándonos en la información obtenida de las entrevistas al personal de seguridad, ello nos permitió conocer de la situación actual de los procesos y determinar la deficiencia de los mismos.	Guía de entrevista a personal especializado.	Jefe del área de Seguridad Corporativa
Encuestas	Permite conocer las expectativas que tienen los usuarios respecto al sistema y necesidades de Información de los usuarios y conocimiento de las consideraciones en seguridad de la información	Cuestionario de preguntas (De tipo cerradas de elección única, tanto dicotómica y politómica.).	Trabajadores del área de Operaciones

Tabla 3. Acta de Constitución del Proyecto

ACTA DE CONSTITUCIÓN DEL PROYECTO CÓDIGO 001 versión 1					
Proyecto	Sistema de gestión de seguridad de la información basada en la norma ISO 27001 para la Caja Sullana.				
Patrocinador	Gerencia Central				
Preparado por:	Crhistian Jhoao Távara Reyes. Maryury Mirella Navarro Chumacero.	fecha	26	04	2015
Revisado por:		fecha	28	11	2015
Aprobado por:	Gerencia Central	fecha	03	12	2015

Revisión (correlativo)	Descripción (realizada por) (motivo de la revisión y entre paréntesis quien la realizó)	fecha (de la revisión)
01		
02		

Breve descripción del producto o servicio del proyecto (características, funcionalidades, soporte entre otros)

El proyecto se implementa en al marco de la Circular G 140.2009, la que define la obligatoriedad de la implementación del Sistema de gestión de seguridad de la información en ciertas entidadesfinancieras del Estado Peruano por mandato de la SBS (Superintendencia de Banca y Seguros).

El producto del proyecto "Sistema de gestión de seguridad de la información basada en la norma ISO 27001 para la Caja Sullana", permitirá proteger los activos de información de la institución, usuarios y clientes, permitiendo de esta forma la justificación del cumplimiento de los objetivos para la institución y la reducción de los riesgos de seguridad de la información mediante el empleo de controles.

Se identifica en los siguientes entregables:

- Política de Seguridad
- Inventario de Activos

- Análisis de Riesgo
- Gestión de Riesgos
- Plan de Tratamiento de Riesgo
- Declaración de Aplicabilidad

Tabla 4. Alineamiento del Proyecto.

ALINEAMIENTO DEL PROYECTO	
1. OBJETIVOS ESTRATÉGICOS DE LA ORGANIZACIÓN (A qué objetivo estratégico se alinea el proyecto.)	**2. PROPÓSITO DEL PROYECTO** (Beneficios que tendrá la organización una vez que el producto del proyecto esté operativo o sea entregado.)
Mantener y garantizar la confidencialidad de los activos de Información de Caja Sullana, así como también el acceso controlado e integridad de la información; estableciendo los controles para identificar y mitigar los riegos operativos, informáticos, financieros y de los colaboradores basados en la norma ISO 27001:2013.	Contar con un Sistema de Gestión de la Información documentado, garantizando la seguridad de susactivos de información del área operativa, minimizando las faltas o violación a sus políticas de seguridad por parte de sus usuarios.
3. OBJETIVOS DEL PROYECTO (Principalmente en términos de costo, tiempo, alcance, calidad)	
• Alcance: El proyecto contempla la implementación de un SGSI en el área de Operaciones de la Caja Sullana. • Tiempo: El proyecto debe culminar en un plazo máximo de 8 meses • Costo : El presupuesto contempla un costo máximo S/. 36, 800 Nuevos Soles, que incluye la consultoría. • Calidad: Contar con personal capacitado y especializado en Seguridad de la información y Gestión de Proyectos.	
4. FACTORES CRÍTICOS DE ÉXITO DEL PROYECTO (Componentes o características que deben cumplirse en el proyecto para considerarlo exitoso.)	
• Asignación del recurso humano calificado y experimentado en proyectos similares a tiempo completo por parte Caja Sullana. • Adecuada comunicación de todas las partes involucradas en el proyecto. • Aceptación de los resultados del proyecto por parte del personal de la empresa. • Entrega de documentos en los plazos establecidos.	
5. REQUISITOS DE ALTO NIVEL (Condiciones o características que deben cumplirse para satisfacer lo solicitado al proyecto)	
• Cumplimiento con la Norma ISO 27001:2013, según exige la SBS, personal capacitado y con experiencia en el desarrollo o implementación de proyectos en Seguridad de la información.	

- Documento del Inventario de Activos de Información de caja Sullana, contar con las herramientas necesarias para su desarrollo.
- Documento de la Política de seguridad de la Información.
- Documento entrevistas a Experto y usuarios.
- Documento de la Declaratoria de Aplicabilidad del proyecto.
- Personal con Experiencia.

Tabla 5. Extension y Alcance del proyecto.

EXTENSIÓN Y ALCANCE DEL PROYECTO	
6. FASES DEL PROYECTO (Agrupamiento lógico de actividades relacionadas que usualmente culminan elaborando un entregable principal)	**7. PRINCIPALES ENTREGABLES** (Un único y verificable producto, resultado o capacidad de realizar un servicio que debe ser elaborado para completar un proceso, una fase o un proyecto)
El Proyecto consta de las fases las cuales se alinean en la metodología del ISO 27001. Inicio	• Acta de Constitución del Proyecto. • Introducción a la Norma ISO 27001:2013. • Objetivos del SGSI.

Planificación	• Descripción de la Empresa.
	• Objetivos del Negocio.
	• Situación Actual de la empresa.
	  ▪ Infraestructura de Seguridad de la Información.
	  ▪ Alcance.
	• Definición de la Política de Seguridad de la Información.
	  ▪ Objetivos.
	  ▪ Alcance.
	  ▪ Dominios de la ISO 27001 :2013
	  o Política de seguridad de la Información.
	  o Organización de la Seguridad de la Información.
	  o Seguridad de los Recursos Humanos.
	  o Gestión de Activos.
	  o Control de Accesos.
	  o Criptografía.

	○ Seguridad Física y del Entorno. ○ Seguridad de las Operaciones. ○ Seguridad de la Comunicaciones. ○ Adquisición, desarrollo y mantenimiento de sistemas. ○ Relación con los Proveedores. ○ Gestión de los Incidentes de Seguridad de la Información. ○ Aspectos de seguridad de la información de la gestión de continuidad del negocio. ○ Cumplimiento.
Ejecución	• Análisis de Riesgo ▪ Procesos del Negocio. ▪ Inventario de Activos. ▪ Valoración de Activos. ▪ Identificación de Amenazas. ▪ Valoración de Riesgo por Activo. ▪ Tratamiento del Riesgo.
Seguimiento y Control	• Declaratoria de Aplicabilidad.
Cierre	• Informe Final.

8. INTERESADOS CLAVE

- Junta General de Accionistas.
- Directorio.
- Gerencia Central.
- Gerencia de Riesgos.
- Unidad de Cumplimiento Normativo.
- Unidad de Prevención de Lavado de Activos.
- Gerencia de Riesgos.
- Asesoría Legal.
- Imagen Corporativa.
- Gestión de Desarrollo Humano.
- Unidad de la Tecnología de Información.
- Operaciones.
- Seguridad Corporativa.
- Unidad de Negocios Empresa.
- Unidad de Negocios Personas.
- Unidad de Negocios Servicios.
- Finanzas.
- Tesorería.
- Caja General.
- Contabilidad.
- Personal de la Empresa.
- Clientes.

9. RIESGOS

(Evento o condición incierta que, si ocurriese, tiene un efecto positivo o negativo sobre los objetivos del proyecto).

- Escaso compromiso con el personal involucrado en el proyecto.
- Demora en las fases del proyecto.
- Retraso en el financiamiento del proyecto.
- Incumplimiento de plazos en la entrega de los resultados.
- Falta de equipo humano.
- No contar con personal calificado.

10. HITOS PRINCIPALES DEL PROYECTO

(Un evento significativo para el proyecto)

- Aprobación de proyecto por la Gerencia Central.
- Desarrollo de entrevistas con usuarios y expertos.
- La verificación de los procesos se desarrolle en el plazo pactado.
- Proceso de Inventarios de Activos.
- La entrega del producto debe ser menor o igual al tiempo estimado.

11. PRESUPUESTO DEL PROYECTO
(Áreas de la organización que tienen algo que aportar al proyecto o que se ven afectadas por su ejecución o su producto)

El costo del proyecto es asumido en un 100% por la entidad financiera Caja Sullana.

12. REQUISITOS DE APROBACIÓN DEL PROYECTO
(Quién evalúa los FCE, decide el éxito del proyecto y quien cierra el proyecto)

FCE (Ver punto 4)	Evaluador (Nombres apellidos y cargo de la persona asignada)	Firma el Cierre del Proyecto (Nombres apellidos y cargo de la persona asignada)
• Asignación del recurso humano competente en el desarrollo de proyectos de automatización de ERP.	Jefe de Recursos Humanos.	Gerencia Central.
• Las áreas o personal involucrado debe de estar a disposición y responder con eficiencia para el desarrollo del proyecto.	Responsables de áreas.	
• Aceptación del producto del proyecto por parte del área de Operaciones.	Supervisor de Operaciones.	

• Entrega de documentos en los plazos establecidos.	Gerente del Proyecto. Maryury Mirella Navarro Chumacero.

13. GERENTE DE PROYECTO ASIGNADO AL PROYECTO

(Nombres apellidos y cargo de la persona asignada como gerente del proyecto)

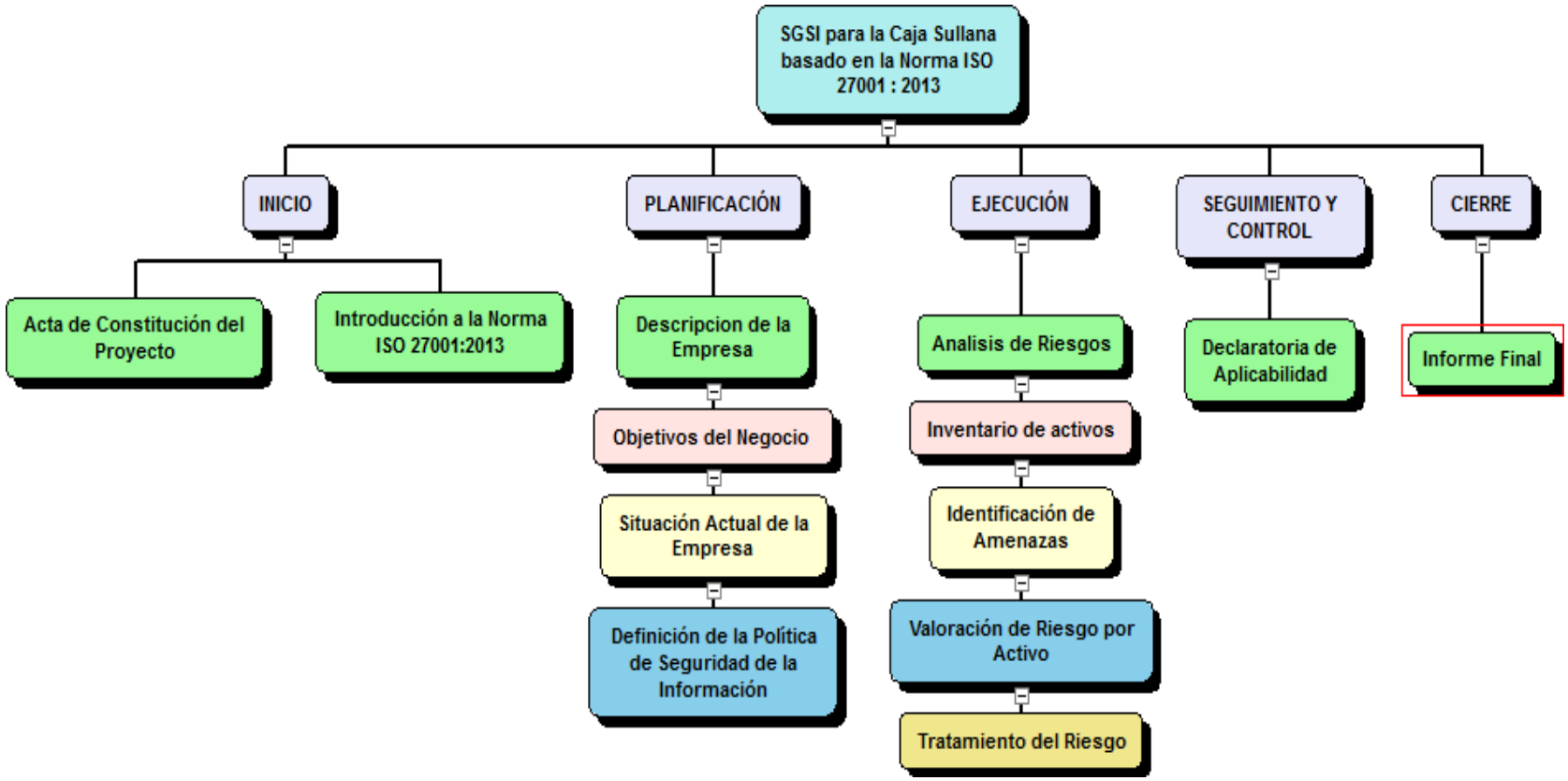
Crhistian Jhoao Távara Reyes. / Gerente de Proyecto.

14. AUTORIDAD ASIGNADA

(Autoridad asignada al gerente del proyecto para el uso de recursos.)

Jefe de Contabilidad.

Figura 8. Estructura detallada de trabajo (EDT)



Diseño metodológico de la Norma ISO 27001:2013

La investigación se basa en el desarrollo de la Norma Internacional ISO 27001:2013, es por ello que se presenta los siguientes alcances;

Para la consideración del proyecto se realizará las siguientes fases:

Fase I: Norma ISO 27001: 2013

Se considera:

- Introducción a la Norma ISO 27001:2013
- Objetivos del SGSI.

Fase II: Análisis de la Empresa

Se considera:

- Descripción de la Empresa.
- Objetivos del Negocio
  - Infraestructura de Seguridad de la Información
  - Alcance
- Definición de la Política de Seguridad de la Información.
  - Objetivos
  - Alcance
- Dominios de la ISO 27001:2013

  - Política de seguridad de la Información
  - Organización de la Seguridad de la Información.
  - Seguridad en los Recursos Humanos.
  - Gestión de Activos
  - Control de Accesos
  - Criptografía
  - Seguridad Física y del entorno
  - Seguridad en las Operaciones
  - Seguridad de las comunicaciones
  - Adquisición, desarrollo, y mantenimiento de sistemas
  - Relaciones con los Proveedores.
  - Gestión de los Incidentes de Seguridad de la Información
  - Aspectos de seguridad de la Información de la Gestión de la continuidad del Negocio.
  - Cumplimiento

Fase III: Análisis de Riesgos

Se considera:

- Procesos del Negocio
- Inventario de Activos
- Valoración de Activos
- Identificación de Amenazas.
- Valoración de Riesgo por Activo.
- Tratamiento del Riesgo.

Fase IV: Declaración de Aplicabilidad

Se considera:

- Controles Aplicados.

Aplicación de la Norma ISO 27001:2013

FASE I: Norma ISO 27001: 2013

- **Introducción a la Norma ISO 27001:2013**

  Es un modelo de gestión de seguridad de la información , el cual se define como un conjunto de lineamientos el cual especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Estos requisitos describen cual es el comportamiento esperado del sistema de Gestión una vez que esté en funcionamiento; por lo tanto para el desarrollo del proyecto se tomó a la Norma ISO 27001:2013 como marco de referencia en la implementación del Sistema de Gestión de Seguridad de la información.

  La ISO 27001:2013 cuenta con 114 controles, 14 Dominios de Seguridad y 130 Requisitos de Gestión.

- **Objetivos del Sistema de Gestión de Seguridad de la Información**

  - ✓ Llevar a cabo el análisis de riesgos, identificando amenazas, vulnerabilidades e impactos en la Empresa en estudio con el objetivo de proporcionar una mejora en la adopción de la norma en cuanto a la forma de trabajo con respecto a la seguridad de la información.
  - ✓ Una mejora continua en la gestión de la seguridad, en consideración al control de personas que interactúan en los procesos.
  - ✓ Garantía de continuidad y disponibilidad del negocio.
  - ✓ El incremento de los niveles de confianza tanto para sus usuarios como a sus clientes.

Fase II: Análisis de la Empresa

- **Descripción de la Empresa**

La empresa considerada para el desarrollo de la aplicación de la Norma ISO 27001:2013 es Caja Sullana S.A la cual es un entidad financiera, con presencia a nivel nacional, con más de 25 años en el sector de la microfinanzas y en la prestación de servicios y productos financieros.

La Oficina Principal a nivel nacional de Caja Sullana, se encuentra ubicada en Plaza de Armas 138. Sullana.

Actualmente cuanta con un número aproximado de 3500 trabajadores a nivel Nacional.

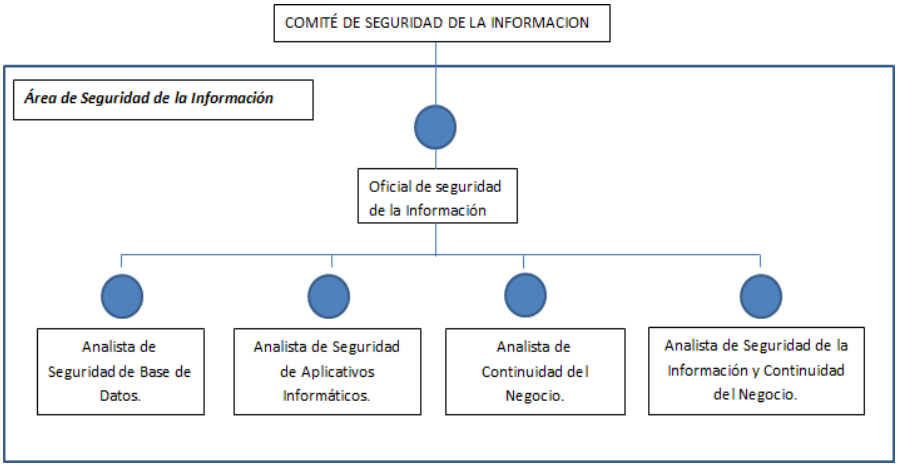
- **Visión:** Ser la Nueva banca de las Grandes Mayorías.

- **Misión:** Trabajamos para acercar la Nueva banca a las empresas y familias peruanas de una forma simple, oportuna y personalizada.

- **Objetivos del Negocio**

El objetivo del negocio de caja Sullana es facilitar el acceso al mercado financiero formal de la población de las localidades de la zona norte y a nivel nacional.

Figura 09. Infraestructura de Seguridad de la Información



El siguiente cuadro presente la jerarquía del Comité de Seguridad de la Información, la cual es presidida, evaluada y fiscalizada por el Oficial de seguridad de la Información. Este comité debe reunirse al menos una vez al mes para revisar el estado de la seguridad de la información de la Institución.

- **Alcance**

  El Sistema de gestión de seguridad de la información se basa en la Norma ISO 27001:2013, el cual está limitado al área de operaciones, considerando esta área principal para el negocio, además se limita a la fase de desarrollo, ya que para una posible implementación sería necesario una inversión en recurso de tiempo, económico y humano por parte de la empresa.

- **Definición de la Política de Seguridad de la Información.**

La política de Seguridad es un conjunto de normas y procedimientos de obligado cumplimiento para el tratamiento de los riesgos de seguridad de la Empresa. La política de Seguridad de la Información de Caja Sullana se encuentra bajo la exigencia de la Circular N G-140-2209 SBS; la cual establece los lineamientos mínimos para una adecuada gestión de la Seguridad de la información y toma como referencia estándares internacionales como es la Norma ISO 27001. Todos los trabajadores de Caja Sullana deben conocer, aceptar y cumplir dichas políticas.

Las políticas de seguridad son las directrices y declaraciones de principios que seguirá la organización en materia de seguridad.

- **Objetivos**

Con la propuesta de la política se pretende conseguir lo siguiente:

- Elaborar un marco de referencia para asegurar que lo elementos del Sistema de Seguridad de la Información sean los apropiados y sirvan de apoyo como guía y control cuando el proyecto se ejecute.
- Establecer las expectativas de la gerencia con respecto al uso que el personal debe hacer de los activos de información de Caja Sullana, así como las medidas que se deben adoptar para la protección de estos recursos.

- Infundir en todo el personal de la empresa la conciencia de la necesidad de la seguridad de la información y la comprensión de sus responsabilidades individuales.

- **Alcance**

Dentro del alcance de la política de Seguridad de la información se encuentra involucrado todo el personal que forma parte del área de operaciones los cuales interactúen con los activos de información del área en mención.

- **Dominios de la ISO 27001:2013**

  - **Política de seguridad de la Información**

    Normas y exigencias para los trabajadores para la protección de la confidencialidad integridad y disponibilidad en los activos de información en la compañía

  - **Organización de la Seguridad de la Información**

    Identificación de roles dentro del sistema de gestión de seguridad de la información, para asignar responsabilidades y acuerdos de confidencialidad correspondientes

  - **Seguridad en los Recursos Humanos.**

    Se encarga de asegurarse de que los empleados, contratistas y terceros entiendan y conozcan sus responsabilidades en cuanto a la protección de la información y estén capacitados adecuadamente para el rol que desempeñan dentro de la organización, para reducir el riesgo de robo, fuga de la información y fraude.

  - **Gestión de Activos**

Identificación y clasificación de activos en la compañía asignando responsables y clasificando la información de acuerdo a su valor, Requerimientos legales, confidencialidad y grado crítico para la organización.

- **Control de Accesos**

  Este control se encarga de vigilar el acceso adecuado a la información, asegurándose que la manipulación de los sistemas de información se encuentre autorizado y controlado por la organización, como permisos para modificar información, asignación de privilegios para utilizar aplicaciones entre otros.

- **Criptografía**

  Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

- **Seguridad Física y del entorno**

  Se encarga de asegurarse de que la organización cumpla la seguridad adecuada, para evitar el acceso físico no autorizado daño e interferencia al local y la información de la compañía esto abarca al tema de cámaras de seguridad Vigilancia de edificios etc.

- **Seguridad en las Operaciones**

  Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

- **Seguridad de las comunicaciones**

  Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

- **Adquisición, desarrollo, y mantenimiento de sistemas.**

Se encarga de asegurarse que la seguridad sea una parte importante en los sistemas de información para evitar errores, pérdidas, modificación no autorizada o mal uso de la información por medio de las aplicaciones de la organización.

- **Relaciones con los Proveedores.**

  Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

- **Gestión de los Incidentes de Seguridad de la Información.**

  Se asegura que la información proveniente de eventos y vulnerabilidades en la seguridad de la información que se encuentren asociados con los sistemas de información de la organización sean comunicados y conocidos por la administración o partes interesadas de manera que permitan tomar una decisión correctiva acertada y rápida.

- **Aspectos de seguridad de la Información de la Gestión de la Continuidad del Negocio.**

  Se encarga de implementar controles adecuados para contrarrestar las interrupciones de las actividades comerciales críticas para la organización por efectos de fallas o desastres importantes en los sistemas de información, asegurándose que se reanude el proceso de manera correcta y segura.

- **Cumplimiento**

  Se encarga de que el sistema de gestión de seguridad de la información se acomode a la normatividad que exige la legislación del país como por ejemplo derechos de propiedad intelectual protección de data y privacidad de información persona.

Fase III: Análisis de Riesgos

Tabla 6

- **Procesos de Negocio (Área de operaciones)**

Proceso de Área Operaciones	**Descripción**
Ahorros	Consulta de Saldos. Ingreso de Cliente Nuevos Aperturas de Cuentas Entrega de Tarjetas Visa Cancelaciones de Cuentas Operaciones de retiro y depósitos. (Toda operación con Efectivo)
Prendario	Tasación de Joyas, generación, aprobación y Anulación de Garantía prendaria. Custodia y entrega de joyas. Desembolso de préstamos prendario. Procesos de garantías.
Administración (Asistente)	Aprobación y Anulación de Operaciones. Gestión de perfiles.

- **Inventario de Activos:**

En este punto se procede a la identificación de los activos de información que forman parte de toda el área de Operaciones, tanto propietarios, personas o entidades encargadas del control del activo en todo su ciclo de vida y garantizar su seguridad, sin embargo no se le atribuye derecho de autor sobre el mismo.

Tabla 7. Inventario de Activos.

Nombre	Descripción	Categoría	Ubicación	Propietario
Aplicaciones Comerciales	Office 2003, 2007, 2010, Acrobat Reader X, Opens Office. Antivirus Karpesky	Aplicaciones	Servidor	Soporte y T.I
Sistemas Operativos	Windows Xp, 2008 2012	Software	Servidor	Soporte y T.I
Dispositivos de Almacenamiento.	Dvd, Cd, discos duros externos,usb.	Dispositivos	Operaciones	Operaciones
Aplicaciones desarrolladas	Sistema Abanks, Mesa de Servicio. Simpe, Originación., Conecta, Core Web, Intranet	Aplicaciones	Servidor	Soporte y T.I
Equipos de Usuario	Desktops de usuarios, Impresoras, scanners.	Hardware	Operaciones	Soporte y T.I
Clientes	Datos de Clientes.	Datos.	Servidor	Operaciones
Trabajador	Personal propio de la entidad	Personal	Operaciones	RR.HH

Garantía Prendaria	Contrato de joyas	Documento	Bóveda Prendario	Prendario
Documentos – cliente	Fichas Clientes, Contratos cuentas de ahorros, Contratos de Desembolso de Créditos. contratos de tarjetas VISA	Documento.	Bóveda de Ahorros.	Usuario asignado.
Pagare	Documento de compromiso de pago Jurídico.	Documentos	Bóveda de Pagare	Usuario asignado.
Reporte de Operaciones	Reportes diarios, mensuales de Operaciones. vouchers	Documento.	Plataforma back / contabilidad / administración	Usuario asignado.
Correo Electrónico	Correo Electrónico	Herramienta	Servidor	Soporte y T.I
Servicios	Internet, Energía Eléctrica, Cámaras de Videos	Subcontratación	Operaciones	Caja Sullana

- **Valorización de Activos**

  Se valorizará los activos según las escalas de puntuación de 0 (no aplicable /sin valor) a 4 (mucho valor). La valorización total será la suma aritmética de los 4 **valores.**

Tabla 8. Valorización de Activos.

Activos	Confidencial	Integridad	Disponibilidad	Total
Aplicaciones Comerciales	1	2	3	6
Sistemas Operativos	2	3	4	9
Dispositivos de Almacenamiento.	4	4	3	11
Sistemas desarrolladas	3	4	4	11
Equipos de Usuario	2	3	4	9
Clientes	4	4	4	12
Trabajador	2	3	3	8
Garantía Prendaria	2	4	3	9
Documentos – Cliente	4	4	4	12
Pagare	4	4	4	12
Reporte de Operaciones	3	4	4	11
Correo Electrónico	3	3	2	8
Servicios	2	4	4	10

- **Identificación de Amenazas**

  Se procede a identificar las amenazas que pueden afectar a los activos. Una amenaza es cualquier acción o acontecimiento que pueda atentar contra nuestra seguridad.

  - ✓ Amenazas Naturales (Inundaciones, Tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales)

  - ✓ Amenazas a Instalaciones (fuego, daños por agua, explosión, caída de energía, perdida de acceso y fallas mecánicas)

- ✓ Amenazas Humanas (Huelgas, Epidemias, materiales peligrosos, problemas de transporte, perdida del personal clave)
- ✓ Amenazas Tecnológicas (virus, pérdida de datos, hacking, fallas de Software y de Hardware, fallas en las líneas telefónicas)
- ✓ Amenazas Operacionales (Crisis Financieras, mala publicidad, pérdida de suplidores, fallas en equipos)
- ✓ Amenazas Sociales (protestas, vandalismo, terrorismo, bombas, sabotaje, violencia laboral)

- **Valoración de Riesgo por Activo**

Tabla 9. Aplicaciones Comerciales

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	6	1	1	6
Humanas (Robo, renuncias, huelgas, accidentes)	6	1	1	6
Instalaciones (energía, explosión, fuego, fallas)	6	2	2	24
Tecnológicas (Software, Hardware,Red, Virus, Hacking)	6	3	2	36
Operacionales (errores usuario)	6	2	1	12

Tabla 10. Sistemas Operativos

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	9	2	1	18
Humanas (Robo, renuncias, huelgas, accidentes)	9	1	1	9
Instalaciones (energía, explosión, fuego, fallas)	9	2	2	36
Tecnológicas (Software, Hardware,Red, Virus, Hacking)	9	3	2	54
Operacionales (errores usuario)	9	2	1	18

Tabla 11. Dispositivos de Almacenamiento

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	11	1	0	0
Humanas (Robo, renuncias, huelgas, accidentes)	11	1	0	0
Instalaciones (energía, explosión, fuego, fallas)	11	1	1	11
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	11	2	3	66
Operacionales (errores usuario)	11	2	2	44

Tabla 12. Sistemas Desarrollados

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	11	2	2	44
Humanas (Robo, renuncias, huelgas, accidentes)	11	3	1	33
Instalaciones (energía, explosión, fuego, fallas)	11	3	2	66
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	11	3	2	66
Operacionales (errores usuario)	11	2	2	44

Tabla 13. Equipos de usuario

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	9	2	1	18
Humanas (Robo, renuncias, huelgas, accidentes)	9	1	0	0
Instalaciones (energía, explosión, fuego, fallas)	9	2	1	18
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	9	2	3	54
Operacionales (errores usuario)	9	2	2	36

Tabla 14. Cliente (datos)

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	12	2	1	24
Humanas (Robo, renuncias, huelgas, accidentes)	12	3	2	72
Instalaciones (energía, explosión, fuego, fallas)	12	2	1	24
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	12	2	1	24
Operacionales (errores usuario)	12	3	2	72

Tabla 15. Trabajador

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	8	2	1	16
Humanas (Robo, renuncias, huelgas, accidentes)	8	1	1	8
Instalaciones (energía, explosión, fuego, fallas)	8	1	0	0
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	8	0	0	0
Operacionales (errores usuario)	8	3	2	48

Tabla 16. Garantía Prendaria

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	9	3	1	27
Humanas (Robo, renuncias, huelgas, accidentes)	9	2	1	18
Instalaciones (energía, explosión, fuego, fallas)	9	2	1	18
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	9	1	1	9
Operacionales (errores usuario)	9	2	3	54

Tabla 17. Contratos – Clientes

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	12	3	1	36
Humanas (Robo, renuncias, huelgas, accidentes)	12	2	1	24
Instalaciones (energía, explosión, fuego, fallas)	12	2	1	24
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	12	1	1	9
Operacionales (errores usuario)	12	3	2	72

Tabla 18. Pagare

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	12	3	1	36
Humanas (Robo, renuncias, huelgas, accidentes)	12	2	2	48
Instalaciones (energía, explosión, fuego, fallas)	12	2	1	24
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	12	1	1	9
Operacionales (errores usuario)	12	3	2	72

Tabla 19. Reporte de Operaciones

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	11	3	1	33
Humanas (Robo, renuncias, huelgas, accidentes)	11	2	1	22
Instalaciones (energía, explosión, fuego, fallas)	11	2	1	22
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	11	1	1	11
Operacionales (errores usuario)	11	3	2	66

Tabla 20. Correo Electrónico

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	8	1	0	0
Humanas (Robo, renuncias, huelgas, accidentes)	8	3	2	48
Instalaciones (energía, explosión, fuego, fallas)	8	1	1	8
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	8	2	2	32
Operacionales (errores usuario)	8	2	1	16

Tabla 21. Servicios

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	10	2	1	20
Humanas (Robo, renuncias, huelgas, accidentes)	10	1	1	10
Instalaciones (energía, explosión, fuego, fallas)	10	3	2	60
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	10	1	1	10
Operacionales (errores usuario)	10	1	1	10

Tratamiento del riesgo

El valor de riesgo aceptable en este caso se establecerá en 50, por los que se tratarían los que igualan o superan esta cifra y se asumirían los que estuvieran por

debajo, De todas formas se aplicarían los controles mínimos establecidos por la norma.

Tabla 22. Activos y su tratamiento del riesgo.

.

Activos	Riesgo	Tratamiento
Aplicaciones Comerciales.	36	Se asume el riesgo.
Sistemas Operativos.	54	Se asume el riesgo.
Dispositivos de Almacenamiento.	66	Se asume el riesgo.
Sistemas desarrollados.	66	Se asume el riesgo.
Equipos de Usuario.	54	Se asume el riesgo.
Clientes.	72	Se asume el riesgo.
Trabajador	48	Se asume el riesgo.
Garantía Prendaria.	54	Se asume el riesgo.
Documentos – Cliente	72	Se asume el riesgo.
Pagare	72	Se asume el riesgo.
Reporte de Operaciones	66	Se asume el riesgo.
Correo Electrónico	48	Se asume el riesgo.
Servicios	60	Se asume el riesgo

Fase IV: Declaración de Aplicabilidad

Se considera:

- **Controles Aplicados**

  En este punto escogeremos los controles que nos ayudarán a salvaguardas los activos de la empresa según el análisis.

  Tabla 23 Aplicación de controles.

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD		JUSTIFICACIÓN
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN				
A 5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A 5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	1	APLICAR	Se ha identificado los riesgos de información y de sus activos, por lo que es necesario establecer una Política de Seguridad de la información, estas políticas deberán definir exactamente a los responsables del desarrollo e implementación. Los Directivos deberán brindar el apoyo necesario en consideración de los requisitos del negocio y de acuerdo a las políticas, leyes y reglamentos pertinentes. Una vez definido las Políticas de seguridad de la información se deberá publicar y poner a disposición a todas las partes interesadas. Trimestralmente se deberá hacer una revisión para asegurar si idoneidad con respecto a los riesgos de información.
	A 5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	2	APLICAR	
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	3	APLICAR	La Institución mediante la política de seguridad de la información debe definir y asignar las responsabilidades en la Seguridad de la Información y separar las responsabilidades y asignar los deberes de los activos de información de la Institución y así minimizar las posibles modificaciones no autorizadas. Además de mantener los contactos apropiados con las autoridades pertinentes; en consideración con los grupos de interés se debe mantener como contactos a especialistas y profesiones especializados en Seguridad de la Información.
	A 6.1.2 SEPARACIÓN DE DEBERES	4	APLICADO	
	A 6.1.3 CONTACTO CON LAS AUTORIDADES	5	APLICADO	
	A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	6	APLICADO	

	A 6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	7	APLICAR	Todos los procesos de implementación o mejora deben de considerarse mediante el proceso de gestión de Proyectos.
A 6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	A 6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	8	APLICADO	La institución mediante la presente política restringe la conexión a las redes inalámbricas de internet por parte de los dispositivos móviles y equipos de terceros.
	A 6.2.2 TELETRABAJO	9	NO APLICAR	De acuerdo con lo establecido en la ley N 300036 del año 2013, la Institución si cuenta con teletrabajo, la cual es una forma de organización laboral. Se caracteriza por el desempeño de labores remuneradas sin la presencia física del trabajador a través de medios informáticos de telecomunicaciones y análogos. Sin embargo, para el área de operaciones no es necesario este tipo de labores a desempeñar.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS				
A 7.1 ANTES DE ASUMIR EL EMPLEO	A 7.1.1 SELECCIÓN	10	APLICADO	Para el desarrollo del proceso y actividades de selección de personal el área de Recursos Humanos son los responsables de llevar a cabo las etapas para el reclutamiento del personal, en consideración de los reglamentos, códigos de ética y las leyes pertinentes que aseguran la calidad del proceso bajo las consideraciones de la gerencia.
	A 7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	11	APLICADO	
A 7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	A 7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	12	APLICADO	El personal en inducción interactúa permanentemente con los activos de información de la institución por tal motivo se lleva a cabo la firma de aceptación de documentos tales como: Acta de fiel cumplimiento de manual de prevención de lavado de activos, Código de Ética y de Conducta, Reglamento de seguridad y salud en el trabajo, Política de uso de correo electrónico.
	A 7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN, Y FORMACIÓN EN	13	APLICADO	

	A.7.2.3 PROCESO DISCIPLINARIO	14	APLICADO	La institución junta otras áreas de interés se comprometen en el fiel cumplimiento de capacitación y actualización del personal. El cumplimiento del proceso disciplinario debe ser responsabilidad hasta cierto punto del superior del área, esta consideración es basado a las políticas y procedimientos que se le anteponen para la ejecución de sus labores. Lo mencionado anteriormente recae en la ejecución por parte del área de Recursos humanos.
A 7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	A7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	15	APLICADO	
A.8 GESTION DE ACTIVOS				
A 8.1 RESPONSABILIDAD POR LOS ACTIVOS	A 8.1.1 INVENTARIO DE ACTIVOS	16	APLICAR	Se debe identificar los activos de Información del área y las instalaciones de procesamiento de información, además de documentar y mantener un inventario actualizados de estos activos.
	A 8.1.2 PROPIEDAD DE LOS ACTIVOS	17	APLICAR	Se debe identificar los propietarios de los activos de información obtenidos en los inventarios. Además del seguimiento de la regularización de los activos de información faltantes por parte de sus propietarios o interesados y de la verificación de su autenticidad.
	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS	18	APLICAR	Se debe implementar las políticas y procedimientos en la identificación, documentación e implementación de las reglas para el uso aceptable de la información y de activos asociados con la información e instalaciones de procesamiento de información.
	A 8.1.4 DEVOLUCIÓN DE LOS ACTIVOS	19	APLICAR	Los activos de la institución deberán ser devueltos por los colaboradores al finalizar su relación contractual o uso del mismo bajo un documento de entrega al superior o área responsable. El superior o área responsable debe asegurar la devolución de los activos cuando se presentan renuncias, rotaciones, terminaciones o cambios de la contratación del personal que conforman los diferentes proyectos o áreas transversales de la institución.

	A 8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	20	APLICAR	La institución debe asegurar que la información reciba un nivel apropiado de protección, de acuerdo con su importancia para la institución, así mismo todos los usuarios deben de estar comprometidos en respetar la clasificación de la información propuesta o definida.
A 8.2 CLASIFICACIÓN DE LA INFORMACIÓN	A 8.2.2 ETIQUETADO DE LA INFORMACIÓN	21	APLICAR	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la institución. Toda información que sea clasifica como "confidencial" debe de poseer una etiqueta de seguridad que provea todos los datos correspondientes a esta
	A 8.2.3 MANEJO DE ACTIVOS	22	APLICAR	Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la institución.
A 8.3 MANEJO DE MEDIOS	A 8.3.1. GESTIÓN DE MEDIOS REMOVIBLES	23	APLICAR	Se debe implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la institución en tal sentido establecer un formato de asignación de propietario de medios removibles tales como: Correo electrónico laboral, servicios de mensajería, USB, CD, entre otros además de un formato para la entrega o custodia y destrucción de tales medios o dispositivos.
	A 8.3.2 DISPOSICIÓN DE LOS MEDIOS	24	APLICAR	Se debe llevar un control de la disposición de los medios cuando ya no se requieran, mediante procedimiento y formato establecido que dispongan el área de Seguridad de la Información, así como la información contenida en dichos medios conforme a políticas correspondientes.

	A 8.3.3 TRANSFERENCIA DE MEDIOS FÍSICOS.	25	APLICAR	Se debe llevar a cabo un procedimiento para el manejo y almacenamiento de la información, para asegurar la que se eviten eventos como divulgación, modificación, retiro o destrucción de información no autorizada cuando se traslade un medio físico de un punto a otro.
A.9 CONTROL DE ACCESO				
A 9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	A 9.1.1 POLÍTICA DE CONTROL DE ACCESO	26	APLICAR	La institución día a día genera y desarrolla activos de información lo cuales deben estar salvaguardados o custodiados de acuerdo a su importancia o clasificación por lo que se debe controlan el acceso a la información.
	A 9.1.2 ACCESO A REDES Y A SERVICIOS EN RED	27	APLICAR	Se debe asegurar que los usuarios de la red o los que usan el sistema de la institución sólo acceden a los servicios para los que están autorizados y que sus accesos solo se establezcan de acuerdo a un perfil definido o mediante la autorización del área de Seguridad de la Información.
A 9.2 GESTIÓN DE ACCESO DE USUARIOS	A 9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	28	APLICAR	Se debe implementar un procedimiento para llevar a cabo el Registro y Cancelación de los Registro de cada usuario de la Institución, además de evitar el acceso no autorizado a los sistemas y servicios de información.
	A 9.2.2 SUMINSITRO DE ACCESO DE USUARIOS	29	APLICAR	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios de la Institución.
	A 9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	30	APLICAR	Se debe llevar el control y un registro formal mediante un formato de la asignación y uso del acceso privilegiado a la información de los sistemas y servicios.

	A 9.2.4 GESTIÓN DE LA INF. DE AUTENTICACIÓN SECRETA DE USUARIOS	31	APLICAR	La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal a través de un gestor de identidad en un portal web.
	A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	32	APLICAR	Se debe llevar a cabo una revisión periódica de cada 2 menes y así asegurar que cada usuario solamente tenga acceso a la información que requiere para sus funciones.
	A 9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.	33	APLICAR	Si debe llevar a cabo un registro por parte de área de Seguridad de la Información de los colaboradores que culminan vínculos laborales, por lo que se debe proceder a retirar los derechos de los accesos a los sistemas u activos de información de la institución.
A 9.3 RESPONSABILIDADES DE LOS USUARIOS	A 9.3.1 USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	34	APLICAR	Se debería exigir y promover a los usuarios que cumplan las buenas prácticas de la institución para el uso de información de autenticación secreta de su contraseña.
A 9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A 9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	35	APLICADO	Evitar que usuarios no autorizados tengan acceso a los sistemas de información, además que cada 30 días se cambien las claves las cuales permitan la autorización de operaciones usadas en las áreas de operaciones.
	A 9.4.2 PROCEDIMIENTO DE INGRESO SEGURO.	36	APLICADO	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
	A 9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS.	37	APLICAR	Se debe hacer una evaluación a los sistemas de gestión de contraseñas, ya que estas deberían ser interactivas y deberían asegurar la calidad de las contraseñas. Se debe promover el protocolo de las buenas prácticas de la creación de una contraseña por parte de los usuarios; además de establecer el cambio de clave cada treinta días (30) para cada portal, por consiguiente la existencia de un formato como Política del buen uso de las contraseñas, y que su prestación o mal uso se considere falta grave.

	A 9.4.4 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS.	38	APLICAR	Restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
	A 9.4.5 CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS.	39	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
A. 10 CRIPTOGRAFIA				
A 10.1 CONTROLES CRIPTOGRAFICOS	A 10.1.1 POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	40	APLICADO	Los sistemas de información que se manejan en los diferentes proyectos deben establecer controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información, además de asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la
	A 10.1.2 GESTIÓN DE LLAVES	41	APLICADO	Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A. 11 SEGURIDAD FISICA Y DEL ENTORNO				
	A 11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	42	APLICADO	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización. Limitar la posibilidad de pérdida de activos de información definiendo perímetros de seguridad física.
A 11.1 ÁREAS SEGURAS	A 11.1.2 CONTROLES DE ACCESO FÍSICOS	43	APLICADO	Evitar el acceso no autorizado a áreas seguras como área de servidores, área de comunicaciones, archivo con información confidencial. El personal que deba ingresar será con la Aprobación autorización del área de Seguridad Física, Seguridad de la Información y al resto de áreas interesadas.

	A 11.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	44	APLICADO	Se mantiene la información bajo llave, (estrictas medidas de seguridad) y se restringe el acceso sin autorización, o se permite bajo un documento de autorización con avisos impresos.
	A 11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	45	APLICADO	Se cuenta con sistema de aire acondicionado en todos los ambientes y en data center, protección con UPS y Generador Eléctrico, protegido con extintores especiales para data center y sistema completo contra incendios.
	A 11.1.5 TRABAJO EN ÁREAS SEGURAS	46	APLICAR	Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras, además de la implementación de las políticas y procedimientos del área de Seguridad Física y Medio Ambiente.
	A 11.1.6 ÁREAS DE DESPACHO Y CARGA	47	APLICADO	Se controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A 11.2 EQUIPOS	A 11.2.1 UBICACIÓN Y PROTECCION DE LOS EQUIPOS	48	APLICADO	Todos los equipos de la institución se encuentran ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. La institución realiza anualmente inventarios de todos los equipos tales como: servidores, computadores de escritorio, portátiles, impresoras, fotocopiadoras, faxes, escáneres, entre otros por tal razón es necesario establecer controles que permitan evitar la ocurrencia de eventos como pérdida, daño, robo o interrupción de los equipos tanto dentro como fuera de la organización. Así como el registro de los bienes o activos robados.
	A 11.2.2 SERVICIOS DE SUMINSITRO	49	APLICADO	
	A 11.2.3 SEGURIDAD EN EL CABLEADO	50	APLICADO	
	A 11.2.4 MANTENIMIENTO DE EQUIPOS	51	APLICADO	
	A 11.2.5 RETIRO DE ACTIVOS	52	APLICAR	Los equipos, información o software no se deberían retirar de su sitio sin autorización previa, para ello se necesita la aprobación de las áreas supervisoras de, tanto del área de Seguridad física como el área de seguridad de la información, además del visto del Supervisor de operaciones y/o de Administrador.

	A 11.2.6 SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	53	APLICAR	Para evitar daños o pérdidas a los equipos cuando se encuentran fuera de las instalaciones se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
	A 11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	54	APLICAR	Se deberían verificar que todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
	A 11.2.8 EQUIPOS DE USUARIO DESATENDIDO	55	APLICADO	El personal de la institución es responsable de los activosde información que se encuentran a su cargo, así como de la protección de estos activos en cuanto confidencialidad, integridad y disponibilidad, de tal forma que se han definido responsabilidades claras en cuanto a seguridad de la información en los manuales de funciones que son entregados al personal, en tal sentido es necesarioestablecer controles de seguridad para asegurar que se evitael acceso de usuarios no autorizados y el robo de información de equipos en desuso. La institución cuenta con una política de escritorio limpio y una política depantalla limpia en las instalaciones de procesamiento de información.
	A 11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.	56	APLICADO	
A.12 SEGURIDAD DE LAS OPERACIONES				
A 12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	A 12.1.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	57	APLICAR	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten segmentados por áreas y por perfiles de usuarios con especificaciones del nivel de activo con el que interactué o genere, estos procedimientos deberían estar a disposición mediante un portal., además se debería de entregar un manual básico de operaciones que sirva como guía de operaciones al personal nuevo o en inducción.

	A 12.1.2 GESTIÓN DE CAMBIOS	58	APLICAR	Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. Estos cambios deben llevar un registro histórico en consideración al área de operaciones por parte del área de Seguridad de la Información y de las áreas
	A 12.1.3 GESTIÓN DE CAPACIDAD	59	APLICAR	Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura en consideración con los procesos de cada área y su giro de negocio.
	A 12.1.4 SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.	60	APLICADO	La institución mantiene los ambientes de cada área separados ya sea de desarrollo, prueba y operación, para así reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A 12.2 PROTECCION CONTRA CODIGOS MALICIOSOS	A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	61	APLICAR	Para el desarrollo de las actividades de la Institución se utilizan servicios como Internet, medios extraíbles, los cuales pueden afectar el correcto funcionamiento de activos de información como equipos, software entre otros, por lo tanto, es importante establecer controles de seguridad que permitan la detección y prevención de la acción de códigos maliciosos, así como también procedimientos de concientización de los usuarios. Se debería llevar a cabo el manteniendo de cada uno de los equipos y actualización de antivirus en horarios que no afecten el desarrollo de las funciones de los usuarios y la atención a los clientes.
A 12.3 COPIAS DE RESPALDO	A 12.3.1 RESPALDO DE LA INFORMACIÓN	62	APLICAR	La información de la Institución, como correos institucionales, reportes de clientes, históricos de reportes, documentos de usuarios y de los diferentes áreas se encuentra ubicada en los equipos asignados a los colaboradores así como en el servidor de archivos, en tal sentido es importante establecer controles de seguridad que aseguren la ejecución de procedimientos de back up y recuperación que permitan restaurar en el menor tiempo la información ante la materialización de un riesgo, y así permitir que la Institución continué con sus actividades

				habituales sin ningún inconveniente y la atención a sus clientes.
A 12.4 REGISTRO Y SEGUIMIENTO	A12.4.1 REGISTRO DE EVENTOS	63	APLICAR	La Institución para el desarrollo de sus actividades cuenta con colaboradores que tienen acceso a los diferentes activos de información ya sea a nivel de base de datos, o parte operativa del negocio, por lo que para la ejecución de sus actividades, en tal sentido es importante establecer controles de seguridad que permitan la detección oportuna de actividades de procesamiento de información no autorizadas y herramientas para investigaciones futuras de incidentes de seguridad de la información. Además, se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. Registrode eventos en los sistemas operativos de acceso de errores, de aplicación y se revisan
	A12.4.2 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	64	APLICADO	La Institución mantiene y protege el historial de logs, por lo que solo los Administradores de los equipos tienen acceso a la información de registro.

	A12.4.3 REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR	65	APLICAR	La Institución mantiene el histórico de las actividades del administrador y del operador del sistema mediante reportes físicos diarios o mensuales o generados por el usuario del sistema. Tales registros se deberían almacenar como histórico ya sea como archivos o escanear los físicos, proteger y custodiar. Se debería desarrollar un procedimiento de autenticidad o calidad bajo un muestreo aleatorio de los activos de información físicos correspondientes de los clientes, además de la implementación de un ambiente donde se custodie cada activo de información, ya sea por área y por clasificación del mismo,
	A12.4.4 SINCRONIZACIÓN DE RELOJES	66	APLICADO	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la Institución o ámbito de seguridad se encuentran sincronizados con una única fuente de referencia de tiempo.
A 12.5 CONTROL DE SOFTWARE OPERACIONAL	A 12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	67	APLICADO	La Institución ha establecido controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos. De igual forma para los equipos asignados a los Usuarios se restringe la posibilidad de instalación de programas y/o aplicativos; y así asegurar la integración de los sistemas operativos.
A 12.6 GESTION DE LA VULNERABILIDAD TÉCNICA	A 12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	68	APLICADO	La Institución mantiene activos de información tecnológicos los cuales están expuestos a vulnerabilidades de tipo técnico, por lo tanto, se establecía controles de seguridad para garantizar la reducción de los riesgos derivados de las vulnerabilidades técnicas, así como un histórico de sus
	A 12.6.2 RESTRICCIÓN SOBRE LA INSTALACION DE SOFTWARE	69	APLICADO	La Institución para el desarrollo de sus actividades utiliza diferentes sistemas operativos, en tal sentido estableció controles de seguridad para garantizar la protección,control y correcto uso de los sistemas operativos, es por ello que cuenta con controles para la Restricción sobre la Instalación de cualquier Software.

A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	A 12.7.1 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	70	APLICADO	La Institución cuenta con sistemas operativos o procesos que pueden ser objeto de auditoria de seguridad de la información, por lo tanto es importante establecer controles de seguridad que garanticen un adecuado uso de las herramientas de auditoria y minimizar la interrupción de los sistemas durante el proceso o atención a los clientes.
A. 13 SEGURIDAD DE LAS COMUNICACIONES				
A 13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	A 13.1.1 CONTROLES DE REDES	71	APLICADO	La institución mantiene asegurada la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte. Se ha desarrollado mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red.
	A 13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	72	APLICADO	
	A 13.1.3 SEPARACIÓN EN LAS REDES	73	APLICADO	Los grupos de servicios de información, usuarios y sistemas de información se mantienen separados en las redes para así evitar que el tráfico de una subred afecte a las demás.
A 13.2 TRANSFERENCIA DE INFORMACIÓN	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRASNFERENCIA DE INFORMACIÓN	74	APLICADO	Dentro del desarrollo normal de las actividades de la entidad se presentan actividades de intercambio de información con clientes, colaboradores, entre otros como parte del desarrollo de la prestación de productos y servicios, por lo cual es importante establecer controles de seguridad para asegurar que se cumplen las políticas y procedimientos de la institución para el intercambio de información y para garantizar que no se presente el uso
	A 13.2.2 ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN	75	APLICADO	

	A 13.2.3 MENSAJERIA ELECTRÓNICA	76	APLICADO	inadecuado, violación o corrupción cuando la información sale de las instalaciones de la organización. Parte de los controles es la identificación de la clasificación de la Información, ya sea del tipo; confidencial, uso interno y pública.
	A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN	77	APLICAR	Se debería considerar el promover los acuerdos de Confidencialidad en cada uno de los colaboradores de la entidad, sobre todo quienes interactúan con el público a diario, es decir: No divulgar información de la entidad ni de sus clientes que haya sido clasificada como confidencial. Está prohibido que los usuarios saquen información de la entidad.
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
A 14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	A 14.1.1 ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SI	78	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
	A 14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	79	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
	A 14.1.3 PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES	80	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
A 14.2 CONTROL DE ACCESO AL SISTEMA OPERATIVO	A 14.2.1 POLÍTICA DE DESARROLLO SEGURO	81	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
	A 14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	82	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
	A 14.2.3 REVISIÓN TÉCNICAS DE LAS APLICACIONES DESPUES DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN	83	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas

	A 14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	84	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
	A 14.2.5 PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS	85	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
	A 14.2.6 AMBIENTE DE DESARROLLO SEGURO	86	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
	A 14.2.7 DESARROLLO CONTRATADO EXTERNAMENTE	87	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
	A 14.2.8 PRUEBAS DE SEGURIDAD DE SISTEMAS	88	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
	A 14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS	89	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
A 14.3 DATOS DE PRUEBA	A14.3.1 PROTECCIÓN DE DATOS DE PRUEBA	90	NO APLICAR	No es necesario aplicar dicho control, porque los únicos responsables de su administración es el Área de Sistemas
A.15 RELACIONES CON LOS PROVEEDORES				
A. 15.1 RELACIONES CON LOS PROVEEDORES	A 15.1.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	91	APLICADO	La institución desarrolla actividades para las cualesrequiere realizar diferentes tipos de compras, en tal sentidoexisten controles que garantizan la seguridad del negocio; antes de gestionar compras de bienes o servicios que afecten la seguridad de la información de la organización y la infraestructura que sobre la cual esta soportada.
	A 15.1.2 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	92	APLICADO	La institución estableció y mantiene acuerdos de requisitos de seguridad de la información con los proveedores. Estos requisitos de seguridad se definen en los conceptos técnicos y en los pliegos de condiciones.

	A 15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	93	APLICADO	Los acuerdos con terceros deben incluir requisitos para tratar los riesgos de seguridad de la información. Acuerdo de Confidencialidad con terceros.
A 15.2 GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES	A 15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	94	APLICADO	La institución determina el grado de cumplimiento de terceras partes conforme contrato y/o acuerdos.
	A 15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	95	NO APLICAR	No se considera que este control ayude a reducir el riesgo de los activos identificados.
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION				
A 16.1 GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A 16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	96	APLICAR	La institución debe asegurar una respuesta oportuna, efectiva y organizada de los incidentes de seguridad de la información ocurrido en el área operativa y áreas administrativas, por lo que mediante su política de seguridad de la información establezca su compromiso, organización y asignación de para su cumplimiento, de igual forma velar por mantener protegido sus activos de información mediante la revisión del sistema de gestión de seguridad de la información, la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales, y la revisión independiente de sus activos, por lo que la programación periódica de auditorías, arqueos y muestreos aleatorios de la autenticidad de activos físicos le permitirán a reducir el riesgo de los mencionados.
	A 16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	97	APLICAR	Se debe de asegurar que los eventos e incidentes de seguridad de información sean reportados oportunamente y que las áreas involucradas deberán emitir el Reporte de Eventos vinculados a la Seguridad de la Información, dichos reporte deben de ser documentos por los involucrados o participantes en el menor tiempo posible.

	A 16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	98	APLICAR	Se debería exigir a todos los colaboradores y terceros que usan los servicios y sistemas de información de la institución, que observen e informen cualquier debilidad, falta en seguridad de la información observada o sospechosa en los sistemas o servicios.
	A 16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS	99	APLICAR	Cada uno de los eventos de seguridad de la información se debería evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información considerando el activo de información y tipo afectado.Estos incidentes de seguridad de la información deben ser analizados por el personal designado por la gerencia o área interesada para identificar acciones de mejora, en tal sentido es necesario establecer controles de seguridad para garantizar un manejo eficaz y consistente de los incidentes de seguridad de la información.
	A 16.1.5 RESPUESTA A INCIDENTES DE SEGUIRIDAD DE LA INFORMACIÓN	100	APLICAR	Se debería tener un Procedimiento para atender incidentes de seguridad de la información y así dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
	A 16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	101	APLICAR	Todo conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para prever, reducir y mitigar la posibilidad o el impacto de incidentes futuros.
	A 16.1.7 RECOLECCIÓN DE EVIDENCIA	102	APLICAR	La institución debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia ante los eventos en contra de la seguridad de la Información de la Institución o clientes de la misma.
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO				

	A 17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	103	APLICAR	La institución mantiene un gran vinculo y responsabilidad con la atención de sus clientes, por lo que debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre naturales; lo que permitaseguir con la atención a sus clientes, minimizando los riesgos vinculados ante tales. Tanto los procedimientos como los formatos deben estar aprobados por la Gerencia y publicados en el portal para su
A 17.1 CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	A 17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	104	APLICAR	La institución debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. Se debe nombrar a representantes los cuales dirigirán dichos eventos cuando se presenten; ellos informarán y serán quienes reporten y documenten dichos eventos. El área de Seguridad de la información, Continuidad del Negocio y el Jefe de Operaciones se harán responsables de la toma de decisiones según lo amerite ante dicho evento.
	A 17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SI	105	APLICAR	La institución debe verificar a intervalos regulares y mantener actualizados los controles de continuidad de la seguridad de la información establecidos e implementados acordes a la realidad, con el fin de asegurar su eficiencia durante situaciones adversas, para ello el área de seguridad de la información de debe de hacer responsables de tales tareas
A 17.2 REDUNDANCIAS	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	106	NO APLICAR	No se considera que este control ayude a reducir el riesgo de los activos identificados.
A. 18 CUMPLIMIENTO				

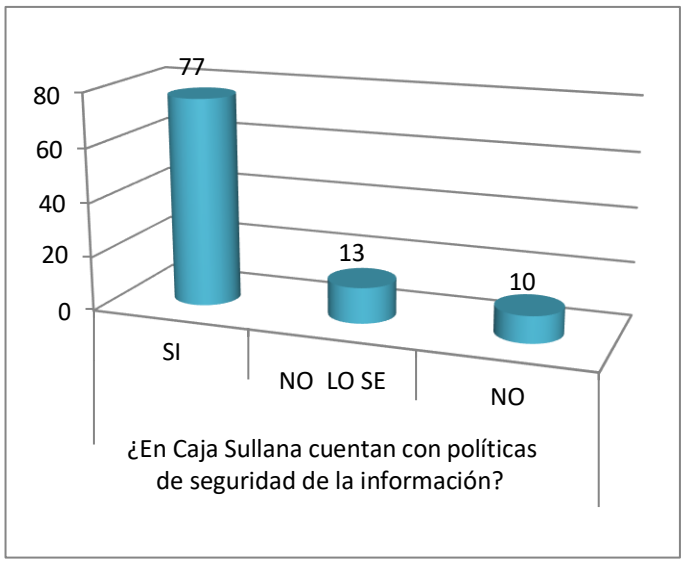
A 18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A 18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES.	107	APLICADO	La institución evita el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito orientado a la seguridad.
	A 18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	108	APLICADO	La institución asegura el cumplimiento de los requisitos legislativos de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados o adquiridos.
	A 18.1.3 PROTECCIÓN DE REGISTROS	109	APLICADO	La institución Protege los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.
	A 18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	110	APLICADO	La institución cuida las bases de datos y expedientes con datos personales tanto como de sus clientes como de sus colaboradores y otros, como parte de las buenas prácticas de seguridad para evitar violar los derechos de seguridad en la información y ocasionar daños al personal o a los clientes.
	A 18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	111	APLICADO	La institución para los sistemas de información a establecido el uso de controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información.
A 18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	A 18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	112	APLICAR	La institución mediante su política de seguridad de la información establece su compromiso, organización y asignación para su cumplimiento, de igual forma vela por mantener protegido sus activos de información; así mismo establece la revisión del sistema de gestión de seguridad de la información por lo que deberá actualizar en consideración a la última versión de la norma estándar ISO 27001: 2013 bajo la exigencia de la Superintendencia de Banca y seguros y AFP en su Circular G.140.2009. La revisión y actualización de los controles y objetivos de control deben de estar bajo la Dirección del área de seguridad de la Información bajo el apoyo de las áreas pertinentes.

	A 18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD A 18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	113 114	APLICAR APLICAR	El personal de la institución interactúa permanentemente con los activos de información para los cuales se han diseñado políticas y controles en materia de seguridad de la información, en tal sentido es importante establecer controles de seguridad que garanticen que todo el personal de la institución conozca y aplique las políticas de seguridad de la información y los respectivos controles. Además es necesaria la inclusión de la Alta Dirección en este proceso, como requisito de la norma y condición de éxito del Sistema de Gestión de Seguridad de la Información por lo tanto se debería considerar desarrollar un historial de Actas de comité de calidad del proceso gestión de recursos informáticos y considerar la revisión de los controles y consideraciones de los requisitos mínimos de seguridad.

Resultados

El cuestionario realizado al personal de Operaciones de la Caja Sullana; consta de 34 preguntas el cual se encuentra en Anexos, para el análisis de los resultados tomaremos 17 preguntas.

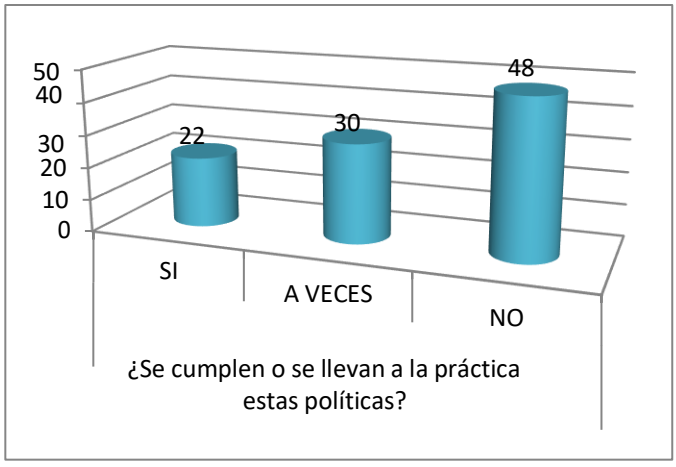
1.



Análisis:

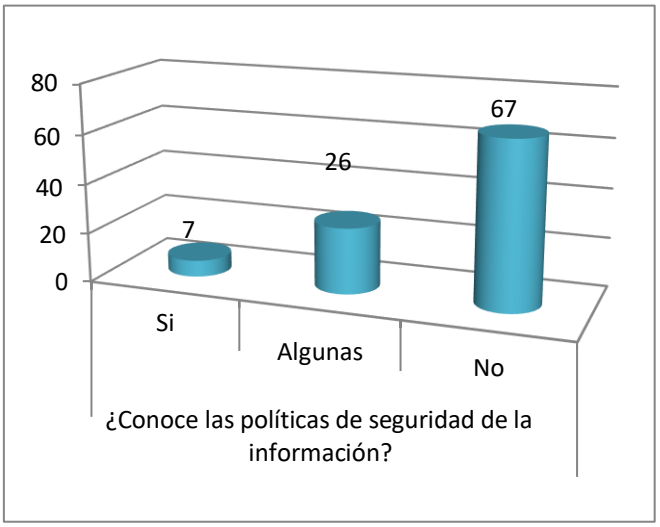
En el gráfico podemos apreciar que del 100% de la encuesta, el 77 % de los trabajadores saben que Caja Sullana cuenta con políticas de Seguridad de la Información, un 13% no saben si existen dichas políticas y el 10% afirma que no cuentan con políticas de seguridad de la Información.

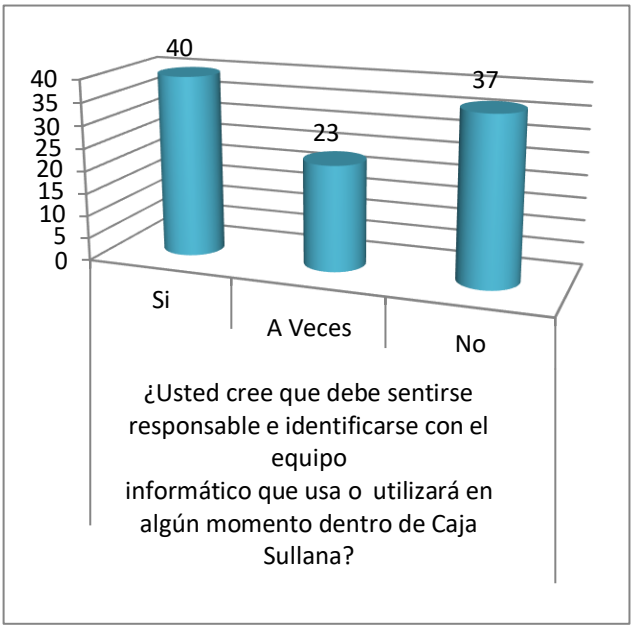
2.

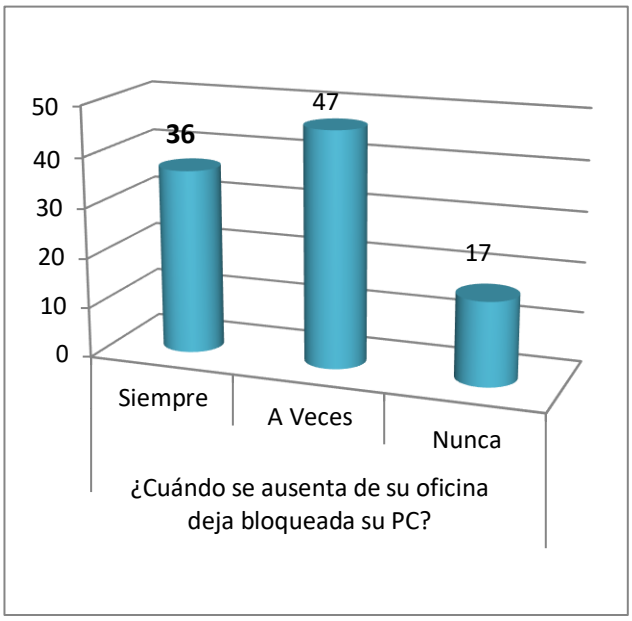


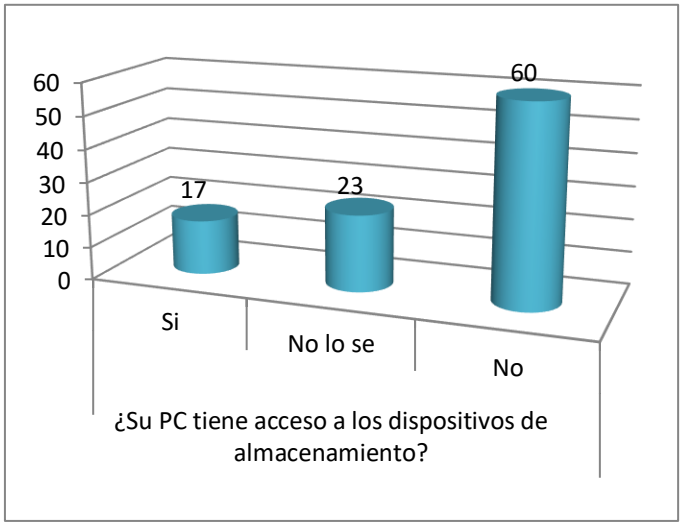
Análisis:

Esta pregunta guarda relación a la anterior con respecto al cumplimiento de las Políticas de Seguridad de la Información, por lo que la mayoría con un 48% resalta el incumplimiento de las Políticas de Seguridad de la Información, un 30% las cumpliría en ocasiones y un escaso 22% afirma su cumplimiento.

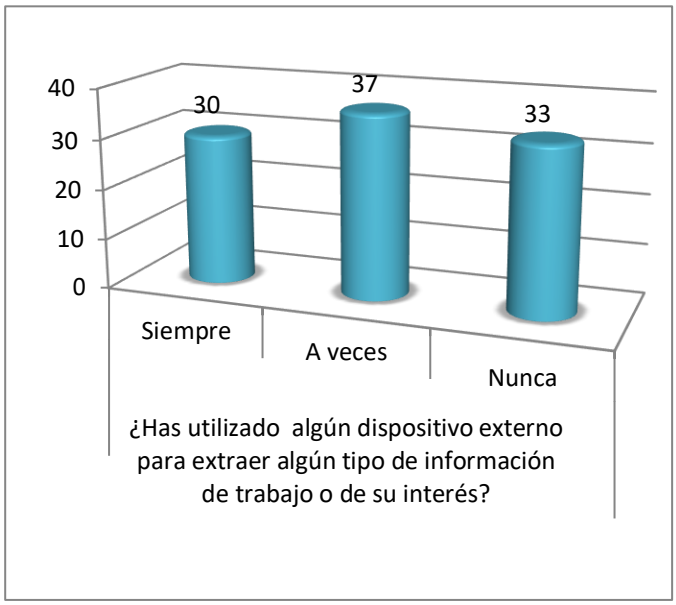
3.  	**Análisis:** El siguiente cuadro refleja el escaso conocimiento de las políticas de Seguridad de la Información considerando que el 67 % afirma no conocerlas, mientras que el 26% afirma conocer escasamente de las políticas de seguridad de la información de la Institución; un 7% de ellos si las conoce (personal con mayor estancia).

4.  	**Análisis:** En el gráfico podemos observar que el 40% de los trabajadores se sienten responsables de los equipos que utilizan dentro de las instalacionesdel área, un 23% sólo en ocasiones y37% restante no se siente responsable del equipo que utiliza, por lo que podríamos decir que casi la mayoría se siente responsable.

5.  	**Análisis:** Se puede apreciar que sólo el 36% siempre deja bloqueada su PC cuando no la está utilizando; el 47% bloquea su pc en ciertas ocasiones; y el 17% nunca deja bloqueando su computador.

6.  	**Análisis:** Se puede observar que el 17 % de los trabajadores tiene los accesos para dispositivos de almacenamiento, el 23% no ha verificado y un 60 % no cuenta con dicho acceso.

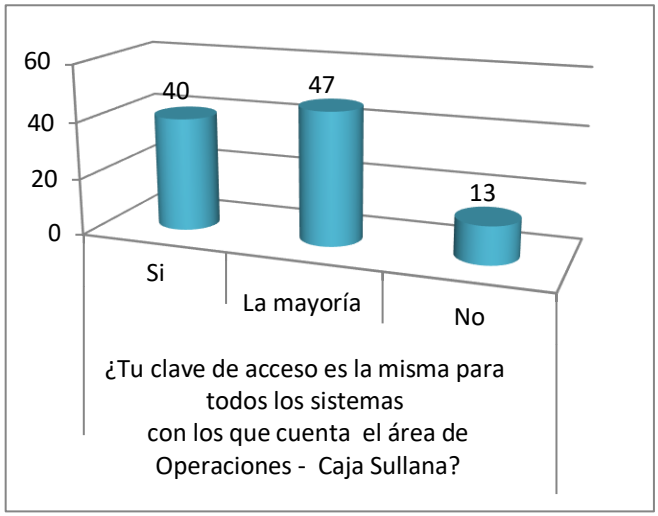
7.



Análisis:

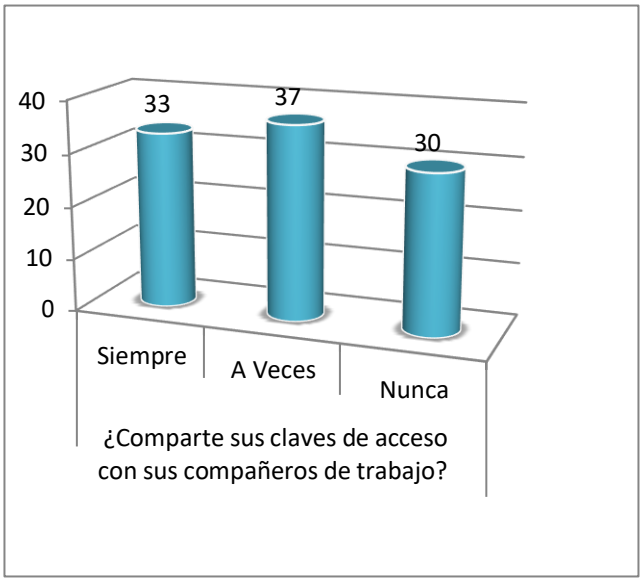
En el gráfico se observa que el 30% utiliza algún tipo de dispositivo para extraer información, el 37% utilizó algunas veces y el 33% nunca hizo uso de dispositivos para extraer información.

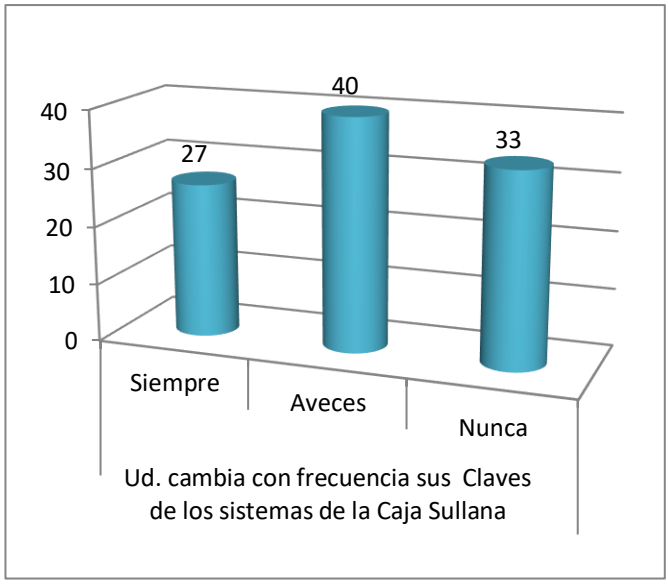
8.



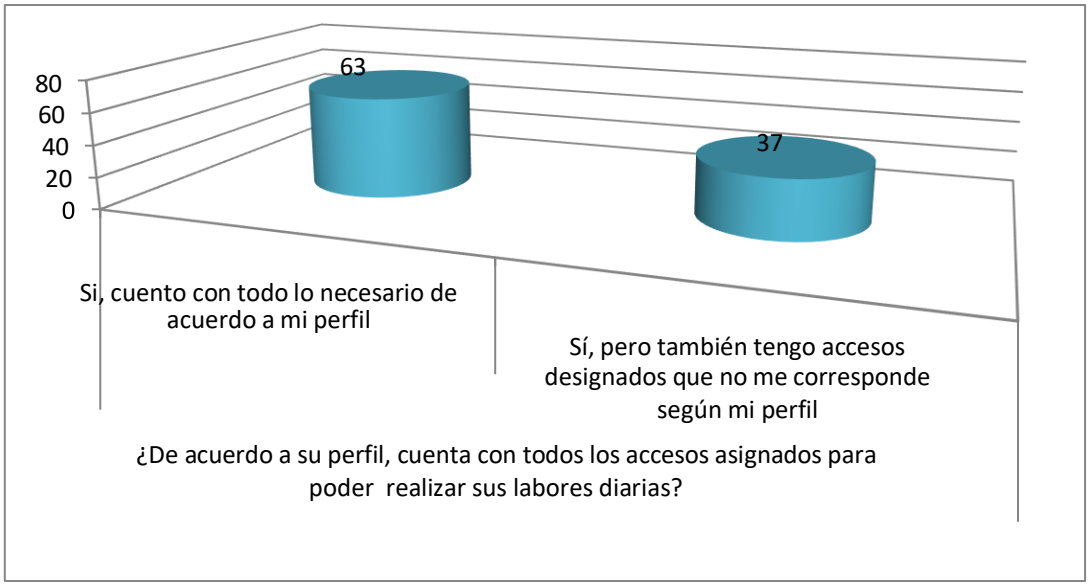
Análisis:

Se puede observar que el 40% cuentan con una misma clave de acceso para todos los sistemas con los que cuenta Caja Sullana , el 47 % utiliza la misma clave solo para algunos sistemas , por ultimo vemos que solo el 13 % tiene una clave diferente para cada sistema.

9.  	**Análisis:** Aunque estos valores tienen un promedio similar sus resultados demuestran la escasa responsabilidad y mal uso de los activos de información por parte de los trabajadores, por lo que la mayoría con el 37% suele compartir claves de acceso, el 33% siempre las comparte y el 30% nunca comparte dichas claves.

10.  	**Análisis:** Podemos apreciar que sólo un 27% siempre cambia con frecuencia sus claves de acceso a los sistemas para una mayor seguridad, un 40% en ocasiones realiza cambios de sus claves de acceso; sin embargo el 33 % afirmó nunca cambiar sus claves de acceso.

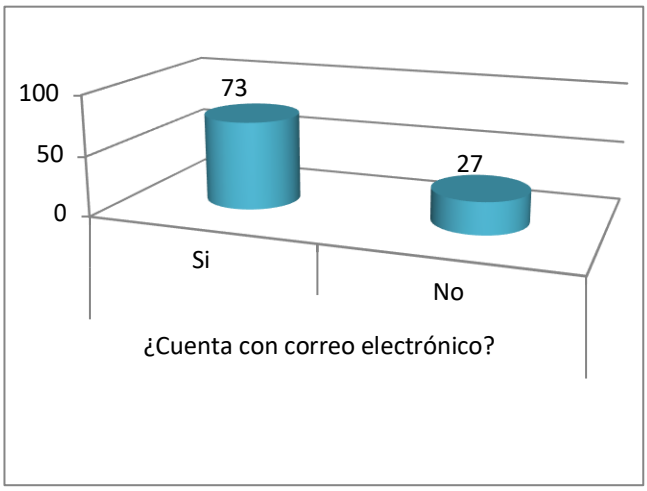
11.



Análisis :

Como podemos observar en el gráfico la mayoría de trabajadores cuentan con sus accesos necesarios para poder cumplir con sus funciones, sin embargo el 37% de ellos disponen de accesos que no corresponden a su perfil asignado o mantienen accesos no autorizados.

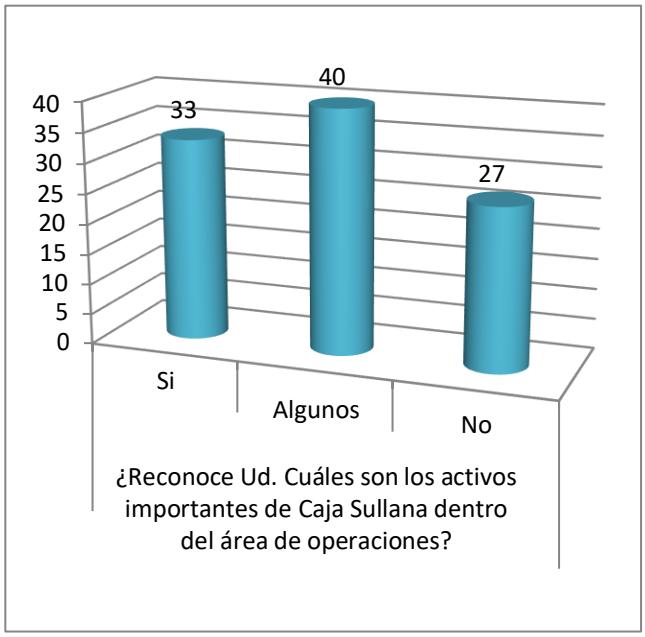
12.



Análisis:

Podemos ver que el 73 % hace uso del correo electrónico institucional que se le ha sido asignado, mientras que el 27% no cuenta con correo electrónico. Este medio permite a muchos de los usuarios el ingreso y salida de información confidencial de la institución.

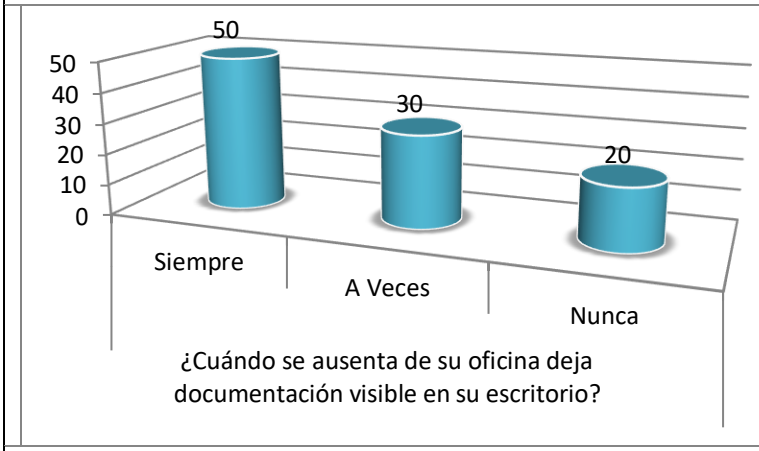
13.



Análisis:

Como podemos apreciar el 40% representa el escaso conocimiento de la identificación de los activos de información del área, mientras que el 27% no logra identificar los activos de información; y menos de la mitad del personal, reflejado con el 33% si logra identificarse con los activos de información del área.

14.

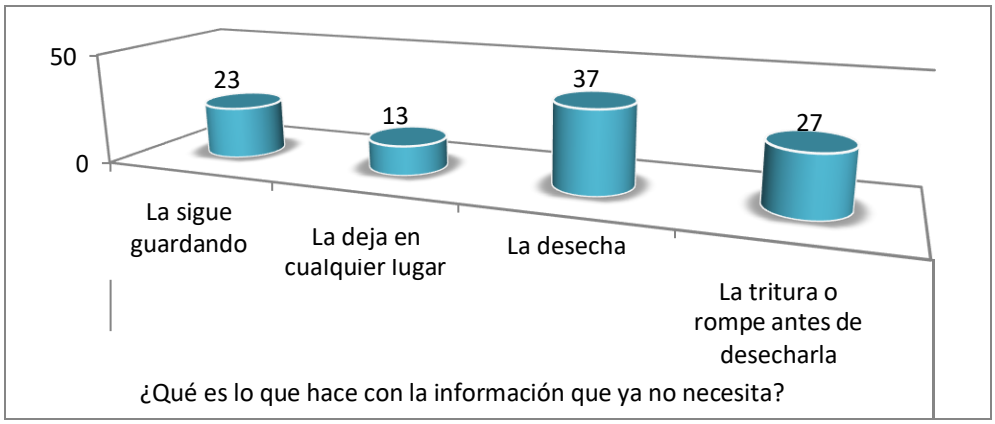


Análisis:

Como podemos apreciar la falta de identificación con el protocolo de escritorios limpios se manifiesta con los siguientes resultados.

La mitad del personal con el 50% siempre deja documentos en el escritorio, el 30% a veces deja documentación visible y el 20% nunca deja documentos sobre sus escritorios.

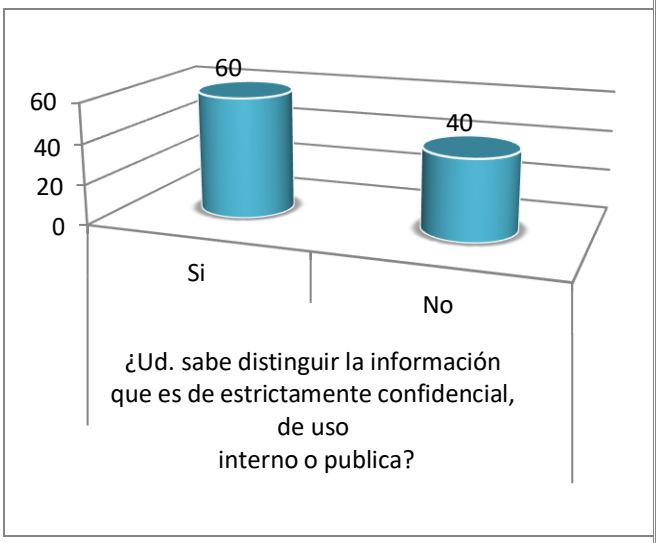
15.



Análisis:

Como se puede apreciar; aunque el 37% de los trabajadores deseche la información aun así ese no es el procedimiento para deshacerse de cierta información, el 27% procede a cumplir con el procedimiento, sin embargo, tanto el 23% que la sigue guardando y el 13% que la deja en cualquier lugar no procede a darle el tratamiento adecuado.

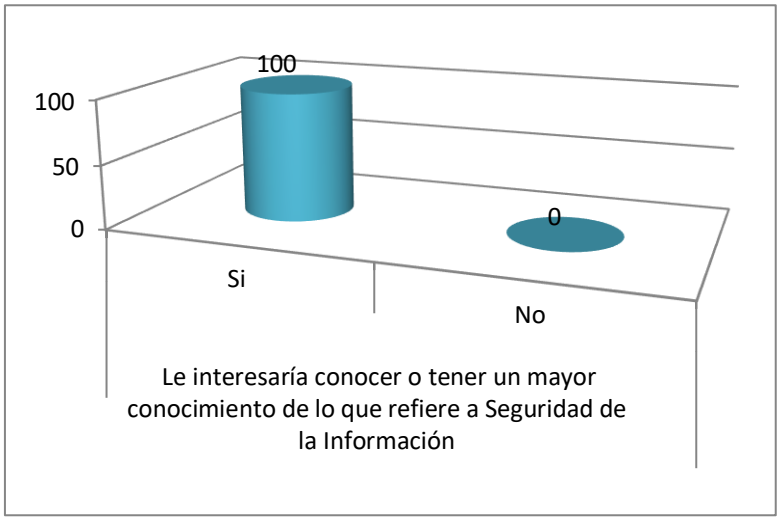
16.



Análisis:

Se puede ver que el 60 % si sabe diferenciar la clasificación de la información quedando un 40 % que un no sabe distinguir la información que es privada, interna o pública.

17.



Análisis:

En el grafico podemos observar que todos los trabajadores están interesados en conocersobre temas de seguridad de la información.

Análisis y discusión

El presente estudio fue realizado a la entidad financiera Caja Sullana, en donde se llevó a cabo la aplicación de la metodología de la norma ISO 27001, por lo que, de los antecedentes encontrados coincidimos con Montoya Pachas, N. K. (2012), su investigación brindó de apoyo en la consideración del diseño del Sistema de Gestión de Seguridad de la Información el cuál se basó en la misma Norma ISO 27001 de la presente investigación, por lo que les permitió gestionar la seguridad de sus activos con el objetivo de darles un tratamiento adecuado, ello nos permitió aplicarlo en esta investigación.

Además, se coincide con Villena Aguilar, M. A. (2006), aplicando de manera exitosa un modelo de Sistema de gestión de seguridad de la información (SGSI) en una entidad financiera peruana; coincidiendo en la aplicación de la investigación a una institución financiera, además de orientarnos en base a los 3 pilares en la seguridad de la información, tales como; confidencialidad, integridad y disponibilidad de sus activos de información.

Como soporte de la investigación de De la Cruz Guerrero, C. W. (2009), nos orientó como apoyo en relación de su marco teórico la cual destaca la base de sus antecedentes con investigaciones en Sistemas de Gestión de la Información; así como su análisis en riesgos y el alcance en la elaboración de las encuestas, guardando similitud en la gestión de la capacitación de las personas involucradas y las áreas que están directamente comprometidas en el desarrollo y la implementación del SGSI.

Finalmente, la presente investigación de Barragán, I., Góngora I., & Martínez, E. (2013), nos apoyó en el alcance del objetivo de sus políticas generales en seguridad de la información, y de las condiciones del uso de las claves de acceso como parte de las recomendaciones de las políticas de seguridad de la información.

Por otro lado se desarrolló la guía de las buenas prácticas para la Gestión de proyectos PMBOK, donde se consideró los procesos de dirección del proyecto de Inicio y Planificación, bajo el área de conocimiento de la Gestión de la Integración del Proyecto y la Gestión del Alcance del Proyecto y se obtuvo los entregables tales como;el Acta de Constitución del Proyecto, además del desarrollo de la EDT/WBS (Estructura Desagregada de Trabajo) el cual permitió subdividir el trabajo del proyecto en componentes más pequeños y manejables enfocados al objetivo del proyecto.

Conclusiones y recomendaciones

Conclusiones

En el desarrollo de la presente investigación fue fundamental realizar una serie de actividades lo cual nos permitió establecer el objetivo de la presente investigación. Culminado el desarrollo de la investigación se tuvo las siguientes conclusiones:

Se llevó a cabo entrevistas y encuestas a los usuarios y expertos del área de operaciones lo que su resultado nos permitió identificar el nivel del conocimiento de las Políticas de seguridad de la información de la institución, además de su nivel de compromiso con el mismo.

Se desarrolló la guía de las buenas prácticas para la Gestión de proyectos PMBOK, donde se consideró los procesos de dirección del proyecto de Inicio y Planificación, bajo el área de conocimiento de la Gestión de la Integración del Proyecto y la Gestión del Alcance del Proyecto y se obtuvo los entregables tales como; el Acta de Constitución del Proyecto, el cual presenta la autorización formal de la existencia del proyecto y la asignación de recursos para las actividades del proyecto; además del desarrollo de la EDT/WBS (Estructura Desagregada de Trabajo) el cual permitió subdividir el trabajo del proyecto en componentes más pequeños y manejables enfocados al objetivo del proyecto.

Se desarrolló un inventario de los activos de información pertenecientes o vinculados al área, lo que nos permitió la identificación de los activos más importantes del área, se documentó el modelo del Sistema de Gestión de Seguridad de la información basada en la Norma ISO 27001:2013, la documentación del Análisis de riesgo y de su Gestión de riesgo; además se desarrolló la Declaración de Aplicabilidad la cual nos permitió presentar las consideraciones de la mejoras de los procesos del área que fueron vulnerados y que se considera cuentan con cierto nivel de riesgo en sus procesos operativos.

Recomendaciones

Se recomienda la ejecución de una evaluación general a todo el personal de la institución; ya sea escrita o virtual con el fin de identificar el porcentaje de conocimiento de las políticas y procesos generales en seguridad de la información y así reforzar al personal con capacitaciones y evaluaciones periódicas para mejorar los niveles de conocimiento de este mismo.

Se recomienda dar a conocer a las respectivas áreas y Jefaturas inmediatas que intervienen en el Acta de constitución del Proyecto de las tareas que deberán realizar en el proceso de ejecución del proyecto indicando las fechas de compromiso.

Se recomienda llevar a cabo la actualización y publicación del documento del nuevo modelo Sistema de Gestión de Seguridad de la información basado en la norma ISO 27001:2013, por lo que existe dar la prioridad a las consideraciones que a la fecha presentan vulnerabilidad en la institución y mantener una constante revisión de la política del Sistema de Gestión de Seguridad de la Información y verificar el cumplimiento de la misma parte de los empleados de la institución, además de la existencia de cambios en los requisitos legales que impacten en el SGSI. Y finalmente se recomienda; formar, capacitar y promover el compromiso periódicamente al personal en temas de seguridad de la información.

Referencias bibliográficas

Montoya Pachas, N. k. (2012). *Diseño de un sistema de gestión de seguridad de información para un centro cultural binacional.* (Tesis de título) Pontificia Universidad Católica del Perú. Recuperado de: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5005/MONTOYA_NELSON_DISE%C3%91O_SISTEMA_GESTION_SEGURIDAD_INFORMACION_CENTRO_CULTURAL_BINACIONAL.pdf?sequence=1

Villena Aguilar, M. A. (2006). *Sistema de gestión de seguridad de información para una institución financiera.* (Tesis de título) Pontificia Universidad Católica del Perú. Lima. Recuperado de: http://m.tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/362/villena_mois%c3%89s_sistema_de%20gesti%c3%93n_de_seguridad_de_informaci%c3%93n_para_una_instituci%c3%93n_financiera.pdf?sequence=1

De la Cruz Guerrero, C. W. (2009). *Elaboración Y Aplicación de un Sistema de gestión de la Seguridad de La Información (SGSI) para la realidad tecnológica de la USAT* (Tesis de título) Universidad Católica Santo Toribio De Mogrovejo. Chiclayo. Recuperado de : https://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBwQFjAA&url=http%3A%2F%2Fcip.org.pe%2Fimagenes%2Ftemp%2Ftesis%2F42464064.doc&ei=wLRkVeC1KMWrNsS_gE&usg=AFQjCNEj6q1oWgHRBksZ1cWqhFq8ZChRrA&bvm=bv.93990622,d.eXY

Barragán, I. , Góngora I., & Martínez, E. (2013). *Implementación de políticas de seguridad informática para la M.I. municipalidad de Guayaquil aplicando la norma iso/iec 27002*. (Tesis de título) Escuela Superior Politécnica del Litoral) Guayaquil, Ecuador.

Recuperado de: http://www.dspace.espol.edu.ec/bitstream/123456789/21546/2/ManualTopico.pf

Aguirre Cardona, J. D., Y Aristizabal Betancourt, C. (2013). *Diseño del sistema de gestión de seguridad de la información para el Grupo Empresarial La Ofrenda.* (Proyecto de grado) Universidad tecnológica de Pereira. Colombia.

Recuperado de: http://repositorio.utp.edu.co/dspace/bitstream/11059/4117/1/0058A284.pdf

Aguirre Mollehuanca, D. A. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.* (Tesis de título) Pontificia Universidad Católica del Perú.

Recuperado de: http://tesis.pucp.edu.pe/repositorio/handle/123456789/5677

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

Recuperado de: http://tesis.pucp.edu.pe/repositorio/handle/123456789/4957?show=full

Superintendencia de Banca, Seguros y AFP (2009). Circular G140-2009-SBS

Recuperado de:

http://intranet1.sbs.gob.pe/IDXALL/FINANCIERO/DOC/CIRCULAR/PDF/G-140-2009.C.PDF

Apéndices y anexos

Anexo 01: Entrevista Sobre Seguridad De La Información

Dirigido al Jefe del Área de Seguridad Corporativa de la Caja Sullana.

1. ¿La Caja Sullana cuenta con un comité de seguridad de la información?

SI ( )

Las funciones del comité se encuentran detalladas en el manual de funciones y organización u otro documento

_____

¿Quién conforma ese comité?

_____

¿Ese comité es plenamente identificable por los usuarios de la Caja Sullana?

_____

NO ( )

Si no cuentan con ese comité; ¿Quiénes son los encargados de establecer las políticas de seguridad de la información?

_____

O, ¿Sólo las políticas son establecidas por sí mismo como jefe del área de seguridad Corporativa?

_____

¿Estas políticas son conocidas por todos los usuarios?

_____

¿A través de que medio se les dio a conocer?

_____

2. ¿Existe algún tipo de manual o documento donde se especifique los controles para la seguridad de la información?

   _____

3. ¿De qué manera controla a sus trabajadores y todo el personal, con respecto al tema de seguridad de la información?

   _____

4. ¿De qué forma controla los accesos a la red y quién ordena que se genere esos permisos?_____

5. ¿Se registran los accesos de personas a las áreas donde se encuentran los equipos servidores?_____

6. ¿Existe un documento donde se especifique las políticas de seguridad de la información?

   SI ( )

   ¿Quién elaboró ese documento y por quién fue aprobado?

   _____

   ¿Los usuarios conocen este documento?

   _____

   ¿Se aplican estas políticas a todo el personal de Caja Sullana?

   _____

   ¿Cada que tiempo se revisan esas políticas?

   _____

   NO ( )

   ¿Según Usted, a que cree que se deba, que hasta ahora no se implementa las políticas de seguridad de la información en Caja Sullana?

   _____

   ¿Cree Usted, que es de suma urgencia la elaboración de políticas de seguridad de la información para la Caja Sullana?

   _____

Porqué_____

Y para su área_____

7. Frente a cualquier desastre natural, provocado o humano ¿Su personal conoce cuales son los activos más importantes que debe proteger en relación a la información?

SI ( )

¿Para ello existen procedimientos documentados para actuar antes, durante y después del desastre?_____

¿Ha realizado algún simulacro con defensa civil o tiene previsto hacerlo en el futuro?

_____

Lo cree necesario hacerlo con esta organización_____

¿Su área posee algún plan de contingencia, si no lo tiene ha motivado a sus trabajadores para elaborarlo?

_____

NO ( )

¿A qué se debe?_____

8. ¿Cuáles son los errores más comunes cando se usa internet y correo electrónico?

_____

9. ¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información?

MF: Muy frecuente RF: Regularmente frecuente PF: Poco frecuente

Riesgos	MF	RF	PF
Fenómenos Naturales (Terremotos, Inundaciones)			
Fallas mecánicas (Cortes de fluido eléctrico, incendios)			
Divulgación ilícita de la información por el personal			
Destrucción o modificación de la información por el personal			
Intrusos al sistema de la red Virus informáticos, gusanos, spam			
Otros:			

10. ¿Los equipos de cómputo en el área tienen fuente de poder ininterrumpible (UPS),

generadores de energía, baterías ante cortes de energía eléctrica?

_____

11. ¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?

    _____

12. ¿Quiénes se encargan de capacitar al personal sobre seguridad de la Información?

    _____

13. ¿A Usted se le brinda capacitación por parte de la Caja Sullana acerca de seguridad de la información?

    Si ( ) No ( )

    Si la respuesta es **Sí;** Cada que tiempo y quien se encarga de hacerlo

    _____

    En caso contrario, ¿cómo se capacitan?

    _____

14. ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?

    _____

15. ¿A qué área se le debe se comunicar oportunamente los incidentes de seguridad detectados?

    _____

16. ¿Cuáles son sus recomendaciones al personal de la Caja Sullana (Área de Operaciones) para un buen uso de la información?

    _____

Anexo 02: Encuesta sobre Seguridad de La Información

1. ¿En Caja Sullana cuentan con políticas de seguridad de la información?

   Si ( ) No lo sé ( ) No ( )

2. ¿Si en la Pregunta 1 respondió si, Se cumplen o se llevan a la práctica estas políticas?

   Si ( ) A veces ( ) No ( )

3. ¿Conoce las políticas de seguridad de la información?

   Si ( ) Algunas ( ) No ( )

4. ¿Cuándo fue la última vez que asistió a un taller o capacitación sobre seguridad de la información?

   Hace 3 meses ( ) Hace 6 meses ( ) Hace 1 año ( ) Nunca ( )

5. Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información

   Si ( ) No ( )

6. Si le interesaría conocer más acerca del tema de Seguridad de la Información, a través de que medio te gustaría ser informado:

   a) Folletos y boletines
   b) Capacitaciones, Charlas o conferencias
   c) Como parte de algún curso en tu carrera

7. ¿Puede identificar a las personas que no trabajan en la Caja Sullana?

   Si ( ) A Veces ( ) No ( )

   Si tu respuesta es **sí,** fue por medio de:

   a. Fotocheck de la empresa en que trabaja ( )
   b. Fotocheck de visitante (entregado por la Caja Sullana) ( )
   c. Otros, Especificar**…….** ( )

8. ¿Has observado que algún compañero ha bebido líquidos o ingerido algún alimento cuando realiza algún trabajo en cualquiera de las computadoras de la Caja Sullana?

   Siempre ( ) A veces ( ) Nunca ( )

9. ¿Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro de la Caja Sullana?

   Si ( ) A veces ( ) No ( )

10. ¿Tu clave de acceso es la misma para todos los sistemas con los que cuenta el área de Operaciones - Caja Sullana?

    Si ( ) La mayoría ( ) No ( )

    Normalmente tu clave hace referencia a:

    a. Tu nombre y apellido ( )
    b. Tú fecha de nacimiento ( )
    c. Teléfono (de casa o móvil) ( )
    d. Nombre de tu enamorada o enamorado ( )
    e. Otros, Especifique**……..** ( )

    Y si nunca cambiaste tu clave, cuál es y porque motivo no lo hiciste

    ……

11. ¿Ud. cambia con frecuencia sus Claves de los sistemas de la Caja Sullana?

    Siempre ( ) A veces ( ) Nunca ( )

12. ¿Comparte sus claves de acceso con sus compañeros de trabajo?

    Siempre ( ) A veces ( ) Nunca ( )

13. ¿Usted ha utilizado alguna Laptop dentro de la Caja Sullana?

    Siempre ( ) A veces ( ) Nunca ( )

Si su respuesta es Afirmativa; Ha recibido algún mensaje en el cual le comunique que su equipo ha sido registrado y puede acceder a la red

Siempre ( ) A veces ( ) Nunca ( )

14. ¿Todos los empleados deben portar su identificación visible durante su permanencia en el centro de labores?

Siempre ( ) A veces ( ) Nunca ( )

15. ¿La responsabilidad por la seguridad de la información debe ser una obligación diaria de quién?

Sólo Jefes ( ) Todo el personal ( ) Área de seguridad Corporativa ( )

16. ¿Cuándo se ausenta de su oficina deja bloqueada la PC?

Siempre ( ) A veces ( ) Nunca ( )

17. ¿Cuándo se ausenta de su oficina deja documentación visible en su escritorio?

Siempre ( ) A veces ( ) Nunca ( )

18. ¿Qué es lo que hace con la información que ya no necesita?

a. La sigue guardando ( )
b. La deja en cualquier lugar ( )
c. La desecha ( )
d. La tritura o rompe antes de desecharla ( )
e. Otros Explicar.....( )

19. ¿Usted apaga los equipos informáticos debidamente después de utilizarlos?

Siempre ( ) A veces ( ) Nunca ( )

Si tu respuesta es afirmativa, ¿Cómo apaga el equipo después de trabajar?

a. Apagando directamente el estabilizador. ( )
b. Manteniendo presionando el botón de apagado del CPU. ( )
c. Haciendo clic en el botón de apagado del menú del sistema operativo. ( )

20. Cada vez que sufre algún inconveniente con la PC o aplicación (sistemas) con el cual se desea trabajar, ¿Por qué medio informa o reporta el inconveniente?

a. Teléfono (anexo) ( )
b. Correo electrónico al área de Sistemas ( )

c. Voy físicamente a buscar algún encargado de cómputo ( )
d. Espero que pasen por mi área de trabajo ( )
e. Mesa de Servicios ( )
f. Otros, Especifique…… ( )

21. ¿Has manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, mouse y conexiones de red que conectan al CPU para hacerlos funcionar?

Siempre ( ) A veces ( ) Nunca ( )

22. ¿Con qué frecuencia solicita que le revisen su PC frente a cualquier falla?

Siempre ( ) A veces ( ) Nunca ( )

23. ¿Su PC tiene acceso a los dispositivos de almacenamiento?

Si ( ) No lo sé ( ) No ( )

Si la respuesta es Si, a que dispositivos tiene acceso

…….

24. ¿Has utilizado algún dispositivo externo para extraer algún tipo de información de trabajo o de su interés?

Siempre ( ) A veces ( ) Nunca ( )

Si la respuesta es afirmativa; ¿Cuál fue el medio que utilizo para extraer dicha información?

a. Memoria USB ( )
b. CD ( )
c. DVD ( )
d. Otros ( )

25. ¿Cuenta con correo electrónico?

Si ( ) No ( )

Si su respuesta es **sí;** Que uso le da:

a. Sólo para asuntos Laborales ( )
b. Para asuntos personales ( )

c. Para ambos asuntos (Personales, Laborales) ( )

d. Otros, Especificar… .....( )

26. ¿Qué haría si recibe un e-mail externo donde se solicita información de carácter personal?

a. No responder e informar al área correspondiente ( )
b. Responder ante lo que solicitan ( )
c. No le doy importancia ( )
d. Otros , Especificar…… ( )

27. ¿Qué recomienda para hacer el uso adecuado del internet de Caja Sullana?

a. Realizar descargar, pero de sitios que sean confiables ( )
b. No realizar descargas de música, programas entre otros. ( )
c. Otros, Especificar…… ( )

28. ¿Usted ha detectado que el antivirus de la Caja Sullana funciona adecuadamente y que se encuentra actualizado?

Si ( ) No ( )

29. ¿De acuerdo a su perfil, cuenta con todos los accesos asignados para poder realizar sus labores diarias?

a. Si, cuento con todo lo necesario de acuerdo a mi perfil ( )
b. Sí, pero también tengo accesos designados que no me corresponde según mi perfil. ( )

30. ¿Reconoce Ud. Cuáles son los activos importantes de la Caja Sullana dentro del área de operaciones?

Si ( ) Algunos ( ) No ( )

31. ¿La información, ya sea documentos entre otros que es de uso interno debe ser divulgada a terceras personas?

Si ( ) No lo sé ( ) No ( )

32. ¿Ud. sabe distinguir la información que es de estrictamente confidencial, de uso interno o publica?

Si ( ) No ( )

33. ¿Se cuenta con servicio de vigilancia, personas y/o videocámaras?

a) Solo Vigilante ( )
b) Solo videocámaras ( )
c) Ambos ( )

34. Existe alarma para:

a) Detectar fuego (calor o humo) en forma automática ( )

b) Avisar en forma manual la presencia del fuego ( )

b) Otros (Robo) ( )

d) Existen alarmas para fuego y robos ( )

d) No existe

RESULTADOS DE LA ENCUSTA DIRIGIDA AL PERSONAL DEL AREA DE OPERACIONES DE LA CAJA SULLANA

1. ¿En Caja Sullana cuentan con políticas de seguridad de la información?

Opción	Frecuencia	Porcentaje %
Si	23	77
No lo se	4	13
No	3	10
Total	30	100

2. ¿Si en la Pregunta 1 respondió si, Se cumplen o se llevan a la práctica estas políticas?

Opción	Frecuencia	Porcentaje %
Si	5	22
A veces	7	30
No	11	48
Total	23	100

3. ¿Conoce las políticas de seguridad de la información?

Opción	Frecuencia	Porcentaje %
Si	2	7
Algunas	8	26
No	20	67
Total	30	100

4. ¿Cuándo fue la última vez que asistió a un taller o capacitación sobre seguridad de la información?

Opción	Frecuencia	Porcentaje %
Hace 3 meses	4	13
Hace 6 meses	12	40
Hace 1 año	11	37
Nunca	3	10
Total	30	100

5. Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información

Opción	Frecuencia	Porcentaje %
Si	30	100
No	0	0
Total	30	100

6. Si le interesaría conocer más acerca del tema de Seguridad de la Información, a través de que medio te gustaría ser informado:

Opción	Frecuencia	Porcentaje %
Folletos y boletines	5	17
Capacitaciones, Charlas o conferencias	12	40
Como parte de algún curso en tu carrera	13	43
Total	30	100

7. ¿Puede identificar a las personas que no trabajan en la Caja Sullana?

Opción	Frecuencia	Porcentaje %
Si	18	60
A Veces	4	13
No	8	27
Total	30	100

Si tu respuesta es **sí,** fue por medio de:

Opción	Frecuencia	Porcentaje %
Fotocheck de la empresa en que trabaja	12	67
Fotocheck de visitante (entregado por la Caja Sullana)	2	11
Otros, Especificar	4	22
Total	18	100

8. ¿Has observado que algún compañero ha bebido líquidos o ingerido algún alimento cuando realiza algún trabajo en cualquiera de las computadoras de la Caja Sullana?

Opción	Frecuencia	Porcentaje %
Siempre	20	67
A Veces	7	23
Nunca	3	10
Total	30	100

9. ¿Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro de la Caja Sullana?

Opción	Frecuencia	Porcentaje %
Si	12	40
A Veces	7	23
No	11	37
Total	30	100

10. ¿Tu clave de acceso es la misma para todos los sistemas con los que cuenta el área de Operaciones - Caja Sullana?

Opción	Frecuencia	Porcentaje %
Si	12	40
La mayoría	14	47
No	4	13
Total	30	100

Normalmente tu clave hace referencia a:

Opción	Frecuencia	Porcentaje %
Tu nombre y apellido	6	20
Tú fecha de nacimiento	4	13
Teléfono (de casa o móvil)	2	7
Nombre de tu enamorada o enamorado	1	3
Otros, Especificar	17	57
Total	30	100

11. ¿Usted cambia con frecuencia sus Claves de los sistemas de la Caja Sullana?

Opción	Frecuencia	Porcentaje %
Siempre	8	27
A veces	12	40
Nunca	10	33
Total	30	100

12. ¿Comparte sus claves de acceso con sus compañeros de trabajo?

Opción	Frecuencia	Porcentaje %
Siempre	10	33
A Veces	11	37
Nunca	9	30
Total	30	100

13. ¿Usted ha utilizado alguna Laptop dentro de la Caja Sullana?

Opción	Frecuencia	Porcentaje %
Siempre	0	0
A Veces	0	0
Nunca	30	100
Total	30	100

Si su respuesta es afirmativa; Ud. presento algún inconveniente al momento de ingresar a las instalaciones de Caja Sullana.

Opción	Frecuencia	Porcentaje %
Siempre		
A Veces		
Nunca		
Total		

14. ¿Todos los empleados deben portar su identificación visible durante su permanencia en el centro de labores?

Opción	Frecuencia	Porcentaje %
Siempre	21	70
A Veces	7	23
Nunca	2	7
Total	30	100

15. ¿La responsabilidad por la seguridad de la información debe ser una obligación diaria de quién?

Opción	Frecuencia	Porcentaje %
Solo Jefes	8	27
Todo el Personal	10	33
Área de Seguridad Corporativa	12	40
Total	30	100

16. ¿Cuándo se ausenta de su oficina deja bloqueada su PC?

Opción	Frecuencia	Porcentaje %
Siempre	11	36
A Veces	14	47
Nunca	5	17
Total	30	100

17. ¿Cuándo se ausenta de su oficina deja documentación visible en su escritorio?

Opción	Frecuencia	Porcentaje %
Siempre	15	50
A Veces	9	30
Nunca	6	20
Total	30	100

18. ¿Qué es lo que hace con la información que ya no necesita?

Opción	Frecuencia	Porcentaje %
La sigue guardando	7	23
La deja en cualquier lugar	4	13
La desecha	11	37
La tritura o rompe antes de desecharla	8	27
Total	30	100

19. ¿Usted apaga los equipos informáticos debidamente después de utilizarlos?

Opción	Frecuencia	Porcentaje %
Siempre	19	63
A Veces	9	30
Nunca	2	7
Total	30	100

Si tu respuesta es afirmativa, ¿Cómo apagás tu equipo después de trabajar?

Opción	Frecuencia	Porcentaje %
Apagando directamente el estabilizador	1	5
Manteniendo presionando el botón de apagado del CPU.	2	11
Haciendo clic en el botón de apagado del menú del sistema operativo.	16	84
Total	19	100

20. Cada vez que sufre algún inconveniente con la PC o aplicación (sistemas) con el cual se desea trabajar, ¿Por qué medio informa o reporta el inconveniente?

Opción	Frecuencia	Porcentaje %
Teléfono (anexo)	14	47
Correo electrónico al área de Sistemas	3	10
Voy físicamente a buscar algún encargado de cómputo	1	3
Espero que pasen por mi área de trabajo	1	3
Mesa de Servicios	9	30
Otros, Especificar	2	7
Total	30	100

21. ¿Has manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, Mouse y conexiones de red que conectan al CPU para hacerlos funcionar?

Opción	Frecuencia	Porcentaje %
Siempre	22	73
A Veces	6	20
Nunca	2	7
Total	30	100

22. ¿Con qué frecuencia solicita que le revisen su PC frente a cualquier falla?

Opción	Frecuencia	Porcentaje %
Siempre	10	33
A Veces	12	40
Nunca	8	27
Total	30	100

23. ¿Su PC tiene acceso a los dispositivos de almacenamiento?

Opción	Frecuencia	Porcentaje %
Si	5	17
No lo se	7	23
No	18	60
Total	30	100

24. ¿Has utilizado algún dispositivo externo para extraer algún tipo de información de trabajo o de su interés?

Opción	Frecuencia	Porcentaje %
Siempre	9	30
A veces	11	37
Nunca	10	33
Total	30	100

Si la respuesta es afirmativa, cual fue el medio que utilizo para extraer dicha información

Opción	Frecuencia	Porcentaje %
Memoria USB	13	65
CD	2	10
DVD	1	5
Otros	4	20
Total	20	100

25. ¿Cuenta con correo electrónico?

Opción	Frecuencia	Porcentaje %
Si	22	73
No	8	27
Total	30	100

Si su respuesta es **sí;** Que uso le da:

Opción	Frecuencia	Porcentaje %
Solo para asuntos Laborales	10	45
Para asuntos personales	3	14
Para ambos asuntos	9	41
Total	22	100

26. ¿Qué harías si recibe un e-mail externo donde se solicita información de carácter personal?

Opción	Frecuencia	Porcentaje %
No responder e informar al área correspondiente.	9	30
Responder ante lo que solicitan	2	7
No le doy importancia	15	50
Otros, Especificar	4	13
Total	30	100

27. ¿Qué recomienda para hacer el uso adecuado del internet de Caja Sullana?

Opción	Frecuencia	Porcentaje %
Realizar descargas, pero de sitios que sean confiables.	12	40
No realizar descargas de música, programas entre otros.	10	33
Otros	8	27
Total	30	100

28. ¿Usted ha detectado que el antivirus de la Caja Sullana funciona adecuadamente y que se encuentra actualizado?

Opción	Frecuencia	Porcentaje %
Si	22	73
No	8	27
Total	30	100

29. ¿De acuerdo a su perfil, cuenta con todos los accesos asignados para poder realizar sus labores diarias?

Opción	Frecuencia	Porcentaje %
Si, cuento con todo lo necesario de acuerdo a mi perfil	19	63
Sí, pero también tengo accesos designados que no me corresponde según mi perfil	11	37
Total	30	100

30. Reconoce Usted, ¿Cuáles son los activos importantes de la Caja Sullana dentro del área de operaciones?

Opción	Frecuencia	Porcentaje %
Si	10	33
Algunos	12	40
No	8	27
Total	30	100

31. ¿La información, ya sea documentos entre otros que es de uso interno debe ser divulgada a terceras personas?

Opción	Frecuencia	Porcentaje %
Si	6	20
No lo se	11	37
No	13	43
Total	30	100

32. ¿Ud. sabe distinguir la información que es estrictamente confidencial, de uso interno o publica?

Opción	Frecuencia	Porcentaje %
Si	18	60
No	12	40
Total	30	100

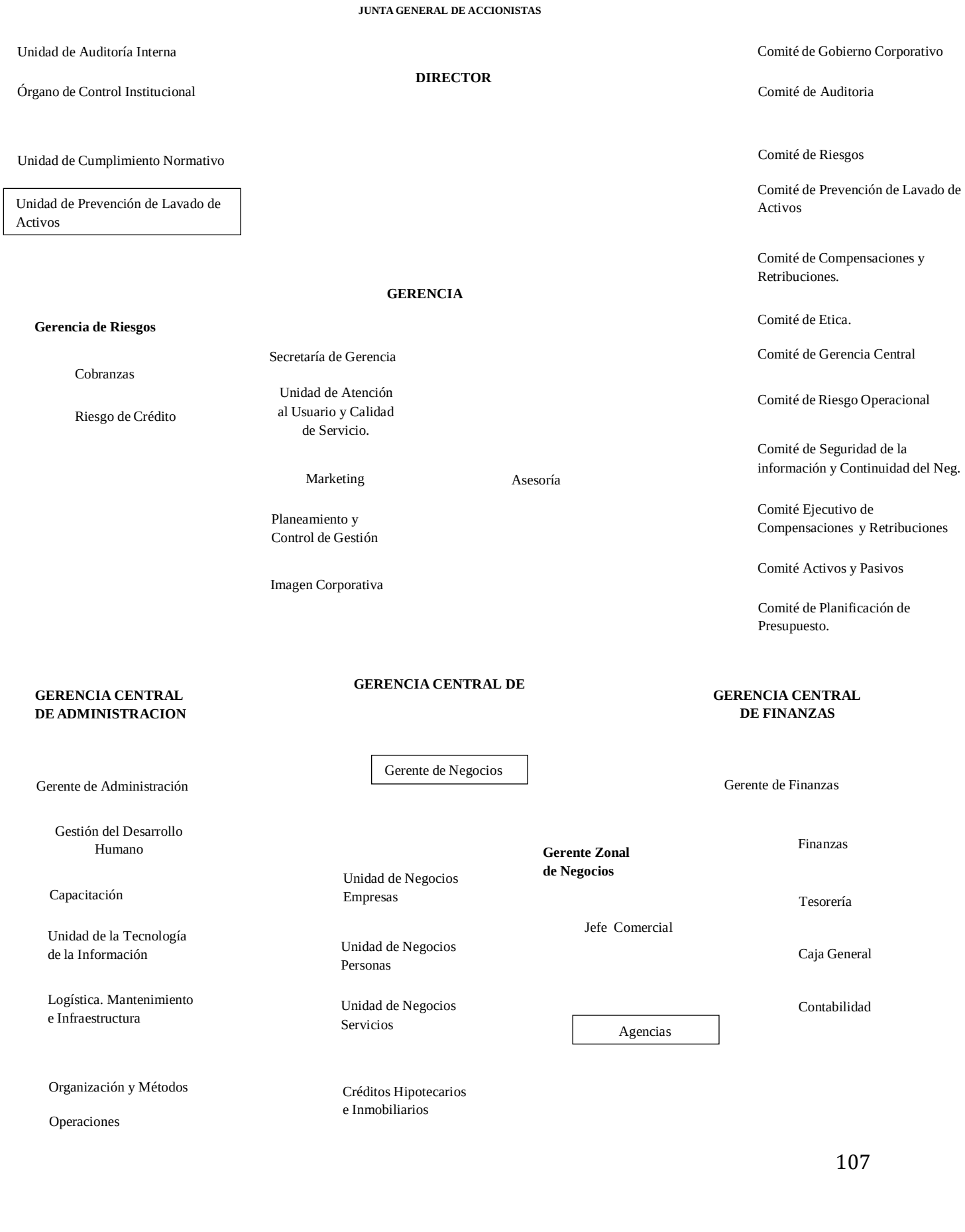
33. ¿Se cuenta con servicio de vigilancia, personas y/o videocámaras?

Opción	Frecuencia	Porcentaje %
Solo vigilante	9	30
Solo videocámaras	1	3
Ambos	20	67
Total	30	100

34. Existe alarma para:

Opción	Frecuencia	Porcentaje %
Detectar fuego (calor o humo) en forma automática	10	33
Avisar en forma manual la presencia del fuego	0	0
Otros (Robo)	6	20
Existen alarmas para fuego y robos.	14	47
No existe	0	0
Total	30	100

Anexo 03: Organigrama de la Empresa



Seguridad Corporativa.