UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

CARRERA: INGENIERÍA DE SISTEMAS

Trabajo previa a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:

ANÁLISIS EN SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001- SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DIRIGIDO A UNA EMPRESA DE SERVICIOS FINANCIEROS.

AUTORES:
KELLY GABRIELA BERMÚDEZ MOLINA
EDBER RAFAEL BAILÓN SÁNCHEZ

DIRECTOR:
ING. JOFFRE LUIS LEÓN VEAS

Guayaquil, marzo de 2015

DECLARACIÓN DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Nosotros Kelly Bermúdez Molina y Rafael Bailón Sánchez autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Srta. Kelly Bermúdez Molina	Sr. Edber Bailón Sánchez
CC: 0930063540	CC: 0915121321

DEDICATORIA

A Dios, porque tanto me ama que me dio pilares fuertes y sólidos para que pueda construir mi base de vida, por ser mi fuerza espiritual, mi guía, por regalarme cada día el milagro de la vida y permitir así luchar por mis sueños.

A mi mami, por estar en todas conmigo, por ser incondicional y nunca bajar los brazos, a ella le dedico mi esfuerzo, mi dedicación, mis malas noches, mis logros y todo mi trabajo.

A mi papá por su apoyo, por su comprensión, por estar conmigo cuando sentía miedo, por las noches de cuentos, y porque a pesar de la distancia sé que me ama tanto como yo lo amo a él.

A mi gran amor, por ser mí complemento ideal, porque durante todos estos años no pude encontrar mejor compañero, amigo, profesional y novio que él.

A mis abuelitos que están en el cielo y a los que están aún con vida, porque con sus enseñanzas, amor, palabras y abrazos oportunos me hicieron sentir siempre respaldada.

Y finalmente a mi segundo papá porque su apoyo, y su disposición en ayudarme siempre, sus acciones me permitieron darme cuenta que me había convertido en su hija de corazón.

A todos ellos que son y serán mis pilares durante toda mi vida, les dedico este logro, porque cada uno de ellos supo quererme y apoyarme a su manera. Gracias por todos ellos porque creyeron en mí, incluso cuando ni yo misma lo hice. Los amo y sé que ustedes lo saben.

Kelly Bermúdez Molina

DEDICATORIA

Para obtener grandes resultados, hay que realizar grandes sacrificios.

El tiempo es algo que no podemos retomar de nuestras vidas, y lo que a menudo no se considera importante.

A lo largo de varios años donde obtuve los fundamentos para lograr muchos objetivos, entre unos de esos el trabajo aquí presente, también se realizó con tiempo y apoyo de los tres soportes principales en mi vida, gracias por el inmenso sacrificio que realizaron por mí.

Agradezco a Dios por darme las oportunidades, salud y sabiduría para tomar decisiones.

A mi madre por acompañarme, cuidarme y comprenderme en todo momento

A mi hermana por mostrarme que estudiando se pueden conseguir varias metas y ser felices por aquello.

A mi mejor amiga Gaby, que juntos lograremos lo inalcanzable en nuestras vidas.

A mi familia en general por el apoyo incondicional.

Edber Rafael Bailón Sánchez

AGRADECIMIENTO

Agradecemos a todas las personas que directa o indirectamente colaboraron para la elaboración de la presente tesis, entre las cuales podemos nombrar:

Ing. Soledad Camposano, Gerente de Sistemas de la empresa Credigestión, por la apertura para el desarrollo de la investigación dentro de la empresa.

A la Universidad Politécnica Salesiana por el nivel de educación implementada en la institución, que permite formar profesionales con valores.

A los diferentes profesores que durante todos estos años nos impartieron sus valores, experiencias y conocimientos, permitiéndonos crecer en lo profesional y en lo personal.

Y a nuestro director de tesis, el Ing. Joffre León Veas, por su ayuda en el aporte con sus conocimientos a lo largo del desarrollo del trabajo de tesis.

Kelly Gabriela Bermúdez Molina
Edber Rafael Bailón Sánchez

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

Mediante la elaboración del análisis de seguridad de la información y seguridad informática basada en la norma ISO/IEC 27001, el presente trabajo tuvo como finalidad conocer las vulnerabilidades a las que está expuesta la información por la falta de aplicación de controles de seguridad.

El análisis estuvo dirigido a una empresa financiera, teniendo como objetivo principal el estudio de seguridad en los procesos críticos. A través de reuniones, revisión de documentación, consultas, observación, encuestas y ejecución de entrevistas con directivos que poseen un amplio conocimiento del negocio, se logró identificar los riesgos actuales a los que se exponen los datos tanto físicos, lógicos y sistemas de procesamiento de información.

La ejecución del análisis de riesgos da a conocer el nivel de impacto que tendría la ocurrencia de las amenazas identificadas en cada activo de la información que pueden afectar datos relevantes utilizados o resultantes de la ejecución de las actividades propias del negocio.

Los resultados obtenidos dan a conocer que, para minimizar los riesgos existentes, es necesario implementar controles de seguridad, lo cual ayuda a fortalecer tres aspectos importantes: la confidencialidad, integridad y disponibilidad de la información. Pero los resultados también muestran la importancia del compromiso y trabajo en equipo que debe tener la empresa.

ABSTRACT

By developing the analysis of information security and information security based on ISO / IEC 27001, this study was established on identify the vulnerabilities which information is exposed because of the lack of implementation of security controls.

The analysis was aimed to a financial company, having as main objective the study of safety risk over critical processes. Through meetings, documentation review, consultations, observation, surveys and execution of interviews with managers who have extensive knowledge of the business, it was possible to identify the current risks, which physical data, logic and processing systems are exposed to.

The implementation of risk analysis discloses the level of impact that the occurrence of the threats identified in each asset of the relevant information being used or as a result of the executions on business activities.

The results disclosed that, to minimize the risks, it is necessary to implement security controls, which helps to strengthen three important aspects: confidentiality, integrity and availability of information. But the results also show the importance of commitment and teamwork that the company should have.

INTRODUCCIÓN

En la actualidad toda empresa se basa en la información para tomar decisiones que permitan la continuidad del negocio, transformándose así en un activo importante para las organizaciones, siendo necesario protegerla ante cualquier evento que puede causar corrupción en los datos. Dada la importancia de la información, organizaciones internacionales de estandarización han elaborado normas de buenas prácticas para el resguardo y buen uso de la información y de los activos en general.

El presente trabajo de Análisis en Seguridad Informática y Seguridad de la Información basado en la Norma ISO/IEC 27001, está dirigido hacia la empresa Credigestión S.A; en el afán de aplicar mejores prácticas en la gestión de la seguridad de la información, se prioriza como objetivo general el análisis de seguridad en los procesos críticos de la empresa.

El desarrollo del tema de tesis se formuló bajo las directrices que se especifican en la norma ISO/IEC 27001 para la gestión de seguridad de la información, teniendo el objetivo de disminuir el riesgo identificado, mediante procedimientos establecidos sistemáticamente.

En el primer capítulo se encuentra detallado los principales factores que motivaron a la realización de este análisis. En el segundo capítulo se describe el diccionario de palabras que ayudan a comprender el significado de cada término utilizado, así como las situaciones que han ocurrido en referencia a la seguridad de la información.

Las modalidades y tipos de investigación utilizados se describen en el tercer capítulo, en el cual también se definió el número de funcionarios que aportaron en la investigación. En esta sección se destaca los mecanismos que se utilizan para la recolección y procesamiento de la información.

Uno de los capítulos más importantes de esta investigación consistió en la ejecución del análisis de la situación actual y el análisis de riesgo en el que se determinó las amenazas a las que están expuestos los activos de la empresa. Se ha empleado una metodología de gestión de riesgos que puede ser aplicada a cualquier empresa sin

importar el giro de negocio que posea, pues se basa en la identificación de los activos de información propios de la empresa.

En este estudio se presentan la matriz de activos, matriz de riesgo calculado en base a las vulnerabilidades encontradas, el impacto y probabilidad de ocurrencia de las áreas críticas de la empresa nombradas así debido a la importancia que desempeña cada entidad en los procesos de la empresa, donde el flujo de la información es constante y se requiere la disponibilidad de la información inmediata. Todas las conclusiones y recomendaciones se basan en lo anteriormente descrito.

Finalmente se propone una metodología de implementación, tomando en cuenta lo indicado en la norma ISO/IEC 27001 y de acuerdo a la realidad de aplicación dentro de la empresa a la cual se dirigió la investigación.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1. Enunciado del Problema

1.1.1. Factores Estructurales

Credigestión es una empresa de mediana escala en el mercado financiero, tiene como proceso crítico del negocio la gestión de crédito y cobranza de cartera, siendo su objetivo facilitar el proceso integral del crédito para sus clientes. En los últimos años la empresa ha crecido considerablemente, ganando competencia y experiencia, de tal forma que ha obtenido una destacable presencia local.

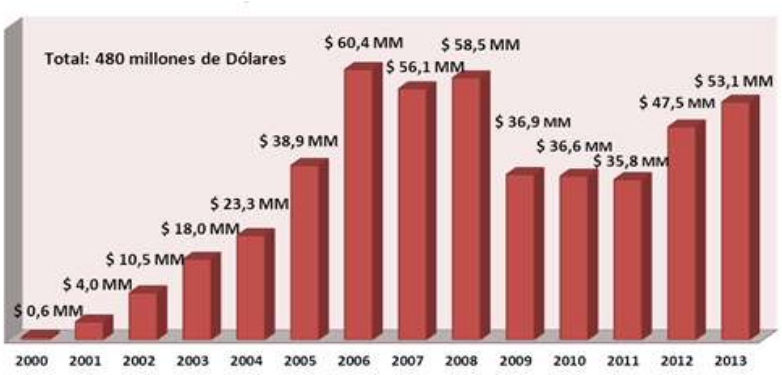

Figura 1. Cartera Recuperada desde el 2000 al 2013
(Credigestión, 2013)

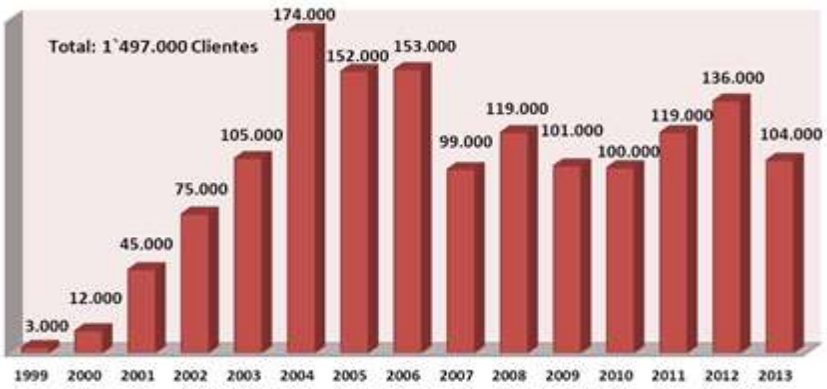

Figura 2. Clientes Verificados y Calificados desde el 1999 al 2013
(Credigestión, 2013)

Credigestión lleva a cabo sus operaciones en las ciudades de Guayaquil (matriz principal) y Quito (Sucursal), está conformada por 230 empleados a nivel nacional, los cuales de dividen de la siguiente manera:

- Presidente ejecutivo, Vicepresidente ejecutivo, Vicepresidente de tecnologías de información, Subgerente de operaciones, Gerente de sucursal de Quito.
- Doce personas entre Supervisores, Recepcionistas, Cajeras, Personal de apoyo
- 204 son personal operativo.

Estructura	Guayaquil	Quito	Total
Gestores Telefónicos	92	29	121
Digitadores	25	3	28
Personal Terreno	42	13	55
Total	**159**	**45**	**204**

Figura 3. Estructura de funcionarios a nivel nacional
(Credigestión, 2013)

La gestión de las operaciones que realiza Credigestión se llevan a cabo a través de medios automatizados, tanto el flujo de registro de transacciones como información propia de los clientes. Al igual que las empresas de prestación de servicios financieros, Credigestión contribuyen al flujo de capital obteniendo su principal fuente generadora de recursos a través del dinero debido a los movimientos y transacciones que se efectúen del mismo. Juegan un papel relevante en la economía local ya que son facilitadoras de capital inmediato que contribuyen al impulso de crecimiento o inversión, dando origen al intercambio comercial.

A pesar de que la empresa se mantiene estable en sus operaciones, nace la necesidad de empezar a gestionar controles de seguridad, para poder garantizar que la información no será alterada o manejada por personas no autorizadas, actualmente no cuenta con un área de Seguridad Informática por lo que no han realizado ninguna acción para empezar a mitigar los temas relacionados con seguridad informática y seguridad de la información.

La falta de lineamientos de seguridad no permite tener el control adecuado del manejo y los accesos a los sistemas de procesamiento de información, abriendo la posibilidad de que la información manejada sea utilizada para fines que perjudiquen a la empresa. De continuar bajo la misma línea de gestión con respecto a la seguridad, la empresa puede ser susceptible a la ocurrencia de cualquier incidente de seguridad que perjudique las operaciones del negocio.

1.1.2. Factores Intermedios

Durante el último año se han presentado incidentes de seguridad que han generado molestias en los funcionarios y han sido causa de interrupciones de las actividades que se desarrollan dentro de la empresa, por esta razón se necesita implementar lineamientos de seguridad en las áreas donde se desarrollan los procesos críticos del negocio, de tal forma que puedan garantizar la confidencialidad, disponibilidad e integridad de la información, mitigando riesgos que puedan ocasionar retrasos en las actividades o incluso la ocurrencia de incidentes graves que contribuyan a la pérdida de clientes o dinero.

1.1.3 Factores Inmediatos

El resultado del análisis basado en la norma ISO/IEC 27001, pretende dar a conocer lineamientos de seguridad para prevenir y mitigar vulnerabilidades existentes, proporcionándole a Credigestión controles de seguridad que puedan aplicarse dentro de cada área, en especial de las áreas críticas del negocio.

La documentación resultante guiará a la empresa para que empiece a alinearse en temas de seguridad, ocasionando que se integre a su estructura organizacional un área o persona responsable que se encargue de la seguridad de la información, así como la existencia de una política de seguridad de la información donde se detalle los roles, responsabilidades y controles que se deben aplicar tomando en cuenta desde la seguridad en los sistemas de información hasta la concienciación de los funcionarios en el manejo de la información.

1.2. Formulación del Problema

¿Cómo se podría minimizar los riesgos de pérdida, daño o alteración de la información administrada dentro de la empresa Credigestión?

1.2.1. Sistematización del problema de investigación

¿De qué forma se podría garantizar que la información solo sea accedida por personas autorizadas?

¿De qué forma se podría realizar concienciaciones al personal acerca de temas de seguridad de la información?

¿De qué forma se podría salvaguardar la información tanto física como lógica de la empresa?

¿Cómo se podría garantizar que la información es manejada de forma adecuada dentro de la organización?

¿De qué forma se podría proteger adecuadamente los activos organizacionales?

¿Cómo se podría asegurar que los funcionarios, contratistas y terceros cumplan con sus responsabilidades tomando en cuenta la seguridad de la información?

¿Cómo se podría asegurar que los procedimientos para la operación de los medios de procesamiento de información son los adecuados?

¿De qué forma se podría garantizar la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones?

¿Qué acciones se deberían tomar ante la ocurrencia un incidente de seguridad en los sistemas de procesamiento de información y comunicaciones?

¿De qué forma se podría garantizar que el proceso de desarrollo del software y soporte sea seguro?

1.3. Objetivos de la Investigación

1.3.1. Objetivo General

Analizar los procesos críticos de Credigestión respecto a las gestiones de seguridad adecuadas para garantizar la confidencialidad, integridad y disponibilidad de la información, mediante la formulación recomendaciones de seguridad y controles basados en la Norma ISO/IEC 27001.

1.3.2. Objetivos Específicos

- Conocer la situación actual referente a seguridad informática y seguridad de la información dentro de la empresa.

- Analizar vulnerabilidades de seguridad que pudiesen existir en el manejo de información y en los sistemas de procesamiento de información de la empresa.

- Identificar posibles riesgos que afecten a la continuidad del negocio.

- Determinar salvaguardas que permitan fortalecer los procesos críticos de la empresa para que se cumplan los criterios básicos de seguridad.

- Proveer lineamientos de seguridad para garantizar la confidencialidad, disponibilidad e integridad de la información.

- Establecer mecanismos de sensibilización para el personal sobre temas Seguridad de la información.

1.4. Justificación

La Información es parte de los activos más importantes de toda empresa, y a su vez es uno de los recursos más propenso a vulnerabilidades, siendo necesario protegerlo de amenazas internas y externas. En la actualidad las empresas necesitan que la información que manejan esté siempre disponible, sin alteraciones en sus datos y sea confiable.

La norma ISO/IEC 27001: Sistemas de Gestión de Seguridad de la Información, proporciona un estándar de calidad de seguridad de la información, ayudando a minimizar los riesgos de daño, robo o fuga de información; permitiendo mantener la integridad, confidencialidad y disponibilidad de la información, además de garantizar la autenticidad y el no repudio de la misma.

Mediante el análisis de seguridad informática y seguridad de la información, Credigestión podrá conocer y aplicar controles de seguridad en la información que se maneja en la empresa para asegurarse que éste siendo utilizada adecuadamente y solo tenga acceso personas autorizadas.

El desarrollo del análisis de seguridad de la información basada en las Normas ISO/IEC 27001 permitirá conocer las vulnerabilidades existentes en el manejo de la información física así como la que está contenida en los sistemas de procesamiento de información, de tal forma que se puedan tomar acciones preventivas y correctivas dentro de la empresa, para evitar que se lleguen a comprometer datos confidenciales.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes de la Investigación

Durante muchos años las empresas se han preocupado por perfeccionar todos los sistemas informáticos, dejando en una prioridad casi nula la seguridad de la información. La evolución de los sistemas computacionales, del internet y de las comunicaciones en general han abierto una puerta para que las personas empiecen a descubrir el valor de la información y la facilidad de acceder a los datos.

Desafortunadamente ese fácil acceso a la información la expone a que también sea utilizada por personas no autorizadas. Existen miles de personas que se dedican a realizar ataques informáticos con la finalidad de obtener información para cometer actos ilícitos, de tal manera que puede llegar a perjudicar una empresa.

Actualmente es necesario garantizar que en los perfeccionamientos realizados en los sistemas informáticos y en la manipulación de la información física se incluyan criterios de seguridad de la información, pues está debe resguardarse y limitarse para evitar exponerla a personas ajenas a la utilización de la misma.

Los controles relacionados a la Seguridad de la Información y de los Sistemas Informáticos se refieren al conjunto de normas, procedimientos y mecanismos utilizados para garantizar la confidencialidad, integridad y disponibilidad en los sistemas de procesamiento de datos y en la información utilizada por personal de las organizaciones.

Bajo las consideraciones antes mencionadas es importante realizar un análisis de seguridad en los procesos ejecutados en una empresa, de esta manera se podría detectar posibles vulnerabilidades y amenazas que puedan afectar a la continuidad del negocio.

Siendo conocido que la información forma parte de los activos más importantes dentro de una organización, Credigestión definió la necesidad de adaptar a su gestión

de negocio, controles de seguridad que les permita garantizar que la información contenida en sus sistemas informáticos sea confiable, siempre esté disponible y se mantenga íntegra, por lo cual incorporar lineamientos de seguridad en los procesos críticos de la empresa le permitiría minimizar posibles riesgos de fuga de información o el manejo incorrecto de la misma.

2.1.1. Marco Referencial

A continuación se detalla los conceptos que se utilizan para el desarrollo de la investigación planteada, teniendo como propósito mostrar un procedimiento coordinado y coherente de conceptos, contribuyendo de esta forma a la interpretación correcta de los resultados de la investigación.

2.1.1.1. Norma ISO/IEC 27001

Es una norma internacional que detalla lineamientos de seguridad de la información, los cuales permiten implementar en la gestión de seguridad de la información de cualquier empresa controles para mejorar continuamente la seguridad física y lógica de la información, ayudando así a proteger la información de posibles robos o daños. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. (Kosutic, 2014)

2.1.1.2. Beneficio de la Norma ISO/IEC 27001

Permite disminuir posibles riesgos de vulnerabilidades en los sistemas informáticos y en la información en general manejada por personal de la empresa, además mejora los procesos y servicios prestados, teniendo una mejor organización de los procesos, aumentando la competitividad de la empresa debido a que se demuestra el interés por salvaguardar la integridad, confiabilidad y disponibilidad de la información de los clientes.

2.1.1.3. Dominios de seguridad de la ISO/IEC 27001

- Política de seguridad

- Organización de la seguridad
- Gestión de activos
- Seguridad de los Recursos Humanos
- Seguridad Física y del Entorno
- Gestión de Comunicaciones y Operaciones
- Control de Accesos
- Adquisición, Desarrollo y mantenimiento de los sistemas
- Gestión de Incidentes de Seguridad de la Información
- Gestión de la continuidad de los negocios
- Cumplimiento

2.1.1.4. Sistema de gestión de seguridad de la información

Permite implementar controles de seguridad, ayudando a monitorear, revisar, mantener, y mejorar la seguridad de la información.

2.1.1.5. Seguridad de la Información

Esa parte del sistema gerencial general, basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información (ISO/IEC 27001:2005)

2.1.1.6. Seguridad Informática

Se entiende por seguridad informática al conjunto de reglas y normas diseñadas para garantizar la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica abarcando hardware y software.

2.1.1.7. Comité de Gestión de la seguridad de la información

Se refiere a un grupo de personas especializadas en temas tecnológicos y de seguridad de la información, y necesariamente se incluye a la máxima autoridad de la empresa.

2.1.1.8. Manual de Políticas de Seguridad de la Información

Se refiere al documento donde se detallan todos los controles de seguridad que están implementados en la empresa, así como la definición de responsabilidades para cada actividad.

2.1.1.9. Propietario de la Información

"Propietario" no significa ser dueño de los activos de información, se refiere a las personas responsables de velar que se le dé buen uso aquellos activos, así como el analizar quien debe tener acceso a los mismos.

2.1.1.10. Confidencialidad de la información

La propiedad que esa información esté disponible y no se divulgada a personas, entidades o proceso no autorizado. (ISO/IEC 27001:2005).

2.1.1.11. Integridad de la información

Tener la certeza de que la información y métodos de procesamiento no han sido modificados.

2.1.1.12. Disponibilidad de la información

Tener la certeza de que la información va a estar disponible en el momento que requiera ser accedida por las personas que están autorizadas a acceder a la misma.

2.1.1.13. No repudio de la información

Permite garantizar que determinada acción realizada por algún usuario no pueda ser negada, siendo de esa manera irrefutable.

2.1.1.14. Autenticación

Se refiere al mecanismo de seguridad que permite identificar que usuario está intentando acceder a determinado sistema. Evita las suplantaciones de identidad.

2.1.1.15. Autorización de la información

Garantiza que el emisor tiene permisos de accesos a los servicios o a la información que quiere acceder.

2.1.1.16. Activo de Información

Se refiere a toda la información que se genera en una empresa.

2.1.1.17. Tecnología de Información

Se refiere a las herramientas que son utilizadas para manipular o distribuir información, es decir son el hardware y software operado por una empresa.

2.1.1.18. Incidente de seguridad de la información

Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información (ISO/IEC, 2005).

2.1.1.19. Evento de seguridad de la Información

Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad. (ISO/IEC, 2005).

2.1.1.20. Riesgo Residual

El riesgo remanente después del tratamiento del riesgo. (ISO/IEC, 2005).

2.1.1.21. Aceptación de riesgo

Decisión de aceptar el riesgo. (ISO/IEC, 2005).

2.1.1.22. Análisis de Riesgo

Uso sistemático para identificar fuentes y para estimar el riesgo. (ISO/IEC, 2005).

2.1.1.23. Valuación del riesgo

Proceso general de análisis del riesgo y evaluación del riesgo. (ISO/IEC, 2005).

2.1.1.24. Evaluación del riesgo

Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo. (ISO/IEC, 2005).

2.1.1.25. Gestión del riesgo

Actividades coordinadas para dirigir y controlar una organización con relación al riesgo. (ISO/IEC, 2005).

2.1.1.26. Tratamiento del riesgo

Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo. (ISO/IEC, 2005).

2.1.1.27. Delitos Informáticos

Se refiere a todas las acciones se cometen mediante medios informáticos con la finalidad de robar, dañar o cambiar información y que afectan a empresas y personas.

2.1.1.28. Hackers

Es una persona que posee conocimientos avanzados en cuanto a tecnología y los utiliza para descubrir vulnerabilidades que pueda existir en los sistemas informáticos.

2.1.1.29. Crackers

Es una persona que posee conocimientos avanzados en cuanto a tecnología pero a diferencia de los hackers, los crackers utilizan sus conocimientos para vulnerar los sistemas informáticos, muchas veces es con fines de lucro. Logrando así robar información confidencial de la empresa.

2.1.1.30. Virus Informático

Son programas maliciosos que alteran el funcionamiento de las computadoras, logrando de esa forma dañar y borrar información valiosa.

2.1.1.31. Antivirus

Programa utilizado para detectar la presencia de virus informático en equipos tecnológicos y archivos enviados por medios tecnológicos.

2.1.1.32. Spam

Mensajes basura no deseados, generalmente enviados mediante correos electrónicos masivos.

2.1.1.33. Anti-spam

Software utilizado para detectar correo basura, de tal forma que pueda bloquear su entrada.

2.1.1.34. Antispyware

Software utilizado para detectar programas espías que se ocultan en la computadora

2.1.1.35. Firewall

Programa utilizado para bloquear el acceso a un determinado programa, impidiendo la ejecución de toda actividad dudosa.

2.1.1.36. Falsificación de información por terceros

Se refiera a una acción consciente por parte de personas ajenas a la empresa con la finalidad de alterar o modificar información de algún documento.

2.1.1.37. Capacitación de seguridad de la información

Se refiere a las charlas y/o conferencias acerca de temas de seguridad de la información que se deben dar de forma periódica a los funcionarios con la finalidad de mantenerlos informados de los riesgos a las que está expuesta la información que manejan.

2.1.2. Marco Teórico

SGSI: Sistema de Gestión de Seguridad de la Información.

Normas: Principio para establecer acciones y procesos en el desarrollo de una actividad cumpliendo con políticas.

ISO: Organización Internacional para la Estandarización.

IEC: Comisión Electrotécnica Internacional.

Activo: Cualquier recurso que tiene valor para la empresa.

Riesgos: Vulnerabilidad a que se produzca un daño potencial.

Vulnerabilidad Informática: Incapacidad de protegerse ante un ataque.

Ataque Informático: Es el intento de acceder a información a la cual no se está autorizado.

Amenaza Informática: Hace referencia a la posibilidad de que ocurra alguna situación que representa un peligro.

Impacto Informático: Son las consecuencias de que se materialice un riesgo.

Controles de seguridad: Acción o acciones que se utilizan para minimizar el riesgo.

Evitar un riesgo: Son acciones preventivas y oportunas que se realizan para no llegar a ser afectado por la materialización de un riesgo.

2.2. Fundamentación legal

El marco legal se basa en estándares internacionales aceptados para la práctica de norma ISO/IEC 27.001 Sistemas de Gestión de Seguridad de la Información, en las regulaciones de la Superintendencia de Bancos estipuladas para el sector comercial de créditos y el reglamento interno de la empresa Credigestión.

2.3. Formulación de Hipótesis

2.3.1. Hipótesis General

A través de controles de seguridad basados en la norma ISO/IEC 27001 se establecen mecanismos adecuados para mitigar riesgos que se puedan presentar en el uso de los sistemas de información y en el manejo de la información.

2.3.2. Hipótesis Específicas

- Aplicar mecanismos de seguridad mejorará la gestión de la seguridad de la información.

- Establecer un responsable del manejo, monitoreo y seguimiento de los controles de seguridad, mejorará la gestión de la seguridad de la información.

- Incluir charlas de temas relacionado a la seguridad de la información mejorara la cultura organizacional.

- Establecer responsabilidades y obligaciones del manejo de la información de acuerdo a las funciones que realiza cada persona dentro de la empresa mejorará la cultura organizacional respecto a la seguridad de la información.

- Mantener documentados y actualizados los procesos, procedimientos e instructivos de cada área mejorará la gestión organizacional.

- A través de los controles de seguridad se puede monitorear posibles amenazas que afecten los sistemas tecnológicos de la empresa.

- Mediante controles de seguridad se puede mejorar el ámbito financiero, pues ayudará a prevenir incidentes de seguridad que puedan incurrir en altos costos para la empresa.

- Permite mejorar el aspecto comercial generando credibilidad y confianza entre sus clientes.

2.4. Señalamiento de variables

2.4.1. Variables Independientes

- Controles de seguridad
- Nivel de compromiso
- Infraestructura informática
- Madurez de los procesos

2.4.2. Variables Dependientes

- Madurez de la seguridad de información
- Vulnerabilidades en los procedimientos
- Amenazas

CAPÍTULO III
MARCO METODOLÓGICO

3.1. Modalidad básica de la investigación

El proyecto se basa en las siguientes modalidades de investigación:

De campo: Se utilizará la investigación de campo pues se necesitó recurrir al lugar donde se desarrollan los hechos, obteniendo información veraz de lo ocurrido, de tal forma que el análisis realizado este acorde a los objetivos de la investigación.

Bibliográfica: Debido al estudio de seguridad que se realizara, nos enmarcamos en torno al direccionamiento de la norma ISO/IEC 27001, que cubre criterios de buenas prácticas y gestión referente a la información.

3.2. Tipo de Investigación

- **Tipo de investigación de campo:** Este tipo de investigación se apoya en la información levantada, obtenida mediante observaciones en el lugar donde se desarrolla cada proceso, reuniones con los Gerentes y Supervisores de cada área.

- **Tipo de investigación descriptiva:** Este tipo de investigación detalla las actividades que se llevan a cabo en los procesos manejados en el objeto de estudio, permitiendo conocer en forma sistemática las falencias que se presentan en los mismos.

- **Tipo de investigación no experimental:** El objeto de estudio de la investigación no se puede modificar deliberadamente, basándose principalmente en la observación de eventos para que puedan ser posteriormente analizados.

- **Tipo de investigación explicativa:** Esta investigación es explicativa porque intenta establecer los aspectos que causan el objeto de la investigación, plantea

una valoración de hipótesis que ayude a comprender las causas de los eventos que se estén presentando.

3.3. Población y Muestra

3.3.1. El Universo

Las unidades básicas objeto de investigación la conforman los empleados de los departamentos de la empresa Credigestión:

- Crédito y Cobranzas
- Cartera
- Control de Calidad
- Administración
- Recursos Humanos
- Caja
- Contabilidad
- Sistemas
- Servicios Generales

Cuya población se totaliza en 230 empleados.

3.3.2. Muestra

Para el estudio y análisis de datos, se realizó un muestreo intencional donde los criterios para la selección dentro de la población consistieron:

- Directivo del departamento que posee un amplio conocimiento del proceso y actividades que deben realizar los operarios del área y que mantenga un rol de ejecutor en la toma de decisiones.

- Operario típico de la unidad o departamento que realice o manipule información para llevar a cabo las actividades que su rol exige.

Es factible que con un número de 23 funcionarios a entrevistar y encuestar se puede lograr una apreciación muy real de la situación actual, ya que el análisis se centra sobre el grupo de personas que cumplen un papel relevante en los procesos de la empresa.

3.4. Operacionalización de variables e indicadores

Tabla 1. Matriz de Operacionalización de Variables

Variable	Definición Conceptual	Dimensiones	Indicadores
Controles de Seguridad	Los controles de seguridad ayudan a regular las actividades realizadas sobre la información	Divulgación de las medidas de Seguridad	Políticas de políticas de seguridad que los usuarios deben conocer y aplicar.
			Medios determinados para la comunicación de las políticas de seguridad.
		Valoración de las políticas de seguridad	Periodicidad en la verificación de la efectividad de las medidas de seguridad.
			Periodos determinados para la evaluación interna.
Nivel de compromiso	Es el nivel de apoyo que se brinda a los sistemas de seguridad de la información.	Inversión realizada en la adquisición de recursos que permitan el control y monitoreo continuo de las políticas de seguridad	Adquisición de herramientas tecnológicas y/o contratación de personal especializado en gestión de la seguridad de la información.
		Cumplimento de los procedimientos y controles de seguridad	Revisiones periódicas de las actividades establecidas de acuerdo al rol del funcionario.

establecidos

Infraestructura informática	Es el conjunto de software y hardware que dan soporte al procesamiento y almacenamiento de datos.	Seguridad brindada por los sistemas de procesamiento, transmisión y almacenamiento de datos.	Periodos de revisión de la configuración de seguridad de los equipos de almacenamiento de datos. Periodos de evaluación de seguridad de los sistemas informáticos de procesamiento de datos. Periodos de revisión de la seguridad en los sistemas de comunicación.
Madurez de los procesos	La madurez de los procesos se refiere a la definición, estandarización, automatización y regulación de los procesos.	Nivel de los procesos de la empresa	Evaluación del estado actual del proceso.
Madurez de la seguridad de la Información	La madurez de la seguridad de la información, implica el cumplimiento e implementación de los controles establecidos.	Establecimiento de controles de Seguridad de la información Seguridad de la información a nivel de Tecnologías de la Información.	Capacitaciones del Personal. Incidentes detectados sobre las políticas de seguridad. Auditorías realizadas en las áreas administrativas. Incidentes reportados en las aplicaciones que puedan afectar la información. Incidentes reportados en los equipos de cómputo de los funcionarios. Criterios determinados en las evaluaciones de los sistemas de información.
Vulnerabilidad en los procedimientos	Las vulnerabilidades se consideran como una falencia que puede ser explotada.	Vulnerabilidades que se conocen y no ha	Histórico de las vulnerabilidades sobre las cuales se ha tomado acciones correctivas. Vulnerabilidades encontradas y reportadas.

		podido ser cubiertas	
Amenazas	Es el conjunto de vulnerabilidades que se han detectado y significan un riesgo para la seguridad de la información.	Identificación de las amenazas existentes	Reporte de amenazas detectadas.
		Gestión sobre las amenazas	Procedimientos definidos para la gestión y control de amenazas. Seguimientos sobre amenazas críticas gestionadas Históricos de la gestión de amenazas

3.5. Plan de recolección de información

Para desarrollar el análisis de seguridad de la información se utilizará los siguientes mecanismos de recolección de información:

- Encuestas
- Entrevistas
- Consultas
- Reuniones
- Observación
- Revisión de documentación

3.6. Plan de procesamiento de la información

Se podrá utilizar el siguiente criterio:

- Levantamiento de Información
- Clasificación de la Información
- Registro de la Información
- Análisis de la información obtenida
- Verificación de la Información

- Archivo de la información

El proceso de los datos se realizará sobre la herramienta ofimática de Microsoft, Excel la cual nos permitirá clasificar, verificar y contrastar las variables de la investigación. Con los datos obtenidos se analizará los controles de seguridad que podrá acoger la empresa.

Como soporte para la recolección de datos y procesamiento, serán necesarios dos equipos de cómputo portátiles, por movilización, facilidad para compartir información y poder de procesamiento necesario para detallar resultados y recomendaciones finales.

CAPÍTULO IV
ANÁLISIS Y RESULTADOS

4.1. Análisis de los Resultados

Los resultados obtenidos en la evaluación del análisis de Seguridad de la Información y Seguridad Informática, ayudarán a Credigestión en la implementación de buenas prácticas que mitigará las vulnerabilidades y amenazas que han sido identificadas.

El proceso central analizado fue el del área de Sistemas, por ser considerada como soporte fundamental para el procesamiento y almacenamiento de datos, así mismo se analizó el grado de concientización en seguridad de la información y manejo de la información en áreas críticas como: Cartera, Crédito y Cobranzas y áreas de apoyo, Administrativo, Recursos Humanos, Control de Calidad, Contabilidad, Caja y Servicios Generales.

4.1.1. Responsabilidad de la ejecución de los controles correctivos y preventivos

Es importante indicar que será de exclusiva responsabilidad del área de Sistemas o Responsable de Seguridad Informática en coordinación con el Presidente Ejecutivo de Credigestión, el evaluar los controles que han resultado de este análisis, para que puedan ser implementados en la empresa, tomando en cuenta la infraestructura tecnológica y recurso humano disponible.

Ejecutan: Área de Sistemas o Responsable de Seguridad Informática en coordinación con los Propietarios de la Información.

Monitoreo de cumplimiento: Área de Sistemas y/o Responsable de Seguridad Informática

4.1.2. Planificación de entrevistas

Con la finalidad de obtener resultados reales de la situación en la empresa referente a temas de seguridad de la información, se elaboró una planificación de entrevistas con personal directivo de las áreas consideradas críticas (Sistemas, Cartera. Crédito y Cobranzas), así mismo se mantuvo entrevistas con directivos de las áreas de apoyo.

Con la colaboración del área de Sistemas se programaron un total de 13 entrevistas. A continuación se detallan los nombres y cargos de cada una de las personas entrevistadas:

Tabla 2. Cuadro de Planificación de entrevistas

Fechas	Nombres	Cargos
Viernes, 6-feb-2015	Soledad Camposano	Gerente de Sistemas
Lunes, 9-feb-2015	Paola Terán	Especialista en Redes y base de datos
Lunes, 9-feb-2015	Maritza López	Jefa de Desarrollo e implementación de Sistemas
Martes, 10-feb-2015	Mery Cajamarca	Jefe de Cartera
Martes, 10-feb-2015	Mariela Fierro	Subgerente de Operaciones Crédito y Cobranzas
Miércoles, 10-feb-2015	María Calle	Supervisor de Cobranzas
Miércoles, 11-feb-2015	Elba Candelario	Coordinador de Cobranzas Terrenas
Miércoles, 11-feb-2015	Pedro Avelino	Coordinador de Cobranzas Telefónicas
Jueves, 12-feb-2015	Verónica Gamarra	Jefe del área Administrativa
Jueves, 12-feb-2015	Luis Cárdenas	Jefe de Control de Calidad
Viernes, 13-feb-2015	Olga Escobar	Supervisor de Contabilidad
Viernes, 13-feb-2015	Aracely Mendoza	Jefe de Recursos Humanos
Viernes, 13-feb-2015	Jacqueline Villalta	Supervisor de Caja

4.1.3. Cuestionario de preguntas a realizar en las entrevistas y encuestas

El resultado del análisis de riesgo tiene como base la recolección de información, en la cual se aplicaron técnicas de observación, revisión de documentación, reuniones, consultas, preguntas de entrevistas y encuestas.

Cabe indicar que se considera muy importante el criterio de la persona entrevistada, pues es quien posee el nivel de conocimiento de los procesos que se llevan a cabo en cada área.

Las entrevistas y encuestas realizadas al área de Sistemas y demás áreas de la empresa, tuvieron como base los controles detallados en los dominios de la ISO 27001. A continuación se detalla en forma general los criterios para la identificación de vulnerabilidades sobre las cuales se elaboraron las entrevistas y encuestas las cuales están incluidas en el anexo 1.

Criterios de seguridad para las preguntas de entrevistas y encuestas en el área de Sistemas

- Existencia del Manual de Política de Seguridad de la Información
- Periodos de actualización del Manual de Política de Seguridad de la Información
- Socialización del Manual de Política de Seguridad de la Información
- Existencia del área o responsable de seguridad informática
- Herramientas de seguridad implementadas
- Existencia de procedimientos e instructivos propios del área
- Periodos de actualización de los procedimientos e instructivos
- Participación y apoyo de las máximas autoridades de la empresa
- Concientización al personal acerca de temas de seguridad de la información
- Perfiles y roles de usuarios
- Clasificación de la información
- Controles y políticas de seguridad implementadas en la empresa
- Mecanismos de autenticación
- Gestión de contraseña en los diferentes aplicativos
- Infraestructura tecnológica
- Software Malicioso
- Mantenimientos en equipos tecnológicos
- Inventarios tecnológicos

- Respaldos de información
- Incidentes de seguridad
- Plan de contingencia

Criterios de seguridad para las preguntas de entrevistas y encuestas en las demás áreas

- Conocimiento acerca del tema de Seguridad de la información y seguridad informática
- Existencia de Procedimientos e instructivos propios del área
- Periodos de actualización de los procedimientos e instructivos
- Conocimiento de un Responsable de Seguridad en la empresa
- Identificación y categorías de los activos de información de cada área
- Incidentes o eventos de seguridad
- Control de acceso mediante mecanismos como tarjetas de acceso, llaves. entre otros
- Responsables de solicitar accesos a los diferentes aplicativos y módulos de acuerdo a lo que se utilice en cada área.
- Concientización en temas de seguridad de la información
- Importancia de la aplicación de controles de seguridad dentro de la empresa
- Detección de vulnerabilidades de seguridad en los aplicativos

4.1.4. Situación actual

De acuerdo a las respuestas obtenidas en las diferentes entrevistas y encuestas realizadas a personal de Credigestión; así como la utilización de técnicas como la observación, consultas y revisión de documentación, se pudo identificar el estado actual de la empresa, referente a temas de seguridad de la información y seguridad informática, basado en los controles de la norma ISO/IEC 27001.

- **Políticas de seguridad**

- Credigestión no posee un manual de políticas de seguridad de la información, pero tienen implementados y documentados algunos controles de seguridad que permiten limitar accesos no autorizados a la información, los cuales no han sido actualizados desde su fecha de elaboración. Además la única persona que conoce en su totalidad la existencia de dicha la documentación es la Gerente de Sistemas, pues el resto del personal del área de Sistemas solo se limita a conocer la documentación y controles conforme a las funciones que desempeñan.

- Solo las áreas de Sistemas, Caja, Crédito y Cobranzas, cuentan con procedimientos e instructivos documentados formalmente. Pero aun así el personal que labora en el área de Caja no conoce de la existencia de instructivos y procedimientos de su área.

- **Organización de la seguridad de la información**

- Existe el compromiso adecuado de la máxima autoridad con temas relacionados a la tecnología e implementación de controles de seguridad.

- La coordinación tanto de la seguridad de la información como de los sistemas de procesamientos de información son realizadas entre el personal de sistemas y la Gerente de Sistemas, solo en casos de que la actividad a realizar infiera en costos se informa a los altos directivos sobre lo que se va a implementar.

- No existe un Comité de Gestión de Seguridad de la información que se encargue expresamente de la toma de decisiones referentes a implementaciones de controles y herramientas que permitan mejorar la seguridad de la información.

- La Especialista de Redes y Base de datos encargada de la seguridad de las redes y bases de datos, es además la responsable de la administración de accesos a los diferentes aplicativos que utilizan los funcionarios, por tal razón se la considera como la Responsable de Seguridad Informática, pero no realiza ninguna actividad acorde a la gestión de seguridad de la información, ni ninguna función

propia de este cargo, no existen la definición de actividades a cumplir con respecto a seguridad de la información.

- Los funcionarios tienen la certeza de que cuando se habla del área Seguridad Informática o Seguridad de la Información se están refiriendo al área de Sistemas, pues se piensa que ambas áreas realizan las mismas actividades, y lo único que cambia es el nombre.

- La mayoría de funcionarios tiene la seguridad de que en la empresa existe un área de Seguridad Informática y Seguridad de la Información o al menos existe un Responsable de Seguridad Informática, por otro lado también existen funcionarios que desconocen si existe aquella área en la empresa.

- Falta de un proceso formal donde se indique como se debe realizar la autorización de funcionamiento y uso de los nuevos medios de procesamiento de información, de tal forma que se establezcan responsabilidades de autorización, y se pueda evidenciar que el nuevo sistema está acorde a las necesidades de la empresa o área.

- El área de Recursos Humanos incluye en el contrato de los funcionarios una cláusula que indica que el trabajador se compromete expresamente a guardar confidencialidad y reserva de la información, pero esta cláusula no tiene la relevancia suficiente pues los funcionarios no recuerdan que exista ese compromiso de confidencialidad de la información que están manejando.

- Mantienen un apropiado registro de contactos con autoridades externas en caso de incidentes de seguridad de nivel mayor.

- Por no existir una persona o área que se dedique exclusivamente a gestionar los temas de seguridad informática y seguridad de la información no se mantiene contacto con grupos o empresas que les aporten conocimientos, observaciones, entre otros referente a la seguridad de la información.

- Todos los controles implementados actualmente no son objeto de monitoreo, mientras nadie reporte que está funcionando mal algún sistemas, se asume que

todo funciona correctamente. Cuando ocurre un cambio significativo como actualizaciones o implementación de nuevos sistemas de procesamientos de información, el área de Sistemas se encarga de elaborar un manual de uso.

- No se realiza ninguna acción que permita la identificación de riesgos en la información a la que tienen acceso proveedores o contratistas, por lo que no saben que controles podrían implementar referente a ese tema.

- El área Sistemas es quien se encarga expresamente de la elección y contrato de personal externo (mantenimientos de equipos, entre otros), en el contrato realizado no se incluye un acuerdo de confidencialidad y no divulgación de la información que vaya a ser manejada proveedores o contratistas.

- **Gestión de Activos**

- Se cuenta con inventarios de equipos de computación y dispositivos de almacenamiento, lo cuales son actualizados por el área de Sistemas cada vez que se adquiere un nuevo equipo o dispositivo. Además poseen un documento donde se detallan las licencias utilizadas para cada servidor que poseen. Ninguna persona del área de Sistema pudo identificar exactamente cuántos sistemas operativos se están usando en la empresa; se conoce que actualmente el uso es de tres sistemas operativos Windows XP, Windows 7 y Windows 8. En lo referente a inventarios o documentación de propia de la institución el área de Recursos Humanos indico que no se tiene un organigrama que permita conocer claramente todos los departamentos existentes, los cargos y perfiles que corresponden a cada uno de ellos.

- No existe un documento formal donde se designen los propietarios de la información y de los activos asociados con los medios de procesamiento de la información. Únicamente el área de Sistemas es quién tiene establecido responsabilidades con respecto a los activos de equipos de cómputos, dispositivos almacenamientos, tóner por ser quién se encarga de la compra de esos suministros para toda la empresa.

- Poseen políticas referentes al uso de correo electrónico institucional, e internet, las cuales tienen restricciones conforme a las actividades que desempeña cada funcionario. Se tienen grupos de categorías definidos para el acceso al internet, aquellas políticas se encuentran documentadas, pero no se define en ninguna de ellas, cuál será el uso correcto que deben darle los funcionarios y que se considera un uso incorrecto de aquellos activos.

- No se encuentran definidos criterios para la clasificación de la información y manejo de la información, por lo que las áreas no cuentan con un catálogo de clasificación de la información, el cual les permita determinar qué información es confidencial o de uso interno; los funcionarios no tienen claro a que se le puede considerar información confidencial y/o de uso interno.

- No se posee ningún criterio de etiquetado y manejo de la información, se pudo apreciar que solo las cintas de respaldo se rotulan con fecha, número secuencial y nombre que hace referencia a lo respaldado. Para el archivo de información física no se utiliza ningún criterio, pues se archiva la información de acuerdo a las necesidades de cada persona, solo ciertas carpetas cuentan con el nombre que hace referencia a lo que contiene.

- **Seguridad de los Recursos Humanos**

- El área de Recursos Humanos no posee documentación donde se defina las funciones y responsabilidades de los empleados, en los contratos solo se incluyen responsabilidades y obligaciones que tienen con la empresa.

- El área de Recursos Humanos realiza el proceso de contratación de nuevos funcionarios siguiendo el proceso definido en base a la experiencia de la actual Jefe de área, no se tiene definido un proceso formal.

- En los contratos con empleados, contratistas y terceros solo se incluyen responsabilidades y obligaciones que se deben cumplir en el trabajo a realizar dentro de la empresa y acorde a las políticas de la misma, pero no se estable las

responsabilidades y obligaciones que deben tener en referencia a la seguridad de la información.

- Conforme a los contratos firmados por empleados, contratistas y terceros se gestiona las responsabilidades que deben cumplir durante el tiempo de sus labores en la empresa; estas responsabilidades a cumplir están solamente enfocadas a políticas e la empresa y no a políticas de seguridad de la información.

- Desde las máximas autoridades hasta los usuarios finales no poseen conocimiento claro de los temas relacionados con seguridad de la información y seguridad informática, además no conocen si en la empresa existen controles de seguridad para mitigar algún incidente de seguridad. Los funcionarios nunca han recibido capacitaciones de temas relacionados con seguridad de la información, muchos creen que se trata de seguridad del empleado, y otros no tienen idea de que se trata.

- No existe un procedimiento que indique las sanciones en caso de faltas cometidas por los funcionarios en la seguridad de los sistemas de procesamiento de información o información física que manejan; en las políticas general de Credigestión se establece que establecerán sanciones que conllevarán a la terminación de contrato laboral, pero no se define qué acciones son las que se consideran graves.

- No cuentan con procedimientos donde indiquen que antes del término de contrato laboral deben devolver los activos fijos que se les ha entregado al inicio de sus labores. Cada supervisor de área se encarga de recibir los materiales de oficinas utilizados por el funcionario, pero tiene la certeza de que aquellos materiales de oficina que son devueltos sean los mismos que se le asignaron al inicio de las labores del funcionario.

- Cuando los funcionarios terminan su contrato laboral con la empresa, es el jefe correspondiente quien se encarga de revisar que el funcionario haga la entrega de toda la información utilizada y generada durante sus actividades laborales

además es quien procede a notificar al área de Sistemas para que se elimine o desactive los accesos a los diferentes aplicativos de los cuales hacía uso, no existe ninguna documentación formal donde se detalle el proceso antes mencionado.

- **Seguridad Física y Ambiental**

- La empresa alquila dos pisos del edifico en el que se encuentra, únicamente en el primer piso es donde se encuentra el área de recepción, por lo que el acceso del personal ajeno a la empresa que se dirige al segundo piso no es supervisado.

- El área de Control de Calidad, se encuentra ubicada en el mismo espacio que el área de Caja, por lo que clientes que requieren realizar pagos entran al área sin ningún tipo de control de seguridad, no existe la correcta separación entre estas dos áreas.

- El área de Sistemas es la única área que cuenta con un mecanismo de control de acceso por ser considerada un área restringida.

- No existen detectores de humo, ni alarmas contra incendios en la empresa. Hay un extintor en el pasillo de uno de los pisos, no existen extintores dentro de las oficinas.

- El sistema de cámaras no es propio de la empresa, lo maneja personal ajeno, pues el edificio en el que se encuentran no es propio, lo comparten con más empresas.

- El Rack de comunicaciones así como el UPS se encuentra dentro del área de Sistemas, en un espacio físico separado, las llaves las tiene únicamente la Especialista de Redes y Bases de datos, esta área solo cuenta con detector de humo como medida de protección contra alguna amenaza externa o ambiental (fuego, agua, entre otros).

- Las áreas no se pueden identificar fácilmente, pues no cuentan con el señalamiento apropiado. Así mismo el área donde está el Rack y UPS no cuenta con la señalética adecuada.

- Todos los equipos están ubicados dentro de las áreas, de esa forma intentan limitar los accesos no autorizados de personas ajenas a la empresa.

- Se cuenta con un UPS que les permite tener energía eléctrica 20 minutos después que ocurre el corte de energía, lo que les permite a los funcionarios guardar la información y apagar las computadoras para evitar daños.

- El área de Sistemas realiza dos veces al año mantenimientos en los equipos de procesamiento de información, pero no existe documentación donde se detallen qué tipos de mantenimientos se realizaron, los responsables, ni ninguna información que permita conocer detalles del trabajo realizado.

- Debido a que está prohibido sacar equipos de propiedad de la empresa, no se tiene implementado ningún control referente a la seguridad de equipos fuera de la empresa. Esa prohibición no se encuentra detallada en ninguna política de seguridad; los únicos autorizados para sacar equipos en este caso laptops son los altos directivos por temas de reuniones.

- No se realiza ningún procedimiento que permita la eliminación de información de las computadoras que fueron utilizados por funcionarios que ya no laboran en la empresa.

- **Gestión de las Comunicaciones y Operaciones**

- El área de Sistemas únicamente cuenta con documentación de respaldos, dejando a un lado los demás procedimiento de operación propia del área, como lo son mantenimientos, instructivos o procedimientos de manejo de errores, documentación de recuperación del sistema en caso de fallas, entre otros.

- El área de Sistema realiza revisiones los cambios realizados a los sistemas y versiones que se actualicen. La Especialista en Redes y Base de datos, indica que

todos los cambios que se realizan en algún módulo del ISYSystem son comunicados y coordinados con los Gerentes, Subgerentes o Jefes de cada área; antes de pasar producción se realizan las pruebas pertinentes para así poder garantizar que los cambios realizados no afectan la utilidad del sistema. No se encuentra documentado el proceso de "Gestión de Cambios".

- Cada funcionario del área de Sistemas tiene claro cuáles son sus funciones y responsabilidades a cumplir de acuerdo al cargo que tienen y funciones adicionales que pueden ser encargadas por la Gerencia del área.

- La Jefa de Desarrollo e implementación de sistemas es quien se encarga de designar al personal que debe participar en cada una de las fases de producción o actualización de un sistema.

- No se encuentra documentado las actividades que deben realizarse en cada ambiente: Desarrollo, Pruebas, Capacitación y Producción, debido a que es la Jefa de Desarrollo e Implementación de Sistemas quien se encarga de indicar al personal que actividades se deben realizar en cada fase(ambiente).

- El área de Sistemas al encargarse de la contratación de los servicios de terceros, es quién define los términos que deben cumplir los proveedores y revisa que lo entregado esté acorde a lo requerido.

- Nos se realizan revisiones regularmente de los servicios de terceros; actualmente mantienen contrato con una empresa externa que es quien les provee el servicio de desarrollo de la página web de la empresa y actualiza constantemente la información en la página, al ser una página web solo informativa no se consideran ningún tipo de monitoreo ni controles de seguridad mínimo que deba cumplir la empresa contratada para el manejo de aquella página.

- El área de Sistemas no realiza ningún tipo de análisis de la capacidad de los recursos utilizados, pues solo consideran las necesidades actuales, más no proyecciones futuras, lo que genera un mayor costo en adquisiciones de nuevos recursos.

- No se tiene establecido criterios mínimos de seguridad en la aceptación y aprobación del uso de un sistema de información, los cuales deben ser aplicados antes de la apuesta en producción de un nuevo servicio o actualización realizada en un servicio existente.

- Se posee mecanismos para la detección de software malicioso en correos electrónicos entrantes que permiten detectar cuando se trata de un correo spam o con virus estos muestra un mensaje de alerta y no pueden ser recibidos por su destinatario final, de tal forma que evita que mediante correos electrónicos se instalen software malicioso en las computadoras. El área de Sistemas indica que todas las computadoras tienen instalado antivirus, pero no realizan monitoreo para garantizar que aquellos antivirus ese estén actualizando de acuerdo a la política implementada.

- Existe la política de respaldos de información, en la cual detallan tres frecuencias de respaldos que se realizan y la información que se respalda en cada una de ellas. Todas las tareas de respaldos son registradas en el documento "Bitácora Procesos especiales", en se detalla el responsable del respaldo, fecha, hora y observaciones en caso de que se llegue a presentar algún evento durante el proceso de respaldo de información.

- Poseen un servidor Telesynergy para central telefónica en Guayaquil, donde se encuentra documentada toda configuración concerniente al esquema de conexión por voz de líneas VoIP, líneas análogas y celulares disponibles, este servicio actualmente es utilizado por las ciudades de Guayaquil y Quito.

- Se encuentran bloqueados los medios removibles en los computadores de los funcionarios, con el propósito de evitar la fuga de información, actualmente nos e realizan ningún tipo de monitoreo que permita garantizar que esta política esté funcionando correctamente

- Inexistencia de controles de seguridad para el intercambio de información, tanto de medios físicos como mensajería electrónica, no se tiene implementado ningún

control cuando un funcionario por temas laborales requiere intercambiar información con otras entidades.

- La empresa cuenta con un equipo de mensajeros que son los responsables de llevar la documentación externa, asegurándose que la documentación enviada llega al destino indicado. Se lleva un registro donde constan las firmas de las personas externas que recibieron la documentación.

- No existe monitoreo de los registros de auditoría que producen las actividades realizadas en los sistemas, consideran que no es necesario revisar aquello.

- **Control de acceso**

- No existe una política que establezca controles de seguridad para el control de accesos.

- El área de Sistemas es la encargada de dar acceso a los diferentes aplicativos que necesita utilizar el funcionario mediante el formulario de "solicitud de acceso a usuarios", el cual fue creado recientemente en mayo de 2014.

- En ninguna documentación se detalla que el aplicativo Financiero debe ser únicamente utilizado por el área de Contabilidad. El área de Sistemas no ha considerado importante que el aplicativo maneje el cambio de contraseña, pues como lo utilizan desde hace varios años las mismas personas y nunca ha ocurrido algún incidente de seguridad con este aplicativo, no ven factible implementar el cambio de contraseña.

- El área de Recursos Humanos y el personal de Verificaciones telefónicas tienen acceso de modificación al módulo de "Datos Personales" de los funcionarios, lo que significa un alto riesgos de integridad de datos que debería ser de uso exclusivo del área de Recursos Humanos. No existe una evaluación correcta de los accesos y privilegios que deben tener cada área.

- Debido a la alta demanda de bloqueo de las estaciones de trabajo, el área de Sistema delego a cada Supervisor de área, la actividad de desbloqueo, es decir que cada Supervisor para que puedan desbloquear a las estaciones de trabajo de los usuarios y que sigan inmediatamente con sus actividades normales.

- No existe un mecanismo que permite bloquear automáticamente las estaciones de trabajo cuando se encuentran desatendidas. Son pocos los funcionarios que bloquean sus computadoras cuando necesitan salir de su puesto de trabajo.

- Se tiene establecido la utilización de mínimo 6 caracteres para la creación de las contraseñas en los aplicativos, la mayoría de funcionarios utiliza los parámetros de caracteres establecidos, pero no guardan la confidencialidad debida de sus contraseñas, pues de vez en cuando las comparten con sus compañeros.

- Las áreas que almacenan información impresa confidencial no cuentan con la seguridad física requerida, pues la información se encuentra accesible para cualquier funcionario. Así mismo en los puestos de trabajo se observó que están llenos de documentación sin archivar y muchas veces son documentos confidenciales, a pesar de ello la mayoría de funcionarios considera que se guarda la información pertinente para evitar su daño o pérdida en los gabinetes con llaves.

- La red de la empresa no se encuentra segmentada, cada usuario de la red puede acceder libremente a las IP’s de los servidores lo que ocasiona que pudiesen aprovecharse de una debilidad de configuración.

- Existen redes inalámbricas (wifi) que es utilizado por la máxima autoridad, incluyendo Gerentes y Subgerentes, la cual está abierta sin ningún tipo de seguridad, cualquier funcionario que sepa la clave y usuario puede acceder a ella, sin quedar videncia alguna.

- Cada funcionario maneja como mínimo tres USER ID, los cambios de contraseñas son diferentes para cada aplicativo teniendo lo siguiente:

Estación de trabajo: cada 35 días
Correo institucional: no pide cambio de contraseña
Sistema ISISystem: cada 25 días
Sistema Financiero: no pide cambio de contraseña

- **Adquisición, desarrollo y mantenimiento de los sistemas de información**

- No existe una política donde se determine los requerimientos de seguridad que deben ser exigidos para el desarrollo o adquisición de un software. Todo se centra en que el sistema funcione de acuerdo a lo que se necesita.

- Para la adquisición e implementación de un nuevo aplicativo el área de Sistemas se encarga de realizar revisiones y pruebas que garanticen que el nuevo aplicativo funciona de acuerdo a las necesidades del usuario final (funcionario); en caso de que el personal de desarrollo e implementación de sistemas sea quien desarrolle un nuevo aplicativo, a más de realizar las pruebas pertinentes elaboran manuales y entregables.

- Únicamente el personal de desarrollo e implementación de Sistemas está autorizado a tener acceso al código fuente del sistema en caso de requerirse alguna modificación; previa aprobación de la jefa de desarrollo e implementación de sistemas.

- No existe documentación formal donde se registre las actividades que se realizan en cada instancia (desarrollo, pruebas, capacitación y producción).

- No existe una política formal donde se detalla los controles a implementar para prevenir la fuga de información, lo que se tiene implementado como medida de seguridad es la inhabilitación de todo medio extraíble de almacenamiento, este control se exceptúan para los altos directivos, gerentes y subgerentes.

- No se realiza ninguna acción de monitoreo y control ante posibles vulnerabilidades técnicas de los sistemas, que permitan dar un trato adecuado a posibles nuevos riesgos de seguridad

- **Gestión de incidentes en la seguridad de la información**

- En el documento de Política y procedimientos de Seguridad de Sistemas de Credigestión S.A, se indica "que ante la sospecha de que la contraseña que haya sido comprometida deberá notificar inmediatamente el incidente de seguridad al líder de seguridad o Gerencia de Sistemas, para proceder con el cambio de contraseña", aquel párrafo es considerado como el único control en caso de un incidente de seguridad.

- No existe un procedimiento formal para el manejo de incidentes de seguridad, por lo cual no se conoce que pasos se debe seguir ante la presencia de un incidente de seguridad menor y/o grave, en caso de que se llegue a presentar un incidente de seguridad mayor o grave la única persona que da las indicaciones de las acciones a tomar es la Gerente de Sistemas.

- En el último año se han reportado al área de Sistemas dos casos de incidentes de seguridad, uno de ellos los reporto la Jefa de Recursos Humanos, la cual indicó que al ingresar al módulo de "Personal" detectó que había alteraciones en los nombres, apellidos y demás datos de un funcionario, se logró identificar que el causante de estas modificaciones había sido otro funcionario del área de Servicios Generales - Verificaciones telefónicas, el cual antes de salir de la empresa cambió los datos personales de su compañero, acción que se le hizo fácil pues tenía acceso y permisos de modificación al módulo "Personal", Cabe indicar que el personal de Verificaciones Telefónica debe tener acceso a este módulo porque modifica los montos del gestor (monto de gestiones realizadas), pero lo que es innecesario es que tenga habilitado los demás campos de los datos del funcionario. El segundo caso fue un problema que sucede cada vez que se va la luz, en esta ocasión la interrupción fue de 30 minutos, pero el sistema de ups que ellos poseen les permite estar con electricidad 20 minutos después de que sucede el corte de luz, es decir que en total estuvieron sin luz 10 minutos y 15 minutos más fueron perdidos pues es el tiempo que se tarda para que se restablezca los sistemas que utilizan, en total fueron 25 minutos de interrupción de actividades.

- El incidente de seguridad que se presenta frecuentemente en las estaciones de trabajo es el bloqueo de las estaciones de trabajo, aunque en el último año no se han presentado tantos incidentes de seguridad sobre este caso.

- Cuando ha presentado algún incidente de seguridad leve, muchos de los funcionarios se comunican directamente con el área de Sistemas para indicarle el problema, sin embargo otros prefieren comunicarle al Jefe inmediato para que sean ellos los encargados de resolver el inconveniente con el área pertinente.

- No se tiene establecidas responsabilidades para la gestión de incidentes, además no se encuentra detalladas ni registradas las acciones correctivas que se realizan luego de un incidente de seguridad.

- **Gestión de la continuidad comercial**

- En la Gestión de continuidad de la empresa no se ha considerado la inclusión de la seguridad de la información., por lo que no se tiene identificado cuales son los eventos que causan o podrían causar interrupciones en procesos normales de la empresa, ni el impacto que puede tener la paralización de las actividades que conllevan a la realización de estos procesos; así como tampoco se tienen considerado las consecuencias que podrían causar en la seguridad de la información.

- El área de Sistemas realiza respaldo por demanda los cuales son para proteger información sensible, en caso de un daño mayor en el centro de datos, permitiendo de esa manera recuperarse en el menor tiempo posible y continuar con las actividades propias del negocio.

- En caso de los servidores, se cuenta con el instructivo “contingencia servidores” el cual detalla los pasos a seguir ante un posible problema o daño en uno o varios servidores.

Nombre de Servidores:

- Active Directory (Servidor de red, file server, usuarios operativos)
- Base de Datos
- Aplicativo COM+ (aplicativo y file server sistemas)
- Contingencias (AD/BD)

- **Cumplimiento**

  - Todo cumplimiento de responsabilidades y obligaciones dentro de la empresa está relacionado a la política de la empresa, la cual contempla requerimientos legales. No poseen lineamientos de seguridad que eviten incumplimiento por la reproducción, copia o alteración de información sobre la cual la empresa no tiene derecho de autor, pudiendo esto ocasionar incumplimientos con la ley.

4.1.5. Matriz de hallazgos y recomendaciones basadas en la situación actual de la empresa

En la matriz que a continuación se muestra, se detalla los hallazgos y recomendaciones que permiten mejorar los controles implementados y considerar controles inexistentes, los cuales están basados en la norma ISO/IEC 27001; adicionalmente se agrega una columna donde se incorpora que control es necesario implementar primero de acuerdo a su prioridad.

Tabla 3. Control basado en la ISO 27001 – Prioridad

Prioridad	Detalle
Primario	Se refiere al control que es necesario considerar primordial en su implementación
Secundario	Se refiere al control que va a reforzar los controles primarios implementados

Tabla 4. Matriz de recomendaciones basadas en la situación actual

Dominio	Área Responsable	Hallazgo	Recomendaciones	Control basado en la ISO 27001	
1. Política de Seguridad					
Política de Seguridad de la Información	Responsable de Seguridad Informática	Inexistencia de un manual de políticas de seguridad de la información	Se debe elaborar un manual de Política de Seguridad de la Información alineada a las mejores prácticas de seguridad, que recoja todos los controles actualmente implementados en la empresa, adicionalmente se debe incluir nuevos controles de seguridad acorde a las necesidades de la empresa.	A.5.1.1 Políticas de seguridad de la información	Primario
			El manual de las Política de Seguridad de la Información deberá ser puesta en conocimiento de la máxima autoridad para su aprobación, y posteriormente debe ser sociabilizada a todos los funcionarios de la empresa. Además el Responsable de Seguridad Informática deberá actualizar el manual de Política de Seguridad de la Información cuando ocurran cambios significativos acerca de la seguridad de la información.	A 5.1.2 Revisión de la Política de seguridad de la información	Secundario
	-Todas las áreas	Falta de procedimientos e instructivos documentados	Es importante que dentro de las áreas exista documentación clara	A.5.1.1 Políticas de seguridad de la	Secundario

			(Procedimientos, Instructivos, log, bitácoras) de todas las actividades que se realizan, a más de llevar un orden eso ayuda a mantener registros del trabajo realizado, establece responsabilidades y determina que el trabajo se está realizando de una forma adecuada.	información	

2. Organización de la Seguridad de la Información

Organización Interna	Presidente Ejecutivo	Existe el apoyo de la máxima autoridad para temas relacionados con la tecnología e implementación de controles de seguridad.	Es importante continuar con el compromiso y la comunicación permanente entre el Responsable de Seguridad Informática y la máxima autoridad, para que así se logren mitigar cualquier tema relacionado con seguridad informática y seguridad de la información de forma oportuna.	A 6.1.2 Compromiso de la Gerencia con la Seguridad de la Información	Primario
	Comité de la Gestión de la Seguridad de la Información	No existe un Comité de Gestión de Seguridad de la información	Es importante que se conforme un Comité de Gestión de Seguridad de la Información, pues esto logrará que se puedan tratar y profundizar temas que permitan mejorar el manejo de la información, así como la mejora de tiempos de respuesta de los servicios de sistemas utilizados; adicionalmente se permitirá analizar controles de seguridad que permitan el conocer cómo se lleva a cabo la seguridad de la información dentro de la empresa.	A.6.1.2 Coordinación de la seguridad de la información	Primario

		El Comité debe estar conformado como mínimo por la Máxima autoridad, Gerente de Sistemas, Responsable de seguridad informática y Secretario		
Comité de la Gestión de la Seguridad de la Información	Coordinación de temas de seguridad entre personal de Sistemas y Gerente de Sistemas, solo en casos especiales se comunica a la máxima autoridad	Toda coordinación que de temas de seguridad de la información deben ser tratados por la Máxima autoridad, Gerente de Sistemas, Responsable de seguridad informática y en casos extremos que se necesite la participación de otras áreas se deberá incluir en las coordinaciones a los demás Gerentes de la empresa	A.6.1.2 Coordinación de la seguridad de la información	Secundario
Presidente Ejecutivo	No se tiene designado formalmente a un "Responsable de Seguridad Informática"	Se deberá designar formalmente al "Responsable de Seguridad informática" y definir claramente las actividades que debe realizar, de tal forma que se encargue de mitigar todos los temas relacionados con la seguridad informática y seguridad de la información. Es importante que todos los funcionarios conozcan quien es el "Responsable de Seguridad informática", de tal forma que puedan saber a quién dirigirse oportunamente en casos de incidentes de seguridad.	A.6.1.3 Asignación de responsabilidades de la Seguridad de la Información	Primario

Sistemas	Inexistencia de proceso de autorización de utilización de nuevos sistemas	Se debe elaborar un procedimiento de autorización de nuevos sistemas en la empresa, además se debe incluir un registro donde se pueda evidenciar la conformidad de la utilización del nuevo sistema dentro de la empresa, por parte del área que solicita su implementación.	A.6.1.4. Proceso de autorización para los medios de procesamiento de información	
Responsable de Seguridad Informática, Recursos Humanos, Administrativo, Sistemas	Se incluye en el contrato de los funcionarios una cláusula que indica que el trabajador se compromete expresamente a guardar confidencialidad y reserva de la información.	El área de Recursos Humanos, Administrativo y Sistemas en coordinación con el Responsable de Seguridad Informática deberán elaborar un acuerdo de confidencialidad y no divulgación de la información para los funcionarios, proveedores, contratistas, en el que se debe al menos detallar lo siguiente: Compromiso de responsabilidad en el manejo de la información que se le proporcione. Obligación de mantener la reserva o confidencialidad de la información durante y después de su contrato No reproducir, divulgar, ni copiar parcial o totalmente la información que se le proporcione	A.6.1.5.Acuerdos de confidencialidad	Primario

		Responsabilidad absoluta de los daños que pudiesen ocasionarle a la empresa la pérdida de información confidencial por mal manejo o divulgación de la información. Además se deberá incluir la aceptación y entendimiento de lo expuesto en el acuerdo de confidencialidad y no divulgación de la información.		
Recursos Humanos, Responsable de Seguridad Informática	Contacto apropiado con entidades externas	Se debe actualizar y revisar periódicamente el listado de contactos.	A.6.1.6 Contactos con autoridades	Secundario
Responsable de Seguridad Informática	No existe contacto con grupos o empresas que aporten conocimientos, referentes a seguridad de la información	Se debe identificar las empresas que actualmente estén aplicando controles de seguridad basados en las mejores prácticas de seguridad, de tal forma que se pueda intercambiar conocimientos y opiniones de implementación de nuevos controles de seguridad dentro dela empresa.	A.6.1.7 Contacto con grupos de interés especial	Secundario
Responsable de Seguridad Informática	Inexistencia de revisiones independientes de seguridad	Se debe monitorear todos los controles implementados actualmente para garantizar que estén funcionando correctamente, y no deriven ninguna nueva	A.6.1.7 Revisión independiente de la seguridad de la información	Secundario

			vulnerabilidad. Es importante realizar revisiones independientes de la seguridad de la información para poder garantizar que los controles implementados y procedimientos utilizados para la seguridad de la información son los adecuados.		
Entidades Externas	Sistemas, Responsable de Seguridad Informática	No existe un análisis que permita la identificación de riesgos cuando se debe otorgar accesos a terceras personas	Se debe planificar un análisis de riesgos referente al acceso a la información que tienen las terceras, de tal forma que se identifique vulnerabilidades que pueden existir.	A.6.2.1 Identificación de riesgos relacionados con entidades externas	Primario
	Sistemas, Administrativo, Responsable de Seguridad Informática	No existen controles y acuerdos de responsabilidades para personal externo que tenga que realizar trabajos dentro de la empresa.	Es importante que en caso de requerir servicios de personal externo a la empresa, este firme y tenga conocimiento de sus responsabilidades y obligaciones en el manejo de la información, equipos de procesamiento de la información. Adicionalmente de deben establecer controles de seguridad y actividades que permitan identificar posibles riesgos a los que están expuestos los sistemas de procesamiento de información y la información física a la cual necesitan tener acceso personal externo que se haya contratado	A.6.2.2 Tratamiento de la seguridad cuando se trabaja con clientes A.6.2.3 Tratamiento de la seguridad en contratos con terceras personas	Secundario

			para realizar trabajos dentro de la empresa.		

3. Gestión de Activos

Responsabilidad por los activos	Propietario de la Información	No poseen inventarios de inventarios de equipos de red, licencias, software, periféricos entre otros activos importantes de la empresa	Se debe elaborar un inventario de activos por cada categoría (software, hardware, estructura organizacional), de tal forma que se pueda identificar claramente los activos con los que cuenta actualmente la empresa.	A.7.1.1 Inventarios de activos	Primario
	Presidente Ejecutivo	No existe un documento formal donde se designen a los responsables de la información y de los activos asociados con los medios de procesamiento de la información, y demás activos.	Luego de que el Responsable de Seguridad Informática en coordinación con las áreas pertinentes, clasifique los activos por categoría, la Máxima autoridad deberá designar formalmente a los Propietarios de la Información, los cuales tendrán la responsabilidad de actualizar la matriz de activos que estén a su cargo.	A.7.1.2 Propiedad de los activos	Primario
	Responsable de Seguridad Informática	Existencia de políticas para el correo institucional e internet.	Dentro de las políticas de correo electrónico institucional y de internet se deberá detallar lo que se debe considerar para el uso aceptable de correo e internet así como lo que se considera como	A.7.1.3 Uso aceptable de los activos	Secundario

			uso inaceptable. Adicionalmente se deberá incluir controles de uso aceptable del resto de activos de información.		
Clasificación de la información	Propietario de la Información, Responsable de Seguridad Informática	No se encuentran establecidos criterios para la clasificación de la información	Se debe elaborar un catálogo de clasificación de la información en el cual se establezca que documentos son confidenciales o de uso interno. El Responsable de Seguridad Informática deberá monitorear el cumplimiento de elaboración de este catálogo, el cual posteriormente deberá ser socializado a los funcionarios.	A.7.2.1 Lineamientos de clasificación de la información	Secundario
	Responsable de Seguridad Informática	No se encuentran definidos criterios para la el etiquetado de la información	Se debe elaborar lineamientos para el etiquetado de información tato física como lógica, el cual deberá ser actualizado por lo menos cada 6 meses.	A.7.6.2 Etiquetado y manejo de la información	Secundario

4. Seguridad de los Recursos Humanos

Antes del empleo	Recursos Humanos, Administrativo	No tienen documentadas las funciones y responsabilidades de los funcionarios	Se debe documentar y definir los roles y responsabilidades de los funcionarios de la empresa, pasantes o practicantes y contratistas.	A.8.1.1 Roles y responsabilidades	Primario

	Recursos Humanos	El área de Recursos Humanos tiene definido el proceso de contratación del personal, pero no lo tienen documentado, pues es un proceso que lo siguen a partir de que la nueva Jefe de recursos Humanos labora ahí.	Se debe documentar el proceso actual que se tiene para la contratación de funcionarios	A.8.1.2 Selección A.8.1.3 Términos y condiciones de empleo A.8.3.1 Responsabilidades de terminación	Primario
	Recursos Humanos, Responsable de Seguridad Informática, Sistemas, Administrativo	No establecen responsabilidades y obligaciones que deben tener en referencia a la seguridad de la información	Se debe incluir en los contratos las obligaciones y responsabilidades que tienen que cumplir los funcionarios y/ o contratistas, acorde a las políticas de seguridad de la información.	A.8.2.1 Gestión de responsabilidad	Primario
Durante el empleo	Responsable de Seguridad Informática	No existe una adecuada capacitación ni conocimiento acerca de los temas relacionado con Seguridad de la información.	Es necesario que se planifiquen capacitaciones tanto para el personal que maneja la seguridad de la información como para los funcionarios, de tal forma que ambos estén conscientes de las consecuencias de llegar a perder, dañar y alterar información importante de la empresa. Al menos debe realizarse dos capacitaciones al año de temas de seguridad de la información	A.8.2.2 Capacitación y educación en seguridad de la información	Primario

	Recursos Humanos, Responsable de Seguridad Informática	No existe un procedimiento que indique las sanciones en caso de faltas cometidas en la seguridad de los sistemas de procesamiento de información o información física que manejan.	Es necesario que se elabore un procedimiento, clausulas o se establezcan controles que detallen claramente las sanciones que tendrá un empleado en caso de cometer alguna violación en la seguridad de los sistemas de procesamiento de información o información física que manejan.	A.8.2.3 Proceso disciplinario	Primario
Terminación o cambio del empleo	Recursos Humanos	No existen procedimientos donde indiquen que antes del término de contrato laboral deben devolver los activos fijos que se les ha entregado al inicio de sus labores.	Se deberá elaborar una lista de verificación en el cual se detalle todos los activos fijos que se le entrega al funcionario al inicio de sus actividades, el cual será firmado por el funcionario de tal forma que cuando el funcionario termine su relación laborar con la empresa, se verifique que está entregando los activos que estuvieron bajo su responsabilidad y en casos de daños de activos debe tener su debida justificación.	A.8.3.2 Devolución de activos	Secundario
	Recursos Humanos, Responsable de seguridad informática	No existe un proceso formal para la eliminación de derechos de accesos	Se deberá documentar formalmente el proceso de eliminación de accesos, de tal forma que el área de Recursos Humanos comunique oportunamente Responsable de Seguridad Informática, la salida de un funcionario con la finalidad de que los accesos sean eliminados inmediatamente.	A.8.3.3 Eliminación de derechos de acceso	Primario

5. Seguridad física y ambiental

Áreas Seguras	Administrativo	El edificio en el que se encuentra la empresa alquila dos piso, únicamente en el primer piso es donde se encuentra el área de recepción, no se supervisa al personal (terceros) que se dirige al segundo piso.	Debido a que la empresa utiliza dos pisos para el funcionamiento de las diferentes áreas, siempre que sea posible debe establecer otro punto de recepción en el segundo piso, para prevenir que personal no autorizado o ajeno a la empresa ingrese a las áreas sin la supervisión debida.	A.9.1.1 Perímetro de seguridad física	Primario
	Administrativo	El área de Sistemas es la única área que cuenta con un mecanismo de control de acceso por ser considerada un área restringida.	Por temas de seguridad física, se debe considerar la colocación de mecanismos de accesos en las entradas de cada área, de tal forma que se garantice que solo el personal autorizado ingrese a dichas áreas	A.9.1.2 Controles de entrada físicos	Secundario
	Administrativo	Inadecuada separación entre las áreas de Caja y Control de calidad	Se debe considerar la correcta separación del área de Control de Calidad del área de Cajas, para evitar que clientes o personal externo acceda al área de Control de Calidad sin autorización	A.9.1.3 Seguridad de oficinas, habitaciones y medios	Primario
	Administrativo	No existen detectores de humo, ni alarmas contra incendios.	Por termas de seguridad de los funcionarios, seguridad de la información y de los equipos de procesamiento de información, se debe de contar al menos con alarmas que detecte humo para así prevenir daños en casos de incendios.	A.9.1.1 Perímetro de seguridad física A.9.1.4 Protección contra amenazas externas y ambientales	Primario Secundario

Administrativo	El sistema de cámaras no es propio de la empresa, lo maneja personal ajeno, pues el edificio en el que se encuentran no es propio, lo comparten con más empresas.	Es importante que la empresa monitoree la entrada y salida principalmente de personal externo mediante un sistema de video cámaras.	A.9.1.1 Perímetro de seguridad física	Secundario
Sistemas	El Rack de comunicaciones así como el UPS se encuentra dentro del área de Sistemas, en un espacio físico separado, las llaves las tiene únicamente la Especialista de Redes y Bases de datos.	Es necesario considerar un back up para el manejo de las llaves del Data Center en caso de no encontrase el Responsable principal. De ser posible implementar un mecanismos de acceso al área donde se encuentran estos equipos Adicionalmente se deben considerar todas las medidas de seguridad para el área donde se encuentra el Rack de comunicaciones y UPS	A.9.1.2 Controles de entrada físicos A.9.1.5 Trabajo en áreas seguras	Secundario Primario
Administrativo	Las áreas no se pueden identificar fácilmente, pues no cuentan con el señalamiento apropiado. Así mismo el área donde está el Rack y UPS no cuenta con la señalética	Se debe considerar el uso de señalamiento en las áreas, en el cual se indique el nombre del área para que así todos puedan conocer donde se encuentra cada área, además en coordinación con el área Sistemas se deberá colocar	A.9.1.3 Seguridad de oficinas, habitaciones y medios A.11.6.2 Aislamiento del sistema sensible	

		adecuada.	señalética adecuada (no fumar, no comer, área restringida, entre otros), dentro y fuera del área donde se encuentra el rack de comunicaciones y UPS		
Seguridad del Equipo	Administrativo	Todos los equipos están ubicados dentro de las áreas, de esa forma intentan limitar los accesos no autorizados de personas ajenas a la empresa.	Es necesario que se implementen mecanismos de accesos en las áreas	A.9.1.2 Controles de entrada físicos	Secundario
	Sistemas	Se cuenta con un UPS que les permite tener energía eléctrica 20 minutos después que ocurre el corte de energía, lo que les permite a los funcionarios guardar la información y apagar las computadoras para evitar daños	Se debe considerar el uso de un UPS que les permita tener electricidad cuando el servicio público tenga fallas, de tal forma que no se paralicen las actividades normales dentro de la empresa	A.9.2.2 Servicios públicos	Primario
	Sistemas	Inexistencia de bitácoras donde se registren los mantenimientos realizados a los equipos .	Se debe registrar todos los mantenimientos que se realicen en los sistemas de procesamiento de la información, por lo que se debe elaborar una bitácora donde se registre al menos lo siguiente: Responsable, nombre del equipo al cual se le dio mantenimiento, hora, fecha, tarea realizada.	A.9.2.4 Mantenimiento de equipo	Secundario

	Sistemas	Prohibición de sacar equipos de la empresa.	Se debe documentar la prohibición de sacra los equipos de la empresa, además las laptops de la empresa utilizada por los altos directivos fuera de la misma, debe contar con todas las medidas de seguridad como si estuviera dentro de la empresa. (antivirus, autenticación de usuario, entre otras)	A.9.2.5 Seguridad del equipo fuera del local A.9.2.7 Traslado de propiedad	Primario Secundario

6. Gestión de las Comunicaciones y operaciones

Procedimientos y responsabilidades operacionales	Sistemas	Inexistencia de documentación de los procedimientos de operación	Se debe documentar todos los procedimientos de las tareas que se realizan, de tal forma que queden registros y la evidencia de las actividades, cambio o trabajos realizados en los sistemas de procesamiento de información	A.10.1.1 Procedimiento de operación documentados	Secundario
	Sistemas	Cuentan con un procedimiento de Gestión de cambio, pero este no se encuentra documentado	Documentar el procedimiento que se tiene para la Gestión de cambios, y de ser necesario crear instructivos donde se pueda detallar paso a paso las correctas acciones a seguir.	A.10.1.2 Gestión de cambio	Secundario
	Sistemas	La Jefa de Desarrollo e implementación de sistemas es quien se encarga de designar al personal que debe participar en cada una de las fases de producción o actualización de un sistema.	Se debe tener documentado y definidas cada una de las responsabilidades que se tiene en el desarrollo de sistemas	A.10.1.3 Segregación de deberes	Primario

	Sistemas, Responsable de Seguridad Informática	No se encuentra documentado las actividades que deben realizarse en cada ambiente: Desarrollo, Pruebas, Capacitación y Producción, debido a que es la Jefa de Desarrollo e Implementación de Sistemas quien se encarga de indicar al personal que actividades se deben realizar en cada fase(ambiente).	Como una buena práctica se debe definir dentro del manual de Políticas de Seguridad de la Información, las actividades que se deben realizar en cada ambiente (Desarrollo, Pruebas, Capacitación y Producción), estos ayudarán a llevar un mejor control de las tareas. Además es importante incluir controles de seguridad que indiquen que personal debe participar en cada ambiente, así se puede evitar accesos no autorizados o cambios no autorizados en el sistema de operación.	A.10.1.4 Separación de los medios de desarrollo y operacionales	Primario
Gestión de la entrega del servicio de terceros	Sistemas, Responsable de Seguridad Informática	El área de Sistemas al encargarse de la contratación de los servicios de terceros, es quién define los términos que deben cumplir los proveedores y revisa que lo entregado esté acorde a lo solicitado.	En la contratación de servicios externos, se debe considerar ciertos criterios de seguridad, de tal forma que a más que se cumpla con lo que se esté contratando, se pueda garantizar que el servicio adquirido no va a generar nuevas vulnerabilidades de seguridad. Además se pueden incorporan controles de seguridad para que el área de Sistemas o Responsable de Seguridad Informática realice el monitoreo y revisión periódica del sistemas o servicio contratado.	A.10.2.1 Entrega de servicio A.10.2.3 Manejar los cambios en los servicios de terceros	Primario Secundario

	Sistemas, Responsable de Seguridad Informática	No se realiza monitoreo de los servicios que proveen terceras partes	Es importante revisar que los servicios que proveen terceras partes, estén funcionando acorde a lo contratado y que no esté afectado en las actividades diarias. Toda revisión debe ser registrada y documentada de tal forma que en casos de incumplimientos se pueda tener evidencia y exigirle a los contratistas que mejoren o arreglen el servicio ofrecido	A.10.2.2 Monitoreo y revisión de los servicios de terceros	Primario
Planeación y aceptación del sistema	Sistemas	No se realizan análisis de Gestión de capacidad que les permita tener una proyección del uso de los recursos	Para prevenir la disponibilidad de los recursos informáticos que utiliza la empresa, es importante que se realice por lo menos una vez al año, la Gestión de Capacidad, la cual permite realizar proyecciones del uso de recursos para asegurar el desempeño óptimo de los sistemas utilizados.	A.10.3.1 Gestión de capacidad	Secundario
	Responsable de seguridad informática	No se tiene definido criterios de seguridad para la aceptación del sistema	Se debe definir y establecer criterios de seguridad sobre los cuales serán revisados todos los nuevos sistemas o actualizaciones que se realicen en los sistemas de tal forma que se garantice que el sistema que se vaya a poner en producción no ocasiones nuevas vulnerabilidades de seguridad.	A.10.3.2 Aceptación del sistema	Primario

Protección contra software malicioso y código móvil	Responsable de Seguridad Informática	Se posee mecanismos para la detección de software malicioso en correos entrantes, además a cada computador de la empresa se le instala antes de entregarlo al funcionario el antivirus, pero no se realizan acciones de monitoreo para verificar periódicamente que el antivirus esté actualizado.	Es importante realizar monitoreo a intervalos regulares, de tal forma que se garantice que las políticas aplicadas en los computadores de la empresa se encuentren funcionando correctamente, por lo que el Responsable de Seguridad Informática debe elaborar una planificación que le permita revisar y registrar que las políticas de seguridad implementadas estén actualizadas y funcionen sin ningún tipo de problemas.	A.10.4.1 Controles contra software malicioso	Primario
Respaldo (Back - up)	Sistemas	Existe la política de respaldos de información, en la cual detallan tres frecuencias de respaldos que se realizan y la información que se respalda en cada una de ellas. Todas las tareas de respaldos son registradas en el documento "Bitácora Procesos especiales", en se detalla el responsable del respaldo, fecha, hora y observaciones en caso de que se llegue a presentar algún evento durante el proceso de respaldo de información.	Se debe incorporar en la bitácora utilizada para los registros de respaldos la firma del responsable y conformidad del Gerente de Sistemas	A.10.5.1 Back-up o respaldo de la información	Primario

Gestión de medios	Responsable de Seguridad Informática	Se encuentran bloqueados los medios removibles en los computadores de los funcionarios, con el propósito de evitar la fuga de información.	Se sugiere realizar actividades de monitoreo para garantizar que esta política de seguridad esté funcionando correctamente en los computadores de los funcionarios. Además se debe elaborar procedimientos para el manejo de información	A.10.7.1 Gestión de los medios removibles	Primario
				A.10.7.2 Eliminación de medios	Secundario
				A.10.7.3 Procedimientos de manejo de la información	Primario
				A.10.7.4 Seguridad de documentación del sistema	Secundario
Intercambio de información	Sistemas	Inexistencia de controles de seguridad para el intercambio de información, tanto de medios físicos como mensajería electrónica.	En el intercambio de información debe ser considerado controles de seguridad que permitan garantizar la integridad y confidencialidad de los datos físicos o lógicos, pues si no se consideran controles necesarios, este intercambio podría considerarse como un mecanismo de fuga de información.	A.10.8.1 Procedimientos y políticas de información y software	Primario
				A.10.8.2 Acuerdos de intercambio	Primario

			En caso de la información física que debe ser entregada fuera de los límites físicos de la empresa, es necesario asegurar que el servicio de mensajería contratado es confiable y la información enviada va a llegar a su destinatario de forma íntegra. Para el envío de información lógica se podría considerar la encriptación de la información, se podría considerar el uso de firmas electrónicas.	A.10.8.4 Mensajes electrónicos	Secundario
		La empresa cuenta con un equipo de mensajeros que son los responsables de llevar la documentación externa, asegurándose que la documentación enviada llega al destino indicado. Se lleva un registro donde constan las firmas de las personas externas que recibieron la documentación.	Debe elaborarse un procedimiento formal donde se indique responsabilidades y actividades que deben realizan el personal encargado de transportar la documentación de la empresa	A.10.8.3 Medios físicos en tránsito	Secundario
Monitoreo	Sistemas	No existe monitoreo de los registros de auditoría de los sistemas, consideran que no	En aplicación de las buenas prácticas se debe revisar a intervalos regulares los registros de	A.10.10.1 Registro de auditoría	Primario

		es necesario revisar las actividades realizadas en los sistemas.	auditoría de los sistemas de procesamientos de la información, registros de fallas, entre otros que permitan detectar actividades no autorizadas en los sistemas.	A.10.10.2 Uso del sistema de monitoreo	Primario
				A.10.10.3 Protección de la información del registro	Secundario
				A.10.10.4 Registros del administrador y operador	Primario
				A.10.10.5 Registro de fallas	Primario
				A.10.10.6 Sincronización de relojes	Secundario

7. Control de acceso

Requerimiento comercial para el control del acceso	Responsable de Seguridad Informática	No existe una política que establezca controles de seguridad para el control de accesos.	Se deberá incluir en el manual de Políticas de Seguridad de la Información, una política de control de accesos que permita definir responsabilidades para identificar, gestionar y mantener perfiles de los accesos de usuarios a los diferentes aplicativos	A.11.1.1 Política de control de acceso	Primaria
Gestión del acceso del usuario	Responsable de Seguridad Informática Sistemas	El área de Sistemas es la encargada de dar acceso a los diferentes aplicativos que necesita utilizar el funcionario mediante el formulario de "solicitud de acceso a usuarios"	Es importante que todo control de seguridad implementado sea revisado y monitoreado, de tal forma que se pueda garantizar que se está cumpliendo con aquellos controles. Así mismo es importante que mínimo una vez	A.11.2.1 Inscripción del usuario	Primario

		cada mes se realice la revisión del cumplimiento de depuración de cuentas de usuarios que ya no están siendo utilizadas.		
Sistemas	El sistema Financiero no pide cambio de clave	Se debe incorporar en el sistema Financiero el cambio de clave mínimo 1 vez al mes	A.11.2.3 Gestión de la clave del usuario	Primario
Sistemas	El área de Recursos Humanos y el personal de Verificaciones telefónicas tienen acceso de modificación al módulo de "Datos Personales" de los funcionarios, lo que significa un alto riesgos de integridad de datos	Debido a incidentes de seguridad presentados, es necesario que se revise los accesos de los funcionarios a los módulos de ISISystem, de tal forma que se restringa y controle la asignación de privilegios adecuada, para evitar modificaciones o eliminaciones de información, así se garantiza que los usuarios solo podrán modificar o eliminar lo que esté acorde a las funciones que desempeña	A.11.2.4 Revisión de los derechos de acceso del usuario	Primario
Responsable de Seguridad Informática Sistemas	Debido a la alta demanda de bloqueo de las estaciones de trabajo, el área de Sistema delego a cada Supervisor de área, la actividad de desbloqueo, es decir que cada Supervisor para que puedan desbloquear a las estaciones de trabajo de los usuarios y que sigan inmediatamente	La gestión de accesos solo debe ser manejada por el Responsable de seguridad informática o un personal designado del área de Sistemas de tal forma que se minimicen vulnerabilidades en la gestión de claves de usuario	A.11.2.3 Gestión de la clave del usuario	Primario

		con sus actividades normales.			
Responsabilidad del usuario	Responsable de Seguridad Informática Sistemas	No existe un mecanismo que permite bloquear automáticamente las estaciones de trabajo cuando se encuentran desatendidas. Son pocos los funcionarios que bloquean sus computadoras cuando necesitan salir de su puesto de trabajo.	Como adopción de una buena práctica, se debe implementar un mecanismo que permita el bloqueo automático de los computadores cuando están desatendidos.	A.11.3.2 Equipo de usuario desatendido	Primario
			Además el Responsable de Seguridad Informática debe incluir en las capacitaciones de seguridad de la información a los usuarios, el tema de bloqueo de computadoras cuando no estén haciendo uso de ellas, en especial cuando no están en sus puestos de trabajo.	A.11.3.3 Política de pantalla y escritorio limpio	Secundario
	Responsable de Seguridad Informática	Se tiene establecido la utilización de mínimo 6 caracteres para la creación de las contraseñas en los aplicativos, la mayoría de funcionarios utiliza los parámetros de caracteres establecidos, pero no guardan la confidencialidad debida de sus contraseñas, pues de vez en cuando las comparten con sus compañeros.	Incluir en las capacitaciones de seguridad de la información a los usuarios, el tema de confidencialidad de las contraseñas que manejan los usuarios	A.11.3.1 Uso de clave	Primario

	Responsable de Seguridad Informática	Las áreas que almacenan información confidencial no cuentan con la seguridad física requerida.	Se debe adoptar controles de seguridad que permitan concientizar a los funcionarios, se sugiere implementar una política de pantallas y escritorios limpios, de esta forma se minimizan riesgos de fuga de información.	A.11.3.3 Política de pantalla y escritorio limpio	Secundario
Control de acceso a redes	Sistemas	La red de la empresa no se encuentra segmentada, cada usuario de la red puede acceder libremente a las IP's de los servidores lo que ocasiona que pudiesen aprovecharse de una debilidad de configuración.	Se debe crear un segmento de red específicamente para administración de servidores y otro segmento de red donde solamente los usuarios tengan acceso y a los servicios de red de la empresa, así como incorporar controles para salvaguardar la confidencialidad y datos que pasan por las redes locales e inalámbricas. Es necesario establecer dentro del manual de políticas de seguridad de la información controles sobre el uso de servicios de red	A.10.6.1 Controles de red	Primario
				A.10.6.2 Seguridad de los servicios de red	
				A.11.4.1 Política sobre el uso de servicios en red	Primario
				A.11.4.3 Identificación del equipo en red	Primario
				A.11.4.5 Segregación en redes	Primario
				A.11.4.6 Control de conexión de redes	Primario
				A.11.4.7 Control de routing de redes	Primario
	Sistemas	Existen redes inalámbricas (wifi) que es utilizado por la máxima autoridad, incluyendo Gerentes y Subgerentes, la cual está	Siempre que sea posible se deberá mantener registros de accesos a la red wifi que permita detectar accesos no autorizados a la misma.	A.10.6.1 Controles de red	Primario
				A.10.6.2 Seguridad de los servicios de red	Primario

		abierta sin ningún tipo de seguridad, cualquier funcionario que sepa la clave y usuario puede acceder a ella, sin quedar videncia alguna.		A.11.4.1 Política sobre el uso de servicios en red	Primario
				A.11.4.3 Identificación del equipo en red	Primario
				A.11.4.5 Segregación en redes	Primario
				A.11.4.6 Control de conexión de redes	Primario
				A.11.4.7 Control de routing de redes	Primario
Control de acceso al sistema de operación	Sistemas	Cada funcionario maneja como mínimo tres USER ID	Se sugiere que se sincronicen los identificadores de los usuarios ISISystem con la estación del trabajo, para evitar la creación de varios usuarios innecesarios para un mimo funcionarios, lo cual dificulta dificulten el monitoreo de estas cuentas. Además en aplicación a las buenas prácticas de seguridad se sugiere que todos los aplicativos pidan cambio de contraseña por lo menos una vez al mes.	A.11.5.1 Procedimiento de registro en el terminal	Primario
				A.11.5.2 Identificación del usuario	Primario
				A.11.5.3 Sistema de gestión de claves	Primario
				A.11.5.4 Uso de utilidades del sistema	Primario
				A.11.5.5 Sesión inactiva	Secundario

				A.11.5.6 Limitación de tiempo de conexión	Primario
8. Adquisición, desarrollo y mantenimiento de los sistemas de información					
Requerimiento de seguridad de los sistemas	Sistemas, Responsable de Seguridad Informática	No existe una política donde se determine los requerimientos de seguridad para el desarrollo o adquisición de un sistema de información	El área de Sistemas en coordinación con el Responsable de Seguridad Informática deberá definir y detallar controles de seguridad los cuales deben ser exigidos para el desarrollo o adquisición de un software.	A.12.1.1 Análisis y especificación de los requerimientos de seguridad	Primario
				A.12.2.1 Validaciones de entrada	Secundario
				A.12.2.2 Control de procesamiento interno	Secundario
				A.12.2.3 Integridad del mensaje	Secundario
				A.12.2.4 Validación de salida	Secundario
Seguridad en los procesos de desarrollo y soporte	Sistemas	No existe documentación formal donde se detalle las actividades que se realizan en cada instancia (desarrollo, pruebas, capacitación y producción).	Es importante definir las actividades de cada ambiente de operación del sistema, para que así se pueda controlar el ingreso y manejo del código fuente, únicamente por personal autorizado.	A.12.4.1 Control de software operacional	Primarios
				A.12.4.3 Control de acceso al código fuente del programa	Secundario
			Así mismo se debe elaborar un procedimiento para la gestión de cambios tanto para software, base de datos y hardware, que permita	A.12.5.1 Procedimientos de control de cambio	Primario

		registrar el paso del ambiente de pruebas a producción, el cual al menos debe reflejar la siguiente información: archivos a modificar, script de base de datos, creación de directorios, plan de contingencias, protocolo de pruebas de verificación del cambio, entre otra información que se considere importante y acorde al cambio realizado en software, bases de datos o hardware.	A.12.5.2 Revisión técnica de las aplicaciones después de cambios en el sistema operativo A.12.5.3 Restricciones sobre los cambios en los paquetes de software A.12.5.5 Desarrollo de outsourced software	Secundario Primario Primario
Sistemas Responsable de Seguridad Informática	No existe una política formal donde se detalla los controles a implementar para prevenir la fuga de información, lo que se tiene implementado como medida de seguridad es la inhabilitación de todo medio extraíble de almacenamiento, este control se exceptúan para los altos directivos, gerentes y subgerentes	Es primordial que se implemente una política de fuga de información que permita determinar controles que eviten perdida de confidencialidad, integridad y disponibilidad de la información, de tal forma que la empresa no pierda credibilidad, ni información importante para la gestión del negocio. El Responsable de Seguridad Informática debe ser incluir este tema en la concientización a los funcionarios.	A.12.5.4 Fuga de información	Primario

Gestión de vulnerabilidad técnica	Sistemas	No se realiza ninguna acción de monitoreo y control ante posibles vulnerabilidades técnicas de los sistemas, que permitan dar un trato adecuado a posibles nuevos riesgos de seguridad	Se debe elaborar un procedimiento para la gestión de vulnerabilidad técnica que en base a errores públicos conocidos se monitoree posible vulnerabilidades en los servicios, aplicaciones, sistemas operativos entre otros que son utilizados en la empresa.	A.12.6.1 Control de vulnerabilidades técnicas	Secundario
9. Gestión de incidentes en la seguridad de la información					
Reporte de eventos y debilidades en la seguridad de la información	Responsable de Seguridad Informática	En el último año se han reportado al área de Sistemas dos casos de incidentes de seguridad.	Los incidentes de seguridad ocurridos deben documentarse, para así tener registros con al menos: responsable a quienes ele reporto el incidentes, fecha, hora, detalle de lo ocurrido, solución dada, entre otra información que se considere importante	A.13.1.1 Reporte de eventos en la seguridad de la información A.13.1.2 Reporte de debilidades en la seguridad	Primario Primario
Gestión de incidentes y mejoras en la seguridad de la información	Responsable de Seguridad Informática	No existe un procedimiento para el manejo de la gestión de incidentes	Se debe elaborar un procedimiento para la gestión de incidentes, en el cual se establezcan responsabilidades y acciones que se realizarán en caso de que se llegue a presentar un incidente de seguridad mayor	A.13.2.1 Responsabilidades y procedimientos	Primario
	Responsable de Seguridad Informática	No se tiene establecidas responsabilidades para la gestión de incidentes, además no se encuentra definido las acciones correctivas que se realizan luego de un incidente de	Todo incidente de seguridad que se presente que se considere de tipo medio o alto, debe estar documentado para que de esa forma se puedan establecer un antecedente y poder tomar medidas correctivas, de tal forma que no se	A.13.2.1 Responsabilidades y procedimientos A.13.2.2 Aprendizaje de los incidentes en la seguridad de la información	Primario Secundario

		seguridad.	presente nuevamente. De ser el caso se debe anexar evidencia de lo ocurrido.	A.13.2.3 Recolección de evidencia	Secundario

10. Gestión de la continuidad comercial

Aspectos de la seguridad de la información de la gestión de continuidad comercial	Sistemas	En la Gestión de continuidad de la empresa no se ha considerado la inclusión de la seguridad de la información.	Es importante que la Gestión de la continuidad de la empresa se incluyan la seguridad de la información, de tal forma que se puedan definir planes de acción en caso de daños en los servicios y aplicaciones críticas del negocio, para así contrarrestar interrupciones que afecten la continuidad de las actividades propias del negocio	A.14.1.1 Incluir seguridad de la información en el proceso de gestión de continuidad comercial	Primario
				A.14.1.2 Continuidad comercial y evaluación del riesgo	Primario
				A.14.1.3 Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Secundario
				A.14.1.4 Marco referencial para planeación de la continuidad comercial	Primario
				A.14.1.5 Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales	Secundario

11. Cumplimiento

Cumplimiento con requerimientos legales	Sistemas, Legal, Responsable de Seguridad Informática	No poseen lineamientos de seguridad que eviten incumplimiento por la reproducción, copia o alteración de información sobre la cual la empresa no tiene derecho de autor	Se debe considerar establecer controles de seguridad para evitar incurrir en incumplimientos con las leyes vigentes ecuatorianas sobre el derecho de propiedad intelectual. Complementariamente se debe incluir aspectos que permitan el cumplimiento con las políticas de la empresa, políticas de seguridad así como el cumplimiento de las observaciones de los organismos de control que regulan a la empresa. Además como en la empresa se utiliza las grabaciones de llamadas para controlar la calidad de atención que da el call center a los clientes, se debe incluir controles de seguridad que prohíban la duplicación , convertir en otro formato las grabaciones de llamas.	A.15.1.1 Identificación de legislación aplicable A.15.1.2 Derechos de propiedad intelectual (IPR) A.15.1.3Protección de los registros organizacionales A.15.1.5 Prevención de mal uso de medios de procesamiento de información A.15.2.1 Cumplimiento con las políticas y estándares de seguridad A.15.3.1 Controles de auditoria de sistemas de información	Primario Secundario Secundario Primario Primario Primario

4.1.6. Metodología de Análisis de riesgos

La identificación de riesgos es una actividad fundamental a realizar si se quiere diseñar un Sistema de Seguridad de la Información (SGSI), ya que en primera instancia es necesario identificar los factores que puedan amenazar a la empresa y conocer las vulnerabilidades que pueden ser explotadas por las amenazas.

MAGERIT es una metodología que abarca de forma completa, las pautas a seguir para el análisis de riesgos, a la vez que se encuentran alineadas a los estándares de gestión de riesgos ISO 27005 e ISO 31000.

4.1.6.1. Fases de ejecución del análisis de riesgos de MAGERIT

1. Identificación de Activos

Se determinan los activos que son de valor significativo para la empresa, en los que el impacto por la ausencia, deterioro o pérdida del activo se traducen en problemas para afrontar la continuidad del negocio.

2. Determinar las Amenazas

Identificar todos los factores internos o externos que pueden inferir un daño a los activos de información de forma predeterminada o accidental con el fin de poder evaluar la magnitud del deterioro ejercido sobre el activo y la probabilidad de ocurrencia en la que puede darse.

3. Determinar las salvaguardas

Se debe conocer las salvaguardas desplegadas con el propósito de poder conocer el impacto al activo de información, aplicando una contramedida a la vulnerabilidad cuando esta sea explotada, conociendo con mayor exactitud el riesgo a afrontar.

Cuando existe una salvaguarda desplegada, estas pueden disminuir el daño sobre el activo de información y la probabilidad de que una amenaza pueda afectar a la empresa.

4. Estimación del impacto ejercido por las amenazas

Se debe conocer cuál sería el impacto resultante del daño infringido por la amenaza cuando esta se materializa de tal forma que se pueda determinar el estado del activo luego del suceso.

5. Estimación del riesgo

Se determina que el riesgo sobre las amenazas sean estas de carácter potencial o residual en base la expectativa de ocurrencia de la amenaza, considerando si existen o no salvaguardas desplegadas.

4.1.7. Análisis de Riesgo

4.1.7.1. Activos de Información

4.1.7.1.1. Propietarios de la Información

Se les llamará "Propietarios de la información" al funcionario que tenga un cargo de dirección dentro de cada área, quien tendrá la responsabilidad de otorgar accesos a los activos de información, tomando en cuenta las funciones que realiza cada funcionario dentro del área a la cual pertenecen.

4.1.7.1.2. Identificación de activos de Información

Para la identificación de los activos de información y su clasificación se consideró únicamente las áreas críticas de la empresa, matriz que se obtuvo en coordinación los directivos de dichas áreas.

Los criterios de clasificación que se utilizaron fueron los siguientes:

Tabla 5. Cuadro de clasificación de valores de activos – Confidencialidad

Valor	Confidencialidad
3	Información que sólo puede ser accedida por funcionarios que estén autorizados debido al daño que podría causar si es divulgado dentro o fuera de la empresa.
2	Información que solo puede ser accedida por funcionaros la .necesiten para realizar una labor determinada dentro de la empresa
1	Información que puede ser accedida por cualquier funcionario sin necesidad de autorización

Tabla 6. Cuadro de clasificación de valores de activos – Integridad

Valor	Integridad
3	Información cuya modificación sin autorización es imposible de repararse, deteniendo cualquier actividad dependiente del activo.
2	Información cuya modificación sin autorización toma tiempo en exceso en repararse y puede ocasionar un daño en las actividades realizadas con el activo.
1	Información cuya modificación sin autorización es posible reparar, pero puede ocasionar un daño sobre las actividades realizadas con el activo

Tabla 7. Cuadro de clasificación de valores de activos - Disponibilidad

Valor	Disponibilidad
3	Recurso que no puede ser accedido durante un periodo corto de tiempo y que podría ocasionar la detención de las actividades de la empresa.
2	Recurso que no puede ser accedido durante un periodo mediano de tiempo y que podría ocasionar la detención de las actividades de la empresa.
1	Recurso que no puede ser accedido durante un periodo largo de tiempo y que podría ocasionar la detención de las actividades de la empresa

Tabla 8. Matriz de Activos de Información

Criticidad	Área	Propietario de la Información	Activo de Información	Documentos – Servicios - Aplicativos	Confidencialidad	Disponibilidad	Integridad	Clasificación actual
3	Crédito	Gerente de Operaciones	Información de Crédito - Datos del cliente en el Sistema	Carpeta Cliente: Solicitud y anexos del cliente Contratos Informes Aprobaciones Resoluciones internas Solicitudes de Crédito Registro de información	2	3	3	2
3	Crédito	Gerente de Operaciones	Información física de clientes directos	Solicitud de crédito física Contrato Pagaré de reserva de dominio buro de crédito Proforma de solicitud de compra	2	2	3	2
2	Crédito	Gerente de Operaciones	Información de crédito	Impresión de documentos Autorización reimpresión Instrumentar/reversar el créditos Datos de factura	2	2	2	2
2	Cobranzas	Subgerente de Operaciones Crédito y Cobranzas	Información física de Cobranzas - Datos del cliente	Informe de respuestas de cliente telefónica Reporte de gestión de cobranzas Registro de respuesta de verificación terrena	2	1	2	2

2	Cobranzas	Subgerente de Operaciones Crédito y Cobranzas	Información para el control de gestión	Gestiones atrasadas Cobranzas telefónicas Control de cartera Reporte de seguimiento	2	2	2	2
2	Cartera	Jefe de Cartera	Información de cartera - Datos del cliente	Registro de Información Estados de Cuenta, Pagos	2	1	2	2
3	Cartera	Jefe de Cartera	Información de Recuperación de Cartera	Hoja de negociación Solicitud de postergación de vencimiento de cuotas Control de desembolso	3	3	3	3
3	Cartera	Jefe de Cartera	Información de Reportes para Gestión de Cartera	Balance del cliente Movimientos de Caja Depuración de datos Cupones entregados por cajera Movimientos de pagos Reportes de control Liquidación Reportes Gerenciales	3	2	3	3
3	Sistemas	Gerente de Sistemas	Información de aplicaciones informáticas (Software)	Servicio de base de datos Servicio COM + (aplicativo y file server sistemas) Servicio de Antivirus Servicio de red (balanceo AD-contingencia base de datos) Ofimática Sistemas operativo Servicio de Máquinas Virtuales	2	3	3	3

				Servicio de proxy de navegación y correo Servicio Firewall GYE/ UIO Licencias Aplicativo ISYSystem Aplicativo Financiero				
2	Sistemas	Gerente de Sistemas	Información de Hardware	Equipos de cómputo Router Switch Módems Impresoras Copiadoras Servidores Periféricos Laptops	2	1	1	2
3	Sistemas	Gerente de Sistemas	Información de redes de comunicaciones	Central telefónica Telesynergy Central telefónica Telesynergy IP Sistema Telecontac Equipo de acceso remoto (Teamviewer) Telesynergy Red inalámbrica WIFI Rack de comunicaciones	3	3	3	3
3	Sistemas	Gerente de Sistemas	Soporte de información	Discos de respaldos Discos virtuales	3	2	3	3
2	Sistemas	Gerente de Sistemas	Equipamiento auxiliar	UPS	2	1	2	1

Tabla 9. Responsables de Activos de Información - ISISYSTEM

Sistema ISISYSTEM	Propietarios de la Información	
Módulo Central	Gerente de Operaciones	Subgerente de Operaciones
Módulo de Crédito	Gerente de Operaciones	Subgerente de Operaciones
Módulo Cartera	Jefa del Cartera	Jefe del área Administrativa
Módulo Cobranzas	Gerente de Operaciones	Subgerente de Operaciones
Módulo Personal	Jefe de Recursos Humanos	Subgerente de Operaciones

Tabla 10. *Responsables de Activos de Información – Financiero*

Sistema Financiero	Propietarios de la Información	
Módulo Contabilidad	Jefe del área Administrativa	Supervisor de Contabilidad
Módulo Cuentas por pagar	Jefe del área Administrativa	Supervisor de Contabilidad
Módulo Cuentas por cobrar	Jefe del área Administrativa	Supervisor de Contabilidad
Facturación	Jefe del área Administrativa	Supervisor de Contabilidad
Bancos	Jefe del área Administrativa	Supervisor de Contabilidad

4.1.7.2. Amenazas, vulnerabilidades, salvaguardas, impacto y riesgo residual de los activos de información

En la matriz que a continuación se muestra, se puede identificar los riesgos a los que están expuestos los activos de información de las áreas críticas de Credigestión, de tal forma que se puedan reforzar e incorporar controles de seguridad que permitan mitigar todas las vulnerabilidades existentes y poder protegerlos de amenazas internas y externas, evitando perder datos e información valiosa.

Se utilizó el siguiente criterio para la valoración de criticidad, probabilidad, impacto y riesgo:

Tabla 11. Valores de criticidad

Criticidad	
3	Alta
2	Media
1	Baja

Tabla 12. Valores de la probabilidad

Probabilidad	
3	Alta
2	Media
1	Baja

Tabla 13. Valores del impacto

Impacto	
3	Alta
2	Media
1	Baja

Tabla 14. Valores del Riesgo

Riesgo	
7- 9	Alta
4- 6	Media
1-3	Baja

Tabla 15. Matriz de Amenazas, vulnerabilidades, salvaguardas, impacto y riesgo residual

Activo	Crit.	Amenazas	Degradación causado por Amenazas			Vulnerabilidad	Salvaguardas implementadas	Prob.	Imp.	Rsg.
			Confd. %	Integ. %	Disp. %					
Información de Crédito - Datos del cliente en el Sistema	3	Modificación intencional de la información	0	100	0	No existen reglamentos de seguridad que delinean las responsabilidades y sanciones en el daño de la información Falta de concientización en el uso, manejo e importancia de la información Falta de procedimientos para el manejo de la información	Registros de auditoria (Sistema registra las acciones realizadas en el sistema) Respaldo de bases de datos diarias	2	3	6
		Eliminación intencional de información	0	0	100			2	3	6
		Fuga de Información	100	0	0			3	3	9
Información física de clientes directos	3	Fuga de Información	100	0	0	Falta de concientización en temas de seguridad de la información a los funcionarios Falta de seguridad físicas para documentos confidenciales (archiveros, caja fuertes) Falta de mecanismos de acceso al área Falta de procedimientos para el manejo de la información	No existen controles de seguridad	3	3	9
		Acceso no Autorizado	100	0	0			3	3	9
		Robo de Documentos	100	0	100			1	3	3

Información de crédito	2	Fuga de Información	100	0	0	Falta de concientización en temas de seguridad de la información a los funcionarios Falta de seguridad físicas para documentos confidenciales (archiveros, caja fuertes) Falta de mecanismos de acceso al área Falta de Catálogo de clasificación de la información Falta de procedimientos para el manejo de la información	No existen controles de seguridad	3	2	6
		Acceso no Autorizado	100	0	0			3	2	6
		Robo de Documentos	100	0	50			1	2	2
Información física de Cobranzas - Datos del cliente	2	Fuga de Información	100	0	0	Falta de concientización en temas de seguridad de la información a los funcionarios Falta de seguridad físicas para documentos confidenciales (archiveros, caja fuertes) Falta de mecanismos de acceso al área Falta de Catálogo de clasificación de la información Falta de procedimientos para el manejo de la información	No existen controles de seguridad	3	2	6
		Acceso no Autorizado	100	0	0			3	2	6
		Robo de Documentos	100	0	50			1	2	2

Información para el control de gestión	2	Fuga de Información	100	0	0	Información física: Falta de concientización en temas de seguridad a los funcionarios Falta de seguridad físicas para documentos confidenciales (archiveros, caja fuertes) Falta de mecanismos de acceso Información lógica: No existen reglamentos de seguridad que delinean las responsabilidades y sanciones en el daño de la información Falta de concientización en el uso, manejo e importancia de la información Falta de procedimientos para el manejo de la información	No existen controles de seguridad	3	2	6
		Acceso no Autorizado	100	0	0			3	2	6
		Robo de Documentos	100	0	50			1	2	2
Información de cartera - Datos del cliente	2	Errores y Fallos no intencionados	0	100	50	Información física: Falta de concientización en temas de seguridad a los funcionarios Falta de seguridad físicas para documentos confidenciales (archiveros, caja fuertes) Falta de mecanismos de acceso	No existen controles de seguridad	2	2	4
		Fuga de Información	100	0	0			3	2	6

						Información lógica: No existen reglamentos de seguridad que delineen las responsabilidades y sanciones en el daño de la información Falta de concientización en el uso, manejo e importancia de la información Falta de procedimientos para el manejo de la información				
Información de Recuperación de Cartera	3	Errores y Fallos no intencionados	0	100	50	Información física: Falta de concientización en temas de seguridad a los funcionarios Falta de seguridad físicas para documentos confidenciales (archiveros, caja fuertes) Falta de mecanismos de acceso Información lógica: No existen reglamentos de seguridad que delinean las responsabilidades y sanciones en el daño de la información Falta de concientización en el uso, manejo e importancia de la información	No existen controles de seguridad	2	3	6
		Fuga de Información	100	0	0			3	3	9
		Acceso no Autorizado	100	0	0			3	3	9
		Robo de Documentos	100	0	50			1	3	3

						Falta de procedimientos para el manejo de la información				
Información de Reportes para Gestión de Cartera	3	Fuga de Información	100	0	0	Falta de concientización en temas de seguridad de la información a los funcionarios	No existen controles de seguridad	3	3	9
		Acceso no Autorizado	100	0	0			3	3	9
		Robo de Documentos	100	0	50	Falta de seguridad físicas para documentos confidenciales (archiveros, caja fuertes) Falta de mecanismos de acceso al área Falta de procedimientos para el manejo de la información		1	3	3
Información de aplicaciones informáticas (Software)	3	Errores de monitorización	0	50	0	Inexistencia de procedimientos y controles para la Gestión de la Capacidad No se tiene documentado formalmente el procedimiento para la Gestión de Cambio. Además no existen registros (log's) de los cambios que se realizan Inexistencia de inventario de Software Autorizado Falta de controles de seguridad para los	Se realizan revisiones y pruebas supervisando que el aplicativo funcione adecuadamente. Perfiles de seguridad definidos. Formulario de solicitud de acceso a usuarios. Copias de Seguridad. Procedimientos e instructivos para copia de seguridad y Configuración de servicios definidos Plan de contingencia de Servidores	2	2	3
		Vulnerabilidades del software	0	80	90			1	3	3
		Caída del sistema por agotamiento de recursos	0	0	100			2	3	6
		Abuso de privilegios de acceso por parte del administrador	100	80	50			3	3	9
		Denegación del Servicio	0	0	100			1	3	3
		Manipulación no	80	50	50			2	2	5

		autorizada de programas por parte del administrador				ambientes de las etapas en la producción de software Falta de procedimientos y gestión para la identificación de vulnerabilidades técnicas	Políticas de restricción de correo Políticas de navegación de internet			
Información de Hardware	2	Fuego (Incendio)	0	0	100	Falta de mecanismos contra incendio, detector de humo dentro del centro de datos.	Mantenimientos semestrales de hardware Control de seguridad que prohíbe la salida de equipos de hardware de la empresa	1	2	2
		Polvo-Humedad	0	0	80			1	2	2
		Avería de Origen Físico	0	50	50	No existen mecanismos adecuados que provean de electricidad durante un corte de energía eléctrica prolongado.		2	1	2
		Corte del Suministro Eléctrico	0	0	100			3	2	6
		Robo	100	0	100	Falta de procedimientos y gestión para la identificación de vulnerabilidades técnicas en servidores y computadoras Falta de mecanismos de control de acceso en la mayoría de áreas Inexistencia de inventario del hardware que posee la empresa Falta de registros de mantenimiento realizados.		1	2	2
		Errores de actualización/Mantenimiento de hardware	0	0	50			2	1	2
Información de redes de comunicaciones	3	Suplantación de Identidad	100	80	50	Falta de procedimientos que prevengan suplantación en los medios de comunicación	Diagrama de conexión de los medios de comunicación	2	3	6
		Análisis de tráfico	100	0	0			2	3	6

		Interceptación de información	100	0	0	No existe encriptación en las vías de comunicación	Instructivo de configuración central telefónica	2	3	6
		Manipulación de Configuración	0	0	100	No existe ningún tipo de monitoreo en redes		1	3	3
		Fallo de servicio de comunicaciones	0	0	100	Faltan procedimientos que ayuden en la configuración de nuevos recursos de red y comunicación		1	3	3
		Errores y Fallos no intencionados	80	80	100	No hay soporte de un esquema de red alterno que permita mantener las operaciones No se han determinado segmentos de segregación en redes de comunicación		3	3	9
Soporte de información	3	Degradación de los soportes de almacenamiento de la información	0	0	100	Inexistencia de procedimientos y controles para la Gestión de la Capacidad	No existen controles de seguridad	2	3	6
		Avería de Origen Lógico	0	0	100	Inexistencia del registro de control de cambio de medios de almacenamiento		2	3	6
Equipamiento auxiliar	2	Avería de Origen Físico	0	0	100	No existen planes de mantenimiento específicos	No existen controles de seguridad	2	2	4

Tabla 16. Tabla de riesgos

Tabla de riesgo	media
Información de Crédito - Datos del cliente en el Sistema	7
Información física de clientes directos	7
Información de crédito	5
Información física de Cobranzas - Datos del cliente	5
Información para el control de gestión	5
Información de cartera - Datos del cliente	5
Información de Recuperación de Cartera	7
Información de Reportes para Gestión de Cartera	7
Información de aplicaciones informáticas (Software)	5
Información de Hardware	3
Información de redes de comunicaciones	6
Soporte de información	6
Equipamiento auxiliar	4

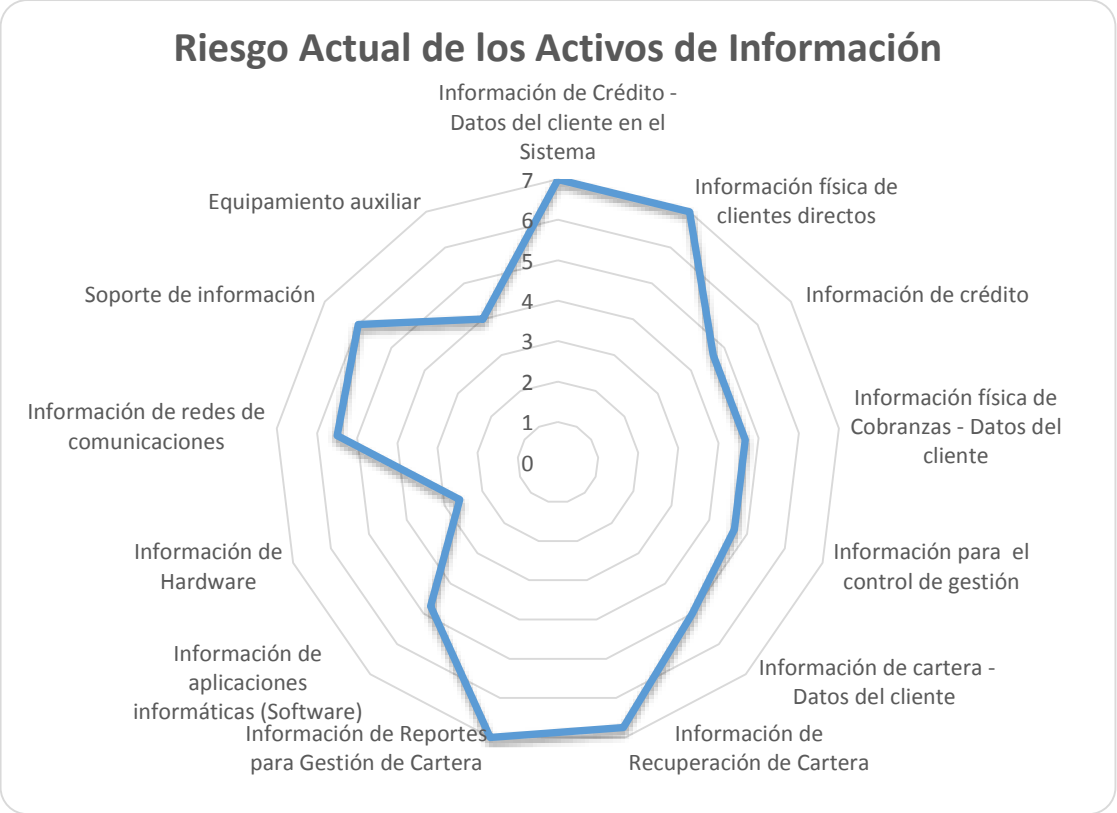

Figura 4. Representación de la media del riesgo actual de los activos de información

(Elaborado por: Kelly Bermúdez, Rafael Bailón)

4.2. Interpretación de Datos

Conforme al plan de recolección de información, se realizó una muestra selectiva para las encuestas a 23 personas de las diferentes áreas de la empresa y 3 personas del área de Sistemas. Se obtuvo los resultados que a continuación se muestran, donde es posible visualizar el nivel de la gestión de seguridad de la información de la empresa en estudio.

Pregunta:

¿Existen procedimientos e instructivos establecidos en el área?

Objetivo:

Identificar que el área posee instructivos de como los funcionarios deben realizar adecuadamente las actividades sin necesidad de tener una dependencia para su ejecución.

Tabla 17. Existencia de procedimientos establecidos

Detalle	Frecuencia	Porcentaje
Si	7	30,43
No	4	17,39
Desconoce	12	52,17

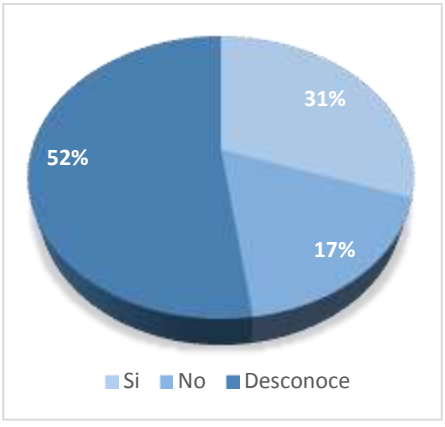

Figura 5. Respuestas obtenidas de los funcionarios sobre la existencia de procedimientos.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 30.43% de los funcionarios conocen que existen procedimientos e instructivos establecidos, el 17.39% no sabe acerca de estos, mientras un 52.16% dice no conocer nada sobre tales documentos.

Existe un porcentaje de más de la mitad de los funcionarios, que no conocen sobre los documentos de procedimientos e instructivos del área donde laboran, lo que se traduce en una falencia en la administración de estos activos.

Pregunta:

¿Conoce si en la empresa existe un responsable o área encargada de la seguridad informática y seguridad de la información?

Objetivo:

Conocer si los funcionarios de la empresa son conscientes de la existencia del responsable encargado de la seguridad de la información o similar.

Tabla 18. Apreciación sobre la existencia del responsable de la seguridad informática e información

Detalle	Frecuencia	Porcentaje
Si	13	56,52
No	4	17,39
Desconoce	6	26,08

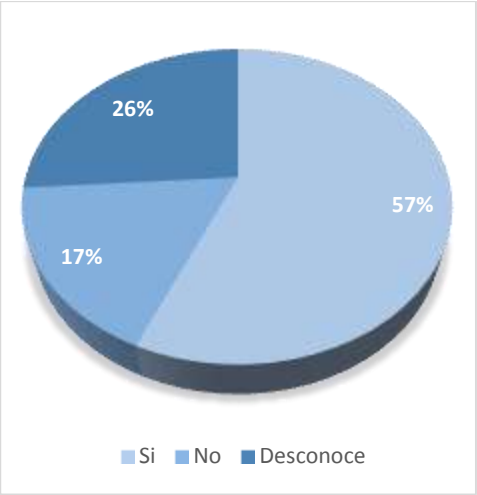

Figura 6. Respuestas obtenidas de los funcionarios sobre la existencia del responsable de la seguridad informática e información.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 56.52% de los funcionarios dice conocer que existe un encargado de la seguridad de la información mientras el 17.39% dice que no existe un encargado y el 26.08% de los funcionarios dice que desconoce de la existencia del responsable.

Con lo que se puede entender que existe una figura que cumple parcialmente con el rol de responsable de seguridad de la información pero no están formalmente establecidas sus funciones.

Pregunta:

¿Qué área considera que debe ser responsable de la seguridad de la informática y de la información? *(Varias alternativas)*

Objetivo:

Identificar que los funcionarios tengan nociones acerca de la seguridad de la información y la importancia de que exista un mecanismo de control

Tabla 19. Apreciación de la pertenencia de la responsabilidad de la seguridad de la información

Detalle	Frecuencia	Porcentaje
Sistemas	23	100
Administrativo	1	4,35
Todas las áreas	1	4,35
Otras	0	0

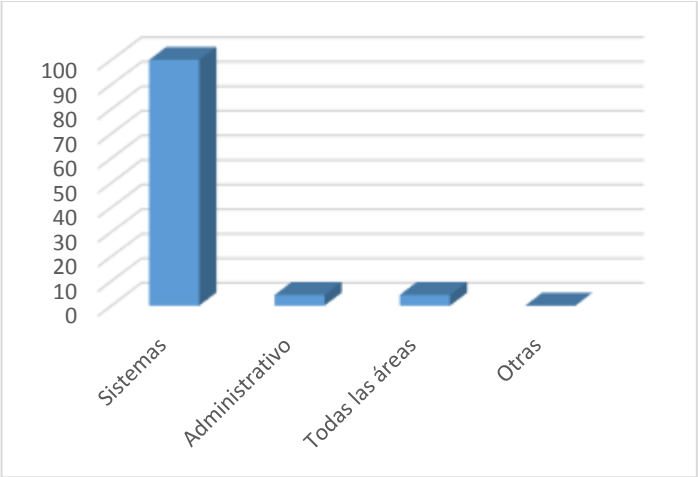

Figura 7. Respuestas obtenidas de los funcionarios respecto a quien consideran como responsable de la información
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

La totalidad de los funcionarios respondieron que el área de sistemas debería ser el responsable de la seguridad de la información, mientras un 4.35% señaló que administrativo también debería ser responsable de la seguridad de la información y otro 4.35% indicó además que todas las áreas deberían gestionar la seguridad de la información.

Lo que da a entender, que los funcionarios a ciencia cierta no conocen qué área de la empresa es responsable de mantener la seguridad de la información, pero conocen que sistemas realiza ciertas actividades referentes al tema.

Pregunta:

¿Cuántas capacitaciones han recibido acerca de temas seguridad de la información en el último año?

Objetivo:

Conocer si los funcionarios han mantenido capacitaciones sobre temas de seguridad que les permita realizar un buen uso de los activos de información.

Tabla 20. Capacitaciones recibidas por los funcionarios

Detalle	Frecuencia	Porcentaje
Más de 5	0	0
Menos de 5	2	8,7
Nunca ha recibido	21	91,3

Figura 8. Respuestas obtenidas de los funcionarios respecto a las capacitaciones recibidas referente a la seguridad de la información.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 91.30% de los funcionarios no han recibido capacitaciones y el 8.70% menciona haber recibido al menos una vez alguna capacitación acerca de la seguridad de la información.

Por lo que se puede apreciar, que en temas de capacitaciones sobre la seguridad de la información existe una grave falencia en lo que respecta a la concientización que da cabida al mal uso de activos de información.

Pregunta:

¿Las contraseñas que utiliza tiene combinación de números, letras y es de más de 10 caracteres?

Objetivo:

Conocer el estado de los sistemas de procesamiento de la información referente a las medidas mínimas de seguridad que estos deben poseer.

Tabla 21. Seguridad de contraseñas de los funcionarios

Detalle	Frecuencia	Porcentaje
Solo Números y más de 10 caracteres	1	4,35
Solo letras y más de 10 caracteres	1	4,35
Números y letras, más de 10 caracteres	3	13,04
Otras	18	78,26

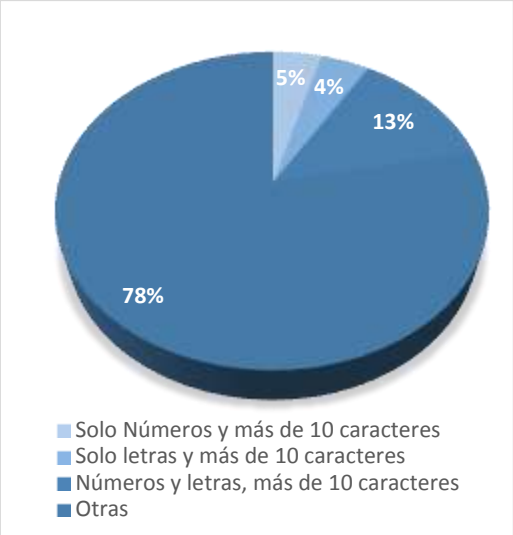

Figura 9. Respuestas obtenidas de los funcionarios respecto a las contraseñas utilizadas en los sistemas de procesamiento de la información.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 4.35% de los funcionarios opta por utilizar números o letras y más de 10 caracteres, mientras otro 13.04% opta por una combinación de letras y números y más de 10 caracteres.

El resto de los funcionarios utiliza una contraseña que pueda contener símbolos, números y letras con una longitud variable.

Esto demuestra que la gestión de autenticación de los usuarios en los sistemas de procesamiento de la información no es estricta ni homogénea según la apreciación en base a los datos recopilados de los funcionarios.

Pregunta:

¿Ha ocurrido algún incidente de seguridad en su puesto de trabajo en el último año? (bloqueo de la computadora, pérdida de documentos, daño de computadora, entre otros)

Objetivo:

Identificar los incidentes de seguridad han reportado los funcionarios

Tabla 22. Incidentes de seguridad acontecidos

Detalle	Frecuencia	Porcentaje
Si	11	47,82
No	11	47,83
Desconoce	1	4,35

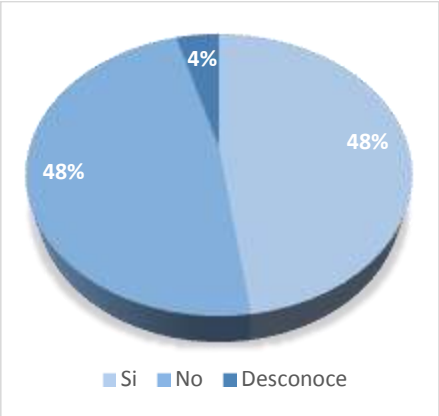

Figura 10. Respuestas obtenidas de los funcionarios respecto a los incidentes de seguridad acontecidos
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 47.82% de los funcionarios han experimentado un problema de seguridad, otro 47.83% en cambio no ha tenido ningún incidente, en tanto el 4.35% desconoce si ha tenido un incidente de seguridad.

Lo que da a entender que, por lo menos, la mitad de los funcionarios han estado expuestos a problemas de seguridad de cualquier nivel.

Pregunta:

¿Se le bloquea automáticamente su computadora cuando no la está utilizando?

Objetivo:

Conocer el mecanismo de seguridad instaladas en los equipos de trabajo de los funcionarios para evitar la fuga de la información

Tabla 23. Bloqueo automático de los computadores

Detalle	Frecuencia	Porcentaje
Si	1	4,35
No	22	95,65
Desconoce	0	0

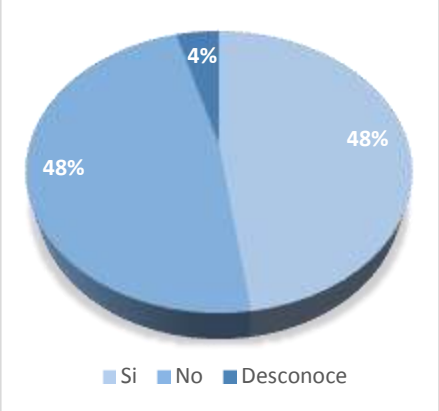

Figura 11. Respuestas obtenidas de los funcionarios respecto al bloqueo automático de los computadores
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 4.35% de los funcionarios asegura que su equipo cuenta con un mecanismos de seguridad, mientras el 95.65% menciona no poseer medida alguna.

Se puede identificar una grave falla de seguridad, dado que cualquier persona diferente del propietario del equipo de cómputo puede acceder a la información, incluso a la confidencial y actuar sobre la misma.

Pregunta:

¿Guarda en un lugar seguro (caja fuerte, gabinetes con llave) los documentos confidenciales cuando ya no los está utilizando?

Objetivo:

Conocer el buen resguardo y etiquetado de los activos de información

Tabla 24. Almacenaje y etiquetado de documentos

Detalle	Frecuencia	Porcentaje
Siempre	12	52,17
A veces	1	4,35
Casi nunca	1	4,35
Nunca	9	39,13

Figura 12. Respuestas obtenidas de los funcionarios respecto al almacenaje y etiquetado de documentos
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 52.17% de los funcionarios siempre almacena y resguarda los activos de información, mientras que el 4.35% de los funcionarios sólo cierta información considera almacenarla adecuadamente, mientras otro 4.35% de funcionarios rara vez almacena o etiqueta la información, el 39.13% nunca ha dado un buen resguardo de los activos de información.

Por lo que se puede apreciar, existe la posibilidad de fuga o hurto de información dado que los funcionarios no tienden a almacenar los activos de información adecuadamente.

Pregunta:

¿Cuándo tiene algún incidente de seguridad (falla de equipo, bloqueo de contraseña, pérdida de información) a quién lo notifica? (varias alternativas)

Objetivo:

Conocer de parte de los funcionarios, quién es el responsable de gestionar los incidentes de seguridad que se originan en la empresa.

Tabla 25. Notificaciones realizadas a quien los funcionarios consideran como responsable de la seguridad

Detalle	Frecuencia	Porcentaje
Gerente de Sistemas	14	60,87
Jefe del área	10	43,48
Altos directivos	0	0
No notifica	0	0
Otros	4	17,39

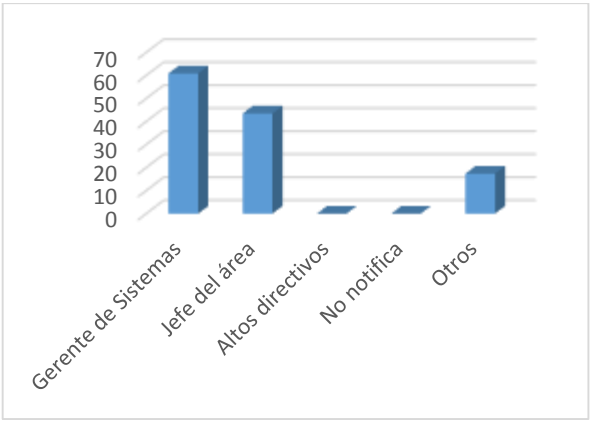

Figura 13. Notificaciones de los funcionarios de los incidentes ocurridos a quien consideran como responsable de la seguridad.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

Un 60.87% de los funcionarios notificaría al gerente de sistemas sobre los incidente de seguridad, mientras un 43.48% lo reportaría al jefe del área y otro 17.39% utilizaría otro método para dar a conocer el incidente.

Se puede entender que no existe un responsable determinado, al cual los funcionarios puedan acudir cuanto se suceda un incidente de forma que le pueda dar gestión oportuna.

Pregunta:

¿Cree que es necesario aplicar controles de seguridad para evitar robo o daño de información importante para la empresa?

Objetivo:

Reconocer el grado de disposición de los funcionarios acerca del buen uso e importancia que estos estos deben dar a los activos de información debido a la relevancia o valor que tienen para la empresa.

Tabla 26. Aprobación de los funcionarios respecto a implementar controles de seguridad

Detalle	Frecuencia	Porcentaje
Totalmente de acuerdo	22	95,65
De acuerdo	1	4,35
Ni de acuerdo ni en desacuerdo	0	0
Desacuerdo	0	0

Figura 14. Aprobación de aplicación de medidas de control de acuerdo a los funcionarios.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 95.65% de los funcionarios conocer la importancia de los activos de información para la empresa y la protección de los mismos, mientras tan solo el 4.35% considera que es relativamente importante.

El criterio de los funcionarios acerca de la protección de los activos de información de la empresa es correcta y reconoce la importancia de protegerlos.

Pregunta:

¿Qué documentos que maneja, considera usted que son catalogados como confidencial o de acceso restringido?

Objetivo:

Conocer si se tiene identificado los documentos de información sensible, y si se han definido los criterios para catalogarlos.

Tabla 27. Catalogación de documentos según los funcionarios

Detalle	Frecuencia	Porcentaje
Todos	9	39,13
Algunos	11	47,83
Ninguno	3	13,04

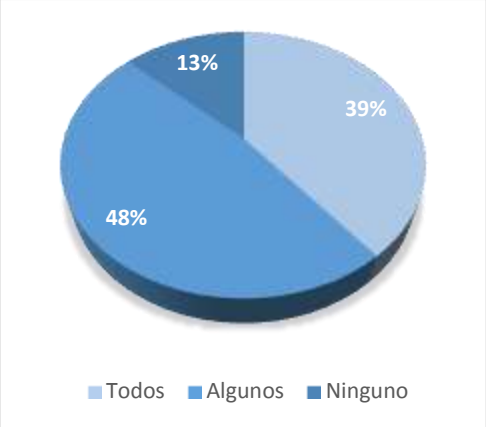

Figura 15. Consideración de los funcionarios acerca de los documentos que deben ser catalogados.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 39.13% de los funcionarios considera que todos los activos de información con los cuales labora son confidenciales, mientras el 47.83 cree que solo algunos son

confidenciales, y tan solo el 13.04 cree que ningún activo de información tiene mayor importancia.

Se puede identificar que los funcionarios han determinado la importancia de ciertos o todos los activos de información, de forma que los han considerado confidenciales debido a la relevancia de los datos, pero no se tienen identificado de forma uniforme los criterios por los cuales deben clasificar los documentos.

Pregunta:

¿Conoce si existe en la empresa áreas restringidas a las cuales solo puede acceder personal autorizado?

Objetivo:

Conocer la existencia de controles o mecanismos de accesos a las distintas áreas departamentales de la empresa

Tabla 28. Existencia de controles o mecanismos de accesos según los funcionarios

Detalle	Frecuencia	Porcentaje
Si	15	65,21
No	8	34,78
Desconoce	0	0

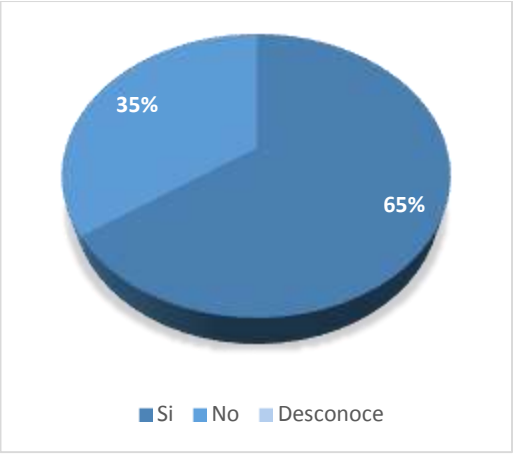

Figura 16. Consideración de los funcionarios sobre mecanismos de acceso instalados en la empresa.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 65.21% de los funcionarios dice que si existen medidas para el acceso físico a las distintas áreas de la empresa, mientras el 34.78% menciona que tales medidas no existen.

Por lo cual se puede inferir que puede que existan controles de seguridad pero estos son mínimos y nos son considerados por todos los funcionarios como medidas adecuadas de control de acceso.

- **Análisis e Interpretación de datos sobre la muestra recopilada específicamente en el área de sistemas.**

Pregunta:

¿Existe un área o persona responsable de seguridad informática y seguridad de la información en la empresa?

Objetivo:

Conocer si los funcionarios del área de sistemas de Credigestión son conscientes de la existencia del responsable encargado de la seguridad de la información o similar.

Tabla 29. Apreciación sobre la existencia del responsable de la seguridad informática e información.

Detalle	Frecuencia	Porcentaje
Si	3	100
No	0	0
Desconoce	0	0

Figura 17. Consideración de los funcionarios sobre mecanismos de acceso instalados en la empresa.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios del área de sistemas conoce que existe un responsable encargado de la seguridad de la información.

Se puede interpretar, que el área de sistemas conoce al responsable o es partícipe de cumplir las actividades de seguridad informática y seguridad de información de la empresa.

Pregunta:

¿Qué tipo de herramientas de seguridad tiene implementado en la empresa?
(Varias alternativas)

Objetivo:

Conocer las herramientas de seguridad sean éstas de software o hardware que actualmente se encuentran instaladas y/o gestionadas

Tabla 30. Uso de herramientas de seguridad de los sistemas de procesamiento de la información

Detalle	Frecuencia	Porcentaje
Software	3	100
Hardware	0	0
Otras	0	0
No posee	0	0

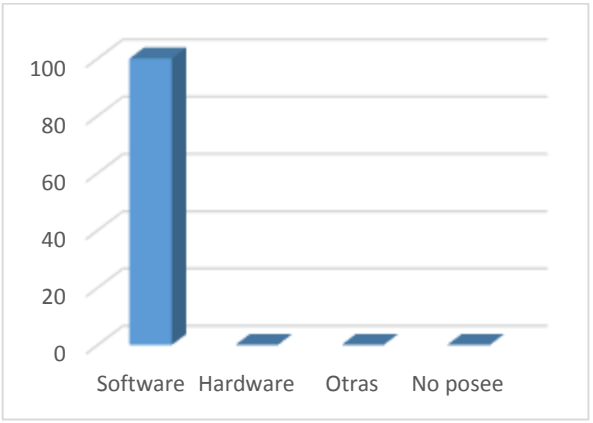

Figura 18. Tipos de herramienta instalados para el control de la seguridad de los sistemas de procesamiento de la información.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios dice conocer que todas las herramientas de seguridad, están basadas en software

El uso de herramientas de software es un buen método de protección, pues pueden ser actualizadas y configuradas según la necesidad.

Pregunta:

¿Tiene instalado antivirus en los equipos de computación?

Objetivo:

Conocer las herramientas de seguridad instaladas en los equipos de cómputo otorgados a los funcionarios de la empresa.

Tabla 31. Uso de herramientas de seguridad en los equipos de cómputo de los funcionarios

Detalle	Frecuencia	Porcentaje
Si	3	100
No	0	0

Figura 19. Herramientas instaladas en los equipos de cómputo de los funcionarios. (Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios del área de sistema conoce de las herramientas instaladas en los equipos de cómputo que se entrega a los funcionarios de la empresa.

En este sentido, es una buena práctica de seguridad dotar de estos mecanismos de a los equipos de cómputo destinados al usuario común ya que previenen de introducir amenazas de software a los medios de procesamiento de información de la empresa.

Pregunta:

¿Qué software utiliza en la empresa para controlar software malicioso?
(Varias alternativas)

Objetivo:

Conocer qué herramientas se poseen instaladas en la empresa sean estas de software o hardware, que ayuden a gestionar la seguridad en los equipos de procesamiento de la información

Tabla 32. Uso de Software de prevención de amenazas en los equipos de procesamiento de la información

Detalle	Frecuencia	Porcentaje
Antivirus	3	100
Anti-Spam	3	100
Antispyware	3	100
Cortafuegos/firewall	3	100
Otros	0	0

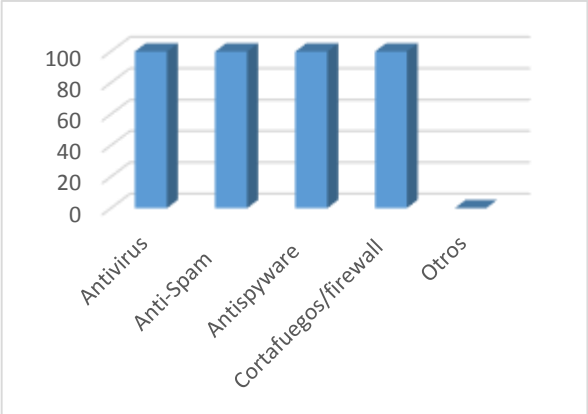

Figura 20. Herramientas de software instaladas en los equipos de procesamiento de la información.
(Elaborado por: Los Autores)

Análisis e interpretación

El 100% de los funcionarios dice que existen Antivirus, Anti spam, Antispyware y firewall instalados como medidas de protección a los equipos de procesamiento de la información.

La empresa cuenta al menos con los mecanismos básicos para detectar y detener cualquier acción de software malicioso.

Pregunta:

¿Cuáles de los siguientes mecanismos de autenticación utiliza en la empresa?
(Varias alternativas)

Objetivo:

Conocer los mecanismos con los que un funcionario puede identificarse ante los servicios de procesamiento de la información dispuestos en la empresa.

Tabla 33. Mecanismos de autenticación utilizados en la empresa

Detalle	Frecuencia	Porcentaje
Firma electrónica	0	0
Clave de Acceso	3	100
No tiene	0	0
Otros	0	0

Figura 21. Uso de mecanismos de autenticación utilizados en los sistemas de procesamiento de la información.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios del área de sistemas, indica que la clave de acceso es el único medio de autenticación.

Mantener varios mecanismos de autenticación para acceso a los servicios, se transforma en mayor seguridad siempre y cuando sean correctamente implementados, en el caso de la empresa puede que el mecanismo vigente cumpla con las necesidades actuales.

Pregunta:

¿Se realiza un mantenimiento periódico en los sistemas de procesamiento de información y equipos informáticos?

Objetivo:

Conocer la existencia de los procedimientos de prevención contra daños en los sistemas de procesamiento de la información los cuales aseguren una continua disponibilidad

Tabla 34. Existencia de mantenimientos periódicos en los sistemas de procesamiento de la información

Detalle	Frecuencia	Porcentaje
Si	3	100
No	0	0

Figura 22. Mantenimiento realizado en los sistemas de procesamiento de la información.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios indican que si existe un procedimiento periódico para el mantenimiento de los equipos.

Se da a conocer de las existencias de planes de mantenimiento, los cuales ayudan al control y buen funcionamiento de los equipos de cómputo asegurando la disponibilidad de los mismos y los servicios que estos proveen.

Pregunta:

¿Cada cuánto tiempo realizan mantenimientos en los sistemas de procesamiento de información? (varias alternativas)

Objetivo:

Conocer la frecuencia de los mantenimientos realizados en los equipos de cómputo, pues debido al uso permanente, puede que sea necesario adecuar los planes de acuerdo a la carga que soporta el hardware.

Tabla 35. Existencia de mantenimientos periódicos en los sistemas de procesamiento de la información

Detalle	Frecuencia	Porcentaje
Trimestral	0	0
Semestral	2	66,67
Mensual	0	0
Otros	2	66,67

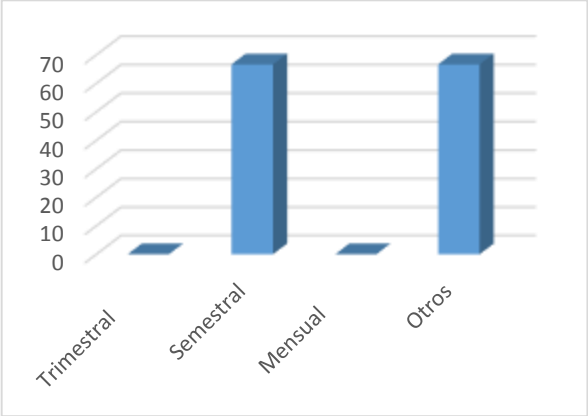

Figura 23. Planes de mantenimiento que se realizan sobre los equipos.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 66.67% de los funcionarios conoce que se realiza un plan de mantenimiento semestral y otro 66.67% indican que se realizan otros tipos de planes de mantenimiento.

Existe una incongruencia en la definición de los planes de mantenimiento o no se tiene documentado el procedimiento, por lo que puede resultar en un problema para la ejecución de la actividad.

Pregunta:

¿De cuántos computadores dispone su empresa?

Objetivo:

Identificar si el área de sistemas mantiene un inventario de los activos de información que se encuentran instalados o en bodegas de la empresa.

Tabla 36. Numero de computadores destinados a los funcionarios.

Detalle	Frecuencia	Porcentaje
20 – 40	0	0
40 - 60	0	0
60 o más	3	100

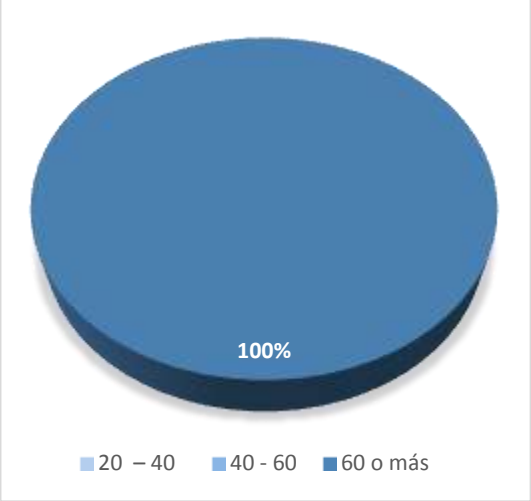

Figura 24. Planes de mantenimiento que se realizan sobre los equipos.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios mencionan que mantienen más de 60 computadores en la empresa.

Se interpreta, que realizan inventario de los activos de sistemas o poseen algún medio que les permita realizar tal actividad, esto, referente a equipos de cómputo dirigido a los funcionarios.

Pregunta:

¿Disponen de un espacio específico restringido para los servidores centrales de datos en la empresa?

Objetivo:

Identificar si el área de sistemas ha determinado un espacio determinado libre de amenazas físicas para los activos de procesamiento de la información.

Tabla 37. Áreas especiales determinadas para albergar los sistemas de procesamiento de la información.

Detalle	Frecuencia	Porcentaje
Si	3	100
No	0	0

Figura 25. Existencia de áreas restringidas donde se alojan los sistemas de procesamiento de la información. (Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios mencionan que si existe un área donde se mantienen estos activos en una zona restringida.

Se interpreta, que hay áreas especiales con acceso restringido donde solo personal autorizado por sistemas puede ingresar, y además estas instalaciones cuentan con la protección requeridas para evitar daños en los equipos centrales de procesamiento como servidores, ups, etc.

Pregunta:

Si su empresa tiene conexión WIFI, ¿existen restricciones de seguridad para el acceso de dichas conexiones?

Objetivo:

Conocer si se tienen definidos controles para el acceso a las redes inalámbricas de la empresa, las cuales suelen ser las más sensibles a ataques externos debido a su naturaleza.

Tabla 38. Existencia de controles sobre las redes de comunicación inalámbrica instaladas en la empresa

Detalle	Frecuencia	Porcentaje
Si	3	100
No	0	0

Figura 26. Restricciones de acceso en los sistemas de comunicación inalámbricos. (Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios mencionan que si existe un control sobre redes inalámbricas.

La gestión sobre redes que realiza la empresa es importante, pues les ayuda a controlar las amenazas que puedan afectar a través de este medio de comunicación.

Pregunta:

¿Se realizan respaldo de la información de la empresa?

Objetivo:

Conocer los procedimientos de respaldo de la información que se hayan establecido para salvaguardar los datos de la empresa.

Tabla 39. Procedimiento de respaldos de información definidos por el área de sistemas

Detalle	Frecuencia	Porcentaje
Si	3	100
No	0	0

Figura 27. Existencia de procedimientos de respaldo de la información.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios conoce acerca de los planes de respaldo.

Se interpreta que el área de sistemas realiza un control sobre los respaldos de la información que esta soportada por los medios de almacenamiento de información de la empresa.

Pregunta:

¿En caso de que se realice respaldo de información, con qué frecuencia lo realizan? (Varias alternativas)

Objetivo:

Conocer la efectividad de la completitud de los respaldos realizados en los distintos planes que se han determinado

Tabla 40. *Frecuencia de ejecución de los planes de respaldo de información*

Detalle	Frecuencia	Porcentaje
Diaria	3	100
Semanal	3	100
Mensual	3	100
Otros	0	0

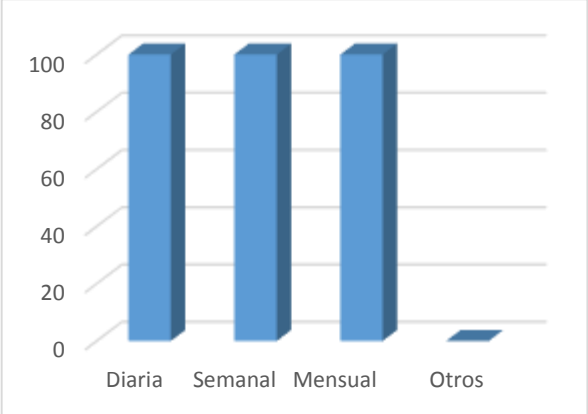

Figura 28. Ejecución de los planes de respaldo.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

Al 100% de los funcionarios conocen los periodos de respaldos establecidos.

En base a lo mencionado en las encuestas, se puede decir que el área de sistemas lleva un control adecuado del respaldo de la información que reposa en los servidores, y se puede interpretar además que tienen documentado el procedimiento según la importancia de los activos.

Pregunta:

¿Se utilizan mecanismos de bloqueo automático de las estaciones de trabajo para cuando se encuentran desatendidos?

Objetivo:

Conocer los mecanismos de seguridad que se tienen instalados en los equipos de los funcionarios y que es de conocimiento del área de sistemas.

Tabla 41. Mecanismos de seguridad automáticos instalados en los equipos de cómputo de los funcionarios

Detalle	Frecuencia	Porcentaje
Si	0	0
No	3	100

Figura 29. Existencia de mecanismos de seguridad en los equipos de cómputo de los funcionarios de la empresa.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios conoce no mantener un mecanismo automático de bloqueo

Se entiende que no existe ningún mecanismo, lo que da apertura a que puedan ocurrir fugas de información, ya que cualquier otro usuario podrá interactuar con el equipo en el periodo de tiempo en que el funcionario responsable se ausente.

Pregunta:

¿Existen equipos que provean de energía ininterrumpida a los servidores y computadores de los funcionarios?

Objetivo:

Conocer el plan de seguridad que permita operar a los sistemas de procesamiento de la información en caso de corte energético.

Tabla 42. *Disponibilidad de equipos que provean energía ininterrumpida*

Detalle	Frecuencia	Porcentaje
Si	2	66,67
No	1	33,33

Figura 30. Existencia del soporte energético en caso de corte de la electricidad.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 66.67% de los funcionarios del área de sistemas, conoce que existen equipos que permitan el funcionamiento continuo de los sistemas de procesamiento de la información.

Otro 33.33% no conoce de la existencia de equipos que provean energía ininterrumpida.

Se puede entender, que no existe documentación sobre los planes de contingencia o no existen planes de contingencia que todo el personal de sistemas debe conocer para poder actuar ante una eventualidad de corte energético, ya que los equipos de energía continua puede que sí estén instalados de acuerdo a las respuestas obtenidas.

Pregunta:

¿Qué servicios y sistemas considera más críticos en términos de disponibilidad? (Varias alternativas)

Objetivo:

Conocer si se ha considerado un plan de contingencia donde se haya identificado que activo de la información tiene mayor relevancia.

Tabla 43. Consideración de los funcionarios de sistemas sobre los servicios críticos

Detalle	Frecuencia	Porcentaje
De almacenamiento de datos	0	0
Servicios de comunicación	2	66,67
Sistemas de procesamiento de datos	2	66,67
Otros	1	33,33

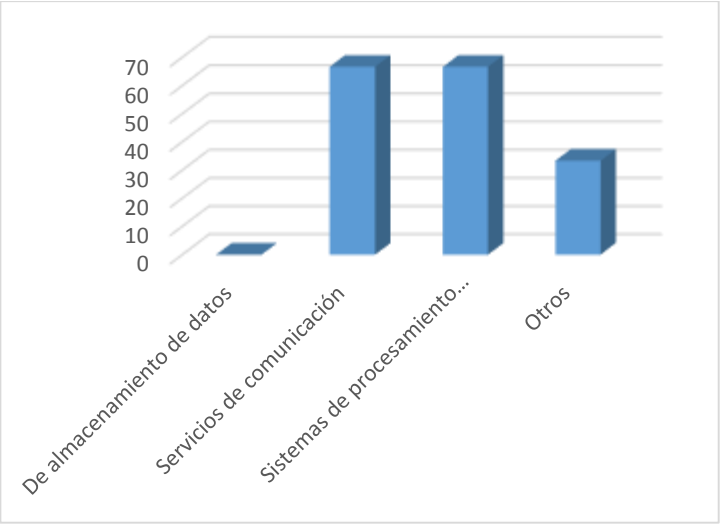

Figura 31. Consideración de la importancia de los activos controlados por el área de sistemas.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

Ningún funcionario considera importante el almacenamiento de datos, mientras que el 66.67% de los funcionarios considera que son importantes los sistemas de comunicación tanto como los de procesamiento de datos, y en otros, el 33.33% de los funcionarios mencionan que hay demás servicios que tiene importancia y se considera crítico para la empresa.

Se puede interpretar que el plan de contingencia no está establecido, por ende la importancia para el resguardo y protección de activos tampoco se ha determinado lo que puede conllevar una consecuencia grave en caso de ocurrir alguna calamidad.

Pregunta:

¿Dónde se encuentran almacenados los medios de respaldos?
(Varias alternativas)

Objetivo:

Identificar la efectividad de los respaldos al ser protegidos de cualquier amenaza que deteriore su integridad.

Tabla 44. Disposición de los respaldos de la información

Detalle	Frecuencia	Porcentaje
Dentro del área de sistemas	1	33,33
Dentro de la empresa, pero fuera del área de sistemas	0	0
Fuera de la empresa	3	100
No se realizan almacenamientos.	0	0
Otros	0	0

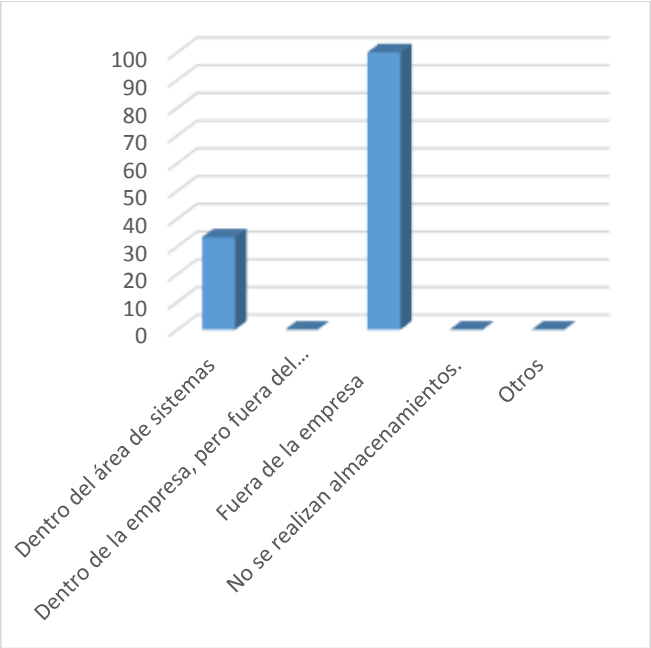

Figura 32. Lugares donde se disponen los respaldos de la información realizados por el área de sistemas.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 33.33% de los funcionarios del área de sistemas señala que se posee un tipo de respaldo dentro del área de sistemas mientras, que todos los funcionarios señala que los respaldos también se almacenan fuera de la empresa.

Se puede evidenciar que existen dos tipos de respaldos en la empresa, siendo uno de

estos almacenados fuera de la empresa, ya que pueden haber considerado evitar daños en los respaldos en caso de algún evento catastrófico.

Pregunta:

¿Durante el último año tuvieron algún incidente de seguridad grave de la información?

Objetivo:

Conocer si se registra la bitácora de los incidentes de seguridad que se han reportado al área de sistemas

Tabla 45. Incidentes de seguridad reportados y registrados

Detalle	Frecuencia	Porcentaje
Si	0	0
No	3	100
Desconoce	0	0

Figura 33. Registros de los incidentes de seguridad reportados al área de sistemas.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios del área de sistemas menciona no llevar un registro de los incidentes de seguridad reportados.

Se denota una falencia grave en la gestión de la seguridad, pues no se lleva un control o bitácora donde se registre la gestión de inicio a fin sobre el incidente para detectar los fallos de seguridad que lo produjeron y podría inducir a futuro.

Pregunta:

¿El acceso a internet en la empresa es limitado por?
(Varias alternativas)

Objetivo:

Conocer si se mantienen controles sobre el uso de los recursos en red

Tabla 46. Criterios de acceso hacia los recursos de red

Detalle	Frecuencia	Porcentaje
Cargo	0	0
Usuario	3	100
Indique el mecanismo	0	0
Ninguna	0	0

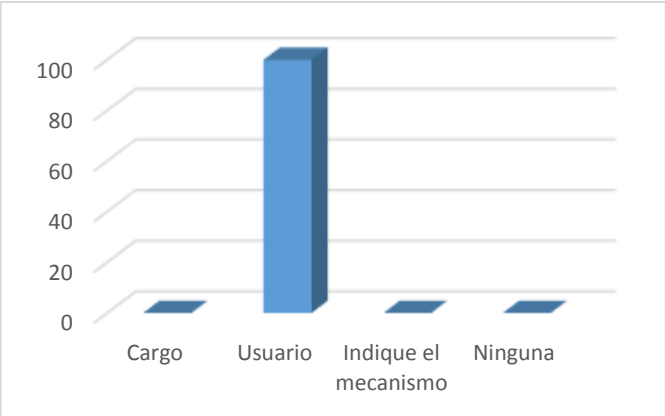

Figura 34. Registros de los incidentes de seguridad reportados al área de sistemas.

(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 100% de los funcionarios del área de sistemas confirma que existen reglas de uso que son configurados por usuarios para hacer uso de los servicios en red.

La segregación de los permisos por usuario permite un buen control sobre los recursos a los cuales pueden acceder, en este caso, se tiene bien implementado el control sobre los recursos de red.

Pregunta:

¿Se mantiene un registro de fallas cuando ocurre algún evento en los sistemas de procesamiento de información (servidores, computadores, redes, etc.)?

Objetivo:

Identificar si se realiza monitoreo a los sistemas de procesamiento de la información

Tabla 47. Monitoreo de los sistemas de procesamiento de la información

Detalle	Frecuencia	Porcentaje
Si	1	33,33
No	2	66,67

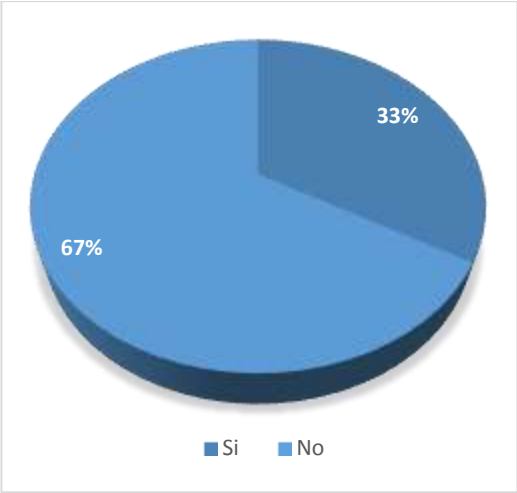

Figura 35. Monitoreo realizado a los sistemas de procesamiento.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 33.33% de los funcionarios mencionan que si se realiza un registro de fallas en los sistemas de procesamiento de la información, por otro lado, el 66.67% menciona no realizar ningún registro de control de fallos.

Se puede entender que no existe un procedimiento de control establecido, pero que de alguna forma si se está registrando las eventualidades en los sistemas de procesamiento de la información.

Pregunta:

¿Posee un plan de contingencia vigente en caso de desastres naturales?

Objetivo:

Conocer sobre el plan de contingencia que se tenga establecido ejecutar en caso de catástrofes.

Tabla 48. Planes de contingencia establecidos

Detalle	Frecuencia	Porcentaje
Si	2	66,67
No	1	33,33
Desconoce	0	0

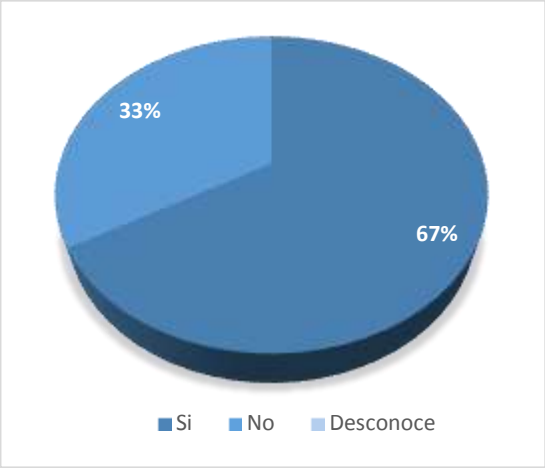

Figura 36. Conocimiento de los funcionarios de sistemas acerca de los planes de contingencia definidos.
(Elaborado por: Kelly Bermúdez, Rafael Bailón)

Análisis e interpretación

El 66.67% de los funcionarios afirma que existe un plan de contingencia en el área de sistemas, mientras otro 33.33% afirma que no existe plan alguno.

Se interpreta que existe algún plan o mecanismo de contingencia, pero el mismo no se encuentra debidamente documento por lo que los demás usuarios no tiene conocimiento del mismo.

4.3. Verificación de Hipótesis

La hipótesis establecida al inicio de la investigación, podrá ser verificada según los datos y evidencias recogidas en torno a las variables de investigación con soporte de las hipótesis específicas.

"*A través de controles de seguridad basados en la norma ISO/IEC 27001 se establecen mecanismos adecuados para mitigar riesgos que se puedan presentar en el uso de los sistemas de información y en el manejo de la información.*"

Conforme al análisis realizado el cual se basó en los dominios y controles de la norma ISO/IEC 27001, se comprobó que el establecer controles de seguridad permiten establecer, medir y mejorar mecanismos que ayudan a procurar el buen uso que los funcionarios deben darle a los sistemas de procesamiento de información así como al manejo adecuado de la información física.

- **Aplicar mecanismos de seguridad mejorará la gestión de la seguridad de la información.**

La empresa bajo estudio a pesar de poseer reglamentos y mecanismos que les permiten prevenir la ocurrencia de un incidente que afecten los activos de información, se encuentra en un alto índice de riesgos de seguridad debido a las vulnerabilidades presentes en las actividades a diario que realizan los funcionarios. El aplicar mecanismos y controles basados en las buenas prácticas de seguridad, les ayudará a encaminar la gestión de la seguridad de la información de una forma adecuada, permitiéndoles así disminuir el nivel de riesgo a los que está expuesta la información y los sistemas de procesamiento de información

- **Se podrá establecer el responsable del manejo, monitoreo y seguimiento de la gestión de seguridad de la información.**

Como una de las buenas prácticas principales de seguridad, se encuentra el establecer y designar al menos a una persona que se encargue de la gestión de la seguridad de la información dentro de la empresa, de tal forma que se analice y se planifique tiempos de implementación de controles de seguridad que mitigará los riesgos existentes.
Actualmente la falta de un responsable de seguridad informática y seguridad de la información no les permite realizar monitoreo constante de todo lo que implica temas de seguridad de la información, ni seguimiento a los incidentes ocurridos.

- **Se podrá incluir en la cultura organizacional charlas de temas relacionado a la seguridad de la información.**

Uno de los principales objetivos debe ser por empezar a mejorar la cultura organizacional en temas de seguridad, de acuerdo a encuestas realizadas a los funcionarios de la empresa se comprobó que la implementación de charlas referentes a temas de seguridad, les ayudará a mantener informados a los funcionarios sobre la importancia del buen uso de los activos de información, de tal forma que se dará cumplimiento a políticas tanto de la empresa como de los controles de seguridad actualmente implementados.

- **Se podrá establecer responsabilidades y obligaciones del manejo de la información de acuerdo a las actividades que realizan las áreas dentro de la empresa.**

Mediante la elaboración del manual de Políticas de Seguridad de la información se podrá detallar responsabilidades acorde a las actividades que realicen las diferentes áreas, de tal forma que se logre un trabajo integral en equipo, involucrando a todo el personal de la empresa, dado que en la actualidad según la información obtenida como resultado del estudio, no se tienen definidas responsabilidades con respecto a la seguridad de la información.

- **Permite mantener documentados y actualizados los procesos, procedimientos e instructivos de cada área.**

En base a los resultados obtenidos, se identificó que la mayoría de áreas no tienen definidos procedimientos e instructivos que les permita seguir a los funcionarios un mismo orden de actividades.

La norma ISO/IEC 27001 mediante el dominio Gestión de activos establece como buena práctica la documentación y actualización periódica de procedimientos, e instructivos necesarios para el cumplimiento de las actividades propias de las áreas, los cuales al estar detallados de forma ordenada y organizada, le permite el control al Gerente o Jefe de área de las actividades realizadas por los funcionarios así como

para poder tener evidencias para futuras auditoría externas que se realicen en la empresa.

- **A través de los controles de seguridad se puede monitorear posibles amenazas que afecten los sistemas tecnológicos de la empresa.**

Mediante la implementación de mecanismos de seguridad que permitan el monitoreo del funcionamiento y uso de los sistemas tecnológicos instalados en la empresa, se puede controlar la integridad de la información que estos almacenan o comunican a través de los medios y la disponibilidad de los activos de información ya que actualmente consideramos según los resultados que la gestión de seguridad realizada sobre estos activos no está siendo adecuadamente realizada.

- **Mediante controles de seguridad se puede mejorar el ámbito financiero, pues ayudará a prevenir incidentes de seguridad que puedan incurrir en altos costos para la empresa.**

Potenciar los controles de seguridad en los sistemas de procesamiento de la información, permite obtener de los sistemas datos claros y precisos , conforme a lo requiere la empresa y los clientes, minimizando incidentes de seguridad como daño de aplicaciones, equipos tecnológicos hasta incluso robo o alteración de información, lo que puede costarle mucho dinero a la empresa; en base al análisis realizado se ha podido detectar que la ocurrencia de sucesos esporádicos han afectado la integridad de la información almacenada en los repositorios de datos, ocasionando cierto retraso en la consulta de la información requerida.

- **Permite mejorar el aspecto comercial generando credibilidad y confianza entre sus clientes.**

En los últimos años la empresa ha tenido un crecimiento considerable, por lo que aplicar la norma ISO/IEC 27001, permite mejorar significativamente las operaciones en la empresa, organizando los esfuerzos realizados en el cumplimiento de objetivos.
El conjunto de todos los controles de seguridad, permite a los altos directivos garantizar una correcta y adecuada confidencialidad integridad y disponibilidad de

datos e información que es valiosa tanto para la empresa como para sus clientes, aumentando la credibilidad y la confianza de los clientes externos de la empresa.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

En conclusión, el análisis realizado demuestra que los activos de información de las áreas consideradas críticas y la situación actual de la empresa con respecto a la seguridad de la información, refleja potenciales índices de riesgos, los cuales exponen a la información a daños, robo o modificaciones que pueden causar un impacto negativo dentro de las actividades del negocio.

Mediante las recomendaciones indicadas, se pretende que la empresa tome acciones que le permitan prevenir y detectar oportunamente vulnerabilidades a las que están expuestos los sistemas de procesamiento de información, así como la información que es manejada y generada por los funcionarios. La implementación de controles de seguridad basados en la norma ISO/IEC 27001, les permite mejorar tres características importantes como son: la confidencialidad, integridad y disponibilidad de la información.

El elaborar un manual de políticas de seguridad de la información donde se detallen controles de seguridad acorde a la realidad y necesidades actuales de la empresa, la constante concienciación a los funcionarios, así como el monitoreo continuo, encamina a la empresa a la correcta gestión de la seguridad de la información.

La seguridad total no existe, pero gestionar controles de seguridad en el proceso y manejo de la información, se vuelve un complemento esencial, pues le permite asegurar información valiosa no sólo de la empresa sino también de los clientes.

5.2. Recomendaciones

Para empezar a tratar los temas de seguridad de la información y seguridad informática, es importante que se esté consciente de que el trabajo de implementación y cumplimiento de controles de seguridad es en equipo, e involucra a todos los funcionarios de la empresa.

La concientización en los funcionarios y el compromiso de los altos directivos, permite que todos empiecen a conocer la importancia que tiene garantizar que la información de la empresa está siendo manejada y procesada adecuadamente.

La implementación de la gestión de seguridad de la información dentro de la empresa, es un proceso que nunca termina, pues el éxito se enfoca en la revisión, monitoreo y seguimiento continuo de todos los controles que se tienen implementados.

Es importante analizar y planificar la implementación de cada control de seguridad, pues jamás se debe priorizar un control que solo cause inestabilidad en la seguridad de los sistemas de procesamiento de información, pues precisamente lo que se busca es garantizar la disponibilidad, confidencialidad e integridad de estos y no lo contrario; además se debe tomar en cuenta que no todas las empresas tienen la misma infraestructura tecnológica ni las mismas necesidades.

Tomando en consideración lo antes indicado se debe considerar la "Matriz de recomendaciones basadas en la situación actual" la cual indica situación actual de la empresa en temas de seguridad; además detalla los controles que permiten mitigar aquellas vulnerabilidades, y la "Matriz de Amenazas, vulnerabilidades, salvaguardas, impacto y riesgo residual" que se basa en los activos de información de las áreas críticas de la empresa, para poder poner en práctica las recomendaciones dadas.

Para una mejor gestión se debe considerar la elaboración de un "Plan estratégico" basado en la seguridad de la información, el cual debe establecer pequeños proyectos para así llevar acabo la implementación de cada uno de los controles de seguridad basados en la ISO/IEC 27001 de una forma ordenada y acorde a las necesidades prioritarias de la empresa y dejando para una segunda fase los controles detallados como secundarios.

CAPÍTULO VI
PROPUESTA

6.1. Datos Informativos de la empresa

Credigestión es una empresa financiera que ofrece un servicio de Gestión Integral de Cartera, de tal forma que facilita el proceso integral de créditos para que los clientes realicen ventas seguras y rentables a plazos. (Credigestión, 2013)

Cuentan con 230 empleados entre Guayaquil y Quito.

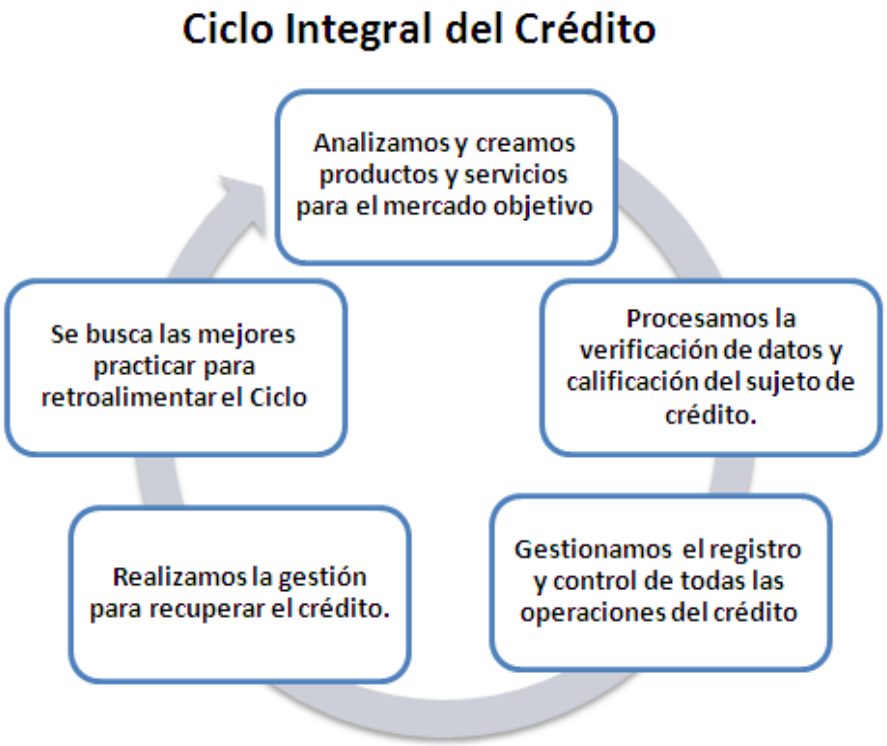

Figura 37. Ciclo Integral de Crédito
(Credigestión, 2013)

Misión

Satisfacer las necesidades de empresas comerciales, financieras y de servicios, que buscan un servicio externalizado, para el manejo integral de sus procesos de crédito y cobranzas. Así nuestros clientes podrán enfocarse en su negocio base y obtener

mejores índices de recuperación en su cartera y por lo tanto mejores resultados. Esto se logra con la ayuda de un sistema tecnológico integrado, nuestra experiencia en el mercado y la importancia que le damos a nuestros valores (Credigestión, 2013).

Visión

"En el año 2012 Credigestión será reconocida en Ecuador como la mejor empresa de gestión integral de crédito al consumidor y traspasaremos las fronteras de nuestro país. Lograremos el liderazgo gracias a nuestro excelente sistema integrado, el compromiso con nuestros clientes y a la continua auto-motivación que fomentamos en nuestros colaboradores." (Credigestión, 2013)

Valores

- Formalidad y profesionalismo en nuestra gestión.
- Honestidad y confidencialidad en el manejo de datos e información.
- Incentivar continuamente la auto-motivación de nuestros colaboradores.
- Buscar la retroalimentación constante, y reforzar continuamente nuestro sistema con los nuevos conocimientos que nuestra organización obtiene. (Credigestión, 2013)

6.2. Antecedentes de la propuesta

Debido al constante crecimiento de Credigestión y a la ocurrencia de ciertos incidentes de seguridad, nace la necesidad de precautelar la correcta gestión de sus operaciones y activos de información, de tal forma que se puedan adaptar buenas prácticas de seguridad con la finalidad de otorgar un servicio confiable y oportuno; dado al tipo de información que la empresa utiliza de sus clientes.

La norma ISO/IEC 27001 es el medio por el cual la empresa puede iniciar a aplicar controles de seguridad y buenas prácticas, ya que en esta se consideran objetivos de control y ciclos que deben de cumplirse para prevenir o menguar la afectación que puedan ocasionar eventos fortuitos que entorpezcan o detengan las operaciones de la

empresa; persiguiendo siempre la mejora continua de los objetivos de control, sea que ya estén implantados o requieran serlo.

En caso de que la empresa no adapte sus operaciones y no establezca mecanismos de control, puede darse la ocurrencia de algún suceso que afecte las operaciones, debido a la falta de confidencialidad, integridad o disponibilidad que puede ocurrir sobre los activos de información o las operaciones que se realizan sobre estos activos.

6.3. Justificación de la propuesta

Actualmente el aumento de los delitos informáticos en el país permiten tener una percepción de las amenazas a los que están propensos los sistemas de procesamiento de información y con ello los datos se ven expuestos a daños irreparables que pueden causar un gran impacto en el negocio.

Credigestión al igual que las demás empresas manejan a diario información importante que le genera valor al negocio, la cual tiene diferente nivel de importancia para cada área, pues lo que puede ser importante o confidencial para un área para otra puede no ser tan relevante, por esa razón antes de empezar a implementar controles de seguridad se debe analizar y considerar la situación actual en cuanto a la seguridad de la información, de tal forma que se puedan mitigar vulnerabilidades y amenazas a las cuales está expuesta la empresa.

De acuerdo a los resultados obtenidos en el análisis de seguridad de la información y seguridad informática realizado, se demuestra que los activos de información de Credigestión se encuentran expuestos a riesgos que podrían ocasionar pérdida de información. La situación actual refleja que la falta de monitoreo, seguimiento e implementación de controles expone a la información a la ocurrencia de incidentes de seguridad.

6.4. Objetivos de la propuesta

6.4.1. Objetivo General

Aportar en la disminución del riesgo existente, mediante controles de seguridad que permitan mitigar y detectar peligros potenciales a los que están expuestos los sistemas de procesamiento de información, datos y documentación física confidencial.

6.4.2. Objetivos Específicos

- Elaborar un manual de Políticas de Seguridad de la Información alineadas a las necesidades de la empresa.
- Elaborar y documentar procedimientos de seguridad
- Reforzar los controles de seguridad implementados en la empresa
- Incorporar nuevos controles de seguridad que prevengan la ocurrencia de nuevas vulnerabilidades.
- Monitorear el cumplimiento de controles de seguridad

6.5. Análisis de factibilidad

Con la finalidad de obtener los resultados previstos, es necesario considerar las siguientes dimensiones para la implementación de la gestión de la seguridad de la información.

6.5.1. Capacidad Económica

En base al apoyo que el gerente de la empresa está dispuesto a brindar para la ejecución del plan para la gestión de seguridad de la información, se cuenta con los recursos económicos necesarios, en la adquisición de equipos o contratación de personal, por lo cual se considera que por la parte económica es factible que el plan se desarrolle sin ningún problema.

6.5.2. Capacidad Operativa

Los directivos de la empresa están dispuestos a contratar el personal capacitado para la gestión de la seguridad de la información y la creación del área responsable de la empresa, en conjunto a la necesidad de la instalación de equipamiento informático

que sirva de apoyo para el monitoreo de los sistemas de procesamiento de la información, por lo cual se considera que la capacidad operativa no es impedimento para que a corto plazo se pueda iniciar la ejecución del plan de gestión para la seguridad de la información.

6.5.3. Capacidad Técnica

Actualmente la empresa no cuenta con personal especializado, pero se prevé que se realice la contratación inmediata para la ejecución del plan de gestión para la seguridad de la información, aun así es un factor importante, y puede provocar que no se pueda ejecutar el plan en la empresa lo que disminuye la factibilidad de realización.

6.5.4. Disposición del Personal

El personal de la empresa tiene buena disposición en la aceptación de las medidas de control para la seguridad de la información, pues consideran que es de importancia precautelar que los activos de la empresa sean manipulados adecuadamente, por lo cual, es muy factible aplicar en plan en la empresa debido a la aceptación positiva de los funcionarios respecto al cuidado de los activos de información.

6.6. Fundamentación

Las empresas se sustentan en la información que procesan y manejan a diario, pues es aquella información la que les permite la toma decisiones. Hoy en día la información aún se sigue presentando de varias formas, ya sea en proyectos, reportes, registros e incluso en el conocimiento que posee una persona y no solo en los sistemas de procesamiento de información, lo que la hace valiosa pero también vulnerable a incidentes de seguridad.

La implementación de controles de seguridad dentro de una empresa, permite minimizar aquellas brechas de seguridad que dan paso a la corrupción de la información, actualmente varias instituciones del país han podido comprobar que gestionar la seguridad de la información en sus empresas les ha permitido cumplir

con organismos los organismos de control que las regulan, un orden dentro de las actividades que se realizan en el negocio, reducción de incidentes de seguridad, entre otros aspectos.

El análisis realizado, ayudó a comprobar que la incorporación de controles de seguridad basada en este caso en la norma ISO/IEC 27001 ayudará a reducir y mitigar riesgo existente así como reducir la posibilidad de ocurrencia de nuevos riesgos.

Todos los controles de seguridad que se han recomendado empezar a gestionar se fundamentan en la norma ISO/IEC 27001, por ser una norma que ayuda a la gestión de la seguridad de la información, delineando cada paso a seguir para la implementación de un Sistema de Gestión de Seguridad de la Información que permite planear, implementar, monitorear y mejorar continuamente los procedimientos, métodos y proyectos.

6.7. Metodología

La metodología a continuación propuesta está alineada a la norma ISO/IEC 27001 y corresponde al análisis de seguridad de la información y seguridad informática realizado, el cual empezó con la identificación de las vulnerabilidades de la situación actual, así como la evaluación de amenazas, vulnerabilidades, impacto y riesgos de los activos de información de las áreas que son consideradas críticas en Credigestión.

Para mitigar las vulnerabilidades encontradas se debe definir y priorizar actividades que conlleven a la aplicación del plan de gestión de la seguridad de la información mediante la implementación de controles de seguridad. Para esto se ha considerado las siguientes fases, en las cuales se detallan un conjunto de actividades a ser realizadas por la empresa.

Primera Fase: Definición

Esta primera fase comprende el inicio del plan de gestión de la seguridad de la información, donde se establecen responsabilidades, estándares y procedimientos sobre la dirección del plan de gestión de seguridad.

- Designar formalmente al Responsable de Seguridad de la información y/o Seguridad Informática.

- Definir y establecer las responsabilidades y objetivos del Responsable de Seguridad de la información y/o Seguridad Informática.

- Conformar el Comité de Gestión de la Seguridad de la Información.

- Analizar cada una de las recomendaciones dadas, de tal forma que se dé prioridad de implementación a los controles de seguridad que puedan disminuir el riesgo de mayor impacto.

- Diseñar el manual de políticas de seguridad de la información en base a los controles implementados actualmente y considerando nuevos controles que podrán ser implementados dentro de la empresa.

- Establecer los procedimientos e instructivos de seguridad.

- Designar formalmente a los Propietarios de los activos de información.

- Elaborar un catálogo de Clasificación de la información por área, el cual debe ponerse en conocimiento de todos los funcionarios (categorización: confidencial o pública).
- Evaluar con personal especializado todo lo referente a requerimientos legales, tomando en cuenta organismos de control que regulan a la empresa, leyes ecuatorianas, entre otros.

Segunda Fase: Aplicación

Esta fase comprende la aplicación de los controles de seguridad anteriormente definidos, se realizan las actividades que han sido diseñadas con el propósito de disminuir el riesgo actual.

- Crear e implementar un programa de capacitación para los funcionarios de la empresa acerca de temas relacionados con la seguridad informática (charlas, boletines, seminarios, entre otros).

- Implementar los controles de seguridad recomendados en la matriz de situación actual y activos de la información, tomando en cuenta la protección física y lógica de la información y de los sistemas de procesamiento de información.

- Definir y establecer políticas y responsabilidades sobre la administración de accesos de los sistemas de información.

- Estandarizar los user ID, de tal forma que los funcionarios utilicen un solo usuario para el ingreso a los diferentes aplicativos de la empresa.

- Definir y establecer políticas que detallen el buen uso que se le debe dar a los activos de la empresa.

- Definir procesos que permitan conocer las responsabilidades y obligaciones de funcionarios, pasantes, practicantes y terceros en cuanto a la seguridad de la información.

- Gestionar el buen uso de las redes y comunicaciones, generando procedimientos e instructivos.

- Definir el proceso para gestionar los cambios que se necesiten realizar en los aplicativos de la empresa.

- Incorporar la seguridad de la información en la Gestión de la continuidad del negocio.

- Administrar y registrar los incidentes de seguridad de la información que se presente.

- Analizar la posibilidad de implementación de sistemas de video vigilancia, detectores de humo, sistemas contra incendios.

- Registrar pistas de auditorías en los sistemas de información de la empresa.

- Definir un backup para cada funcionario que desempeñe un rol crítico dentro de las actividades del área de sistemas.

Tercera Fase: Monitoreo

- Monitorear la gestión de seguridad de la información, comprobar su eficacia con la finalidad de poder realizar ajustes al plan de seguridad.

- Monitoreo continuo de los controles de seguridad implementados para prevenir incidentes de seguridad.

- Analizar la posibilidad de adquirir herramientas para monitorear las aplicaciones, redes, código maliciosos, entre otros.

- Diseñar y ejecutar los indicadores de gestión de seguridad.

- Monitorear el cumplimiento de la gestión del buen uso de los activos.

- Monitorear el acceso y buen uso de redes y comunicación.

- Monitorear el correcto funcionamiento de servicios prestados por terceros.

- Monitorear el cumplimiento de estándares de seguridad del Data-Center.

- Registrar el resultado de los monitoreos realizados.

Cuarta Fase: Mejora

Mejorar la gestión de seguridad de la información considerando las vulnerabilidades encontradas luego de monitorear el plan vigente.

- Identificar e incorporar mejoras a la gestión de la seguridad de la información.

- Actualizar el manual de políticas de seguridad de la información cuando ocurran cambios significativos.

- Comprobar la eficacia de las mejoras incorporadas.

- Comunicar las mejoras realizadas a las máximas autoridades.

- Capacitar al personal que maneja la seguridad de la información así como al personal técnico del área de Sistemas (administradores, desarrolladores, entre otros).

6.8. Administración

6.8.1. Recurso Humano

A continuación se detalla el personal principal para gestionar la Seguridad de la información

- Personal especializado en seguridad de la información (asesores o consultores).

- Responsable de Seguridad de la Información.

- Gerente de Sistemas.

- Directivos de cada una de las áreas involucradas en la implementación de controles de seguridad.

Así mismo se debe involucrar a todo el personal de la empresa, dando a conocer los temas de seguridad de la información, su importancia y beneficios mediante concientizaciones periódicas.

6.8.2. Cronograma

Se presenta el cronograma como guía de aplicación de la gestión de la seguridad de la información que cumple con el propósito de mejora continua, en la cual existen periodos de autoevaluación y reformas consiguiendo disminuir la ocurrencia de incidentes de seguridad respecto a los activos de información de la empresa.

Tabla 49. Cronograma de Actividades del plan de Seguridad de la información

Actividad Macro	Responsable	Tiempo Est. (d)
Designar formalmente al Responsable de Seguridad de la información y/o Seguridad Informática. Definir y establecer las responsabilidades y objetivos del Responsable de Seguridad de la información y/o Seguridad Informática.	Presidente Ejecutivo	8
Conformar el Comité de Gestión de la Seguridad de la Información.	Responsable de la seguridad de la información y/o seguridad informática	7
Analizar cada una de las recomendaciones dadas, de tal forma que se dé prioridad de implementación a los controles de seguridad que puedan	Comité de la gestión de la seguridad de la información	7

disminuir el riesgo de mayor impacto.		
Diseñar el manual de políticas de seguridad de la información en base a los controles implementados actualmente y considerando nuevos controles que podrán ser implementados dentro de la empresa. Establecer los procedimientos e instructivos de seguridad.	Responsable de la seguridad de la información y/o seguridad informática	60 (Actividad periódica)
Designar formalmente a los Propietarios de los activos de información	Comité de la gestión de la seguridad de la información Presidente Ejecutivo	7
Elaborar un catálogo de Clasificación de la información por área, el cual debe ponerse en conocimiento de todos los funcionarios (categorización: confidencial o pública)	Responsable de la seguridad de la información y/o seguridad informática Propietarios de la información	15
Evaluar con personal especializado todo lo referente a requerimientos legales, tomando en cuenta organismos de control que regulan a la empresa, leyes ecuatorianas, entre otros	Responsable de la seguridad de la información y/o seguridad informática Área Legal	15
Crear e implementar un programa de capacitación para los funcionarios de la empresa acerca de temas relacionados con la seguridad informática (charlas, boletines, seminarios,	Responsable de la seguridad de la información y/o seguridad informática	15

entre otros)		
Implementar los controles de seguridad recomendados en la matriz de situación actual y activos de la información, tomando en cuenta la protección física y lógica de la información y de los sistemas de procesamiento de información.	Responsable de la seguridad de la información y/o seguridad informática Todas las áreas involucradas	90
Definir y establecer políticas y responsabilidades sobre la administración de accesos de los sistemas de información.	Responsable de la seguridad de la información y/o seguridad informática Área de sistemas	15
Estandarizar los user ID, de tal forma que los funcionarios utilicen un solo usuario para el ingreso a los diferentes aplicativos de la empresa.	Responsable de la seguridad de la información y/o seguridad informática Área de sistemas	30
Definir y establecer políticas que detallen el buen uso que se le debe dar a los activos de la empresa.	Responsable de la seguridad de la información y/o seguridad informática	15
Definir procesos que permitan conocer las responsabilidades y obligaciones de funcionarios, pasantes, practicantes y terceros en cuanto a la seguridad de la información	Responsable de la seguridad de la información y/o seguridad informática Recursos Humanos	15
Gestionar el buen uso de las redes y comunicaciones, generando procedimientos e instructivos.	Responsable de la seguridad de la información y/o seguridad informática Área de sistemas	15
Definir el proceso para gestionar los cambios que se	Responsable de la seguridad de la información y/o seguridad informática	15

necesiten realizar en los aplicativos de la empresa.	Área de sistemas	
Incorporar la seguridad de la información en la Gestión de la continuidad del negocio.	Responsable de la seguridad de la información y/o seguridad informática Comité de la gestión de la seguridad de la información	60
Administrar y registrar los incidentes de seguridad de la información que se presente	Responsable de la seguridad de la información y/o seguridad informática	7 (Actividad periódica)
Analizar la posibilidad de implementación de sistemas de video vigilancia, detectores de humo, sistemas contra incendios.	Responsable de la seguridad de la información y/o seguridad informática Área de Administrativo	60
Registrar pistas de auditorías en los sistemas de información de la empresa.	Responsable de la seguridad de la información y/o seguridad informática. Área de sistemas	10
Definir un backup para cada funcionario que desempeñe un rol crítico dentro de las actividades del área de sistemas.	Responsable de la seguridad de la información y/o seguridad informática	10
Monitoreo continuo de los controles de seguridad implementados para prevenir incidentes de seguridad.	Responsable de la seguridad de la información y/o seguridad informática	15 (Actividad periódica)
Analizar la posibilidad de adquirir herramientas para monitorear las aplicaciones, redes, código maliciosos, entre otros.	Responsable de la seguridad de la información y/o seguridad informática	15
Diseñar y ejecutar los indicadores de gestión de seguridad.	Responsable de la seguridad de la información y/o seguridad informática	20

Monitorear el cumplimiento de la gestión del buen uso de los activos	Responsable de la seguridad de la información y/o seguridad informática.	15 (Actividad periódica)
Monitorear el acceso y buen uso de redes y comunicación	Responsable de la seguridad de la información y/o seguridad informática. Área de sistemas	10 (Actividad periódica)
Monitorear el correcto funcionamiento de servicios prestados por terceros.	Responsable de la seguridad de la información y/o seguridad informática.	15 (Actividad periódica)
Monitorear el cumplimiento de estándares de seguridad del Data-Center.	Responsable de la seguridad de la información y/o seguridad informática. Área de sistemas	15
Registrar el resultado de los monitoreos realizados	Responsable de la seguridad de la información y/o seguridad informática	Actividad periódica
Identificar e incorporar mejoras a la gestión de la seguridad de la información	Responsable de la seguridad de la información y/o seguridad informática	30 (Actividad periódica)
Actualizar el manual de políticas de seguridad de la información cuando ocurran cambios significativos	Responsable de la seguridad de la información y/o seguridad informática	Actividad periódica
Comprobar la eficacia de las mejoras incorporadas	Responsable de la seguridad de la información y/o seguridad informática	10
Comunicar las mejoras realizadas a las máximas autoridades	Responsable de la seguridad de la información y/o seguridad informática	Actividad periódica
Capacitar al personal que maneja la seguridad de la información así como al personal técnico del área de Sistemas (administradores, desarrolladores, entre otros)	Responsable de la seguridad de la información y/o seguridad informática	10

REFERENCIAS

Credigestión. (2013). *Misión, Visión y Valores organizacionales*. Noviembre 10, 2014, Recuperado de: http://www.credigestion.biz/

Credigestión. (2013). *Nuestra Operación*. Noviembre 10, 2014, Recuperado de: http://www.credigestion.biz/index.php?option=com_content&view=article&id=84&Itemid=88

Credigestión. (2013). *El Equipo Credigestión*. Noviembre 10, 2014, Recuperado de: http://www.credigestion.biz/index.php?option=com_content&view=article&id=86&Itemid=84

ISO/IEC. (2005). *Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos*. Octubre 10, 2014, de ISO/IEC, Recuperado de: http://www.cva.itesm.mx/biblioteca/pagina_con_formato_version_oct/apaweb.html

ISOTools Excellence. (2014). ISO *27001*. Octubre 10, 2014, de ISOTools Excellence Recuperado de: http://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISOTools Excellence. (2014). *La Norma ISO 27001 y la importancia de la gestión de la seguridad de la información*. Octubre 10, 2014, de ISOTools Excellence, Recuperado de: http://www.isotools.org/pdfs/Monografico-ISO-27001-ISOTools.pdf

Kosutic, D. (2014). *La lógica básica de la norma ISO 27001*. Noviembre 12, 2014, de 27001 Academy, Recuperado de:

http://www.iso27001standard.com/blog/2014/05/05/the-basic-logic-of-iso-27001-how-does-information-security-work/#

Kosutic, D. (2014). *Qué es norma ISO 27001*. Noviembre 15, 2014, de 27001 Academy Sitio web: http://www.iso27001standard.com/es/que-es-iso-27001/

Kosutic, D. (2014). Porque ISO 27001 es importante para su empresa. Noviembre 22, 2014, de 27001 Academy, Recuperado de: http://www.iso27001standard.com/es/que-es-iso-27001/

Kosutic, D. (2014). Cómo es realmente ISO 27001. Diciembre 8, 2014, de 27001 Academy, Recuperado de: http://www.iso27001standard.com/es/que-es-iso-27001/

Dirección General de Modernización Administrativa y Procedimientos e Impulso de la Administración Electrónica. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. España, Noviembre 15, 2014, Recuperado de: https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_metodo.pdf

Xerox. (2012). SO 27001 Certificaciones Seguridad Comprometidos con el más alto nivel de seguridad de la información. Diciembre 18, 2014, de Xerox ISO 27001 security certifications, Recuperado de: https://www.xerox.com/download/security/white-paper/27b1e0-4b3fde3a23980/ISO-27001-Security-Certification.pdf

ANEXO 1

Encuesta acerca de Seguridad Informática dirigida al área de Sistemas

Nota: Marcar con una **X** sus respuestas

1. **¿Existe un área o persona responsable de seguridad informática y seguridad de la información en la empresa?**

   Sí ○ No ○

2. **¿Qué tipo de herramientas de seguridad tiene implementado en la empresa? (se puede seleccionar varias alternativas)**

   Software ☐
   Hardware ☐
   No tiene ☐
   Otros, indique cuáles ☐ _____

3. **¿Tiene instalado antivirus en los equipos de computación?**

   Sí ○ No (continuar con la pregunta 5) ○

4. **¿Qué software utiliza en la empresa para controlar software malicioso? (se puede seleccionar varias alternativas)**

   Antivirus ☐
   Anti-Spam ☐
   Antispyware ☐
   Cortafuegos/firewall ☐
   Otros, indique cuáles ☐ _____

5. **¿Cuáles de los siguientes mecanismos de autenticación utiliza en la empresa? (se puede seleccionar varias alternativas)**

   Firma electrónica digital ☐
   Clave de Acceso ☐
   No tiene ☐
   Otros, indique cuáles ☐ _____

6. ¿Se realiza un mantenimiento periódico en los sistemas de procesamiento de información y equipos informáticos?

Sí ○ No (continuar con la pregunta 8) ○

7. ¿Cada cuánto tiempo realizan mantenimientos en los sistemas de procesamiento de información? (se puede seleccionar varias alternativas)

Trimestral ☐
Semestral ☐
Mensual ☐
Otros, Indique el período ☐ _____

8. ¿De cuántos computadores dispone su empresa?

20 – 40 ○ 40 – 60 ○ 60 o más ○

9. ¿Disponen de servidores centrales de datos en la empresa?

Sí ○ No ○

10. Si su empresa tiene conexión WIFI, ¿existen restricciones de seguridad para el acceso de dichas conexiones?

Sí ○ No ○

11. ¿Se realizan respaldo de la información de la empresa?

Sí ○ No (continuar en 13) ○

12. ¿En caso de que se realice respaldo de información, con qué frecuencia lo realizan? (se puede seleccionar varias alternativas)

Diaria ☐
Semanal ☐
Mensual ☐
Otros, indique el período ☐ _____

13. ¿Se utilizan mecanismos de bloqueo automático de las estaciones de trabajo para cuando se encuentran desatendidos?

Sí ○ No ○

14. ¿Existen equipos que provean de energía ininterrumpida a los servidores y computadores de los funcionarios?

Sí ○ No ○

15. ¿Qué servicios y sistemas considera más críticos en términos de disponibilidad? (se puede seleccionar varias alternativas)

De almacenamiento de datos	☐
Servicios de comunicación	☐
Sistemas de procesamiento de datos	☐
Otros, indique cuáles	☐ _____

16. ¿Dónde se encuentran almacenados los medios de respaldos? (se puede seleccionar varias alternativas)

Dentro del área de sistemas	☐
Dentro de la empresa, pero fuera del área de sistemas	☐
Fuera de la empresa	☐
No se realizan almacenamientos.	☐
Otros, indique cuáles _____	☐

17. ¿Durante el último año tuvieron algún incidente de seguridad grave de la información?

Sí ○ No ○ Desconoce ○

18. ¿Se mantiene un registro de fallas cuando ocurre algún evento en los sistemas de procesamiento de información (servidores, computadores, redes, etc.)?

Sí ○ No ○

19. ¿El acceso a internet en la empresa es limitado por? (se puede seleccionar varias alternativas)

Cargo	☐
Usuario	☐
Indique el mecanismo	☐ _____
Ninguna	☐

20. ¿Posee un plan de contingencia vigente en caso de desastres naturales?

Sí ○ No ○ Desconoce ○

ANEXO 2

Entrevista dirigidas al Departamento de Sistemas

1. **¿La empresa cuenta con un Manual de Política de Seguridad de la Información?**

   Si (continuar con la pregunta 2)
   No (continuar con la pregunta 4)

2. **¿Cada que tiempo actualiza el Manual de Política Seguridad de la Información?**

3. **¿El Manual de Política de Seguridad de la Información se encuentran socializadas a todo el personal de la empresa?**

4. **¿Se actualizan periódicamente los procedimientos e instructivos establecidos en el área?**

   Si (continuar con la pregunta 6)
   No (continuar con la pregunta 5)

5. **¿Por qué no se actualizan los procedimientos e instructivos del área?**

No es necesario modificarla	
No se dispone de suficiente personal	
No lo considera importante	
Otra	

6. **¿Existe el apoyo necesario de las máximas autoridades en temas de tecnología?**

   Si
   No

7. **¿Se realizan campañas periódicamente para dar a conocer temas relacionados con seguridad de la información?**

   Si (continuar con la pregunta 9)
   No (continuar con la pregunta 8)

8. **Describa la razón del porqué no se realizan campañas referentes a seguridad de la información**

9. **¿Se tiene establecido perfiles de usuarios de acuerdo a los roles, responsabilidades para otorgar acceso a los funcionarios?**

   Si
   No

10. **¿Existen criterios para la clasificación de la información?**

    Si
    No

11. **¿Existen controles de seguridad implementados en los aplicativos utilizados en la empresa?**

Nombre de Control	Si/ No	Forma de Implementación	Se encuentra documentado	Intervalo de actualización
Medios extraíbles de datos				
Control de Accesos: Creación y Eliminación de privilegios de usuarios				
Clasificación de la información				
Traslado de Propiedad				
Gestión de cambio				
Control contra software malicioso				
Gestión en la entrega de servicios de terceros				
Respaldo de información				

Control de Acceso a Internet				
Control de Acceso a correo				
Control de Acceso/Seguridad de redes alámbricas e inalámbricas				
Aceptación del sistema				
Gestión de Incidentes				
Derecho de Propiedad Intelectual				

12. **¿Cuántos USER-ID y contraseñas manejan cada funcionario de la empresa?**

13. **¿Cada cuánto tiempo obliga el sistema a cambiar la contraseña del correo institucional, estación de trabajo y aplicativos manejados por los funcionarios?**

14. **¿Existe una infraestructura adecuada donde se disponen equipos como ups, rack?**

15. **¿Poseen inventarios de tecnología?**

Si

	Inventario	**Intervalo de actualización**
Software	Licencias	
	Suite ofimática	
	Sistemas Operativos	
	Aplicativos del	

	negocio	
Hardware	Equipos móviles	
	Equipos de computación	
	Equipos de red	
	Dispositivos de almacenamiento	
Otros		

16. **¿Cuál es el motivo de no realizar un inventario de los activos de software y hardware?**

17. **En caso de haber ocurrido un incidente de seguridad en el último año, describa lo ocurrido**

18. **Describa el plan de contingencia en casos de incidentes graves o desastres naturales**

ANEXO 3

Entrevista dirigida para las áreas de Credigestión

1. **¿Existen procedimientos e instructivos establecidos en el área?**

   Si (continuar con la pregunta 2)
   No (continuar con la pregunta 3)

2. **¿Cada qué tiempo se actualizan los procedimientos?**

Mensual	
Trimestral	
Semestral	
Otros	

3. **¿Se tiene identificado y categorizado los activos de información del área?**

   Si

Nombre del activo	**Categoría(Confidencial, pública, de uso interno)**
•	

   No

4. **¿Ha ocurrido algún evento que ha afectado a la continuidad de sus actividades?**

Suceso	**Tiempo de interrupción**

5. **¿Los funcionarios poseen tarjetas de acceso para ingresar al departamento?**

   Si (continuar con la pregunta 7)
   No (continuar con la pregunta 6)

6. **¿Por qué razón los funcionarios no poseen tarjetas de acceso al departamento?**

No las provee la empresa	
No son necesarias	
No hay sistemas de control de acceso	
Otras	

7. **¿Se han presentados retrasos o problemas por falta de controles de seguridad (antivirus no actualizado, la no existencias de restricciones a internet, entre otros) en los equipos utilizados por los funcionarios del área?**

Problema	Criticidad (Alta, media, baja)

8. **¿Quién es la persona responsable de definir los accesos que debe tener cada funcionario del área?**

9. **¿Cuándo se le bloquea el acceso a la estación de trabajo, correo electrónico o sistema utilizado en el área, a quien solicita ayuda?**

10. **¿Ha detectado alguna vez una vulnerabilidad en los aplicativos de la institución?**

    Si (continuar con la pregunta 11)
    No (continuar con la pregunta 12)

11. **¿A quién notificó la vulnerabilidad encontrada?**

12. **¿El Departamento de Sistema los capacita para el correcto uso de los nuevos aplicativos o cuando realiza modificaciones en los aplicativos existentes?**

ANEXO 4

Encuesta acerca de Seguridad Informática dirigida al personal operativo

Nota: Marcar con una **X** sus respuestas

1. **¿Conoce de qué se trata el tema de Seguridad Informática y Seguridad de la Información?**

   Sí ○ No ○ Desconoce ○

2. **¿Conoce si en la empresa existe un responsable o área encargada de la seguridad informática y seguridad de la información?**

   Sí ○ No ○ Desconoce ○

3. **¿Qué área considera que debe ser responsable de la seguridad de la informática y de la información? (se puede seleccionar varias alternativas)**

   Sistemas ☐
   Administrativo ☐
   Todas las áreas ☐
   Otra, cuál? ☐ _____

4. **¿Cuántas capacitaciones ha recibido acerca de temas seguridad de la información en el último año?**

   Más de 5 ○ Menos de 5 ○ Nunca ha recibido ○

5. **¿Las contraseñas que utiliza tiene combinación de números, letras y es de más de 10 caracteres?**

   Solo Números y más de 10 caracteres ☒
   Solo letras y más de 10 caracteres ☐
   Números y letras, más de 10 caracteres ☐
   Otras, describa? ☐ _____

6. **¿Ha ocurrido algún incidente de seguridad en su puesto de trabajo en el último año? (bloqueo de la computadora, pérdida de documentos, daño de computadora, entre otros)**

   Sí ○ No ○ Desconoce ○

7. **¿Se le bloquea automáticamente su computadora cuando no la está utilizando?**

Sí ○ No ○ Desconoce ○

8. **¿Guarda en un lugar seguro (caja fuerte, gabinetes con llave) los documentos confidenciales cuando ya no los está utilizando?**

Siempre ○ A veces ○ Casi Nunca ○ Nunca ○

9. **¿Cuándo tiene algún incidente de seguridad (falla de equipo, bloqueo de contraseña, pérdida de información) a quién lo notifica? (se puede seleccionar varias alternativas)**

Gerente de Sistemas ☐
Jefe Inmediato ☐
Altos Directivos ☐
No notifica ☐
Otros, cuál? ☐ _____

10. **¿Cree que es necesario aplicar controles de seguridad para evitar robo o daño de información importante para la empresa?**

Totalmente de acuerdo ☐
De acuerdo ☐
Ni de acuerdo ni en desacuerdo ☐
En desacuerdo, porque? ☐ _____

11. **¿Qué documentos que maneja, considera usted que son catalogados como confidencial o de acceso restringido?**

Todos ○ Algunos ○ Ninguno ○

12. **¿Conoce si existe en la empresa áreas restringidas a las cuales solo pueden acceder personal autorizado?**

Sí ○ No ○ Desconoce ○