UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA DE SISTEMAS Y ADMINISTRACIÓN DE EMPRESAS

CARRERA PROFESIONAL DE INGENIERIA DE SISTEMAS

“PROPUESTA DEL PLAN PARA LA SEGURIDAD DE LA INFORMACION EN LA EMPRESA DE SOFTWARE QUIPU SOLUCIONES EMPRESARIALES S.A.C. CON LA NORMA ISO 27001”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

GUZMAN MARCHAND, JUNIOR MANUEL

Villa El Salvador

2017

Dedicatoria

Quiero dedicar este proyecto de investigación de fin de carrera a mi familia y amigos, especialmente a mi modelo a seguir, mi madre Mercedes, gracias a su orientación y apoyo en los momentos que lo necesité.

Agradecimiento

Agradezco a Dios por darme esta oportunidad de obtener el título profesional. Agradezco a mis profesores, compañeros por haberme apoyado.

Índice

Listado de Figuras vi
Listado de Tablas vii
Introducción viii
CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA 1
1.1 Descripción de la Realidad Problemática 1
1.2 Justificación del Problema 2
1.3 Delimitación del Proyecto 3
1.4 Formulación del Problema 4
1.4.1 Problema principal 4
1.4.2 Problemas específicos 4
1.5 Objetivos 4
1.5.1 Objetivo General 4
1.5.2 Objetivos Específicos 4
CAPÍTULO II: MARCO TEÓRICO 6
2.1 Antecedentes de la Investigación 6
2.1.1. Nacionales 6
2.1.2. Internacionales 8
2.2. Bases Teóricas 11
2.2.1. Norma ISO/IEC 27001 11
2.2.2. Dominios de seguridad: 13
2.2.3. Ciclo de Deming 19
2.3. Marco Conceptual 21
2.3.1. Controles: 21
2.3.2. Estándar: 22
2.3.3. Gestión: 22
2.3.4. Implementación: 23
2.3.5. Información: 23
2.3.6. ISO: 23
2.3.7. ISO 27001: 24
2.3.8. Norma: 24
2.3.9. Políticas: 24
2.3.10. Políticas de seguridad de información: 25
2.3.11. Riesgo: 25
2.3.12. Seguridad: 25
2.3.13. Seguridad de información: 26

2.3.14. Sistema: 26
2.3.15. Sistema de gestión: 26
2.3.16. Software: 27
2.3.17. TIC: 27
CAPÍTULO III: DESCRIPCIÓN DEL MODELO METODOLÓGICO 28
3.1 Modelo de Análisis de riesgo 28
3.1.1. Identificación de activos de la Información 29
3.1.2. Valoración de Activos de Información 31
3.1.3. Identificación de Amenazas 34
3.1.4. Posibilidad de ocurrencia de amenazas 36
3.1.5. Identificación de vulnerabilidades 37
3.1.6. Posible explotación de Vulnerabilidades 39
3.1.7. Estimado del Valor de los Activos en Riesgo 41
3.1.8. Posibilidad de Ocurrencia del Riesgo 42
3.1.9. Valor del Riesgo de los Activos 44
3.2. Análisis de resultados 48
3.3. Políticas de seguridad de información 50
3.3.1. Políticas Generales de Seguridad de la Información 51
3.3.2. Políticas Específicas de Seguridad de la Información 53
3.4. Selección de controles para mitigar los riesgos 57
3.4.1. Seguridad Lógica 57
3.4.2. Seguridad Personal 59
3.4.3. Seguridad Física y Ambiental 60
3.4.4. Inventario de los activos y clasificación de la información 61
3.4.5. Administración de las comunicaciones 63
3.4.6. Adquisición y mantenimiento de sistemas informáticos 63
3.4.7. Procedimientos de respaldo 64
3.4.8. Gestión de incidentes de seguridad de la información. 65
3.4.9. Cumplimiento Normativo y de Auditoria. 66
3.5. Análisis Costo-Beneficio 78
Conclusiones 78
Recomendaciones 80
Anexos 85

Listado de Figuras

Figura N° 1 Actividades del Análisis de Riesgo..... 28
Figura N° 2 Matriz de Evaluación de Riesgo en Activos de Información..... 48

Listado de Tablas

Tabla N° 1 Activos de información-Gerente General **29**
Tabla N° 2 Activos de información-Responsable del área de desarrollo **29**
Tabla N° 3 Activos de información-Responsable del área de soporte **30**
Tabla N° 4 Valoración de los activos de información **31**
Tabla N° 5 Valoración del Hardware **31**
Tabla N° 6 Valoración del Software **32**
Tabla N° 7 Valoración del Documentos/Archivos **33**
Tabla N° 8 Identificación de amenazas a los activos de información **34**
Tabla N° 9 Valoración de ocurrencias de amenazas **36**
Tabla N° 10 Evaluación de ocurrencias de amenazas **36**
Tabla N° 11 Identificación de vulnerabilidades de los activos de información. **38**
Tabla N° 12 Tabla de valoración de la vulnerabilidad **39**
Tabla N° 13 Evaluación de posibilidad de explotación de vulnerabilidades **40**
Tabla N° 14 Evaluación de los Activos en Riesgo **41**
Tabla N° 15 Evaluación de la posibilidad de ocurrencia del riesgo **42**
Tabla N° 16 Valoración de la probabilidad de ocurrencia **45**
Tabla N° 17 Valoración del impacto **46**
Tabla N° 18 Resultados de Valoración **46**
Tabla N° 19 Riesgo de los Activos de Información **49**
Tabla N° 20 Controles de Política General 1 ..... **67**
Tabla N° 21Controles de Política General 2 ..... **67**
Tabla N° 22Controles de Política General 3 ..... **68**
Tabla N° 23Controles de Política General 4 ..... **68**
Tabla N° 24 Controles de Política General 5 ..... **68**
Tabla N° 25 Controles de Política General 6 ..... **69**
Tabla N° 26 Controles de Política General 7 ..... **69**
Tabla N° 27 Controles de Política General 8 ..... **69**
Tabla N° 28 Controles de Política General 9 ..... **70**
Tabla N° 29 Controles de Política General 10 ..... **70**
Tabla N° 30 Controles de Política General 11 ..... **70**
Tabla N° 31 Controles de Política General 12 ..... **71**
Tabla N° 32 Controles de Política General 13 ..... **71**
Tabla N° 33 Controles de Política General 14 ..... **71**
Tabla N° 34 Controles de Política Específica 1 ..... **72**
Tabla N° 35 Controles de Política Específica 2.1 ..... **72**
Tabla N° 36 Controles de Política Específica 2.2 ..... **73**
Tabla N° 37 Controles de Política Específica 3.1 ..... **73**
Tabla N° 38 Controles de Política Específica 4.1 ..... **74**
Tabla N° 39 Controles de Política Específica 4.2-4.3 ..... **74**
Tabla N° 40 Controles de Política Específica 4.4 ..... **75**
Tabla N° 41 Controles de Política Específica 5.1 ..... **75**
Tabla N° 42 Controles de Política Específica 6 ..... **75**
Tabla N° 43 Controles de Política Específica 7 ..... **76**
Tabla N° 44 Controles de Política Específica 8 ..... **76**
Tabla N° 45 Controles de Política Específica 9 ..... **77**
Tabla N° 46 Controles de Política Específica 10 ..... **77**
Tabla N° 47Analisis Costo-Beneficio **78**

Introducción

El presente trabajo se enfoca en proponer un plan para la seguridad de información en la empresa Quipu Soluciones Empresariales basado en ISO 27001. Esta organización desarrolla soluciones empresariales en el rubro de la gestión de la información.

En los últimos años, con el constante uso de tecnologías de información hace que se vinculen con los objetivos organizacionales y esto ocasiona un aumento de riesgos y amenazas, por lo tanto es necesario proteger este importante activo y garantizar la permanencia de sus propiedades.

Se puede decir que ahora el activo más importante que posee una organización es su información, sin embargo en la mayoría de situaciones estas no desarrollan normas o políticas que se orienten a proteger este activo, por ello se dan espacios que son aprovechados ilícitamente por agentes externos e internos a esta empresa y como resultado de ello se obtienen problemas de perdida de información o alteración; debiendo ser lo contrario con el uso de tecnología de información.

Existen diversos escenarios como: ataques mediante malware o una simple fuga de información, entre otros con el fin de obtener información confidencial y sacar provecho de ella ilícitamente, es necesario gestionar las herramientas de manera efectiva y planificada y reducir estas amenazas.

El presente proyecto, reúne información necesaria para un plan que asegure la información, basado en la norma ISO 27001, teniendo como referencia que contiene un estándar mundialmente reconocido y además sirve como base a otros estándares de seguridad y calidad.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la Realidad Problemática

La empresa software Quipu Soluciones Empresariales S.A.C. día a día genera reportes, actas, cotizaciones y material de diferente índole de suma importancia para la continuidad de sus actividades. Esta información es almacenada en medios físicos y electrónicos, y es puesta a disposición del personal sin ningún control ni de acuerdo a las funciones que estos desempeñan.

Debido al aumento de personal y la falta de un esquema organizacional, la probabilidad de que la información sea manipulada con fines ajenos a la actividad de la empresa, ha aumentado exponencialmente. Lo cual resulta peligroso para la organización, ya que cerca del 80% de estos activos de información se involucran con la cobranza e historial de soporte de los clientes; conllevando de esta manera a una pérdida no solo de información, sino también pérdida de ingresos, en adición a esto del total de atenciones remotas alrededor del 60% de estas presentan una oportunidad de ingresos ya sea por renovación de contrato, pagos pendientes o la adquisición de nuevos servicios,

sin embargo el personal de soporte con la información disponible solo aprovecha el 10% de las atenciones remotas como oportunidad de ingresos a la empresa. (R. Ramírez, Entrevista a la gerencia general de Quipu Soluciones Empresariales S.A.C, 10 de enero de 2017).

Por lo anteriormente mencionado es necesario un plan para la seguridad de información basado en la norma ISO 27001 que proporcione herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; para garantizar el correcto desarrollo de las actividades y proporcionar un orden en la organización.

1.2 Justificación del Problema

Establecer un plan para la Seguridad de Información se hace necesario para mantener un orden con el manejo de los activos de información en la empresa Quipu Soluciones Empresariales S.A.C., asegurando la integridad, disponibilidad y confidencialidad de estos. En la actualidad existen normas y estándares sobre el tema de seguridad de información, más no señalan como lograr llegar al objetivo de un plan de seguridad de información.

Es por ello que se propone implementar este plan para la Seguridad de Información en la empresa Quipu Soluciones Empresariales S.A.C., con el cual se pretende incrementar ese 10% de atenciones remotas con oportunidad ingreso. Con esta meta no solo podemos decir que se aumentará la productividad del Área de Soporte, ya que las oportunidades de ingreso aprovechadas serán en beneficio de toda la organización, también será conveniente para las otras áreas de la organización debido a que las políticas y controles propuestos se aplicarán en toda la empresa permitiendo una mejora

en el uso de los activos de información de cada área y la reducción de riesgos. Además será capaz de:

Identificar y administrar sus activos de información.

Tener un orden en la documentación y en consecuencia tener la información disponible en el momento oportuno.

Reducir la pérdida de información y la alteración de la misma.

Tener planes y estrategias para la solución a corto y largo plazo de problemas relacionados a sus activos de información.

Evaluar los controles para la seguridad, confidencialidad y disponibilidad de la información.

De esta manera se justifica la necesidad de un estudio en la empresa Quipu Soluciones Empresariales S.A.C. para desarrollar un plan para la Seguridad de Información adecuado.

1.3 Delimitación del Proyecto

Delimitación de tiempo:

Tanto la extracción de información, su estudio y análisis se dará en el periodo comprendido entre Enero, Febrero y Marzo.

Delimitación de espacio:

La investigación se realizará en la empresa Quipu Soluciones Empresariales S.A.C.

Delimitación temporal:

Este proyecto es de actualidad, debido al constante uso de la norma ISO 27001.

1.4 Formulación del Problema

1.4.1 Problema principal

¿Un Plan para la Seguridad de Información basado en ISO 27001 permitirá mantener y mejorar la integridad, confidencialidad y disponibilidad de la información de la empresa Quipu Soluciones Empresariales S.A.C.?

1.4.2 Problemas específicos

¿El estudio de los estándares que la organización conoce e identificar sus activos de información será de ayuda para la mejora de la seguridad de información?

¿Con el desglose de los procesos de la organización involucrados con la manipulación de información se podrá reconocer, analizar y evaluar los riesgos y debilidades que presenta la organización en seguridad de información?

¿Con definir políticas y controles se afrontarán los riesgos y reducirán sus impactos que genera pérdida de confiabilidad e integridad?

1.5 Objetivos

1.5.1 Objetivo General

Establecer un Plan para la Seguridad de Información, apoyándose en el estándar de la norma ISO 27001 para mantener la integridad, confidencialidad y disponibilidad de la información de la empresa Quipu Soluciones Empresariales S.A.C.

1.5.2 Objetivos Específicos

Realizar un estudio del estado actual de la organización, en base a las normas y estándares de seguridad de información, e identificar los activos de información.

Analizar y desglosar los procesos de la organización involucrados con la manipulación de información para identificar, analizar y evaluar los riesgos que enfrentan los activos de información.

Definir las políticas y controles necesarios para afrontar los riesgos y reducir sus impactos que puedan conllevar a pérdida de confiabilidad e integridad.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la Investigación

2.1.1. Nacionales

Barrantes Porras, Carlos Eduardo**, Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos,** Lima: la investigación llegó a las siguientes conclusiones:

1. El implementar una política de seguridad y que los colaboradores la conozcan e interiorizan, es de gran utilidad cuando se quiere implementar cualquier sistema de gestión en una organización, ya que otorga una visión clara de cómo sus labores cotidianas aportan para el mantenimiento y mejora de un sistema de gestión empresarial.

2. Diseñando e implementando una buena metodología para gestionar los riesgos y ejecutando los planes de tratamiento de riesgos planteados, se logra reducir a niveles aceptables gran porcentaje de riesgos que afecten a los activos de información.

3. El factor humano es crítico para la implementación de cualquier sistema de gestión organizacional es por ello que la formación y concientización de los mismos es indispensable para lograr una implementación exitosa.

Villena Aguilar, Moisés Antonio**, Sistema de gestión de seguridad de información para una institución financiera,** Lima: la investigación llegó a las siguientes conclusiones:

1. para implantar una adecuada gestión de seguridad de información en una institución financiera, el primer paso es obtener el apoyo y soporte de la alta gerencia, haciéndolos participes activos de lo que significa mantener adecuadamente protegida la información de la institución financiera. Al demostrarles lo importante que es la protección de la información para los procesos de negocio, se debe esperar de la alta gerencia su participación continua.

2. No necesariamente la tecnología de información por sí sola garantiza la seguridad de información. Se vuelve imperativo gestionarla de acuerdo siempre a los objetivos de negocio. De nada sirve contar con los últimos adelantos tecnológicos, si no se da la importancia debida a la protección de la información, la cual se verá reflejada en el cumplimiento de todas las políticas de seguridad de información, siempre actualizadas de acuerdo a los cambios constantes en los negocios propios de una institución financiera.

Aguirre Mollehuanca, David Arturo**, Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.**, Lima: la investigación llegó a las siguientes conclusiones:

1. El apoyo de la alta gerencia para el diseño de este sistema de gestión fue imprescindible, debido a que fue necesaria su intervención para ayudar a concientizar a los jefes de área y dueños de los procesos a participar de las entrevistas de levantamiento de información y ayudó a que entendieran que el SGSI no solo busca proteger la información digital, sino toda la información crítica del negocio independientemente del medio que la contenga.

2. Es necesario difundir las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, esto debido a la poca cultura de seguridad que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas.

3. Existe una clara necesidad en la organización de contratar personal especializado para dar soporte a los procesos involucrados en el SGSI, debido a que los recursos actuales no se dan abasto para atender los requerimientos de los usuarios lo cual en muchos casos se ha utilizado como excusa para realizar actos que afectan la seguridad de la información como el préstamo de credenciales de usuarios, uso de un correo para varias personas o la dejadez en la generación de respaldos de información del área.

2.1.2. Internacionales

Tola Franco, Diana Elizabeth**, Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y**

auditoría aplicando la norma ISO/IEC 27001, Guayaquil: la investigación llegó a las siguientes conclusiones:

1. Es importante establecer los objetivos y políticas del SGSI, ya que estos van delineando el camino hacia donde la organización desea dirigirse para preservar la confidencialidad, integridad y disponibilidad de la información y por lo tanto es relevante la participación de la alta gerencia.

2. La adopción de la metodología MAGERIT para el análisis de riesgos, permitirá identificar de manera oportuna la probabilidad y el impacto de que se materialicen los riesgos y de esta manera poder establecer controles que nos ayuden a prevenirlos.

3. Dentro del ciclo de un Sistema de Gestión de Seguridad de la Información, basado en ISO 27001, se encuentra la mejora continua lo cual hace que sea muy importante que la organización se asegure de crear procedimientos para el monitoreo y revisión del sistema, los mismos que deben cubrir incidentes de seguridad, auditorías internas y revisiones gerenciales. Estos elementos aportan retroalimentación al Sistema posibilitando conocer el estado del mismo y aplicar acciones correctivas, si fuera el caso, que permitan el cumplimiento de los planes y objetivos.

Mesquida Calafat, Antoni Lluis**, Un modelo para facilitar la integración de estándares de gestión de TI en entornos maduros**, Palma: la investigación llegó a las siguientes conclusiones:

1. Se ha ofrecido una visión de la situación actual de los estándares de gestión de TI para identificar sus elementos comunes y crear un nuevo modelo

integrado que facilite la implantación de estos estándares reduciendo esfuerzos y duplicidades.

2. Se han analizado las relaciones, totales o parciales, entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y las mejores prácticas de los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5. A partir de estas relaciones se ha elaborado un Mapa de relaciones entre los procesos de gestión de servicios de TI de la norma ISO/IEC 20000-4 y los procesos del ciclo de vida del software de la norma ISO/IEC 15504-5. Este mapa puede ser utilizado para facilitar la implantación de los procesos de gestión de servicios de TI en empresas de desarrollo de software involucradas en un programa de mejora de procesos según la norma ISO/IEC 15504, y también para maximizar la eficiencia de la implantación simultánea de ambos estándares reduciendo la cantidad de esfuerzo en una organización que vaya a comenzar la implantación de sus procesos por vez primera.

Polanco Velez, Adriana Paola**, Diseño de un manual de procedimientos del sistema contable en la empresa FEVECOMEX S.A.S. basado en la norma técnica colombiana para la seguridad de la información NTC-ISO/IEC 27001/2006**, Cartagena: la investigación llegó a las siguientes conclusiones:

1. Como medida utilizada para manejar el éxito de la organización se establecieron indicadores de gestión en la caracterización de los procesos, clasificados intrínsecamente en: EFICIENCIA organizando los procesos para producir los mejores resultados posibles con los recursos disponibles y en efectividad en el nivel de logro de los requerimientos u objetivos propuestos.

Igualmente se hace seguimiento a la perspectiva del cliente y se busca la mejora continua de los procesos sin dejar de un lado los indicadores financieros clásicos como son: el aumento de ventas y la disminución de costos, pero exigiéndole al gerente realizar un seguimiento mucho más amplio que incluya otras variable de interés para la organización a través de la interacción con todas las actividades de la empresa.

2. Dominar la información dentro de una organización es cada vez más importante y se ha convertido en un requerimiento necesario y estratégico para la toma de decisiones, por tal razón en este manual de procedimientos se enumeran cada una de las actividades que influyen en el área financiera y contable tanto de los funcionarios, como de los procesos y procedimientos propuestos a la organización, logrando así incrementar la productividad y eficiencia de la empresa satisfaciendo la necesidad de los clientes.

2.2. Bases Teóricas

2.2.1. Norma ISO/IEC 27001

a) ISO/IEC 27001:2013

“Desde la versión 2005 surgieron los siguientes cambios:

- Desaparece la sección "enfoque a procesos" dando mayor flexibilidad para la elección de metodologías de trabajo para el análisis de riesgos y mejoras.
- Cambia su estructura conforme al anexo SL común al resto de estándares de la ISO.

- Considerables cambios en los controles establecidos en el Anexo A, incrementando el número de dominios a 14 y disminuyendo el número de controles a 114.
- Inclusión de un nuevo dominio sobre "Relaciones con el Proveedor" por las crecientes relaciones entre empresa y proveedor en la nube.
- Se parte del análisis de riesgos para determinar los controles necesarios y compararlos con el Anexo A, en lugar de identificar primero los activos, las amenazas y sus vulnerabilidades. ” García (2013, ¶ 3)

b) Beneficios

- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

2.2.2. Dominios de seguridad:

a) Políticas de seguridad de la información

Tiene como objetivo otorgar dirección y soporte a la gerencia para la seguridad de información en relación con los requisitos del negocio y las leyes reguladoras relevantes.

“La Política de Seguridad de la Información de una organización debe definir las decisiones que ha tomado la organización en relación a la seguridad del almacenamiento y procesamiento de la información. Este conjunto de decisiones debería basarse en requisitos legales y regulatorios, en la demanda del mercado, en los objetivos de negocio y en la filosofía y cultura de la empresa.” Baldecchi, conferencia, (04 setiembre 2014).

Es un requisito fundamental que todos los miembros de la organización conozcan las políticas de seguridad de la información y deben comprometerse a cumplir y llevar un orden.

b) Organización de la seguridad de información

Tiene como objetivo definir el marco de referencia para la gestión e iniciar la implementación y operación de la seguridad de la información dentro de la organización.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

- Una Política de Seguridad de Información
- Un Responsable de Seguridad de Información
- Un Comité de Gestión de Seguridad de Información

c) Seguridad en los Recursos Humanos

Tiene como objetivo asegurar que el personal comprenda sus responsabilidades y sus respectivos roles para los cuales se consideran. Siempre se toma como recurso más importante de la organización, por ello se lleva un proceso en la conformación del área de recursos humanos:

- Selección
- Contratación
- Formación de empleados
- Cambios de puesto de trabajos

d) Gestión de Activos

Tiene como objetivo la identificación de los activos en la organización y definir las responsabilidades para su debido uso y cuidado.

“Primero se debe incluir un miembro como responsable para así brindar el mantenimiento de los controles. En este caso nos enfocamos en la información que se debería clasificar para indicar las prioridades y el grado esperado de protección al manejar la información.” Baldecchi, conferencia, (04 setiembre 2014)

e) Control de Accesos

Tiene como objetivo la limitación del acceso a la información y a las instalaciones de procesamiento de información.

Como parte de este dominio se desarrollan los lineamientos para la política de control de acceso, la gestión de accesos de usuarios, los controles de acceso a la red, al sistema operativo, a las aplicaciones y a la información.

Incluye las consideraciones para el manejo de ordenadores y portátiles.

- Gestión de acceso de usuarios
- Registro de usuarios
- Responsabilidad de usuario
- Gestión de contraseñas
- Protección de equipos desatendidos

f) Criptografía

Tiene como objetivo asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información. **"**Para introducir un control primero se tiene que determinar siempre de acuerdo a la identificación de cualquier riesgo que la organización aun no asume, sin embargo la inversión de un control no puede tener mayor valor que el activo por lo que no resultaría rentable.**"** Baldecchi, conferencia, (04 setiembre 2014). Se debe establecer un procedimiento que exponga como se ha de llevar a cabo la generación de las claves y certificados, como se tiene que almacenar, como se debe actualizar, como se van a distribuir, o por consiguiente, revocar.

g) Seguridad Física y Ambiental

Tiene como objetivo impedir el acceso físico no autorizado, daño e interferencia hacia la información y a sus instalaciones de procesamiento.
Las instalaciones que estén involucradas con los activos de información deben cumplir con las normas de seguridad física y ambiental, para garantizar que la información manejada en éstas permanezca siempre protegida de accesos

físicos por parte de personal no autorizado o por factores ambientales que no se puedan controlar.

Las normas sobre seguridad física deben contener los controles de acceso a personal no autorizado en las instalaciones y centros de procesamiento de información de la Organización, para garantizar la seguridad de los activos de información.

h) Seguridad en las Operaciones

Tiene como objetivo asegurar que las operaciones se desarrollen de manera correcta y segura.

- Procedimientos y responsabilidades de operación.
- Gestión de servicios tercerizados.
- Planificación y aceptación del sistema.
- Protección contra software malicioso.
- Gestión de respaldo y recuperación.
- Gestión de seguridad en redes.
- Utilización de los medios de información
- Intercambio de información
- Servicios de comercio electrónico
- Monitoreo.

i) Seguridad en las Comunicaciones

Tiene como objetivo asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.

- Manejo de los medios

- Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio. Estos medios se deberían controlar y proteger de forma física.
- Intercambio de la información
- Los intercambios de información y de software entre las organizaciones se deberían basar en una política formal de intercambio, ejecutar según los acuerdos de intercambio y cumplir la legislación correspondiente.
- Se deberían establecer procedimientos y normas para proteger la información y los medios físicos Que contienen información en tránsito.

j) Adquisición, Desarrollo y Mantenimiento de Sistemas

Tiene como objetivo Garantizar la seguridad de la información como parte de los sistemas de información a través de los requisitos que proporciones los sistemas de información.

Este dominio está orientado hacia organizaciones que desarrollan software internamente o adquiera un sistema desarrollado por terceros.

k) Relaciones con Proveedores

Tiene como objetivo asegurar la protección a los activos de la organización que son accesibles por los proveedores.

Para ellos se lleva una colaboración con los proveedores en:

- Registro de proveedores.
- Colaboración para pedidos.
- Colaboración para diseño.
- Reabastecimiento colaborativos.

- Conectividad con proveedores.

l) Gestión de Incidentes de Seguridad de la Información

Tiene como objetivo asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, donde se incluye amenazas y debilidades.

El objeto de análisis en este dominio son las incidencias de seguridad que siempre van a existir y están siempre acompañadas de un riesgo por ello todos los incidentes de seguridad significativos deben quedar registradas.

El procedimiento de gestión de incidencias debe documentar claramente los roles y responsabilidades de los actores participantes.

m) Aspectos de la Seguridad de la Información dentro de la Continuidad del Negocio

Tiene como objetivo la continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización

- Incluir la Seguridad de la Información en el proceso de Gestión de Continuidad del Negocio.
- Continuidad del Negocio y Análisis de Riesgos.
- Desarrollar Planes de Continuidad del Negocio incluyendo aspectos de seguridad de la información.
- Marco Referencial para la Planeación de la Continuidad del Negocio.
- Prueba, mantenimiento y actualización de los planes de continuidad del negocio.

n) Cumplimiento

Tiene como objetivo evitar la infracción de las obligaciones legales o reguladoras relacionadas a la seguridad de información

2.2.3. Ciclo de Deming

a) Definición:

Es una metodología que se basa en cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad.

El ciclo de Deming lo componen 4 etapas cíclicas, de forma que una vez acabada la etapa final se debe volver a la primera y repetir el ciclo de nuevo, de forma que las actividades son reevaluadas periódicamente para incorporar nuevas mejoras. La aplicación de esta metodología está enfocada principalmente para para ser usada en empresas y organizaciones.

b) Etapas:

- **Plan(Planificar)**

"Establecer los objetivos y procesos necesarios para obtener el resultado esperado. Al basar las acciones en el resultado esperado, la exactitud y cumplimiento de las especificaciones a lograr se convierten también en un elemento a mejorar.**"** Briceño (2013, ¶ 3)

Se recomienda seguir los siguientes procesos:

- Establecer el contexto.
- Alcance y Limites.
- Definir Política.

- Definir Enfoque de Evaluación de Riesgos.
- Identificación de riesgos.
- Análisis y Evaluación de riesgos.
- Evaluar alternativas para el Plan de tratamiento de riesgos.
- Aceptación de riesgos.
- Declaración de Aplicabilidad.

- **Do(Hacer)**

"Implementar los nuevos procesos, llevar a cabo el plan. Recolectar datos para utilizar en las siguientes etapas. Teniendo el plan bien definido, hay que poner una fecha a la cual se va a desarrollar lo planeado." Briceño (2013, ¶ 3)

Se recomienda seguir los siguientes procesos:

- Implementar plan de tratamiento de riesgos.
- Implementar los controles seleccionados.
- Definir las métricas.
- Implementar programas de formación y sensibilización.
- Gestionar la operación del plan de seguridad de información.
- Gestionar recursos Implementar procedimientos y controles para la gestión de incidentes de seguridad.

- **Check(Verificar)**

"Pasado un periodo de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora monitorizar la implementación y evaluar el plan de ejecución documentando las conclusiones.**"** Briceño (2013, ¶ 3)

Se recomienda seguir los siguientes procesos:

- Ejecutar procedimientos de seguimiento y revisión de controles.
- Realizar revisiones regulares de cumplimiento y eficacia de los controles del plan de seguridad de información.
- Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad.
- Revisión de la evaluación de riesgos periódicamente.
- Realizar auditorías internas Revisión de alcance y líneas de mejoras del plan de seguridad de información.
- Actualizar los planes de seguridad y registrar acciones que podrían impactar la eficacia y/o eficiencia del plan de seguridad de información.

- **Act(Actuar)**

Se recomienda seguir los siguientes procesos:

- Implementar las mejoras identificadas para el plan de seguridad de información.
- Implementar las acciones correctivas y preventivas pertinentes.
- Comunicar acciones y mejoras a todas las partes involucradas.
- Asegurarse que las mejoras logren los objetivos previstos.

2.3. Marco Conceptual

2.3.1. Controles:

“El control es el proceso de verificar el desempeño de distintas áreas o funciones de una organización. Usualmente implica una comparación entre un

rendimiento esperado y un rendimiento observado, para verificar si se están cumpliendo los objetivos de forma eficiente y eficaz y tomar acciones correctivas cuando sea necesario.

La función de control se relaciona con la función de planificación, porque el control busca que el desempeño se ajuste a los planes. El proceso administrativo, desde el punto de vista tradicional, es un proceso circular que se retroalimenta. Es por esto que en la gestión, el control permite tomar medidas correctivas.**”** Anzil (2010, ¶ 2)

2.3.2. Estándar:

“El estándar es una publicación que recoge el trabajo en común de los comités de fabricantes, usuario, organizaciones, departamentos de gobierno y consumidores y que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional, con el objetivo de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología.**”** ISO27000.ES (2014, ¶ 5)

2.3.3. Gestión:

“Proceso de identificación, análisis y capacidad de respuesta ante todos los posibles factores de riesgo que se podrían presentar durante el proyecto. La correcta gestión de los riesgos permite no solo que se reduzca la posibilidad de aparición del factor de riesgo sino también la de su impacto.**”** ITM Platform (2015, ¶ 1)

2.3.4. Implementación:

Una implementación es la instalación de una aplicación informática, realización o la ejecución de un plan, idea, modelo científico, diseño, especificación, estándar, algoritmo o política.

"En ciencias de la computación, una implementación es la realización de una especificación técnica o algoritmos como un programa, componente software, u otro sistema de cómputo. Muchas implementaciones son dadas según a una especificación o un estándar.**"** Wikipedia (2015, ¶ 1)

2.3.5. Información:

"La información es un conjunto de datos acerca de algún suceso, hecho, fenómeno o situación, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo.**"** Thompson (2008, ¶ 1)

2.3.6. ISO:

"ISO es una federación mundial de organismos nacionales de normalización (Organismos miembros de ISO). El trabajo de preparación de las normas internacionales normalmente se realiza a través de comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se haya establecido un comité técnico, tiene el derecho a estar representado en dicho comité. Las organizaciones internacionales, públicas y privadas, en coordinación con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (CEI) en todas las materias de normalización electrotécnica.**"** Posada (2007, ¶ 1)

2.3.7. ISO 27001:

“El estándar para la seguridad de la información ISO/IEC-27001 fue aprobado y publicado en 2005 por la International Organization for Standardization y por la International Electrotechnical Commission, especificando los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).**”** Acevedo (2011, ¶ 3)

2.3.8. Norma:

Una norma es un documento técnico de aplicación voluntaria, fruto del consenso, basado en los resultados de la experiencia y del desarrollo tecnológico y aprobado por un organismo de normalización reconocido.

“Las normas garantizan unos niveles de calidad y seguridad que permiten a cualquier empresa posicionarse mejor en el mercado y constituyen una importante fuente de información para los profesionales de cualquier actividad económica.**”**AENOR (2010, ¶ 3)

2.3.9. Políticas:

“Lineamientos generales que orienten las actividades que habrán de realizar los trabajadores involucrados en sus aéreas de trabajo. Precisando de antemano la mayor parte de las situaciones que pudieran presentarse o que propicien la toma de decisiones de las autoridades superiores.**”** Gonzales (2008, ¶ 2)

2.3.10. Políticas de seguridad de información:

“Córdova (2012, p.16), define a una política de seguridad de información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma. Son guías para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales.**”**

2.3.11. Riesgo:

“UNISDR (2004, p.9), define al riesgo como la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre. Sin embargo los riesgos pueden reducirse o manejarse.**”**

Para adicionar a esto si somos cuidadosos en nuestra relación con el ambiente, y si estamos conscientes de nuestras debilidades y vulnerabilidades frente a las amenazas existentes, podemos tomar medidas para asegurarnos de que las amenazas no se conviertan en desastres.

2.3.12. Seguridad:

“La seguridad es el sentimiento de protección frente a carencias y peligros externos que afecten negativamente la calidad de vida; en tanto y en cuanto se hace referencia a un sentimiento, los criterios para determinar los grados de seguridad pecarán de tener algún grado de subjetividad.**”** DefinicionABC (2015, ¶ 1)

2.3.13. Seguridad de información:

Se caracteriza por lo siguiente:

- **Confidencialidad:** Tener presente que esta información solo este accesible al personal adecuado y autorizado.
- **Integridad:** Salvaguardar su exactitud y sin modificaciones no deseadas.
- **Disponibilidad:** Asegurar que el personal pueda acceder a esta en el momento requerido.

2.3.14. Sistema:

“Salazar (2014, p.4), define a un sistema como la reunión o conjunto de elementos relacionados. Puede estructurarse de conceptos, objetos y sujetos. Los sistemas se componen de otros sistemas a los que llámanos subsistemas. En la mayoría de los casos, podemos pensar en sistemas más grandes o superordinales, los cuales comprenden otros sistemas que llamamos sistema total y sistema integral.**”**

2.3.15. Sistema de gestión:

Un sistema de gestión es una estructura probada para la mejora continua y así establecer políticas de tal modo que todos cumplan sus objetivos. La implementación de un sistema de gestión aumenta la efectividad operativa y se optimizan costos logrando un incremento de satisfacción por parte de los interesados.

2.3.16. Software:

“El software representa toda la parte inmaterial o intangible que hace funcionar a un ordenador para que realice una serie de tareas específicas, coloquialmente conocidos como programas el software engloba a toda la información digital que hace al conjunto de elementos físicos y materiales que componen el computador trabajar de manera inteligente.**”** Qué es? (2015, ¶ 1)

2.3.17. TIC:

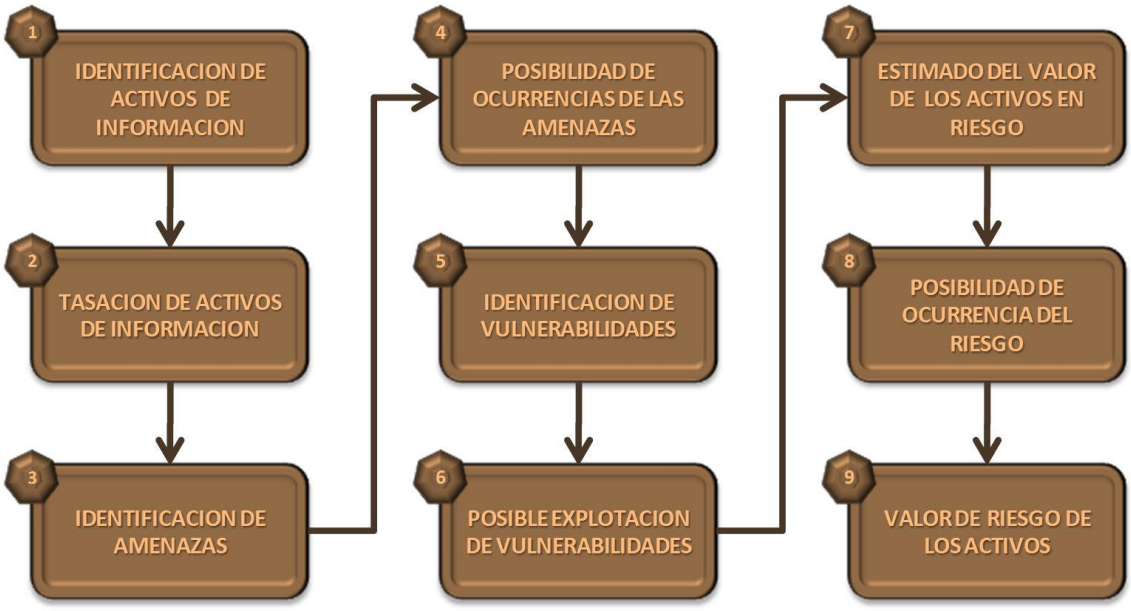
“Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes.**”** ServiciosTIC (2015, ¶ 1)

CAPÍTULO III: DESCRIPCIÓN DEL MODELO METODOLÓGICO

3.1 Modelo de Análisis de riesgo

Este trabajo se basara en la observación y breves entrevistas para identificar los activos de información e iniciar la evaluación sobre amenazas y vulnerabilidades que se irán identificando mediante el proceso de Análisis de riesgo.

Figura N° 1 Actividades del Análisis de Riesgo



Fuente: Elaboración Propia

3.1.1. Identificación de activos de la Información

Se identifican los propietarios funcionales para todos los activos importantes y se asigna la responsabilidad por el mantenimiento de los controles apropiados, como también el tipo de activo de información.

Tabla N° 1 Activos de información-Gerente General

Nro.	Activo de Información	Tipo
1	PC de escritorio	Hardware
2	Impresora-Escaner	Hardware
3	Microsoft Office 2010	Software
4	Antivirus Eset Smart Security 9	Software
5	Microsoft Windows Seven	Software
6	Registros de caja	Documentos Físicos
7	Registros de planilla	Documentos Físicos
8	Documentos de compras	Documentos Físicos
9	Documentos de ventas	Documentos Físicos
10	Registros PDT	Documentos Físicos
11	Cotizaciones	Documentos Físicos
12	Contratos de Venta	Documentos Físicos
13	Registros de RRHH	Documentos Físicos
14	Registros de cobranza	Documentos Físicos

Fuente: Elaboración Propia

Tabla N° 2 Activos de información-Responsable del área de desarrollo

Nro.	Activo de Información	Tipo
1	Laptops	Hardware
2	Servidor	Hardware
3	Impresoras-Ticketeras	Hardware
4	Tablets	Hardware

5	Disco Duro externo	Hardware
6	Programa fuente Quipu-Escritorio	Software
7	Programa fuente Quipu-Web	Software
8	Microsoft SQL-SERVER 2014	Software
9	Microsoft Office 2010	Software
10	Antivirus Eset Smart Security 9	Software
11	Microsoft Windows Seven	Software
12	Microsoft Windows Server 2012	Software
13	Team Viewer 11	Software
14	Visual Studio 2012	Software
15	Actas de Requerimientos	Documentos Físicos
16	Historial de Modificaciones	Documentos Digital
17	Actas de Implementación	Documentos Físicos

Fuente: Elaboración Propia

Tabla N° 3 Activos de información-Responsable del área de soporte

Nro.	**Activo de Información**	**Tipo**
1	Laptops	Hardware
2	Teléfono	Hardware
3	Disco Duro externo	Hardware
4	Microsoft Office 2010	Software
5	Microsoft Windows Seven	Software
6	Team Viewer 11	Software
7	Backups	Archivo Digital
8	Historial de Soportes	Documentos Digital
9	Historial de Actualizaciones	Documentos Digital
10	Solicitudes de Cambio	Documentos Físicos
11	Agenda Telefónica	Documentos Digital
12	Estado de soporte del cliente	Documentos Digital

Fuente: Elaboración Propia

3.1.2. Valoración de Activos de Información

Para valorar los activos de información se emplea la siguiente escala.

Tabla N° 4 Valoración de los activos de información

VALOR		CRITERIO
5	MUY ALTO	Daño muy grave a la empresa
4	ALTO	Daño grave a la empresa
3	MEDIANO	Daño importante a la empresa
2	BAJO	Daño menor a la empresa
1	MUY BAJO	Sin importancia

Fuente: Elaboración Propia

Esta tabla permite evaluar los activos de información mediante su relación a los conceptos claves de información:

- Confidencialidad
- Integridad
- Disponibilidad

Tabla N° 5 Valoración del Hardware

Nº	ACTIVO DE INFORMACIÓN	Confidencialidad	integridad	Disponibilidad	TOTAL
	Hardware				
1	PC de escritorio	4	4	4	4
2	Laptops	4	4	4	4
3	Impresora-Escaner	2	1	2	2

4	Servidor	5	5	5	5
5	Ticketeras	2	1	2	2
6	Tablets	3	1	2	2
7	Disco Duro externo	4	4	3	4
8	Teléfono	2	3	3	3

Fuente: Elaboración Propia

Tabla N° 6 Valoración del Software

Nº	**ACTIVO DE INFORMACIÓN** **Software**	**Confidencialidad**	**integridad**	**Disponibilidad**	**TOTAL**
1	Programa fuente Quipu-Escritorio	5	5	5	5
2	Programa fuente Quipu-Web	5	5	5	5
3	Microsoft Office 2010	2	3	3	3
4	Antivirus Eset Smart Security 9	3	3	3	3
5	Microsoft Windows Seven	2	3	4	3
6	Microsoft SQL-SERVER 2014	4	5	5	5
7	Microsoft Windows Server 2012	5	5	4	5
8	Team Viewer 11	3	2	3	3
9	Visual Studio 2012	3	5	5	4

Fuente: Elaboración Propia

Tabla N° 7 Valoración del Documentos/Archivos

Nº	ACTIVO DE INFORMACIÓN Documentos/Archivos	Confidencialidad	integridad	Disponibilidad	TOTAL
1	Registros de caja	5	5	4	5
2	Registros de planilla	5	5	4	5
3	Documentos de compras	4	5	4	4
4	Documentos de ventas	4	5	4	4
5	Registros PDT	4	5	4	4
6	Cotizaciones	4	5	3	4
7	Contratos de Venta	4	5	3	4
8	Registros de RRHH	5	5	3	4
9	Registros de cobranza	4	5	4	4
10	Actas de Requerimientos	4	3	3	3
11	Historial de Modificaciones	4	2	3	3
12	Actas de Implementación	4	3	3	3
13	Backups	4	5	4	4
14	Historial de Soportes	3	3	2	3
15	Historial de Actualizaciones	3	3	2	3
16	Solicitudes de Cambio	3	3	2	3
17	Agenda Telefónica	3	3	3	3
18	Estado de soporte del cliente	3	2	3	3

Fuente: Elaboración Propia

3.1.3. Identificación de Amenazas

En esta etapa se listará un conjunto de amenazas consideradas vitales que se vincularan a los grupos de activos de información formados según su función y tipo, para poder evaluar el riesgo que generan a la organización y definir controles.

Los controles de seguridad protegerán a los activos de información contra los siguientes tipos de amenazas:

- **Amenazas Lógicas**
- **Amenazas a las Comunicaciones**
- **Amenazas físicas**
- **Fallos Técnicos**
- **Errores Humanos**

En la siguiente tabla se identificará las amenazas para cada grupo de activo de información.

Tabla N° 8 Identificación de amenazas a los activos de información

Nº	GRUPOS DE ACTIVOS DE INFORMACION	AMENAZAS
1	PROGRAMAS FUENTE	Control de cambios.
		Daño intencionado por internos.
		Error de herramienta de programación
		Software malicioso y virus.
2	DOCUMENTOS FISICOS	Alteración y/o plagio
		Entrega incorrecta
		Falsificación
		Incendio, desastres naturales

3	**SERVIDORES**	Error en el mantenimiento de hardware
		Daño intencionado por externos
		Falla de servicio de red y otros servicios
		Falla de software aplicación o Software malicioso
		Incendio y/o desastres naturales
		Suplantación identidad
		Abuso de los recursos del sistema y repudio
4	**EQUIPOS**	Error de operador
		Error en el mantenimiento de hardware
		Suplantación identidad
		Abuso de los recursos del sistema y repudio
		Falla de equipo
5	**DATA ALMACENADA**	Falla de operador
		Falla en dispositivo de almacenamiento
		Backup no autorizado
6	**SOFTWARE**	Robo de licencias
		Software malicioso y virus
		Error de usuario
		Uso no autorizado.
		Error de Actualización

Fuente: Elaboración Propia

3.1.4. Posibilidad de ocurrencia de amenazas

A cada amenaza identificada se ha calculado la posibilidad de ocurrencia y el impacto que puede ocasionar en esta organización.

Tabla N° 9 Valoración de ocurrencias de amenazas

VALOR		CRITERIO
5	MUY ALTO	Definitivamente va a ocurrir, es cuestión de tiempo
4	ALTO	Muy probable
3	MEDIANO	Medianamente probable
2	BAJO	Probable
1	MUY BAJO	Poco Probable

Fuente: Elaboración Propia

En la siguiente tabla se valorará las amenazas para cada grupo de activo de información según la situación que presenta la organización.

Tabla N° 10 Evaluación de ocurrencias de amenazas

Nº	GRUPOS DE ACTIVOS DE INFORMACION	AMENAZAS	POSIBILIDAD DE OCURRENCIA
1	**PROGRAMAS FUENTE**	Control de cambios.	4
		Daño intencionado por internos.	4
		Error de herramienta de programación	2
		Software malicioso y virus.	3
2	**DOCUMENTOS FÍSICOS**	Alteración y/o plagio	3
		Entrega incorrecta	4
		Falsificación	3
		Incendio, desastres naturales	2

3	**SERVIDORES**	Error en el mantenimiento de hardware	3
		Daño intencionado por externos	4
		Falla de servicio de red y otros servicios	2
		Falla de software aplicación o Software malicioso	4
		Incendio y/o desastres naturales	2
		Suplantación identidad	5
		Abuso de los recursos del sistema y repudio	4
4	**EQUIPOS**	Error de operador	3
		Error en el mantenimiento de hardware	3
		Suplantación identidad	5
		Abuso de los recursos del sistema y repudio	4
		Falla de equipo	2
5	**DATA ALMACENADA**	Falla de operador	3
		Falla en dispositivo de almacenamiento	2
		Backup no autorizado	5
6	**SOFTWARE**	Robo de licencias	5
		Software malicioso y virus	3
		Error de usuario	3
		Uso no autorizado.	5
		Error de Actualización	3

Fuente: Elaboración Propia

3.1.5. Identificación de vulnerabilidades

En esta etapa se listará un conjunto de vulnerabilidades que presenten los grupos de activos de información, estas vulnerabilidades pueden ser de los siguientes tipos:

- **Física**
- **Natural**

- **Hardware**
- **Software**
- **Red**
- **Factor Humano**

Tabla N° 11 Identificación de vulnerabilidades de los activos de información

Nº	GRUPOS DE ACTIVOS DE INFORMACION	VULNERABILIDADES
1	PROGRAMAS FUENTE	Política de control de cambios inexistentes
		Políticas de control de usuarios inexistentes
		Política de backups inexistentes
		Falta de antivirus licenciado
2	DOCUMENTOS FISICOS	Inadecuada ubicación
		Política de confidencialidad inexistente
		Política de integridad inexistente
		Falta de implementos de seguridad
3	SERVIDORES	Falta de manual de mantenimiento
		Falta de cortafuegos
		Falta de equipos de red de respaldo
		Antivirus inadecuado
		Inadecuada ubicación
		Políticas de control de usuarios inexistentes
		Configuración de perfiles deficiente
4	EQUIPOS	Falta de manual de usuario
		Falta políticas de mantenimiento
		Políticas de control de usuarios inexistentes
		Configuración de perfiles deficiente
		Falta de equipos de respaldo

5	DATA ALMACENADA	Falta de manual de usuario
		Falta de equipos de respaldo
		Políticas de backup inexistente
6	SOFTWARE	Falta control de activos
		Falta de licencias vigentes
		Falta de manual de usuario
		Configuración de perfiles deficiente
		Política de actualizaciones inexistente

Fuente: Elaboración Propia

3.1.6. Posible explotación de Vulnerabilidades

Por cada amenaza identificada se ha identificado sus vulnerabilidades, es importante recalcar, que una vulnerabilidad no causa daño, es simplemente una condición o conjunto de condiciones que pueden hacer que una amenaza afecte a un activo de información.

Una vez identificadas las distintas vulnerabilidades por cada amenaza, se define el grado en que la amenaza puede explotar cada vulnerabilidad.

Tabla N° 12 Tabla de valoración de la vulnerabilidad

VALOR		**CRITERIO**
5	MUY ALTO	Definitivamente va a ocurrir, es cuestión de tiempo
4	ALTO	Muy probable
3	MEDIANO	Medianamente probable
2	BAJO	Probable
1	MUY BAJO	Poco Probable

Fuente: Elaboración Propia

Tabla N° 13 Evaluación de posibilidad de explotación de vulnerabilidades

Nº	GRUPOS DE ACTIVOS DE INFORMACION	VULNERABILIDADES	POSIBILIDAD EXPLOTACIÓN
1	PROGRAMAS FUENTE	Política de control de cambios inexistentes	4
		Políticas de control de usuarios inexistentes	3
		Política de backup inexistentes	4
		Falta de antivirus licenciado	4
2	DOCUMENTOS FISICOS	Inadecuada ubicación	5
		Política de confidencialidad inexistente	4
		Política de integridad inexistente	5
		Falta de implementos de seguridad	1
	SERVIDORES	Falta de manual de mantenimiento	3
		Falta de cortafuegos	3
		Falta de equipos de red de respaldo	3
		Antivirus inadecuado	4
		Inadecuada ubicación	2
		Políticas de control de usuarios inexistentes	4
		Configuración de perfiles deficiente	4
4	EQUIPOS	Falta de manual de usuario	3
		Falta políticas de mantenimiento	3
		Políticas de control de usuarios inexistentes	4
		Configuración de perfiles deficiente	4
		Falta de equipos de respaldo	4
5	DATA ALMACENADA	Falta de manual de usuario	3
		Falta de equipos de respaldo	4
		Políticas de backup inexistente	5
6	SOFTWARE	Falta control de activos	3
		Falta de licencias vigentes	4
		Falta de manual de usuario	3

		Configuración de perfiles deficiente	4
		Política de actualizaciones inexistente	3

Fuente: Elaboración Propia

3.1.7. Estimado del Valor de los Activos en Riesgo

La siguiente tabla muestra la evaluación del riesgo, a fin de determinar el daño cualitativo que el riesgo pudiera causar a los activos de información

Tabla N° 14 Evaluación de los Activos en Riesgo

Nº	GRUPOS DE ACTIVOS DE INFORMACION	AMENAZAS	POSIBILIDAD DE OCURRENCIA	POSIBILIDAD EXPLOTACIÓN	V. ACTIVO DE INFORMACIÓN
1	PROGRAMAS FUENTE	Control de cambios.	4	4	5
		Daño intencionado por internos.	4	3	
		Error de herramienta de programación	2	4	
		Software malicioso y virus.	3	4	
2	DOCUMENTOS FISICOS	Alteración y/o plagio	3	5	4
		Entrega incorrecta	4	4	
		Falsificación	3	5	
		Incendio, desastres naturales	2	1	
3	SERVIDORES	Error en el mantenimiento de hardware	3	3	5
		Daño intencionado por externos	4	3	
		Falla de servicio de red y otros servicios	2	3	
		Falla de software de aplicación o Software malicioso	4	4	
		Incendio, desastres naturales	2	2	
		Suplantación identidad	5	4	
		Abuso de los recursos del sistema y repudio	4	4	

4	**EQUIPOS**	Error de operador	3	3	4
		Error en el mantenimiento de hardware	3	3	
		Suplantación identidad	5	4	
		Abuso de los recursos del sistema y repudio	4	4	
		Falla de equipo	2	4	
5	**DATA ALMACENADA**	Falla de operador	3	3	4
		Falla en dispositivo de almacenamiento	2	4	
		Backup no autorizado	5	5	
6	**SOFTWARE**	Robo de licencias	5	3	3
		Software malicioso y virus	3	4	
		Error de usuario	3	3	
		Uso no autorizado.	5	4	
		Error de Actualización	3	3	

Fuente: Elaboración Propia

3.1.8. Posibilidad de Ocurrencia del Riesgo

La posibilidad de ocurrencia del riesgo se obtiene analizando cada activo de información, con referencia a las amenazas que sufre y la posibilidad que ocurra, así como sus vulnerabilidades y la posibilidad que tiene de ser explotadas.

Tabla N° 15 Evaluación de la posibilidad de ocurrencia del riesgo

Nº	**GRUPOS DE ACTIVOS DE INFORMACION**	**AMENAZAS**	**VULNERABILIDADES**	**V. ACTIVO DE INFORMACIÓN**	**POSIBLE OCURRENCIA**
1	**PROGRAMAS FUENTE**	Control de cambios.	Política de control de cambios inexistentes	5	4
		Daño intencionado por internos.	Políticas de control de usuarios inexistentes		

		Error de herramienta de programación	Política de backups inexistentes		
		Software malicioso y virus.	Falta de antivirus licenciado		
2	**DOCUMENTOS FISICOS**	Alteración y/o plagio	Inadecuada ubicación	4	3
		Entrega incorrecta	Política de confidencialidad inexistente		
		Falsificación	Política de integridad inexistente		
		Incendio, desastres naturales	Falta de implementos de seguridad		
	SERVIDORES	Error en el mantenimiento de hardware	Falta de manual de mantenimiento	5	4
		Daño intencionado por externos	Falta de cortafuegos		
		Falla de servicio de red y otros servicios	Falta de equipos de red de respaldo		
		Falla de software de aplicación o Software malicioso	Antivirus inadecuado		
		Incendio, desastres naturales	Inadecuada ubicación		
		Suplantación identidad	Políticas de control de usuarios inexistentes		
		Abuso de los recursos del sistema y repudio	Configuración de perfiles deficiente		
4	**EQUIPOS**	Error de operador	Falta de manual de usuario	4	3
		Error en el mantenimiento de hardware	Falta políticas de mantenimiento		
		Suplantación identidad	Políticas de control de usuarios inexistentes		

		Abuso de los recursos del sistema y repudio	Configuración de perfiles deficiente		
		Falla de equipo	Falta de equipos de respaldo		
5	**DATA ALMACENADA**	Falla de operador	Falta de manual de usuario	4	2
		Falla en dispositivo de almacenamiento	Falta de equipos de respaldo		
		Backup no autorizado	Políticas de backup inexistente		
6	**SOFTWARE**	Robo de licencias	Falta control de activos	2	3
		Software malicioso y virus	Falta de licencias vigentes		
		Error de usuario	Falta de manual de usuario		
		Uso no autorizado.	Configuración de perfiles deficiente		
		Error de Actualización	Política de actualizaciones inexistente		

Fuente: Elaboración Propia

3.1.9. Valor del Riesgo de los Activos

El Impacto hace referencia a la magnitud de las consecuencias, que tiene para la organización. el hecho de que uno o varios activos de información hayan visto comprometido su confidencialidad, integridad o disponibilidad debido a que una o varias amenazas en las que se hayan explotado sus vulnerabilidades. Al estimar un determinado nivel de impacto es necesario considerar la criticidad de los activos de información afectados. La exposición al riesgo, también es evaluada desde un análisis cuantitativo y cualitativo del riesgo.

- **Análisis cuantitativo:** Las métricas asociadas con el impacto causado por la materialización de las amenazas se valoran en cifras concretas de forma objetiva. Un modelo cuantitativo habitual es aquel en el que las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto en función de la estimación del costo económico que suponen para la organización

- **Análisis cualitativo:** Las métricas asociadas con el impacto causado por la materialización de las amenazas se valoran en términos subjetivos (Impacto Muy Alto, Alto, Medio, Bajo o Muy Bajo). Las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto en función de multitud de factores (pérdidas económicas efectivas, pérdida de conocimiento, pérdida de competitividad, interrupción de negocio, pérdida de imagen, etc.).

Tabla N° 16 Valoración de la probabilidad de ocurrencia

	VALOR		CRITERIO
5	**MA**	PROBABLE	POSIBILIDAD DE INCIDENTES REPETITIVOS
4	**A**	POSIBLE	POSIBLIDAD DE INCIDENTES AISLADOS
3	**M**	POCO PROBABLE	POSIBILIDAD DE OCURRENCIA MUY MODERADA
2	**B**	RARO	NO ES PROBABLE QUE OCURRA
1	**MB**	IMPERCEPTIBLE	POSIBILIDAD DE OCURRENCIA MUY ESCASA

Fuente: Elaboración Propia

Tabla N° 17 Valoración del impacto

	VALOR		CRITERIO
5	**MA**	CATASTROFICO	Deficiencia detectada, implica cambios en los procedimientos para su corrección (reingeniería de procesos).
4	**A**	SIGNIFICATIVO	Deficiencia detectada, implica más de un procedimiento para su corrección
3	**M**	MODERADO	Deficienciadetectada,implicaun Procedimiento para su corrección.
2	**B**	MENOR	Riesgo controlado el cual revierte la mínima complicación posible para el sistema de información, el cual no requiere ninguna contingencia.
1	**MB**	INSIGNIFICANTE	Este punto se obtiene como producto de la revisión y verificación de las actividades, que resultado tienen luego de ser ejecutadas, si el resultado es satisfactorio o de pleno cumplimiento.

Fuente: Elaboración Propia

Tabla N° 18 Resultados de Valoración

Nº	ACTIVO DE INFORMACIÓN	PROBABILIDAD DE OCURRENCIA		IMPACTO	
1	**PC de escritorio**	3	M	4	A
2	**Laptops**	3	M	4	A
3	**Impresora-Escaner**	3	M	3	M
4	**Servidor**	4	A	5	MA
5	**Ticketeras**	3	M	3	M
6	**Tablets**	3	M	3	M
7	**Disco Duro externo**	3	M	3	M
8	**Teléfono**	3	M	3	M

9	**Programa fuente Quipu-Escritorio**	4	A	5	MA
10	**Programa fuente Quipu-Web**	4	A	5	MA
11	**Microsoft Office 2010**	3	M	2	B
12	**Antivirus Eset Smart Security 9**	3	M	2	B
13	**Microsoft Windows Seven**	3	M	2	B
14	**Microsoft SQL-SERVER 2014**	3	M	4	A
15	**Microsoft Windows Server 2012**	3	M	4	A
16	**Team Viewer 11**	3	M	1	MB
17	**Visual Studio 2012**	3	M	3	M
18	**Registros de caja**	3	M	4	A
19	**Registros de planilla**	3	M	4	A
20	**Documentos de compras**	3	M	4	A
21	**Documentos de ventas**	3	M	4	A
22	**Registros PDT**	3	M	4	A
23	**Cotizaciones**	3	M	3	M
24	**Contratos de Venta**	3	M	4	A
25	**Registros de RRHH**	3	M	4	A
26	**Registros de cobranza**	3	M	4	A
27	**Actas de Requerimientos**	3	M	3	M
28	**Historial de Modificaciones**	2	B	4	A
29	**Actas de Implementación**	3	M	3	M
30	**Backups**	2	B	4	A
31	**Historial de Soportes**	2	B	3	M
32	**Historial de Actualizaciones**	2	B	3	M

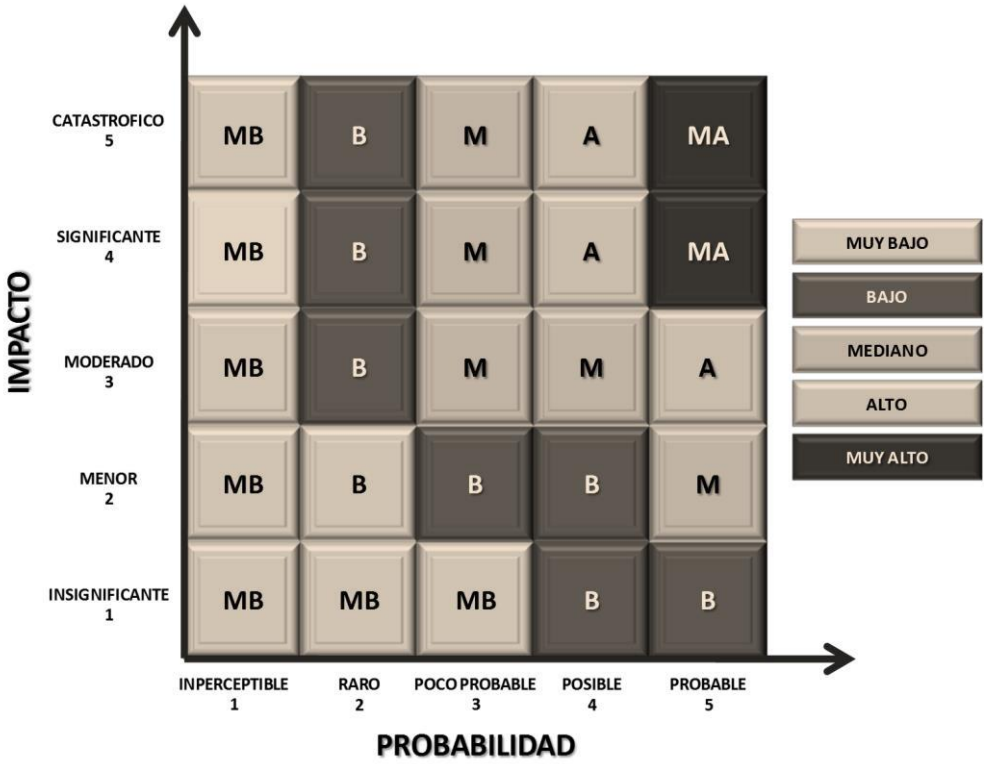
33	**Solicitudes de Cambio**	3	M	3	M
34	**Agenda Telefónica**	2	B	3	M
35	**Estado de soporte del cliente**	2	B	3	M

Fuente: Elaboración Propia

3.2. Análisis de resultados

Luego de las evaluaciones de las amenazas y vulnerabilidades relacionadas a los activos de información de la empresa, mediante la matriz de evaluación de riesgo se obtiene la siguiente tabla con la evaluación de los riesgos.

Figura N° 2 Matriz de Evaluación de Riesgo en Activos de Información



Fuente: Elaboración Propia

Tabla N° 19 Riesgo de los Activos de Información

Nº	ACTIVO DE INFORMACIÓN	RIESGO
1	PC de escritorio	M
2	Laptops	M
3	Impresora-Escaner	M
4	Servidor	A
5	Ticketeras	M
6	Tablets	M
7	Disco Duro externo	M
8	Teléfono	M
9	Programa fuente Quipu-Escritorio	A
10	Programa fuente Quipu-Web	A
11	Microsoft Office 2010	B
12	Antivirus Eset Smart Security 9	B
13	Microsoft Windows Seven	B
14	Microsoft SQL-SERVER 2014	M
15	Microsoft Windows Server 2012	M
16	Team Viewer 11	MB
17	Visual Studio 2012	M
18	Registros de caja	M
19	Registros de planilla	M
20	Documentos de compras	M
21	Documentos de ventas	M
22	Registros PDT	M
23	Cotizaciones	M

24	Contratos de Venta	M
25	Registros de RRHH	M
26	Registros de cobranza	M
27	Actas de Requerimientos	M
28	Historial de Modificaciones	B
29	Actas de Implementación	M
30	Backups	B
31	Historial de Soportes	B
32	Historial de Actualizaciones	B
33	Solicitudes de Cambio	M
34	Agenda Telefónica	B
35	Estado de soporte del cliente	B

Fuente: Elaboración Propia

3.3. Políticas de seguridad de información

Las políticas son parte fundamental de un esquema de seguridad de información eficiente, permiten aminorar los riesgos que ya se detectaron y actuar de manera rápida y acertada en caso de haber una emergencia.

Las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes:

- Aumento de personal
- Cambios en la infraestructura informática
- Rotación de personal
- Desarrollo de nuevos servicios
- Cambio o diversificación del área de negocios, etc.

3.3.1. Políticas Generales de Seguridad de la Información

Con el fin de optimizar el uso de la información, aplicaciones y sistemas de la empresa, se dan las siguientes políticas de observancia general y obligatoria:

1. Todo usuario con acceso a la información, aplicaciones o sistemas de Quipu Soluciones Empresariales S.A.C., tiene la obligación de adoptar todas las medidas de control establecidas en este plan de seguridad de información, así como los ordenamientos legales aplicables para la protección de la información o sistemas a los que tenga acceso, preservando su naturaleza confidencial y evitando su transferencia, modificación, destrucción o divulgación a entidades no autorizadas.
2. Toda información que la infraestructura de sistemas, aplicaciones, programas transmiten o almacenan son propiedad de la empresa, por lo que ningún usuario puede copiar, duplicar, transmitir o divulgar dicha información. La información, propiedad de Quipu Soluciones Empresariales S.A.C., está disponible únicamente para los usuarios que lo requieran dentro del estricto desempeño de sus funciones.
3. Los nombres de usuario y contraseña que son asignadas para el acceso a los sistemas, aplicaciones e información de Quipu Soluciones Empresariales S.A.C., son personales, intransferibles y estrictamente confidenciales. El titular de la misma es el responsable del uso que se haga de ellos, así como de la información y provecho que a través de ellos obtenga, para sí o para terceros y de los daños y perjuicios que se ocasionen sin menoscabo de las responsabilidades y sanciones de naturaleza organizacional, civil y penal que resulten.

4. El acceso a los sistemas de Quipu Soluciones Empresariales S.A.C. mediante el nombre de usuario y contraseña de un ajeno, se considerara como un uso no autorizado de información confidencial, sancionable.
5. Es considerada como una falta grave la ejecución de programas, aplicaciones u otros mecanismos que puedan dañar, alterar o impactar en el desempeño de los componentes de software de una computadora o propiedad de la empresa, o bien, con el fin de molestar a otros usuarios, infiltrarse en un sistema, y en general, intentar violar los estándares de seguridad definidos en Quipu Soluciones Empresariales S.A.C.
6. El usuario tiene la obligación de reportar inmediatamente al Área de seguridad de información cualquier violación a las políticas y estándares de seguridad de información de Quipu Soluciones Empresariales S.A.C.
7. La infraestructura de sistemas, aplicaciones y los recursos de información de Quipu Soluciones Empresariales S.A.C. deben ser utilizados únicamente para los fines de la empresa, no deberá ser usada para provecho personal, tales como entretenimientos, grupos de conversación, juegos recreativos, etc.
8. La infraestructura de sistemas, aplicaciones y los recursos de información de Quipu Soluciones Empresariales S.A.C. no deben ser usados para introducir o traficar con material obsceno, lujurioso o pornográfico, almacenar y/o solicitar mensajes o imágenes con orientación sexual, ni para provocar disgustos, ofensas y daño moral lo cual incluye hostigamiento a otros basado en raza, nacionalidad, sexo, orientación sexual, edad, religión, defecto físico o creencias políticas.

9. Es responsabilidad del usuario ejecutar las acciones necesarias para que los equipos, aplicaciones y sistemas asignados a su responsabilidad cumplan con los procedimientos de detección de virus definidos por el Área de Seguridad de Información.
10. No está permitida la instalación o ejecución de software no autorizado o sin licencia en cualquiera de los equipos que forman parte de la infraestructura de tecnologías de información de Quipu Soluciones Empresariales S.A.C.
11. La custodia de los equipos contenedores de información (servidores, computadoras personales, equipos móviles, dispositivos de almacenamiento secundario) estará a cargo del personal asignado a su uso, debiendo estos informar a su inmediato superior si alguno de estos equipos sufriera algún daño.
12. Los requerimientos mínimos para la compra de equipos tecnológicos referidos a la comunicación e información serán definidos en coordinación con el Área de Seguridad de Información.
13. Es responsabilidad de todo miembro de Quipu Soluciones Empresariales S.A.C., asegurarse que el personal a su cargo (contratado o no) conozca la presente normativa y cumpla con las disposiciones que requieren aprobación o supervisión previa al inicio de su trabajo.
14. La persona encargada de clasificar la información es la única que puede degradar su grado de confidencialidad.

3.3.2. Políticas Específicas de Seguridad de la Información

El personal de la empresa deberá seguir las políticas y estándares de seguridad de la información, a fin de proteger y controlar este activo; las siguientes

políticas son aplicables a todo el personal de Quipu Soluciones Empresariales S.A.C.

1. Las aplicaciones, sistemas e información de Quipu Soluciones Empresariales S.A.C. solamente serán utilizadas para fines laborales aprobados por los responsables del área.

1.1. La información de esta empresa (actas, memorándums, cotizaciones, contratos, registros contables, solicitudes, correos, bases de datos, software), así como los accesos a los equipos deberán ser empleados exclusivamente para propósitos de la empresa. Por lo tanto estos activos están sujetos a revisión en cualquier comento.

2. Políticas para el control de accesos:

2.1. El personal debe estar explícitamente autorizados para usar los sistemas y espacios físicos de Quipu Soluciones Empresariales S.A.C. Este es un privilegio que solo será otorgado cuando sea necesario que un individuo realice una función específica de trabajo y se hayan documentado sus responsabilidades y su perfil de acceso.

2.2. Personas que no sean personal de la empresa no tendrán acceso a los espacios físicos, excepto bajo circunstancias particulares, y tendrán acceso estrictamente a la mínima información que requieran conocer y deberán ser controlados todo el tiempo, salvo indicaciones de los responsables de área.

3. Todo software utilizado en Quipu Soluciones Empresariales S.A.C. debe contar con licencia de uso:

3.1. Todo el software cargado en las computadoras de la empresa deben estar de acuerdo a los compromisos de licencias, las leyes de protección de reproducción y los acuerdos de compra.

4. Los equipos ajenos a la empresa deben ser autorizados por su responsable de área para su uso dentro de las instalaciones de Quipu Soluciones Empresariales S.A.C.

4.1. Los miembros de la empresa pueden utilizar sus propios computadores, dispositivos periféricos, o software en las instalaciones siempre y cuando cuenten con la autorización de su responsable de área correspondiente.

4.2. Los dispositivos de almacenamiento (memorias USB, discos externos, etc.) deberán ser revisados por el Área de Soporte, a fin de garantizar su limpieza de posible software malicioso y virus, antes de su empleo en las instalaciones de la empresa.

4.3. Las computadoras portátiles, deberán ser revisadas en el Área de Soporte por el mismo motivo señalado en el punto anterior

4.4. El incumplimiento de alguna de estas políticas será tomado como una violación del protocolo de seguridad y será motivo de sanción.

5. Cada puesto que se desempeñe dentro de la empresa debe estar completamente descrito y el personal que los desarrolla debe conocer las responsabilidades propias de su puesto.

5.1. Cada alto cargo, debe conocer las responsabilidades del personal que tiene bajo su supervisión, así también las funciones de cada empleado que desarrolla una función específica dentro de la

organización, se debe contar con una descripción formal del puesto y las responsabilidades asociadas (MOF).

6. Políticas de seguridad de la información para la promoción, vacaciones, rotación y/o cese del personal.

6.1. Los estándares relacionados al personal, deben ser aplicados para asegurar que estos sean seleccionados adecuadamente antes de ser reclutados a la organización; a fin de que puedan ser fácilmente identificados mientras formen parte de Quipu Soluciones Empresariales S.A.C y que el acceso sea reevaluado o revocado temporal o indefinidamente cuando un colaborador de la empresa es promocionado, goce de vacaciones, de licencia, sea despedido o transferido, esta política se aplica a todo el personal de la empresa(Gerente, responsable de área, etc.)

7. Manejo adecuado de las pistas de auditoría.

7.1. Área de Seguridad de Información guarda un log de todas las operaciones que se realizan y registran, esto sirve como base para evaluar la seguridad del sistema y el acatamiento de las políticas; asimismo, proporciona pistas que permitan realizar un seguimiento a las actividades del sistema, en caso de una auditoria.

8. Los registros de inventario deben mantenerse actualizados indicando su responsable y ubicación.

9. Las copias de seguridad (backups) solo serán manipuladas por el personal de Desarrollo, esto incluye desde la creación del archivo de respaldo hasta la restauración del mismo. Esta información debe ser almacenada en 2 dispositivos distintos con el fin de contar con más de un respaldo.

10. Políticas sobre las auditorias

10.1. Los jefes deben asegurarse que las responsabilidades de seguridad sean cumplidas y las funciones relacionadas se ejecuten apropiadamente.

10.2. Es responsabilidad del personal encargado de la administración de la seguridad verificar el cumplimiento de las políticas de seguridad.

3.4. Selección de controles para mitigar los riesgos

Los controles asegurarán que los riesgos se reduzcan a un nivel aceptable, tomando en cuenta:

- Requerimientos y restricciones de legislación nacional e internacional y regulaciones.
- Objetivos de la organización.
- Exigencias operacionales y restricciones.
- El costo de implementación y operación en relación con los riesgos siendo reducidos y restando proporcionalmente a la organización requerimientos y restricciones.

Los controles a implementar:

3.4.1. Seguridad Lógica

Objetivo: Controlar adecuadamente los accesos a la información mediante la aplicación de mecanismos de seguridad establecidos para evitar la modificación, destrucción inconsistencia de los archivos y datos, especificando cuando estos se implementan a nivel de un sistema operativo.

Los procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios se mencionan a continuación:

1. Los usuarios del sistema informático tienen un firme compromiso de mantener en secreto sus contraseñas personales y las compartidas por un grupo al cual pertenece, este compromiso está contemplado en los términos y condiciones del contrato o resolución. **Responsable: Gerente General.**
2. Cada usuario pertenecerá a un grupo de trabajo definido y poseerá un determinado perfil, el que permitirá accesos a los mismos recursos y servicios informáticos, de acuerdo a las funciones del área o unidad a la que pertenecen y de acuerdo al rol correspondiente a su cargo. Los accesos personalizados deberán contar con la autorización y aprobación del Jefe Inmediato. Responsable: **Jefe del área de Seguridad de Información.**
3. Todo acceso a la red y al sistema, deberá pedir el nombre de usuario y la contraseña. **Responsable: Jefe del área de Seguridad de Información.**
4. El número máximo de intentos de acceso al sistema informático, será de 3 veces, luego de lo cual el sistema bloqueará automáticamente la cuenta. **Responsable: Jefe del área de Seguridad de Información.**
5. Cada usuario de la entidad tendrá una sola clave de acceso, válida para el ingreso al sistema informático. **Responsable: Jefe del área de Seguridad de Información.**
6. El usuario y contraseña asignada al trabajador no permitirá inicios de sesión simultáneos y registrará información sobre las sesiones activas. **Responsable: Jefe del área de Seguridad de Información.**
7. Los usuarios tendrán acceso a Internet limitado solo a las páginas definidas por las políticas de la empresa, el acceso a otras páginas se trataran mediante solicitud hacia la gerencia. **Responsable: Jefe del área de Seguridad de Información.**

3.4.2. Seguridad Personal

Objetivo: Asegurar que todo el personal de la empresa entienda y acepte sus responsabilidades en cuanto a seguridad de la información.

A continuación se muestra la definición de roles y responsabilidades establecidos sobre la seguridad de información.

1. La seguridad es responsabilidad de todo el personal de Quipu Soluciones Empresariales S.A.C, por ende, todos aquellos con acceso a las instalaciones e información de la institución y deben acatar los estándares documentados en la política de seguridad de información e incluirla como una de sus responsabilidades principales. **Responsables: Jefes de área.**
2. Todos los dispositivos personales de información (computadoras de propiedad de los colaboradores) que interactúen con los sistemas de Quipu Soluciones Empresariales S.A.C., deben estar autorizados y registrados por el Área de Seguridad de Información. **Responsable: Jefe del área de Seguridad de Información.**
3. Cuando se contrate al personal, se debe de entregar la política de seguridad así como las normas y procedimientos para el uso de las aplicaciones y los sistemas de información de la empresa. Asimismo, se debe entregar un resumen escrito de las medidas básicas de seguridad de la información, una copia firmada de la política de seguridad de información debe de ser guardada en el archivo del empleado. **Responsable: Gerente General.**

Para la verificación de antecedentes.

4. Todo personal que labora en Quipu Soluciones Empresariales S.A.C deberá comunicar obligatoriamente a la Gerencia General los cambios ocurridos

en la información proporcionada inicialmente, tales como domicilio, estado civil, estudios entre otros. **Responsable: Gerente General**.

5. Todo participante en el proceso de selección se someterá a la revisión de su documentación original. **Responsable: Gerente General.**

Para la concientización y entrenamiento.

6. Los usuarios de los sistemas de información de Quipu Soluciones Empresariales S.A.C deberán de ser capacitados anualmente sobre la importancia de la seguridad de la información. Un resumen escrito de la información básica debe de ser entregada nuevamente a cada empleado y una copia firmada debe de ser guardada en sus archivos. **Responsables: Jefes de área.**
7. Es responsabilidad de los tutores y/o entrenadores proveer de material escrito al personal en el proceso de capacitación, los materiales pueden ser manuales, guías, separatas, entre otros. Responsables: **Responsables: Jefes de área.**

3.4.3. Seguridad Física y Ambiental

Objetivo: Evitar accesos no autorizados, daños e interferencias contra los ambientes y la información de la organización.

Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.

1. Implementar un sistema de vigilancia con cámaras de seguridad en lugares estratégicos, a fin de mantener un mejor control del movimiento de las personal dentro de la empresa. **Responsable: Jefe del área de Seguridad de Información.**

Controles para prevenir pérdidas, daños o robos de los activos. Esto incluye la protección de los equipos frente a amenazas físicas y ambientales.

2. Cuando el personal se aleje de su estación de trabajo momentáneamente, deberá asegurarse de activar el “protector de pantalla” protegido con una contraseña personal. **Responsable: Jefes de área.**
3. Bajo ningún motivo, ninguna persona deberá retirar un equipo o componente propiedad de la empresa sin una guía de salida previamente autorizada por la dependencia en cuestión. **Responsable: Jefes de área.**
4. Apagar los equipos de cómputo cuando se dejen de usar por un prolongado tiempo, en especial cuando se disponga de feriados largos.

   Responsable: Jefes de área.
5. Los equipos deben marcarse para su identificación y control de inventario.

   Responsable: Jefe del área de Seguridad de Información.
6. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente. **Responsable: Jefes de área.**

3.4.4. Inventario de los activos y clasificación de la información

Objetivo: Asegurar que la información reciba un nivel de protección adecuado.

1. Todo documento o contenedor de información debe ser etiquetado como “Restringido”, “Confidencial”, de “Uso interno” o de “Acceso General”, dependiendo de la clasificación asignada. **Responsable: Jefes de área**
2. Todo documento que presente información clasificada como “Confidencial” o “Restringida”, debe ser etiquetado en la parte superior e inferior de cada página con la clasificación correspondiente. **Responsable: Jefes de área.**

3. Todo documento clasificado como “Confidencial” o “Restringido” debe contar con una carátula en la cual se muestre la clasificación de la información que contiene. **Responsable: Jefes de área**
4. El ambiente donde se almacena la información clasificada como “Restringida”, debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal formalmente autorizado. **Responsable: Jefe del área de Seguridad de Información.**
5. A través de un responsable designado deberá mantener actualizada la relación de productos de software o aplicaciones desarrolladas o adquiridos por la empresa. **Responsable: Jefe del área de Seguridad de Información.**
6. No tirar documentos confidenciales a las papeleras. Destruir dichos documentos con un picador de papel o de manera tal que se impida su reconstrucción. **Responsable: Jefes de área.**
7. No dejar documentos confidenciales sobre el escritorio, durante las horas de ausencia del usuario responsable. **Responsable: Jefes de área.**
8. Para los documentos impresos, para su valida distribución deberá contar con la firma y sello del responsable del Área. **Responsable: Jefes de área.**
9. Al retirarse de las oficinas, dejar con llave los escritorios y estantes que contienen documentos confidenciales. Responsable: **Jefes de área.**
10. A la hora de entrada, verificar que los escritorios y estantes permanezcan con llave y que no hayan sido manipulados, de no ser así se deberá informar a la jefatura de seguridad con copia a la alta dirección de la empresa. **Responsable: Jefes de área.**

3.4.5. Administración de las comunicaciones

Objetivo: Asegurar un adecuado nivel de servicio a los clientes, los requerimientos de seguridad deben ser desarrollados e implementados para mantener el control sobre las comunicaciones y las operaciones.

1. El correo electrónico institucional, es una herramienta de comunicación e intercambio de información oficial entre personas, no es una herramienta de difusión indiscriminada de información. Responsables: **Responsable: Jefes de área.**
2. Nunca deben ejecutarse ni descargarse programas o archivos adjuntos (en correos electrónicos) cuya procedencia y fiabilidad no ofrezcan todas las garantías. **Responsable: Jefes de área.**
3. Todos los intentos de conexión (logon), desconexión (logoff), cambios de contraseña, fallas en los cambios de contraseña, reinstalación de contraseñas, registro de usuarios, actualización de los registros de usuarios, y supresión de usuarios, serán registrados. **Responsable: Jefe del área de Seguridad de Información.**

3.4.6. Adquisición y mantenimiento de sistemas informáticos Objetivo:

Asegurar que la seguridad esté imbuida dentro de los sistemas de información.

1. Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida. **Responsable: Jefes de área.**
2. La información crítica debe ser encriptada cuando se vaya a respaldar o guardar. **Responsable: Jefes de área de Desarrollo y Soporte.**

3. Los sistemas aplicativos deben ser probados en forma exhaustiva, antes de ser liberados a producción, en ambientes controlados de pruebas (Test y Calidad). El proceso de pruebas debe llevar un control estricto en los puntos que debe cumplir la nueva aplicación, y realizar un reporte a desarrollo del resultado de la prueba, se dará reporte con carácter de obligatorio al Jefe del área de Seguridad de Información. **Responsable: Jefes de área de Desarrollo.**
4. Quipu Soluciones Empresariales S.A.C. deberá implantar mecanismos que permitan llevar controles de las modificaciones y accesos a los programas producto y programas fuente con el objeto de mantener integridad sobre los ambientes de prueba y producción. **Responsable: Jefes de área de Desarrollo.**
5. La instalación de software solo será posible con la autorización y previa verificación de licencia por el Área de Seguridad de Información. **Responsable: Jefe de área de Seguridad de Información y Área de Soporte.**

3.4.7. Procedimientos de respaldo

Objetivo: Establecer un conjunto de controles que permitan gestionar adecuadamente el respaldo de la información producida en Quipu Soluciones Empresariales S.A.C.

1. Se llevará una bitácora actualizada de la realización de backups de bases de datos detallando la fecha de backup, la hora, el tamaño, el responsable de la operación, el contenido, la fecha de registro, y observaciones en el caso que

estas existieran. **Responsable: Jefe del área de Seguridad de Información y Jefe de área de Desarrollo.**

2. El Jefe de área de Desarrollo, realizará comprobaciones puntuales para asegurar que las copias de seguridad se realicen correctamente, considerando lo siguiente:
    - Organizar pruebas periódicas de hardware y software para la recuperación de la información.
    - Establecer y ejecutar procedimientos para la restauración de la información de la empresa

    Responsable: Jefe del área de Seguridad de Información y Jefe de área de Desarrollo.

3.4.8. Gestión de incidentes de seguridad de la información.

Objetivo: Asegurar que los eventos y debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva a tiempo.

Procedimientos formales para el reporte de los eventos de seguridad de información y las vulnerabilidades asociadas con los sistemas de información.

1. Luego de reportado el incidente de seguridad, éste debe ser investigado por el personal técnico del Área de Seguridad de Información en forma rápida y confidencial. Se debe identificar la severidad del incidente para la toma de medidas correctivas.
2. Se debe mantener una documentación de todos los incidentes de seguridad ocurridos en Quipu Soluciones Empresariales S.A.C.

3. Se debe mantener intacta la evidencia que prueba la ocurrencia de una violación de seguridad producida tanto por entes internos o externos, para su posterior utilización en procesos legales en caso de ser necesario.

   Responsable: Jefes de área.

Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

4. Luego de la investigación realizada por el personal designado para tal efecto, se elaborará un informe al Jefe del Área de Seguridad de Información indicando la severidad del incidente, para que este tome las medidas del caso e informe a la alta dirección de la organización en caso el incidente sea demasiado grave.
5. Jefe del Área de Seguridad de Información reportará a la alta dirección las medidas de solución al incidente de seguridad ocurrido.

3.4.9. Cumplimiento Normativo y de Auditoria.

Objetivo: Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad.

1. Un proceso documentado asegurara que las violaciones a las políticas de seguridad y procedimientos no se den sin conllevar a un tipo de sanción por parte del usuario que comete dicha falta. **Responsable: Jefes de área.**
2. Los propietarios de la información deben participar en el proceso de auditoría, un proceso de revisión de la auditoria debe asegurar que: existan los informes de la misma, las alertas sean revisadas, se haya completado el

análisis de auditoría, se obtenga la conclusión y sean tomadas las acciones establecidas durante el proceso. **Responsable: Jefes de área.**

3. Todos los registros de auditoría de sistemas, serán consolidados en una base de datos o archivo que facilite la generación de informes.

   Responsable: Jefe del área de Seguridad de Información.

Las siguientes tablas muestran la relación de las políticas propuestas con sus respectivos controles.

Tabla N° 20 Controles de Política General 1

N°	Políticas Generales de Seguridad de la Información	Responsable
1	Todo usuario con acceso a la información, aplicaciones o sistemas de Quipu Soluciones Empresariales S.A.C., tiene la obligación de adoptar todas las medidas de control establecidas en este plan de seguridad de información.	**Gerente General.**

Dominio	N°	Control
Seguridad Lógica	**1**	Los usuarios del sistema informático tienen un firme compromiso de mantener en secreto sus contraseñas personales y las compartidas por un grupo al cual pertenece, este compromiso está contemplado en los términos y condiciones del contrato o resolución

Fuente: Elaboración Propia

Tabla N° 21Controles de Política General 2

N°	Políticas Generales de Seguridad de la Información	Responsable
2	La información, propiedad de Quipu Soluciones Empresariales S.A.C., está disponible únicamente para los usuarios que lo requieran dentro del estricto desempeño de sus funciones	**Jefe del área de Seguridad de Información**

Dominio	N°	Control
Seguridad Lógica	**2**	Cada usuario pertenecerá a un grupo de trabajo definido y poseerá un determinado perfil, el que permitirá accesos a los mismos recursos y servicios
	3	Todo acceso a la red y al sistema, deberá pedir el nombre de usuario y la contraseña
	4	El número máximo de intentos de acceso al sistema informático, será de 3 veces, luego de lo cual el sistema bloqueará automáticamente la cuenta

Fuente: Elaboración Propia

Tabla N° 22Controles de Política General 3

N°	Políticas Generales de Seguridad de la Información	Responsable
3	Los nombres de usuario y contraseña que son asignadas para el acceso a los sistemas, aplicaciones e información de Quipu Soluciones Empresariales S.A.C., son personales, intransferibles y estrictamente confidenciales	**Jefe del área de Seguridad de Información**

Dominio	N°	Control
Seguridad Lógica	**5**	Cada usuario de la entidad tendrá una sola clave de acceso, válida para el ingreso al sistema informático.

Fuente: Elaboración Propia

Tabla N° 23Controles de Política General 4

N°	Políticas Generales de Seguridad de la Información	Responsable
4	El acceso a los sistemas de Quipu Soluciones Empresariales S.A.C. mediante el nombre de usuario y contraseña de un ajeno, se considerara como un uso no autorizado de información confidencial, sancionable.	**Jefe del área de Seguridad de Información**

Dominio	N°	Control
Seguridad Lógica	**6**	El usuario y contraseña asignada al trabajador no permitirá inicios de sesión simultáneos y registrará información sobre las sesiones activas.

Fuente: Elaboración Propia

Tabla N° 24 Controles de Política General 5

N°	Políticas Generales de Seguridad de la Información	Responsable
5	Es considerada como una falta grave la ejecución de programas, aplicaciones u otros mecanismos que puedan dañar, alterar o impactar en el desempeño de los componentes de software de una computadora o propiedad de la empresa.	**Jefe del área de Seguridad de Información**
		Jefe del área de Seguridad de Información

Dominio	N°	Control
Seguridad Lógica	**7**	Los usuarios tendrán acceso a Internet limitado solo a las páginas definidas por las políticas de la empresa
Seguridad Personal	**2**	Todos los dispositivos personales de información que interactúen con los sistemas de Quipu Soluciones Empresariales S.A.C., deben estar autorizados y registrados por el Área de Seguridad de Información

Fuente: Elaboración Propia

Tabla N° 25 Controles de Política General 6

N°	Políticas Generales de Seguridad de la Información	Responsable
6	El usuario tiene la obligación de reportar inmediatamente al Área de seguridad de información cualquier violación a las políticas y estándares de seguridad de información de Quipu Soluciones Empresariales S.A.C.	**Jefe del área de Seguridad de Información**
		Jefes de área
		Jefes de área

Dominio	N°	Control
Seguridad Física y Ambiental	**1**	Implementar un sistema de vigilancia con cámaras de seguridad en lugares estratégicos, a fin de mantener un mejor control del movimiento de las personal dentro de la empresa.
Gestión de incidentes de seguridad de la información	**3**	Se debe mantener intacta la evidencia que prueba la ocurrencia de una violación de seguridad producida tanto por entes internos o externos,
Cumplimiento Normativo y de Auditoria	**1**	Un proceso documentado asegurara que las violaciones a las políticas de seguridad y procedimientos no se den sin conllevar a un tipo de sanción por parte del usuario que comete dicha falta

Fuente: Elaboración Propia

Tabla N° 26 Controles de Política General 7

N°	Políticas Generales de Seguridad de la Información	Responsable
7	La infraestructura de sistemas, aplicaciones y los recursos de información de Quipu Soluciones Empresariales S.A.C. deben ser utilizados únicamente para los fines de la empresa.	**Jefe del área de Seguridad de Información**

Dominio	N°	Control
Seguridad Lógica	**7**	Los usuarios tendrán acceso a Internet limitado solo a las páginas definidas por las políticas de la empresa

Fuente: Elaboración Propia

Tabla N° 27 Controles de Política General 8

N°	Políticas Generales de Seguridad de la Informació n	Responsable
8	La infraestructura de sistemas, aplicaciones y los recursos de información de Quipu Soluciones Empresariales S.A.C. no deben ser usados para introducir o traficar con material obsceno, etc.	**Jefe del área de Seguridad de Información**

Dominio	N°	Control
Seguridad Lógica	**7**	Los usuarios tendrán acceso a Internet limitado solo a las páginas definidas por las políticas de la empresa

Fuente: Elaboración Propia

Tabla N° 28 Controles de Política General 9

N°	Políticas Generales de Seguridad de la Información	Responsable
9	Es responsabilidad del usuario ejecutar las acciones necesarias para que los equipos, aplicaciones y sistemas asignados a su responsabilidad cumplan con los procedimientos de detección de virus definidos por el Área de Seguridad de Información.	**Jefes de Área**
		Jefes de Área

Dominio	N°	Control
Seguridad Personal	**6**	Los usuarios de los sistemas de información de Quipu Soluciones Empresariales S.A.C deberán de ser capacitados anualmente sobre la importancia de la seguridad de la información
Seguridad Personal	**7**	Es responsabilidad de los tutores y/o entrenadores proveer de material escrito al personal en el proceso de capacitación, los materiales pueden ser manuales, guías, separatas, entre otros

Fuente: Elaboración Propia

Tabla N° 29 Controles de Política General 10

N°	Políticas Generales de Seguridad de la Información	Responsable
10	No está permitida la instalación o ejecución de software no autorizado o sin licencia en cualquiera de los equipos que forman parte de la infraestructura de tecnologías de información de Quipu Soluciones Empresariales S.A.C.	**Jefes de área de Desarrollo**

Dominio	N°	Control
Adquisición y mantenimiento de sistemas informáticos	**5**	La instalación de software solo será posible con la autorización y previa verificación de licencia por el Área de Seguridad de Información

Fuente: Elaboración Propia

Tabla N° 30 Controles de Política General 11

N°	Políticas Generales de Seguridad de la Informació n	Responsable
11	La custodia de los equipos contenedores de información estará a cargo del personal asignado a su uso, debiendo estos informar a su inmediato superior si alguno de estos equipos sufriera algún daño.	**Jefes de Área**

Dominio	N°	Control
Seguridad Física y Ambiental	**3**	Bajo ningún motivo, ninguna persona deberá retirar un equipo o componente propiedad de la empresa sin una guía de salida previamente autorizada por la dependencia en cuestión.

Fuente: Elaboración Propia

Tabla N° 31 Controles de Política General 12

N°	Políticas Generales de Seguridad de la Información		Responsable
12	Los requerimientos mínimos para la compra de equipos tecnológicos referidos a la comunicación e información serán definidos en coordinación con el Área de Seguridad de Información.		**Jefe del área de Seguridad de Información**
			Jefes de Área
Dominio	**N°**	**Control**	
Inventario de los activos y clasificación de la información	**5**	A través de un responsable designado deberá mantener actualizada la relación de productos de software o aplicaciones desarrolladas o adquiridos por la empresa.	
Adquisición y mantenimiento de sistemas informáticos	**1**	Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida	

Fuente: Elaboración Propia

Tabla N° 32 Controles de Política General 13

N°	Políticas Generales de Seguridad de la Información		Responsable
13	Es responsabilidad de todo miembro de Quipu Soluciones Empresariales S.A.C., asegurarse que el personal a su cargo conozca la presente normativa y cumpla con las disposiciones que requieren aprobación o supervisión previa al inicio de su trabajo.		**Jefes de área**
Dominio	**N°**	**Control**	
Seguridad Personal	**1**	Aquellos con acceso a las instalaciones e información de la institución y deben acatar los estándares documentados en la política de seguridad de información e incluirla como una de sus responsabilidades principales.	

Fuente: Elaboración Propia

Tabla N° 33 Controles de Política General 14

N°	Políticas Generales de Seguridad de la Información		Responsable
14	La persona encargada de clasificar la información es la única que puede degradar su grado de confidencialidad.		**Jefes de área**
			Jefes de área
			Jefes de área
Dominio	**N°**	**Control**	
Inventario de los activos y clasificación de la información	**1**	Todo documento o contenedor de información debe ser etiquetado como “Restringido”, “Confidencial”, de “Uso interno” o de “Acceso General”, dependiendo de la clasificación asignada	

Inventario de los activos y clasificación de la información	**2**	Todo documento que presente información clasificada como “Confidencial” o “Restringida”, debe ser etiquetado en la parte superior e inferior de cada página con la clasificación correspondiente.
Inventario de los activos y clasificación de la información	**3**	Todo documento clasificado como “Confidencial” o “Restringido” debe contar con una carátula en la cual se muestre la clasificación de la información que contiene.

Fuente: Elaboración Propia

Tabla N° 34 Controles de Política Específica 1

N°	**Políticas Específicas de Seguridad de la Información**	**Responsable**
1.1	La información de esta empresa, así como los accesos a los equipos deberán ser empleados exclusivamente para propósitos de la empresa	**Jefes de área**
		Jefes de área
		Jefes de área
		Jefes de área

Dominio	**N°**	**Control**
Inventario de los activos y clasificación de la información	**6**	No tirar documentos confidenciales a las papeleras. Destruir dichos documentos con un picador de papel o de manera tal que se impida su reconstrucción
Inventario de los activos y clasificación de la información	**7**	No dejar documentos confidenciales sobre el escritorio, durante las horas de ausencia del usuario responsable
Inventario de los activos y clasificación de la información	**8**	Para los documentos impresos, para su valida distribución deberá contar con la firma y sello del responsable del Área.
Administración de las comunicaciones	**1**	El correo electrónico institucional, es una herramienta de comunicación e intercambio de información oficial entre personas, no es una herramienta de difusión indiscriminada de información

Fuente: Elaboración Propia

Tabla N° 35 Controles de Política Específica 2.1

N°	**Políticas Específicas de Seguridad de la Información**	**Responsable**
2.1	El personal debe estar explícitamente autorizados para usar los sistemas y espacios físicos de Quipu Soluciones Empresariales S.A.C.	**Jefe del área de Seguridad de Información**
		Jefes de área
		Jefes de área

Dominio	**N°**	**Control**
Inventario de los activos y clasificación de la información	**4**	El ambiente donde se almacena la información clasificada como “Restringida”, debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal formalmente autorizado.

Inventario de los activos y clasificación de la información	**9**	Al retirarse de las oficinas, dejar con llave los escritorios y estantes que contienen documentos confidenciales
Inventario de los activos y clasificación de la información	**10**	A la hora de entrada, verificar que los escritorios y estantes permanezcan con llave y que no hayan sido manipulados

Fuente: Elaboración Propia

Tabla N° 36 Controles de Política Específica 2.2

N°	**Políticas Específicas de Seguridad de la Información**		**Responsable**
2.2	Personas que no sean personal de la empresa no tendrán acceso a los espacios físicos, excepto bajo circunstancias particulares		**Jefe del área de Seguridad de Información**
Dominio	**N°**	**Control**	
Inventario de los activos y clasificación de la información	**4**	El ambiente donde se almacena la información clasificada como "Restringida", debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal formalmente autorizado.	

Fuente: Elaboración Propia

Tabla N° 37 Controles de Política Específica 3.1

N°	**Políticas Específicas de Seguridad de la Información**		**Responsable**
3.1	Todo el software cargado en las computadoras de la empresa deben estar de acuerdo a los compromisos de licencias, las leyes de protección de reproducción y los acuerdos de compra.		**Jefes de área**
			Jefes de área de Desarrollo
			Jefes de área de Desarrollo
Dominio	**N°**	**Control**	
Administración de las comunicaciones	**2**	Nunca deben ejecutarse ni descargarse programas o archivos adjuntos (en correos electrónicos) cuya procedencia y fiabilidad no ofrezcan todas las garantías	
Adquisición y mantenimiento de sistemas informáticos	**3**	El proceso de pruebas debe llevar un control estricto en los puntos que debe cumplir la nueva aplicación, y realizar un reporte a desarrollo del resultado de la prueba	
Adquisición y mantenimiento de sistemas informáticos	**4**	Implantar mecanismos que permitan llevar controles de las modificaciones y accesos a los programas producto y programas fuente	

Fuente: Elaboración Propia

Tabla N° 38 Controles de Política Específica 4.1

N°	Políticas Específicas de Seguridad de la Información	Responsable
4.1	Los miembros de la empresa pueden utilizar sus propios computadores, dispositivos periféricos, o software en las instalaciones siempre y cuando cuenten con la autorización de su responsable de área correspondiente.	Jefes de área
		Jefes de área

Dominio	N°	Control
Seguridad Física y Ambiental	2	Cuando el personal se aleje de su estación de trabajo momentáneamente, deberá asegurarse de activar el "protector de pantalla" protegido con una contraseña personal
Seguridad Física y Ambiental	4	Apagar los equipos de cómputo cuando se dejen de usar por un prolongado tiempo, en especial cuando se disponga de feriados largos

Fuente: Elaboración Propia

Tabla N° 39 Controles de Política Específica 4.2-4.3

N°	Políticas Específicas de Seguridad de la Información	Responsable
4.2-4.3	Los dispositivos de almacenamiento (memorias USB, discos externos, etc.) deberán ser revisados por el Área de Soporte	Jefe del área de Seguridad de Información.
	Las computadoras portátiles, deberán ser revisadas en el Área de Soporte	Jefe del área de Seguridad de Información.

Dominio	N°	Control
Seguridad Personal	2	Todos los dispositivos personales de información (computadoras de propiedad de los colaboradores) que interactúen con los sistemas de Quipu Soluciones Empresariales S.A.C., deben estar autorizados y registrados por el Área de Seguridad de Información
Seguridad Personal	2	Todos los dispositivos personales de información (computadoras de propiedad de los colaboradores) que interactúen con los sistemas de Quipu Soluciones Empresariales S.A.C., deben estar autorizados y registrados por el Área de Seguridad de Información

Fuente: Elaboración Propia

Tabla N° 40 Controles de Política Específica 4.4

N°	Políticas Específicas de Seguridad de la Información	Responsable
4.4	El incumplimiento de alguna de estas políticas será tomado como una violación del protocolo de seguridad y será motivo de sanción.	**Jefes de área**

Dominio	N°	Control
Gestión de incidentes de seguridad de la información	**3**	Se debe mantener intacta la evidencia que prueba la ocurrencia de una violación de seguridad producida tanto por entes internos o externos,

Fuente: Elaboración Propia

Tabla N° 41 Controles de Política Específica 5.1

N°	Políticas Específicas de Seguridad de la Información	Responsable
5.1	Cada alto cargo, debe conocer las responsabilidades del personal que tiene bajo su supervisión, así también las funciones de cada empleado que desarrolla una función específica dentro de la organización.	**Jefes de área**

Dominio	N°	Control
Seguridad Personal	**1**	La seguridad es responsabilidad de todo el personal de Quipu Soluciones Empresariales S.A.C, por ende, todos aquellos con acceso a las instalaciones e información de la institución y debe acatar los estándares documentados en la política de seguridad de información e incluirla como una de sus responsabilidades principales.

Fuente: Elaboración Propia

Tabla N° 42 Controles de Política Específica 6

N°	Políticas Específicas de Seguridad de la Información	Responsable
6	Políticas de seguridad de la información para la promoción, vacaciones, rotación y/o cese del personal	**Gerente General**
		Gerente General
		Gerente General

Dominio	N°	Control
Seguridad Personal	**3**	Cuando se contrate al personal, se debe de entregar la política de seguridad así como las normas y procedimientos para el uso de las aplicaciones y los sistemas de información de la empresa
Seguridad Personal	**4**	Todo personal que labora en Quipu Soluciones Empresariales S.A.C deberá comunicar obligatoriamente a la Gerencia General los cambios ocurridos en la información proporcionada inicialmente

Seguridad Personal	**5**	Todo participante en el proceso de selección se someterá a la revisión de su documentación original

Fuente: Elaboración Propia

Tabla N° 43 Controles de Política Específica 7

N°	**Políticas Específicas de Seguridad de la Información**		**Responsable**
7	Área de Seguridad de Información guarda un log de todas las operaciones que se realizan y registran, esto sirve como base para evaluar la seguridad del sistema y el acatamiento de las políticas.		**Jefe del área de Seguridad de Información.**
Dominio	**N°**	**Control**	
Administración de las comunicaciones	**3**	Todos los intentos de conexión (logon), desconexión (logoff), cambios de contraseña, fallas en los cambios de contraseña, reinstalación de contraseñas, registro de usuarios, actualización de los registros de usuarios, y supresión de usuarios, serán registrados	

Fuente: Elaboración Propia

Tabla N° 44 Controles de Política Específica 8

N°	**Políticas Específicas de Seguridad de la Información**	**Responsable**
8	Los registros de inventario deben mantenerse actualizados indicando su responsable y ubicación	**Jefe del área de Seguridad de Información**
		Jefes de área

Dominio	**N°**	**Control**
Seguridad Física y Ambiental	**5**	Los equipos deben marcarse para su identificación y control de inventario
Seguridad Física y Ambiental	**6**	La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente

Fuente: Elaboración Propia

Tabla N° 45 Controles de Política Específica 9

N°	Políticas Específicas de Seguridad de la Información	Responsable
9	Las copias de seguridad (backups) solo serán manipuladas por el personal de Desarrollo, esto incluye desde la creación del archivo de respaldo hasta la restauración del mismo	**Jefes de área de Desarrollo y Soporte**
		Jefe del área de Seguridad de Información y Jefe de área de Desarrollo
		Jefe del área de Seguridad de Información y Jefe de área de Desarrollo

Dominio	N°	Control
Adquisición y mantenimiento de sistemas informáticos	**2**	La información crítica debe ser encriptada cuando se vaya a respaldar o guardar
Procedimientos de respaldo	**1**	Se llevará una bitácora actualizada de la realización de backups de bases de datos detallando la fecha de backup, la hora, el tamaño, el responsable de la operación, el contenido, la fecha de registro, y observaciones en el caso que estas existieran
Procedimientos de respaldo	**2**	El Jefe de área de Desarrollo, realizará comprobaciones puntuales para asegurar que las copias de seguridad se realicen correctamente

Fuente: Elaboración Propia

Tabla N° 46 Controles de Política Específica 10

N°	Políticas Específicas de Seguridad de la Información	Responsable
10	Los jefes deben asegurarse que las responsabilidades de seguridad sean cumplidas y las funciones relacionadas se ejecuten apropiadamente	**Jefes de área**
	Es responsabilidad del personal encargado de la administración de la seguridad verificar el cumplimiento de las políticas de seguridad	**Jefe del área de Seguridad de Información**

Dominio	N°	Control
Cumplimiento Normativo y de Auditoria	**2**	Los propietarios de la información deben participar en el proceso de auditoría
Cumplimiento Normativo y de Auditoria	**2**	Todos los registros de auditoría de sistemas, serán consolidados en una base de datos o archivo que facilite la generación de informes

Fuente: Elaboración Propia

3.5. Análisis Costo-Beneficio

Para la implementación de este plan para la seguridad de información es necesario establecer un Área de seguridad de información que pueda realizar el seguimiento y futuras modificaciones que requiera este proyecto, como la adquisición del hardware y software especificado en la siguiente tabla.

Tabla N° 47Analisis Costo-Beneficio

ANALISIS COSTO-BENEFICIO			
Detalle de costos	**Costos**	**Detalle de beneficios**	**Beneficios económicos**
Personal para implementación y seguimiento	**S/. 12,000.00**	**Renovación de licencia**	
Software y equipos		**1er mes**	**S/. 2,010.00**
Licencias Microsoft Office 2016	**S/. 1,980.00**	**2do mes**	**S/. 7,537.50**
Licencia Antivirus Eset Smart Security	**S/. 1,150.00**	**3er mes**	**S/. 7,537.50**
Instalación de cámaras de seguridad	**S/. 670.00**	**4to mes**	**S/. 7,537.50**
Licencia Team Viewer	**S/. 3,700.00**	**5to mes**	**S/. 7,537.50**
Otros			
Archivadores (2)	**S/. 600.00**		
Modificación de MOF	**S/. 200.00**		
Total	**S/. 20,300.00**	**Total**	**S/. 32,160.00**

Fuente: Elaboración Propia

Cabe resaltar que este análisis incluye la adquisición de licencias por un año, la compra de los archivadores y la implementación de cámaras de seguridad. Además de considerar el costo del personal para la implementación-seguimiento del plan y los ingresos que percibirá la empresa durante los 5 meses de implementación donde las mejoras serán percibidas a partir del segundo mes.

Conclusiones

Luego de analizar la situación de la empresa Quipu Soluciones Empresariales S.A.C. tenemos las siguientes conclusiones:

- Un plan para la seguridad de información basado en ISO 27001 es aplicable para toda empresa dedicada a este rubro, sin importar el tamaño de esta.
- Es esencial considerar el inventario de activos de información para análisis de riesgo existentes.
- Gracias a la identificación de riesgos se llegó a conocer el estado actual de los activos de información que posee la empresa.
- Las políticas y controles definidos permitieron la mejora de la seguridad de información en Quipu Soluciones Empresariales S.A.C.
- El apoyo de la gerencia fue un importante apoyo para el desarrollo del proyecto, ya que permitió obtener la información necesaria para el análisis del caso.
- Este plan para la seguridad de información permite a la empresa tener un mayor orden y control sobre sus activos de información.
- El plan permitirá captar las oportunidades de ingresos del área de soporte.

Recomendaciones

Las recomendaciones para Quipu Soluciones Empresariales S.A.C.

- Para complementar este proyecto se recomienda adquirir un sistema de gestión documentaria bajo los estándares de la norma ISO 27001, que permitirá una mejor gestión de los documentos generados en esta organización.
- Se recomienda implementar este plan de seguridad de información, porque la empresa tiene activos de información con valiosos recursos que están a disposición de personal no autorizado.
- Para la implementación de este plan de seguridad se recomienda aplicar el Ciclo de Deming que permite trabajar con los estándares de la norma ISO 27001.
- La empresa necesita adoptar una cultura organizacional a nivel de seguridad de la información, debido a que actualmente sus activos de información no cuenta con la adecuada protección.
- Luego de tomar medidas correctivas y preventivas, se debe realizar una nueva evaluación sobre los controles propuestos para una mejora.
- Se recomienda que los responsables de cada área promueva la práctica de estas políticas para una futura retroalimentación.
- Añadir al manual de funciones las políticas incluidas en este plan.

Bibliografía

1. García, L. (2013) Principales cambios de la nueva versión de la ISO 27001 En QualityTrends. Disponible en Http://qualitytrends.squalitas.com/index.php/item/186-principales-cambios-de-la-nueva-version-de-iso-27001.

2. Canales FH, De Alvarado EL, Pineda EB. Metodología de la investigación. Manual para el desarrollo de personal de salud. T ed. México: Limusa; 1994.

3. Morles, Víctor. (1994). Planeamiento y análisis de investigaciones. El dorado Ediciones. Caracas. Venezuela.

4. Córdova, N. (2012). *Plan de Seguridad Informática para una Entidad Financiera*. Tesis de titulación, Facultad de Economía, Universidad Nacional Mayor de San Marcos, Perú.

5. International Organization of Standardization and International Electrotechnical Commission. ISO 27001:2005. Tecnología de la información Técnicas de seguridad Sistemas de gestión de seguridad de la información Requerimientos (2005). Primera edición.

6. Project Management Institute. Guía de los fundamentos para la dirección de proyectos (Guía del PMBOK). (2013) Quinta edición.

7. Deming, E. (1989). Calidad, Productividad y Competitividad: la salida de la crisis. Madrid, España: Ediciones Díaz de Santos.

8. Briceño A. (2013) Deming y la prevención de riesgos laborales. En *Prevencionar.com.* Disponible en http://prevencionar.com/2013/05/13/deming-y-la-prevencion-de-riesgos-laborales.

9. Anzil F. (2010). Concepto de Control. En *ZonaEconomica*.

Consultado el 15 de noviembre de 2015.

Disponible en http://www.zonaeconomica.com/control.

10. ITM Platform (2015) ¿Qué es la gestión de riesgos? En *ITM Platform*. Consultado el 16 de noviembre de 2015.

Disponible en http://www.itmplatform.com/es/blog/la-gestion-riesgos.

11. Wikipedia (2015). Implementación. En *Wikipedia*.

Consultado el 15 de noviembre de 2015.

Disponible en https://es.wikipedia.org/wiki/Implementaci%C3%B3n.

12. Thompson I. (2008). ¿Qué es Información? En *Promonegocios.net*.

Consultado el 15 de noviembre de 2015.

Disponible en http://www.promonegocios.net/mercadotecnia/que-es-informacion.html.

13. Posada G. (2007) Calidad: ¿Qué es la ISO? En *Degerencia.*

Consultado el 15 de noviembre de 2015.

Disponible en http://www.degerencia.com/articulo/calidad_que_es_la_iso.

14. Acevedo H. (2011) ISO-27001: ¿Qué es y para qué sirve? En *Magazcitum.* Consultado el 15 de noviembre de 2015.

Disponible en http://www.magazcitum.com.mx/?p=1574#.VkzX4_kvfIV.

15. AENOR (2010). ¿Qué es una norma? En *AENOR*. Consultado el 15 de noviembre de 2015. Disponible en http://www.aenor.es/aenor/normas/normas/quees_norma.asp#.Vkz4DfkvfIU.

16. Gonzalez V. (2008). Empresa. Políticas y normas En *Mailxmail.*

Consultado el 15 de noviembre de 2015.

Disponible en http://www.mailxmail.com/curso-empresa-metodos-procedimientos/empresa-politicas-normas.

17. UNISDR (2004). Programa de prevenciones. En *UNISDR*. Consultado el 15 de noviembre de 2015. Disponible en http://www.unisdr.org/2004/campaign/booklet-spa/page9-spa.

18. DefiniciónABC (2015). Definición de Seguridad. En DefiniciónABC. Consultado el 15 de noviembre de 2015. Disponible en http://www.definicionabc.com/social/seguridad.php

19. Salazar, A. (2014) Teoría de sistemas aplicada a la ingeniería industrial. En *Academia*. Consultado el 15 de noviembre 2015. Disponible en https://www.academia.edu/6159440/TEOR%C3%8DA_DE_SISTEMAS_APLICADA_A_LA_INGENIER%C3%8DA_INDUSTRIAL.

20. Quees? (2015). ¿Qué es el software? En Quees?

21. Wikipedia. (2011). Seguridad de la información. En *Wikipedia.* Consultado el 15 de noviembre de 2015. Disponible en http://es.wikipedia.org/wiki/Seguridad de la informaci%C3B3n.

22. GNU. (2015) ¿Qué es el software libre? En *GNU*. Consultado el 15 de noviembre de 2015. Disponible en http://www.gnu.org/philosophy/free-sw.es.html.

23. ServiciosTIC (2015) Las T.I.C. En *Serviciostic*. Consultado el 15 de noviembre de 2015. Disponible en http://www.serviciostic.com/las-tic/definicion-de-tic.html.

24. Bajacalifornia (2014) Organización Internacional para la Estandarización (ISO) 2014. En *Bajacalifornia.* Consultado el 12 de noviembre de 2015. Disponible en http://www.bajacalifornia.gob.mx/registrocivilbc/iso_informa2.htm.

25. Gonzales, D. (2013) ISO-27001:2013 ¿Qué hay de nuevo? En

26. ISO27000.ES (2014) El portal de ISO 27001 en Español. En ISO 27000.ES. Consultado el 12 de noviembre de 2015. Disponible en http://www.iso27000.es/iso27000.html.

27. Explorable.com (Nov 3, 2009). Investigación Cuantitativa y Cualitativa Consultado el 9 de diciembre de 2015. Disponible en Explorable.com: https://explorable.com/es/investigacion-cuantitativa-y-cualitativa

Anexos

Anexo 1: Glosario de términos

1. **Activo:** Es todo a lo que una organización le asigna un valor y por lo tanto la organización debe proteger. También es definido como el conjunto de los bienes y derechos tangibles e intangibles de propiedad de una institución y son generadores de renta o fuente de beneficios como; bienes, inversiones, cuentas por cobrar, inmuebles, instalaciones, maquinarías, etc.
2. **Amenaza:** Se define como una causa potencial de un incidente no deseado, podría resultar dañino para un sistema u organización.
3. **Análisis de riesgo:** Es el sistemático uso de información para identificar fuentes de riesgo y estimar el mismo.
4. **Control de riesgo:** Es el proceso que busca asegurar que las políticas, estándares, límites y procedimientos para el tratamiento de riesgos son apropiadamente tomados y/o ejecutados. Las actividades de control están preferentemente incorporadas en los procesos organizacionales y las actividades de apoyo. Incluye los controles generales así como los de aplicación a los sistemas de información, además de la tecnología de información relacionada.
5. **Evaluación de riesgo:** Se define como el proceso de comparar el riesgo estimado contra criterio de riesgo dado para determinar el significado del riesgo.
6. **Identificación de riesgo:** Es un proceso por el que se determinan los eventos internos y externos que pueden tener un impacto negativo sobre los objetivos de la organización. Entre otros aspectos, considera la posible

interdependencia entre eventos, así como los factores influyentes que los determinan.

7. **Información:** Es definida como cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

8. **La empresa, la organización:** Quipu Soluciones Empresariales S.A.C.

9. **Objetivo de control:** Es una declaración del propósito o resultado deseado mediante la implementación de controles apropiados en una actividad de tecnología de información particular.

10. **Proceso crítico:** Es el proceso considerado indispensable para la continuidad de las actividades y servicios de la organización, y cuya falta o ejecución deficiente puede tener impactos significativos para la empresa.

11. **Riesgo:** Se constituye como la condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la entidad.

12. **Seguridad de la información:** Es la característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad.

13. **Tecnología de la información:** Incluye los sistemas informáticos y la tecnología asociada a dichos sistemas.

14. **Tratamiento de riesgo:** Es el proceso de selección e implementación de medidas para modificar el riesgo.

15. **Vulnerabilidad:** Es una debilidad de una ventaja o un grupo de ventajas que pueden ser explotadas por una o más amenazas.

16. PDT: Programa de Declaración Telemática, sistema informático desarrollado por SUNAT con la finalidad de facilitar la declaraciones juradas bajo condiciones de seguridad del registro de la información.

17. ISO: International Organization for Standardization o también conocida por Organización Internacional de Normalización.

18. Gestión: Se entiende por gestión a la utilización de los recursos de manera eficiente, en el caso del proyecto se gestionan los recursos de la empresa para reducir los riesgos.

Anexo 2: Entrevista para el Gerente General

1. ¿La empresa cuenta con algún plan de contingencia?

   .-

2. ¿El personal tiene conocimiento de alguna política de seguridad en la empresa?

   .-

3. ¿La empresa cuenta con un inventario de activos de información?

   .-

4. ¿Los responsables de área mantienen un control sobre los activos de información?

   .-

5. ¿Cada cuánto tiempo el personal es capacitado? ¿Lo considera importante?

   .-

6. ¿Qué tan significativos son los ingresos obtenidos por el área de soporte?

   .-

7. ¿Las áreas de trabajo manejan la misma información en común?

   .-

Anexo 3: Entrevista para el personal

1. ¿Se tiene la información necesaria para cumplir sus labores?

   .-

2. ¿Los equipos y registros están en buen estado?

   .-

3. ¿Manejan un manual de funciones?

   .-

4. ¿Cómo capacitan al nuevo personal?

   .-

5. ¿Existe disconformidad con los clientes?

   .-

6. ¿Alguna incidencia que sea frecuente?

   .-

7. ¿Quién se responsabiliza de los equipos y documentos?

   .-