**UNIVERSIDAD TÉCNICA DE BABAHOYO**

**FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.**

**PROCESO DE TITULACIÓN**

**JUNIO 2021 – NOVIEMBRE 2021**

**EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA**

**PRUEBA PRÁCTICA**

**INGENIERÍA EN SISTEMAS**

**PREVIO A LA OBTENCION DEL TITULO DE INGENIERO(A) EN SISTEMAS**

**TEMA:**

# ANÁLISIS DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN DE LA INFRAESTRUCTURA INFORMÁTICA DE LA EMPRESA "CERÁMICA Y FERRETERIA ÁNGEL TAPIA" DEL CANTÓN SIMÓN BOLÍVAR

**EGRESADO:**

CARLOS ALBERTO ORTEGA MORA

**TUTOR:**

ING. HUGO GUERRERO TORRES, MGS

**AÑO 2021**

# INTRODUCCIÓN

La información se ha considerado uno de los activos más valiosos para las empresas. Los costos inducidos por la inseguridad de la información no son solo costos económicos directos, sino que también afectan la imagen de la empresa. La seguridad de la información es uno de los objetivos de una organización, a pesar de esta conciencia generalizada, que no respalda a muchas entidades con la profundidad con la que deben tratarse en este aspecto.

El presente documento muestra un análisis de riesgos de seguridad de la información de la empresa "Cerámica y Ferretería Ángel Tapia" se utilizarán diferentes herramientas las cuales servirán para conocer el entorno de la empresa y cuáles son los problemas presentados en los departamentos de caja y gerencia referentes a la perdida de información. Esto se hizo el objetivo de valorar de los activos del departamento del establecimiento los cuales son: Gerencia, cajero y se realizara el proceso de identificación y valoración de los activos de hardware y software para determinar los recursos con los que cuentan el establecimiento.

Adicionalmente, el objetivo de este caso de estudio es determinar la importancia de los activos y el nivel de vulnerabilidad que corre los activos referentes al manejo de la información y conocer por qué motivos se pierde los datos de los registros de la empresa.

La metodología empleada en la investigación es la explicativa, consiste en analizar y reconocer los riesgos que pueden ocurrir en una organización, y la descriptiva es la encargada de definir los problemas encontrado en un mismo escenario a través de la técnica de encuestas que fueron realizada al personal administrativo, con la finalidad de almacenar la información para determinar la problemática de este análisis de investigación.

La sublinea de investigación es “Redes y tecnologías inteligentes de software y hardware” en base al análisis de riesgo de seguridad de la información de la infraestructura de la empresa que permiten reconocer el riesgo operacional de un departamento. Y los instrumentos utilizados son la encuesta y la guía de revisión las cuales estuvieron dirigidas al gerente y al personal de los departamentos de caja y gerencia.

Gracias a los resultados obtenidos del uso de las herramientas de análisis como la tabla de identificación de activos, la tabla de valoración de activo y la tabla de identificación del riesgo que presentan los activos de hardware y software en donde se pudo reconocer las respectivas vulnerabilidades como: errores de configuración, falta de mantenimiento, daño por calentamientos o desconexiones. Y a su vez brindar soluciones optimas como sugerir políticas de seguridad y los debidos mantenimientos a los activos de hardware y software que conforman la infraestructura informática, con el fin brindar una solución eficaz para evitar la pérdida de información del establecimiento, lo cual se puede decir que la realización de este caso de estudio influyo positivamente en la empresa "Cerámica y Ferretería Ángel Tapia”

## DESARROLLO

La empresa Cerámica y ferretería Ángel Tapia está ubicada en el cantón Simón bolívar en las calles Guayaquil y Rocafuerte. se dedica a la venta de productos de ferretería generalmente y materiales de creación, siendo nuestra urbe bastante comercial se vio en la necesidad de darle una contribución económica, por lo que beneficiará a la sociedad y al sector de la construcción. El comercio comenzó como una sencilla ferretería que solo vendía al principio artículos férreos a los pobladores del centro cantonal, empero con el paso del tiempo el comercio se amplía diferenciándose se expande y empieza con la venta de materiales de construcción y otros materiales, tal cual una compañía reconocida en el área y empieza a capturar a los clientes de municipios y otros pueblos de este cantón.

La problemática actual es que no cuenta con una administración adecuada de la información, es decir que existe un mal manejo de datos, a causa de que los empleados cometen errores como borrar accidentalmente registros importantes del sistema, además se reconoció que existen fallos de sobrecalentamiento en el disco duro todo esto ocasionando una secuencia de vulnerabilidades que afectan a sus actividades financieras, porque muchas de estas dependen de la información que se mueve en la empresa, por esta razón la información y los activos de la infraestructura informática debería estar más protegidos, ya que a través de estos activos se mueve datos relevante que no debería perderse.

Otro problema que se pudo conocer que el sistema suele presentar un desbordamiento de información al momento de ingresar los registros al sistema, lo cual compromete la seguridad y la integridad de la empresa, provocando que la información ingresada hasta el momento se pierda al no poder realizar el respaldo necesario.

En el presente análisis se empleó la investigación de campo mediante la técnica de investigación de la guía de observación se pudo recopilar y obtener información relevante que

permitió evidenciar que la empresa presenta problemas en su infraestructura informática como por ejemplo un bajo rendimiento, lentitud y errores de reinicios en su sistema operativo ocasionando graves problemas de seguridad, este problema causa la perdida de mucha información por que no se encuentra protegida.

Esta empresa muestra varias vulnerabilidades referentes a estabilidad de la información, debido a que no cuenta con antivirus eficiente en sus equipos, por lo que puede ser atacada, por virus informáticos e infecciones de malware así sea por phishing, dando sitio a la perdida de información, lo que perjudicaría a sus actividades administrativas, debido a que muchas de estas están sujetas a la información para que el sistema logre funcionar de forma eficiente en la organización.

La identificación de los activos, se la realiza aplicando la técnica de investigación de la guía de observación, es decir, hacer un recorrido por la empresa específicamente en las áreas donde se trabaje con la tecnología que almacenen información, ya que de esta manera se podrá realizar una categórica identificación de los activos. Tales como: datos, de manuales de usuario, aplicación, software del sistema, computadoras, servidores, discos duros. Y todos estos son muy importante porque permiten el correcto funcionamiento del comercial.

El Objetivo general de este estudio de caso es analizar el nivel de riesgo/vulnerabilidad de la información debido a la infraestructura informática actual de la empresa Cerámica y ferretería Ángel Tapia.

Los objetivos específicos son: **i**dentificar y valorar los activos de información perteneciente a los departamentos de gerencia y caja; analizar posibles vulnerabilidades en la seguridad de manejo de datos y en el equipo informático de los departamentos de gerencia y caja; y, definir potenciales amenazas que puedan causar perdida de la información de los departamentos de gerencia y caja.

(González, 2015) explica que la información es un recurso clave, pero también debe considerar lo siguiente: infraestructura, equipos auxiliares, redes de telecomunicaciones, instalaciones y personas. Cuando hablamos de seguridad de la información, estamos hablando de proteger la información frente a riesgos que pueden afectar a uno o más de sus tres atributos principales que son confidencialidad, integridad y disponibilidad. Además, es uno de los activos más importantes de toda una organización, junto con los sistemas y procesos de procesamiento de información, la lucha contra las amenazas puede afectar el nivel competitivo de relevancia, continuidad, productividad y cumplimiento. Debe estar debidamente protegido. Logre los objetivos de su organización.

La infraestructura de TI es un elemento fundamental de las funciones tecnológicas. Como se indicó previamente, otorga una diversidad de funcionalidades de red, almacenamiento seguro de información y procesamiento de datos a gran escala. El sistema posibilita a los usuarios comunicarse con estas infraestructuras por medio de teléfonos capaces, Pc portátiles y tabletas y regir datos particulares y laborales por medio de aplicaciones y servidores de red. Los conjuntos incorporan hardware, programa, recursos de red, sistema operativo y almacenamiento de datos. Todos sirven para brindar servicios y soluciones. (Ohia, 2018)

Indica (Fernández, 2016) que un activo es todo aquello que tiene precio para la entidad, por lo tanto, requiere de protección. Para la examinación de los activos se ofrece analizar el sistema de datos el cual está formado de más recursos que exclusivamente hardware y programa. Se debería ubicar al propietario de cada activo, para entablar la responsabilidad y rendición de cuentas sobre éste. El dueño del activo puede no tener derechos de propiedad sobre el activo, no obstante, tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo a menudo es el individuo más adecuado para establecer el costo que el activo tiene para la organización.

Señala (R.-Solís, 2019) que los equipos tecnológicos son un recurso que brinda la posibilidad de realizar varios tipos de tareas con el fin de cumplir sus obligaciones. Los activos tecnológicos pueden ser tangibles como computadoras o impresoras o intangibles sistemas o aplicaciones virtuales. Se utilizan para optimizar procesos, tiempos y recursos humanos; Tiempos de respuesta y trabajo simplificados.

Menciona (Andreina Matos Ayala, 2015) que el sistema tecnológico un conjunto de procedimientos y métodos destinados a facilitar el trabajo humano en el contexto de una acción de ingeniería. Las unidades integran un sistema coordinado de tecnología para dirigir, manejar, transportar y / o controlar materiales hacia objetivos específicos. A su vez, llamamos al conjunto de factores, procesos, técnicas u otros que funcionan e interactúan para lograr un objetivo común. Sistemas avanzados, manuales, eléctricos o automáticos; se vuelven cada vez más eficientes.

Según (Bertolin, 2018) la seguridad de la información es un proceso dinámico que requiere actualizaciones, revisiones y ajustes continuos de políticas y controles según sea necesario. La gestión eficaz de la seguridad de la información establece y mantiene programas, establece políticas y controles para mantener la confidencialidad, integridad y disponibilidad de la información, comprende las vulnerabilidades y amenazas, las amenazas y los riesgos de causa, y considera su potencial e impacto.

Seguridad física se refiere al establecimiento de barreras físicas y procedimientos de manejo ante posibles amenazas en el área. Se lo conoce como un centro informático donde puede encontrar equipos con el software necesario para el crecimiento normal de la empresa o del negocio. Proteja el hardware y los medios de almacenamiento de su empresa.

Seguridad lógica se refiere a la cantidad de años que puede pasar la información almacenada. Su principal objetivo es proteger los activos o la información de la empresa más importantes mediante la implementación de procedimientos y controles que limitan el acceso a los datos únicamente a personas autorizadas. (Christian José Álava Mero, 2018)

Explica (Gonzales, 2015) que, para garantizar la confidencialidad de la información intercambiada, se utilizan mecanismos de encriptación y ofuscación de comunicación. La seguridad digital de documentos se puede mantener mediante el uso de claves asimétricas. Los mecanismos de cifrado garantizan el secreto durante el tiempo necesario para descifrar el mensaje. Por esta razón, es necesario determinar cuánto tiempo permanecerá secreto el mensaje. No mecanismo de seguridad absolutamente seguro.

Según (Gonzales, 2015) la disponibilidad tiene relación con la continuidad de las ocupaciones de la organización, la pérdida de disponibilidad puede involucrar una pérdida de productividad o de la fama de la organización. El sistema tiene información o da servicios que tienen que estar accesibles de forma adecuada para llevar a cabo con los requisitos o prevenir fugas relevantes, como los sistemas fundamentales de vida y estabilidad.

Explica (González F. C., 2018) que una amenaza es la que ocasiona infracciones de seguridad en el equilibrio de la infraestructura de la empresa de forma que se pueda alterar, borrar violar los parámetros de seguridad de la información que poseen los activos. La estabilidad de la red está compuesta de recursos de hardware y sistemas diseñados para salvaguardar los datos y la información que se tratan en la red. Además, estos recursos dan medidas preventivas estructuradas para proteger la infraestructura de la red y sus datos contra el ingreso no autorizado, la modificación de datos. En última instancia, la igualdad de la red está diseñada para crear un entorno seguro donde los usuarios de Pc, programas de programa y aplicaciones móviles pueden hacer actividades informáticas sin vulnerabilidades de red.

(Morán, 2018) menciona que las vulnerabilidades de los activos de seguridad son las amenazas potenciales o potenciales que se manifiestan en los activos de información. No se puede asimilar la vulnerabilidad con la posibilidad que fue usada a lo largo de un procedimiento científico-técnico, en la que está establecido una teoría-cálculo de probabilidades. El primer paso fue determinar que es susceptibilidad, lo que explica claramente que una vulnerabilidad de la organización puede tener recursos y definirla como cualquier extenuación en los SI que logre permitir a las amenazas causarles perjuicios y crear pérdidas.

Clasificación de las vulnerabilidades:

Vulnerabilidad de Cross Site Scripting es la que le permite insertar código VBScript o JavaScript en la página web que ven los usuarios. El phishing es una de las aplicaciones de esta vulnerabilidad. En Es phishing, la víctima cree que está visitando una URL (que se muestra en la barra de direcciones), pero en realidad está visitando otro sitio web. Cuando un usuario ingresa credencial en este sitio web, se envían al atacante. (González J. A., 2015)

Vulnerabilidad de denegación del servicio es la negación de servicios que hace un recurso no esté libre para los usuarios. Frecuenta ocasionar la pérdida de la conectividad de la red por la implementación del ancho de banda de la red del perjudicado que una y otra vez resulta en la pérdida de la conectividad de la red. (Jiménez, 2016)

Los elementos que están afectando a la probabilidad de las amenazas que se visualizan podrían modificar, como lo harían los componentes que están perjudicando a la idoneidad o el precio de las múltiples probabilidades de procesos. Los cambios notables que están dañando a la institución debería ser revisado con anticipación para tratar de evitar riesgos de perdida de informacion. Por consiguiente, las actividades de monitoreo del riesgo se deben realizar con frecuencia y las probabilidades escogidas para el método de reconocimiento del riesgo se debería verificar periódicamente.

El proceso de gestión del riesgo de la seguridad de la información podría ser iterativo para las actividades de valoración del riesgo y/o de atención del riesgo. Un punto de vista reiterativo para realizar la respectiva valoración de la amenaza la cual puede aumentar la profundidad y el detalle de la valoración en cada iteración. El enfoque iterativo proporciona una óptima estabilización entre la reducción del tiempo y el esfuerzo solicitado para detectar los controles, inclusive permitiendo que los riesgos de efecto alto se valoren correctamente.

Señala (Merino, 2018) que existen normas que ofrecen reglas o protocolos, que deben ser respetados para ajustar ciertas conductas o actividades que deben ser mejoradas, además establecen los requisitos y los recursos mínimos que tienen los sistemas de calidad. Un método de análisis de riesgo que presente las reglas de estabilidad, las cuales se definen como, Las reglas correctas para publicar y examinar su conformidad con la anticipación básica e investigar la ejecución de una actividad de la ejecución de la actividad.

(Areitio, 2017) El análisis de riesgos tiene como objetivo estudiar, evaluar, medir y prevenir fallas y fallas de los sistemas técnicos métodos operativos que tienen la posibilidad de comenzar y desencadenar sucesos no deseados (accidentes) que están afectando a los individuos, información, los bienes y el medio ambiente. La investigación de peligros implica más que el hecho de calcular la probabilidad de que ocurran cosas negativas, se ha de lograr tener una evaluación económica del efecto de estos eventos negativos, y se va a tener presente la posibilidad de que sucedan todos los inconvenientes probables.

A continuación, se presentarán unas normativas que rigen en el análisis de riesgo:

**La regla ISO 27001**: Comprende un grupo de reglas o normas en relación a la estabilidad informática se ha promovido como opción en elemento de estabilidad de los sistemas de información, en esencia para la aplicación de un sistema de administración de la estabilidad de la información el objetivo de esta regla es reducir la vulnerabilidad de una organización a riesgos de estabilidad de la información. (Calder, 2017)

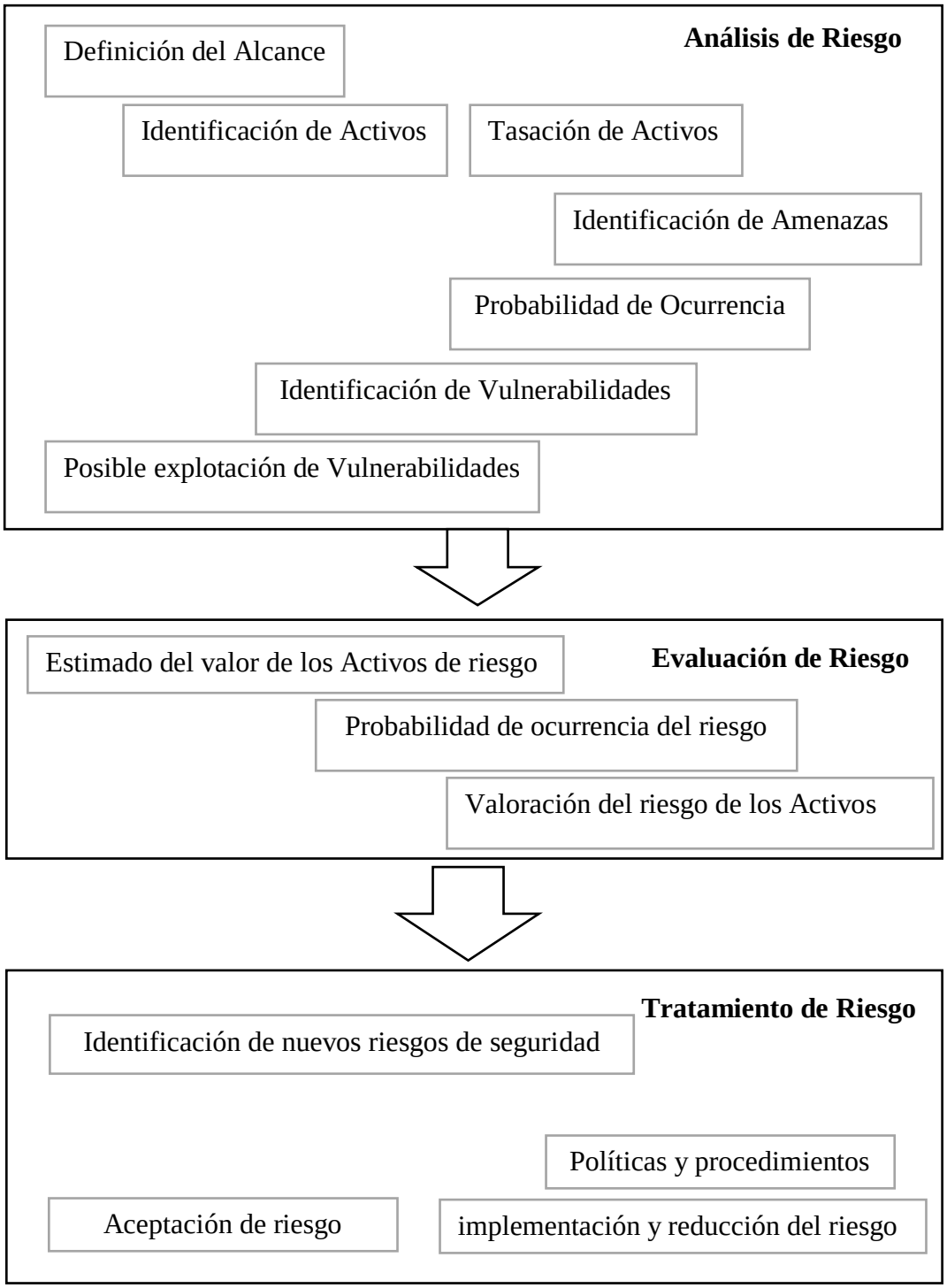
**La regla ISO/IEC 27002:** Es un estándar para la estabilidad de la información también se estima una guía de buenas prácticas en el cual se integran los diversos fines de control y controles recomendados para conservar la estabilidad de la información. (Calder, 2017)

**La regla ISO/IEC 27003:** Es un estándar mundial que constituye una guía para la fijación de un SGSI. Hablamos sobre una regla personalizada que para aquellos que han comenzado a implementar un SGSI en cuanto a los consultores en su trabajo diario porque disuelven algunas preguntas que venían careciendo de un criterio normalizado. (Urbina, 2016)

**La regla ISO/IEC 27004:** Esta norma indica cómo se estructura el sistema de medición, que es medir los valores límite, a qué hora y cómo medirlo. Además, ayuda a las organizaciones al establecimiento de fines involucrados con el rendimiento y los criterios de triunfo. (Urbina, 2016)

**La regla ISO 27005:** Es un instrumento que nos posibilita detectar las amenazas a las que se hallan expuestos todos los activos, se considera la frecuencia en la que se materializan cada una de las amenazas y valora el efecto que implica que se materialice en nuestra organización. (Urbina, 2016)

***Tabla1. Esquema del Analisis y Evaluacion de riesgo de la informacion***




**Elaborado por:** El autor

Este es un esquema que tiene como finalidad dar una idea más clara de lo que se debe realizar para analizar los riesgos de la seguridad de información de la infraestructura informática.

La metodología empleada en este análisis fue la de campo, mediante el método deductivo el cual permite recopilar datos bibliográficos con el fin de tener claros los conceptos esenciales y obtener información que establezca las bases teóricas del análisis de riesgo de seguridad de la información lo mismo que permitió el progreso eficaz para lograr los resultados, permitiendo determinar la solución más idónea haciendo uso de la norma ISO/IEC 27001, la cual está dirigida políticas seguridad de la información referente a riesgos informáticos en sus activos de información.

Se trabajo con el instrumento de investigación de la encuesta para obtener datos sobre la situación actual de la empresa en cuanto al empleo de seguridad de la información; para decidir la categorización e inventario de activos de información, y decidir su costo referente a las amenazas y vulnerabilidades relacionadas a los mismos. Además, se usó la guía de observación para la obtención de información de más relevancia, sobre las actividades que se realizan en la empresa, la aplicación de las normativas de seguridad vigentes y el funcionamiento interno del departamento.

El análisis de Información es una técnica que fue una de las más importantes ya que es la que ha permitió definir antes que nada las necesidades de seguridad de la información en la empresa, además ha sido clave para determinar los resultados para el análisis de riesgos y decidir los mecanismos de control necesarios en la disminución de riesgos en la seguridad de la información.

En el análisis de riesgos, es importante experimentar y determinar las posibilidades de riesgo de calificarlas y evaluarlas para obtener información. Como primer punto es importante reconocer y valorar los activos, los cuales recursos que contribuyen al desarrollo de actividades en la empresa, estos son partes primordiales para el desarrollo de las actividades.

A continuación, se procederá a identificar los activos por área.

***Tabla 2:*** *Activos del área gerencia*

| Activos de hardware | Activos de software | Activo de información |
|---|---|---|
| *Portátil* | *Sistema financiero integrado Ofimática.* | *Licencia de Windows server* |
| *1 disco duro de servidores* | *Base de datos* | *Unidades USB* |
| *1Router* | *Antivirus* | *Documentos en papeles* |
| *1 Servidor* | *Sistema Operativo* | |
| | *Correo electrónico* | |
| | *Internet* | |

**Fuente:** Ficha de observaciones
**Elaboración:** Carlos Ortega

***Tabla 3:*** *Activos del área de caja*

| Activos de hardware | Activos de software | Activo de información |
|---|---|---|
| *1 Equipo de escritorio* | *Sistema financiero integrado Ofimática.* | *Licencia de Windows server* |
| | *Base de datos* | *Unidades USB* |
| | *Antivirus* | *Documentos en papeles* |
| | *Sistema Operativo* | |
| | *Correo electrónico* | |
| | *Internet* | |

**Fuente:** Ficha de observaciones
**Elaboración:** Carlos Ortega

Ya ubicados los activos de ambos apartamentos de la compañía, se le debe asignar un precio, orientado a la confidencialidad, totalidad y disponibilidad, debido a que tal se llega a conocer el valor que tiene un activo para la organización.

Según el análisis anterior de las respectivas necesidades que corresponden a la escala de valoración de los activos se obtuvo los próximos requerimientos que van a ser visualizados en la siguiente tabla

***Tabla 4.*** *Escala de valoración de los activos*

| Valoración | | Dependencia | Funcionalidad | Integridad, confidencialidad y disponibilidad |
|---|---|---|---|---|
| **1** | *MUY BAJO* | *Los activos no están facilitando la transmisión de la información* | *Este activo posee características o programas básicos* | *La circulación, variación y no disponibilidad de este activo, puede perjudicar de forma muy baja la entrega de servicios* |
| **2** | *BAJO* | *Los activos no se encuentran limitados para la entrega de servicios* | *Este activo posee alcances tecnológicos limitados* | *La circulación, variación y no disponibilidad de este activo puede influir en la entrega de servicios* |
| **3** | *MEDIO* | *El 50% de los activos necesitan al equipo principal para la entrega de servicios* | *Este activo posee alcances tecnológicos un poco aceptables* | *La circulación, variación y no disponibilidad de este activo, puede dañar mucho, en la entrega de servicios* |
| **4** | *ALTO* | *El 50% de los activos necesitan a este activo para la entrega de servicios* | *Este activo posee alcances tecnológicos avanzados* | *La circulación, variación y no disponibilidad de este activo, puede arruinar la entrega de servicios* |
| **5** | *CRÍTICO* | *El 100% de los activos necesitan a este activo para la entrega de servicios* | *Este activo posee alcances tecnológicos Modernos más avanzados* | *La circulación, alteración y no disponibilidad de este activo o de la información que este tiene, puede arruinar la entrega de servicios* |

**Fuente:** Ficha de observaciones
**Elaboración:** Carlos Ortega

Una vez establecido los límites y valoración en cuanto a la fiabilidad que tenga cada activo y su totalidad además se verán si estos están expuestos a problemas relacionado a la disponibilidad y el promedio de sus servicios.

Según el análisis previo de las respectivas necesidades correspondientes a la valoración de los activos se determinó los siguientes requerimientos que serán visualizados en la siguiente tabla.

***Tabla 5.*** *Funcionalidad con sus valores de los activos de la empresa*

| Activos de soporte | Función | Confidencialidad | Integridad | Disponibilidad | Promedio |
|---|---|---|---|---|---|
| ***Portátil*** | *autoriza admitir servicios.* | *4* | *4* | *3* | ***4*** |
| ***2 equipo de escritorio*** | *Permite acceder a los servicios.* | *4* | *4* | *3* | ***4*** |
| ***Sistema financiero integrado Ofimática.*** | *autoriza el uso de herramientas* | *2* | *2* | *5* | ***3*** |
| ***Base de datos*** | *autoriza ordenar y tener libre acceso de la información que necesitemos* | *4* | *4* | *5* | ***4*** |
| ***Antivirus*** | *Detecta y da aviso de archivos maliciosos y los elimina* | *2* | *2* | *2* | ***2*** |
| ***Sistema Operativo*** | *Administra y gestiona un equipo computarizado y los diversos aparatos periféricos que lo compongan* | *4* | *4* | *5* | ***4*** |
| ***Correo Electrónico*** | *autoriza enviar y recibir correos* | *3* | *3* | *3* | ***3*** |
| ***Router*** | *autoriza tener acceso a internet* | *2* | *3* | *5* | ***3*** |
| ***Windows server 2010*** *Sistema operativo de la PC?* | *autoriza trabajar con todas las herramientas necesarias para realizar tareas en una oficina.* | *3* | *4* | *5* | ***4*** |
| ***Unidad USB o pendrives.*** | *autoriza transportar información a diferentes lugares.* | *3* | *3* | *3* | ***3*** |
| ***Documentos en papeles*** | ***autoriza*** *tener en forma manual la información.* | ***3*** | ***3*** | ***3*** | ***3*** |

**Fuente:** Ficha de observaciones
**Elaboración:** Carlos Ortega

Esta tabla fue útil para la asignación de valores a los activos intervenidos por la investigación de peligro, siendo esta primordial para el buen desarrollo de este proceso. El impacto tecnológico, es la exploración de la colaboración de la tecnología, ya sea de carácter positivo, negativo o neutro, de esta forma además se conoce a la valoración de activos, ya que de esta manera se llega a saber, el costo de un activo para la organización.

Según el análisis previo de las respectivas necesidades correspondientes a la identificación las probables amenazas de los activos se obtuvo los siguientes requerimientos que serán visualizados en la siguiente tabla.

***Tabla 6. Identificación las probables amenazas de los activos de información***

| Tipo de amenaza | Amenazas |
|---|---|
| *Daños físicos* | *Destrucción de equipo o medios de comunicación* |
| | *Polvo, Corrosión, Congelamiento* |
| *Eventos naturales* | *Fenómenos climáticos* |
| | *Fenómenos sísmicos* |
| | *Fenómenos volcánicos* |
| | *Inundación* |
| *Información comprometida* | *Interceptación de señal* |
| | *indagación remota* |
| | *Hurto de medios o documentos* |
| | *Hurto de equipos* |
| | *Rescate de medios reciclados o desechados* |
| | *Divulgación* |
| | *Datos provenientes de fuentes no confiables* |
| | *Utilización de hardware* |
| | *Utilización de software* |
| *Fallas técnicas* | *desperfecto de equipo* |
| | *Mal funcionamiento del equipo* |
| | *Saturación de sistema de información* |
| | *Mal funcionamiento del software* |
| | *Mantenimiento inadecuado del sistema* |

**Fuente:** Ficha de observaciones
**Elaboración:** Carlos Ortega

Según el análisis previo de las respectivas necesidades correspondientes a la identificación de las vulnerabilidades se determinó los siguientes requerimientos que serán visualizados en la siguiente tabla.

***Tabla 7. Identificación de las vulnerabilidades***

| Vulnerabilidades | |
|---|---|
| *Hardware* | *Mantenimiento insuficiente/ falla de la instalación de los medios de almacenamiento.* |
| *Hardware* | *La ausencia de sistemas de reemplazo periódico. Susceptibilidad para humedad, polvo y suciedad.* |
| *Hardware* | *Susceptibilidad a las fluctuaciones de voltaje* |
| *Hardware* | *Almacenamiento sin protección* |
| *Software* | *Falta de copia de seguridad* |
| *Software* | *La ausencia de antivirus* |
| *Software* | *errores en la producción de gestión de informes* |
| *Red* | *Errores de envíos* |
| *Red* | *Líneas de comunicación sin protección* |
| *Red* | *Tráfico sensible sin protección* |
| *Red* | *Conexión deficiente de los cables.* |
| *Red* | *Sin protección de las conexiones de red* |
| *Red* | *Transferencia de contraseñas autorizadas* |

**Fuente:** Ficha de observaciones
**Elaboración:** Carlos Ortega

Según el análisis previo de las respectivas necesidades correspondientes a las identificaciones de los riesgos se determinó los siguientes requerimientos que serán visualizados en la siguiente tabla.

***Tabla 7. Identificación de los riesgos***

| Código de Riesgo | RIESGO |
|---|---|
| *40* | *Incumplimiento de proveedores* |
| *60* | *Errores Tecnológicos* |
| *65* | *Errores en la seguridad de los sistemas tecnológicos asociados a ataques informáticos* |
| *80* | *Error u omisiones en la implementación de procesos* |
| *130* | *Violación de acuerdos de confidencialidad* |
| *160* | *Variación, pérdida o pérdida de información de información* |
| *180* | *Variación de la disponibilidad de los servicios de la empresa* |
| *190* | *Modificación e inadecuada Uso de la información gestionada.* |

**Fuente:** Ficha de observaciones
**Elaboración:** Carlos Ortega

Según el análisis previo de las respectivas necesidades correspondientes a la frecuencia de las amenazas y vulnerabilidades presentada en infraestructura informática de los activos se obtuvo los siguientes requerimientos que serán visualizados en la siguiente tabla.

***Tabla 8. Infraestructura informática de la empresa***

| ACTIVOS | AMENAZAS | VULNERABILIDA DES | FRECUENCIA DE AMENAZAS | FACILIDAD |
|---|---|---|---|---|
| **Portátil** | Caídas | Perdidas de equipos | BAJO | BAJO |
| | Equivocación en configuración | Falta de conocimiento | MEDIO | MEDIO |
| | carencia mantenimiento | Errores en el sistema | ALTO | ALTO |
| | Manejo no permitido del equipo | Contraseñas débiles | ALTO | ALTO |
| **2 equipos de escritorio** | Daño por Suministro de energía | Cortes de energía | BAJO | BAJO |
| | Caídas | Descuido del equipo | BAJO | BAJO |
| | carencias de mantenimiento | Carencias de mantenimientos | ALTA | ALTA |
| | Manejo no permitido del equipo | Contraseñas débiles | ALTA | ALTA |
| **Software** | Fallos por abastecimiento de energía | insuficiencia de energía | BAJO | BAJO |
| | Equivocación de configuración | Falta de entendimiento | MEDIO | MEDIO |
| | Manejo no permitido de programas | Negligencia del administrador | MEDIO | MEDIO |
| **Unidades USB o pendrive** | Perdida | Descuido del propietario | BAJO | BAJO |
| | Daños por agua | Descuido del propietario | BAJO | BAJO |
| **Base de datos** | Uso no autorizado de la base de datos | Negligencia del administrador | ALTA | ALTA |
| | Equivocación de configuraciones de la base | Falta de entendimiento | | |
| **Sistema operativo** | Equivocación en actualizaciones | error instalación y activación del sistema | MEDIO | MEDIO |
| | Software malicioso | Protección débil | MEDIO | MEDIO |
| | Problemas de compatibilidad | Instalación de herramientas no acorde al equipo | MEDIO | MEDIO |
| **Documentos en papeles** | Perdida | error administración de administración | ALTA | ALTA |
| | Desorganización | Información desordenada | ALTA | ALTA |

**Fuente:** Ficha de observaciones
**Elaboración:** Carlos Ortega

Según el análisis previo de las respectivas necesidades correspondientes a las probabilidades de amenazas se determinó los siguientes requerimientos que serán visualizados en la siguiente tabla.

***Tabla 9. Identificación de la probabilidad de ocurrencia de amenazas***.

| Probabilidad | Descripción |
|---|---|
| BAJA | Amenazas conbaja probabilidad de atacar las vulnerabilidades en un activo |
| MEDIA | Amenazas que a veces atacan las vulnerabilidades en un activo |
| ALTA | Amenazas quecomúnmente puedenatacar las Vulnerabilidades en un activo |

**Fuente:** Ficha de observaciones
**Elaboración:** Carlos Ortega

Debido a la encuesta realizada al personal responsable de los activos tecnológicos de la empresa, se hizo la obtención de la información con en relación a las amenazas y vulnerabilidades que tienen la posibilidad de intervenir en todos los activos, información usada para la evaluación del peligro sobre cada activo.

Según el análisis previo de las respectivas necesidades correspondientes a las necesidades para el tratamiento de los riesgos se obtuvo los siguientes requerimientos que serán visualizados en la siguiente tabla.

***Tabla 9. Necesidad para el tratamiento de los riesgos.***

| Valores | Nivel de riesgo | Descripción del riesgo y acciones |
|---|---|---|
| *8* | *ALTA* | *Necesita la implementación de monitoreo, con informes correspondientes a altos controles.* |
| *6-7* | *MEDIA ALTA* | *Corrección o aplicabilidad de los controles y monitoreo correspondientes con altos controles.* |
| *4-5* | *MEDIA* | *Nivel de riesgo, que requiere la monitorización aplicada frecuentemente* |
| *2-3* | *MEDIA BAJA* | *Nivel de riesgo, que requiere la aplicabilidad la vigilancia debido a que se presentan riesgos al azar.* |
| *0-1* | *BAJA* | *El Administrador de activos es responsable del desempeño normal de, que será comunicado por personal calificado.* |

**Fuente:** Ficha de observaciones
**Elaboración:** Carlos Ortega

En este análisis de riesgo fue un proceso clave que permitió determinar los riesgos y posibles amenazas que pueden presentarse en los activos de información de la empresa, para la ejecución de este proceso se empleó la tabla de identificación de activos la cual fue muy importante porque sirvió para conocer el número de equipos que posee los departamentos de caja y gerencia.

Se realizaron otros procesos el cual fue el de la escala de valoración de los activos el cual en detallar la importancia de los activos de información que posee y fueron valorados en escales de riesgos desde muy bajo hasta el crítico con el fin de identificar que tan importante es la información que se encuentra almacenada en el equipo.

# CONCLUSIONES

Respecto a este caso de estudio se demostró que existen problemas como bajo rendimiento, lentitud y errores de reinicios del sistema de gran parte de los activos que posee los departamentos de caja y gerencia esto se pudo conocer gracias a los diferentes métodos análisis de riesgo de seguridad en donde el objetivo principal identificar las vulnerabilidades y brindar una posible solución.

En el análisis realizado en la empresa se lograron detectar 8 riesgos y 13 vulnerabilidades tanto como hardware, software y en la red que pueden afectar a los activos de información de los respectivos departamentos.

Se llega a la conclusión que se deberá implementar políticas de seguridad a los activos del área de infraestructura informática y su vez intentar prevenir posibles escenarios donde la información se encuentre comprometida ya sea por fallos o daños que pueda ocasionar una paralización de las actividades diarias de la empresa.

Como resultado final se conoció que en los departamentos de caja y gerencia mucha información se vio comprometida todo esto ocasionando perdidas de información sumamente importante para la empresa, por esto se sugiere establecer medidas de seguridad a los activos de la empresa tales como: proteger sus equipos instalando antivirus confiables y realizar respaldo de los equipos frecuentemente. Además, se podría crear políticas obligatorias, que promuevan el respeto de la confiabilidad e integridad de la información por parte de las personas que tengan acceso a los activos y a la información de la empresa.

## Bibliografía


Areitio, J. (2017). *Seguridad de la información. Redes, informática y sistemas de información.* Mexico. Obtenido de https://books.google.com.ec/books?id=_z2GcBD3deYC&pg=PA99&dq=activos+de+informacion&hl=es-419&sa=X&ved=2ahUKEwjh9aeUsv_yAhWQZd8KHW-QBF4Q6AF6BAgGEAI#v=onepage&q=activos%20de%20informacion&f=false

Belmont, Ó. S. (2017). *Análisis de riesgo en operaciones de comercio exterior.* España. Obtenido de https://books.google.com.ec/books?id=ye9GDwAAQBAJ&pg=PT51&dq=concepto+de+amenazas+en+un+sistema&hl=es&sa=X&ved=2ahUKEwj599TIz9LyAhXmFVkFHcrQD7QQ6AEwAnoECAMQAg#v=onepage&q=concepto%20de%20amenazas%20en%20un%20sistema&f=false

Bertolin, J. A. (2018). *Seguridad de la informacion.* Madrid . Obtenido de https://books.google.com.ec/books?id=_z2GcBD3deYC&printsec=frontcover&dq=seguridad++de+la+informacion&hl=es&sa=X&redir_esc=y#v=onepage&q=seguridad%20%20de%20la%20informacion&f=false

Brown, B. (2017). *el poder de la vulnerabilidad.* Madrid. Obtenido de https://books.google.com.ec/books?id=w_HlAAAACAAJ&dq=concepto+de+Vulnerabilidad+de+ventanas+enga%C3%B1osas&hl=es&sa=X&ved=2ahUKEwj6sNjCzdLyAhUEF1kFHUmvB3EQ6AEwBHoECAMQAg

Calder, A. (2017). *ISO27001/ISO27002: Una guía de bolsillo.* Madrid. Obtenido de https://books.google.com.ec/books?id=WL02DwAAQBAJ&printsec=frontcover&dq=La+regla+ISO+27002&hl=es&sa=X&redir_esc=y#v=onepage&q=La%20regla%20ISO%2027002&f=false

Christian José Álava Mero. (2018). *SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Madrid. Obtenido de https://books.google.com.ec/books?id=5Z9yDwAAQBAJ&printsec=frontcover&dq=clasificacion+de+la+seguridad+informatica&hl=es&sa=X&ved=2ahUKEwjL5q-Rh_ryAhWKRzABHXHUDVwQ6AF6BAgKEAI#v=onepage&q&f=false

Fernández, C. H. (2016). *Ejecución de proyectos de implantación de infraestructuras de redes* .. Obtenido de https://books.google.com.ec/books?id=u7hWDwAAQBAJ&pg=PA216&dq=monitoreo+de+red&hl=es-419&sa=X&ved=2ahUKEwj_1uLd-v7yAhVUOH0KHR9eDvcQ6AF6BAgGEAI#v=onepage&q=monitoreo%20de%20red&f=false

González, F. C. (2018). *América Latina en las últimas décadas: procesos y retos.* Madrid. Obtenido de https://books.google.com.ec/books?id=Pq53DwAAQBAJ&pg=PA173&dq=concepto+de+Vulnerabilidad+de+desbordamiento&hl=es&sa=X&ved=2ahUKEwjuhoaAzNLyAhXEEFkFHfcXDjIQ6AEwAnoECAgQAg#v=onepage&q=concepto%20de%20Vulnerabilidad%20de%20desbordamiento&f=false

González, J. A. (2015). *Conceptos Introductorios Al Estudio de la Información.* Salvador. Obtenido de https://books.google.com.ec/books?id=CiXpGyPJKroC&pg=PA31&dq=concepto+de+informacion&hl=es&sa=X&ved=2ahUKEwjk4f7jytLyAhWnmuAKHTqXBCwQ6AEwAHoECAcQAg#v=onepage&q=concepto%20de%20informacion&f=false

Jiménez, J. L. (2016). *UF2406 - El cliclo de vida del desarrollo de aplicaciones.* España. Obtenido de

https://books.google.com.ec/books?id=OVlWDwAAQBAJ&pg=PA337&dq=concepto+de+Vulnerabilidad+de+Cross+Site+Scripting&hl=es&sa=X&ved=2ahUKEwintIaEzdLyAhWgFFkFHRk1AKEQ6AEwBHoECAoQAg#v=onepage&q=concepto%20de%20Vulnerabilidad%20de%20Cross%20Site%20Scripting&f=fa

Merino, M. A. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* España. Obtenido de https://books.google.com.ec/books?id=5Z9yDwAAQBAJ&printsec=frontcover&dq=Hay+normas+que+ofrecen+reglas+o+protocolos+de+riesgo+de+seguridad&hl=es&sa=X&ved=2ahUKEwjWudXBrPXyAhWyFlkFHUR8CPIQ6AF6BAgEEAI#v=onepage&q&f=false

Morán, G. L. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* España . Obtenido de https://books.google.com.ec/books?id=5Z9yDwAAQBAJ&pg=PA46&dq=VULNERABILIDADES+EN+ACTIVOS&hl=es&sa=X&ved=2ahUKEwjSusPf_PTyAhVBQzABHRJ4CsAQ6AF6BAgGEAI#v=onepage&q=VULNERABILIDADES%20EN%20ACTIVOS&f=false

Ohia, N. (2018). *Biblioteca de riesgo y vulnerabilidad de infraestructura de TI: Un registro consolidado de vulnerabilidades de infraestructura operativa y tecnológica.* España . Obtenido de https://books.google.com.ec/books?id=bhuJvgEACAAJ&dq=QUE+ES+LA+infraestructura+de+TI&hl=es&sa=X&redir_esc=y

Parrales, R. (2018). *ANÁLISIS DE VULNERABILIDADES.* Barcelona. Obtenido de https://books.google.com.ec/books?id=5Z9yDwAAQBAJ&printsec=frontcover&dq=gestion+de+riesgo+de+informacion&hl=es-

419&sa=X&ved=2ahUKEwjUruGw9f7yAhVCLX0KHRWxAKEQ6AF6BAgIEAI#v=onepage&q=gestion%20de%20riesgo%20de%20informacion&f=false

POSTIGO PALACIOS, A. (2020). *Seguridad informática.* España . Obtenido de https://books.google.com.ec/books?id=UCjnDwAAQBAJ&printsec=frontcover&dq=seguridad+informatica&hl=es&sa=X&redir_esc=y#v=onepage&q=seguridad%20informatica&f=false

Urbina, G. B. (2016). *Introducción a la seguridad informática.* Mexico . Obtenido de https://books.google.com.ec/books?id=IhUhDgAAQBAJ&pg=PA48&dq=La+regla+ISO+27005&hl=es&sa=X&ved=2ahUKEwiU-9m1qvXyAhWyTTABHftmC6IQ6AF6BAgFEAI#v=onepage&q=La%20regla%20ISO%2027005&f=false

**ANEXO 1**

## INSTRUMENTO DE INVESTIGACION "ENCUESTA"

**1.** ¿Considera usted que la empresa presenta un mal manejo y perdida de la información?

SI ☐ NO ☐

**2.** ¿Piensa usted que los equipos de escritorio presentan algún tipo de problema físico? Indique cuál

Calentamiento ☐ ruido ☐ sin energía ☐ cables expuestos ☐ desconexión ☐

**3.** ¿Cree usted que el sistema actual de información no es confiable y que la información puede ser vulnerada?

SI ☐ NO ☐

**4.** ¿Considera usted han sufrido algún robo de información?

SI ☐ NO ☐

**5.** ¿Cuenta usted con conocimientos acerca de los procedimientos para reconocer los riesgos de la seguridad de información?

SI ☐ NO ☐

**6.** ¿Considera usted que el comercial cuenta con los respaldos necesarios de la información en caso de que ocurra fallas técnicas en los equipos?

SI ☐ NO ☐

**7.** ¿Cree usted que la empresa ha sufrido ataques informáticos donde la información quede comprometida?

SI ☐ NO ☐

**8.** ¿Considera usted que la perdida de la información perjudica las actividades administrativas y financieras del comercial?

SI ☐ NO ☐

**9. ¿**Existe controles de seguridad en los activos usados en la empresa?

SI ☐ NO ☐

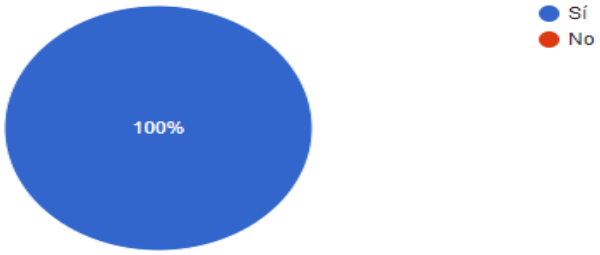
**10.** ¿Considera usted la implementación de medidas preventivas de seguridad para asegurar los activos de información?

SI ☐ NO ☐

**ANEXO 2**

## TABULACION DE LA ENCUESTAS

**1. ¿Considera que la organización tiene una pésima administración y pérdida de datos?**

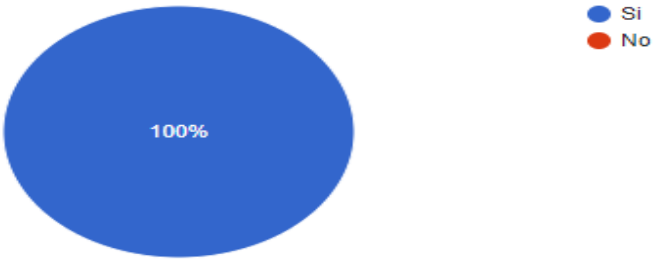



**Interpretación:** se tiende a concluir que el número completo de personas evaluadas certifica que hay una información pésima de los ejecutivos, lo que hace que no haya un equilibrio de datos.

**2. ¿Cree que los ordenadores personales presentan algún tipo de problema real? demuestre cuál**

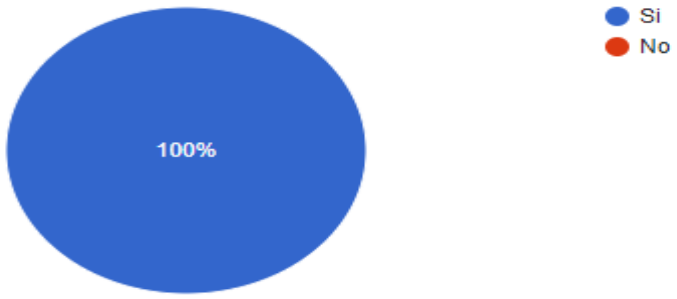

**Interpretación:** se tiende a razonar que el número completo de personas evaluadas certifica que hay problemas en el equipo de recalentamiento y desconexión.

**3. ¿Considera que el actual sistema de datos no es robusto y que se puede acceder a ellos?**



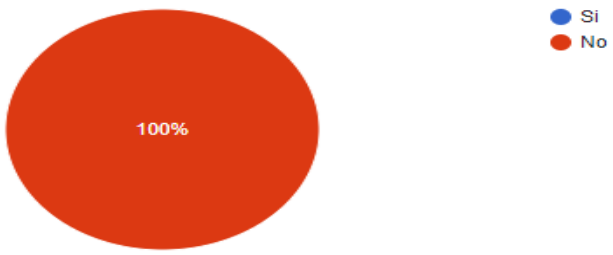
**Interpretación:** se deduce que la mayoría de los encuestados consideran que el marco no es fiable para asegurar los datos, ya que a veces se ha abusado de él.

**4. ¿Considera que ha sufrido algún robo de datos?**



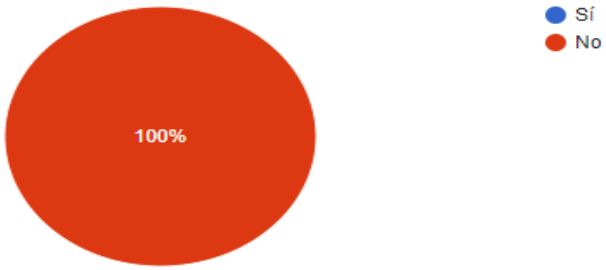

**Interpretación:** se puede asumir que el número completo de personas analizadas expresaron que han sufrido un robo de datos en el que la organización se ha visto comprometida.

**5. ¿Conoce los procedimientos para la detección de riesgos de seguridad informática?**



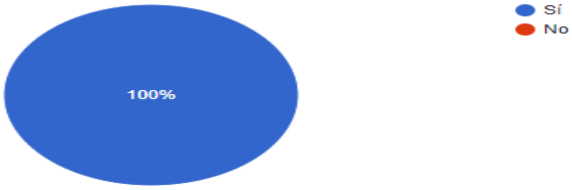

**Interpretación:** se puede justificar que el número completo de personas analizadas demuestra que los recursos de los equipos tienen una baja exposición, lo que provoca en determinados casos reinicios con pérdida de datos.

**6. ¿Considera que la oficina de negocios tiene el refuerzo esencial de los datos si se produce una decepción especializada en el equipamiento?**



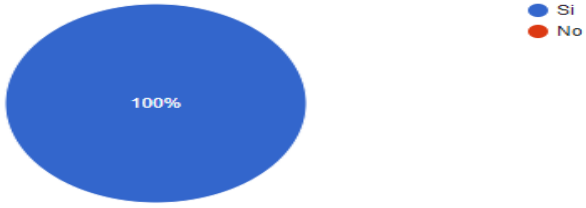

**Interpretación:** se puede concluir que el total de persona encuestadas ha expresado que la organización no está preparada para reforzar la información en caso de que se produzcan fallos de hardware.

**7. ¿Considera que la organización ha sufrido ataques informáticos en los que los datos se han visto comprometidos?**




**Interpretación:** se puede deducir que el número total de personas que han sido encuestadas han manifestado que han sufrido un ataque de phishing en el que se han visto comprometidos sus datos.

**8. ¿Considera que la carencia de datos está obstaculizando los procesos de autorización y financieros de la organización?**

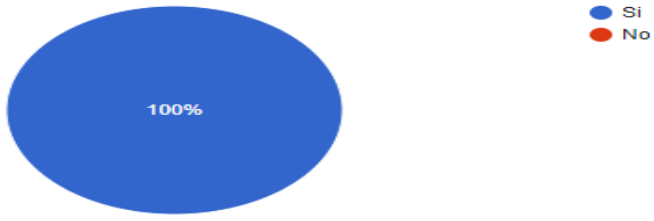


**Interpretación:** Se tiende a interpretar que el número absoluto de personas encuestadas coincide en que la carencia de datos causa perjuicios tanto a nivel de gestión como monetario.

**9. ¿Existen controles de seguridad sobre los recursos utilizados en la organización?**


**Interpretación:** se tiende a razonar que el número absoluto de personas encuestadas coincide en que no hay controles de seguridad que permitan proteger sus datos.

**10. ¿Piensa en la ejecución de esfuerzos de seguridad preventiva para obtener recursos de datos?**




**Interpretación:** se tiende a razonar que el número absoluto de individuos encuestados coincide en que no hay controles de seguridad que les permitan proteger sus datos.

**ANEXO 3**

## GUÍA DE OBSERVACIÓN.

| N.º | INDICADORES DE EVALUACIÓN | SI | NO | OBSERVACIÓN |
|---|---|---|---|---|
| **1** | La infraestructura informática presenta problemas | X | | Se conoció que diferentes equipos presentan fallos técnicos. |
| **2** | Se tiene identificado los activos de información | **X** | | Se ha realizado de una manera organizada la identificación de los activos |
| **3** | Ha ocurrido algún evento que ha afectado las actividades del establecimiento | **X** | | Fallos de reinicios y sobrecalentamiento de equipos |
| **4** | Tiene acceso a internet. | **X** | | |
| **5** | El comercial cuenta con una estrategia para mejorar la seguridad. | | X | |
| **6** | Cuenta con buena ubicación el comercial. | **X** | | Cuenta con un lugar estratégico la ubicación del negocio es muy comercial. |
| **7** | Ha detectado vulnerabilidades en la estabilidad de la información | X | | No cuenta con antivirus para proteger la información de virus informáticos |
| **8** | Cuenta con empleados el comercial | **X** | | 2 empleados |
| **9** | Se observa inconvenientes en el sistema | **X** | | Desbordamiento de información |
| **10** | El establecimiento cuenta con el debido mantenimiento de sus activos de información | | X | |

**CERÁMICA Y FERRETERÍA ÁNGEL TAPIA C. LTDA**
Sucursal: Simón Bolívar-Ecuador
Dirección: Av. Guayaquil 6 y Rocafuerte

**Babahoyo,07 de septiembre de 2021**

**ING GINA CARRASCO ECHEVERRÍA MAE**
**DECANA F.A.F.I**

De mis consideraciones:

Yo, **ÁNGEL GUSTAVO TAPIA** con cedula de identidad No. 020094061-7 Gerente propietario de cerámica y ferretería "ANGEL TAPIA" autorizo al señor **ORTEGA MORA CARLOS ALBERTO**, con cedula de identidad No.095394843-7 de la carrera de ingeniería en sistemas le otorgo el permiso respectivo para realizar su estudio de caso "**Análisis de riesgo de seguridad de la información de la infraestructura informática**", para la empresa "cerámica y ferretería ángel tapia", del cantón simón Bolívar el cual es un requisito indispensable para poder titularse.

Del señor gerente muy atentamente.

VENTA DE ARTÍCULOS
DE CERÁMICA Y FERRETERÍA
*De: Angel Tapia Tapia*
Dir: Velasco Ibarra y Esmeraldas
Cel: 0999335837 Simón Bolivar - Ecuador

**ÁNGEL GUSTAVO TAPIA TAPIA**