1. Situación Actual
   1. Descripción General de la Empresa

La empresa XX  es una empresa con sede en la ciudad de Asunción, con sucursales en la ciudad de Encarnación y en Hohenau, dedicada a la venta de ropa, franquiciada de la marca Hering.

La empresa ofrece una variedad de productos diferenciados cuyos consumidores meta son las personas que estén entra la edad de 1 a 35 años. La marca Hering es una marca reconocida a nivel internacional por su calidad y por sus colecciones en sintonía con las tendencias actuales, manteniendo su identidad y tradición.

* 1. Misión

Desarrollar marcas, crear y vender productos y servicios de ropa con valor percibido y atención al cliente.

* 1. Visión

Ser reconocida como la más rentable y mejor gestión de las marcas de ropa.

* 1. Descripción Organizacional

Para el departamento de Itapúa la organización cuenta con una Coordinación Regional, que coordina y supervisa las sucursales del departamento.

La sucursal a ser auditada cuenta con una gerencia, un salón de ventas y un depósito.

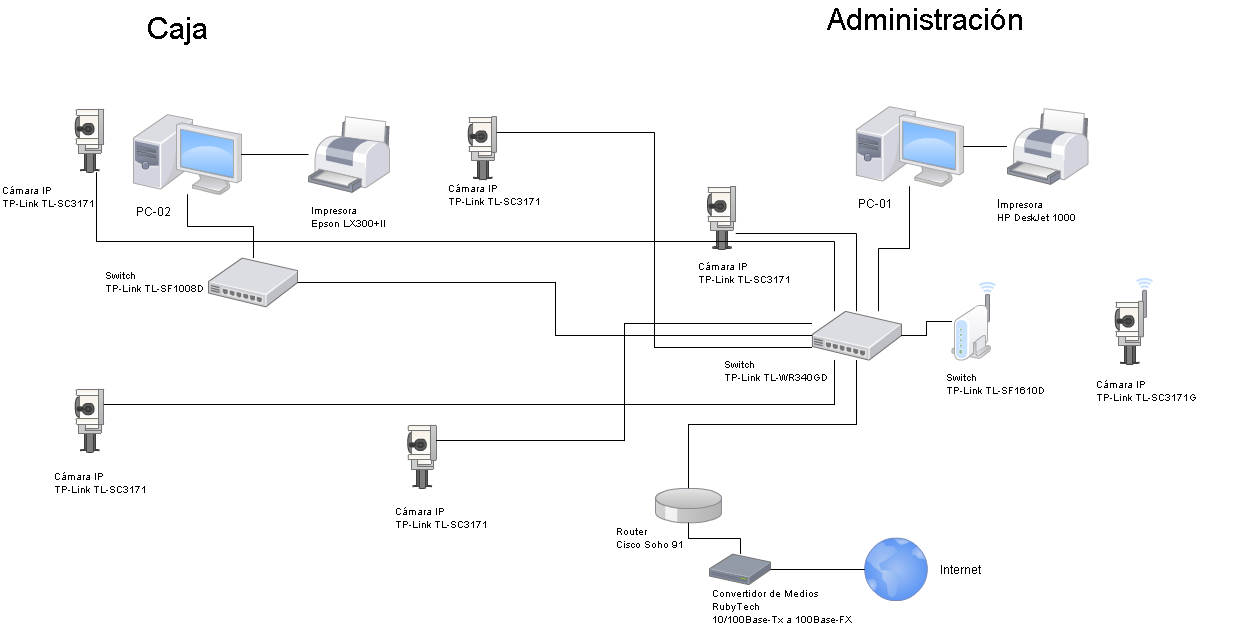
A continuación se presenta el Organigrama de la sucursal:

El plantel de empleados está compuesto de la siguiente manera:

* 1 (Una) Coordinadora Regional
* 1 (Una) Gerente
* 6 (Seis) Vendedoras
* 1 (Un) Depositero
* 1 (Un) Limpiadora

1. Infraestructura de la Red
   1. Inventario de hardware y software

* 1 (Un) Convertidor de Medios RubyTech. Caract.: 10/100 Base-TX a 100 Base-FX
* 1 (Un) Router Cisco Soho 91. Caract.: 4 Puertos.
* 1 (Un) Switch TP-Link TL-SF1610D. Caract.: 16 puertos.
* 1 (Un) Switch WIFI TP-Link TL-WR340GD. Caract.: 4 puertos.
* 1 (Una) PC (PC-1). Caract.: Pentium DualCore E5700 3.00 GHz 1.96 GB de RAM. S.O.: Microsoft Windows XP Professional 2002-Service Pack 3. Antivirus: Kaspersky 2013 Internet Security.
* 1 (Una) PC (PC-2). Caract.: Pentium DualCore E5800 3.2GHz 4GB de RAM. S.O.: Microsoft Windows 7 Professional 2009-Service Pack 1. Antivirus: Kaspersky 2013 Internet Security.
* 1 (Una) Impresora HP DeskJet 1000.
* 1 (Una) Impresora Epson LX300+II.
* 5 (Cinco) Cámaras de vigilancia IP TP-Link TL-SC3171.
* 1 (Una) Cámara de vigilancia IP inalámbrica TP-Link TL-SC3171G.
  1. Diagrama de la red



1. Descripción
   1. Alcance

La presente auditoria será aplicada a la empresa XX en la Casa Central de Itapúa, con los siguientes enfoques:

* Análisis de la estructura física y lógica de la red y;
* Los métodos de respaldo de la información (backups) de la empresa.
  1. Objetivos
* Verificar la existencia de controles de confiabilidad, protección y disponibilidad de la información, basados en los siguientes objetivos de control de COBIT: DS4.9, DS11.3, DS11.
* Evaluar el estado del cableado de la red interna, basado en los estándares TIA/EIA 568-B.
* Verificar el uso de técnicas de seguridad en la red, basado en el objetivo de control de COBIT DS5.10 y el capítulo 13 del estándar ISO 27002
  1. Justificación

La empresa diariamente genera, maneja y distribuye información de vital importancia para la continuidad de las operaciones del negocio. Así mismo maneja informaciones confidenciales como información personal de los clientes, informaciones proveídas por la empresa franquiciadora e informaciones relevantes a costos, proveedores y datos bancarios propios de la empresa entre otras.

Dada la relevancia de la disponibilidad, confiabilidad y protección de la información y de los canales de distribución surge la necesidad de realizar esta auditoría a los equipos pertenecientes a la red interna de la sucursal para minimizar los riesgos de pérdida, fuga o adulteración de la información.

* 1. Recursos

Recursos Humanos: El equipo de auditoría estará conformado por dos personas

Recursos Materiales: Dos Notebooks, Dos celulares, Cuaderno de Anotaciones, Bolígrafo, cámara fotográfica e impresora.

1. Análisis de Riesgos
   1. Definición

El análisis de Riesgos trata sobre como minimizar los efectos de un problema de seguridad; para esto se debe tener identificado claramente qué es lo se quiere proteger, contra qué, y cómo se lo va a proteger.

Se conocen dos alternativas para responder a estas inquietudes, una cuantitativa y otra cualitativa.

La cuantitativa se basa en cálculos complejos que implica la probabilidad de que un suceso ocurra y una estimación a las pérdidas en caso de que éste se de; el llamado “Coste Anual Estimado”, se obtiene del productos de estos términos, (EAC, Estimated Annual Cost), sin embargo, la inexactitud en el cálculo, a menudo hace difícil que esta alternativa sea tomada en cuenta.

El segundo método de análisis de riesgos es el cualitativo, últimamente muy difundido por las llamadas “consultoras de seguridad”, que se especializan en seguridad lógica, cortafuegos, tests de infiltración y similares. Este método toma en consideración realizar estimaciones de pérdidas potenciales, para lo cual relacionan cuatro puntos importantes:

* Las amenazas
* Las vulnerabilidades
* El impacto asociado a una amenaza
* Los controles o salvaguardas.

Con estos cuatro elementos se puede obtener un indicador cualitativo del nivel de riesgo asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

* 1. Evaluación de riesgos de la gestión de seguridad en la red

COBIT se sustenta en varias fuentes para la definición de su estándar, tales como normas, estándares y programas que cuentan con auspicio del gobierno de los Estados Unidos, entre ellos el Instituto de Estándares y Tecnología (NIST), del cual se tomará uno de los documentos emitidos como base para la realización del Análisis de Riesgos.

* 1. Metodología NIST800-30 para la Administración de Riesgos

“La Administración de Riesgos es el proceso de identificar, evaluar y ejecutar acciones para reducir el riesgo a un nivel aceptable”.

El Instituto de Estándares y Tecnología (NIST) liberó su publicación especial 800- 30 con recomendaciones para la administración de riesgo para los sistemas de información del cual se tomará los nueve pasos sugeridos para una correcta evaluación de riesgos. Estos son:

* Paso 1. Caracterización del Sistema.
* Paso 2. Identificación de la Amenaza.
* Paso 3. Identificación de Vulnerabilidad.
* Paso 4. Análisis del Control.
* Paso 5. Determinación de Probabilidad.
* Paso 6. Análisis del Impacto.
* Paso 7. Determinación del Riesgo.
* Paso 8. Recomendaciones de los Controles.
* Paso 9. Documentación de los Resultados.
  1. Identificación de Amenazas y Vulnerabilidades

Luego de identificados los recursos a proteger se deben identificar las vulnerabilidades y amenazas a que están expuestos. Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Las amenazas se catalogan en diferentes grupos según su impacto sobre los sistemas informáticos y la forma como se producen:

* 1. Desastres del entorno

Se refieren a problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Se toman en cuenta desastres naturales (terremotos, inundaciones, etc.), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.

* 1. Amenazas en el sistema

Se refieren a todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad, etc.

* 1. Amenazas en la red

Se debe tener en cuenta los aspectos relativos al cifrado de los datos que son sujetos de transmisión, protección de una red local de la Internet, sistemas de autenticación de usuarios remotos que accedan a ciertos recursos de la red interna.

Cabe anotar que para el análisis de las amenazas no solo se deben tomar en cuenta a los posibles atacantes externos (piratas informáticos, crakers) a la organización, sino que en la mayoría de los casos los potenciales ataques vienen desde el interior de la organización, debido principalmente a los pocos conocimientos sobre sistemas informáticos, seguridades y el trabajo en red básicamente.

Por otro lado, están también los actos accidentales, producidos por los mismos usuarios como pueden ser los borrados accidentales, fallas de programación, desconexión de cables de energía, etc.

* 1. Identificación de Amenazas

Previamente, se tendrán claramente definidos los conceptos de:

Amenaza: Posibilidad de ejercer de forma accidental o intencional una vulnerabilidad.

Vulnerabilidad: Debilidad que puede ser accidental o intencionalmente explotada.

Así, las posibles amenazas identificadas dentro de la red de datos de la empresa auditada son:

* + 1. Amenazas naturales
* Tormentas eléctricas.
  + 1. Amenazas humanas
* Acciones no intencionales como: Ingreso inadvertido de datos, mal uso de recursos.
* Acciones deliberadas como: ataques a la red, acceso no autorizado a información confidencial.
  + 1. Amenazas Medioambientales
* Falla en el Servicio de Energía.
* Falla en el Sistema de Comunicaciones.
* Falla de equipos y aplicaciones.
  1. Identificación de Vulnerabilidades
* No existe un documento específico de políticas de seguridad de TI.
* No existe un acuerdo de confidencialidad entre la empresa y el servicio técnico.
* No existe un plan de clasificación de información o en su lugar una pauta que tome parte en la determinación de cómo la información debe ser manipulada y protegida.
* No existe una acuerdo de confidencialidad o de no revelación de la información como parte de los términos y condiciones iniciales del empleo para el personal.
* No existe un procedimiento para verificar todos los boletines de advertencia e informativos con respecto al uso de software malicioso.
* No existe un procedimiento formal para reportar los incidentes que puedan presentarse en la red por los canales de administración apropiados tan pronto como sea posible.
* Los medios de respaldo y los procedimientos para su restauración no están guardados en un lugar seguro y lejos del sitio actual.
* No existe un procedimiento para el monitoreo y control del uso de los recursos de TI por parte los empleados.
* No existe un plan de contingencia establecido en caso de falla de equipos críticos para las operaciones del negocio.
* No existe un documento formal para el registro de la entrega o retiro de recursos de TI al personal.
* No hay respaldo para el fallo de equipos críticos.
* La BD no se encuentra almacenada en un sector restringido de la empresa.
* Los archivos de la empresa no se encuentran protegidos por contraseña.
* El firewall se encuentra desactivado.
* La licencia del antivirus ha caducado.
* El SO de unos de los terminales ya no cuenta con soporte ni actualizaciones.
* Existe una sobrecarga de conexiones en un solo tomacorrientes
* No existe un procedimiento de revisión periódica de archivos logs de los equipos.
* Las conexiones físicas de la red local no se encuentran adecuadamente estructuradas.
* Los usuarios no guardan confidencialidad de sus cuentas y passwords.
  1. Probabilidad de Impacto de la Amenaza

Para la definición de la probabilidad que una amenaza afecte a una vulnerabilidad se tomó como referencia la tabla de la NIST.

* + 1. DEFINICION DE PROBABILIDADES

|  |  |  |
| --- | --- | --- |
| **Nivel de Probabilidad** | **Ponderación** | **Definición** |
| Alto | 3 | El origen de amenaza es altamente motivado y suficientemente capaz, y los controles para prevenir que se ejerza la vulnerabilidad son ineficaces. |
| Medio | 2 | El origen de amenaza es motivado y capaz, pero los controles presentes pueden impedir que se ejerza con éxito la vulnerabilidad. |
| Bajo | 1 | El origen de amenaza carece de motivación o capacidad, existen controles para prevenir o por lo menos para impedir significativamente que se ejerza la vulnerabilidad. |

De igual manera para la definición del impacto se consideró la tabla proporcionada por la NIST que define la magnitud del impacto en niveles alto, medio y bajo. Cabe notar que para la definición de estos niveles se toma en cuenta los siguientes criterios de seguridad: integridad, disponibilidad y confidencialidad.

* 1. Definición de la magnitud del impacto

|  |  |  |
| --- | --- | --- |
| **Magnitud del Impacto** | **Ponderación** | **Definición** |
| Alto | 3 | (1) puede producir la pérdida costosa de recursos; |
|  |  | (2) puede dañar significativamente o impedir una misión de organización, su reputación o intereses; o |
|  |  | (3) puede resultar muerte o la lesión seria del personal. |
| Medio | 2 | (1) puede producir la pérdida costosa de activos tangibles o recursos; |
|  |  | (2) puede dañar, o puede impedir la misión de la organización, su reputación o intereses; o |
|  |  | (3) puede resultar en lesión del personal. |
| Bajo | 1 | (1) puede producir la pérdida de algunos recursos tangibles o recursos o |
|  |  | (2) puede afectar notablemente la misión de la organización, su reputación, o intereses. |

* 1. Determinación del Riesgo

La siguiente matriz se obtiene del producto entre los niveles de Probabilidad e Impacto definidos anteriormente, para conocer el riesgo que se aplica a la amenaza:

* + 1. MATRIZ DE PONDERACION DE RIESGOS

|  |  |  |  |
| --- | --- | --- | --- |
| Probabilidad de la Amenaza | Impacto de la Amenaza | | |
| Bajo (1) | Medio (2) | Alto (3) |
| Alto (3) | BAJO : 3 x 1 = 3 | MEDIO : 3 x 2 = 6 | ALTO : 3 x 3 = 9 |
| Medio (2) | BAJO : 2 x 1 = 2 | MEDIO : 2 x 2 = 4 | MEDIO : 2 x 3 = 6 |
| Bajo (1) | BAJO : 1 x 1 = 1 | BAJO : 1 x 2 = 2 | BAJO : 1 x 3 = 3 |

* 1. Resultado de la Evaluación del Riesgo

A continuación se presenta la Matriz de Evaluación de Riesgos, en donde se analizan cada uno de los recursos identificados considerados críticos, para cada uno de ellos se reconocen amenazas y vulnerabilidades, el control existente, su posible impacto y probabilidad de ocurrencia se reconoce a partir de la entrevista con el encargado de la sucursal y del checklist aplicado, el nivel de riesgo se obtiene de la aplicación de la matriz de ponderación anterior y finalmente se proponen las recomendaciones necesarias para alcanzar un control considerable.

* + 1. MATRIZ DE EVALUACION DE RIESGOS

| **Recurso** | **Amenaza** | **Vulnerabilidad** | **Control Existente** | **Impacto** | **Probabilidad** | **Nivel de Riesgo** | **Recomendación** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Equipos de conexión de Red y PC | Mal uso de recursos | No existe un documento específico de políticas de seguridad de TI. | Ninguno | Alto | Media | Medio | Definir un documento de políticas de seguridad para TI. |
| Equipos de conexión de Red y PC | Acceso no autorizado a información confidencial. | No existe un documento específico de políticas de seguridad de TI. | Ninguno | Medio | Media | Medio | Definir un documento de políticas de seguridad para TI. |
| Equipos de conexión de Red y PC | Acceso no autorizado | No existe un documento específico de políticas de seguridad de TI. | Ninguno | Alto | Media | Medio | Definir un documento de políticas de seguridad para TI. |
| Aplicaciones de red (Sistema) | Ingreso inadvertido o mal intencionado a datos | Las cuentas utilizadas en este sistema son creadas por área no por usuario. | Ninguno | Alto | Alta | Alto | Definir que la creación de cuentas y sus perfiles sea por empleado. |
| Aplicaciones de red (Sistema) | Acceso no autorizado a información confidencial | Los usuarios no guardan confidencialidad de sus cuentas y passwords. | Los usuarios conocen su responsabilidad sobre la no divulgación de sus cuentas. | Alto | Baja | Bajo | Reforzar la conciencia de responsabilidad de los usuarios sobre el uso de sus cuentas. |
| Aplicaciones de red (Sistema) | Ingreso inadvertido de datos | Definición o asignación errónea de perfiles de usuario. | Ninguno | Alto | Baja | Bajo | Revisión periódica de las cuentas existentes y sus perfiles. |
| Equipos de conexión de Red y PC | Acceso no autorizado a información confidencial | No existe una política de requerimientos de seguridad en contratos con terceros. | Ninguno | Alto | Media | Medio | Añadir cláusulas de confidencialidad de la información en los contratos establecidos con compañías externas. |
| Equipos de Circuito Cerrado | Acceso no autorizado a información confidencial | No existe una política de requerimientos de seguridad en contratos con terceros. | Ninguno | Alto | Media | Medio | Añadir cláusulas de confidencialidad de la información en los contratos establecidos con compañías externas. |
| Aplicaciones de red (Sistema) | Mal uso de recursos y acceso no autorizado | No existe un plan de clasificación de información o una pauta que tome parte en la determinación de cómo la información debe ser manipulada y protegida. | La información considerada clave para un usuario es almacenada en una PC, sin controles de acceso restringido. | Alto | Media | Medio | Elaborar el plan de clasificación de la información y dar a conocer a los involucrados. |
| Aplicaciones de red (Sistema) | Mal uso de recursos y acceso no autorizado | No existe una acuerdo de confidencialidad o de no revelación de la información como parte de los términos y condiciones iniciales del empleo para el personal. | Ninguno | Medio | Alta | Medio | Elaborar un acuerdo de confidencialidad que sea parte de contrato de empleo. |
| Servidor (Pen drive) | Ataque a la red | No existe un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible. | Reportes informales | Alto | Media | Medio | Establecer un procedimiento de formal para reportar incidentes de seguridad. |
| Servidor (Pen drive) | Mal uso de recursos | No existe un servidor dedicado donde sea almacenado el sistema principal | Almacenado en una unidad extraíble (pen drive) | Alto | Alta | Alto | Adquirir un equipo destinado al almacenamiento del sistema. |
| Servidor (Circuito Cerrado) | Mal uso de recursos | No existe un servidor especifico donde sea almacenado el sistema principal | Almacenado en una PC de uso diario | Alto | Alta | Alto | Adquirir un equipo destinado al almacenamiento de las grabaciones del circuito cerrado. |
| Servidor (Pen drive) | Acceso no autorizado a información confidencial | No existe un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible. | Reportes informales | Alto | Media | Medio | Establecer un procedimiento de formal para reportar incidentes de seguridad. |
| Equipos de conexión de Red | Ataque a la red y mal uso de recursos | No existe un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible. | Reportes informales | Alto | Media | Medio | Establecer un procedimiento de formal para reportar incidentes de seguridad. |
| PC | Carga de software malicioso | La licencia del antivirus ha caducado. | Ninguno | Medio | Media | Medio | Adquirir licencias para cada equipo. |
| PC | Carga de software malicioso | El firewall se encuentra desactivado. | Ninguno | Medio | Media | Medio | Activar el firewall de cada equipo y realizar actualizaciones periódicas. |
| Servidor (Pen drive, Circuito Cerrado) y PC | Mal uso de recursos | Los medios de respaldo y los procedimientos para su restauración no están guardados en un lugar seguro y lejos del sitio actual. | Algunos respaldos existen pero se guardan dentro de la oficina. No existen procedimientos de restauración. | Alto | Media | Medio | Almacenar los respaldos en un lugar externo a la empresa. Establecer procedimientos de restauración de datos. |
| PC | Mal uso de recursos | No existe un procedimiento para el monitoreo y control del uso de los recursos de TI por parte los empleados. | Ninguno | Medio | Alta | Medio | Definir un documento para monitorear el uso de los recursos de TI. |
| Servicio de Internet | Mal uso de recursos | No existe un procedimiento para el monitoreo y control del uso de los recursos de TI por parte los empleados. | Ninguno | Medio | Alta | Medio | Definir un documento para monitorear el uso de los recursos de TI. |
| Servidor, PC, Servicio de Internet, Equipos de Conexión de Red, Equipos de Circuito Cerrado | Tormentas Eléctricas | No existe un plan de contingencia. | Ninguno | Alto | Alta | Alto | Establecer un plan de contingencia que contemple amenazas naturales. |
| Servidor, Equipos de Conexión de Red, Equipos de Circuito Cerrado | Ataque a la red | No existe un plan de contingencia. | Ninguno | Alto | Alta | Alto | Establecer un plan de contingencia que contemple este tipo de amenazas. |
| Aplicaciones en red | Ataque a la red | No existe un plan de contingencia. | Ninguno | Alto | Alta | Alto | Establecer un plan de contingencia que contemple este tipo de amenazas. |
| Sistema de UPS | Falla en servicio de energía. | No existe un plan de contingencia. | El sistema de UPS actual es casi obsoleto. | Alto | Media | Medio | Crear un plan de contingencia para cubrir este tipo de amenazas. Adquirir nuevos equipos. |
| Servicio de Internet | Falla en el sistema de comunicaciones. | No existe un plan de contingencia. | Ninguno | Alto | Media | Medio | Establecer un plan de contingencia que contemple este tipo de amenazas. |
| PC, Equipos de conexión de Red y Equipos de Circuito Cerrado | Mal uso de recursos. | No existe un documento formal para el registro de la entrega o retiro de recursos de TI al personal o terceros. | Ninguno | Bajo | Baja | Bajo | Elaborar un documento de entrega y recepción de recursos. |
| Servidor, PC, Equipos de Conexión de Red, Equipos de Circuito Cerrado | Falla de equipos y aplicaciones. | No hay respaldo para el fallo de equipos críticos. | Ninguno | Alto | Media | Medio | Adquirir equipos de respaldo. |
| Servidor | Ataque a la red, mal uso de recursos y carga de software malicioso. | No existe un procedimiento de revisión periódica de archivos logs de los equipos. | Ninguno | Bajo | Baja | Bajo | Definir un procedimiento para la revisión periódica de los logs. |
| Servidor (Pendrive) | Mal uso de recursos. | La BD no se encuentra en un lugar restringido de la empresa. | La BD está almacenada en un equipo con acceso a funcionarios | Alto | Alta | Alto | Almacenar la BD en un lugar restringido con acceso solo a personal autorizado. |
| PC, Equipos de conexión de Red | Mal uso de recursos. | Los archivos de la empresa no se encuentran protegidos por contraseña. | Ninguno | Alto | Media | Medio | Definir políticas para la creación de contraseñas seguras de los archivos de la empresa. |
| Correo Electrónico | Mal uso de recursos. | No existe un procedimiento formal para el monitoreo y control del uso del recurso. | Ninguno | Medio | Alta | Medio | Definir políticas sobre uso de correo, negar envío de cadenas, de información no laboral, posible fuente de virus y pérdida de datos. |
| Servicio de Internet | Mal uso de recursos. | No existe un procedimiento formal para el monitoreo y control del uso del recurso. | Ninguno | Medio | Alta | Medio | Definir nuevas políticas sobre uso de internet, restringir el acceso, posible fuente de virus y pérdida de datos. |
| PC | Mal uso de recursos. | El SO de uno de los terminales ya no cuenta con soporte ni actualizaciones. | Ninguno | Medio | Media | Medio | Actualizar el SO de los equipos y adquirir las licencias correspondientes. |
| PC, Equipos de conexión de Red | Mal uso de recursos. | Existe una sobrecarga de conexiones en un solo tomacorrientes | Ninguno | Alto | Media | Medio | Realizar un reordenamiento de las conexiones eléctricas. |
| PC, Equipos de conexión de Red | Mal uso de recursos. | Las conexiones físicas de la red local no se encuentran adecuadamente estructuradas. | Ninguno | Alto | Media | Medio | Reestructurar el cableado de la red local, canaletear y adquirir un Rack para los equipos de conexión de red. |