

Instituto Tecnológico y de Estudios Superiores de Monterrey

ESCUELA DE INGENIERÍA Y CIENCIAS

INGENIERÍA EN CIENCIA DE DATOS Y MATEMÁTICAS

MA2002B: ANÁLISIS DE CRIPTOGRAFÍA Y SEGURIDAD

AUDITORÍA DE SEGURIDAD Y PLAN DE MITIGACIÓN: CASO HOTEL

Autores:

Miguel Ángel Chávez Robles - A01620402

Arnulfo Andrés Treviño Galán - A00828184

Luis Leopoldo Jiménez Pérez - A01275004

Gerardo del Valle Cuéllar - A01284200

Diego Paasche Portillo - A01028103

Pedro Alan González Arámbula - A01625308

Profesores:

Dr. Alberto Francisco Martínez Herrera

Dr. Jonathan Montalvo Urquizo

Socio Formador: Kaspersky

Monterrey, Nuevo León

11 de Octubre 2021

Índice

1. Introducción	3
2. Contexto general	4
3. Delimitación del objeto de estudio	4
4. Planteamiento del problema	5
5. Justificación	6
6. Marco teórico	6
6.1. Seguridad de red.	6
6.2. Seguridad de aplicaciones.	6
6.3. Seguridad de la información.	7
6.4. Recuperación ante desastres y la continuidad del negocio.	7
6.5. Malware.	7
6.5.1. Virus.	7
6.5.2. Ransomware.	7
6.5.3. Spyware.	7
6.5.4. Adware.	7
6.5.5. Troyanos.	7
6.5.6. Botnets.	8
6.6. Phishing.	8
6.7. Ataque de inyección SQL.	8
6.8. Ataque de denegación de servicio.	8
7. Objetivos	8
7.1. Objetivo general	8
7.2. Objetivos específicos	8
8. Hipótesis	9
9. Recursos utilizados	9
10. Etapa 1. Levantamiento de Inventario	9
10.1. Inventario	10
11. Etapa 2. Diseño e implementación de un plan de evaluación	11

12.Etapa 3	17
12.1. Definición de las vulnerabilidades	17
12.2. Medidas	17
12.2.1. MySQL	17
12.2.2. Firewall	18
12.2.3. Protocolos	19
12.2.4. Antivirus	19
12.2.5. Copias de Seguridad	20
12.2.6. Protección del Hardware	20
12.2.7. Reportes Post Mortem	22
12.3. Costos del Plan de Mitigación	22
12.3.1. Cotización Azure	22
12.3.2. Cotización AWS	23
12.4. Costo final del plan de mitigación	26
13.Etapa 4. Discusión, conclusiones y evaluación final.	26
13.1. Técnicas y herramientas de ingeniería empleadas	26
13.2. Infraestructura	27
13.3. Conclusiones	27

Índice de figuras

1. Diagrama de red de activos principales.	12
2. Diagrama otros activos	15
3. Diagrama de red final.	24

Resumen

Hoy en día la falta de preparación sumada a la poca inversión de las PyME suponen un blanco fácil de ataques cibernéticos, lo que en gran medida puede afectar su economía y del país. El objetivo de este reporte es presentar una propuesta de mejora al diseñar una auditoría de ciberseguridad y plan de mitigación viable técnica y económicamente para una PyME hotelera partiendo del análisis de vulnerabilidad de activos implementable a corto o mediano plazo.

La metodología empleada se divide en:

- Etapa 1. Levantamiento de Inventario.

Realización de inventario de la infraestructura tecnológica, generando una base de datos SQL, de tangibles e intangibles.

- Etapa 2. Diseño e implementación de un plan de evaluación.

Análisis de las vulnerabilidades de activos y creación de un diagrama de redes.

- Etapa 3. Plan de Mitigación.

Creación de plan estratégico y análisis del costo de implementación.

- Etapa 4. Discusión, conclusiones y evaluación final.

El plan considera una protección para 117 activos tangibles y 9 activos no tangibles, suponiendo un total de 31 empleados, siendo capaz de mitigar del 90 % al 100 % de las vulnerabilidades, pensado a un plazo de un año a un costo total recurrente de \$23,761.46 MXN usando herramientas tecnológicas como AWS y prácticas de seguridad como principio de mínimo privilegio. El impacto principal es la protección tecnológica de una PyME hotelera, salvaguardando sus activos fijos y circulantes siendo posible su adaptación a empresas del mismo giro y tamaño.

1. Introducción

La expansión de las tecnologías informáticas han demostrado ser una de las revoluciones tecnológicas más importantes de la historia debido a su distribución tan rápida y generalizada desde su nacimiento; la sociedad actualmente depende profundamente de sistemas informáticos para procesos industriales, económicos, en realidad se puede decir que son empleados para la gestión de casi cualquier actividad. Estas nuevas herramientas además de comodidad y utilidad han generado nuevas amenazas para la integridad y privacidad; debido a que estos sistemas a menudo albergan información patrimonial o procesos industriales, se han generado un gran interés en atacantes debido a lo lucrativo que puede parecer, sumado a que con normalidad es complicado identificar al responsable de estos ataques.

La dependencia a estas tecnologías afecta inclusive a infraestructuras vitales de países, estos sistemas constituyen el núcleo de naciones enteras; para que todo este ecosistema funcione de forma correcta el ciberespacio es fundamental, por consecuente para la soberanía de instituciones e inclusive naciones. Sin embargo, la globalización del internet provoca que las fronteras de la red sean permeables y con ello, que los ataques hacia sistemas informáticos generan mucho daño con poco riesgo para el atacante.

Contemplando el panorama de las amenazas y la importancia de los sistemas informáticos, se ha generado la necesidad de proteger estos mismos. La ciberseguridad se define como: “la práctica de defender los computadores, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.” [1]

Un gran blanco ante las amenazas del mundo cibernético son las PyME. Las PyME tienen una importancia vital en la economía debido a la flexibilidad de adaptarse a cualquier cambio ya sea tecnológico o no, seguido a que generan una gran cantidad de empleos, aportan a la producción y la distribución de bienes y servicios a la población. Estas son la base de la economía mexicana y mundial. Dentro de México estas son un pilar financiero al conformar la gran mayoría de las empresas del país.

Tomando en cuenta todos los factores anteriormente mencionados, se puede ver la responsabilidad de las PyME en materia de ciberseguridad ya no solo como un elemento extra de su operación sino como una parte fundamental en la misma, por lo que este debe tomarse en cuenta al inicio de cualquier emprendimiento, entre más segura se encuentre la operación e información de una empresa como la de sus clientes, más sólido será el crecimiento de esta misma.

2. Contexto general

Hoy en día la falta de preparación de las PyME suponen un blanco fácil de ataques cibernéticos, lo que en gran medida puede afectar su economía y la del país. Generalmente las PyME no tienen la madurez suficiente tanto en cuestiones de seguridad operacional como de infraestructura, por lo que es vital que estas sepan responder adecuadamente ante un ataque tanto interno como externo, para ello deben ser conscientes de que vulnerabilidades tienen y que información desean proteger.

En 2018 el costo promedio de recuperación para una empresa tras recibir un ciberataque en México era de 2.5 millones de pesos esto incrementó en un 38.4% para un total de 6.5 millones de pesos en 2019. [2]

A raíz de la pandemia Covid-19 se ha evidenciado de manera significativa la necesidad de inversión de las empresas mexicanas en procesos y herramientas digitales en pro de aumentar su competitividad y satisfacer las demandas del mercado sin embargo este crecimiento se traduce en una mayor exposición de riesgo, por lo que la ciberseguridad se convierte en una prioridad para preservar de forma adecuada sus operaciones y finanzas. [2]

3. Delimitación del objeto de estudio

Para este caso se considera el inventario de un hotel mediano, el personal del hotel cuenta con 31 miembros en sus filas además de contar con los servicios básicos de un hotel. En la zona de recepción existen 2 computadoras y 2 codificadores magnéticos, 6 elementos de personal, contando al jefe de departamento. Esto debido a la necesidad de tener empleados capaces de trabajar en esta área sobre todo en temporadas altas, para las cuales se requiere una cantidad considerable de personal. El hotel cuenta con 30 habitaciones para huéspedes las cuales cuentan, cada una con teléfono, acceso a internet inalámbrico, un televisor y una

cerradura electrónica que permite el acceso a la habitación.

4. Planteamiento del problema

Son necesarias 4 personas encargadas de la limpieza y un jefe de personal para todo el hotel. Un encargado de limpieza es capaz de limpiar 10 cuartos diarios, lo que implica que diariamente estarán 3 personas encargadas de la limpieza y la persona restante es utilizada para cumplir con una rotación de empleados y estar en días libres de los otros tres.

Es necesario considerar el restaurante del hotel, en este se encuentra el personal de meseros y cocineros que deban de ser suficientes para las comidas del día y cuenta con una PC en cocina la cual permite la administración de las ordenes de los huéspedes. Además de todos los anteriormente mencionados, existe el personal de mantenimiento que se encarga de todos los equipos que puedan tener averías, como también de procurar que todo funcione correctamente. Los equipos incluyen el aire acondicionado, la iluminación, los sistemas de calefacción, la red hidráulica, los equipos de cocina, los aparatos electrónicos, etc. El equipo debe de ser capaz de dar mantenimiento preventivo que todo tenga un plan y que reduzca costos por cosas que se tengan que reemplazar por no haber prevenido. Un caso parecido ocurre con el equipo de sistemas, el cual se encarga de que funcionen correctamente los servidores con los datos de los clientes y el personal, mantenimiento de hardware, software y documentación de los sistemas, cabe destacar que la administración del área de sistemas es realizada a través de un Laptop, dentro de este ámbito se espera que el hotel cuente con una página web en la que los clientes puedan ver la información del mismo y realizar reservaciones. Sin embargo esta no puede usarse para realizar pagos en línea debido a la carencia de infraestructura para realizar estas transacciones; permitir esta función implica un trámite muy largo y una madurez empresarial que la PyME no tiene.

El hosting de la página web se hace por medio de una PC de servidor cuya única función es mantener esta en funcionamiento así como las bases de datos asociadas a esta, al igual que monitorear el tráfico interno de la red de invitados y empleados siendo llevado a cabo este proceso a través de un proxy, mientras existe una Laptop la cual es utilizada para la administración de la página, además el hotel debe contar con un Switch de redes dentro del departamento de sistemas el cual cuenta con su propia cerradura electrónica, lo que permite separar la red interna que maneja el hosting de la administrativa la cual se maneja en recepción y por los visitantes, existe un Router inalámbrico administrativo por el cual pasará todo el tráfico de relevancia para el hotel. Por último, se encuentra el gerente general el cual se encarga de administrar todas las áreas y verifica que todo el establecimiento se encuentre en buen funcionamiento, este proceso administrativo se lleva a cabo a través de una Laptop perteneciente al área de gerencia cuyo control está llevado únicamente por el gerente general.

Es importante destacar los activos intangibles de T.I. pertenecientes a la empresa como son las subredes administrativa como de visitantes, las cuales permiten reducir el tamaño de los dominios como también permitir una mejor administración de la red, cómo también permite segmentar el uso de la red en departamentos en caso de ser necesario.

Cada establecimiento genera información, esta debe ser propiamente resguardada y para ello se emplean 3 bases de datos diferentes las cuales se dividen en base de datos de huéspedes, empleados y activos de la empresa. Esto permite almacenar la información requerida según sea la base de datos correspondiente, es decir, la base de datos de empleados almacena la información personal de cada empleado permitiendo gestionar el personal. También se cuenta con una licencia de software para la administración del restaurante, y el hotel cuenta con 5 licencias de Windows Pro, esto debido a que las políticas de administración de grupos permiten controlar los permisos individuales de cada usuario, teniendo a estos en contenedores de un sistema provocando que cada usuario en lugar de tener libertad del sistema solo tenga permisos mínimos para la realización de sus labores. Una licencia de Windows 10 server 2019, el cual es un sistema operativo de servidor que permite realizar funciones de red como servidor de impresión, controlador de dominio, servidores web, servidores de archivos, etc, además que funciona como plataforma para aplicaciones como SQL Server.

5. Justificación

En los últimos años, diversos atacantes han vulnerado las redes de diversas empresas hoteleras de alta importancia, lo que ha comprometido datos de millones de huéspedes, esta industria es un blanco notable debido al manejo de grandes cantidades de dinero e información valiosa de métodos de pago; por lo tanto es importante preservar la integridad de la información manejada por estas empresas, debido a esto se ha focalizado este proyecto de ciberseguridad en la elaboración de un plan de mitigación dirigido a este tipo de giro empresarial.

6. Marco teórico

6.1. Seguridad de red.

La seguridad de red según cisco se define como: “cualquier actividad diseñada para proteger acceso, el uso y la integridad de la red y los datos corporativos. Incluye tecnologías de hardware y software, está orientada a diversas amenazas, evita que ingresen o se propaguen por la red, la seguridad de red eficaz administra el acceso de la red”. [3]

6.2. Seguridad de aplicaciones.

Se refiere a las medidas de seguridad empleadas a nivel de aplicación como el proceso de desarrollo, añadir o probar características de seguridad, con el objetivo de impedir el robo/secuestro de datos o código dentro de la aplicación, esta puede incluir hardware, software y procedimientos de identificación o minimización de vulnerabilidades. [4]

6.3. Seguridad de la información.

La seguridad de la información se refiere a procesos y herramientas diseñados para la protección de información comercial confidencial de una invasión. [5]

6.4. Recuperación ante desastres y la continuidad del negocio.

Es la capacidad de una organización de responder a incidentes de seguridad informática o evento cualquiera que cause de forma parcial o total el detenimiento de operaciones lo cual genere pérdida de datos e información. [6]

6.5. Malware.

Se define como software malicioso que dentro del ordenador puede causar diversos daños, como controlar el equipo o monitorear actividades. Existen diversos tipos de malware los cuáles son [7]:

6.5.1. Virus.

Programas informáticos maliciosos que tienen como objetivo la alteración del ordenador sin que el usuario note su presencia, este es capaz de reproducirse e incrustarse en un archivo limpio. [7]

6.5.2. Ransomware.

Programa o software malicioso que infecta programas y/o archivos, teniendo capacidad de bloquear pantalla de un ordenador o cifrar archivos predeterminados con una contraseña, generalmente se muestra un mensaje exigiendo un pago de rescate para restablecer el sistema o no borrar los archivos infectados. [8]

6.5.3. Spyware.

Programa cuya función es recabar información sobre un dispositivo o red para luego enviarla al atacante, este suele ser usado para supervisar actividades en internet de una persona y recopilar datos personales o datos sensibles varios. [8]

6.5.4. Adware.

Programa cuya función es generar ingresos para el atacante sometiendo a la víctima a publicidad no deseada, generalmente el adware es instalado de forma legal sin embargo no deja de ser molesto. [8]

6.5.5. Troyanos.

Software malicioso que se infiltra al dispositivo de una víctima presentándose como software legítimo de tal forma que ya instalado el troyano se activa incluso llegando a descargar otros tipos de malware adicional. [8]

6.5.6. Botnets.

Una red de robots capaces de desarrollar o ejecutar malware, estos “bots” forman una red utilizada para coordinar ataques, enviar spam, robar datos e inclusive generar anuncios falsos en el navegador. [8]

6.6. Phishing.

Técnica de ciberdelincuencia que utiliza el fraude, engaño para manipular a las víctimas haciendo que manipulen información personal confidencial, se realiza a través de correo electrónico o llamadas de teléfono, se basa en hacerse pasar por una persona u organización de confianza el objetivo es obtener información confidencial como credenciales o números de tarjeta de crédito. [9]

6.7. Ataque de inyección SQL.

Tipo de ataque cibernético, que se basa en un ”método de infiltración de un código intruso, que aprovecha una entrada vulnerable presente en aplicaciones, esto en el nivel de validación de entradas, al momento de realizar consultas de bases de datos.” [10]

6.8. Ataque de denegación de servicio.

Tipo de ataque cibernético que consiste en la inyección de paquetes falsos (en grandes cantidades) de manera que los componentes del sistema se sobrecarguen y con ello, no sean capaces de procesar tantas solicitudes. [11]

7. Objetivos

7.1. Objetivo general

Realizar un plan de mitigación para una PyME con las especificaciones mencionadas en la sección [3] que sea capaz de cubrir entre el 90 % y 100 % de las vulnerabilidades encontradas, con un costo que justifique el retorno de inversión.

7.2. Objetivos específicos

- Identificar los activos tecnológicos tangibles y no tangibles de la empresa que se desean proteger.
- Levantar un inventario de activos que contenga una descripción del activo, así como su ubicación en la empresa (si aplica) y quien es el responsable directo del mismo.
- Realizar un análisis de vulnerabilidades sobre los activos encontrados, este análisis debe considerar ataques hechos tanto por internos como por externos.
- Proponer una solución así como las herramientas necesarias ante las vulnerabilidades encontradas.

8. Hipótesis

Las PyME específicamente del giro hotelero, son un sector muy vulnerable ante amenazas de carácter informático debido a su falta de preparación e inversión en ciberseguridad. El plan de mitigación plantea la posibilidad de proteger a estas de un posible ciber-ataque y permitir a la empresa reaccionar ante estos, permitiendo que esta tenga continuidad de negocio; idealmente la protección es suficiente para que no exista un paro en las actividades y cuando este suceda se busca que el tiempo de paro sea mínimo, pues la infraestructura implementada debe ser suficiente para reanudar las operaciones lo más pronto posible.

9. Recursos utilizados

Existe una gran variedad de herramientas que ayudan a administrar el inventario, por lo cual se tuvo que realizar un análisis considerando lo que cada herramienta proporciona buscando siempre qué era lo que más funcionaría en la situación problema. Al final se decidió que la herramienta que va a utilizar para realizar el inventario es MySQL a través del cliente phpMyAdmin. Es una de las herramientas más conocidas de administración de bases de datos, que su principal fortaleza es que es sencilla de utilizar, además de que no genera costos, es multiplataforma, por lo que se puede utilizar en cualquier sistema operativo, y tiene buenos mecanismos de conectividad con el servidor. La información de las bases de datos se puede proteger por medio de contraseñas y tiene como opción complejos algoritmos de encriptación que protegen bien la información. Utilizar MySQL es una ventaja significativa para poder controlar el orden del hotel debido a que es la herramienta indicada para realizar este inventario (Automático y bajo costo, además de enormemente consistente). La única desventaja es que el inventario se maneja a nivel local, por lo que esta base de datos no es accesible desde un servidor externo.

La bibliografía utilizada sirvió para definir el problema adecuadamente, así como para identificar que soluciones tecnológicas son adecuadas para la empresa según sus funciones y precios, de manera que esta sea capaz de cubrir las necesidades del cliente sin suponer un sobreprecio o un compromiso de seguridad.

Adicionalmente se trabajó de la mano con un experto de ciberseguridad en Kaspersky, quien brindó asesorías semanales durante la realización del proyecto, resolviendo dudas puntuales en cuanto a aspectos básicos de ciberseguridad, tecnologías específicas, e implementación de soluciones, apoyándonos enormemente en su experiencia en el sector y conocimiento.

10. Etapa 1. Levantamiento de Inventario

En la primera sección del proyecto el objetivo es seleccionar aquellos elementos pertenecientes a un hotel que formen parte de la cuenta de activos, con el objetivo de realizar un inventario en el cual se reflejen estos bienes.

El contar con un inventario es uno de los requerimientos más indispensables en la practica laboral de una empresa, esto debido a múltiples razones, se necesita un inventario para poder llevar control de nuestros activos, saber si estos están en funcionamiento, las condiciones en las que se encuentran, el sitio en el que

están, además de llevar un registro de costos e inclusive saber parte del personal usa estos activos. Por otro lado, un inventario tiene que tener establecido de forma clara que parte de los activos son tangibles como intangibles debido a que desde un punto de vista de seguridad informática, esto permite una segmentación en los ataques recibidos.

En la realización de la situación problema el inventario seleccionado será el de recursos en tecnología computacional, considerando a los trabajadores, los cuales son los encargados de las diferentes secciones donde se encuentra este recurso computacional, los activos tangibles son aquellos que tienen una forma física como lo son computadoras, televisiones, etc; fueron considerados debido a que estos medios pueden ser atacados debido a que en la mayoría de los casos estos se encuentran conectados a una señal inalámbrica, los activos intangibles son aquellos que no tienen una naturaleza física como lo son los dominios web o software utilizado e incluso bases de datos con información del establecimiento, la principal razón de tener enfoque en este tipo de activos es que estos pueden contar con información sensible de la empresa que sería el principal objetivo de ataques realizados a dichos bienes.

10.1. Inventario

En la sección 4 se mencionaron algunos puntos a tomar en cuenta para realizar el inventario del hotel, desde lo que son los activos destinados para el personal, hasta lo que corresponde a las comodidades para los huéspedes. Entonces después de evaluar las herramientas para realizar el inventario, se generó una base de datos de todos los activos en MySQL. Esta se separó en dos primero especificando los activos tangibles y luego los intangibles con un campo por cada activo. En la de activos tangibles se encuentran lo que son las computadoras, las Laptops, cerraduras, televisión, Routers y terminales de pago. En donde primero se especifica qué es, después la marca, una pequeña descripción, el cuarto en el que se encuentra, sistema operativo si es que ocupa, la dirección MAC, y por último el personal del hotel que se va a encargar de su administración. En cuanto a los activos intangibles, estos tienen características diferentes que involucran su nombre, tipo, descripción y a que activo tangible están ligados (cuando aplica) . En este apartado se tomaron en cuenta los diferentes software que se necesitan para las Laptops y el servidor, así las bases de datos administrativas y de huéspedes. Se identificaron 117 activos tangibles y 9 intangibles.

11. Etapa 2. Diseño e implementación de un plan de evaluación

En la etapa 2 del reto se pidió crear el diseño e implementación de un plan de evaluación. En este plan de evaluación se pudo crear una tabla en donde se escribe todo tipo de posible problema que pueda existir con la PyME y la prevención que se usaría para que no ocurriera ningún problema. Luego se demuestran figuras y diagramas en donde se muestra como vamos a conectar la red para que este en manos seguras la PyME.

En un hotel pueden existir muchas problemáticas debido a su extenso nivel de red necesaria para poder operar especialmente en estos tiempos. Unos ejemplos más comunes de problemáticas es el robo de discos duros en el que los podemos encriptar para poder prevenir robo de información a nivel físico. Otro de los posibles problemas sería el robo de bases de datos, pero esto se puede mitigar aplicando correctos principios de autenticación y autorización. Debido a lo extensa que es la red de un hotel presentaremos más de 30 problemáticas en las que todas tendrán una prevención ejemplar para que puedan evitar algún tipo de robo de información o robo económico.

Los datos que se busca proteger dentro del hotel son:

- Información de medios de pago.
- Información de clientes.
- Información de empleados.
- Información de administración (planes de mkt, proyectos futuros, etc).
- Información financiera del hotel.
- Información de activos tecnológicos

En la figura 11 podemos observar un diagrama con todos los activos que se encuentran conectados a internet, con la jerarquía de conexiones entre sí. Empezando desde lo más importante que es el internet, este proporciona señal a cuatro Routers del hotel, con uno en el que primero existe un Firewall que protege el tráfico de datos. Algo que no está representado son los dispositivos de los huéspedes, pero se entiende como que llegan de los Routers señalados con naranja al Switch donde conectan a la red de visitantes. Todo lo rojo representa la red usada en los procesos administrativos del hotel, en el que están conectadas las terminales de pago y las computadoras del personal. Y como procesos especiales se encuentran: la red de administración de la página web señalada con verde, en la que está la Laptop de el administrador de la página web y la computadora de servidor misma. La red denotada con morado es para uso del administrador de sistemas, puede monitorear la red de visitantes desde la misma. Por último, la red denotada con azul tiene acceso a todas las redes anteriores, pues es del administrador general.

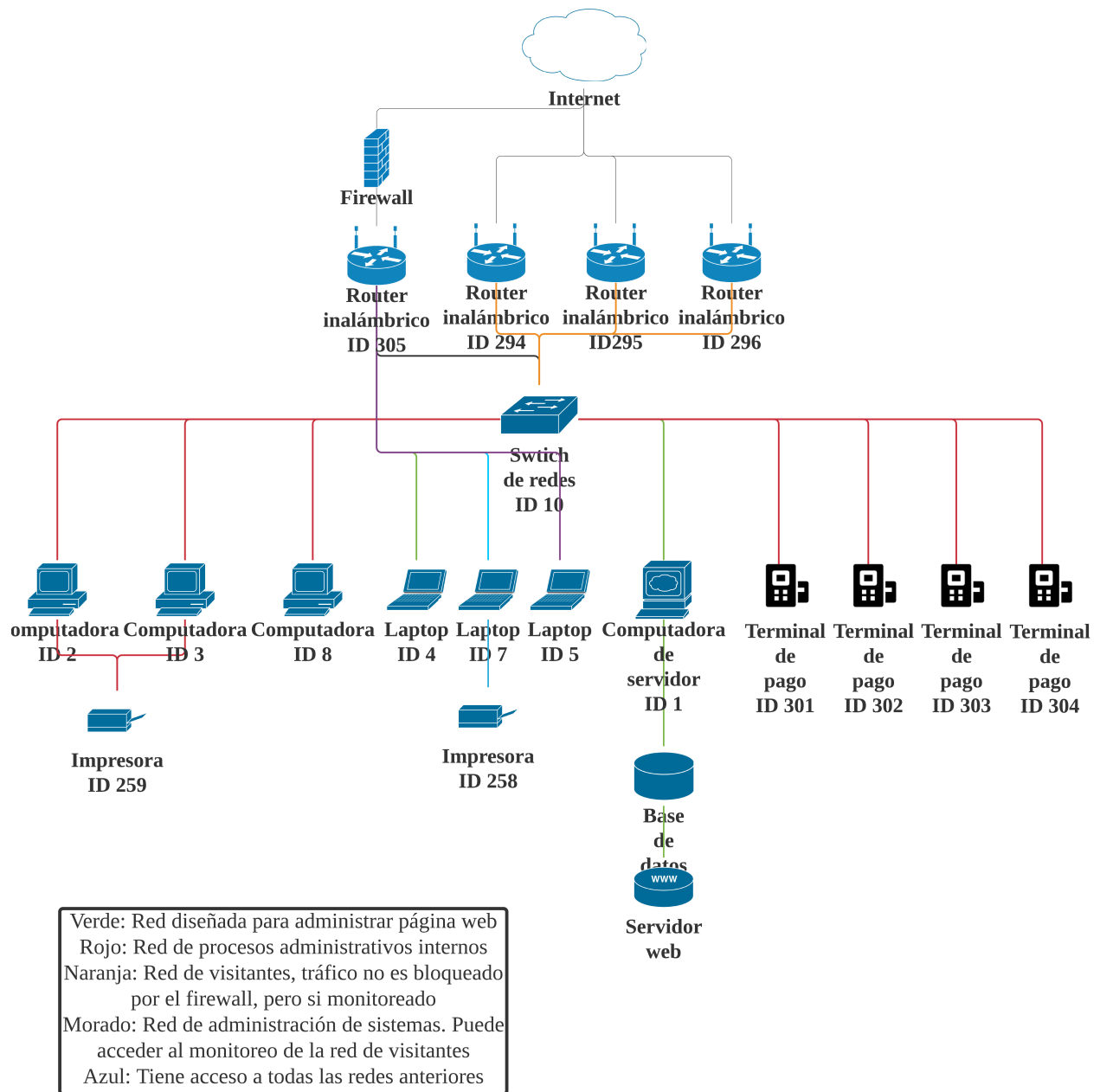


Figura 1: Diagrama de red de activos principales.

En la tabla [11](#) se presenta un listado de las posibles problemáticas encontradas por el equipo en el escaneo de amenazas preliminar. Este listado es específico a la red demostrada en la figura [1](#). Dentro de la misma, se empareja cada problemática con la solución propuesta por el equipo. Es importante tomar en cuenta que las problemáticas desplegadas no son necesariamente todas las existentes en la red.

Problemática	Prevención
Robo de discos duros.	Encriptar discos duros.
Dispositivo no autorizado se conecta a Router administrativo de forma alámbrica.	Deshabilitar interfaces no conectadas de forma directa al Switch y poner el Router en cuarto de sistemas bajo llave.
Dispositivo no autorizado se conecta a Router administrativo de forma inalámbrica.	Uso de Firewall y contraseña de red WPA2. Implementar un sistema IPS/IDS.
Dispositivo no autorizado se conecta a Switch.	Deshabilitar interfaces del Switch que no estén en uso. Implementar un sistema IPS/IDS.
Dispositivo no autorizado se conecta a red de visitantes	Contraseña de la red WPA2. Implementar un sistema IPS/IDS.
Instalación de dispositivo físico capaz de robar información de tarjetas en terminales.	Inspección física de terminal para verificar que todo este en orden.
Robo de información por medio de navegación por internet.	Firewall permita unicamente tráfico bajo el protocolo HTTPS.
Ataques DDoS.	Uso de antispam, Firewall.
Inyección de código a la página web.	Filtros a nivel capa de aplicación que prohíban este tipo de acciones.
Robo de base de datos.	Asegurar servidor y correr verificaciones de integridad en la misma.
Acciones maliciosas realizadas por personal del hotel.	Aplicar el principio de mínimo privilegio.
Instalación de malware.	Uso de antivirus.
Spoofing.	Esconder SSID, lo que permite que solo la persona que necesita saber el nombre lo sepa.
Robo de datos a través de rubber ducky.	Desactivar puertos USB que no sean de uso esencial.
Robo de información por parte de empleados.	Definir políticas de seguridad que prohíban el uso de dispositivos electrónicos personales así como también cualquier dispositivo que sirva para capturar información.
Suplantación de identidad de empleados.	Todo empleado debe portar una identificación oficial de la empresa de manera visible en todo momento.
Personal en áreas en las cuáles no esté autorizado	Restringir el acceso a ciertas áreas con identificación de los empleados.

Ransomware bloqueando la infraestructura entera.	Manejar backups en frio de la infraestructura entera, realizados cada dos semanas.
Servicio de electricidad cortado de forma intencional para acceder a sala de servidores.	Poner equipo bajo llave.
Filtración de información de acceso a cuentas de administración.	Cambio de contraseñas cada mes.

Tabla 1: Tabla de problemáticas y prevenciones preliminares

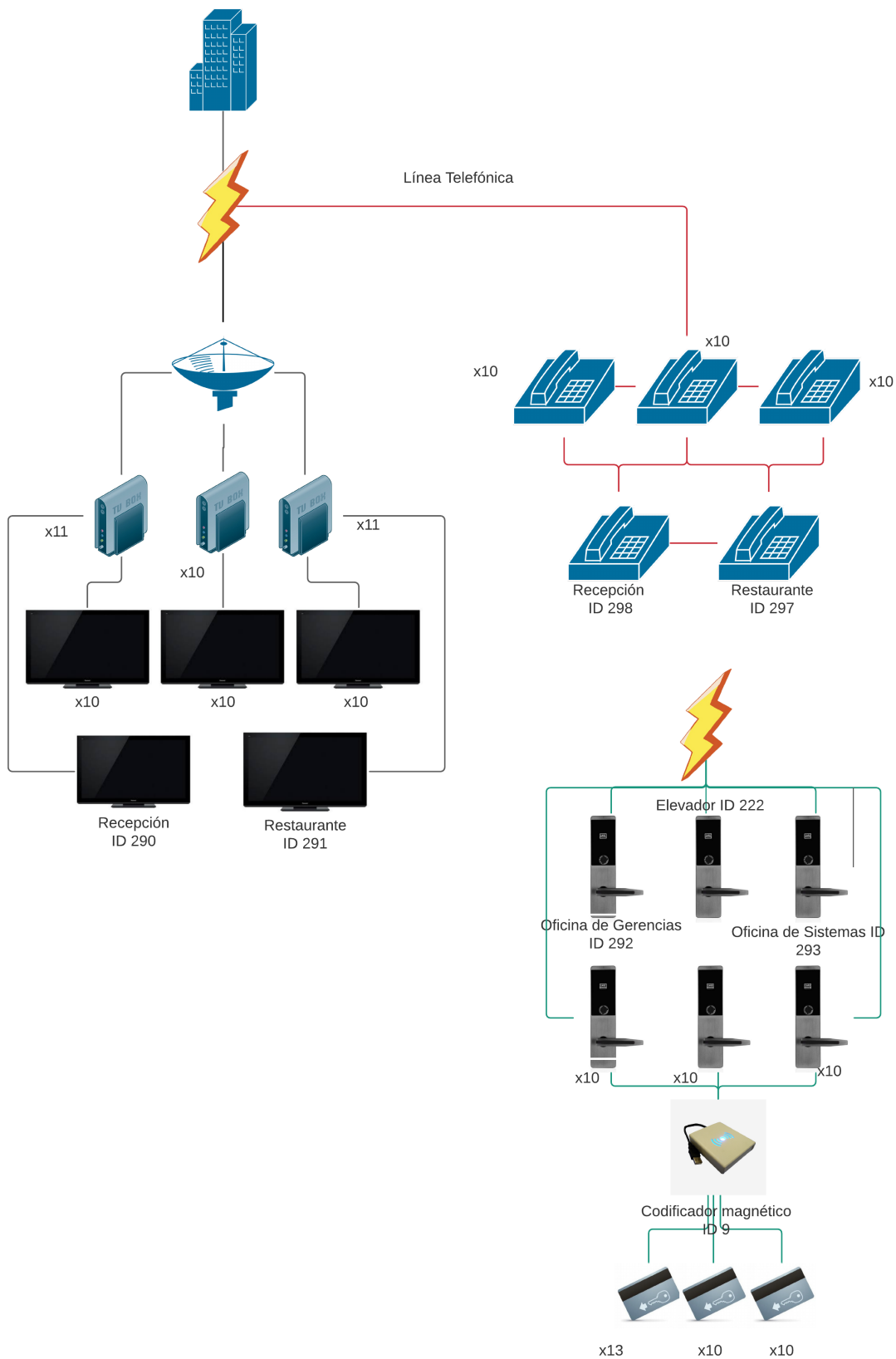


Figura 2: Diagrama otros activos

En la figura 2 se encuentra otro diagrama de activos, pero que no dependen de la red local. En esta encontramos tres clasificaciones diferentes que depende únicamente de la red de electricidad del hotel: el sistema de cable para televisiones, la línea de teléfonos, y las cerraduras de los cuartos. Aquí se procuró indicar el número exacto de activos de cada tipo, con el número general de activos por cuarto y luego especificando los que pertenecen a algún cuarto administrativo del hotel. Se separaron en dos partes, ya que la primera son servicios del hotel primero con lo es el cable especificado en negro que tiene su antena y sus aparatos para los canales para que funcione la televisión, y luego con rojo el servicio de telefonía. En la segunda parte con verde está todo el proceso de las cerraduras magnéticas, que involucra las mismas con su codificador de llaves para el acceso.

En la tabla II se presentan las problemáticas encontradas relacionadas a la red de la imagen 2. Estas problemáticas son únicamente dirigidas a los dispositivos mencionados que son todos conectados a alguna fuente de electricidad. Es posible que, como problemática exista el forcejeo de la cerraduras o la entrada por ruptura de estas, pero al no ser problemas del tipo electrónico no fueron incluidos en la tabla.

Problemática	Prevención
Generación de una llave maestra RFID	Tener un control de las llaves que terminen de usar los huéspedes.
Hackeo de la línea telefónica	Mantener contacto con la compañía que proporciona el servicio para detectar dispositivos ajenos o escuchas ilegales
Hackeo de las antenas de televisión	Mantener en revisión y en mantenimiento constante las antenas y los sintonizadores.
Manipulación del Software de Restaurante	Tener la computadora del restaurante con protección (antivirus) y no permitir el uso a gente que no esté autorizada.
Hackeo a la página web	Mantener en revisión y mantenimiento la página además de tenerla protegida con algún software antivirus.
Robo en habitaciones por parte del personal	Restringir acceso a habitaciones solo a personal de limpieza y mantenimiento en horas de trabajo
Acceso de clientes a pisos que no son los suyos	Instalación de lector RFID en elevadores para limitar acceso de clientes a únicamente el piso de su cuarto y áreas comunes.
Utilización de llaves de reservaciones antiguas para entrar a los cuartos	ID único de tarjetas de acceso por reservación.

Tabla 2: Problemáticas y prevenciones preliminares en otros activos

12. Etapa 3

12.1. Definición de las vulnerabilidades

Existen diversos factores que permiten que actores, internos o externos, logren vulnerar sistemas de la empresa. Factores como malas configuraciones, errores, descuidos, pueden resultar en escenarios fatídicos como el robo de información sensible o pérdida de bienes, es por esto que las instituciones necesitan contar con soluciones para cada posible falla.

Un hotel puede tener muchas vulnerabilidades que van desde lo técnico hasta la propia ingeniería social, las vulnerabilidades principales encontradas en este caso son:

- Bases de datos en texto plano.
- Robo de información por navegación web.
- Poco nivel de seguridad en sistemas a nivel local.
- Exposición a intrusos en redes.
- Malware y virus.
- Exposición ante dispositivos externos conectándose al Router administrativo de forma inalámbrica.
- Ransomware bloqueando infraestructura entera del hotel.
- Exposición por factores de ingeniería social.
- Exposición de hardware externo en los diversos activos tecnológicos del hotel.

Es de vital importancia entender como la práctica de defensa de sistemas tecnológicos puede prevenir y mitigar catástrofes que podrían costar mucho a las empresas, sobre todo cuando estas son pequeñas y medianas, por lo que el siempre contar con un plan de acción es la base para un buen sistema seguro.

12.2. Medidas

12.2.1. MySQL

Es aún muy común el mantener información dentro de las bases de datos en forma de texto plano, esto quiere decir que la información presente en las bases de datos no cuenta con un cifrado en particular por lo que es completamente legible para aquel que tenga acceso a esta base de datos. Es por eso que empresas como Microsoft o IBM han empleado una tecnología conocida como Transparent Data Encryption (TDE) que ofrece un cifrado de datos a nivel archivo, o lo que también es llamado como datos en reposo. Si bien no es capaz de encriptar datos en tránsito, esta tecnología funciona a través de una certificación y una clave maestra, permitiendo que aquel que sea capaz de llegar a obtener esta información simplemente no pueda leerla pues quedará ilegible. Esta tecnología se encuentra disponible como parte de SQL Server de Microsoft en versiones desde 2008 hasta 2019, lo que se conecta directamente con otra vulnerabilidad [12].

El manejar la información desde un servidor local no suele ser la opción más segura existiendo otros servicios por lo que parte del plan de mitigación es migrar a una solución de SQL que este ubicada en la nube, esto se hace para evitar la exposición de los activos internos de la empresa; si bien es cierto que se puede asegurar el servidor de manera física en el hotel, es muchísimo más seguro que los datos se encuentren en un data center de una empresa responsable y madura. Este plan debe implementarse con su debido sistema de acceso a las bases de datos solamente a el personal con las credenciales correspondientes, éstas serían un nombre de usuario y una contraseña bastante robusta que no contenga ninguna especie de patrón fácilmente descifrable. Como se vio con anterioridad este tipo de servicios cuentan con tecnología de cifrado, lo que vuelve ilegible la información presentada para aquel que no cuente con la clave maestra, así como también evita la exposición a riesgos físicos que sí existen teniendo el servidor en las propias instalaciones del hotel. [13]

12.2.2. Firewall

Hoy en día internet es una de las herramientas tecnológicas más usadas en el mundo, por esto mismo es también dónde puede existir mayor riesgo en cuánto a robo de información se trata. Además es uno de los medios por el cual un servidor puede llegar a sufrir mayor cantidad de ataques, por lo que para llevar a cabo una protección de estos ataques se propone el uso de un Firewall de Aplicaciones Web (WAF). Este tiene como principal función realizar un análisis de paquetes de petición ya sean HTTP o HTTPS, así como los modelos de tráfico. El Firewall examina cada petición que se es realizada al servidor antes de que llegue al cliente, esto en pro de asegurarse de que dicha petición cumple con las reglas establecidas por la configuración del Firewall. Este puede ser implementado tanto en software, ya sea instalando una aplicación en el sistema operativo que consumiría recursos del servidor local, como en hardware integrando funcionalidades en una solución "appliance" lo que minimizaría de forma considerable la latencia pero generaría un mantenimiento y almacenamiento de equipos físicos llegando a ser bastante costoso. Existen dos tipos de WAF: de lista negra que se encargan de proteger contra ataques que ya sean conocidos, mientras que los de lista blanca solo admiten un tráfico que haya sido autorizado con antelación. El caso idílico es lograr trabajar con un híbrido capaz de poner ambos tipos en práctica. [14]

En red local suelen existir un sin fin de amenazas ya sea provenientes de forma interna como de forma externa por lo que se llevará a cabo la implementación de un Next Generation Firewall (NGFW). Este es un nuevo sistema de seguridad para redes dentro de un dispositivo hardware o bien en una versión basada en software capaz de detectar ataques sofisticados, esto a través de forzar políticas de seguridad a nivel de aplicación, a nivel de puertos y protocolos de comunicación. Estos mantienen las características de un Firewall con estado, se habla de filtrado de paquetes, compatibilidad con IPsec y VPN SSL, funciones de mapeo de IP, y supervisión de red. Sin embargo también cuentan con capacidades de inspección de contenido más profundas, debido a que son capaces de identificar ataques y malware, y además de bloquearlos al momento. Este Firewall es sobre todo recomendado para llevar a cabo un control del contenido de la red local hacia internet. Se debe tomar en cuenta que los NGFW son capaces de llevar a cabo inspecciones de SSL, App Control, previsión de intrusiones, y provee una visibilidad de toda la superficie del ataque e inclusive incluye rutas para futuras actualizaciones proporcionando flexibilidad para evolucionar a través del panorama de

amenazas manteniendo la red segura. [15]

12.2.3. Protocolos

Es muy común en empresas enfrentarse a amenazas capaces de afectar el funcionamiento de los sistemas, como pueden ser las redes de comunicaciones, es por eso que existen estrategias para que la seguridad de los sistemas prevalezca, hablamos particularmente de *Intrusion Prevention System (IPS)* y de *Intrusion Detection System (IDS)*. IDS permite ver que está sucediendo en la red en tiempo real, esto a través de la recopilación de información, reconoce modificaciones y automatiza patrones de búsqueda en paquetes de datos enviados a través de la red, sin embargo este sistema solo es capaz de detectar, no previene ni detiene ataques. Es aquí donde entra IPS este es capaz de proteger sistemas de ataques e intrusiones, realiza análisis de tiempo real para determinar si se está produciendo o se va a producir alguna especie de incidente, esto a través de patrones, anomalías e inclusive comportamientos de carácter sospechoso, permite lanzar alarmas, descartar paquetes y desconectar conexiones. Es común encontrar tanto a IPS como IDS en productos mixtos, por lo que suelen ir de la mano y ayudaría a la infraestructura del hotel obtener una capa más para prevenir y remediar ataques. [16]

12.2.4. Antivirus

Los virus de computadora son una de las problemáticas más frecuentes que existen en la actualidad, pudiendo llegar desde a dispositivos de uso domestico hasta dispositivos corporativos. Ante estas amenazas tan comunes se propone la implementación de un antivirus, estos tienen la misión principal de detectar y eliminar todo software malicioso de equipos y dispositivos. Realizan análisis continuos los cuales hacen una comparación de archivos presentes en el sistema operativo contra una base de datos que contiene firmas, las cuales son características identificativas de diversos tipos de malware, esta bases de datos están en continua actualización. Algunos antivirus son capaces de detectar diversas amenazas mediante la identificación de patrones en archivos localizando alteraciones del sistema o analizando comportamiento que no suelen ser normales en algunos componentes informáticos. Protegen de amenazas como virus, los cuales son programas maliciosos que se esconden como ficheros de usuario con el propósito de acceder a equipos sin consentimiento, y tienden a robar información, borrar archivos o alterar configuraciones del equipo. Existen los gusanos informáticos los cuales son programas diseñados para ejecutarse y propagarse a través de una red con el objetivo de colapsar equipos y redes. [17]

En ocasiones existen vulnerabilidades tan obvias como dispositivos externos a la institución conectándose a la red administrativa sin autorización, por lo que el protocolo recomendado para evitar este tipo de filtraciones es WPA2 el cual mejoró a la versión anterior es decir WEP, implementando dos nuevos protocolos como lo son negociación de 4 mensajes y negociación de clave de grupo, esto permite establecer y cambiar de forma apropiada las claves criptográficas. [18]

El antivirus cotizado para ser implementado en los dispositivos del hotel es la licencia de Kaspersky específicamente “Internet Security” se recomienda contratar el plan anual para 5 dispositivos a un precio de 1,119 MXN y un plan anual para 3 dispositivos a 979 MXN, cabe destacar que si bien se contrata las

licencias para un total de 8 dispositivos, el hotel solo cuenta con 7 sin embargo esto se decide así debido a que contratar un plan para 3 dispositivos es más barato que dos planes individuales los cuales tienen un costo anual de 559 MXN. [19]

12.2.5. Copias de Seguridad

El Ransomware es un software de carácter extorsivo de modo que la finalidad que tiene es impedir el uso de un dispositivo hasta que no se haya pagado un rescate, la forma en la que se lleva a cabo es introduciéndose al dispositivo y cifrando parte o todo el sistema operativo, para prevenir ataques de este tipo es fundamental mantener todos los dispositivos actualizados y llevar a cabo un uso responsable del dispositivo [20].

Por otro lado en caso de tener un ataque de Ransomware en el cual detenga operaciones completas se recomienda que el hotel posea una copia de seguridad en frío o también conocida como fuera de línea, es una copia de seguridad de la infraestructura entera que no se accederá con frecuencia, pero si se actualiza con frecuencia. Es la forma más segura de realizar copias de seguridad debido a que evita el riesgo de copiar datos que puedan estar en un proceso de actualización, sin embargo esta implica tener un tiempo de inactividad por lo que los usuarios no pueden acceder a los activos involucrados. Debido a que se tiene inactividad al hacer esto, se recomienda hacer estos respaldos a altas horas de la noche cuando el uso de los aparatos es muy bajo, y para el caso de los equipos de recepción estos no deben respaldarse al mismo tiempo. Además de contarse con un respaldo en site que a diferencia del anterior que era un respaldo completo, este simplemente sería un respaldo incremental la cual solo agrega información cuando se agrega al equipo, mientras que si es completo este hace un respaldo de maquina entera. Un ataque de Ransomware puede suceder en cualquier momento por lo que como respuesta a este tipo e incidentes por lo que se tiene una imagen de cada computadora con programas mínimos que permitan el funcionamiento correcto de la empresa en lo que son recuperados dichos respaldos [21].

12.2.6. Protección del Hardware

Las empresas tienen una gran vulnerabilidad a la cual no suele ponerse atención sin embargo es una debilidad con el potencial de ser más devastadora que el apartado técnico y se trata de ingeniería social, la cuál es la práctica de obtener información, accesos o permisos a través de manipular usuarios legítimos, esta clase de problemas necesita sobre todo un programa de entrenamiento en el cual se lleve a cabo una capacitación de todo el personal acerca de medidas que deben tomarse para evitar riesgos en los activos tecnológicos de la empresa, este programa debe ser personalizada y centrada en función de las necesidades específicas, debe ser periódico y ser actualizado durante el tiempo [22], las medidas que deben emplearse son:

- Prohibición de acceso a áreas no autorizadas, el personal del hotel debe mantenerse alejado de aquellas áreas que no le competen, sobre todo en áreas que puedan poner en riesgo los activos T.I. de la empresa.
- Especificar el uso en todo momento de una identificación en la que se muestre nombre, área de trabajo y puesto, para evitar que personas ajenas al hotel finjan ser empleados del mismo.

- El personal no puede tener acceso a información que no le corresponde dígame bases de datos, configuraciones de red, por lo que se limitarán las credenciales de acceso única y exclusivamente a las personas que les corresponda.
- Informar y capacitar empleados acerca de las amenazas más comunes en ciberseguridad como phishing o malware.
- Toda cuenta del personal debe estar asegurada con método de doble autenticación.
- Principio de mínimo privilegio, el cual consiste en la configuración de cuentas para que estas no dispongan de privilegios de administrador y reduciendo las acciones que se puedan realizar en estos a lo mínimo para que puedan llevar a cabo su trabajo.
- Sin embargo hay una amenaza que no suele tomarse en cuenta que es un ataque a consciencia del propio personal, por lo que se llevará a cabo la instalación de un write blocker físico, dispositivo capaz de interceptar cualquier escritura de disco inadvertida, al detectar actividad maliciosa se detendrán las operaciones en dicho dispositivo, se instalará el dispositivo por protocolo, se copia el disco duro y se lleva a cabo una auditoría desde el disco copiado, esto se realiza para conservar la integridad en la evidencia y el empleado no pueda alegar que se haya agregado información con el fin de inculparlo, write blocker no puede quedarse instalado de forma permanente en el dispositivo pues la computadora dejaría de funcionar.
- Se prohíbe el acceso con cualquier herramienta en la que se pueda capturar información, esto puede ser desde un celular hasta cualquier tipo de papel, esto permite evitar cualquier robo de información por medios externos de la empresa.

En cuanto a la seguridad del hardware en físico existen muchos elementos que hay que plantear para su protección. El primer punto estaría en el lugar del hotel en el que estén localizados los servidores, ya que debe de ser un lugar alejado del acceso al personal no autorizado. Es muy probable que no todas las edificaciones se hayan planeado con la intención de tener un cuarto seguro para almacenar la información, pero se pueden tomar medidas que ayuden a contra restar esto. En lo que respecta a la seguridad del cuarto en sí, se deben de tener planes contra elementos que comprometan la integridad de los servidores, como lo podrían ser incendios, filtraciones de agua, o externos que pretendan dañar el sistema. Claro que la opción más segura sería la reestructuración de este cuarto para que estos no sean problemas sea la mejor opción, pero también sería algo bastante costoso que no sería viable en principio para una PyME. Es por ello que soluciones alternativas en este caso serían lo mejor, como la instalación de sistemas contra incendios, capacitación al personal en el caso de desastres, copias de seguridad en frío como se habían mencionado anteriormente, y pólizas de seguro para proteger a este equipo.

Y como segundo punto estaría en lo que respecta a la seguridad de este hardware para robo de información en físico. Es importante mantener los equipos seguros en la parte del costo que representaría si se daña, pero es aún más el costo que tendría el robo de información por la posible pérdida de confianza de los clientes o de

la productividad en lo que se regresa a la actividad normal. Es por ello que como se mencionó anteriormente, debe de haber un control del personal que no sea necesario en este ámbito, además de huéspedes que puedan llegar. Las personas responsables deben de realizar constantes revisiones al sistema en búsqueda de dispositivos externos que se dediquen a robar la información de manera remota, y asegurarse que no tengan conectados nada inusual. También estaría la opción de desactivar todos los puertos que no se encuentren en uso, ya que de lo contrario son susceptibles a estos accesos no deseados. Estas acciones son posibles de llevar a cabo con una simple planeación, y no ocupan de muchos recursos económicos del hotel.

12.2.7. Reportes Post Mortem

Cada que ocurra un incidente se debe realizar un reporte post mortem en el que se detalle lo siguiente:

- Suceso.
- Involucrados.
- Activos afectados.
- Respuesta.
- Downtime (hubo o no hubo y en caso de que sí, cuanto).
- Perdidas.
- Oportunidades detectadas.
- Que acciones fueron implementadas de forma correcta.

Esto para poder ser un proceso de mejora continua.

Para que este plan sea un programa de seguridad integral y completo, el propósito se basó en cumplir de forma adecuada con el pilar fundamental de la ciberseguridad el cual es la tríada CIA, Confidentiality, Integrity And Availability (confidencialidad, integridad y disponibilidad). El modelo presentado es Zero Trust por lo que se asume que puede haber atacantes tanto dentro de la red como fuera de ella, por lo que no se debe confiar en ningún usuario o dispositivo de forma predeterminada.

12.3. Costos del Plan de Mitigación

12.3.1. Cotización Azure

Este plan de mitigación hace 1 década o 5 años hubiera forzado a PyME's a tener que encontrar servicios por todos lados en constantes llamadas para poder asegurar que la mayoría de su red no pueda ser robada. Dado el crecimiento que se ha tenido en la tecnología, ya existen empresas de confianza como Amazon Web Services, Microsoft Azure, u Oracle que te pueden hacer un paquete de servicios necesarios para la seguridad de tu empresa y te facilita todos los aspectos. En vez de tener que andar en constante busca por servicios por el internet en Microsoft por ejemplo te vas a la calculadora de precios e ingresas los servicios necesarios.

En este caso necesitamos lo siguiente: Transparent Data Encryption (TDE), Microsoft SQL server, Firewall, Intrusion Prevention System (IPS), Intrusion Detection System, antivirus, y Ransomware.

Luego incluyendo todos los demás servicios de Azure que en este caso serian Azure database for MySQL, Azure Firewall, Azure Backup, y Azure Defender. Estos servicios son los que podrían cubrir todo lo necesario en este caso para tener una seguridad impecable en el hotel. El costo mensual seria alrededor de los 908 USD, pero no solo cubriría ese tipo de situaciones, sino hay varios servicios de Azure que podrían hacer un servicio superior a lo que necesitas para poder garantizar de manera superior un nivel de seguridad. Estas medidas con Azure si se conecta de manera apropiada podrían servir a la empresa de manera inmediata para que desde el día 1 ya tengan la seguridad que necesitan para proteger su negocio. Debido a el numero de oferta que ha tenido el crear servicios de seguridad en el internet y todo relacionado con la nube, existe una gran posibilidad de que por temas de economía pueda reducir su costo aunque la demanda siga subiendo pero cada día existen más empresas tratando de ofrecer servicios debido al margen alto que están recibiendo los grandes como Amazon y Microsoft [23].

12.3.2. Cotización AWS

Otra alternativa recomendada para el uso del hotel es la de Amazon Web Services que maneja esquemas de precios mucho más adecuados a una PyME.

El primer servicio que debe considerarse es AWS RDS que es una base de datos conectada con MySQL y el AWS Shield Standard que incluye protección contra ataques DDoS comunes. El costo de este plan es de 12.41 USD mensuales e incluye el Shield Standard sin costo adicional. Otro de los paquetes de servicios recomendados para la empresa es la utilización de instancias AWS EC2 para migrar el hosting de la página web a la nube de Amazon y asegurarla con ellos, el AWS CloudTrail que es un sistema de registros para eventos de AWS, este permitirá auditar la actividad que los empleados realicen con los activos de AWS, el AWS KMS que es un administrador de claves y uso de cifrado de Amazon enfocado en seguridad de hardware, el AWS S3 Glacier que es el sistema de copia de seguridad en frío. Todos estos servicios por un precio total de 91.55 USD mensuales, y para el caso de las instancias de EC2 si fuese necesario se pueden pedir más recursos bajo demanda si se llegase a tener una temporada muy ocupada. Estos precios son mucho mas reducidos en comparación con Azure, sin embargo no se están ofreciendo los mismos servicios en ambos pero AWS tiene la ventaja de manejar mensualidades por volumen para dar el costo final [24].

La cotización se puede consultar en:

<https://calculator.aws/#/estimate?id=288c678905b84da7bf504a7ea262b5e6a0afc4c7>

Como resumen de esta etapa podemos ver el diagrama final de nuestra red (Figura 3) con las estrategias de mitigación añadidas y una tabla de estas mismas (Tabla 12.3.2).

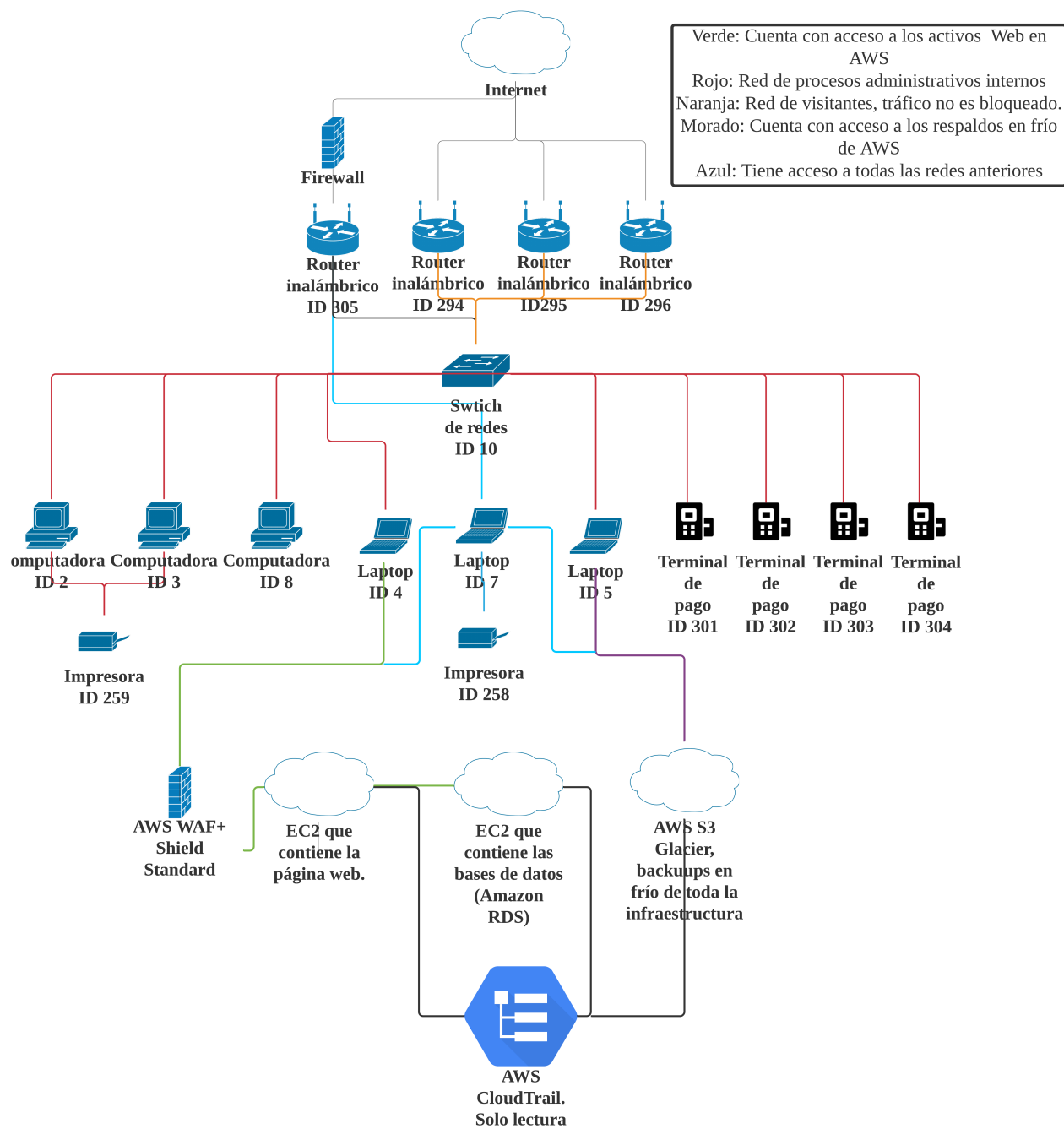


Figura 3: Diagrama de red final.

# de estrategia	Nombre	Descripción
1	Áreas restringidas	El personal del hotel debe mantenerse alejado de aquellas áreas que no le competen, sobre todo en áreas que puedan poner en riesgo los activos T.I. de la empresa.
2	Uso de identificación	Especificar el uso en todo momento de una identificación en la que se muestre nombre, área de trabajo y puesto, para evitar que personas ajenas al hotel finjan ser empleados del mismo.
3	Acceso a información restringido	El personal no puede tener acceso a información que no le corresponde dígame bases de datos, configuraciones de red, por lo que se limitarán las credenciales de acceso única y exclusivamente a las personas que les corresponda.
4	Capacitación a empleados	Informar y capacitar empleados acerca de las amenazas más comunes en ciberseguridad como phishing o malware.
5	Doble autenticación	Toda cuenta del personal debe estar asegurada con método de doble autenticación.
6	Principio de mínimo privilegio	Consiste en la configuración de cuentas para que estas no dispongan de privilegios de administrador y reduciendo las acciones que se puedan realizar en estos a lo mínimo para que puedan llevar a cabo su trabajo.

# de estrategia	Nombre	Descripción
7	Write Blocker	En caso de detectar actividad maliciosa en un equipo, se detendrán las operaciones en dicho dispositivo, se usará el Write Locker para copiar el disco duro y se lleva a cabo la auditoría desde el disco copiado. Esto se realiza para conservar la integridad de la evidencia y que el empleado no pueda alegar que se ha agregado información al disco con el fin de inculparlo.
8	Herramientas de captura prohibidas	Se prohíbe el acceso con cualquier herramienta en la que se pueda capturar información, esto puede ser desde un celular hasta cualquier tipo de papel, esto permite evitar cualquier robo de información por medios externos de la empresa.

12.4. Costo final del plan de mitigación

Al escogerse el plan anual de Amazon Web Services y los planes de antivirus de Kaspersky el total anual del plan de mitigación es de 23,761.46 MXN al año.

13. Etapa 4. Discusión, conclusiones y evaluación final.

13.1. Técnicas y herramientas de ingeniería empleadas

Técnicas de ingeniería empleadas:

1. Levantamiento de inventario de activos
2. Registro de empleados
3. Registro de ubicaciones de la empresa
4. Mapeo de redes de activos
5. Análisis de vulnerabilidades
6. Compromiso ciudadano para la transformación social
7. Argumentación ética
8. Seguridad informática
9. Algoritmos criptográficos

10. Principio de mínimo privilegio

11. Control 17

Herramientas de ingeniería empleadas:

1. MySQL
2. phpMyAdmin
3. Calculadora de precios de Amazon Web Services
4. Calculadora de precios de Microsoft Azure

13.2. Infraestructura

Para llevar a cabo el proyecto es necesaria la siguiente infraestructura: Servicios virtualizados de Amazon Web Services:

1. Servicio AWS Cloud Trail
2. AWS Key Management Service
3. AWS Web Application Firewall (WAF)
4. 2 instancias de Amazon EC2 t3 micro de 30 GB de almacenamiento
5. Amazon Simple Storage Service (S3) 2TB
6. Amazon RDS for SQL server db.t2.micro de 30 GB con 2 nodos

También se requiere capacitar a los empleados del hotel sobre amenazas comunes en ciberseguridad, y un write blocker en caso de requerir auditar un equipo. Además, en caso de que el hotel no contase con las licencias de Windows 10 pro, se deben adquirir pues son necesarias para poder aplicar el principio de mínimo privilegio.

13.3. Conclusiones

En conclusión el plan de mitigación se diseñó con éxito y es capaz de brindar la cobertura deseada a un precio razonable para una PyME, con un costo que justifica la inversión y permite tener respaldos en caso de que suceda un desastre y se tenga que restaurar una versión anterior de los sistemas. El plan es escalable y afín a empresas de giro similar, por lo que su diseño es sólido. El uso de sistemas virtualizados agrega una capa de seguridad extra pues la responsabilidad de la empresa contratada es cuidar que no existan accesos no autorizados a los equipos que mantienen estos recursos.

Referencias

- [1] Kaspersky, “¿Qué es la ciberseguridad?,” 08 2021.
- [2] Oxford Business Group, “Report: The post-pandemic role of cybersecurity for companies in Mexico,” 08 2021.
- [3] Cisco, “¿Qué es la seguridad de red?,” 09 2021.
- [4] vmware, “Seguridad de las aplicaciones,” 2021.
- [5] Cisco, “¿Qué es la Seguridad de TI?,” 09 2021.
- [6] L. Correa, “CONTINUIDAD DE NEGOCIO Y RECUPERACIÓN DE DESASTRES,” *Universidad Piloto de Colombia*, 2017.
- [7] J. Gamboa Suárez, “IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD EN EL MUNDO ACTUAL,” *Universidad Piloto de Colombia*, 2020.
- [8] I. Belcic, “¿Qué es el malware?,” 05 2021.
- [9] I. Belcic, “Guía esencial del phishing: cómo funciona y cómo defenderse,” 09 2021.
- [10] T. O. Valencia, “Inyección de SQL, tipos de ataques y prevención en ASP.NET-C#,” 08 2018.
- [11] N. A. Aziz, T. Mantoro, M. A. Khairudin, and A. F. b. A. Murshid, “Software Defined Networking (SDN) and its Security Issues,” *2018 International Conference on Computing, Engineering, and Design (ICCED)*, 2018.
- [12] Microsoft, “Transparent Data Encryption (TDE),” 04 2012.
- [13] Microsoft, “SQL Server 2019.”
- [14] Oracle, “¿Qué es un WAF?.”
- [15] S. Lascano and D. Olivo, “Evaluación de tecnologías utm (unified threatment management) y ngfw (next generation firewall) para detección de vulnerabilidades en la red.,” 2020.
- [16] M. Papadaki and S. Furnell, “Ids or ips: what is best?,” *Network Security*, vol. 2004, no. 7, pp. 15–19, 2004.
- [17] Kaspersky, “Datos y preguntas frecuentes sobre virus informáticos y malware,” 01 2021.
- [18] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, “A survey on wireless security protocols (wep, wpa and wpa2/802.11 i),” in *2009 2nd IEEE International Conference on Computer Science and Information Technology*, pp. 48–52, IEEE, 2009.
- [19] Kaspersky, “Internet Security 2021,” 2021.

- [20] Kaspersky, “El ransomware: qué es, cómo se lo evita, cómo se elimina,” 04 2021.
- [21] F. Grabski, “Semi-markov reliability model of system composed of main subsystem, cold backup component and switch,” *Journal of Polish Safety and Reliability Association*, vol. 8, 2017.
- [22] CIS (Center for Internet Security), “Control 17: Implement a Security Awareness and Training Program,” 05 2018.
- [23] Microsoft, “Pricing Calculator,” 04 2012.
- [24] Amazon Web Services, “ Amazon Web Services Pricing,” 05 2018.

✔ Mostrando filas 0 - 116 (total de 117, La consulta tardó 0,0007 segundos.)							
SELECT * FROM `activos tangibles`							
id	tipo	marca	descripción	ubicación	versión	dirección MAC	encargado
1	Computadora de servidor	Dell	Servidor Dell PowerEdge T40, Intel Xeon E-2224G 3.50GHz, 8GB DDR4, 1TB, 3.5", SAS/SATA, Mini Tower	Cuarto de sistemas	Windows Server 2019 (Long-Term Servicing Channel) (Datacenter, Essentials, Standard) Version 1809	fa:55:8f:df:e2:e9	Juan Campos
2	Computadora de escritorio	Hp	Computadora All in One Hp 290-A006BLA / Intel Celeron / 21.5 Pulg. / 1tb / 4gb RAM / Negro	Recepción	Windows 10 Pro, versión 21H1	3a:bb:fd:dd:9c:79	Pedro Rodríguez
3	Computadora de escritorio	Hp	Computadora All in One Hp 290-A006BLA / Intel Celeron / 21.5 Pulg. / 1tb / 4gb RAM / Negro	Recepción	Windows 10 Pro, versión 21H1	7a:8a:e5:a6:2a:64	Pedro Rodríguez
4	Laptop	Acer	Laptop Gaming Acer Nitro 5 AN515-54-5579 Intel Core i5 Gen 9th 8GB RAM 512GB SSD	Móvil	Windows 10 Pro, versión 21H1	42:d7:41:6c:cb:19	Alejandro Capo
5	Laptop	Acer	Laptop Gaming Acer Nitro 5 AN515-54-5579 Intel Core i5 Gen 9th 8GB RAM 512GB SSD	Cuarto de sistemas	Windows 10 Pro, versión 21H1	ee:cb:3c:ba:11:bd	Pedro Rodríguez
7	Laptop	Acer	Laptop Gaming Acer Nitro 5 AN515-54-5579 Intel Core i5 Gen 9th 8GB RAM 512GB SSD	Móvil	Windows 10 Pro, versión 21H1	ce:ac:a0:57:2e:e5	José Vizcaíno
8	Computadora de escritorio	Hp	Computadora All in One Hp 290-A006BLA / Intel Celeron / 21.5 Pulg. / 1tb / 4gb RAM / Negro	Restaurante	Windows 10 Pro, versión 21H1	46:e4:a7:6b:97:38	Macarena Pico
9	Codificador magnético	Deftun	Lector de tarjetas MSR606 para Comupter, lector de tarjetas magnéticas, igual que MSR605X, solo para Windows	Recepción	NULL	NULL	Pedro Rodríguez
10	Switch de redes	Cisco	Cisco SWTCIS1810 Switch Sg250-26-K9-Na, Negro, 24 puertos	Cuarto de sistemas	15.9	NULL	Juan Campos
11	Codificador magnético	Deftun	Lector de tarjetas MSR606 para Comupter, lector de tarjetas magnéticas, igual que MSR605X, solo para Windows	Recepción	NULL	NULL	Pedro Rodríguez
12	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 1	NULL	NULL	José Vizcaíno
13	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 2	NULL	NULL	José Vizcaíno
14	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 3	NULL	NULL	José Vizcaíno
15	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 4	NULL	NULL	José Vizcaíno
16	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 5	NULL	NULL	José Vizcaíno
17	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 6	NULL	NULL	José Vizcaíno
18	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 7	NULL	NULL	José Vizcaíno
19	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 8	NULL	NULL	José Vizcaíno
20	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 9	NULL	NULL	José Vizcaíno
21	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 10	NULL	NULL	José Vizcaíno
22	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 11	NULL	NULL	José Vizcaíno
23	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 12	NULL	NULL	José Vizcaíno
24	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 13	NULL	NULL	José Vizcaíno
25	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 14	NULL	NULL	José Vizcaíno
26	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 15	NULL	NULL	José Vizcaíno
27	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 16	NULL	NULL	José Vizcaíno
28	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 17	NULL	NULL	José Vizcaíno
29	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 18	NULL	NULL	José Vizcaíno
30	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 19	NULL	NULL	José Vizcaíno
31	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 20	NULL	NULL	José Vizcaíno
32	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 21	NULL	NULL	José Vizcaíno
33	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 22	NULL	NULL	José Vizcaíno
34	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 23	NULL	NULL	José Vizcaíno
35	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 24	NULL	NULL	José Vizcaíno
36	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 25	NULL	NULL	José Vizcaíno
37	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 26	NULL	NULL	José Vizcaíno
38	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 27	NULL	NULL	José Vizcaíno
39	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 28	NULL	NULL	José Vizcaíno
40	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 29	NULL	NULL	José Vizcaíno
41	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Habitación 30	NULL	NULL	José Vizcaíno
222	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Elevador	NULL	NULL	José Vizcaíno
226	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 1	NULL	NULL	José Vizcaíno
227	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 2	NULL	NULL	José Vizcaíno
228	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 3	NULL	NULL	José Vizcaíno
229	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 4	NULL	NULL	José Vizcaíno
230	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 5	NULL	NULL	José Vizcaíno
231	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 6	NULL	NULL	José Vizcaíno
232	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 7	NULL	NULL	José Vizcaíno
233	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 8	NULL	NULL	José Vizcaíno
234	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 9	NULL	NULL	José Vizcaíno
235	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 10	NULL	NULL	José Vizcaíno
236	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 11	NULL	NULL	José Vizcaíno
237	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 12	NULL	NULL	José Vizcaíno
238	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 13	NULL	NULL	José Vizcaíno
239	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 14	NULL	NULL	José Vizcaíno
240	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 15	NULL	NULL	José Vizcaíno
241	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 16	NULL	NULL	José Vizcaíno
242	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 17	NULL	NULL	José Vizcaíno
243	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 18	NULL	NULL	José Vizcaíno
244	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 19	NULL	NULL	José Vizcaíno
245	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 20	NULL	NULL	José Vizcaíno
246	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 21	NULL	NULL	José Vizcaíno
247	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 22	NULL	NULL	José Vizcaíno
248	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 23	NULL	NULL	José Vizcaíno
249	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 24	NULL	NULL	José Vizcaíno
250	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 25	NULL	NULL	José Vizcaíno
251	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 26	NULL	NULL	José Vizcaíno
252	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 27	NULL	NULL	José Vizcaíno
253	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 28	NULL	NULL	José Vizcaíno
254	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 29	NULL	NULL	José Vizcaíno
255	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Habitación 30	NULL	NULL	José Vizcaíno
258	Impresora	HP	Multifuncional HP Deskjet IA 2775	Área de gerencia	2116L/2116M/2116N	0e:ab:a0:f0:60:20	José Vizcaíno

id	tipo	marca	descripción	ubicación	versión	dirección MAC	encargado
259	Impresora	HP	Multifuncional HP Deskjet IA 2775	Recepción	2116L/2116M/2116N	0e-3c-f6-32-69-07	Pedro Rodríguez
260	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 1	NULL	NULL	José Vizcaíno
261	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 2	NULL	NULL	José Vizcaíno
262	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 3	NULL	NULL	José Vizcaíno
263	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 4	NULL	NULL	José Vizcaíno
264	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 5	NULL	NULL	José Vizcaíno
265	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 6	NULL	NULL	José Vizcaíno
266	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 7	NULL	NULL	José Vizcaíno
267	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 8	NULL	NULL	José Vizcaíno
268	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 9	NULL	NULL	José Vizcaíno
269	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 10	NULL	NULL	José Vizcaíno
270	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 11	NULL	NULL	José Vizcaíno
271	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 12	NULL	NULL	José Vizcaíno
272	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 13	NULL	NULL	José Vizcaíno
273	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 14	NULL	NULL	José Vizcaíno
274	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 15	NULL	NULL	José Vizcaíno
275	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 16	NULL	NULL	José Vizcaíno
276	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 17	NULL	NULL	José Vizcaíno
277	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 18	NULL	NULL	José Vizcaíno
278	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 19	NULL	NULL	José Vizcaíno
279	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 20	NULL	NULL	José Vizcaíno
280	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 21	NULL	NULL	José Vizcaíno
281	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 22	NULL	NULL	José Vizcaíno
282	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 23	NULL	NULL	José Vizcaíno
283	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 24	NULL	NULL	José Vizcaíno
284	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 25	NULL	NULL	José Vizcaíno
285	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 26	NULL	NULL	José Vizcaíno
286	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 27	NULL	NULL	José Vizcaíno
287	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 28	NULL	NULL	José Vizcaíno
288	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 29	NULL	NULL	José Vizcaíno
289	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Habitación 30	NULL	NULL	José Vizcaíno
290	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Recepción	NULL	NULL	José Vizcaíno
291	Televisión	Atvio	TV Atvio 32 Pulgadas 720p HD LED ATV32	Restaurante	NULL	NULL	José Vizcaíno
292	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Área de gerencia	NULL	NULL	José Vizcaíno
293	Cerradura magnética	Mifare	LOCKPRO-1HD plateada	Oficina de sistemas	NULL	NULL	Juan Campos
294	Router	Linksys	Router Inalámbrico Linksys Dual-band Wifi 5 Ac1200 E540 /vc	Piso de habitaciones 1	1.0	a6:da:f9:6c:d4:98	Juan Campos
295	Router	Linksys	Router Inalámbrico Linksys Dual-band Wifi 5 Ac1200 E540 /vc	Piso de habitaciones 2	1.0	aa:0e:74:4c:dd:e4	Juan Campos
296	Router	Linksys	Router Inalámbrico Linksys Dual-band Wifi 5 Ac1200 E540 /vc	Piso de habitaciones 3	1.0	16:18:2f:6e:ef:24	Juan Campos
297	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Restaurante	NULL	NULL	Macarena Pico
298	Teléfono	Panasonic	Telefono Panasonic Kx-ts550 Alambrico Basico Unilinea	Recepción	NULL	NULL	Pedro Rodríguez
301	Terminal de pago	Pax	Pax S80 EMV Ready tarjeta de crédito	Recepción	1.0	ae-c6-78-55-e9-d5	Pedro Rodríguez
302	Terminal de pago	Pax	Pax S80 EMV Ready tarjeta de crédito	Recepción	1.0	6e:d3:6c:a1:4d:6e	Pedro Rodríguez
303	Terminal de pago	Pax	Pax S80 EMV Ready tarjeta de crédito	Restaurante	1.0	72:de:86:54:fc:16	Macarena Pico
304	Terminal de pago	Pax	Pax S80 EMV Ready tarjeta de crédito	Restaurante	1.0	62-77-19-09-e6-76	Macarena Pico
305	Router	Linksys	Router Inalámbrico Linksys Dual-band Wifi 5 Ac1200 E540 /vc	Cuarto de sistemas	1.0	82:38:ac:84:eb:63	Juan Campos


✔ Mostrando filas 0 - 8 (total de 9, La consulta tardó 0,0011 segundos.)

SELECT * FROM `activos no tangibles`

id	nombre	tipo	descripción	Ligado a
1	base de datos de empleados	Base de datos	contiene información de los empleados, su nombre, área y turno asignado	Servidor Dell PowerEdge T40, Intel Xeon E-2224G 3.50GHz, 8GB DDR4, 1TB, 3.5", SAS/SATA, Mini Tower
2	base de datos de huéspedes	Base de datos	contiene información de los huéspedes, su nombre, habitación asignada y fecha de entrada-salida. La información se guarda hasta 30 días después del check-out	Servidor Dell PowerEdge T40, Intel Xeon E-2224G 3.50GHz, 8GB DDR4, 1TB, 3.5", SAS/SATA, Mini Tower
3	Cuiner	Licencia de Software	Software de administración de restaurantes	Computadora All in One Hp 290-A006BLA / Intel Celeron / 21.5 Pulg. / 1tb / 4gb RAM / Negro
4	Licencia Windows 10 pro	Licencia de Software	Windows 10 pro usada en recepción	Computadora All in One Hp 290-A006BLA / Intel Celeron / 21.5 Pulg. / 1tb / 4gb RAM / Negro
5	Licencia Windows 10 pro	Licencia de Software	Windows 10 pro usada en recepción	Computadora All in One Hp 290-A006BLA / Intel Celeron / 21.5 Pulg. / 1tb / 4gb RAM / Negro
6	Licencia Windows 10 pro	Licencia de Software	Windows 10 pro usada en la computadora del administrador de sistemas	Laptop Gaming Acer Nitro 5 AN515-54-5579 Intel Core i5 Gen 9th 8GB RAM 512GB SSD
7	Licencia Windows 10 pro	Licencia de Software	Windows 10 pro usada en la computadora del administrador de la página web	Laptop Gaming Acer Nitro 5 AN515-54-5579 Intel Core i5 Gen 9th 8GB RAM 512GB SSD
8	Licencia Windows 10 pro	Licencia de Software	Windows 10 pro usada en el restaurante	Laptop Gaming Acer Nitro 5 AN515-54-5579 Intel Core i5 Gen 9th 8GB RAM 512GB SSD
9	Licencia de Windows server 2019	Licencia de Software	Licencia de Windows server 2019 usada en computadora de servidor	Servidor Dell PowerEdge T40, Intel Xeon E-2224G 3.50GHz, 8GB DDR4, 1TB, 3.5", SAS/SATA, Mini Tower

✔ Mostrando filas 0 - 30 (total de 31, La consulta tardó 0,0009 segundos.) [puesto: 1... - 15...]

SELECT * FROM `empleados` ORDER BY `puesto` ASC

id	nombre	puesto  1	Turno
18	Juan Campos	Jefe de sistemas	On call
3	Alejandro Capo	Administrador de página web	On call
2	Pedro Rodríguez	Jefe de recepción	Mañana
4	Sonia Elizalde	Trabajador de recepción	Mañana
5	Alexa Hernández	Trabajador de recepción	Tarde
6	Tulio Treviño	Trabajador de recepción	Tarde
7	César Chávez	Trabajador de recepción	Noche
8	Alberto Armas	Trabajador de recepción	Noche
32	Luis Jiménez	Jefe de cocina	Mañana
26	Abdellah Ye	Mesero	Mañana
27	Neus Riera	Mesero	Tarde
28	Marti Arnau	Mesero	Tarde
29	Ariadna Ribas	Mesero	Noche
30	Benigno Moreira	Mesero	Noche
25	Macarena Pico	Jefe de meseros	Mañana
19	Emilio Carrasco	Jefe de limpieza	Mañana
20	Maria Riquelme	Trabajador de limpieza	Mañana
21	Leandro Villaverde	Trabajador de limpieza	Tarde
22	Maria Quintana	Trabajador de limpieza	Tarde
23	Ander Melero	Trabajador de limpieza	Noche
24	Regina Gomis	Trabajador de limpieza	Noche
1	Juan Pérez	Jefe de mantenimiento	Mañana
12	Jorge Pérez	Trabajador de mantenimiento	Tarde
13	Arturo Suarez	Trabajador de mantenimiento	Noche
9	Cynthia Palos	Botones	Mañana
10	Guillermo Torres	Botones	Mañana
14	Josefina Arámbula	Botones	Tarde
15	Marco Robles	Botones	Tarde
16	Andres Cortés	Botones	Noche
17	Julieta Newman	Botones	Noche
31	José Vizcaíno	Administrador general	On call

✔ Mostrando filas 0 - 41 (total de 42, La consulta tardó 0,0009 segundos.) [ubicacion: **ÁREA DE GERENCIA ... - RESTAURANTE...**]

SELECT * FROM `ubicaciones` ORDER BY `ubicacion` ASC

id	ubicación <small>▲ 1</small>
42	Área de gerencia
1	Cocina
4	Cuarto de sistemas
5	Elevador
10	Habitación 1
9	Habitación 1
19	Habitación 10
20	Habitación 11
21	Habitación 12
22	Habitación 13
23	Habitación 14
24	Habitación 15
25	Habitación 16
26	Habitación 17
27	Habitación 18
28	Habitación 19
11	Habitación 2
29	Habitación 20
30	Habitación 21
31	Habitación 22
32	Habitación 23
33	Habitación 24
34	Habitación 25
35	Habitación 26
36	Habitación 27
37	Habitación 28
38	Habitación 29
12	Habitación 3
39	Habitación 30
13	Habitación 4
14	Habitación 5
15	Habitación 6
16	Habitación 7
17	Habitación 8
18	Habitación 9
41	Móvil
40	Oficina de sistemas
6	Piso de habitaciones 1
7	Piso de habitaciones 2
8	Piso de habitaciones 3
3	Recepción
2	Restaurante