UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

CARRERA: MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

INFORME FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR, MODALIDAD PROYECTO DE INVESTIGACIÓN

TEMA:

"PLAN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD EN LA INDUSTRIA HOTELERA. CASO DE ESTUDIO: JW MARRIOT DE LA CIUDAD DE QUITO"

Trabajo de titulación previo a la obtención del título de Magister en Computación con mención en Seguridad Informática

Línea de investigación: Desarrollo, aplicación de software y cybersecurity (seguridad cibernética)

AUTOR:

ESTEBAN XAVIER MOYOLEMA PAZ

DIRECTOR:

MSC. IVAN PATRICIO ORTIZ GARCÉS

Ibarra, noviembre 2024

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 10 de noviembre de 2024

Msc. Iván Ortiz Garcés

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

(f) .....

Msc. Iván Ortiz Garcés

C.C.: 0602356776

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1721772075		
APELLIDOS Y NOMBRES:	Moyolema Paz Esteban Xavier		
DIRECCIÓN:	Calderón, Elías Godoy y E1c		
EMAIL:	Javier_esteban99@hotmail.com		
TELÉFONO FIJO:	N/A	**TELÉFONO MÓVIL:**	0995263405

DATOS DE LA OBRA			
TÍTULO:	PLAN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD EN LA INDUSTRIA HOTELERA. CASO DE ESTUDIO: JW MARRIOT DE LA CIUDAD DE QUITO		
AUTOR:	ESTEBAN XAVIER MOYOLEMA PAZ		
FECHA:	08/11/2024		
SOLO PARA TRABAJOS DE GRADO			
PROGRAMA:	☐ **GRADO**	☒ X	**POSGRADO**
TITULO POR EL QUE OPTA:	Magister en Computación con mención en Seguridad Informática		
ASESOR /DIRECTOR:	MSC. IVAN ORTIZ GARCÉS		

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 08 días del mes de noviembre de 2024

EL AUTOR:

.....

Nombre: Esteban Xavier Moyolema Paz

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

PLAN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD EN LA INDUSTRIA HOTELERA. CASO DE ESTUDIO: JW MARRIOT DE LA CIUDAD DE QUITO

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con Mención en Seguridad Informática

AUTOR: ESTEBAN XAVIER MOYOLEMA PAZ

DIRECTOR: Msc. Ortiz Garcés Ivan Patricio

ASESOR: Msc. Guevara Vega Alexander

IBARRA – ECUADOR

2024

Dedicatoria

Esta tesis está dedicada a mi querida familia, cuyo apoyo y aliento inquebrantables han iluminado mi camino a lo largo de este desafiante camino. Su fe en mí me ha impulsado a luchar por la grandeza. Extiendo mi gratitud a Dios por concederme fuerza, sabiduría y resistencia. Su gracia divina me ha sostenido a través de las pruebas y los triunfos de este viaje académico. También reconozco a los excepcionales instructores de la UTN, cuya experta orientación, tutoría y dedicación han moldeado mi crecimiento académico y encendido mi pasión por el aprendizaje. Su inquebrantable compromiso con el conocimiento y el fomento del pensamiento crítico han desempeñado un papel fundamental en la formación de mi destreza intelectual. Esta tesis es un testimonio de los esfuerzos de colaboración de aquellos que me han apoyado y motivado a lo largo de este viaje.

Índice de contenido

Índice general

Índice de figuras

Índice de tablas

RESUMEN

En la era digital actual, los hoteles dependen en gran medida de la tecnología, lo que los hace más vulnerables a los ciberataques. Estos ataques, como el ransomware, el phishing, la ingeniería social y las violaciones del sistema, interrumpieron las operaciones de varios hoteles alrededor del mundo y ponen en peligro los datos de los huéspedes. Las amenazas se extienden a sistemas clave como la gestión de reservas, los servicios a los huéspedes y las transacciones financieras, afectan a la continuidad del negocio y a la privacidad de los huéspedes. El sector hotelero es una parte vital de la economía mundial y es responsable de atender a innumerables viajeros. Con el creciente uso de la tecnología en este sector lo ha hecho más vulnerable a los ciberataques. Incluso cadenas hoteleras tan conocidas como JW Marriott ya que han sufrido distintos tipos de ciber amenazas que pueden provocar pérdidas económicas, daños a la reputación y problemas legales. Aunque las empresas hoteleras son conscientes de los riesgos cibernéticos, muchas no tienen planes claros para responder a incidentes de seguridad específicos de sus operaciones. Este estudio utilizó a JW Marriott Quito como ejemplo para mostrar los riesgos de ciberseguridad que tienen las principales empresas hoteleras y se definieron documentos que ayudaron a la restauración de los principales sistemas hoteleros, JW Marriott es una cadena hotelera de lujo que trabaja en un mercado muy competitivo y centrado en lo digital. Esto nos convirtió en un buen ejemplo de lo vulnerables que pueden llegar a ser los hoteles a los ciberataques. El estudio examinó de cerca la ciberseguridad de JW Marriott y cómo se respondió a los incidentes. El objetivo fue averiguar información importante que pueda utilizarse para elaborar y poner en práctica los planes de respuesta ante incidentes y que se pueda utilizar en propiedades similares.

Palabras clave: Incidentes de ciberseguridad, Empresas hoteleras, Ciber amenazas y Planes de respuesta a incidentes

ABSTRACT

In today's digital age, hotels rely heavily on technology, making them more vulnerable to cyberattacks. These attacks, such as ransomware, phishing, social engineering and system breaches, disrupted the operations of several hotels around the world and put guest data at risk. The threats extend to key systems such as reservation management, guest services and financial transactions, affecting business continuity and guest privacy. The hospitality industry is a vital part of the global economy and is responsible for serving countless travelers. With the increasing use of technology in this sector has made it more vulnerable to cyber-attacks. Even well-known hotel chains such as JW Marriott as they have suffered from different types of cyber threats that can lead to financial losses, reputational damage and legal issues. While hotel companies are aware of cyber risks, many do not have clear plans for responding to security incidents specific to their operations. This study used JW Marriott Quito as an example to show the cybersecurity risks that major hotel companies have and documents were defined that helped in the restoration of major hotel systems, JW Marriott is a luxury hotel chain that works in a very competitive and digital-centric market. This made us a good example of how vulnerable hotels can be to cyber-attacks. The study took a close look at JW Marriott's cybersecurity and how it responded to incidents. The goal was to find out important information that can be used to develop and implement incident response plans and that can be used at similar properties.

Keywords: Cybersecurity incidents, Hotel companies, Cyber threats and Incident response plans

CAPÍTULO I

EL PROBLEMA

1.1.Planteamiento del problema

El caso de estudio será JW Marriott Quito sirve como ejemplo ilustrativo de una marca hotelera líder que se enfrenta a retos de ciberseguridad. Como cadena mundial de hoteles de lujo, JW Marriott opera en un entorno altamente competitivo e impulsado digitalmente, lo que la hace susceptible a una amplia gama de amenazas cibernéticas como las que se presentaran en esta sección. Al examinar el panorama de la ciberseguridad y las prácticas de respuesta a incidentes de JW Marriott, se pueden obtener valiosos conocimientos para informar sobre el desarrollo y la aplicación de planes de respuesta adaptados en entornos hoteleros similares.

Actualmente JW Marriott Quito no cuenta con un plan de respuesta a incidentes de ciberseguridad por lo que si llega a existir una amenaza de este tipo no se tiene un lineamiento a seguir, este documento servirá para estructurar dichos lineamientos que utilizará la propiedad en caso de un desastre cibernético, también se pretende que este documento sirva como guía para otras propiedades hoteleras.

A continuación, se presentan cuatro casos donde se dieron violaciones de seguridad a empresas hoteleras:

Hoteles Hyatt (2015): Hyatt sufrió una importante filtración de datos en 2015, que afectó a la información de las tarjetas de pago de clientes que habían utilizado sus tarjetas de crédito o débito en determinados establecimientos gestionados por Hyatt en todo el mundo. (Pagnotta, Welivesecurity, 2016)

Hilton Worldwide (2015): Hilton sufrió una filtración de datos en 2015, en la que un malware infectó los sistemas de los puntos de venta de algunas de sus propiedades,

comprometiendo potencialmente la información de las tarjetas de pago de los clientes. (Pagnotta, Welivesecurity, 2015)

Starwood Hotels & Resorts (2016): En 2016, Starwood Hotels reveló una violación de datos que afectaba a más de 50 de sus propiedades. La brecha involucró malware instalado en sistemas de pago, exponiendo potencialmente información de tarjetas de pago. (Borner, 2018)

Marriott International (2018): Marriott reveló una violación masiva de datos en 2018, que afectó a aproximadamente 500 millones de huéspedes. La brecha se produjo dentro del sistema de reservas de huéspedes de Starwood, que Marriott había adquirido en 2016. Se comprometió información personal, incluidos números de pasaporte, fechas de nacimiento y detalles de contacto. (Borner, 2018)

El problema de los incidentes de ciberseguridad en las empresas hoteleras es una preocupación importante y creciente en el panorama digital actual. A medida que los hoteles dependen cada vez más de la tecnología para gestionar las reservas, los servicios a los huéspedes, el procesamiento de pagos y otras funciones críticas, se vuelven vulnerables a una serie de amenazas de ciberseguridad como el ransomware, phishing, ataques de ingeniería social, ataques a sistemas de puntos de venta (POS), ataques a sistemas de gestión hotelera (PMS), ataques a redes Wi-Fi, entre otros lo que afecta a los sistemas de puntos de ventas, de reservas, llaves magnéticas y a la integridad de los datos del huésped. (Jímenez, 2024)

La industria hotelera desempeña un papel crucial en la economía mundial, proporcionando alojamiento y servicios de hospitalidad a millones de huéspedes en todo el mundo. (Ceupe, 2024) Con la llegada de la digitalización y la integración de la tecnología en diversas facetas de las operaciones hoteleras, la ciberseguridad se ha convertido en una preocupación primordial. El sector hotelero, incluidas cadenas de renombre como JW Marriott,

se enfrenta a una multitud de amenazas cibernéticas que van desde la violación de datos a los ataques de ransomware, poniendo en peligro la confidencialidad, integridad y disponibilidad de la información sensible de los huéspedes y las operaciones críticas del negocio. (Jímenez, 2024)

Los incidentes de ciberseguridad en el sector hotelero pueden tener consecuencias devastadoras, como pérdidas económicas, daños a la reputación y responsabilidades legales. A pesar del reconocimiento de los riesgos de ciberseguridad, muchos hoteles carecen de planes sólidos de respuesta a incidentes adaptados para abordar los retos y complejidades únicos del sector hotelero. Esta laguna de conocimiento subraya la urgente necesidad de desarrollar planes de respuesta a incidentes de ciberseguridad completos y eficaces dentro de la industria hotelera. (Albornoz, 2022)

1.2.Interrogantes de la investigación

¿Qué amenazas específicas de ciberseguridad son más frecuentes en el sector hotelero y cómo afectan a las operaciones del hotel y a la seguridad de los datos de los huéspedes?

¿Cómo gestionan actualmente los incidentes de ciberseguridad las empresas hoteleras, incluidas las grandes cadenas como JW Marriott, y qué lagunas existen en sus estrategias de respuesta a incidentes?

¿Cuáles son los principales retos y complejidades a los que se enfrentan las empresas hoteleras a la hora de desarrollar y aplicar planes eficaces de respuesta a incidentes adaptados a sus requisitos operativos específicos?

¿Cómo puede el sector hotelero mejorar su resistencia frente a las ciber amenazas en evolución y salvaguardar la integridad de la información de los huéspedes y las operaciones empresariales críticas?

1.3.Objetivos de la investigación

1.3.1. Objetivo general

Implementar un plan de respuesta a incidentes de ciberseguridad aplicado a la industria hotelera para proveer de una efectiva respuesta para la toma de decisiones, considerando como caso de estudio al hotel JW Marriot de la ciudad de Quito

1.3.2. Objetivos específicos

- Determinar los principales incidentes de ciberseguridad que se suscitan en la industria hotelera.
- Identificar los activos y riesgos del hotel JW Marriott de Quito aplicando el marco metodológico NIST.
- Desarrollar un plan de respuesta para los incidentes de ciberseguridad identificados contemplando la legislación y la normativa interna vigente.
- Evaluar el plan de respuesta a incidentes de ciberseguridad para la toma de decisiones, aplicado al hotel JW Marriot como caso de estudio.

1.4.Hipótesis del trabajo

Elaborar un plan de respuesta a incidentes adaptado a los requisitos operativos de las empresas hoteleras, informados por los conocimientos obtenidos del panorama de ciberseguridad de JW Marriott, con el fin de mitigar salvaguardarán la información de los huéspedes y las operaciones comerciales críticas.

1.5.Hipótesis alternativa

Los planes de respuesta a incidentes desarrollados a partir de las prácticas de ciberseguridad de JW Marriott pueden no abordar adecuadamente los desafíos y complejidades a

los que se enfrentan las empresas hoteleras, lo que resulta en una vulnerabilidad continua a las amenazas cibernéticas y las operaciones comerciales.

1.6.Categorización de variables

Variable independiente. Implementar un plan de respuesta a incidentes de ciberseguridad aplicado a la industria hotelera.

Variable dependiente. Respuesta efectiva para la toma de decisiones.

1.7.Justificación

La tesis aborda un problema crítico en la industria hotelera, ejemplificado por la renombrada cadena JW Marriott, la necesidad de contar con planes fuertes de respuesta a incidentes de ciberseguridad. Esta necesidad está justificada por varios factores clave:

Aumento de las ciber amenazas: El sector hotelero está cada vez más en el punto de mira de los ciberdelincuentes debido a la gran cantidad de datos confidenciales almacenados en los sistemas de los hoteles, incluida la información de los huéspedes y los registros financieros. La proliferación de ciber amenazas, como los ataques de ransomware y las filtraciones de datos, plantea riesgos significativos para la confidencialidad, integridad y disponibilidad de las operaciones críticas de los hoteles. (Jímenez, 2024)

Falta de preparación: A pesar del creciente reconocimiento de los riesgos de ciberseguridad, muchos hoteles, incluido JW Marriott, carecen de planes integrales de respuesta a incidentes adaptados a sus necesidades operativas específicas. Esta deficiencia hace que los hoteles sean vulnerables a interrupciones prolongadas y agrava el impacto potencial de los incidentes cibernéticos en los huéspedes, los empleados y la continuidad del negocio.

Retos únicos del sector: El sector hotelero presenta desafíos únicos en términos de ciberseguridad, incluyendo la naturaleza descentralizada de las operaciones del hotel, la

dependencia de proveedores externos y las altas tasas de rotación de personal. Los marcos tradicionales de respuesta a incidentes suelen pasar por alto estos matices, por lo que se necesitan planes de respuesta según consideren las características distintivas de las operaciones hoteleras. (Jímenez, 2024)

Exigencias de cumplimiento normativo: Con la aplicación de estrictas normativas de protección de datos como General Data Protection Regulation (GDPR) y California Consumer Privacy Act (CCPA) (Duque, 2021), los hoteles se enfrentan a una mayor presión para garantizar la seguridad y privacidad de los datos de los huéspedes. El incumplimiento de estas normativas puede acarrear graves consecuencias legales y económicas, lo que subraya la necesidad imperiosa de adoptar medidas eficaces de respuesta ante incidentes.

Preservación de la reputación: En un sector en el que la reputación es primordial, las consecuencias de un incidente de ciberseguridad pueden ser muy perjudiciales. Una filtración de los datos de los clientes o la interrupción de los servicios pueden erosionar la confianza en la marca y disuadir a los clientes de volver a utilizarla en el futuro. (Alves, 2023)

CAPÍTULO II

MARCO REFERENCIAL

2.1 Antecedente

Según el contexto de estudio, se han identificado diferentes artículos científicos relacionados con el problema.

El artículo redactado por (Munir, 2020), Identifica y analiza una serie de amenazas a la red prevalentes y sugiere procedimientos y métodos prácticos de seguridad. Utilizando los datos más recientes y actualizados disponibles en el sector hotelero, este estudio constituye un valioso recurso para que los Chief Information Officers (CIO) y los directores de tecnologías de la información (TI) avancen en sus políticas y procedimientos de seguridad de la información electrónica en los hoteles.

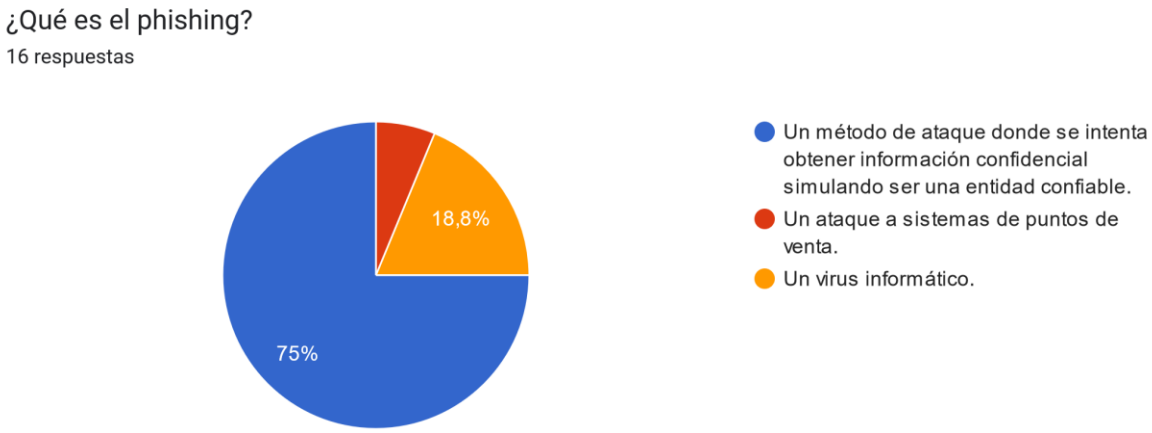
Tenemos también la metodología de (Neda & Arslan, 2020) aplicando un enfoque cualitativo único con un método de revisión para comprender los problemas del sector como se plantean en la realidad, los avances tecnológicos recientes y las soluciones útiles de los hoteles para gestionar y resolver estos problemas. Además, la investigación muestra que la mayoría de los empleados de los hoteles carecen de las habilidades y conocimientos necesarios para hacer frente a posibles riesgos, lo que hace que el sector hotelero sea aún más susceptible a las amenazas y ataques en línea. Con el fin de proteger los datos de hoteles y visitantes frente a las brechas de seguridad, el estudio concluye con algunas implicaciones y sugerencias para los responsables políticos del sector hotelero. Teniendo en cuenta que los empleados que están más expuestos son aquellos que tienden a servir, se dirigió una encuesta en la propiedad a este grupo con el fin de saber cuál es su nivel de conocimiento ante algunas amenazas comunes. (Alvarez, 2011)

Para este caso se seleccionan dos preguntas clave, relacionadas con el conocimiento acerca del phishing y los ataques a los POS, con esto podemos tener un entendimiento de cuál es el nivel de conocimiento que maneja el personal. (Guaña-Moya, et al., 2022)

La primera pregunta de la encuesta está relacionada con el phishing estaba orientada al área del Front Desk esto para saber si comprenden que significa el término, puesto que esta área es donde más actividades con el correo manejan.

FIGURA 1

¿QUÉ ES EL PHISHING?

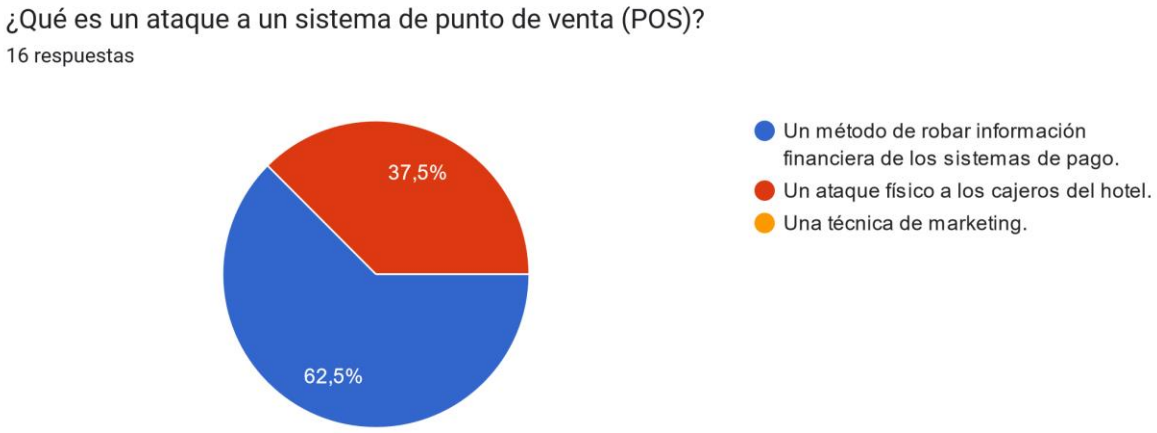


Nota: Encuesta orientada al entendimiento de los colaboradores hacia las amenazas existentes. Elaborada por Esteban Moyolema y realizada mediante Google Forms, junio de 2024

La segunda pregunta de la encuesta está orientada al departamento de alimentos y bebidas y de la misma forma el objetivo era entender si estaban al tanto de las amenazas que representaba el estar en un puesto como cajero.

FIGURA 2

¿QUÉ ES UN ATAQUE POS?



Nota: Encuesta orientada al entendimiento de los cajeros sobre que entienden por un ataque POS.

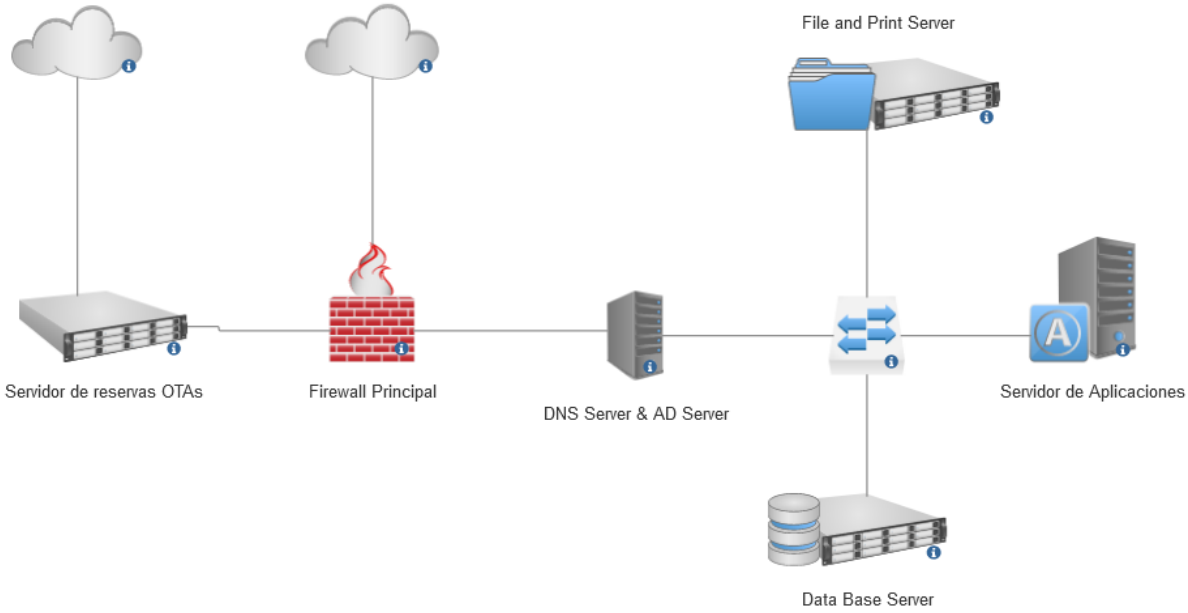
Encuesta elaborada por Esteban Moyolema y realizada mediante Google Forms, junio de 2024

Según (Aryee, 2020), trabajar con información individual de los huéspedes respecto a la elección del cliente y utilizar esos datos para generar experiencias únicas para estos es el pilar de las operaciones de la mayoría de los hoteles. Teniendo en cuenta ese importante papel, proteger la privacidad, la precisión y la accesibilidad de los datos de los visitantes es esencial para garantizar la felicidad y la fidelidad de los clientes. Según el estudio, la mayoría de los hoteles suelen ser objeto de ciberataques por la forma en que está configurada su infraestructura informática y cómo realizan su actividad.

Cuando los ciberdelincuentes se proponen acceder ilegalmente a la información de los huéspedes, los establecimientos se arriesgan a sufrir daños en su marca, multas y otros gastos. En el siguiente gráfico se muestra como usualmente los hoteles mantienen su infraestructura.

FIGURA 3

DIAGRAMA DE RED EN UN HOTEL



Nota: Diagrama general de la infraestructura de una red hotelera. E. Moyolema, diagrama común en redes hoteleras, realizado mediante SmartDrow, junio de 2024

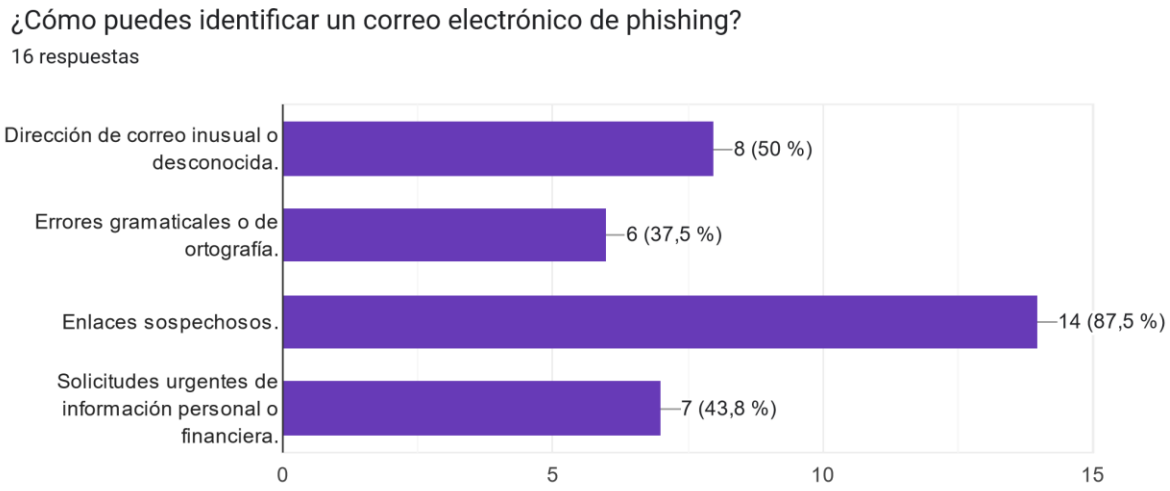
Esta información es aprovechada por los atacantes para buscar vectores de ataque por lo que se recomienda la segmentación de redes y el uso de IDS para prevenir daños en los sistemas y no solo de atacantes externos sino también de ataques internos. (Vivancos, 2022)

Podemos tomar en cuenta también el estudio realizado por (Shabani, 2016), según las entrevistas para este estudio que se realizaron en cinco hoteles diferentes de Reno, Nevada, en Estados Unidos de América. Se entrevistó a cincuenta clientes, diez empleados de recepción, tres directores de informática y dos asistentes del director general. Los resultados demuestran lo débil que es la ciberseguridad de los hoteles y lo expuestos que están en este ámbito por la falta de conocimiento del personal ante que hacer frente a un ataque informático o cómo manejar

posibles ataques de phishing. A continuación, se presentan los resultados obtenidos en la encuesta acerca del phishing en la propiedad JW Marriott Quito.

FIGURA 4

¿COMO IDENTIFICAR EL PHISHING?



Nota: Con el fin de determinar si un usuario puede diferenciar entre un correo normal y un phishing. Encuesta elaborada por Esteban Moyolema y realizada mediante Google Forms, junio de 2024

Cabe mencionar que cuando se tiene un nuevo ingreso de colaborador estos reciben una capacitación por parte del área de sistemas donde se les explica los riesgos de abrir un correo sospechoso y como identificarlos.

Finalmente tomamos como referencia a (Tong, Kong, & Kwan, 2022), el cual realiza un estudio para arrojar a la luz las estrategias útiles para construir y reforzar la ciberseguridad con el fin de detener y hacer frente a las violaciones de datos en el sector hotelero. Este informe examina una serie de incidentes de ciberataques ocurridos en hoteles de todo el mundo entre enero de 2014 y febrero de 2022. Con el fin de prevenir, identificar y responder a las violaciones de datos, se anima a hoteles, gobiernos y proveedores de tarjetas de pago y monederos

electrónicos a implementar y mejorar las medidas de ciberseguridad. Los hoteleros pueden utilizar la abundante información de este estudio para renovar su estructura organizativa, sus normas y sus métodos para mejorar la seguridad de los datos electrónicos en sus establecimientos.

2.2 Marco teórico

2.2.1 Incidente de ciberseguridad

Según él (NIST, 2021), Un incidente de ciberseguridad se refiere a cualquier evento malicioso o no autorizado que comprometa la confidencialidad, integridad o disponibilidad de los sistemas de información, redes o datos. Esto incluye, entre otros, ciberataques como infecciones de malware, violaciones de datos, ataques de denegación de servicio, amenazas internas y acceso no autorizado a sistemas o datos.

También tenemos la descripción de (United States Department of Homeland Security, 2020), Un incidente de ciberseguridad es un suceso que pone en peligro real o potencial la confidencialidad, integridad o disponibilidad de un sistema de información o de la información que el sistema procesa, almacena o transmite, o que constituye una violación o amenaza inminente de violación de las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable.

Un incidente de ciberseguridad es cualquier suceso que comprometa la confidencialidad, integridad o disponibilidad de los activos de información. Esto incluye el acceso no autorizado a sistemas o datos, infecciones de malware, violaciones de datos, ataques de denegación de servicio y amenazas internas. (ENISA, 2021)

Finalmente, según la ISO 27000:2018: Un incidente de ciberseguridad se refiere a cualquier suceso o serie de sucesos que supongan una amenaza real o potencial para la seguridad

de los sistemas de información, redes o datos de una organización. Abarca accesos no autorizados, filtraciones de datos, infecciones por malware, ataques de denegación de servicio y otras violaciones de la seguridad que pueden comprometer la confidencialidad, integridad o disponibilidad de los activos de información. (Lindemulder & Kosinski, 2024)

2.2.2 Incidentes de ciberseguridad en hotelería

En la industria hotelera, un incidente de ciberseguridad se refiere a cualquier evento o suceso que comprometa la seguridad de los sistemas de información, redes o datos del hotel. Esto incluye el acceso no autorizado a la información de los huéspedes, violaciones de datos de tarjetas de pago, infecciones de malware en los sistemas de reservas, ataques de phishing dirigidos al personal del hotel o a los huéspedes, y otras violaciones de seguridad que pueden poner en peligro la confidencialidad, integridad o disponibilidad de información sensible. Los incidentes de ciberseguridad en el sector hotelero pueden acarrear pérdidas financieras, daños a la reputación y responsabilidades legales para el hotel, así como afectar a la confianza y satisfacción de los huéspedes. (Security, 2021)

2.2.3 Principales Incidentes de ciberseguridad en el sector hotelero

Violación de datos: Acceso no autorizado a la información de los huéspedes, incluidos detalles personales, datos de tarjetas de pago y registros de reservas, que conducen al robo o exposición de datos.

Ataques de ransomware: El software malicioso cifra archivos o sistemas críticos, haciéndolos inaccesibles hasta que se paga un rescate, interrumpiendo las operaciones del hotel y comprometiendo potencialmente los servicios a los huéspedes. (Ayerdi, 2023)

Phishing e ingeniería social: Correos electrónicos, llamadas telefónicas o mensajes engañosos inducen al personal del hotel a divulgar información confidencial o a realizar acciones

que comprometen la seguridad, como facilitar credenciales de acceso o abrir archivos adjuntos maliciosos. (Aryee, 2020)

Ataques a sistemas de punto de venta (TPV): Los programas maliciosos atacan los terminales de punto de venta o los sistemas de procesamiento de pagos, interceptando los datos de las tarjetas de pago durante las transacciones, lo que provoca pérdidas económicas y daños a la reputación. (Rajiah, Las vulnerabilidades de seguridad de los sistemas de punto de venta y cómo abordarlas, 2020)

Ataques a sistemas de gestión hotelera: Los ciberdelincuentes aprovechan las vulnerabilidades del software de gestión hotelera para obtener acceso no autorizado a los sistemas de reservas, las bases de datos de huéspedes y los controles administrativos, lo que supone un riesgo para la privacidad de los huéspedes y la integridad operativa. (Ayerdi, 2023)

Ataques a redes Wi-Fi: Los piratas informáticos comprometen las redes Wi-Fi de los hoteles para interceptar las comunicaciones de los huéspedes, desplegar malware o realizar ataques man-in-the-middle, exponiendo potencialmente información sensible y comprometiendo la confianza de los huéspedes. (Ayerdi, 2023)

Amenaza interna: Una amenaza interna ocurre cuando individuos dentro de una organización abusan de sus privilegios de acceso para comprometer su seguridad deliberada o inadvertidamente. Puede tratarse de empleados que roban datos, filtran intencionadamente información confidencial o des configuran accidentalmente los sistemas. (Ayerdi, 2023)

Violaciones de la seguridad física: Acceso no autorizado a instalaciones físicas, como habitaciones de huéspedes, oficinas o centros de datos, que provoca robos, vandalismo o manipulación de infraestructuras y activos críticos. (Ayerdi, 2023)

2.2.4 Marco de ciberseguridad

Un marco de ciberseguridad es un conjunto estructurado de directrices, mejores prácticas y normas diseñadas para ayudar a las organizaciones a gestionar y mejorar su postura de ciberseguridad. Estos marcos proporcionan un enfoque sistemático para identificar, evaluar y mitigar los riesgos de ciberseguridad, así como para establecer procesos de detección de incidentes, respuesta y recuperación. Los marcos de ciberseguridad suelen esbozar objetivos, principios, controles y medidas clave de ciberseguridad que las organizaciones pueden adoptar para proteger sus sistemas de información, redes y datos frente a las ciber amenazas. (OEA, 2019)

Existen varios marcos de ciberseguridad ampliamente reconocidos y utilizados por organizaciones de todo el mundo, entre los que se incluyen:

Marco de Ciberseguridad del NIST: Desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), este marco proporciona un enfoque voluntario y basado en el riesgo para gestionar el riesgo de ciberseguridad. Consta de cinco funciones básicas: Identificar, Proteger, Detectar, Responder y Recuperar. (OEA, 2019)

ISO/IEC 27001: Esta norma internacional especifica los requisitos para establecer, implantar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información (SGSI). Proporciona un marco completo para gestionar los riesgos de seguridad de la información y proteger los activos de información sensibles. (Solutions, 20223)

Controles CIS: Desarrollados por el Centro para la Seguridad en Internet (CIS), los Controles CIS son un conjunto de acciones prioritarias que las organizaciones pueden llevar a cabo para mejorar su postura de ciberseguridad. Se dividen en tres categorías: Básica,

Fundacional y Organizativa, y abarcan una amplia gama de controles de seguridad y mejores prácticas. (Tunggal, 2023)

COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas): Desarrollado por ISACA, COBIT es un marco para regir y gestionar el gobierno y la gestión de las TI empresariales. Proporciona un amplio conjunto de directrices y mejores prácticas para alinear las TI con los objetivos empresariales y gestionar los riesgos relacionados con las TI. (Simplilearn, 2024)

ITIL (Biblioteca de Infraestructuras de Tecnologías de la Información): ITIL es un conjunto de mejores prácticas para la gestión de servicios de TI (ITSM) que se centra en alinear los servicios de TI con las necesidades de la empresa. Aunque no es específicamente un marco de ciberseguridad, ITIL incluye procesos y controles relacionados con la gestión de incidentes de ciberseguridad, la continuidad del servicio y la gestión de riesgos. (Rouse, 2024)

2.2.5 NIST

El Instituto Nacional de Normas y Tecnología (NIST) es una agencia no reguladora del Departamento de Comercio de los Estados Unidos. Fundado en 1901, la misión del NIST es promover la innovación y la competitividad industrial mediante el avance de la ciencia de la medición, las normas y la tecnología. (Technology, 2021)

El NIST desempeña un papel crucial en el desarrollo y mantenimiento de normas de medición, tecnología y directrices de ciberseguridad para aumentar la seguridad económica de la nación y mejorar la calidad de vida de los estadounidenses. Actúa como asesor de confianza de los organismos gubernamentales, la industria y el mundo académico en una amplia gama de asuntos científicos y técnicos. (Technology, 2021)

La ciberseguridad consiste en proteger los sistemas y redes informáticos de accesos no autorizados. El NIST elabora directrices para proteger infraestructuras importantes. Crean normas como el Marco de Ciberseguridad. Ayuda a las organizaciones a gestionar los riesgos de ciberseguridad. El NIST también publica series de Publicaciones Especiales (SP) y otros recursos. (Law, 2023)

El NIST fomenta la innovación y la transferencia de tecnología. Proporcionan financiación para la investigación. Ofrecen ayuda técnica. Las organizaciones pueden acceder a las instalaciones y los expertos del NIST. El NIST colabora con la industria, las universidades y otras entidades. Impulsan tecnologías emergentes como la IA, la computación cuántica y la fabricación avanzada. (Law, 2023)

El NIST desempeña un papel clave en la elaboración de normas y guías de ciberseguridad. Estas ayudan a proteger sistemas importantes, redes gubernamentales y empresas privadas. El NIST desarrolla el Marco de Ciberseguridad, Publicaciones Especiales y otras herramientas. Las organizaciones las utilizan para gestionar y reducir los riesgos de ciberseguridad. (Technology, 2021)

El NIST apoya las nuevas ideas y el intercambio de tecnología. Proporciona financiación para la investigación, ayuda técnica y acceso a instalaciones y expertos avanzados. El NIST trabaja con la industria, las escuelas y otras entidades. Esto ayuda a hacer avanzar tecnologías emergentes como la IA, la computación cuántica y la fabricación avanzada. (Technology, 2021)

Aunque el propio NIST es un organismo no regulador, sus normas y directrices son adoptadas a menudo por organismos reguladores, consorcios industriales y organizaciones internacionales como mejores prácticas o requisitos normativos. Por ejemplo, el Marco de Ciberseguridad del NIST ha sido ampliamente adoptado por las organizaciones como un marco

voluntario para la gestión de los riesgos de ciberseguridad, y algunos sectores, como las agencias gubernamentales federales y los sectores de infraestructuras críticas, están obligados a cumplir con las normas y directrices del NIST. (Technology, 2021)

2.2.6 Evaluación de la encuesta

En el marco teórico, las encuestas realizadas en diversas áreas clave del hotel, incluidos los departamentos de comidas y bebidas, finanzas y recepción, se guiarán por los principios establecidos de la metodología de investigación mediante encuestas. El proceso de evaluación consistirá en valorar la validez, fiabilidad y calidad general del instrumento de encuesta para garantizar que mide eficazmente los constructos previstos y produce datos fiables para el análisis. Los criterios de evaluación incluyen la validez del contenido, que garantiza que la encuesta cubre adecuadamente las dimensiones y variables claves pertinentes para los objetivos de la investigación, y pruebas de fiabilidad como la coherencia interna y la fiabilidad test-retest para garantizar resultados coherentes a lo largo del tiempo y entre los encuestados. (Law, 2023)

La validez de constructo se evaluará mediante análisis para examinar la estructura de los ítems de la encuesta y evaluar su validez convergente y discriminante. Se tomarán medidas para minimizar el sesgo de respuesta, como garantías de anonimato y confidencialidad, instrucciones claras y el uso de técnicas de aleatorización. Además, se llevarán a cabo pruebas piloto para evaluar la claridad, la comprensibilidad y la facilidad de uso del instrumento de encuesta a través de los comentarios solicitados a una pequeña muestra de encuestados, guiados por los principios descritos en "La práctica de la investigación social" de Babbie, un libro de texto completo que proporciona orientación sobre el diseño de la investigación de encuestas, la recopilación de datos y el análisis. (Law, 2023)

2.2.7 Plan de respuesta ante una amenaza de ciberseguridad

Según (Technology, 2021) un plan de respuesta a incidentes de ciberseguridad es un conjunto estructurado de procedimientos y protocolos diseñados para guiar eficazmente la respuesta de una organización a incidentes de ciberseguridad. En él se describen las funciones, responsabilidades y medidas que deben adoptar las partes interesadas de la organización para detectar, contener, mitigar y recuperarse de las violaciones o incidentes de ciberseguridad. El plan suele incluir pasos para identificar y clasificar los incidentes, evaluar su gravedad e impacto, notificar a las partes interesadas pertinentes, coordinar los esfuerzos de respuesta, preservar las pruebas para la investigación y restaurar los sistemas y datos afectados para que vuelvan a funcionar con normalidad. El objetivo de un plan de respuesta a incidentes de ciberseguridad es minimizar el impacto de los incidentes, mitigar los daños futuros y garantizar que la organización pueda recuperarse rápida y eficazmente de las ciber amenazas.

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Descripción del área de estudio

En el panorama digital actual, el sector de la hostelería se enfrenta a una serie de amenazas importantes que pueden comprometer la seguridad y la integridad de sus operaciones. Estas amenazas, que van desde el ransomware y la fuga de datos hasta el malware y el tiempo de inactividad, plantean graves riesgos para el buen funcionamiento de los establecimientos hosteleros y la seguridad de la información confidencial de los clientes. Por ello, es imperativo que las partes interesadas de los distintos departamentos comprendan la gravedad de estos riesgos y las medidas necesarias para mitigarlos eficazmente.

Para el personal de recepción responsable de la utilización de los sistemas de gestión de la propiedad (PMS), es esencial una comprensión completa de las amenazas digitales. Los sistemas PMS son esenciales para gestionar las reservas, el registro de los huéspedes y las operaciones generales del hotel. Sin embargo, también representan un objetivo prioritario para los ciberataques, incluidos el ransomware y la infiltración de malware. El personal de recepción debe ser educado en las mejores prácticas para acceder y gestionar de forma segura los sistemas PMS, así como para reconocer y responder a posibles brechas de seguridad con prontitud. (Haenraets, 2024)

El personal de los puntos de venta desempeña un papel fundamental para salvaguardar los datos de pago de los clientes y garantizar la seguridad de las transacciones. Con la creciente prevalencia de las ciber amenazas dirigidas a los sistemas de punto de venta, como los programas maliciosos de extracción de datos y el robo de información de tarjetas de pago, el personal de los puntos de venta debe recibir formación para identificar actividades sospechosas y cumplir

estrictamente los protocolos de seguridad. Esto incluye la actualización periódica del software de los TPV, la aplicación de medidas de cifrado y la vigilancia frente a intentos de phishing y otras tácticas de ingeniería social. (Stripe, 2024)

Además, la colaboración con el director de TI o el responsable de la gestión de datos de tarjetas bancarias es primordial para establecer una defensa sólida contra las amenazas digitales en el sector de la hostelería. Como custodio de la infraestructura crítica y de los protocolos de seguridad de datos, el director de TI desempeña un papel fundamental en la aplicación de medidas de ciberseguridad, la realización de evaluaciones de riesgos y la fortificación de las defensas de la red. La estrecha coordinación entre el personal de primera línea y el personal de TI garantiza que las políticas y los procedimientos de seguridad se comuniquen y apliquen eficazmente en toda la organización, minimizando así las vulnerabilidades y las posibles infracciones. (Staff, 2024)

En resumen, hacer frente a las amenazas digitales en el sector de la hostelería requiere un enfoque polifacético que implique educación, colaboración y medidas de seguridad proactivas en todos los niveles de la organización. Al dotar al personal de recepción y cajeros de los conocimientos y herramientas necesarios para reconocer y responder a las ciber amenazas, y al fomentar una cultura de vigilancia y responsabilidad bajo la dirección de los responsables de TI, los establecimientos hosteleros pueden mejorar su resistencia frente a los riesgos de ciberseguridad en constante evolución y salvaguardar la confianza de sus clientes. (Vargas, 2024)

3.2 Enfoque y tipo de investigación

En consonancia con el carácter exploratorio de este estudio, se empleará una estrategia cualitativa para la recopilación y el análisis de datos primarios para examinar cómo diseñar y

reforzar la ciberseguridad y prevenir y atajar la filtración de datos en la industria hotelera. Se seleccionarán entrevistas semi estructuradas como método de recopilación de datos porque proporciona a los encuestados la flexibilidad necesaria para expresar sus opiniones libremente. (Kong, 2022)

3.3 Procedimiento de investigación

Fase 1: En esta fase se habrían determinado los principales incidentes de ciberseguridad que se suscitan en la industria hotelera.

También se realizó entrevistas semi estructuradas con el personal del hotel de los departamentos de Alimentos y Bebidas, Recepción y Finanzas, con el fin de desarrollar una guía de entrevista que consista en preguntas relacionadas con incidentes de ciberseguridad experimentados por el hotel en el pasado, incidentes experimentados en otros hoteles, la frecuencia de estos, el impacto y las medidas de respuesta adoptadas.

Seleccionando una muestra representativa del personal del hotel de cada departamento, garantizando la diversidad en roles laborales y niveles de experiencia. Se tratará de contar con aproximadamente 3 participantes, de los 3 departamentos.

Mediante el uso del análisis temático para identificar patrones y temas recurrentes en las respuestas de la entrevista. Clasificaremos los incidentes de ciberseguridad según su naturaleza, gravedad e impacto en las operaciones del hotel.

Fase 2: Identificando los principales activos y riesgos del hotel JW Marriott Quito aplicando el marco metodológico NIST.

Una vez se identificó todos los activos digitales y la infraestructura dentro del Hotel JW Marriott en Quito que son críticos para sus operaciones, incluyendo, pero no limitado a:

- Sistema de Gestión de la Propiedad (PMS)

- Sistemas de Punto de Venta (POS)
- Sistemas de bloqueo de puertas
- Red Wi-Fi para huéspedes
- Bases de datos de empleados

Para conocer las vulnerabilidades y amenazas potenciales asociadas a cada activo identificado.

Vulnerabilidades y exploits, con la probabilidad de que se produzcan amenazas (por ejemplo, infección por malware, violación de datos). Teniendo un impacto potencial en las operaciones del hotel, la seguridad de los huéspedes y la reputación. También con controles de seguridad y salvaguardas existentes utilizando metodologías de evaluación de riesgos como el análisis de riesgos cualitativo o cuantitativo para priorizar los riesgos identificados.

Basados en los resultados de la identificación de activos y el análisis de riesgos, desarrollar recomendaciones para mejorar la postura de seguridad del Hotel JW Marriott en Quito. Priorizar las recomendaciones basándose en el nivel de riesgo y el impacto potencial en las operaciones del hotel. Alinear las recomendaciones con las mejores prácticas de la industria, los requisitos reglamentarios y las políticas internas para garantizar el cumplimiento y la eficacia. Al llevar a cabo la identificación de activos y el análisis de riesgos específicamente adaptados al Hotel JW Marriott de Quito

Después de utilizar el marco de gestión de riesgos del NIST (Instituto Nacional de Normas y Tecnología) para orientar la identificación de activos y el análisis de riesgos.

Realizamos entrevistas con el personal clave responsable de la infraestructura y la seguridad de TI en el hotel JW Marriott de Quito.

Fase 3: En esta fase se desarrolló un plan de respuesta a los incidentes de ciberseguridad identificados, teniendo en cuenta la legislación vigente y la normativa interna.

Se realizó un análisis bibliográfico sobre las regulaciones de ciberseguridad, los estándares de la industria y las políticas internas relevantes. Se realizarán entrevistas con consultores en ciberseguridad para recopilar información sobre las mejores prácticas para la planificación de respuesta a incidentes.

Sintetizando información de documentos reglamentarios, estándares de la industria y entrevistas con especialistas para identificar componentes clave de un plan de respuesta a incidentes. Incorporar consideraciones como requisitos legales, regulaciones de protección de datos y desafíos específicos de la industria que enfrenta la industria hotelera.

Fase 4: Se evalúa el plan de respuesta a incidentes de ciberseguridad aplicado al hotel JW Marriott como caso de estudio.

Generamos el plan de respuesta a incidentes implementado por el hotel JW Marriott. Se realizarán las entrevistas con el personal clave involucrado en el desarrollo e implementación del plan de respuesta.

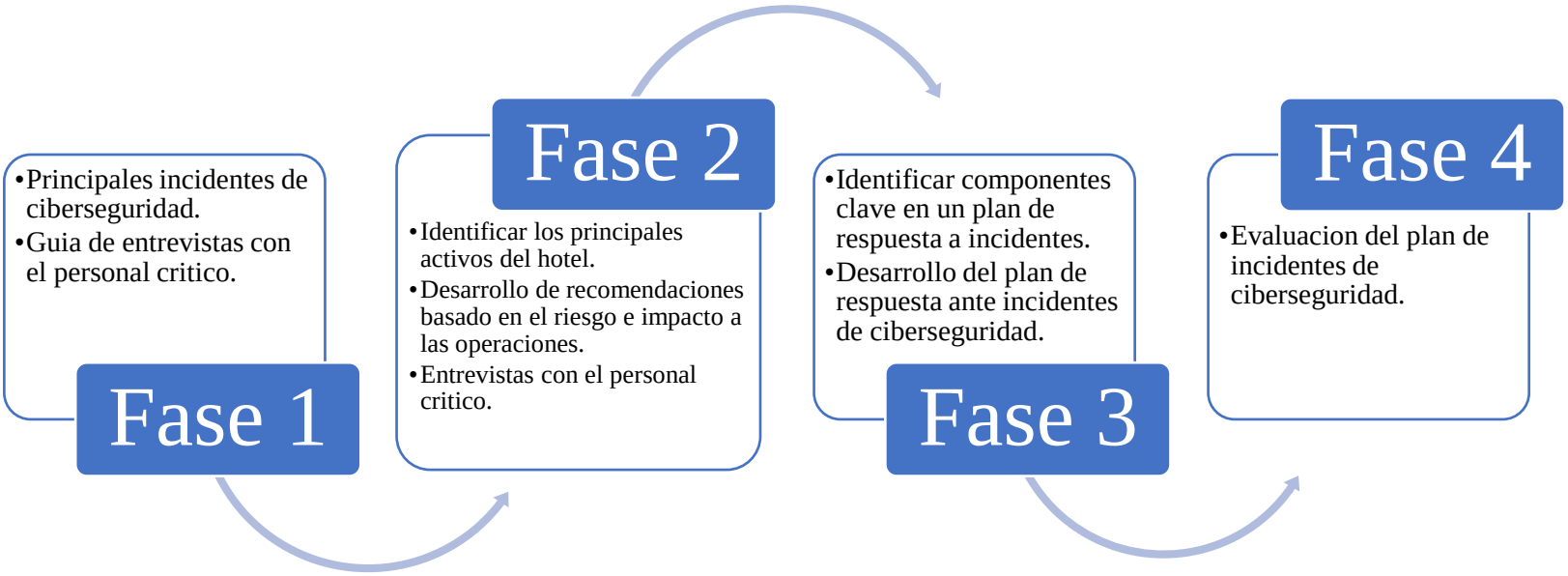
Seleccionando personas de diferentes departamentos involucrados en la respuesta a incidentes, como TI, seguridad y administración. Utilizando un enfoque de análisis comparativo para evaluar el plan de respuesta a incidentes de JW Marriott en comparación con las mejores prácticas y los requisitos reglamentarios identificados.

Después se evaluarán las fortalezas, debilidades y áreas de mejora del plan según los hallazgos de la entrevista y la revisión de documentos

3.3.1 Flujo de fases y actividades

FIGURA 5

FLUJO DE FASES



Nota: Se describe cuáles serán las fases para realizar para completar el capítulo 4, junio de 2024

3.4 Consideraciones bioéticas

Ciertamente, es crucial garantizar la transparencia y la confidencialidad al realizar entrevistas con fines de investigación, especialmente cuando se discuten temas delicados como los incidentes de ciberseguridad. Así se informará a los participantes sobre el anonimato y los objetivos de la entrevista:

Se informará a los participantes antes de la entrevista que su identidad permanecerá anónima durante todo el proceso de investigación. Esto significa que cualquier información que proporcionen se utilizará únicamente con fines de investigación y no se les atribuirá personalmente. Sus nombres, puestos de trabajo y cualquier detalle de identificación se mantendrán confidenciales para proteger su privacidad.

Además, se asegurará a los participantes que el objetivo de la entrevista es identificar patrones o brechas en los procedimientos de respuesta a incidentes de ciberseguridad para futuras mejoras. El propósito no es asignar culpas o criticar acciones individuales, sino más bien obtener información sobre cómo los sistemas informáticos se ven afectados por los ciberataques y cómo estos impactos pueden mitigarse en el futuro.

Se alentará a los participantes a hablar de manera abierta y honesta sobre sus experiencias y observaciones relacionadas con incidentes de ciberseguridad. Se les recordará que sus aportes son valiosos para mejorar la resiliencia de los sistemas informáticos del hotel y garantizar la continuidad de las operaciones en caso de un ataque.

Durante todo el proceso de la entrevista, se mantendrá la confidencialidad y cualquier información compartida por los participantes se tratará con la máxima discreción. Solo se utilizarán datos agregados y anonimizados para análisis e informes, garantizando que las contribuciones individuales no puedan rastrearse hasta individuos específicos.

CAPÍTULO IV

DESARROLLO

4 Desarrollo de objetivo

4.1 Analizar los principales incidentes de ciberseguridad en la industria hotelera

La industria hotelera ha tenido varios incidentes de ciberseguridad y los podemos englobar de la siguiente manera:

4.1.1 Filtración de datos

Las filtraciones de datos se han convertido en una de las amenazas de ciberseguridad más graves a las que se enfrenta la industria hotelera. Estos incidentes implican el acceso no autorizado a datos sensibles, incluida la información personal y financiera de los huéspedes, lo que puede dar lugar a importantes pérdidas financieras, daños a la reputación y sanciones reglamentarias para las organizaciones afectadas. Comprender el alcance, el impacto y las medidas preventivas relacionadas con las violaciones de datos es esencial para garantizar una ciberseguridad sólida en el sector hotelero.

Marriott International (2018): Uno de los incidentes más significativos, donde los hackers accedieron a la base de datos de reservas, comprometiendo la información personal de alrededor de 500 millones de huéspedes, incluidos nombres, direcciones, números de teléfono, direcciones de correo electrónico, números de pasaporte e información de tarjetas de crédito. La brecha se atribuyó a un sofisticado ciberataque que comenzó en 2014, antes de la adquisición de Starwood por parte de Marriott en 2016. Los atacantes explotaron vulnerabilidades en los sistemas de Starwood para obtener acceso persistente. La brecha resultó en costos financieros significativos, incluyendo multas regulatorias de £ 18,4 millones por la Oficina del Comisionado de Información del Reino Unido, honorarios legales y compensación para los huéspedes afectados.

Marriott también sufrió daños en su reputación y perdió la confianza de sus clientes. (News, 2018)

Podemos tomar medidas preventivas y aplicar buenas prácticas como las que se detallan a continuación.

1. Protocolos de seguridad reforzados
    - Realización de auditorías de seguridad exhaustivas y frecuentes para identificar y corregir las vulnerabilidades de los sistemas informáticos del hotel.
    - Garantizar que todos los datos sensibles, tanto en tránsito como en reposo, estén cifrados utilizando estándares de cifrado fuertes.
2. Formación de los empleados
    - Implantación de programas regulares de formación para educar a los empleados sobre los riesgos de los ataques de phishing e ingeniería social y sobre cómo reconocer y responder a actividades sospechosas.
    - Aplicar controles de acceso estrictos y garantizar que los empleados tengan el acceso mínimo necesario para desempeñar sus funciones.
3. Detección y respuesta a amenazas avanzadas
    - Despliegue de IDS e IPS para supervisar el tráfico de red en busca de indicios de actividad maliciosa y responder automáticamente a las amenazas.

4.1.2 Ataques de Ransomware

Los ataques de ransomware representan una de las amenazas de ciberseguridad más perturbadoras para la industria hotelera. Estos ataques implican el uso de software malicioso que

cifra los datos de la víctima, dejando inoperativos los sistemas críticos hasta que se paga un rescate. El impacto de estos incidentes puede ser devastador, provocando importantes tiempos de inactividad operativa, pérdidas financieras y daños a la reputación. Comprender la naturaleza de los ataques de ransomware, su impacto en la industria hotelera y las estrategias de prevención y respuesta es esencial para garantizar una ciberseguridad sólida y la continuidad del negocio. (Alawida, 2022)

Los hoteles y cadenas más pequeños se han convertido cada vez más en blanco de ataques de ransomware debido a sus recursos de ciberseguridad, a menudo limitados. Por ejemplo, en 2017, el Romantik Seehotel Jägerwirt en Austria experimentó un ataque de ransomware que bloqueó a los huéspedes de sus habitaciones al desactivar el sistema de tarjeta de llave electrónica del hotel. El ataque interrumpió las operaciones, impidiendo a los huéspedes acceder a sus habitaciones y causando importantes molestias. (Belton, 2017) El hotel tuvo que pagar el rescate para restablecer la funcionalidad, lo que provocó pérdidas económicas directas y daños a su reputación. Este incidente subrayó la importancia de proteger todos los aspectos de las operaciones hoteleras, incluidos los sistemas electrónicos de tarjetas llave, y puso de relieve la necesidad de adoptar medidas de ciberseguridad exhaustivas incluso para los establecimientos más pequeños.

En 2017, los ataques de ransomware WannaCry y NotPetya tuvieron un impacto global, afectando a múltiples industrias, incluido el sector hotelero. Las principales cadenas hoteleras experimentaron interrupciones en sus sistemas de reservas, el ransomware encriptó sistemas críticos, lo que provocó tiempos de inactividad en los sistemas de reservas, servicios a huéspedes y operaciones internas. (Trautman, 2018)

Podemos tomar medidas preventivas y aplicar buenas prácticas como las que se detallan a continuación.

1. Buenas prácticas
    - Garantizar que todo el software, incluidos los sistemas operativos, las aplicaciones y el firmware, se actualiza y parchea periódicamente para cerrar las vulnerabilidades conocidas que el ransomware puede explotar.
    - Implementar la segmentación de la red para limitar la propagación del ransomware dentro de la red de la organización.
2. Detección y respuesta ante amenazas avanzadas
    - Despliegue de soluciones EDR para supervisar continuamente los endpoints en busca de indicios de actividad maliciosa.
    - Utilización de herramientas de análisis de comportamiento para detectar patrones de comportamiento inusual.
3. Copias de seguridad y respaldos
    - Implementar una estrategia integral de copias de seguridad que incluya copias de seguridad periódicas y automatizadas de los datos críticos. Las copias de seguridad deben almacenarse sin conexión o en un entorno seguro en la nube para evitar que se vean comprometidas durante un ataque.
    - Probar periódicamente los procesos de restauración de copias de seguridad para garantizar que los datos puedan restaurarse de forma rápida y fiable en caso de ataque de ransomware.

4.1.3 Ataques a sistemas POS

Los ataques a los sistemas de punto de venta (PoS) según (Jímenez, 2024): se han convertido en una importante amenaza para la ciberseguridad en el sector hotelero. Estos ataques se dirigen a los sistemas responsables de procesar los pagos, con el objetivo de robar información confidencial de las tarjetas de crédito de los huéspedes.

InterContinental Hotels Group (IHG) (2017) (ROLFE, 2017): Un malware infectó los sistemas PoS en varias propiedades, comprometiendo los datos de las tarjetas de pago de los huéspedes. La brecha afectó a aproximadamente 1.200 hoteles franquiciados en América y el malware capturó datos de tarjetas de pago, incluidos nombres de titulares de tarjetas, números de tarjetas, fechas de caducidad y códigos de verificación internos. La brecha se facilitó a través de un malware que se infiltró en los sistemas PoS, permitiendo a los atacantes recopilar información de tarjetas de crédito durante las transacciones.

Hoteles Trump (2014-2017) (Schwartz, 2015): Una serie de filtraciones a lo largo de varios años expusieron información de tarjetas de crédito y otros datos personales debido a un malware en los sistemas PoS.

Según (Bower, 2016) en el hotel Hyatt, En diciembre de 2015, Hyatt informo de una filtración de datos causada por malware dirigido a sus sistemas de PoS en 250 establecimientos de 50 países. La brecha expuso información de tarjetas de crédito, incluidos nombres de titulares de tarjetas, números de tarjetas, fechas de caducidad y códigos de verificación.

Podemos tomar medidas preventivas y aplicar buenas prácticas como las que se detallan a continuación.

1. Seguridad en los sistemas PoS

- Garantizar que todos los sistemas de PoS y el software asociado se actualizan y parchean periódicamente para protegerlos frente a vulnerabilidades conocidas.
- Implementar el cifrado de extremo a extremo para todos los datos de tarjetas de pago procesados por los sistemas PoS, garantizando que los datos estén protegidos tanto en tránsito como en reposo.

2. Seguridad en la red
    - Segregar los sistemas PoS de otras partes de la red del hotel para limitar la propagación de malware y reducir la superficie de ataque.
3. Protección contra malware
    - Utilización de herramientas antimalware avanzadas diseñadas específicamente para detectar y prevenir el malware de punto de venta. Estas herramientas deben incluir supervisión en tiempo real y análisis heurístico para identificar y detener las amenazas nuevas y en evolución.
    - Realización de escaneos y auditorías de seguridad frecuentes de los sistemas PoS

4.1.4 Ataques de phishing e ingeniería social

Los ataques de phishing y de ingeniería social según (Árnason, 2024) se encuentran entre las ciber amenazas más frecuentes y eficaces a las que se enfrenta el sector hotelero en la actualidad. Estos ataques se aprovechan de la psicología humana para engañar a empleados y huéspedes con el fin de que divulguen información confidencial o realicen acciones que comprometan la seguridad. Dado el elevado volumen de datos confidenciales que manejan los hoteles -desde los datos personales de los huéspedes hasta la información de pago-, comprender

los mecanismos, el impacto y las contramedidas del phishing y la ingeniería social es esencial para mantener una ciberseguridad sólida.

Según (Lazaricheva, 2024) en 2020, una importante cadena hotelera sufrió un sofisticado ataque de phishing dirigido a sus empleados. Los atacantes enviaron correos electrónicos que parecían proceder del departamento de TI del hotel, solicitando a los empleados que actualizaran sus credenciales de inicio de sesión en un portal falso. Varios empleados fueron víctimas de la estafa, proporcionando sus datos de acceso a los atacantes. Esta brecha dio lugar a un acceso no autorizado a los sistemas internos del hotel, comprometiendo datos sensibles y pudiendo provocar nuevos incidentes de seguridad. El incidente puso de relieve la necesidad crítica de programas continuos de formación y concienciación de los empleados para reconocer y responder a los intentos de phishing.

Esta misma empresa recibió llamadas telefónicas de individuos que se hacían pasar por soporte informático, alegando que necesitaban acceso remoto para solucionar un problema técnico. Confiando en las personas que llamaban, el personal proporcionó credenciales de acceso remoto, lo que permitió a los atacantes infiltrarse en los sistemas del hotel (Lazaricheva, 2024)

Podemos tomar medidas preventivas y aplicar buenas prácticas como las que se detallan a continuación.

1. Formación y concienciación de los empleados
    - Implantar sesiones de formación continua para educar a los empleados sobre las últimas técnicas de phishing y tácticas de ingeniería social. La formación debe abarcar cómo identificar correos electrónicos, enlaces y llamadas telefónicas sospechosos.

- Llevar a cabo simulaciones regulares de phishing para poner a prueba la conciencia de los empleados y mejorar su capacidad para reconocer y responder a los intentos de phishing.

2. Autenticación de multifactor o MFA
    - Exigir MFA para acceder a sistemas y datos sensibles. MFA añade una capa adicional de seguridad, dificultando el acceso a los atacantes incluso si obtienen las credenciales de inicio de sesión mediante phishing.
3. Procesos de verificación
    - Implantación de procesos de verificación estrictos para las transacciones financieras, como exigir múltiples aprobaciones y confirmación verbal para las transferencias de fondos de gran cuantía.
    - Formar al personal para que verifique la identidad de las personas que llaman solicitando información sensible o acceso al sistema.

4.1.5 Vulnerabilidades en las redes Wi-Fi

Según (Bardají, 2022) las vulnerabilidades de las redes Wi-Fi plantean importantes riesgos de ciberseguridad en el sector hotelero. Los hoteles ofrecen servicios Wi-Fi a sus huéspedes, lo que convierte a sus redes en objetivos atractivos para los ciberdelincuentes. Las redes Wi-Fi comprometidas pueden dar lugar a un acceso no autorizado a información confidencial de los huéspedes y a sistemas internos, y pueden facilitar otros ataques como la distribución de malware y los ataques man-in-the-middle. Comprender estas vulnerabilidades, su impacto y aplicar medidas de seguridad sólidas es crucial para proteger tanto las operaciones del hotel como la privacidad de los huéspedes.

La comisión federal de comunicaciones, multo a Marriott International en el 2014 con un monto de 600.000 de dólares por interferir las redes Wi-Fi personales de los huéspedes para obligarles a utilizar el servicio del Hotel. Este incidente puso de relieve los riesgos asociados a la gestión de redes Wi-Fi y la necesidad de prácticas legales y seguras a la hora de proporcionar conectividad a los huéspedes. Aunque no se trató directamente de una violación de datos, el incidente llamó la atención sobre la importancia de unas prácticas Wi-Fi transparentes y seguras. (Donelson, 2014)

Auditoria de redes inalámbricas en hoteles, Investigadores de seguridad descubrieron vulnerabilidades en las redes Wi-Fi de varios hoteles de lujo. Estas vulnerabilidades permitían a los atacantes interceptar y manipular el tráfico de los huéspedes, obteniendo acceso a información personal y credenciales de inicio de sesión. Los huéspedes de estos hoteles corrían el riesgo de sufrir robos de identidad, fraudes financieros y otros delitos informáticos. Los hoteles se enfrentaron a daños en su reputación y a posibles consecuencias legales debido a la seguridad comprometida de sus redes. Las evaluaciones periódicas de la seguridad y el análisis de vulnerabilidades de las redes Wi-Fi son esenciales para identificar y mitigar los riesgos potenciales. (Chehayeb, 2022)

Podemos tomar medidas preventivas y aplicar buenas prácticas como las que se detallan a continuación.

- Cifrado avanzado y autenticación
    - Implantación de WPA3 en todas las redes inalámbricas para proporcionar un cifrado robusto y proteger contra ataques de fuerza bruta.
    - Utilización de la autenticación 802.1X con un servidor RADIUS para un control seguro del acceso a la red.

- Gestión de los puntos de acceso
    - Garantizar que todos los puntos de acceso estén configurados de forma segura con contraseñas seguras.
    - Asegurar físicamente los puntos de acceso para evitar manipulaciones o reinicios no autorizados.
- Segmentación de la red
    - Uso de VLAN (redes de área local virtuales) para segmentar el tráfico de red y aislar las redes de huéspedes de los sistemas internos del hotel.
    - Activación del aislamiento de clientes en redes Wi-Fi de huéspedes para evitar que los dispositivos se comuniquen directamente entre sí, reduciendo el riesgo de ataques laterales.
- Pruebas de penetración y auditorias
    - Realización de auditorías de seguridad y pruebas de penetración periódicas de las redes Wi-Fi para identificar y corregir vulnerabilidades.
    - Implementar soluciones de monitorización continua para detectar actividades sospechosas y accesos no autorizados en tiempo real.

4.1.6 Amenazas internas

Incidentes relacionados con empleados que, o bien hacen un mal uso intencionado de su acceso a los sistemas del hotel, o bien exponen inadvertidamente información sensible por acciones negligentes.

4.2 Guía de entrevistas con personal crítico de la empresa

La técnica aplicada para la recolección de datos en esta ocasión será la entrevista con 10 preguntas, el grupo de estudio es el personal del Hotel JW Marriott en Quito en específico la

entrevista se centrará en tres áreas en Alimentos y Bebidas: Cajeros, Personal de Front Office: Recepcionistas y Personal de Finanzas: Crédito y Cobro.

Antes de la entrevista se informará a los participantes de que su identidad permanecerá anónima durante todo el proceso de investigación. Esto significa que cualquier información que proporcionen se utilizará únicamente con fines de investigación y no se les atribuirá personalmente. Sus nombres, cargos y demás datos identificativos serán confidenciales para proteger su intimidad

Además, se asegurará a los participantes que el objetivo de la entrevista es identificar patrones o lagunas en los procedimientos de respuesta a incidentes de ciberseguridad para mejorarlos en el futuro. El propósito no es culpar o criticar acciones individuales, sino más bien obtener información sobre cómo se ven afectados los sistemas informáticos por los ciberataques y cómo se pueden mitigar estos impactos en el futuro.

4.2.1 Procedimiento de la entrevista

Objetivo: Recopilar datos cualitativos sobre las experiencias, desafíos y prácticas relacionadas con los incidentes de ciberseguridad y las estrategias de respuesta en la industria hotelera, centrándose específicamente en el Hotel JW Marriott de Quito.

4.2.2 Preguntas de la entrevista

Concienciación sobre la ciberseguridad

1.- ¿Puede describir algún programa de formación o concienciación sobre ciberseguridad en el que haya participado en el hotel?

Incidentes anteriores

2.- ¿Alguna vez ha experimentado o presenciado un incidente de ciberseguridad (por ejemplo, violación de datos, ataque de malware) en el desempeño de sus funciones? En caso afirmativo, ¿puede describir lo sucedido?

Impacto de los incidentes

3.- ¿Cómo afectó el incidente de ciberseguridad a sus operaciones diarias y al funcionamiento general del hotel?

Respuesta al incidente

4.- ¿Cómo respondió el hotel al incidente de ciberseguridad? ¿Qué medidas inmediatas se tomaron?

Comunicación durante los incidentes

5.- ¿Cómo se comunicó la información durante y después del incidente? ¿Existía un plan de comunicación claro?

Gestión de activos

7.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para tu departamento y para el hotel en general?

Percepción del riesgo

6.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para su departamento y para el hotel en general?

Medidas preventivas

8.- ¿Qué medidas preventivas se aplican actualmente para protegerse contra las amenazas de ciberseguridad? ¿Hay algún aspecto que considere necesario mejorar?

Cumplimiento y normativa

9.- ¿Está familiarizado con las políticas del hotel y la normativa externa en materia de ciberseguridad? ¿Cómo influyen en sus operaciones diarias?

Sugerencias de mejora

10.- ¿Qué sugerencias tiene para mejorar la postura de ciberseguridad del hotel y las estrategias de respuesta?

4.3 Identificar los activos y riesgos del hotel JW Marriott de Quito aplicando el marco metodológico NIST.

Para lograr el objetivo de identificar los activos y riesgos del Hotel JW Marriott de Quito, empleamos un enfoque sistemático guiado por el marco de gestión de riesgos del NIST (Instituto Nacional de Normas y Tecnología). Se utilizó un formato de Excel el cual es indispensable en caso de que se desee aplicar este trabajo en otra propiedad para tener en cuenta todos los activos este archivo también es el primer anexo y el nombre de este archivo es “Amazonashot Sistemas Anexo 1”, en ese archivo se documentó meticulosamente todos los activos informáticos, tanto físicos como virtuales, que forman parte integral de las operaciones del hotel. En el Anexo 1, se estructura el inventario de activos físicos, incluidos equipos informáticos, servidores, conmutadores y sistemas de punto de venta (POS), entre otros. Cada activo físico se describió exhaustivamente, detallando especificaciones como marca y modelo, número de serie, ubicación dentro del hotel.

Además, en la sección de software del Anexo 1, se encuentran especificados los servidores virtuales y físicos desplegados en la infraestructura informática del hotel. Para cada servidor, registramos información esencial como el nombre del servidor, la dirección IP, la capacidad de almacenamiento y los recursos que ocupan. Además, documentamos meticulosamente las bases de datos importantes alojadas en cada servidor, incluidos sus

nombres, direcciones IP e información general. Este enfoque integral garantizó que todos los activos digitales críticos del entorno informático del hotel estuvieran identificados y documentados con precisión, sentando las bases para una evaluación y gestión de riesgos eficaz.

Al formalizar y ampliar esta información dentro del Anexo 1, pudimos crear un repositorio de activos y riesgos para el hotel JW Marriott de Quito. Esta información servirá como un valioso recurso para desarrollar un sólido plan de respuesta a incidentes de ciberseguridad adaptado a las necesidades y desafíos específicos del hotel, garantizando la salvaguarda de sus operaciones y los datos de los huéspedes contra las amenazas de ciberseguridad.

Es importante destacar que si desea implementar este trabajo en otra propiedad se debe contar con las consideraciones presentadas de la Figura 6 hasta la Figura 14, a continuación, se detalla cada figura con un breve resumen.

Figura 6. Plan de organización de TI: Un resumen rápido del contenido del archivo, ya sea el listado de los equipos, servicios, bases de datos, recurso humano del departamento de sistemas, etc.

Figura 7. Lista de servicios: Listado de los servicios que corren sobre los servidores y servicios informáticos que maneje la propiedad.

Figura 8. Listado de equipos físicos: Un desglose de todos los equipos físicos a cargo del departamento de IT con la información necesaria para poder identificarlos.

Figura 9. Listado de equipos virtuales: Un desglose de todos los equipos virtuales con la información necesaria para poder identificarlos.

Figura 10. Recurso Humano: Descripción del personal de sistemas con el número de contacto nombres, correos y estado con respecto a si está o no activo en los sistemas.

Figura 11. Actividades x servicio: Detallar cada servicio o recurso que se utiliza en la empresa y que actividades de mantenimiento se realiza para evitar fallos.

Figura 12. Actividades x equipos físicos: Detallar que equipos necesitan supervisión y que procedimiento se realiza para verificar el correcto funcionamiento de estos.

Figura 13. Bases de datos: Desglose a detalle de todas las bases de datos que se utilizan y para que aplicaciones se utiliza, especificar el motor y las instancias donde se encuentra cada base.

Figura 14. Matriz de riesgos: Con la información recabada podemos crear una matriz de riesgos tomando en cuenta factores ambientales o errores humanos.

FIGURA 6

PLAN DE ORGANIZACIÓN DE TI

Plan de Organización de TI

ID	Título	Ubicación	Comentarios	Estado
1	**Gestión de activos y servicios**			
1.1	Listado Equipos físicos	Equipos Hardware	Instalaciones (equipo pasivo) Equipo Data Center: servidores, comunicaciones, firewall, router, UPS, Sensores, cámaras, etc) Equipo usuarios (computadoras, teléfonos fijos, celulares, cámaras, etc) - Datos: Fecha de compra, ubicación, etc. Ver pestaña "Equipos físicos" de ejemplo	100%
1.2	Listado Equipos Virtuales	Máquina Virtuales	Lista de los equipos virtuales onpremise y en la nube. Detallado	100%
1.3	Listado Servicios	Listado de servicios	Servicios, propios y de terceros. Incluir mis sistemas y mis servicios instalados, también licencias, dominios, contratos	100%
1.4	Listado de Bases de datos	Bases de Datos	Bases de datos locales o en la nube	100%
1.5	Lista de Recurso humano	Recurso Humano	Personal de tecnología	100%
1.6	Diagrama físico de la red		Url a la imagen o al sistema	
1.7	Diagrama lógico		Descripción de redes, Vlan, ruteo, VPN (gráfico o texto)	
2	**Gestión de mesa de ayuda**		Se puede gestionar con GLPI, revisar política del corporativo, se puede administrar un solo procedimiento como mesa de ayuda que cubra todos los temas	
2.1	Procedimiento Gestión de cambios			
2.2	Procedimiento Base de conocimiento PyR		Incluir en los manuales, documentos técnicos y de usuario, los problemas recurrentes	N/A
2.3	Procedimiento de soporte remoto		Uso de GLPI para tickets, uso de consola remota	100%
3	**Gestión de Políticas**			
3.1	Política de uso del antivirus		Todas las PCs deben contar con un antivirus y llevar control de ello	100%
3.2	Política de creación de usuarios y política de claves			100%
3.3	Política de uso de correo electrónico			
3.4	Política de desarrollo de software		(Desarrollo o adquisición)	N/A
3.5	Politica de equipos nuevos		Estos equpos siempre deben ser provistos por el area de sistemas, las diferentes areas del hotel no podran realizar compras de dispositivos como: Computadoras, Celulares, Tabletas, Puntos de ventas, etc. sin la autorizacion y conocimiento del area de sistemas.	100%

FIGURA 7

LISTA DE SERVICIOS.

DataCenter	EMPRESAS	Nombre	UsoServicio	Tecnología	Aprovisionamiento	Proveedor	Nivel_Impacto	Test Conexión	Descripción	Ambiente
AMAZONASHOT	AMAZONASHOT S.A.	ANTISPAM	Interno	Harmony	Nube	Telefonica	Medio	Https	ANTISPAM	Produccion
AMAZONASHOT	AMAZONASHOT S.A.	FIREWALL	Interno	PALO ALTO	Local	Palo alto	Alto	Https	FIREWALL	Produccion
AMAZONASHOT	AMAZONASHOT S.A.	Antimalware	Interno	SOPHOS	Local	Sophos	Medio	Https	Antimalware	Produccion
AMAZONASHOT	AMAZONASHOT S.A.	VPN	Interno/Externo	PALO ALTO	Local	Palo alto	Medio	Https	VPN	Produccion
AMAZONASHOT	AMAZONASHOT S.A.	raices.com.ec	externo	DNS	dominiosecuador.ec	dominiosecuador.ec	Alto	Whois	dominio restaurant	Produccion
AMAZONASHOT	AMAZONASHOT S.A.	fogo.com.ec	externo	DNS	dominiosecuador.ec	dominiosecuador.ec	Alto	Whois	dominio restaurant	Produccion
AMAZONASHOT	AMAZONASHOT S.A.	marriottquito.com	externo	DNS	godady	godady	Alto	Whois	dominio hotel	Produccion
AMAZONASHOT	AMAZONASHOT S.A.	Office 365	externo	DNS	Azure	Otecel	Alto	Whois	Office 365 Cuentas de correo hote	Produccion
AMAZONASHOT	AMAZONASHOT S.A.	Office 365	externo	DNS	Azure	Otecel	Alto	Whois	Office 365 Cuentas de correo fogo	Produccion

FIGURA 8

LISTADO DE EQUIPOS FÍSICOS.

EMPRESA	Tipo	Marca	Modelo	Descripción	NroParte	Serie	Voltaje	Tipo Presentacion	Alto en U	IP Adminis	S.O.	Modelo CPU	RAM	Cant HD	Consur	DataCen	Usuario asignado	FechaCom	FinGaran	Proveedo	Estado
AMAZONASHOT S.A	Notebook	LENOVO	Thinkpad X1 Yoga Gen2	Executive Offices	20JES0CH3Q	R90Q2CSD	110 y 220V	LAPTOP	1		Windows 10	I7-7650U	16	1 SSD 512Gb		NO	Antonela Maya	1/1/2019	31/12/2021	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	Yoga 3 14IRP8	Executive Offices	83B1001XUS	PF4BP7V3	110 y 220V	LAPTOP	1		Windows 11	I7-1360P	16	1 SSD 1024Gb		NO	Joseph Cina	1/1/2023	31/12/2025	USA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	Thinkpad X1 Yoga Gen2	Food & Beverage	20JES0CH3Q	R90Q2CSJ	110 y 220V	LAPTOP	1		Windows 10	I7-7650U	16	1 SSD 512Gb		NO	Valeria Posso	1/1/2019	31/12/2021	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	Thinkpad X1 Yoga Gen2	Event Management	20JES0CH3Q	R90Q2CSG	110 y 220V	LAPTOP	1		Windows 10	I7-7650U	16	1 SSD 512Gb		NO	Astrid Mievis	1/1/2019	31/12/2021	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	Thinkpad X1 Yoga Gen2	Front Office	20JES0CH3Q	R90Q2CSH	110 y 220V	LAPTOP	1		Windows 10	I7-7650U	16	1 SSD 512Gb		NO	Andrea Macias	1/1/2019	31/12/2021	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	Yoga 3 14IRP8	Engineering	83B1001WUS	PF4D12RD	110 y 220V	LAPTOP	1		Windows 11	I7-1360P	16	1 SSD 1024Gb		NO	Claudia Velazco	1/1/2023	31/12/2025	USA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	Thinkpad X1 Carbon 6th	Executive Offices	20KGS1VR2B	PF1KFADN	110 y 220V	LAPTOP	1		Windows 10	I7-8550U	16	1 SSD 512Gb		NO	Jenny Aguirre	1/1/2019	31/12/2021	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	Thinkpad X1 Carbon 6th	Human Resources	20KGS1VR2B	PF1KFAE1	110 y 220V	LAPTOP	1		Windows 10	I7-8550U	16	1 SSD 512Gb		NO	Xavier Constante	1/1/2019	31/12/2021	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	Thinkpad X1 Carbon 6th	Sales	20KGS1VR2B	PF1KFAEK	110 y 220V	LAPTOP	1		Windows 10	I7-8550U	16	1 SSD 512Gb		NO	Diana Murcia	1/1/2019	31/12/2021	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	Thinkpad X1 Carbon 6th	Accounting	20KGS1VR2B	PF1KFAEY	110 y 220V	LAPTOP	1		Windows 10	I7-8550U	16	1 SSD 512Gb		NO	Yenifer Hernandez	1/1/2019	31/12/2021	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	Thinkpad X1 Carbon 6th	SSU-Systems	20KGS1VR2B	PF1KFAFD	110 y 220V	LAPTOP	1		Windows 10	I7-8550U	16	1 SSD 512Gb		NO	Darvin Cantuña	1/1/2019	31/12/2021	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	T530	Human Resources	2429-70L	PK200PJR	110 y 220V	LAPTOP	1		Windows 10	I5-2520m	8	1 SSD 512Gb		NO	Capacitación	1/1/2019	31/12/2021	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	L13 Yoga	Sales	20R6-S4E100	R913E8SW	110 y 220V	LAPTOP	1		Windows 10	I7-1355U	16	1 SSD 512Gb		NO	Giannela Trujillo	1/1/2019	31/12/2021	BINARIA	Producción
AMAZONASHOT S.A	Notebook	MICROSOFT	Surface Go 2	Housekeeping	1V810000024	12374403051	110 y 220V	TABLET	1		Windows 10	m3-8100Y	8	1 SSD 512Gb		NO	Gennys Velez	2/1/2022	1/1/2025	QUANTIK	Producción
AMAZONASHOT S.A	Notebook	MICROSOFT	Surface Go 2 - LTE	Housekeeping	1V810000372	51274210451	110 y 220V	TABLET	1		Windows 10	m3-8100Y	8	1 SSD 512Gb		NO	Gennys Velez	3/1/2022	2/1/2025	QUANTIK	Producción
AMAZONASHOT S.A	Notebook	MICROSOFT	Surface Go 2 - LTE	Housekeeping	1V810000372	44537604551	110 y 220V	TABLET	1		Windows 10	m3-8100Y	8	1 SSD 512Gb		NO	Gennys Velez	4/1/2022	3/1/2025	QUANTIK	Producción
AMAZONASHOT S.A	Notebook	LENOVO	ThinkPad X1 Yoga Gen 7	Sales	21CES1Q400	PF4A11K0	110 y 220V	LAPTOP	1		Windows 11	I7-1355U	32	1 SSD 512Gb		NO	Irene Landivar	1/1/2023	31/12/2025	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	ThinkPad P16S Gen1	Housekeeping	21BU50GF00	PF4ANHAF	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO	Isabel Delgado	1/5/2023	30/4/2026	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	ThinkPad P16S Gen1	Food & Beverage	21BU50GF00	PF4ANNAZ	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO	Juan Carlos Moncayo	1/5/2023	30/4/2026	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	ThinkPad P16S Gen1	Accounting	21BU50GF00	PF4CRA9Z	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO	Roberto Largo	1/5/2023	30/4/2026	BINARIA	Producción
AMAZONASHOT S.A	Notebook	LENOVO	ThinkPad P16S Gen1	Accounting	21BU50GF00	PF4ANKJJ	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO	Miguel Heredia	9/8/2023	8/8/2026	TelyStore	Producción
AMAZONASHOT S.A	Notebook	LENOVO	ThinkPad P16S Gen1	Human Resources	21BU50GF00	PF4ANN9R	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO	Xavier Constante	9/8/2023	8/8/2026	TelyStore	Producción
AMAZONASHOT S.A	Notebook	LENOVO	ThinkPad P16S Gen1	SSU-Systems	21BU50GF00	PF4ANKES	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO	Darvin Cantuña	9/8/2023	8/8/2026	TelyStore	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D42	110 y 220V	DESKTOP	1		Windows 10	I5-7500	8	1 SSD 250GB		NO	Sebastian Landazuri	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4H	110 y 220V	DESKTOP	1		Windows 10	I5-7501	8	1 SSD 250GB		NO	Diego Maldonado	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4M	110 y 220V	DESKTOP	1		Windows 10	I5-7502	8	1 SSD 250GB		NO	Gustavo Mosquera	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Front Office	2DR82UP	MXL8071D51	110 y 220V	DESKTOP	1		Windows 10	I5-7503	8	1 SSD 250GB		NO	Edison Piofrio	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4N	110 y 220V	DESKTOP	1		Windows 10	I5-7504	8	1 SSD 250GB		NO	Finanzas (Gustavo Mosquera)	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D3V	110 y 220V	DESKTOP	1		Windows 10	I5-7505	8	1 SSD 250GB		NO	Freddy Viteri	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4W	110 y 220V	DESKTOP	1		Windows 10	I5-7506	8	1 SSD 250GB		NO	Jorge Cruz	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Human Resources	2DR82UP	MXL8071D3T	110 y 220V	DESKTOP	1		Windows 10	I5-7507	8	1 SSD 250GB		NO	Karina Morales	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D3W	110 y 220V	DESKTOP	1		Windows 10	I5-7508	8	1 SSD 250GB		NO	Oswaldo Alvarez	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4T	110 y 220V	DESKTOP	1		Windows 10	I5-7509	8	1 SSD 250GB		NO	Talia Tillaguango	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4L	110 y 220V	DESKTOP	1		Windows 10	I5-7510	8	1 SSD 250GB		NO	Yadira Vinueza	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Purchasing	2DR82UP	MXL8071D4Q	110 y 220V	DESKTOP	1		Windows 10	I5-7511	8	1 SSD 250GB		NO	Talia Tillaguango	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	Purchasing	2DR82UP	MXL8071D4P	110 y 220V	DESKTOP	1		Windows 10	I5-7512	8	1 SSD 250GB		NO	Kwag Nojun	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	At Your Service	2DR82UP	MXL8071D47	110 y 220V	DESKTOP	1		Windows 10	I5-7513	8	1 SSD 250GB		NO	AYS3	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	At Your Service	2DR82UP	MXL8071D48	110 y 220V	DESKTOP	1		Windows 10	I5-7514	8	1 SSD 250GB		NO	AYS1	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G3 SFF	At Your Service	2DR82UP	MXL8071D49	110 y 220V	DESKTOP	1		Windows 10	I5-7515	8	1 SSD 250GB		NO	AYS2	20/4/2018	19/4/2021	Akros	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G4 SFF	Banquets	5GL94UP	MXL8491RL7	110 y 220V	DESKTOP	1		Windows 10	I5-7516	8	1 SSD 250GB		NO	Jorge Guanochanga	2/1/2019	20/1/2022	Gensystems	Producción
AMAZONASHOT S.A	Desktop	HP	HP EliteDesk 800 G4 SFF	Banquets	5GL94UP	MXL8491RL8	110 y 220V	DESKTOP	1		Windows 10	I5-7517	8	1 SSD 250GB		NO	Luis Yepez / Jorge Guanochan	2/1/2019	20/1/2022	Gensystems	Producción

FIGURA 9

LISTADO DE EQUIPOS VIRTUALES.

ID	DataCenter	HW	Empres	NombreMaquinaVirtual	Funcionali	Est. Actu	EstadoAlar	Host	Host	vCPU	Host Me	IP4	IP4-2	IP6	Nombre Redes	Guest OS	Provisioned Space	Used Space	Versior	Responsable (Sop	Responsable (Sop
3	AMAZONASHOT	HP	TI	UIODTVMDLS1	Control de puert	TRUE	OFF	10.163.132.15	33SMHz	4	12	10.163.132.11			VM Network	Microsoft Windows Ser	60	72		DARWIN CANTUNA	ESTEBAN MOYOLEMA
4	AMAZONASHOT	HP	TI	UIODTVMERP1	ERP	TRUE	OFF	10.163.132.15	981MHz	8	32	10.163.132.6			VM Network	Microsoft Windows Ser	160	192.08		DARWIN CANTUNA	ESTEBAN MOYOLEMA
5	AMAZONASHOT	HP	TI	UIODTVMIFC1	Interfaz	TRUE	OFF	10.163.132.15	406MHz	4	8	10.163.132.3			VM Network	Microsoft Windows Ser	60	68.08		DARWIN CANTUNA	ESTEBAN MOYOLEMA
6	AMAZONASHOT	HP	TI	UIODTVMDPRS5	PMS	TRUE	OFF	10.163.132.15	15.92GH	8	128	10.163.132.2			VM Network	Microsoft Windows Ser	600	728.08		DARWIN CANTUNA	ESTEBAN MOYOLEMA
7	AMAZONASHOT	HP	TI	UIODTVMPAYROLL1	Roll de pagos	TRUE	OFF	10.163.132.15	263MHz	4	8	10.163.132.34			VM Network	Microsoft Windows Ser	130	127.72		DARWIN CANTUNA	ESTEBAN MOYOLEMA
10	AMAZONASHOT	HP	TI	UIODTVMDC1	AD	TRUE	OFF	10.163.132.16	746MHz	4	8	10.163.132.20			VM Network	Microsoft Windows Ser	100	108		DARWIN CANTUNA	ESTEBAN MOYOLEMA
11	AMAZONASHOT	HP	TI	UIODTVMFP2	File And Print	TRUE	OFF	10.163.132.16	293MHz	4	6	10.163.132.23			VM Network	Microsoft Windows Ser	1.97TB	1.17TB		DARWIN CANTUNA	ESTEBAN MOYOLEMA
12	AMAZONASHOT	HP	TI	UIODTVMBE1	BackUp	TRUE	OFF	10.163.132.18	353MHz	4	12	10.163.132.18			VM Network	Microsoft Windows Ser	50	50.11		DARWIN CANTUNA	ESTEBAN MOYOLEMA
13	AMAZONASHOT	HP	TI	UIODTVMCAPS	POS	TRUE	OFF	10.163.132.18	2.37GH	8	12	10.163.132.18			VM Network	Microsoft Windows Ser	55	67.11		DARWIN CANTUNA	ESTEBAN MOYOLEMA
14	AMAZONASHOT	HP	TI	UIODTVMIFC2	Interfaz	TRUE	OFF	10.163.132.18	353MHz	4	8	10.163.132.3			VM Network	Microsoft Windows Ser	60	68.11		DARWIN CANTUNA	ESTEBAN MOYOLEMA
15	AMAZONASHOT	HP	TI	UIODTVMDPRS52	PMS	TRUE	OFF	10.163.132.18	12.15GH	8	64	10.163.132.2			VM Network	Microsoft Windows Ser	600	664.11		DARWIN CANTUNA	ESTEBAN MOYOLEMA
16	AMAZONASHOT	HP	TI	UIODTVMPOS	POS	TRUE	OFF	10.163.132.18	379MHz	8	12	10.163.132.18			VM Network	Microsoft Windows Ser	180	192.11		DARWIN CANTUNA	ESTEBAN MOYOLEMA
17	AMAZONASHOT	HP	TI	UIODTVMPOS1	POS	TRUE	OFF	10.163.132.18	1.12GHz	8	6	10.163.132.13			VM Network	Microsoft Windows Ser	531.11	525		DARWIN CANTUNA	ESTEBAN MOYOLEMA
18	AMAZONASHOT	HP	TI	UIODTVMRA	Reportes	TRUE	OFF	10.163.132.18	418MHz	4	12	10.163.132.9			VM Network	Microsoft Windows Ser	150	162.11		DARWIN CANTUNA	ESTEBAN MOYOLEMA
19	AMAZONASHOT	HP	TI	UIODTVMVC	VC	TRUE	OFF	10.163.132.18	353MHz	2	12	10.163.132.185			VM Network	Microsoft Windows Ser	100	598.14		DARWIN CANTUNA	ESTEBAN MOYOLEMA
20	AMAZONASHOT	HP	TI	UIODTVMVEEAM1	BackUp	TRUE	OFF	10.163.132.18	957MHz	4	8	10.163.132.184			VM Network	Microsoft Windows Ser	2.5TB	1.29TB		DARWIN CANTUNA	ESTEBAN MOYOLEMA
21	AMAZONASHOT	HP	TI	UIODTVMW10	Cliente	TRUE	OFF	10.163.132.18	3.19GH	8	12	10.163.132.105			VM Network	Windows 10	65	77.11		DARWIN CANTUNA	ESTEBAN MOYOLEMA

FIGURA 10

ACTIVIDADES X SERVICIO.

TipoRecurso	Empresa	Recurso	Actividad	Procedimiento
EQUIPOVIRTUAL	AMAZONASHOT S.A.	MySatcom	Revision de espacio en disco	Ingresar al servidor y comprobar que los dispositivos de almacenamiento tengan espacio suficiente
EQUIPOVIRTUAL	AMAZONASHOT S.A.	DB MySatcom	Verificacion de datos ingresados	Ingreso al servidor obtener un respaldo de la base y verificar que los datos respeten ACID
EQUIPOVIRTUAL	AMAZONASHOT S.A.	VimBackup	Cambio de cintas	Proceso automatico cuando se realiza el cambio de la cinta a tiempo en caso de que se desee re programar la tarea hacerlo desde el servidor
EQUIPOVIRTUAL	AMAZONASHOT S.A.	VMware vCenter Server	Revisar alertas del servidor	Ingresar al administrador de maquinas virtuales y desde el monitor de actividad verificar que no existan alertas
EQUIPOVIRTUAL	AMAZONASHOT S.A.	NEW_7 Dominio QM	Verificar conexiones con el corporativo	Ingresar al servidor y revisar si tiene conexion con la IP publica del corporativo
EQUIPOVIRTUAL	AMAZONASHOT S.A.	O8 VIRT_11	Verificar conexiones con el corporativo	Ingresar al servidor y revisar si tiene conexion con la IP publica del corporativo
EQUIPOVIRTUAL	AMAZONASHOT S.A.	SiaWeb_3	Verificar conexiones con el corporativo	Ingresar al servidor y revisar si tiene conexion con la IP publica del corporativo
SERVICIO	AMAZONASHOT S.A.	Sophos Antivirus	- Instalar clientes en los equipos de usuario - Monitoriear/solucionar casos reportados por Sophos - Actualizar permisos y accesos a los dispositivos	

FIGURA 11

RECURSO HUMANO.

email	Nombre	Fortalezas	Telf	Estado
darwin.cantuna@marriottquit	Darwin Cantuña		999586026	Activo
systems.assistant@marriottqu	Esteban Moyolema		999585912	Activo

FIGURA 12

ACTIVIDADES X EQUIPOS FÍSICOS.

Tipo Activo	Actividad	Procedimiento	URL Procedimiento	Tiempo Horas	Tipo	Frecuencia dias	Responsable
Pantalla y NUC	Verificacion de funcionamiento	Conexion remota por AnyDesk para verificar si estan encendidas		10 minutos		Período	Esteban Moyolema
Pantallas y PC Stick	Actualizacion de contenido	Conexion remota por LogicalSignage		2 horas		Mensual	Esteban Moyolema
UPS	Revision de alarmas y luces led de alerta	Verificar si algun UPS se encuentra en mal estado		10 Minutos		Mensual	Esteban Moyolema
Switches	- Revisión de ruidos, alarmas audibles - Revisar leds de alerta - Encender ventiladores de backup	Recorrido piso por piso para descubrir posibles fallos en los equipos de red		10 minutos		Mensual	Esteban Moyolema
Cintas de Backup	Cambio de cintas de manera periodica	Obtener el nuevo type correspondiente a ese dia y realizar el format en caso de ser necesario o el cambio		5 minutos		Diario	Esteban Moyolema

FIGURA 13

BASES DE DATOS.

ID	NombreBD	Maquina Virtual	Descripción	SGBD	Instancia	EstadoBD	Tamaño Giga	Ubicación Backup	Ubicación	Frecuencia (	Responsable	IDAlerta	Ambiente
1	fiscalDB	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	0.58			DIARIA	DARWIN CANTUNA		PRODUCCION
2	sat_catalogo	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	0.32			DIARIA	DARWIN CANTUNA		PRODUCCION
3	sat_comprobante	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	7.94			DIARIA	DARWIN CANTUNA		PRODUCCION
4	sat_comprobante_his	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	1			DIARIA	DARWIN CANTUNA		PRODUCCION
5	sat_conciliacion	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	0.08			DIARIA	DARWIN CANTUNA		PRODUCCION
6	sat_ecommerce	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	0.08			DIARIA	DARWIN CANTUNA		PRODUCCION
7	sat_logging	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	1.25			DIARIA	DARWIN CANTUNA		PRODUCCION
8	sat_seguridad	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	0.72			DIARIA	DARWIN CANTUNA		PRODUCCION
9	ACTIVOFIJO	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	0.8			DIARIA	DARWIN CANTUNA		PRODUCCION
10	ACTIVOFIJO_PRUEBA	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	0.8			-	DARWIN CANTUNA		PRUEBAS
11	CONTAB_NUEVA	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	1.79			DIARIA	DARWIN CANTUNA		PRODUCCION
12	CONTAB_PRUEBA	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	1.79			-	DARWIN CANTUNA		PRUEBAS
13	CONTABILIDAD	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	1.97			DIARIA	DARWIN CANTUNA		PRODUCCION
14	dbGYM	UIODTVMERP1	Sistema GYM	SqlServer	UIODTVMERP1	ACTIVA	0.72			DIARIA	DARWIN CANTUNA		PRODUCCION
15	INVEN_NUEVO	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	3.43			DIARIA	DARWIN CANTUNA		PRODUCCION
16	INVEN_PRUEBA	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	3.43			-	DARWIN CANTUNA		PRUEBAS
17	INVENTARIO	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	3.6			DIARIA	DARWIN CANTUNA		PRODUCCION
18	NOMINA	UIODTVMERP1	RRHH	SqlServer	UIODTVMERP1	ACTIVA	0.24			DIARIA	DARWIN CANTUNA		PRODUCCION
19	NOMINA_PRUEBA	UIODTVMERP1	RRHH	SqlServer	UIODTVMERP1	ACTIVA	0.24			-	DARWIN CANTUNA		PRUEBAS
20	SiesaAccess_HMRR	UIODTVMERP1	RRHH	SqlServer	UIODTVMERP1	ACTIVA	0.17			DIARIA	DARWIN CANTUNA		PRODUCCION

FIGURA 14

MATRIZ DE RIESGOS.

HW	Inundación	1	5	6	Medio	Elevar la altura de los servidores y racks
HW	Sobre tensión	2	2	4	Bajo	
HW	Corte eléctrico	2	2	4	Bajo	
HW	Sabotaje físico	3	5	8	Importante	Monitoreo de cámaras y auditoría de accesos
HW	Incendio	1	5	6	Medio	Extintores
HW	Falla de generador	1	3	4	Bajo	
HW	Falla de UPS	1	5	6	Medio	Contar con doble sistema
HW	Corte de comunicaciones	1	5	6	Medio	Mantener una alternativa en caso de que un switch falle
HW	Fallo o daño de un disco	2	3	5	Medio	
HW	Sin acceso al cuarto	2	4	6	Medio	Se supone que si se requiere entrar es necesario
HW	Terremoto	1	5	6	Medio	
HW	Fallo General	1	5	6	Medio	Documentar y crear un plan para el fallo encontrado
Servicios	Error en actualización	2	2	4	Bajo	
Servicios	Falla del Sistema Operativo	2	2	4	Bajo	
Servicios	Error en autenticación	3	1	4	Bajo	
Servicios	Error con servicios externos	4	2	6	Medio	Tener una snapshot del servidor antes de realizar cambios
Servicios	Acceso no autorizado	2	5	7	Importante	Auditar cada tres meses los usuarios con acceso a los sistemas
Servicios	Información no confiable	1	4	5	Medio	
Servicios	Corrupción de la Data	1	5	6	Medio	Tomar uno de los respaldos que generan diariamente los servidores de base de datos
Servicios	Daño en el código ejecutable	3	5	8	Importante	Tener un clon del servidor cuando realizen cambios importantes en las aplicaciones
Servicios	Daño por manipulacion del SO	1	2	3	Bajo	
Servicios	Error en DNS	3	3	6	Medio	En caso de falla del servidor o un apagado del mismo tratar de mover la maquina virtual a otro host

4.4 Desarrollo de recomendaciones basado en el riesgo e impacto a las operaciones.

Las recomendaciones se desarrollan con base en a la Figura 14 donde podemos ver la matriz de riesgos de la propiedad, esta información se encuentra en el Anexo 1 y solo se realizan recomendaciones para los riesgos que superan el nivel 6, a continuación, en la Tabla 1 se presentan las recomendaciones basadas en el riesgo para JW Marriott Quito.

TABLA 1

RECOMENDACIONES BASADAS EN RIESGOS.

Riesgo	Recomendación
Inundación	• Hay que asegurar que el cuarto del servidor esté ubicado en una zona elevada. • Instalar sistemas de drenaje adecuados. • Usar sensores de agua para alertas tempranas. • Tener planes de contingencia y equipos de bombeo disponibles.
Sabotaje físico	• Implementar controles de acceso físicos estrictos. • Instalar cámaras de seguridad. • Realizar verificaciones de antecedentes para el personal. • Capacitar al personal en la identificación de comportamientos sospechosos.
Incendio	• Instalar sistemas de detección y extinción de incendios. • Hay que asegurar que los materiales inflamables estén almacenados adecuadamente. • Realizar simulacros de emergencia regularmente. • Verificar que los extintores estén accesibles y en buen estado.

Falla de UPS	• Realizar mantenimiento y pruebas periódicas de los UPS. • Tener UPS redundantes. • Hay que asegurar que los UPS sean de capacidad adecuada para la carga conectada.
Corte de comunicación entre las computadoras	• Implementar redundancia en la red de comunicación. • Usar herramientas de monitoreo de red. • Tener un plan de contingencia para restaurar la comunicación rápidamente. • Mantener equipos de respaldo en caso de la falla de alguno de estos
Sin acceso al centro de datos	• Implementar procedimientos de acceso de emergencia. • Mantener múltiples métodos de autenticación de acceso. • Tener copias de las llaves o códigos de acceso en una ubicación segura pero accesible.
Terremoto	• Hay que asegurar que el cuarto del servidor esté diseñado para resistir terremotos. • Anclar los racks de servidores al suelo. • Tener planes de recuperación ante desastres y copias de seguridad fuera del sitio.
Fallo General	• Implementar soluciones de alta disponibilidad. • Tener un plan de recuperación ante desastres detallado. • Realizar pruebas de recuperación ante fallos.
Error con servicios externos	• Tener soluciones alternativas o redundantes.

	• Establecer comunicación efectiva con los proveedores de servicios.
Acceso no autorizado	• Implementar controles de acceso estrictos. • Utilizar autenticación multifactor (MFA). • Monitorear y registrar los accesos a los sistemas.
Corrupción de los datos en servidores de BD	• Implementar redundancia de datos y sistemas de replicación. • Realizar verificaciones de integridad de datos regularmente. • Tener procedimientos claros para la restauración de datos.
Daño en el código ejecutable	• Mantener copias de seguridad del código fuente. • Implementar sistemas de control de versiones. • Realizar pruebas de calidad y seguridad del código.
Error en DNS	• Implementar redundancia en los servidores DNS. • Monitorear la salud del DNS. • Tener procedimientos de restauración rápida del servicio DNS.
No tener el conocimiento adecuado de las herramientas	• Capacitar al personal en el uso adecuado de herramientas y sistemas. • Crear y mantener documentación accesible y clara. • Realizar revisiones y actualizaciones de las competencias del personal.
Borrado accidental de las máquinas virtuales	• Implementar políticas de control de acceso y confirmaciones antes de borrar. • Realizar copias de seguridad regulares de las máquinas virtuales. • Tener procedimientos claros para la restauración de máquinas virtuales.

Acceso no autorizado a las máquinas virtuales	• Utilizar autenticación multifactor (MFA) para acceso a máquinas virtuales. • Monitorear y registrar accesos. • Implementar controles de seguridad en las máquinas virtuales.
Indisponibilidad de las bases de datos	• Implementar soluciones de alta disponibilidad para bases de datos. • Realizar monitoreos constantes del rendimiento y salud de la base de datos. • Tener planes de contingencia y procedimientos de restauración.
Backup nulo o incorrecto de las bases de datos	• Implementar políticas estrictas de Backup. • Realizar verificaciones regulares de las copias de seguridad. • Hay que asegurar que las copias de seguridad estén almacenadas en ubicaciones seguras y fuera del sitio.
Restaurar y no hay Backup de las bases de datos	• Hay que asegurar que siempre se realicen y se verifiquen las copias de seguridad. • Tener planes de contingencia para casos de pérdida de datos. • Capacitar al personal en la importancia y los procedimientos de Backup y restauración.

Nota: Descripción detallada de las recomendaciones por amenaza.

4.5 Entrevista con el personal crítico.

4.5.1 Análisis de resultados de la encuesta

Resumen General

El análisis de las respuestas a la encuesta revela áreas clave de mejora y potencial en términos de ciberseguridad en el hotel estas entrevistas están adjuntas en el Anexo 3 al final del documento, abarcando varios departamentos, incluyendo Alimentos y Bebidas, Finanzas y Recepción. Aunque todos los encuestados han recibido una iniciación a la ciberseguridad al incorporarse a sus respectivos puestos, está claro que existen lagunas en la formación continua, la comunicación durante los incidentes y la percepción de los riesgos a los que se enfrentan.

1. Programas de Formación y Concienciación en Ciberseguridad

La mayoría de los empleados han participado en programas de formación básica centrados en temas como el phishing, la protección de contraseñas y el manejo seguro de la información. Los departamentos de Finanzas y Recepción han recibido formación específica relacionada con los riesgos inherentes a sus funciones, como la protección de datos financieros y la seguridad de la información de los huéspedes.

Áreas de Mejora:

Frecuencia y Actualización de la Formación: Los empleados en general coinciden en que la formación es útil, pero sugieren que debería ser más frecuente y actualizada para reflejar las nuevas amenazas. Aunque se han realizado sesiones formativas, la rápida evolución de las amenazas cibernéticas hace necesario que la formación sea continua y se adapten los contenidos a los escenarios más recientes.

Formación Basada en Escenarios Reales: Se sugiere incorporar más simulaciones y estudios de casos en las formaciones para que los empleados estén mejor preparados para identificar y responder a incidentes reales.

Recomendación: Implementar un programa de formación continua, actualizado al menos trimestralmente, que incluya simulaciones de ataques cibernéticos y escenarios reales. Además,

debería considerarse un seguimiento post formación para evaluar la efectividad de estas capacitaciones.

2. Experiencia con Incidentes de Ciberseguridad

Algunos encuestados han presenciado incidentes menores de ciberseguridad, como alertas de malware o intentos de phishing. En todos los casos, el departamento de TI respondió rápidamente, minimizando el impacto en las operaciones diarias del hotel. Sin embargo, la experiencia directa con incidentes graves parece ser limitada.

Áreas de Mejora:

Concienciación sobre Incidentes Menores: Los empleados mencionan que, aunque han presenciado intentos de ataque, sienten que la concienciación sobre cómo identificar estos incidentes podría ser mejorada. Esto incluye comprender los signos de un ataque inminente y saber cómo actuar rápidamente.

Comunicación Durante Incidentes: Algunos encuestados expresaron que la comunicación durante los incidentes fue adecuada, pero podría mejorarse con un plan de comunicación más estructurado y claro, que defina los roles y responsabilidades de cada miembro del equipo durante un incidente.

Recomendación: Fortalecer la comunicación interna durante los incidentes mediante la creación de un plan de respuesta a incidentes detallado y ampliamente distribuido. Este plan debe incluir líneas claras de comunicación, asignación de responsabilidades y procedimientos estándar para diferentes tipos de incidentes.

3. Percepción de los Riesgos de Ciberseguridad

Los empleados reconocen los riesgos significativos que enfrentan sus departamentos, como los ataques de phishing, el acceso no autorizado a sistemas, y la posible filtración de datos sensibles, especialmente en los departamentos de Finanzas y Recepción.

Áreas de Mejora:

Identificación y Priorización de Riesgos: Existe una conciencia general sobre los riesgos, pero parece que falta una comprensión más profunda de cómo estos riesgos pueden afectar directamente sus funciones específicas. Además, algunos empleados sugieren que la encriptación de datos y las auditorías de seguridad regulares deberían ser áreas de enfoque.

Adaptación de Medidas Preventivas: Si bien se aplican medidas como la autenticación multifactorial y el uso de cortafuegos, se ha señalado que las auditorías y las actualizaciones de seguridad no se realizan con la frecuencia que sería deseable.

Recomendación: Implementar un programa de evaluación de riesgos regular que incluya la participación de todos los departamentos. Este programa debería identificar, priorizar y mitigar los riesgos específicos que enfrenta cada departamento. Asimismo, aumentar la frecuencia de las auditorías de seguridad y asegurarse de que las medidas preventivas estén actualizadas y sean efectivas.

4. Sugerencias para Mejorar la Postura de Ciberseguridad

Los encuestados sugieren que el hotel debería seguir mejorando su postura de ciberseguridad mediante la actualización continua de los protocolos y la formación regular del personal. Existe una percepción general de que, aunque se están haciendo esfuerzos significativos, siempre hay margen para la mejora.

4.6 Identificar componentes clave en un plan de respuesta a incidentes.

Debemos tomar en cuenta los siguientes puntos para realizar un plan de respuesta a incidentes:

Inventario de sistemas primordiales

Según (Gasbarrino, 2023) mantener un registro detallado de todos los sistemas críticos de la organización permite una respuesta más rápida y efectiva ante cualquier interrupción. El inventario incluye todos los sistemas necesarios para las operaciones diarias, describiendo su función, ubicación y cualquier dependencia que puedan tener con otros sistemas.

Inventario de equipos primordiales

Es crucial para gestionar eficazmente la infraestructura física de TI. Este inventario debe incluir detalles sobre servidores, switches y cualquier otro equipo crítico. Es importante mantener registros de la ubicación física, especificaciones técnicas, fechas de mantenimiento y cualquier historial de reparaciones. (Gasbarrino, 2023)

Segmentación de sistemas por su importancia y tiempo de inactividad tolerable

Según (Trout, 2024) no todos los sistemas son igualmente críticos, algunos van a tolerar más tiempo de inactividad. Clasificar los sistemas en categorías basadas en su criticidad y el impacto del tiempo de inactividad permite una gestión más eficiente durante una crisis.

Configuración del servidor de respaldos

Para (Thome, 2024) es fundamental para asegurar que los datos puedan ser restaurados rápidamente en caso de una pérdida. Para esto debemos tener servidores de respaldo dedicados, configurar las políticas de respaldo y asegurarse de que los respaldos se realicen de manera regular

Política de respaldos

Las políticas especifican qué datos se van respaldarán, con qué frecuencia, y dónde se almacenarán los respaldos. También se incluyen procedimientos para verificar la integridad de los respaldos y para realizar pruebas de restauración periódica. (Edwards, 2021)

Guía de recuperación

La guía debe incluye los pasos específicos de cada tipo de incidente, así como los procedimientos necesarios para recuperar los sistemas, pero no se incluyen contactos de emergencia de los proveedores. (Kirvan, 2024)

Detalle de cada sistema con su configuración y proceso de recuperación

Documentando la configuración específica de cada sistema, junto con los pasos necesarios para su recuperación, permitiendo que las personas a cargo den respuesta de manera más rápida y precisa. (Edwards, 2021)

Contacto de soporte para los diferentes servicios que tiene la propiedad

Poder dar respuesta para obtener ayuda rápidamente al realizar un seguimiento de los contactos de soporte para todos los servicios críticos, incluidos los detalles de los contactos de emergencia y los niveles de soporte disponibles. (Edwards, 2021)

Diagramas de red

El diagrama mostrará la topología de la red, incluido la ubicación de todos los dispositivos, las conexiones entre ellos y la redundancia. Con los diagramas de red podemos identificar problemas y solucionar incidentes a nivel de red.

4.7 Desarrollo del plan de respuesta ante incidentes de ciberseguridad.

El documento Anexo 2, describe un plan integral de recuperación ante desastres para el JW Marriott Quito, cuyo objetivo principal es garantizar la protección y restauración efectiva de los aspectos fundamentales de la red local en situaciones de emergencia o crisis. Este plan es

crucial para asegurar que la información de la propiedad esté respaldada y protegida de manera consistente, y que existan procedimientos claros para restaurar esta información en caso de que ocurra un fallo grave.

La realización de copias de seguridad diarias es un componente esencial de este plan, y se especifica que deben llevarse a cabo sin excepción para todos los servidores y configuraciones de la propiedad. Esto asegura que, en caso de un incidente, los sistemas, aplicaciones y datos críticos puedan ser restaurados rápidamente, minimizando cualquier interrupción en las operaciones del hotel. Además, el documento detalla cómo los equipos deben estar preparados para manejar diversas contingencias, como desastres naturales, brotes de virus o fallos en la conectividad de red.

Además, el plan de recuperación subraya la importancia de la planificación de contingencias para minimizar el tiempo de inactividad y asegurar que el hotel pueda seguir operando con la menor interrupción posible. Este plan se integra en el Plan de Continuidad del Negocio del hotel y es accesible para todo el personal clave, incluyendo el equipo de tecnología de la información, los jefes de departamento y otros equipos relevantes. También se mencionan políticas y procedimientos estándares de Marriott Internacional, como las políticas de protección de la información y ciberseguridad, que proporcionan un marco adicional para la gestión de incidentes tecnológicos.

Finalmente, se enfatiza la necesidad de revisar y actualizar anualmente el plan de recuperación de desastres, de acuerdo con las políticas de Marriott Internacional (MIP-30). Esta revisión anual es fundamental para asegurarse de que el plan siga siendo relevante y efectivo, especialmente ante la incorporación o eliminación de nuevos sistemas. El documento también destaca la importancia de realizar pruebas de recuperación, como la construcción de servidores

virtuales de repuesto, para validar el proceso de restauración de copias de seguridad y garantizar que el hotel esté preparado para enfrentar cualquier tipo de desastre.

Tenemos que definir cuál es la importancia de cada servicio y el tiempo de recuperación de estos, para ello nos basaremos en la siguiente tabla que se encuentra en el Anexo 2.

TABLA 2

SEGMENTACIÓN DE CRITICIDAD

Grado de Criticidad	Tiempo de inactividad permitido
Misión Critica (Mission Critical)	1 hora 8 horas 24 horas
Operaciones críticas (Business Critical)	48 horas 72 horas
Esenciales para el negocio (Buisness Essential)	1 semana (7 días) 2 semanas (14 días)
Aplazables (Deferrable)	Más de 2 semanas (15 días o más) si es necesario

Nota: Detalle de grado de criticidad y tiempos de recuperación permitidos.

También por el giro del negocio podemos realizar los respaldos de la siguiente manera en los siguientes días.

TABLA 3

DÍAS DE RESPALDOS

	lunes	martes	miércoles	jueves	viernes	sábado	domingo
Full Backup	SI	NO	SI	NO	SI	NO	SI
Incremental Backup	NO	SI	NO	SI	NO	SI	NO

Nota: Por el giro del negocio se recomienda realizar respaldos completos e incrementales en los días seleccionados.

4.8 Evaluación del plan de incidentes de ciberseguridad

Para iniciar esta parte debemos tener en cuenta los siguientes parámetros los cuales serán evaluados en esta sección, Mantener la inactividad del servicio en los límites definidos en el Disaster recovery plan Anexo 2, establecer un periodo de recuperación mínimo, recuperar la situación inicial antes de cualquier incidente de seguridad, analizar los resultados y los motivos de los incidentes, finalizando con evitar que las actividades de la empresa se interrumpan.

En esta ocasión vamos a realizar únicamente la restauración del sistema suponiendo que un malware del tipo Ransomware infectó los servidores de la empresa, este malware no fue detectado por ningún sistema de antivirus, puesto que estaba camuflado en uno de los ejecutables de actualización del sistema PMS de la empresa, al momento de terminar de realizar la actualización empezó a correr una cuenta regresiva de donde todos los archivos del servidor principal PMS se encriptaron y la aplicación dejo de funcionar en todas las máquinas que requerían de este servicio, el problema fue reportado a las 6:30 AM cuando el personal de Front Desk empezó el turno de la mañana.

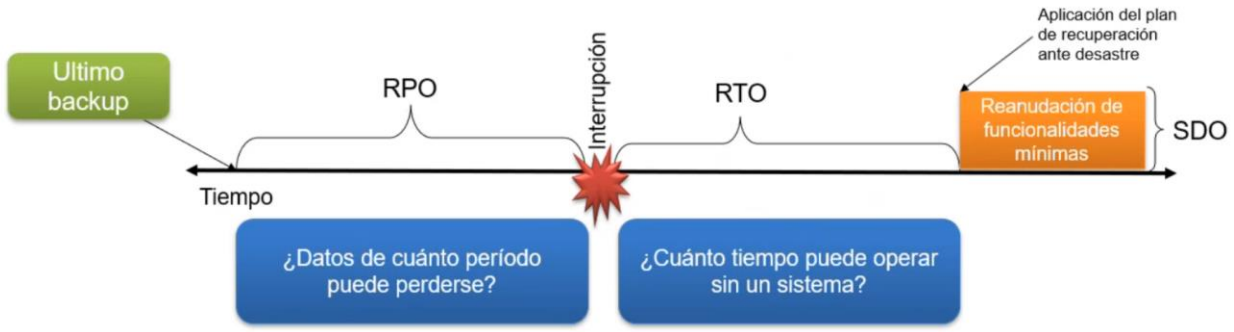
Teniendo en cuenta los siguientes términos:

- RPO (Recovery Point Objective) = Punto de recuperación
- RTO (Recovery Time Objective) = Tiempo de recuperación
- SDO (Service Delivery Objective) = Objetivo de prestación de servicios
- WRT (Working Recovery Time) = Tiempo de recuperación en operación básica

Teniendo en cuenta estos cuatro puntos podemos encasillarnos dentro de los tres primeros parámetros descritos al principio de esta fase, nos podemos ayudar del siguiente diagrama para entender de mejor manera como se realizará la actividad de restauración en base a los puntos mencionados.

FIGURA 15

GRÁFICO RESTAURACIÓN DEL SISTEMA

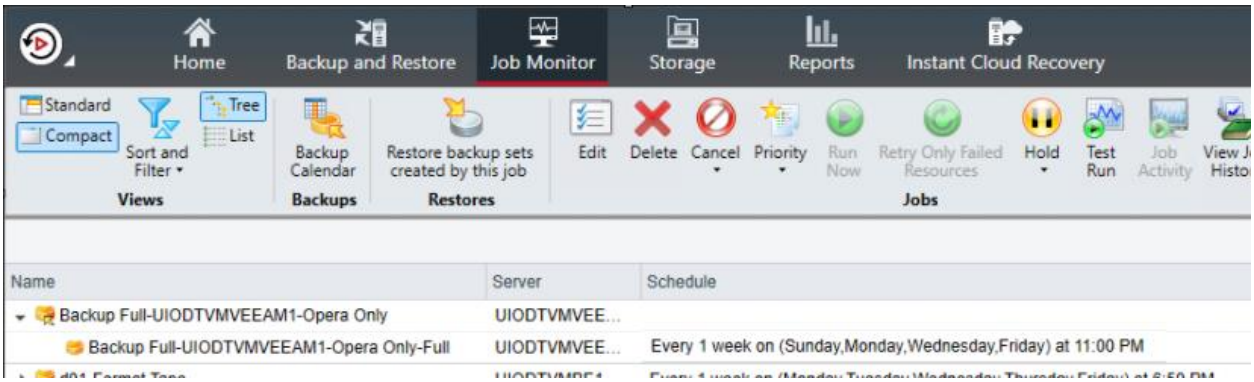


Nota: Se seguirá este gráfico como guía para realizar este ejercicio., Dr. Yoo Sang Guun MSc.

Para el caso del RPO describe cuanto tiempo ha transcurrido desde el último respaldo hasta el momento de la interrupción en este caso vamos a suponer que el incidente se presentó el día de hoy a las 12:00 horas ya que por el bajo movimiento de la madrugada se realizó la actualización a esa hora tratando de no afectar los sistemas críticos por el tiempo de Down time y recordando que como recomendación del área afectada por la actualización siempre se actualizara este sistema los días lunes en la madrugada por la baja ocupación, tenemos que según nuestro Disaster recovery plan Anexo 2, el último respaldo del servidor UIODTVMOPRSS1 está programado para las 11:00 PM y este se realiza cuatro veces por semana incluido el día domingo.

FIGURA 16

SERVIDOR PARA RECUPERAR



Nota: Revisamos el servidor que vamos a restauraren este caso vamos a utilizar la copia completa Backup Full-UIODTVMCWWAM1-Opera Only-Full, Esteban Moyolema

Este respaldo incluye toda la información del servidor no solo la base de datos como es el caso del respaldo d50-UIODTOPRDB1 y también solo incluye el servidor Opera, tampoco utilizaremos el respaldo Full-UIODTVMVEEAM1 ya que este respalda todos los servidores dentro del host principal.

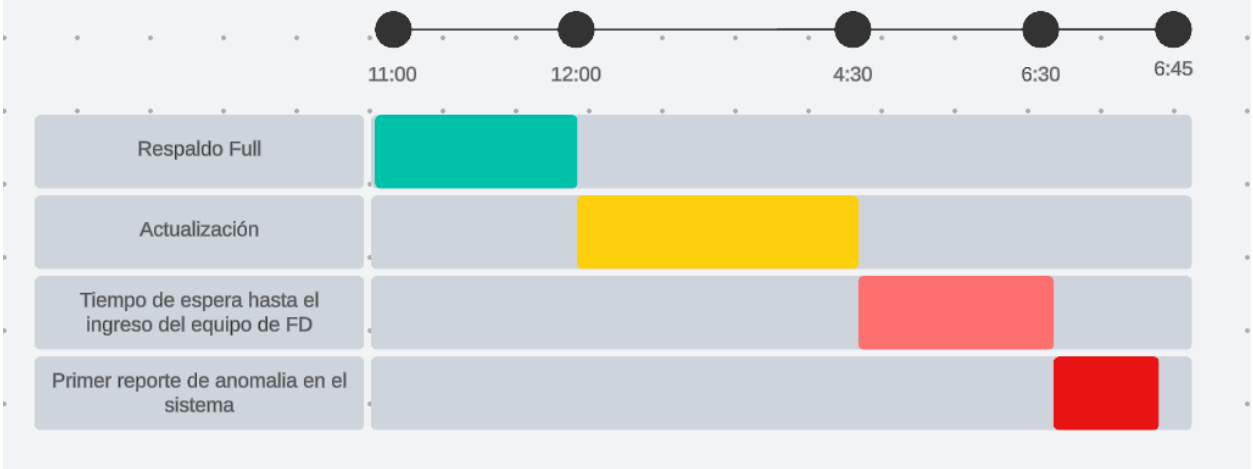
4.8.1 Primera fase de restauración: RPO

Ahora que ya tenemos el panorama claro podemos empezar definiendo que el tiempo transcurrido desde el último respaldo hasta el momento del reporte que hizo Front Desk fue de siete horas y treinta minutos tiempo en el cual no se tiene certeza de si se comprometió la integridad de los datos, transcurrió una hora desde el respaldo hasta la actualización, pero siempre antes de la actualización se realiza un respaldo y un snapshot del servidor, para este ejercicio no tomaremos en cuenta que se realizaron estas actividades y supondremos que la persona a cargo del respaldo no lo realizo por descuido humano, la actualización tomo desde las 12:00 horas hasta las 4:30 de la mañana y a partir de esa hora se terminó la actualización, aparentemente ya se encontraba todo el sistema funcionando con normalidad.

Nos vamos a guiar en la siguiente imagen para entender el transcurso de tiempo mencionado hasta ahora.

FIGURA 17

LÍNEA DE TIEMPO



Nota: Describe el panorama desde el inicio del incidente hasta el momento del reporte, Esteban Moyolema.

A las 6:45 se reporta el primer error desde el Front Desk al equipo de sistemas y nos comparten la siguiente imagen vía telefónica.

FIGURA 18

ERROR EN EL SISTEMA

Nota: Imagen demostrativa de un error en el sistema Opera PMS, Esteban Moyolema.

El personal de sistemas de turno al ver el error trata de acceder desde su computadora al servicio de Opera PMS que corre en línea y al tratar de acceder se topa con el siguiente mensaje.

FIGURA 19

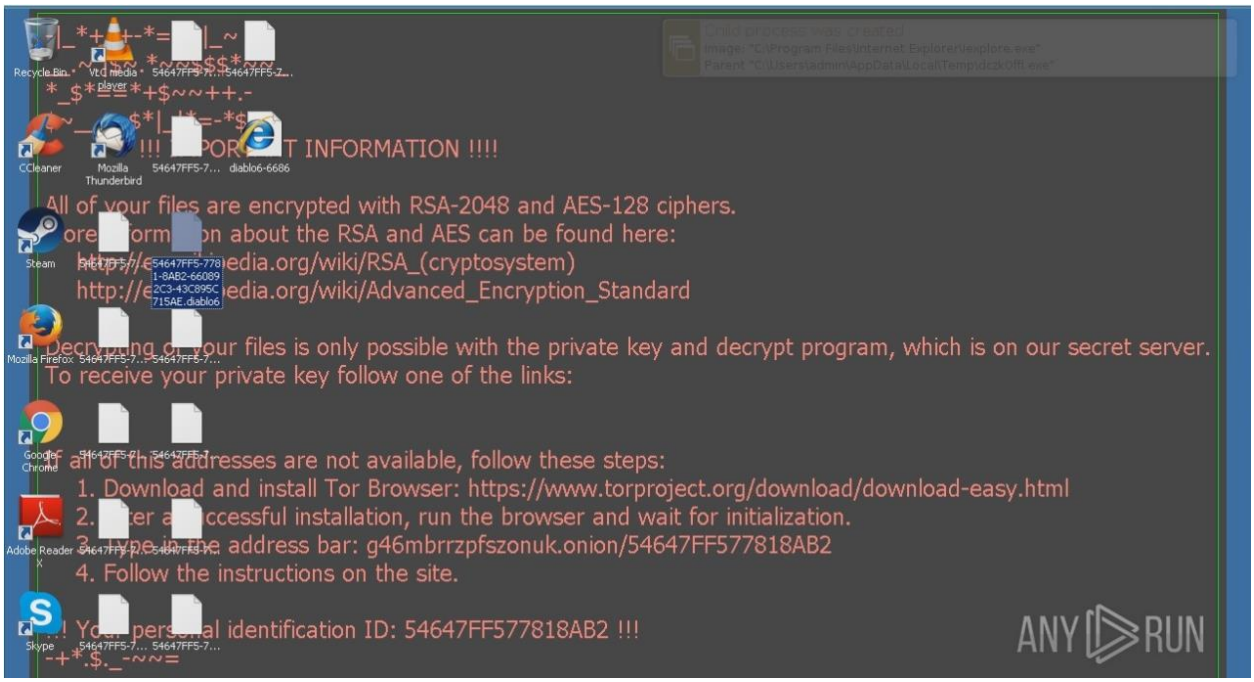
SERVICIO INACTIVO DEL PMS

N*ota: Imagen demostrativa del servicio del PMS cloud opera fuera de línea, Esteban Moyolema.*

Al ver este mensaje se procede con el ingreso al servidor y notamos que los archivos de este se encuentran con otra extensión.

FIGURA 20

ARCHIVOS ENCRIPTADOS



Nota: Imagen demostrativa archivos encriptados en el servidor afectado, Ontinet Nueva campaña del ransomware

En este momento confirmamos que todas las operaciones del servidor Opera PMS fueron interrumpidas y que hemos perdido la información desde el último respaldo hasta este momento.

4.8.2 Segunda fase de restauración: interrupción

Una vez confirmamos que el sistema fue comprometido procedemos según indica la *Tabla 1. Segmentación de criticidad*, con la recuperación del sistema se tiene definido que sistemas de misión crítica como en este caso el servidor PMS del hotel tiene una tolerancia de 1, 8 o 24 horas para ser restaurado.

Revisando el tiempo de recuperación de las operaciones para el servidor Opera PMS tenemos un tiempo de tolerancia de 12 horas en donde el sistema debe ser restaurado y probado, no se debe exceder de esta maca de tiempo, puesto que esto afectara significativamente las operaciones del hotel por la llegada de grupos que se realiza en la mañana y en la noche.

TABLA 4

TIEMPO DE RESTAURACIÓN POR SISTEMAS

Orden	Tipo de sistema	Propósito	Prioridad	Tiempo de recuperación
1	ESX Host – UIODTVMH1	Servidor principal donde se almacenan todos los servidores virtuales.	High	8 horas
2	Backup/Media Server	Host de respaldos	High	8 horas
3	Opera PMS	Property Managment System	High	12 horas
4	Micros Symphony	Servidor de punto de venta	High	24 horas
5	Saflok	Sistema de bloqueo de puertas	High	24 horas

6	PMS Interfaces	OXI, POS, WWW, PBX, Saflok Interfaces, TV Samsung	Medium	24 horas
7	UIODTVMERP1	Sistema de inventarios, contabilidad, recursos humanos y timbre.	Medium	24 horas

Nota: En esta tabla que se encuentra en el Anexo 2 podemos ver cuál es el tiempo tolerable de recuperación por cada sistema considerado crítico.

4.8.3 Tercera fase de restauración: RTO

Ahora debemos determinar cuánto tiempo podemos esperar hasta que el sistema cuente con las funcionalidades mínimas para la operación de la propiedad, para este sistema está definido que no se debe exceder de 12 horas para la recuperación total del sistema y con las operaciones normales. El tiempo fue estimado por Marriott Internacional en base a la recuperación de otras propiedades en casos de tener que reconstruir el servidor nuevamente incluyendo partes y piezas, pero para este ejemplo el servidor no recibió ninguna afectación física. Por lo que esto se puede reducir a la mitad tiempo y dejaremos un estimado de 6 horas como tiempo límite para recuperar las operaciones de la propiedad.

Desde este punto tomaremos el Proceso de recuperación para el sistema Opera PMS del Disaster recovery plan Anexo 2, el cual tiene ocho puntos a tomar en cuenta para restaurar el servidor y nos basaremos en eso para realizar la práctica.

1. Por error en el servidor ponerse en contacto con el soporte de Oracle para el levantamiento nuevamente del PMS.
2. Póngase en contacto con el proveedor de hardware para agilizar la adquisición de nuevo hardware (incluya el servidor de medios de copia de seguridad si ya no está disponible)

3. Configure el servidor según las especificaciones de hardware indicadas anteriormente.
4. Crear una imagen del servidor mediante el proceso de creación de servidores MDT.
5. Solicite al proveedor de aplicaciones que restaure la copia de seguridad o restaure el servidor desde un Backup.
6. Valide el proceso de restauración
7. Póngase en contacto con MSSC Nivel 2 para obtener los códigos de recuperación de PKI para restaurar todos los certificados PKI según la guía Opera PKI.

Ahora con los pasos para el proceso de recuperación vamos a ir uno por uno viendo si aplica o no en nuestra situación.

Tenemos como primer punto el ponernos en contacto con el soporte de Oracle para el levantamiento del PMS, como el último cambio que se efectuó en el servidor fue una actualización misma que las realiza el equipo de soporte de Oracle nos pondremos en contacto con ellos, el contacto se encuentra en la misma sección donde se obtiene el proceso de recuperación.

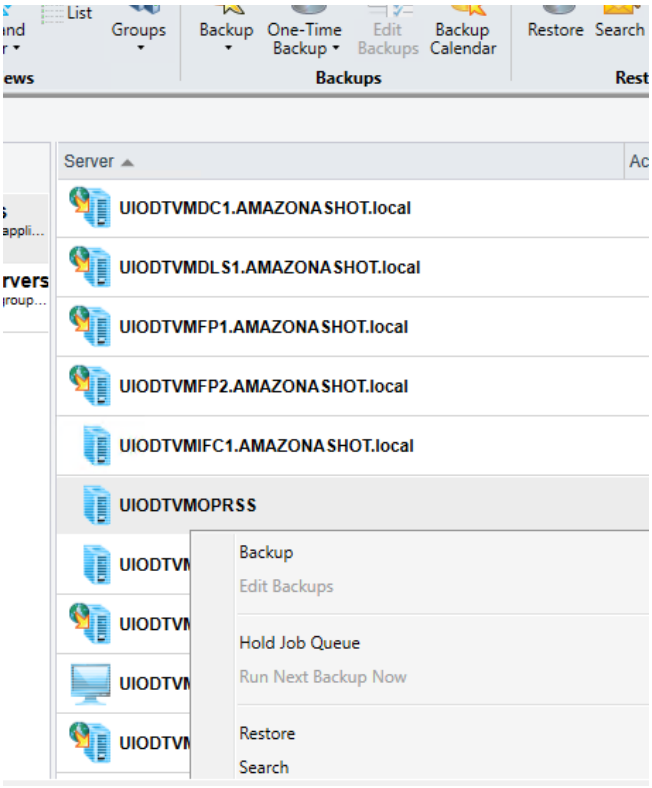
El segundo punto no aplica en nuestro caso, puesto que el servidor físicamente no tiene ningún problema de igual manera en el punto número tres.

Por el estado del servidor no es posible crear una imagen con la herramienta MDT.

Después de contactar con el servicio de Opera vamos a proceder con la restauración del servidor desde la última copia conocida, este proceso se lo realiza desde el servidor UIODTVMBE1, una vez en el servidor nos dirigimos a la pestaña de Backup and Restore, aquí se desplegarán todos los servidores, daremos clic sobre el servidor que deseamos y finalmente clic en Restore.

FIGURA 21

RESTAURACIÓN DEL SISTEMA

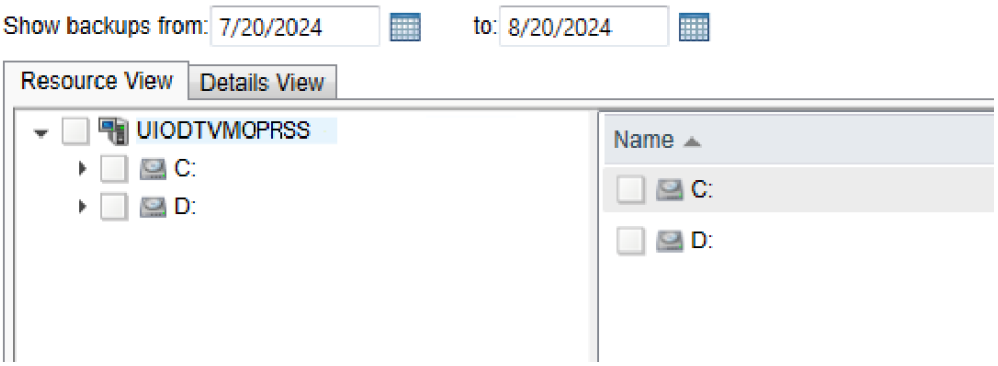


Nota: Guía para restaurar el sistema Opera PMS con Veritas Backup Excec.

Después de seleccionar la opción de Restore, se desplegará el agente de restauración de información con las imágenes que se presentan a continuación.

FIGURA 22

ARCHIVOS PARA RESTAURAR

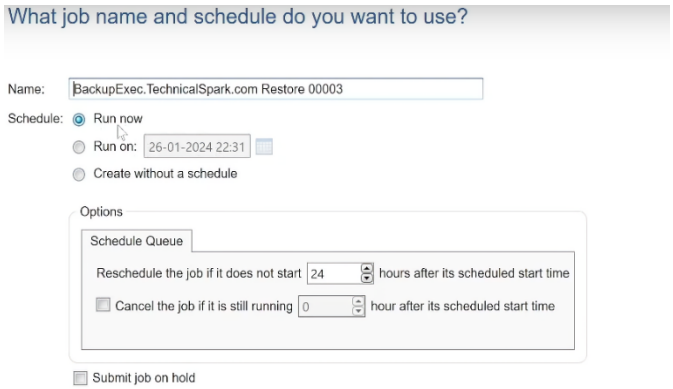


Nota: Guía para restaurar el sistema Opera PMS con Veritas Backup Excec.

En la primera ventana del agente de restauración nos muestra que es lo que deseamos restaurar en este caso seleccionaremos todo el host no solo uno de los discos y también seleccionaremos el destino donde irán los archivos restaurados.

FIGURA 23

UBICACIÓN DE LA RESTAURACIÓN

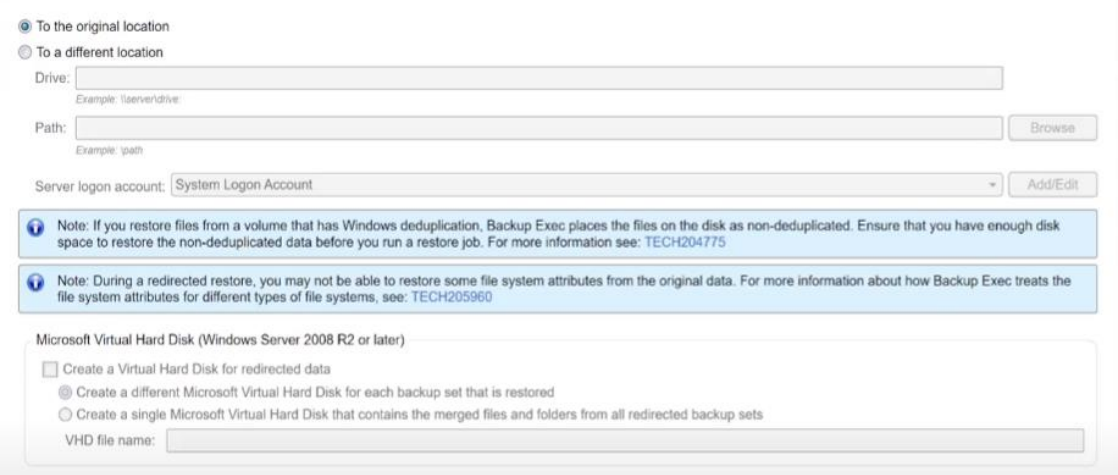


Nota: Guía para restaurar el sistema Opera PMS con Veritas Backup Excec.

Para finalizar le daremos un nombre al trabajo y el proceso de restauración empezará.

FIGURA 24

NOMBRE DE LA RESTAURACIÓN



Nota: Guía para restaurar el sistema Opera PMS con Veritas Backup Excec.

FIGURA 25

EMPIEZA LA RESTAURACIÓN

NOta: Guía para restaurar el sistema Opera PMS con Veritas Backup Excec.

Para este proceso dos factores son tomados en cuenta como el tamaño de los discos y el tipo de discos donde se colocará el nuevo respaldo, para este caso práctico se realizó el respaldo y recuperación del servidor copia del PMS resultando en un tiempo de **dos horas y media** para poder restaurar todo el servidor al estado de las 12AM antes de la actualización.

4.8.4 Cuarta fase de restauración: SDO y WR

Una vez tengamos recuperado el sistema debemos realizar las validaciones necesarias para garantizar que tenemos las funcionalidades esenciales del mismo, para ello se generaran los reportes de guest in house del día actual, también se generara el reporte de guest balance y el reporte de check outs.

Cabe mencionar que es responsabilidad de cada supervisor de Front Desk generar estos reportes al finalizar el turno para garantizar la operación en caso de un desastre como el que se simulo, contando con esos reportes se puede tener una tolerancia máxima de 12 horas sin el sistema PMS ya que las cuentas por dar salida solo se cobraran mediante el POS.

4.8.5 Resumen de restauración

TABLA 5

RESUMEN DE RESTAURACIÓN RPO Y RTO

Servicio	RPO (Punto de recuperación)	RTO (Tiempo de recuperación)	Recursos Críticos	Notas especiales
Opera PMS	7 horas	3 horas	Servicio de asignación de reservas y asignación de habitaciones	Prioridad alta, pero al siempre realizar actualizaciones los lunes de baja ocupación en la madrugada tenemos un lapso para actual.

Nota: Detalle de los tiempos empleados desde el reporte de la falla hasta la recuperación, Esteban Moyolema.

4.8.6 Control de RPO del servidor afectado

TABLA 6

CONTROL DE RPO

Servicio	RPO	Soluciones de seguridad
Opera PMS	3~4 horas	Servicio de respaldo con Veritas Backup Servicio de respaldo con Veam Backup RAID 1+0 Respaldo en medio extraíble

Nota: Tiempo máximo para recuperar el sistema y soluciones que se utilizan para restaurar el sistema, Esteban Moyolema.

CAPÍTULO V

ANÁLISIS DE LOS RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

5.1 Análisis de los resultados

El análisis de los resultados de este trabajo se basa en solventar las interrogantes de la investigación que se presentan en la sección 1.2. Interrogantes de la investigación. A continuación, se presentarán las interrogantes de la investigación y el análisis que se realizó en este trabajo para solventar esas interrogantes.

1.- ¿Qué amenazas específicas de ciberseguridad son más frecuentes en el sector hotelero y cómo afectan a las operaciones del hotel y a la seguridad de los datos de los huéspedes?

Phishing: Los empleados son el blanco de correos electrónicos fraudulentos que buscan obtener credenciales de acceso. Si un empleado cae en la trampa, los atacantes pueden comprometer los sistemas internos, afectando la operación diaria, como reservas, check-ins y check-outs, y acceso a información confidencial.

Ataques a sistemas de puntos de venta (POS): El sistema POS es uno de los principales objetivos de los cibercriminales. Si se compromete, pueden robarse datos de tarjetas de crédito de los huéspedes. Esto afecta la confianza de los clientes y puede causar sanciones legales por el incumplimiento de normativas de protección de datos.

Ransomware: Los sistemas hoteleros, incluidos los sistemas de gestión de propiedades (PMS), son atacados con software malicioso que bloquea el acceso a los datos a cambio de un rescate. Estos incidentes pueden interrumpir la operación del hotel por completo, afectando la capacidad de gestionar reservas, servicios al huésped y facturación, por esa razón se ejemplificó un escenario en este trabajo.

Violación de datos personales: Los hoteles almacenan una gran cantidad de información personal de los huéspedes, incluyendo datos de tarjetas de crédito, preferencias de estancia y pasaportes. Una violación de estos datos afecta la privacidad y seguridad de los huéspedes, lo que puede generar daños reputacionales y financieros.

2.- ¿Cómo gestionan actualmente los incidentes de ciberseguridad las empresas hoteleras, incluidas las grandes cadenas como JW Marriott, y qué lagunas existen en sus estrategias de respuesta a incidentes?

Monitoreo continuo: Utilizan sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para monitorear su red en tiempo real y detectar actividades anómalas, aunque en esta ocasión no se utilizaron este tipo de sistemas se podría ver qué ventajas tiene el uso de estos en trabajos futuros.

Políticas de respuesta a incidentes: Para este trabajo se establecieron políticas para responder a ataques una vez detectados. Estas incluyen la desconexión de sistemas afectados, análisis de los incidentes, respuesta a los incidentes, inventarios de activos a proteger y restauración de sistemas mediante copias de seguridad.

Formación del personal: A las personas recién ingresadas con acceso a computador reciben capacitaciones regulares para enseñarles a reconocer correos electrónicos fraudulentos y a seguir protocolos seguros, sin embargo, estas capacitaciones se deben realizar con mayor continuidad exponiendo los nuevos ataques y promoviendo la concientización de riegos.

3.- ¿Cuáles son los principales retos y complejidades a los que se enfrentan las empresas hoteleras a la hora de desarrollar y aplicar planes eficaces de respuesta a incidentes adaptados a sus requisitos operativos específicos?

Integración de la ciberseguridad en la operación diaria: En el caso de esta propiedad se manejan márgenes ajustados y grandes volúmenes de huéspedes, lo que dificulta la implementación de nuevas medidas de ciberseguridad sin afectar el servicio al cliente. Equilibrar la seguridad con la operatividad puede ser un desafío y es por ello que es importante realizar un trabajo a conciencia generando los anexos indispensables para implementar un plan de respuestas a incidentes, empezando con el inventario de activos solo de esa manera sabremos que debemos proteger.

Diversidad de sistemas tecnológicos: Los hoteles manejan diferentes tipos de tecnologías, desde sistemas de gestión de propiedades hasta aplicaciones de reserva en línea. La integración y protección de todos estos sistemas bajo una estrategia unificada es compleja, especialmente cuando algunos de estos sistemas son antiguos o no compatibles con soluciones modernas de ciberseguridad como por ejemplo los sistemas de troncales telefónicas.

Falta de un enfoque especializado: Las empresas hoteleras suelen contar con generalistas de TI en lugar de especialistas en ciberseguridad, lo que limita la capacidad de respuesta ante amenazas específicas y es por esa razón que este documento ayudara a tener en consideración los puntos que un equipo de TI debe cubrir.

5.2 Conclusiones

Los ataques de ransomware y las filtraciones de datos son los incidentes más críticos en la industria hotelera. Estos ataques pueden llevar a la pérdida de datos sensibles de clientes y empleados, así como a la paralización de operaciones, lo que resulta en importantes repercusiones financieras y de reputación para los hoteles. Las amenazas emergentes requieren una vigilancia constante y la implementación de medidas preventivas y reactivas para proteger la información y mantener la continuidad del negocio.

La aplicación del marco metodológico NIST al hotel JW Marriott de Quito revela una serie de activos críticos, como la infraestructura de red, los sistemas de gestión de habitaciones y la información de los huéspedes, que deben ser protegidos contra diversos riesgos cibernéticos. Identificar estos activos y evaluar los riesgos asociados permite priorizar las áreas que requieren una mayor protección y desarrollar estrategias específicas para mitigar las amenazas identificadas.

El análisis de riesgos según el marco NIST destaca la importancia de evaluar tanto las amenazas internas como externas para el JW Marriott. Los riesgos incluyen vulnerabilidades en los sistemas informáticos y la posibilidad de ataques dirigidos. Esta identificación detallada permite al hotel implementar controles adecuados y políticas de seguridad para proteger sus activos, asegurando una respuesta efectiva ante cualquier incidente de ciberseguridad.

Un plan de respuesta a incidentes de ciberseguridad bien estructurado que tenga en cuenta la legislación vigente y la normativa interna es crucial para el JW Marriott de Quito. Este plan debe incluir procedimientos claros para la identificación, contención y recuperación de incidentes, así como para la comunicación con las partes interesadas y la notificación a las autoridades reguladoras.

La integración de la legislación local e internacional en el plan de respuesta a incidentes asegura que el JW Marriott no solo cumpla con las regulaciones aplicables, sino que también esté preparado para enfrentar posibles sanciones y responsabilidades legales. La normativa interna del hotel, cuando se alinea con estas regulaciones, fortalece el plan de respuesta, permitiendo una gestión más eficiente y legalmente acorde de los incidentes de ciberseguridad.

Evaluar el plan de respuesta a incidentes en el contexto del JW Marriott permite identificar áreas de mejora y ajustar estrategias para asegurar que el plan sea efectivo en la

práctica. Esta evaluación proporciona una visión clara de cómo el plan aborda las amenazas específicas del hotel y permite realizar ajustes basados en simulaciones de incidentes.

La aplicación del plan de respuesta a incidentes en el caso del JW Marriott demuestra su utilidad para la toma de decisiones operativas y estratégicas durante un incidente de ciberseguridad. Un plan bien evaluado permite a la gerencia tomar decisiones informadas y rápidas, minimizando el impacto en las operaciones del hotel y asegurando una recuperación eficaz, lo que refuerza la importancia de mantener y revisar regularmente el plan para adaptarse a nuevas amenazas y cambios en el entorno operativo.

5.3 Recomendaciones

Se recomienda revisar y ajustar el calendario de respaldos, considerando la frecuencia de respaldos completos e incrementales. El plan debe asegurar que los respaldos se realicen en momentos de baja actividad para minimizar el impacto en las operaciones. Además, es crucial validar periódicamente que los respaldos se completen exitosamente y que sean accesibles para la restauración rápida en caso de un incidente.

Se debe llevar a cabo una evaluación regular del plan de recuperación ante desastres mediante simulacros y pruebas de recuperación. Estas pruebas deben incluir escenarios de incidentes diversos para verificar la eficacia de los procedimientos y la capacidad de restauración de sistemas críticos. Además, se recomienda actualizar el plan de recuperación y los procedimientos asociados en función de los resultados de estas pruebas y de los cambios en la infraestructura tecnológica.

Es fundamental proporcionar capacitación continua al personal clave sobre el plan de recuperación ante desastres y las mejores prácticas de ciberseguridad. Asegurarse de que todos los involucrados comprendan sus roles y responsabilidades durante un incidente es esencial para

una respuesta rápida y efectiva. Además, fomentar la conciencia sobre las amenazas cibernéticas y las técnicas de prevención ayudará a reducir la probabilidad de incidentes y a mejorar la resiliencia general del sistema.

CAPÍTULO VI

TRABAJO FUTURO

Para los trabajos futuros, existen varias oportunidades para expandir y probar la validez de esta tesis en escenarios más reales y complejos

Aunque la tesis actual se basa en simulaciones y pruebas controladas, un trabajo futuro importante sería aplicar y validar estas estrategias durante una crisis real. Esto permitiría observar el comportamiento de los sistemas en situaciones auténticas de estrés y ofrecería datos más precisos sobre la eficacia de las medidas de seguridad propuestas. Es crucial diseñar estudios de caso en colaboración con hoteles durante incidentes de ciberseguridad para documentar y analizar el impacto en tiempo real.

Otra dirección interesante para futuros trabajos sería considerar hoteles que operan con infraestructuras completamente en la nube. A diferencia del enfoque actual, que se centra en sistemas locales, los sistemas en la nube presentan desafíos y oportunidades únicos. Por ejemplo, la escalabilidad y la redundancia son mayores, pero también lo son las amenazas en términos de acceso no autorizado y dependencias de terceros. Estudiar estas configuraciones permitirá desarrollar estrategias más robustas y adaptadas a las necesidades de la industria moderna.

En el futuro también podría ver la integración de tecnologías emergentes como la automatización y la inteligencia artificial en la ciberseguridad hotelera. Esto podría incluir el uso de sistemas automatizados de detección y respuesta ante amenazas, análisis predictivo para la prevención de incidentes, y la utilización de IA para la monitorización continua y en tiempo real. Evaluar cómo estas tecnologías pueden mejorar o complementar las estrategias actuales será vital.

Finalmente, se debe poner mayor énfasis en la formación continua y la concienciación del personal. A medida que las amenazas evolucionan, es esencial que los empleados estén equipados con el conocimiento y las herramientas necesarias para reconocer y responder a los ataques, los futuros trabajos podrían investigar métodos más efectivos de formación y evaluar el impacto de estas intervenciones en la reducción de incidentes de ciberseguridad.

Bibliografía

Alawida, M. (03 de Agosto de 2022). *A deeper look into cybersecurity issues in the wake of Covid-19: A survey*. Obtenido de ScienceDirect: https://www.sciencedirect.com/science/article/pii/S1319157822002762

Albornoz, Á. C. (2022). *Ciberseguridad en el sector hotelero.* Madrid: Instituto Tecnologico Hotelero.

Alvarez, C. A. (2011). *Metodologia de la investigacion cuantitativa y cualitativa.* Neiva: Universidad Surcolombiana.

Alves, M. (5 de Octubre de 2023). *Cobis Topaz*. Obtenido de Cómo la ciberseguridad reduce la fricción en la experiencia del cliente: https://blog.cobistopaz.com/es/blog/como-la-ciberseguridad-reduce-la-friccion-en-la-experiencia-del-cliente

Árnason, Á. T. (16 de Abril de 2024). *Social Engineering vs Phishing: Understanding the Differences*. Obtenido de Keystrike: https://keystrike.com/social-engineering-vs-phishing-understanding-the-differences/

Aryee, D. (2020). *Cybersecurity Threats to the Hotel Industry and Mitigation Strategies.* New York: Utica College.

Ashari, R., Grimshaw, D. J., Whitman, M. E., & Townsend, A. M. (1996). *A Study of the Ethical Perceptions of Students in the School of Computer Studies.* San Jose - Recoletos.

Ashari, R., Grimshaw, D. J., Whitman, M. E., Townsend, A. M., & Hendrickson, A. R. (1996). RESEARCH REPORT SERIES-UNIVERSITY OF LEEDS SCHOOL OF COMPUTER STUDIES LU SCS RR. *A Study of the Ethical Perceptions of Students in the School of Computer Studies.*

Ayerdi, A. (27 de Noviembre de 2023). *Ciberataques: ¿Cómo proteger a tu empresa?* Obtenido de DocuWare: https://start.docuware.com/es/blog/ciberataques-proteger-empresa

Bardají, E. (1 de Agosto de 2022). *Ciberseguridad en el sector hotelero*. Obtenido de esed: https://www.esedsl.com/blog/ciberseguridad-en-el-sector-hotelero

Belton, P. (18 de Diciembre de 2017). *El curioso caso del hotel de Austria donde se perdió el control de las cerraduras cuatro veces*. Obtenido de CCN News: https://www.bbc.com/mundo/noticias-42374443

Borner, P. (4 de Diciembre de 2018). *The Data Privacy Group*. Obtenido de El hackeo de Marriott afecta a 500 millones: https://thedataprivacygroup.com/es/blog/marriott-hack-affects-500-million/#

Bower, M. (1 de Enero de 2016). *Hyatt credit card breach affected 250 hotels worldwide*. Obtenido de Global Security Mag: https://www.globalsecuritymag.fr/Hyatt-credit-card-breach-affected,20160118,59006.html

Ceupe. (24 de Junio de 2024). *European Business School*. Obtenido de La hospitalidad en la industria turística: https://www.ceupe.com/blog/la-hospitalidad-en-la-industria-turistica.html

Chehayeb, K. (24 de Marzo de 2022). *Hotel WiFi across MENA compromised and exposing private data*. Obtenido de Aljazeera: https://www.aljazeera.com/news/2022/3/24/hotel-wifi-across-mena-compromised-and-exposing-private-data

Chen, S.-T., Huang, T.-W., & Yang, C.-T. (2020). *High-SNR steganography for digital audio signal in the wavelet domain.*

Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H. (2019). *Comparative study of digital audio steganography techniques.* India.

Donelson, B. (18 de Diciembre de 2014). *Marriott Fined $600,000 For Wi-Fi Jamming*. Obtenido de BAKER DONELSON: https://www.bakerdonelson.com/Marriott-Fined-600000-For-Wi-Fi-Jamming-12-18-2014

Duque, A. (9 de Noviembre de 2021). *Wortise*. Obtenido de Protección de datos ¿Qué debes saber sobre GDPR y CCPA?: https://wortise.com/blog/proteccion-datos-gdpr-ccpa/

Edwards, J. (11 de Octubre de 2021). *An easy 10-step guide for testing backups*. Obtenido de TechTarget: https://www.techtarget.com/searchdatabackup/tip/Ten-important-steps-for-testing-backups

Gasbarrino, S. (19 de Julio de 2023). *Guía de control de inventarios: qué es, cómo hacerlo y ejemplos*. Obtenido de HubSpot: https://blog.hubspot.es/sales/que-es-control-de-inventarios

Guaña-Moya, J., Chiluisa-Chiluisa, M., Jaramillo-Flores, P. d., Naranjo-Villota, D., Mora-Zambrano, E. R., & Larrea-Torres, L. G. (2022). *Ataques de phishing y cómo prevenirlos.* Quito: UCE.

Haenraets, B. (2024 de July de 2024). *Sistema de Gestión Hotelera (PMS)*. Obtenido de Viqal: https://www.viqal.com/es/blog/sistema-de-gestion-hotelera-pms

HOLZER, J. C., DEW, A. J., RECUPERO, P. R., & GILL, P. (2022). Developing a Risk Assessment and Intervention Strategy.

Jimenez, G. (22 de Agosto de 2024). *Ciberseguridad en hoteles: amenazas en aumento y cómo protegerse*. Obtenido de Rio Bravo: https://www.riobravosystems.com/es/ciberseguridad-en-hoteles-amenazas-en-aumento-y-como-protegerse/

Jímenez, G. (24 de Junio de 2024). *Rio Bravo Systems*. Obtenido de Ciberseguridad en hoteles: amenazas en aumento y cómo protegerse: https://www.riobravosystems.com/es/ciberseguridad-en-hoteles-amenazas-en-aumento-y-como-protegerse/

Jiménez, M. M. (13 de Abril de 2022). *Vulnerabilidades que afectan la seguridad de la información*. Obtenido de pirani: https://www.piranirisk.com/es/blog/vulnerabilidades-en-seguridad-de-la-informacion

Kirvan, P. (22 de Enero de 2024). *How to build an incident response plan, with examples, template*. Obtenido de TechTarget: https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan

Kong, A. (1 de Mayo de 2022). *How to design and strengthen cyber security to cope with data breach in the hotel industry?* Obtenido de ResearchGate:

https://www.researchgate.net/publication/360950915_How_to_design_and_strengthen_cyber_security_to_cope_with_data_breach_in_the_hotel_industry

Law, M. (12 de Septiembre de 2023). *Cyber*. Obtenido de Trustwave report on hospitality industry security threats: https://cybermagazine.com/articles/trustwave-report-on-hospitality-industry-security-threats

Lazaricheva, A. (22 de Agosto de 2024). *E-mail attacks on the hotel business*. Obtenido de kasperky Daily: https://www.kaspersky.com/blog/attacks-on-hotel-business/51393/

Lindemulder, G., & Kosinski, M. (12 de Agosto de 2024). *¿Qué es la ciberseguridad?* Obtenido de IBM: https://www.ibm.com/es-es/topics/cybersecurity

Martin, S., Bengtsson, J. E., & Dröes, R. M. (2010). Assistive technologies and issues relating to privacy, ethics and security. Supporting people with dementia using pervasive health technologies. *Springer Link*.

Mitroff, I. I., & Alpaslan, M. C. (2004). *Vulnerability Management for Enterprises: The Impact of Ethical Orientation of Enterprises on their Ability to Manage.* The Marshall School of Business.

Munir, A. (2020). *A Review of Cyber Security Issues in Hospitality Industry.* Manhattan: ResearchGate.

Neda, S., & Arslan, M. (2020). *A Review of Cyber Security Issues in Hospitality Industry.* Springer International Publishing.

News, B. (30 de Noviembre de 2018). *Marriott: un ataque informático deja expuestos los datos de 500 millones de clientes del grupo hotelero*. Obtenido de BBC News: https://www.bbc.com/mundo/noticias-46404767

OEA. (2019). Ciberseguridad Marco NIST. *OEA*, https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf.

Pagnotta, S. (25 de Noviembre de 2015). *Welivesecurity*. Obtenido de Hilton confirma que fue víctima de un malware PoS: https://www.welivesecurity.com/la-es/2015/11/25/hilton-victima-malware-pos/

Pagnotta, S. (15 de Enero de 2016). *Welivesecurity*. Obtenido de Roban datos de huéspedes del Hyatt en 50 países, algunos de Latinoamérica: https://www.welivesecurity.com/la-es/2016/01/15/roban-datos-huespedes-hyatt-paises-latinoamerica/

Prasanna, M., & Nandi, S. (2019). *An Overview of Digital Audio Steganography.* Michigan.

Rajiah, S. K. (16 de Julio de 2020). *Las vulnerabilidades de seguridad de los sistemas de punto de venta y cómo abordarlas*. Obtenido de encora: https://www.encora.com/es/blog/the-security-vulnerabilities-of-pos

Rajiah, S. K. (16 de Julio de 2020). *Las vulnerabilidades de seguridad de los sistemas de punto de venta y cómo abordarlas*. Obtenido de encora: https://www.encora.com/es/blog/the-security-vulnerabilities-of-pos

ROLFE, A. (19 de Abril de 2017). *InterContinental confirms malware based payment card breach at 1200 hotels*. Obtenido de Payments: https://www.paymentscardsandmobile.com/intercontinental-confirms-malware-based-payment-card-breach-1200-hotels/

Rouse, M. (22 de August de 2024). *ITIL, Librería de Infraestructura de Tecnologías de Información*. Obtenido de TechTarget: https://www.computerweekly.com/es/definicion/ITIL-Libreria-de-Infraestructura-de-Tecnologias-de-Informacion

Schwartz, M. J. (29 de Septiembre de 2015). *Trump Hotels Confirms POS Malware Breach*. Obtenido de Bank Info: https://www.bankinfosecurity.com/trump-hotels-confirms-malware-attack-a-8555

Security, O. D. (2021). La ciberseguridad en la industria hotelera. *ODS*, https://opendatasecurity.io/wp-content/uploads/2021/02/Ciberseguridad-en-la-industria-hotelera.pdf.

Shabani, N. (2016). *A STUDY OF CYBER SECURITY IN HOSPITALITY INDUSTRY.* Florida: College of Hospitality and Tourism leadership.

Simplilearn. (13 de August de 2024). *What is COBIT? Understanding the COBIT Framework*. Obtenido de SimplLearn: https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article

Solutions, G. (22 de Septiembre de 20223). *¿Qué es la norma ISO 27001 y para qué sirve?* Obtenido de GlobalSuite: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

Spinello, R. (2011). *Cyberethics: Morality and law in cyberspace. Jones & Bartlett Learning.* Fourth Editorial.

Staff, C. (2 de Abril de 2024). *Cybersecurity in the Hospitality Industry: Your 2024 Guide*. Obtenido de coursera: https://www.coursera.org/articles/cyber-security-in-hospitality-industry

Stripe. (13 de Marzo de 2024). *Aspectos básicos del software malicioso en sistemas POS: qué factores de riesgo debes conocer y cómo proteger tu negocio*. Obtenido de Stripe: https://stripe.com/es/resources/more/pos-malware-101-risk-factors-to-know-and-how-to-protect-your-business

Technology, N. I. (2021). NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide. *NIST*.

Thome, C. (15 de Enero de 2024). *Guide to Server Backups: Creating a Backup Strategy*. Obtenido de Chicorporation: https://chicorporation.com/guide-to-server-backups-creating-a-backup-strategy/

Tong, L., Kong, A., & Kwan, M. (2022). *How to design and strengthen cyber security to cope with data.* Hong Kong: APacCHRIE 2022 Conference (23-25 May 2022).

Trautman, L. (1 de Enero de 2018). *Wannacry, Ransomware, and the Emerging Threat to Corporations*. Obtenido de ResearchGate: https://www.researchgate.net/publication/327463247_Wannacry_Ransomware_and_the_Emerging_Threat_to_Corporations

Trout, J. (23 de Febrero de 2024). *ANÁLISIS DE CRITICIDAD: QUÉ ES Y POR QUÉ ES IMPORTANTE*. Obtenido de Congreso de mantenimiento y confiabilidad: https://cmc-latam.com/2022/02/23/analisis-de-criticidad-que-es-y-por-que-es-importante/

Tunggal, A. T. (15 de Septiembre de 2023). *What are the CIS Controls for Effective Cyber Defense?* Obtenido de UpGard: https://www.upguard.com/blog/cis-controls

Vargas, M. (26 de Marzo de 2024). *La ciberseguridad en el sector educativo: desafíos y estrategias para proteger datos sensibles* . Obtenido de Inova: https://inovasolutions.com.ec/la-ciberseguridad-en-el-sector-educativo-desafios-y-estrategias-para-proteger-datos-sensibles/

Vivancos, E. (06 de September de 2022). *Los 10 vectores de ataque más utilizados por los ciberdelincuentes*. Obtenido de INCIBE: https://www.incibe.es/empresas/blog/los-10-vectores-ataque-mas-utilizados-los-ciberdelincuentes

Anexos

Anexo 1 – Inventario de activos

A continuación, se presentan capturas de las tablas del Anexo 1 inventario de activos, al ser un archivo de Excel la única manera de adjuntarlo como un anexo.

Para el documento debemos crear el libro donde se especifican las empresas esto se hace referencia en la Figura 1, también se debe crear un pequeño resumen del documento que se hace referencia en la Figura 7, debemos describir todos los activos físicos del hotel que usan nuestros colaboradores por ello en la Figura 6 se describen estos equipos, de la misma manera se debe describir los activos virtuales como en la Figura 2, los servicios que se ejecutan en los servidores ya sean virtuales o físicos también se deben de especificar como en la Figura 3, se debe tener en cuenta el factor humano que opera el departamento de sistemas este se especifica en la Figura 4, también se deben especificar las actividades que se realizan por cada servicio como en la Figura 5 y las actividades por cada equipo físico como en la Figura 9, las bases de datos sin indispensables por lo que debemos obtener un listado de cada una de ellas Figura 8, después de obtener los activos de la propiedad tendremos que medir el impacto que pueden tener los incidentes en la continuidad de negocio para ello nos guiaremos en la Figura 10, finalmente describiremos como los riesgos afectan cada factor del negocio como en la Figura 11.

ID	DataCenter	HW	Empres	NombreMaquinaVirtual	Funcionali	Est. Activ	EstadoAlar	Host	Host	vCPU	Host Me	IP4	IP4-2	IP6	Nombre Redes	Guest OS	Provisioned Sp
3	AMAZONASHOT	HP	TI	UIODTVMDLS1	Control de puert	TRUE	OFF	10.163.132.15	335MHZ	4	12	10.163.132.11			VM Network	Microsoft Windows Ser	
4	AMAZONASHOT	HP	TI	UIODTVMERP1	ERP	TRUE	OFF	10.163.132.15	981MHZ	8	32	10.163.132.6			VM Network	Microsoft Windows Ser	
5	AMAZONASHOT	HP	TI	UIODTVMIFC1	Interfaz	TRUE	OFF	10.163.132.15	406MHZ	4	8	10.163.132.3			VM Network	Microsoft Windows Ser	
6	AMAZONASHOT	HP	TI	UIODTVMOPRSS	PMS	TRUE	OFF	10.163.132.15	15.92GH	8	128	10.163.132.2			VM Network	Microsoft Windows Ser	
7	AMAZONASHOT	HP	TI	UIODTVMPAYROLL1	Roll de pagos	TRUE	OFF	10.163.132.15	263MHZ	4	8	10.163.132.34			VM Network	Microsoft Windows Ser	
10	AMAZONASHOT	HP	TI	UIODTVMDC1	AD	TRUE	OFF	10.163.132.16	746MHZ	4	8	10.163.132.20			VM Network	Microsoft Windows Ser	
11	AMAZONASHOT	HP	TI	UIODTVMFP2	File And Print	TRUE	OFF	10.163.132.16	293MHZ	4	6	10.163.132.23			VM Network	Microsoft Windows Ser	1.97TB
12	AMAZONASHOT	HP	TI	UIODTVMBE1	BackUp	TRUE	OFF	10.163.132.18	353MHZ	4	12	10.163.132.18			VM Network	Microsoft Windows Ser	
13	AMAZONASHOT	HP	TI	UIODTVMCAPS	POS	TRUE	OFF	10.163.132.18	2.37GH	8	12	10.163.132.18			VM Network	Microsoft Windows Ser	
14	AMAZONASHOT	HP	TI	UIODTVMIFC2	Interfaz	TRUE	OFF	10.163.132.18	353MHZ	4	8	10.163.132.3			VM Network	Microsoft Windows Ser	
15	AMAZONASHOT	HP	TI	UIODTVMOPRSS2	PMS	TRUE	OFF	10.163.132.18	12.15GH	8	64	10.163.132.2			VM Network	Microsoft Windows Ser	
16	AMAZONASHOT	HP	TI	UIODTVMPOS	POS	TRUE	OFF	10.163.132.18	379MHZ	8	12	10.163.132.18			VM Network	Microsoft Windows Ser	
17	AMAZONASHOT	HP	TI	UIODTVMPOS1	POS	TRUE	OFF	10.163.132.18	1.12GHZ	8	6	10.163.132.13			VM Network	Microsoft Windows Ser	
18	AMAZONASHOT	HP	TI	UIODTVMRA	Reportes	TRUE	OFF	10.163.132.18	418MHZ	4	12	10.163.132.9			VM Network	Microsoft Windows Ser	
19	AMAZONASHOT	HP	TI	UIODTVMVC	VC	TRUE	OFF	10.163.132.18	353MHZ	2	12	10.163.132.185			VM Network	Microsoft Windows Ser	
20	AMAZONASHOT	HP	TI	UIODTVMVEEAM1	BackUp	TRUE	OFF	10.163.132.18	957MHZ	4	8	10.163.132.184			VM Network	Microsoft Windows Ser	2.5TB
21	AMAZONASHOT	HP	TI	UIODTVMW10	Cliente	TRUE	OFF	10.163.132.18	3.19GHz	8	12	10.163.132.105			VM Network	Windows 10	

Figura 1. Libro de empresas

EMPRESA	ID	RUC	emailFacturacion	Representante Legal	emalRepresentante	Contador	emailContador
AMAZONASHOT S.A.		179124025100	contabilidad.general@torresdesuites.com	CINA UGARTE DOUGLAS JOSEPH	joseph.cina@marriottquito.com		contabilidad.general@torresdes

Figura 2. Libro de equipos virtuales

EMPRESAS	Nombre	UsoServicio	Tecnología	Aprovisionamiento	Proveedor	Nivel_Impacto	Test Conexión	Descripción	Ambiente	Fecha
AMAZONASHOT S.A.	ANTISPAM	Interno	Harmony	Nube	Telefonica	Medio	Https	ANTISPAM	Produccion	
AMAZONASHOT S.A.	FIREWALL	Interno	PALO ALTO	Local	Palo alto	Alto	Https	FIREWALL	Produccion	
AMAZONASHOT S.A.	Antimalware	Interno	SOPHOS	Local	Sophos	Medio	Https	Antimalware	Produccion	
AMAZONASHOT S.A.	VPN	Interno/Externo	PALO ALTO	Local	Palo alto	Medio	Https	VPN	Produccion	
AMAZONASHOT S.A.	raices.com.ec	externo	DNS	dominiosecuador.ec	dominiosecuador.ec	Alto	Whois	dominio restaurant	Produccion	
AMAZONASHOT S.A.	fogo.com.ec	externo	DNS	dominiosecuador.ec	dominiosecuador.ec	Alto	Whois	dominio restaurant	Produccion	
AMAZONASHOT S.A.	marriottquito.com	externo	DNS	godady	godady	Alto	Whois	dominio hotel	Produccion	
AMAZONASHOT S.A.	Office 365	externo	DNS	Azure	Otecel	Alto	Whois	Office 365 Cuentas de correo hote	Produccion	
AMAZONASHOT S.A.	Office 365	externo	DNS	Azure	Otecel	Alto	Whois	Office 365 Cuentas de correo fogo	Produccion	

Figura 3. Libro de servicios

email	Nombre	Fortalezas	Telf	Estado	No
darwin.cantuna@marriottquit	Darwin Cantuña		999586026	Activo	
systems.assistant@marriottqu	Esteban Moyolema		999585912	Activo	

Figura 4. Libro de recurso humano

TipoRecurso	Empresa	Recurso	Actividad	Procedimiento	URL Procedimien	Tiempo Horas
EQUIPOVIRTUAL	AMAZONASHOT S.A.	MySatcom	Revision de espacio en disco	Ingresar al servidor y comprobar que los dispositivos de almacenamiento tengan espacio suficiente		15 minutos
EQUIPOVIRTUAL	AMAZONASHOT S.A.	DB MySatcom	Verificacion de datos ingresados	Ingreso al servidor obtener un respaldo de la base y verificar que los datos respeten ACID		10 minutos
EQUIPOVIRTUAL	AMAZONASHOT S.A.	VimBackup	Cambio de cintas	Proceso automatico cuando se realiza el cambio de la cinta a tiempo en caso de que se desee re programar la tarea hacerlo desde el servidor		5 minutos
EQUIPOVIRTUAL	AMAZONASHOT S.A.	VMware vCenter Server	Revisar alertas del servidor	Ingresar al administrador de maquinas virtuales y desde el monitor de actividad verificar que no existan alertas		5 minutos
EQUIPOVIRTUAL	AMAZONASHOT S.A.	NEW_7 Dominio QM	Verificar conexiones con el corporativo	Ingresar al servidor y revisar si tiene conexion con la IP publica del corporativo		5 minutos
EQUIPOVIRTUAL	AMAZONASHOT S.A.	O8 VIRT_11	Verificar conexiones con el corporativo	Ingresar al servidor y revisar si tiene conexion con la IP publica del corporativo		5 minutos
EQUIPOVIRTUAL	AMAZONASHOT S.A.	SiaWeb_3	Verificar conexiones con el corporativo	Ingresar al servidor y revisar si tiene conexion con la IP publica del corporativo		5 minutos
SERVICIO	AMAZONASHOT S.A.	Sophos Antivirus	- Instalar clientes en los equipos de usuario - Monitoriear/solucionar casos reportados por Sophos - Actualizar permisos y accesos a los dispositivos			60 minutos

Figura 5. Libro de actividades x servicio

EMPRESA	Tipo	Marca	Modelo	Descripción	NroParte	Serie	Voltaje	Tipo Presentacion	Alto en U	IP Adminis	S.O.	Modelo CPU	RAM	Cant HD	Consur	DataCer
AMAZONASHOT S.A.	Notebook	LENOVO	Thinkpad X1 Yoga Gen2	Executive Offices	20JES0CH3Q	R90Q2C5D	110 y 220V	LAPTOP	1		Windows 10	I7-7650U	16	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	Yoga 9 14IRP8	Executive Offices	83B1001XUS	PF4BP7V3	110 y 220V	LAPTOP	1		Windows 11	I7-1360P	16	1 SSD 1024Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	Thinkpad X1Yoga Gen2	Food & Beverage	20JES0CH3Q	R90Q2C5J	110 y 220V	LAPTOP	1		Windows 10	I7-7650U	16	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	Thinkpad X1Yoga Gen2	Event Management	20JES0CH3Q	R90Q2C5G	110 y 220V	LAPTOP	1		Windows 10	I7-7650U	16	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	Thinkpad X1Yoga Gen2	Front Office	20JES0CH3Q	R90Q2C5H	110 y 220V	LAPTOP	1		Windows 10	I7-7650U	16	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	Yoga 9 14IRP8	Engineering	83B1001WUS	PF4D12RD	110 y 220V	LAPTOP	1		Windows 11	I7-1360P	16	1 SSD 1024Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	Thinkpad X1Carbon 6th	Executive Offices	20KGS1VR2B	PF1KFADN	110 y 220V	LAPTOP	1		Windows 10	I7-8550U	16	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	Thinkpad X1Carbon 6th	Human Resources	20KGS1VR2B	PF1KFAE1	110 y 220V	LAPTOP	1		Windows 10	I7-8550U	16	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	Thinkpad X1Carbon 6th	Sales	20KGS1VR2B	PF1KFAEK	110 y 220V	LAPTOP	1		Windows 10	I7-8550U	16	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	Thinkpad X1Carbon 6th	Accounting	20KGS1VR2B	PF1KFAEY	110 y 220V	LAPTOP	1		Windows 10	I7-8550U	16	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	Thinkpad X1Carbon 6th	SSU-Systems	20KGS1VR2B	PF1KFAFD	110 y 220V	LAPTOP	1		Windows 10	I7-8550U	16	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	T530	Human Resources	2429-70L	PK200RR	110 y 220V	LAPTOP	1		Windows 10	I5-2520m	8	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	L13 Yoga	Sales	20R6-S4E100	R913E8SW	110 y 220V	LAPTOP	1		Windows 10	I7-1355U	16	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	MICROSOFT	Surface Go 2	Housekeeping	1V810000024	12374403051	110 y 220V	TABLET	1		Windows 10	m3-8100Y	8	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	MICROSOFT	Surface Go 2 - LTE	Housekeeping	1V810000372	51274210451	110 y 220V	TABLET	1		Windows 10	m3-8100Y	8	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	MICROSOFT	Surface Go 2 - LTE	Housekeeping	1V810000372	44597604551	110 y 220V	TABLET	1		Windows 10	m3-8100Y	8	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	ThinkPad X1Yoga Gen 7	Sales	21CES1Q400	PF4A11KD	110 y 220V	LAPTOP	1		Windows 11	I7-1355U	32	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	ThinkPad P16S Gen1	Housekeeping	21BUS0GR00	PF4ANHAF	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	ThinkPad P16S Gen1	Food & Beverage	21BUS0GR00	PF4ANNAZ	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	ThinkPad P16S Gen1	Accounting	21BUS0GR00	PF4CRA9Z	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	ThinkPad P16S Gen1	Accounting	21BUS0GR00	PF4ANKJJ	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	ThinkPad P16S Gen1	Human Resources	21BUS0GR00	PF4ANN9R	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Notebook	LENOVO	ThinkPad P16S Gen1	SSU-Systems	21BUS0GR00	PF4ANKES	110 y 220V	LAPTOP	1		Windows 11	I7-1260P	32	1 SSD 512Gb		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4Z	110 y 220V	DESKTOP	1		Windows 10	I5-7500	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4H	110 y 220V	DESKTOP	1		Windows 10	I5-7501	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4M	110 y 220V	DESKTOP	1		Windows 10	I5-7502	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Front Office	2DR82UP	MXL8071D51	110 y 220V	DESKTOP	1		Windows 10	I5-7503	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4N	110 y 220V	DESKTOP	1		Windows 10	I5-7504	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D3Y	110 y 220V	DESKTOP	1		Windows 10	I5-7505	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4W	110 y 220V	DESKTOP	1		Windows 10	I5-7506	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Human Resources	2DR82UP	MXL8071D3T	110 y 220V	DESKTOP	1		Windows 10	I5-7507	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D3W	110 y 220V	DESKTOP	1		Windows 10	I5-7508	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4T	110 y 220V	DESKTOP	1		Windows 10	I5-7509	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Accounting	2DR82UP	MXL8071D4L	110 y 220V	DESKTOP	1		Windows 10	I5-7510	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Purchasing	2DR82UP	MXL8071D4Q	110 y 220V	DESKTOP	1		Windows 10	I5-7511	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Purchasing	2DR82UP	MXL8071D4P	110 y 220V	DESKTOP	1		Windows 10	I5-7512	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	At Your Service	2DR82UP	MXL8071D47	110 y 220V	DESKTOP	1		Windows 10	I5-7513	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	At Your Service	2DR82UP	MXL8071D48	110 y 220V	DESKTOP	1		Windows 10	I5-7514	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	At Your Service	2DR82UP	MXL8071D49	110 y 220V	DESKTOP	1		Windows 10	I5-7515	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Banquets	5GL94UP	MXL8491RL7	110 y 220V	DESKTOP	1		Windows 10	I5-7516	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Banquets	5GL94UP	MXL8491RL8	110 y 220V	DESKTOP	1		Windows 10	I5-7517	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Culinary - Restaurants	5GL94UP	MXL8491RM6	110 y 220V	DESKTOP	1		Windows 10	I5-7518	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Culinary - Restaurants	5GL94UP	MXL8491RM7	110 y 220V	DESKTOP	1		Windows 10	I5-7519	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Human Resources	5GL94UP	MXL8491RM8	110 y 220V	DESKTOP	1		Windows 10	I5-7520	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Culinary - Restaurants	5GL94UP	MXL8491RM9	110 y 220V	DESKTOP	1		Windows 10	I5-7521	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Culinary - Restaurants	5GL94UP	MXL8491RMB	110 y 220V	DESKTOP	1		Windows 10	I5-7522	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Culinary - Restaurants	5GL94UP	MXL8491RMC	110 y 220V	DESKTOP	1		Windows 10	I5-7523	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Engineering	5GL94UP	MXL8491RL9	110 y 220V	DESKTOP	1		Windows 10	I5-7524	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Engineering	5GL94UP	MXL8491RLB	110 y 220V	DESKTOP	1		Windows 10	I5-7525	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Engineering	5GL94UP	MXL8491RLC	110 y 220V	DESKTOP	1		Windows 10	I5-7526	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Engineering	5GL94UP	MXL8491RLD	110 y 220V	DESKTOP	1		Windows 10	I5-7527	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Engineering	5GL94UP	MXL8491RLF	110 y 220V	DESKTOP	1		Windows 10	I5-7528	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Event Services	5GL94UP	MXL8491RLG	110 y 220V	DESKTOP	1		Windows 10	I5-7529	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Event Services	5GL94UP	MXL8491RLH	110 y 220V	DESKTOP	1		Windows 10	I5-7530	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Sales	5GL94UP	MXL8491RLJ	110 y 220V	DESKTOP	1		Windows 10	I5-7531	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Event Services	5GL94UP	MXL8491RLL	110 y 220V	DESKTOP	1		Windows 10	I5-7532	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Event Services	5GL94UP	MXL8491RLM	110 y 220V	DESKTOP	1		Windows 10	I5-7533	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Executive Offices	5GL94UP	MXL8491RLN	110 y 220V	DESKTOP	1		Windows 10	I5-7534	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Food & Beverage	5GL94UP	MXL8491RLP	110 y 220V	DESKTOP	1		Windows 10	I5-7535	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Food & Beverage	5GL94UP	MXL8491RLQ	110 y 220V	DESKTOP	1		Windows 11	I5-7536	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	SPA	5GL94UP	MXL8491RLR	110 y 220V	DESKTOP	1		Windows 10	I5-7537	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Food & Beverage	5GL94UP	MXL8491RLY	110 y 220V	DESKTOP	1		Windows 10	I5-7538	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Front Office	2DR82UP	MXL8071D41	110 y 220V	DESKTOP	1		Windows 10	I5-7539	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Front Office	2DR82UP	MXL8071D4G	110 y 220V	DESKTOP	1		Windows 10	I5-7540	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Front Office	2DR82UP	MXL8071D46	110 y 220V	DESKTOP	1		Windows 10	I5-7541	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	SSU-Systems	2DR82UP	MXL8071D45	110 y 220V	DESKTOP	1		Windows 10	I5-7542	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Front Office	2DR82UP	MXL8071D42	110 y 220V	DESKTOP	1		Windows 10	I5-7543	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Front Office	2DR82UP	MXL8071D43	110 y 220V	DESKTOP	1		Windows 10	I5-7544	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Front Office	2DR82UP	MXL8071D50	110 y 220V	DESKTOP	1		Windows 10	I5-7545	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Front Office	2DR82UP	MXL8071D44	110 y 220V	DESKTOP	1		Windows 10	I5-7546	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Front Office	5GL94UP	MXL8491RLZ	110 y 220V	DESKTOP	1		Windows 11	I5-7547	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Banquets	5GL94UP	MXL8491RM0	110 y 220V	DESKTOP	1		Windows 10	I5-7548	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Housekeeping	2DR82UP	MXL8071D3Z	110 y 220V	DESKTOP	1		Windows 10	I5-7549	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Housekeeping	2DR82UP	MXL8071D4C	110 y 220V	DESKTOP	1		Windows 10	I5-7550	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Housekeeping	5GL94UP	MXL8491RM4	110 y 220V	DESKTOP	1		Windows 10	I5-7551	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G4 SFF	Housekeeping	5GL94UP	MXL8491RMD	110 y 220V	DESKTOP	1		Windows 10	I5-7552	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Human Resources	2DR82UP	MXL8071D4B	110 y 220V	DESKTOP	1		Windows 10	I5-7553	8	1 SSD 250GB		NO
AMAZONASHOT S.A.	Desktop	HP	HP EliteDesk 800 G3 SFF	Human Resources	2DR82UP	MXL8071D3X	110 y 220V	DESKTOP	1		Windows 10	I5-7554	8	1 SSD 250GB		NO

Figura 6. Libro de equipos físicos

ID	Titulo	Ubicación	Comentarios	Estado
1	**Gestión de activos y servicios**			
1.1	Listado Equipos físicos	Equipos Hardware	Instalaciones (equipo pasivo) Equipo Data Center: servidores, comunicaciones, firewall, router, UPS, Sensores, cámaras, etc) Equipo usuarios (computadoras, teléfonos fijos, celulares, cámaras, etc) - Datos: Fecha de compra, ubicación, etc. Ver pestaña "Equipos físicos" de	100%
1.2	Listado Equipos Virtuales	Máquina Virtuales	Lista de los equipos virtuales onpremise y en la nube. Detallado	100%
1.3	Listado Servicios	Listado de servicios	Servicios, propios y de terceros. Incluir mis sistemas y mis servicios instalados, también licencias, dominios, contratos	100%
1.4	Listado de Bases de datos	Bases de Datos	Bases de datos locales o en la nube	100%
1.5	Lista de Recurso humano	Recurso Humano	Personal de tecnología	100%
1.6	Diagrama físico de la red		Url a la imagen o al sistema	
1.7	Diagrama lógico		Descripción de redes, Vlan, ruteo, VPN (gráfico o texto)	
2	**Gestión de mesa de ayuda**		Se puede gestionar con GLPI, revisar política del corporativo, se puede administrar un solo procedimiento como mesa de ayuda que cubra todos los temas	
2.1	Procedimiento Gestión de cambios			
2.2	Procedimiento Base de conocimiento PyR		Incluir en los manuales, documentos técnicos y de usuario, los problemas recurrente	N/A
2.3	Procedimiento de soporte remoto		Uso de GLPI para tickets, uso de consola remota	100%
3	**Gestión de Políticas**			
3.1	Política de uso del antivirus		Todas las PCs deben contar con un antivirus y llevar control de ello	100%
3.2	Política de creación de usuarios y política de claves			100%
3.3	Política de uso de correo electrónico			
3.4	Política de desarrollo de software		(Desarrollo o adquisición)	N/A
3.5	Politica de equipos nuevos		Estos equpos siempre deben ser provistos por el area de sistemas, las diferentes areas del hotel no podran realizar compras de dispositivos como: Computadoras, Celulares, Tabletas, Puntos de ventas, etc. sin la autorizacion y conocimiento del area de sistemas.	100%
3.6	Política de escritorio limpio		Evitar exposicion de documentos sensibles sobre la mesa	20%
3.7	Políticas de enlaces e internet		Mantener al menos dos enlaces de internet en caso de falla de alguno de los servicic	100%
4	**Planes (Procedimientos), Políticas, Documentos**			
4.1	Plan de mantenimiento preventivo (Activos: Hardware, MV, Servicios)		Se realizan mantenimiento a los activos cada año y medio para no interferir con las actividades de los departamentos	100%
4.1.1	Actividades por recurso (HW)	Hardware	(Parte del plan de mantenimiento y gestión de recursos)	100%
4.1.2	Actividades por recurso (Servicios)		(Parte del plan de mantenimiento y gestión de recursos)	N/A
4.2	Procedimiento de respaldos, recuperación		Los respaldos deben tener tres vias de gestion, mediante cintas magneticas las cuales abandonan la propiedad a un lugar seguro, mediante backups virtuales a maquinas externas y backup a un dispositivo de almacenamiento externo.	100%
4.3	Procedimiento de monitoreo Antivirus y gestión de incidentes		Se utiliza la plataforma de Sophos Center para el monitoreo de Antivirus y gestion de incidentes	100%
4.4	Procedimiento de compra de Bienes y servicios en teconología		Comparacion de ofertas con al menos tres proveedores en caso de que las ofertas superen los $300 dolares americanos	100%
4.5	Documentos técnicos		Listar los documentos técnicos, manuales de usuario, etc, con la ubicación de cada uno, puede integrarlos a la base de conocimiento	100%
4.6	Procedimiento acceso remoto		Lista de usuarios con acceso remoto, por SSH, RDP, VPN, etc. (Es para usuarios no administrador u operador del sistema) El procedimiento debe indicar frecuencia de revisión de los accesos Los usuarios creados deben tener fecha de caducidad de credenciales (ej. 3	100%
4.7	Procedimiento de gestión de credenciales		Contar con las credenciales de administración de los equipos y servicios en un repositorio seguro o en papel, documentar formalmente. (Se lo realizo mediante el departamento de procesos y la altagerencia del hotel)	100%
5	**Monitoreo, Alertas e Incidentes**		(Logs)	
5.1	Monitoreo, gestión de alertas generadas (Activos y Servicios)		Usar un sistema de monitoreo como Zabix, PRTG, dude	0%
5.2	Procedimiento para la gestión alertas e incidentes de monitoreo		Gestionar las alertas y notificaciones. Integrar con SMS, Telgram o whatsapp. Se utiliza SMS como sistema de gestion de novedades la tener todas las cuentas corporativas con el servicio de Office 365	60%
6	**Plan de continuidad del negocio**			
6.1	Matriz de impacto			
6.2	Gestión de Riesgos estratégicos		Documento que incluye planes, procedimientos publiado y la gestión de riesgo	
6.2.1	Matriz de riesgos	Matriz de riesgos		
6.3	Plan de mitigación			
7	**Mejora**			
7.1	Plan de reuniones planificadas y periódicas de Mejora		Detalle de la frecuencia y agenda que se va a tratar. Suele ser revisar el plan de continuidad del negocio, revisión de incidentes por gravedad,	
7.2	Acta de revisión y mejora (lecciones aprendidas)	Acta de revision	Resultado de cada reunión con las acciones a tomar y documentar en la base de conocimiento si fuera el caso	
8	**Personal de tecnología**			
8.1	Recurso Humano (Ver 1.5)	Recurso Humano!A1		
8.2	Plan de capacitación			
8.3	Perfil de Actividades y responsabilidades		Cada recurso cuenta con un conjunto de actividades a realizarse de forma periódica o por evento y cuenta con un responsable para realizarlo. Se consultar en las tablas de actividades x <recurso> y mantener actualizado	

Figura 7. Libro de plan

ID	NombreBD	Maquina Virtual	Descripción	SGBD	Instancia	EstadoBD	Tamaño Giga	Ubicación Backup	Ubicación	Fr
1	fiscalDB	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	0.58			DI
2	sat_catalogo	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	0.32			DI
3	sat_comprobante	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	7.94			DI
4	sat_comprobante_his	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	1			DI
5	sat_conciliacion	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	0.08			DI
6	sat_ecommerce	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	0.08			DI
7	sat_logging	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	1.25			DI
8	sat_seguridad	UIODTVMERP1	Facturador Electronico	SqlServer	MYSATCOM5	ACTIVA	0.72			DI
9	ACTIVOFIJO	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	0.8			DI
10	ACTIVOFIJO_PRUEBA	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	0.8			-
11	CONTAB_NUEVA	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	1.79			DI
12	CONTAB_PRUEBA	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	1.79			-
13	CONTABILIDAD	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	1.97			DI
14	dbGYM	UIODTVMERP1	Sistema GYM	SqlServer	UIODTVMERP1	ACTIVA	0.72			DI
15	INVEN_NUEVO	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	3.43			DI
16	INVEN_PRUEBA	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	3.43			-
17	INVENTARIO	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	3.6			DI
18	NOMINA	UIODTVMERP1	RRHH	SqlServer	UIODTVMERP1	ACTIVA	0.24			DI
19	NOMINA_PRUEBA	UIODTVMERP1	RRHH	SqlServer	UIODTVMERP1	ACTIVA	0.24			-
20	SiesaAccess_HMRR	UIODTVMERP1	RRHH	SqlServer	UIODTVMERP1	ACTIVA	0.17			DI
21	TECHIND	UIODTVMERP1	RRHH	SqlServer	UIODTVMERP1	ACTIVA	2.44			DI
22	ZeusComplementos	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	0.8			DI
23	ZEUSEXCELCOMPLEMENTOS	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	0.8			DI
24	ZeusInterfacesExternas	UIODTVMERP1	Contabilidad e Inventarios	SqlServer	UIODTVMERP1	ACTIVA	0.9			DI
25	CheckPostingDB	UIODTVMCAPS	POS	SqlServer	SQLEXPRESS	ACTIVA	4			DI
26	DataStore	UIODTVMCAPS	POS	SqlServer	SQLEXPRESS	ACTIVA	4			DI
27	Softland	UIODTVMPAYROLL1	RRHH	Oracle	UIODTVMPAYROLL1	ACTIVA	2.85			DI
28	MCRSPOS01	UIODTVMPOS	POS	Oracle	UIODTVMPOS	ACTIVA	14.5			DI
29	UNDOTBS01	UIODTVMPOS	POS	Oracle	UIODTVMPOS	ACTIVA	10.3			DI
30	LOCDB	UIODTVMPOS	POS	Oracle	UIODTVMPOS	ACTIVA	4.12			DI
31	OPERA	UIODTVMOPRSS	PMS	Oracle	UIODTVMOPRSS	ACTIVA	159			DI

Figura 8. Libro de Bases de Datos

ID	Tipo Activo	Actividad	Procedimiento	URL Procedimiento	Tiempo Horas	Tipo
1	Pantalla y NUC	Verificacion de funcionamiento	Conexion remota por AnyDesk para verificar si estan encendidas		10 minutos	
2	Pantallas y PC Stick	Actualizacion de contenido	Conexion remota por LogicalSignage		2 horas	
3	UPS	Revision de alarmas y luces led de alerta	Verificar si algun UPS se encuentra en mal estado		10 Minutos	
4	Switches	- Revisión de ruidos, alarmas audibles - Revisar leds de alerta - Encender ventiladores de backup	Recorrido piso por piso para descubrir posibles fallos en los equipos de red		10 minutos	
5	Cintas de Backup	Cambio de cintas de manera periodica	Obtener el nuevo type correspondiente a ese dia y realizar el format en caso de ser necesario o el cambio		5 minutos	

Figura 9. Libro de Actividades x Equipos Físicos

			Gravedad (Impacto)				
			Muy bajo	Bajo	Medio	Alto	Muy Alto
			1	2	3	4	5
Probabilidad	Muy baja	1	2	3	4	5	6
	Baja	2	3	4	5	6	7
	Media	3	4	5	6	7	8
	Alta	4	5	6	7	8	9
	Muy Alta	5	6	7	8	9	10

Verde 2-4 Bajo	Riesgo bajo, no requiere medidas, se debe hacer un control periódic
Amarillo 5-6 Medio	Se debería buscar implementar medidas preventivas, sino buscar mantener el riesgo controlado
Naranja 7-8 Importante	Es importante establecer medidas preventivas, buscar reducir el ries
Rojo 9-10 Alto	Muy grabe, establecer medias preventivas inmediatas, mantener la variables del riesgo controladas

Figura 10. Libro de empresas

Tipo	Riesgos	Probabilidad	Gravedad	Riesgo	Impacto	Acciones	Comentarios
HW	Inundación	1	5	6	Medio	Elevar la altura de los servidores y racks	Aumentó con la congelación del aire A
HW	Sobre tensión	2	2	4	Bajo		
HW	Corte eléctrico	2	2	4	Bajo		
HW	Sabotaje físico	3	5	8	Importante	Monitoreo de cámaras y auditoría de accesos	
HW	Incendio	1	5	6	Medio	Extintores	
HW	Falla de generador	1	3	4	Bajo		
HW	Falla de UPS	1	5	6	Medio	Contar con doble sistema	
HW	Corte de comunicaciones	1	5	6	Medio	Mantener una alternativa en caso de que un switch falle	
HW	Fallo o daño de un disco	2	3	5	Medio		
HW	Sin acceso al cuarto	2	4	6	Medio	Se supone que si se requiere entrar es necesario	
HW	Terremoto	1	5	6	Medio		
HW	Fallo General	1	5	6	Medio	Documentar y crear un plan para el fallo encontrado	
Servicios	Error en actualización	2	2	4	Bajo		
Servicios	Falla del Sistema Operativo	2	2	4	Bajo		
Servicios	Error en autenticación	3	1	4	Bajo		
Servicios	Error con servicios externos	4	2	6	Medio	Tener una snapshot del servidor antes de realizar cambios	
Servicios	Acceso no autorizado	2	5	7	Importante	Auditar cada tres meses los usuarios con acceso a los sistemas	
Servicios	Información no confiable	1	4	5	Medio		
Servicios	Corrupción de la Data	1	5	6	Medio	Tomar uno de los respaldos que generan diariamente los servidores de base de datos	
Servicios	Daño en el código ejecutable	3	5	8	Importante	Tener un clon del servidor cuando realizen cambios importantes en las aplicaciones	
Servicios	Daño por manipulacion del SO	1	2	3	Bajo		
Servicios	Error en DNS	3	3	6	Medio	En caso de falla del servidor o un apagado del mismo tratar de mover la maquina virtual a otro host	
Servicios	No conce el uso adecuado	3	3	6	Medio	Por la rotacion constante del personal es posible que no todos tengan el conocimiento adecuado de los sistemas	
Servicios	Dependencias obsoletas	2	2	4	Bajo		
MV	Borrado accidental	1	5	6	Medio	Para evitar este borrado accidental se utilizan distintos sistemas de respaldo	
MV	Falta de recursos	3	2	5	Medio		
MV	Acceso no autorizado	1	5	6	Medio	Cambio constante de las contraseñas	
MV	Mala configuración	2	3	5	Medio		
BD	Corrupción de data	1	4	5	Medio		
BD	Indisponibilidad	2	5	7	Importante	Se prevee implementar un sistema para almacenar solo las bases de datos	
BD	Lentitud (No responde)	2	3	5	Medio		
BD	Error en scripts (Actualización)	1	1	2	Bajo		
BD	Backup Incorrecto o Nulo	1	5	6	Medio		
BD	Restaurar y no hay backup	1	5	6	Medio		

Figura 11. Libro de empresas

Anexo 2 – Disaster Recovery Plan

Av. Orellana 1172 y Av. Amazonas

Número del Hotel: +593 22972000

Fax: +593 22972050

Gerente de IT: +593 999586026

Asistente de IT: +593 999585912

Ultima actualización: Julio 15, 2024

Contenido

Control de versiones

Versión	Fecha	Descripción	Autor
1.0	Julio 10 2024	Borrador inicial	Esteban Moyolema
1.1	Julio 28 2024	Primer cambio en el proceso de recuperación	Esteban Moyolema

Aprobación de la alta gerencia

	Nombre	Cargo	Firma	Fecha
Modificado por	Esteban Moyolema	Analista de Sistemas		
Aprobado por	Joseph Cina	Gerente General		
Aprobado por	Isabel Delgado	Directora de Habitaciones		
Aprobado por	Miguel Heredia	Director de finanzas		
Aprobado por	Xavier Constante	Director de talento humano		
Aprobado por	Irene Landívar	Directora de ventas		

Resumen Ejecutivo

El propósito de este documento es proveer a las personas o grupos la adecuada documentación simple y concisa sobre la copia de seguridad y restauración de los aspectos fundamentales de la red local en caso de una emergencia o crisis que requiera tales acciones.

Las copias de seguridad son una tarea esencial para la protección y recuperación de la información de la propiedad. Estas copias deben completarse cada noche sin excepción y deben realizarse para cada servidor ubicado en la propiedad. Otras aplicaciones y configuraciones deben ser respaldadas regularmente para que puedan ser fácilmente restauradas si es necesario.

Este documento servirá como guía para garantizar que los sistemas, aplicaciones y datos asociados críticos para el negocio de JW Marriott Quito sean respaldados de manera constante y confiable, y que exista un proceso por el cual estos activos estén protegidos una vez completado el proceso de respaldo.

Además, este plan elabora cómo restaurar los diversos sistemas, aplicaciones y datos asociados en un evento de contingencia; un suceso que afecta adversamente la operabilidad normal de estos activos o la integridad de los datos del hotel causando una pérdida prolongada del servicio o una falla total de la red (es decir, desastre natural, virus, pérdida de conectividad LAN/WAN, etc.).

La planificación de contingencias permite al hotel sufrir la menor cantidad de tiempo de inactividad, y esta documentación será parte del Plan de Continuidad del Negocio del hotel y fácilmente accesible por el equipo, los jefes de departamento y el equipo de Servicios de tecnología de la información.

Este documento incluye referencias a políticas internacionales existentes de Marriott, manuales de seguridad de la información y procedimientos operativos estándar.

Políticas de Marriott Internacional (MIPs – Marriott International Policies)

Los siguientes MIPs están regulados por Marriott Internacional:

- MIP-29 Information Protection & Cyber Security Policy
- MIP-30 Technological Disaster Response Plan
- MIP-29 S07 PCI Data Security Standards Compliance

Estos archivos se los puede encontrar en el siguiente enlace a excepción de "MIP-30 Technological Disaster Response Plan" puesto que este se referencia en el presente documento.

https://mgscloud.marriott.com/common/technology/systems-security

Revisión del proceso para el plan de respuesta ante incidentes tecnológicos

Objetivos:

- Realizar la planificación adecuada y tomar medidas para continuar las operaciones de la infraestructura informática.
- Apoyar a la empresa facilitando y participando en las pruebas de recuperación de aplicaciones que se soliciten.
- Gestionar cualquier proveedor de servicios externo en la implantación, gestión y ejecución de planes estratégicos de continuidad en las actividades de recuperación en caso de catástrofe.

Como parte de la Política MIP-30, es imperativo que el Plan de Recuperación de Catástrofes se revise y actualice anualmente actualizado anualmente. Además, al departamento de tecnologías de la información le interesa asociarse con la dirección de operaciones empresariales y ayudar a identificar las necesidades específicas de recuperación de las aplicaciones de propiedad y ayudar a proporcionar el plan de recuperación más rentable.

Entre los sistemas más importantes para esta propiedad podemos destacar a Opera PMS puesto que este maneja las reservas, asignación de habitaciones, creación de llaves, estado de limpieza, información de huéspedes, etc. Por lo que es de misión crítica para el negocio, de acuerdo con la definición de la Política MIP-30 esto requeriría una disponibilidad continua y ser recuperable en menos de 24 horas. Aunque la mayoría de los sitios tienen un entorno Opera Data Guard, en el caso de esta propiedad esto no aplica por ser una franquicia y no una propiedad administrada por Marriott Internacional, significaría que debemos dar una alternativa fuera del sitio si ambos servidores fallaran y por lo tanto sería apropiado etiquetar Opera PMS como Business Critical ya que todavía es posible sobrevivir varios días con los informes de contingencia apropiados sin que el sistema funcione.

Grado de Criticidad	Tiempo de inactividad permitido
Misión Critica (Mission Critical)	• 1 hora • 8 horas • 24 horas
Operaciones criticas (Business Critical)	• 48 horas • 72 horas
Esenciales para el negocio (Buisness Essential)	• 1 semana (7 días) • 2 semanas (14 días)
Aplazables (Deferrable)	• Más de 2 semanas (15 días o más) si es necesario

Otro requisito de la política del PIM 30 es revisar y validar anualmente el plan de recuperación en caso de catástrofe. Es imprescindible que este plan se actualice con frecuencia como parte del proceso general de gestión de cambios cuando se añadan o retiren nuevos sistemas.

En la mayoría de los casos no es factible realizar una prueba de recuperación de desastres e intentar restablecer todos los sistemas críticos en equipos de repuesto.

Si un sitio utiliza infraestructura virtual, es posible intentar construir un servidor virtual de repuesto y probar el proceso de restauración de la copia de seguridad. Esta prueba también permitirá validar el proceso global de recuperación.

Inventario de activos

Para poder recuperarse de una catástrofe hay que saber de qué equipos se dispone y cuál de estos son críticos. En esta sección se indica qué tipo de hardware (servidores, equipos de copia de seguridad, componentes de red, etc.) y softwares críticos del hotel se encuentran en la propiedad.

Aplicación	**Hostname**	**Modelo de servidor físico**	**Numero de parte**	**Número de serie**	**Fecha de expiración de la garantía**
Opera PMS	UIODTVMOPRSS1	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024
Call Accounting Omnivista 4760	UIODTCA1	HP DL380 Gen7	583966-001	2M2104019D	Abril-2019
File & Print	UIODTVMFP2	HP DL380 Gen7	583966-001	2M2104019D	Abril-2019
OXI Server	UIODTVMOXI1	HP DL380 Gen7	583966-001	2M210500UU	Julio-2018
Opera interface	UIODTVMIFC1	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024
Doorlock system	UIODTVMDLS1	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024
OVI Server Guest-tek	-	Dell PowerEdge R210		36383530357	Octubre-2023
VM Host Server	UIODTVMH1	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024
Servidores ejecutándose en el host de VM Ware	UIODTVMDC1	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024
	UIODTVCENTER1	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024
	UIODTVMBE1	HP DL380 Gen8	655227-J21	2M2247000C	Febrero-2024
	UIODTVMAPPS	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024
	UIODTVMERP1	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024

	UIODTVMEXACTUS1	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024
	UIODTVMCAPS	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024
	UIODTVMPOS1	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024
	UIODTVMRA	HP DL380 Gen10	P50751-B21	2M2435000K	Febrero-2024

Equipo de respaldos

Tipo de respaldo	**Modelo del hardware**	**Número de Parte**	**Número de serie**	**Carepack**	**Fecha de expiración de la garantía**
Tape Drive	HP StorageWorks Ultrium 3000 – tape drive – LTO 5 Ultrium	693416001	HUJ42710YN	N/A	Septiembre-2019

Equipos de red

Proveedor	**Descripción**	**Modelo de hardware**	**Puertos**	**Número de serie**	**Ubicación**
Cisco	Marriott Router				Centro de datos
Cisco	Switch FX Core	WS-C3560E-12SD-S	12x SE	FDO1316R0C0	Centro de datos
Cisco	Switch	WS-C3560G-48TS-S	48X SFP	FOC1316Z08X	Rack core switch server
Cisco	Switch	WS-C2960G-48TC-L	48X SFP	FOC1314V7PC	Rack Ventas
Cisco	Switch	WS-C3560G-24TS-S	24X SFP	FOC1137Y122	Backup sistemas
Cisco	Switch	WS-C2960G-48TC-L	48X SFP	FOC1319W2JR	Rack Finanzas

Cisco	Switch	WS-C3560G-24TS-S	24X SFP	FOC1314W75N	Rack Finanzas
Cisco	Switch	WS-C2960G-48TCL	48X SFP	FOC1137Y129	Rack S1
Cisco	Switch	WS-C3560G-24TS-S	24X SFP	FOC1314V7K0	Rack S1
Cisco	Switch	WS-C2960G-48TC-L	48X SFP	FOC1137Y12J	Rack Lavandería
Cisco	Switch	WS-C2960G-48TC-L	48X SFP	FOC1314V7NY	Rack Lavandería
Cisco	Switch	WS-C2960G-24TC-L	24X SFP	FOC1319W2JY	Rack Audio y video
Cisco	Switch	WS-C2960G-24TC-L	24X SFP	FOC1314W757	Centro de datos
Cisco	Switch	WS-C3560G-24TS-S	24X SFP	FOC1314W73T	Backup Sistemas

Configuración de respaldos

Esta sección cubrirá a detalle la estructura del respaldo en sistemas críticos, quien es responsable del proceso, y escribir instrucciones sobre cómo funciona el sistema de respaldo actual.

Esta sección tratará en detalle la estructura de la copia de seguridad de nuestros sistemas críticos, quién es responsable de este proceso y las instrucciones escritas para realizar la copia de seguridad. Como referencia general, los términos «copia de seguridad» o «copia de seguridad de los sistemas» se referirán a la realización de una copia digital de los datos críticos de los distintos sistemas de la propiedad y al almacenamiento de esta copia en un medio extraíble (cinta de copia de seguridad de alta capacidad) que se guarda fuera de las instalaciones.

Extraíble (cinta de copia de seguridad de alta capacidad) que se guarda fuera de las instalaciones o in situ en una caja fuerte ignífuga segura con fines de seguridad y recuperación en caso de desastre a prueba de incendios por motivos de seguridad y recuperación en caso de catástrofe.

Servidores de medios

Servidor de Windows

Copias de seguridad para todos los servidores basados en Windows se ejecutan utilizando el sistema Veritas Backup Exec 2022: Rev. 1193 (64 bits) que se ejecuta en UIODTVMBE1 todos los servidores deben tener instalado el Backup Exec Remote Agent.

Los trabajos de copia de seguridad se crean para cada aplicación/servidor mediante este software y se configuran para realizar copias de seguridad de una lista predefinida de datos críticos una lista predefinida de archivos y directorios críticos suministrados por el proveedor para que se ejecuten a horas programadas. La única acción necesaria es cambiar las cintas DAILY en la unidad de cinta.

Log de respaldos

El gestor de TI es responsable de supervisar y verificar todas las copias de seguridad de aplicaciones/servidores basados en Windows. Cualquier problema se resolverá de inmediato y las copias de seguridad fallidas se volverán a ejecutar siempre que sea posible.

Modificación del plan de copias de seguridad

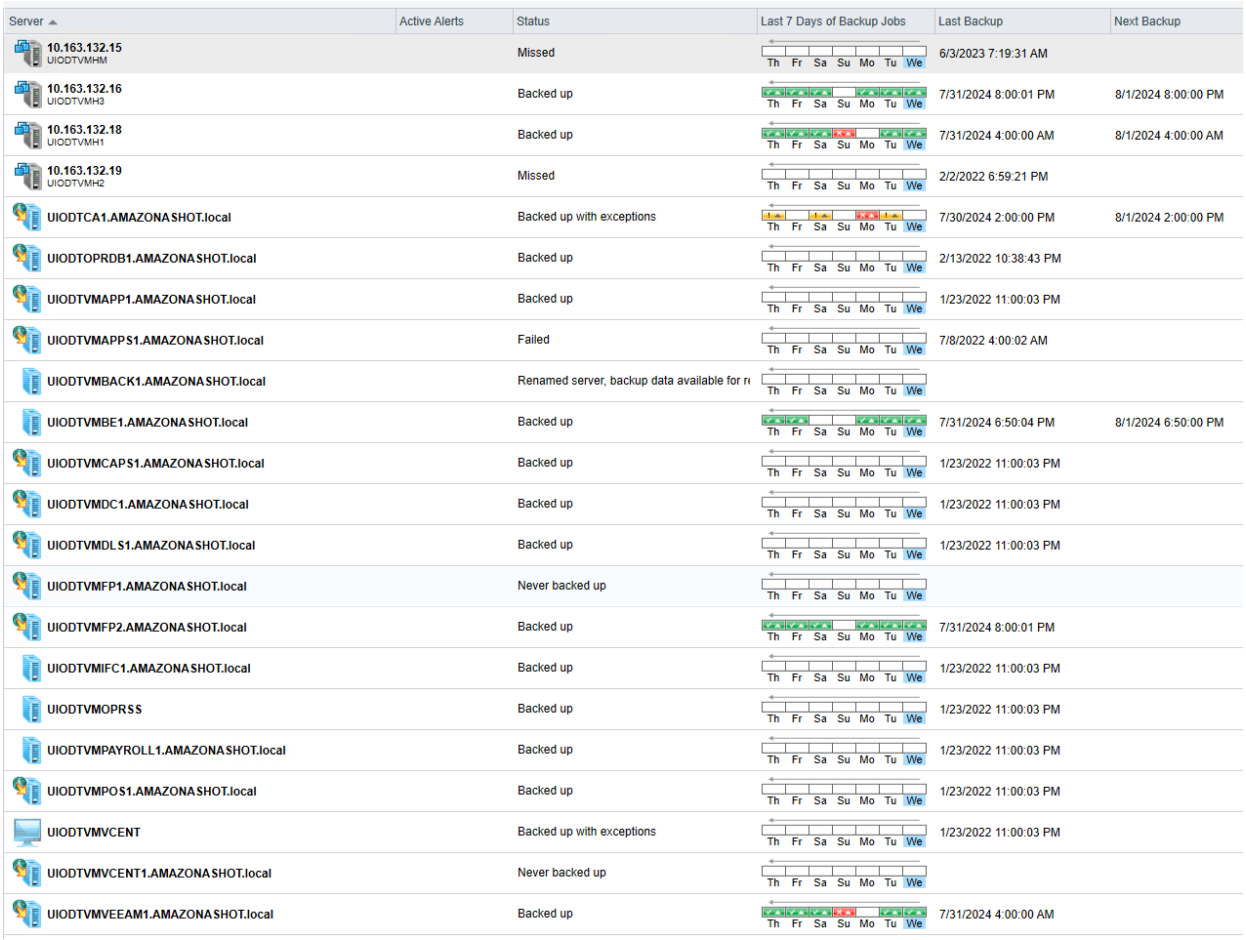
Es responsabilidad del director de tecnologías de la información realizar los cambios necesarios en el Plan de copias de seguridad del hotel. Todos los cambios deben ajustarse a las políticas internacionales de Marriott (MIP) y a los procedimientos operativos estándar establecidos. Como mínimo, el plan de copias de seguridad se revisará como parte del requisito de certificación anual MIP-30, pero deberá actualizarse cada vez que se produzca un cambio de hardware o software que provoque un cambio en un proceso descrito en este documento.

Instrucciones escritas para realizar la copia de seguridad

1.- Ingresar a UIODTVMBE1 (10.163.132.179) con privilegios de administrador

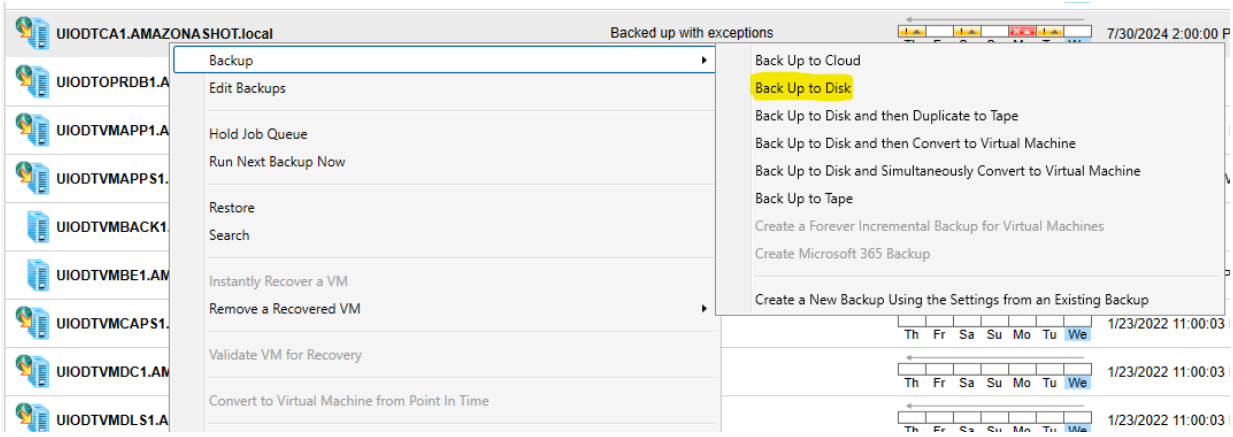
2.- Ejecuta Veritas Backup Exec desde el escritorio de Windows o desde el panel de aplicaciones

3.- Da un clic en “Backup and Restore” esta opción se encuentra en la cinta superior de la aplicación, a continuación, podrás ver los servidores físicos y los servidores virtuales.



Server	Active Alerts	Status	Last 7 Days of Backup Jobs	Last Backup	Next Backup
10.163.132.15 UIODTVMHM		Missed	Th Fr Sa Su Mo Tu We	6/3/2023 7:19:31 AM	
10.163.132.16 UIODTVMH3		Backed up	Th Fr Sa Su Mo Tu We	7/31/2024 8:00:01 PM	8/1/2024 8:00:00 PM
10.163.132.18 UIODTVMH1		Backed up	Th Fr Sa Su Mo Tu We	7/31/2024 4:00:00 AM	8/1/2024 4:00:00 AM
10.163.132.19 UIODTVMH2		Missed	Th Fr Sa Su Mo Tu We	2/2/2022 6:59:21 PM	
UIODTCA1.AMAZONASHOT.local		Backed up with exceptions	Th Fr Sa Su Mo Tu We	7/30/2024 2:00:00 PM	8/1/2024 2:00:00 PM
UIODTOPRDB1.AMAZONASHOT.local		Backed up	Th Fr Sa Su Mo Tu We	2/13/2022 10:38:43 PM	
UIODTVMAPP1.AMAZONASHOT.local		Backed up	Th Fr Sa Su Mo Tu We	1/23/2022 11:00:03 PM	
UIODTVMAPPS1.AMAZONASHOT.local		Failed	Th Fr Sa Su Mo Tu We	7/8/2022 4:00:02 AM	
UIODTVMBACK1.AMAZONASHOT.local		Renamed server, backup data available for r	Th Fr Sa Su Mo Tu We		
UIODTVMBE1.AMAZONASHOT.local		Backed up	Th Fr Sa Su Mo Tu We	7/31/2024 6:50:04 PM	8/1/2024 6:50:00 PM
UIODTVMCAPS1.AMAZONASHOT.local		Backed up	Th Fr Sa Su Mo Tu We	1/23/2022 11:00:03 PM	
UIODTVMDC1.AMAZONASHOT.local		Backed up	Th Fr Sa Su Mo Tu We	1/23/2022 11:00:03 PM	
UIODTVMDLS1.AMAZONASHOT.local		Backed up	Th Fr Sa Su Mo Tu We	1/23/2022 11:00:03 PM	
UIODTVMFP1.AMAZONASHOT.local		Never backed up	Th Fr Sa Su Mo Tu We		
UIODTVMFP2.AMAZONASHOT.local		Backed up	Th Fr Sa Su Mo Tu We	7/31/2024 8:00:01 PM	
UIODTVMIFC1.AMAZONASHOT.local		Backed up	Th Fr Sa Su Mo Tu We	1/23/2022 11:00:03 PM	
UIODTVMOPRSS		Backed up	Th Fr Sa Su Mo Tu We	1/23/2022 11:00:03 PM	
UIODTVMPAYROLL1.AMAZONASHOT.local		Backed up	Th Fr Sa Su Mo Tu We	1/23/2022 11:00:03 PM	
UIODTVMPOS1.AMAZONASHOT.local		Backed up	Th Fr Sa Su Mo Tu We	1/23/2022 11:00:03 PM	
UIODTVMVCENT		Backed up with exceptions	Th Fr Sa Su Mo Tu We	1/23/2022 11:00:03 PM	
UIODTVMVCENT1.AMAZONASHOT.local		Never backed up	Th Fr Sa Su Mo Tu We		
UIODTVMVEEAM1.AMAZONASHOT.local		Backed up	Th Fr Sa Su Mo Tu We	7/31/2024 4:00:00 AM	

4.- Al dar un clic derecho sobre un servidor o máquina virtual podremos realizar la copia de seguridad.



Medios de respaldo

Rotación de cintas

El asociado de turno en el departamento de IT es el responsable de realizar la rotación manual de los medios de almacenamientos. Actualmente el hotel utiliza un solo controlador de cintas y mantiene una rotación de 25 cintas.

- Siempre se deberá mantener un respaldo con la información del fin de semana en un casillero de seguridad en el Banco del Austro casillero #C-2 estos respaldos corresponden a un full Backup realizado por el sistema.
- Los respaldos que correspondan a días entre semana se mantendrán en la caja de seguridad a prueba de fuego que se encuentra en la oficina de sistemas, estos respaldos serán full backups e incremental backups.
- Por último, se mantendrá una copia de todos los servidores al finalizar el año y esta cinta se almacenará en la caja de seguridad del Front Desk casillero #114.

- Las cintas deberán rotar todos los días.

El asociado de área de TI asumirá la responsabilidad de garantizar que los nuevos soportes o equipos se pongan en servicio. Todas las cintas de los servidores se sustituirán anualmente y deberán solicitarse a través del proveedor local de HP. Puede utilizar el siguiente número de parte para realizar la compra de las cintas.

- C7975A 3TB Ultrum LTO 5
- C7978A Cartucho de limpieza universal HP

Sistema de etiquetado de medios

El asociado de IT es responsable de etiquetar los medios de respaldos para JW Marriott Quito. Se adherirá una etiqueta en el lomo posterior de cada cinta y en cada etiqueta se imprimirá la siguiente información.

LTO-01-001

Marriott Confidental and Proprietary Information

Medio de almacenamiento

La calidad de los datos archivados en las cintas de seguridad depende de la calidad de las propias cintas. Los fabricantes de cintas exigen que las cintas se almacenen en un entorno fresco y seco. Dado que es imposible restaurar un sistema de cintas deñadas o corruptas, se deben seguir los siguientes procedimientos de almacenamiento:

Almacenamiento local

- Todas las cintas de respaldo se almacenan en el casillero de seguridad #114 en la Recepción y en el casillero de seguridad C-02 en el Banco del Austro.
- La caja fuerte está cerrada en todo momento
- Sólo otro software puede compartir espacio en la caja fuerte: ningún otro tipo de artículo se almacena allí
- La caja fuerte se encuentra en una zona segura lo suficientemente alejada de la sala de ordenadores para evitar una pérdida común
- El acceso a la caja fuerte de los respaldos está restringido a excepción: asociados de IT, GM, DOF, y sólo en casos de emergencia departamento de seguridad.

Almacenamiento externo

En el JW Marriott Quito, la cinta utilizada durante el fin de semana se almacena en la taquilla de seguridad C-02 del Banco del Austro.

Se lleva un registro de las cintas almacenadas fuera de las instalaciones, que se encuentra en una carpeta en la oficina de TI. Las hojas de registro completas se transfieren a la oficina de IR Field Associates y se conservan durante un año.

Inventario de medios

Todos los soportes de cinta que contengan información de tarjetas de crédito deben inventariarse al menos cada cuatro meses para garantizar que no faltan cintas. Debe mantenerse un registro que documente los resultados del inventario. En el JW Marriott Quito, el registro se mantiene en la oficina de TI en un folio y todas las cintas se inventariaron semanalmente. Las hojas de registro completas se transfieren a la oficina de IR Field Associates y se conservan durante un año.

Días de respaldos

Se definen tres días entre semana para realizar backups completos y dos días para realizar respaldos incrementales. El fin de semana se asigna un día para un Full Backup y para un incremental como se muestra en la tabla a continuación.

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
Full Backup	SI	NO	SI	NO	SI	NO	SI
Incremental Backup	NO	SI	NO	SI	NO	SI	NO

Destrucción de medios

El asociado de campo de TI es responsable de destruir los soportes de cinta cuando ya no sean necesarios por motivos empresariales o legales, o cuando las nuevas cintas de copia de seguridad hayan completado con éxito una rotación completa. Las cintas antiguas se destruyen de forma segura siguiendo el procedimiento de destrucción segura. La eliminación se lleva a cabo con la ayuda del departamento de Loss Prevention y se guarda un registro en la oficina de IR Field Associates.

Fecha: 24 de julio del 2024

ACTA DE DESTRUCCION DE CINTAS DE BACKUP

Por medio del presente se detalla lo siguiente:

#	Ítem	Nombre	# Serie	Modelo	Fecha de Destrucción	Firmas		
						Sistems	Dir. Loss Prevention	Dir. Finanzas
1	Backup Tape	LTO-001-014	G10601001813	HP C7971A 200GB	24-07-2024			
2	Backup Tape	LTO-001-023	L02904001614	HP C7973A 800GB	24-07-2024			

Este procedimiento se cumple bajo las instrucciones establecidas en el documento de manejo de equipos de cómputo en desuso.

Nota: Adjunto a este documento se encuentran fotos del procedimiento que se realizó para garantizar la destrucción de lo detallado anteriormente.

Guía de recuperación

Esta sección describirá cómo restaurar las aplicaciones clave en la propiedad. Cuando se produce un desastre, es imperativo que se notifique a la dirección continental de iT para que preste apoyo adicional en momentos de emergencia.

Además, es necesario definir el orden de los sistemas críticos a restaurar para agilizar el proceso de recuperación de la manera más eficiente.

Dependiendo de la infraestructura de que se disponga, deberán cumplirse ciertos requisitos previos, por ejemplo, reconstruir el servidor de soportes de copia de seguridad para poder restaurar a partir de una cinta. Si este servidor es virtual, el primer servidor físico que habrá que reconstruir será un host VMware ESX.

En la siguiente tabla se indica el orden de restauración en función de la dependencia de la infraestructura de la propiedad y de la actividad crítica de la aplicación.

Orden	Tipo de sistema	Propósito	Prioridad	Tiempo de recuperación
1	ESX Host – UIODTVMH1	Servidor principal donde se almacenan todos los servidores virtuales.	High	8 horas
2	Backup/Media Server	Host de respaldos	High	8 horas
3	Opera PMS	Property Managment System	High	12 horas
4	Micros Symphony	Servidor de punto de venta	High	24 horas
5	Saflok	Sistema de bloqueo de puertas	High	24 horas
6	PMS Interfaces	OXI, POS, WWW, PBX, Saflok Interfaces, TV Samsung	Medium	24 horas
7	UIODTVMERP1	Sistema de inventarios, contabilidad, recursos humanos y timbre.	Medium	24 horas

Opera PMS

Resumen

Opera PMS es el sistema de gestión de la propiedad PMS y la aplicación más crítica de los hoteles alojados en las instalaciones. La propiedad lo ha definido como "Buisness Critical", lo que significa que tiene que ser recuperado dentro de 12 horas.

Support Vendor Contacts

Nombre, Teléfono, Mail, Dirección

Oracle Support

+541152997777

+5716118570

Hotel code number: 59300005

Support Identifier: 20560883

Orscle Acount Manager: Ursula Ugaz (Ursula.ugaz@oracle.com)

Hardware Vendor Contacts

Nombre, Teléfono, Mail, Dirección

HP Enterprise

1800255528 then 8448458165

Nota: Para verificar que el servidor tiene un carepack activo. Por lo general, esto tendría que ser la renovación cada año para carepack 24x7x4

Hardware Details

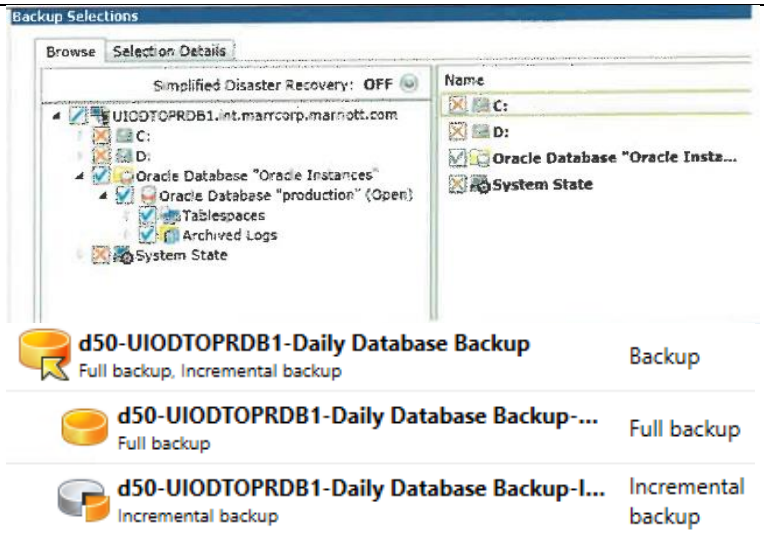
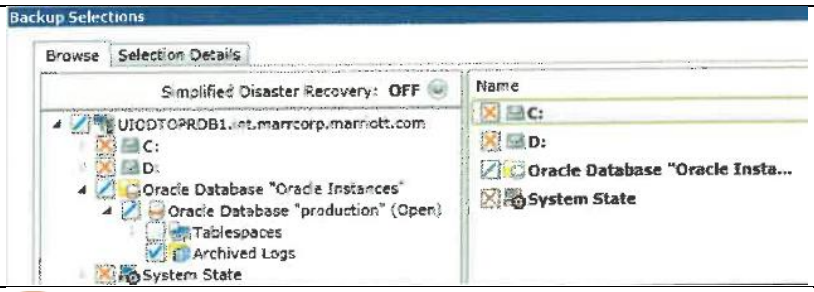
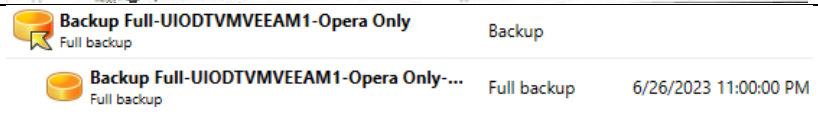
Opera Database Server Details

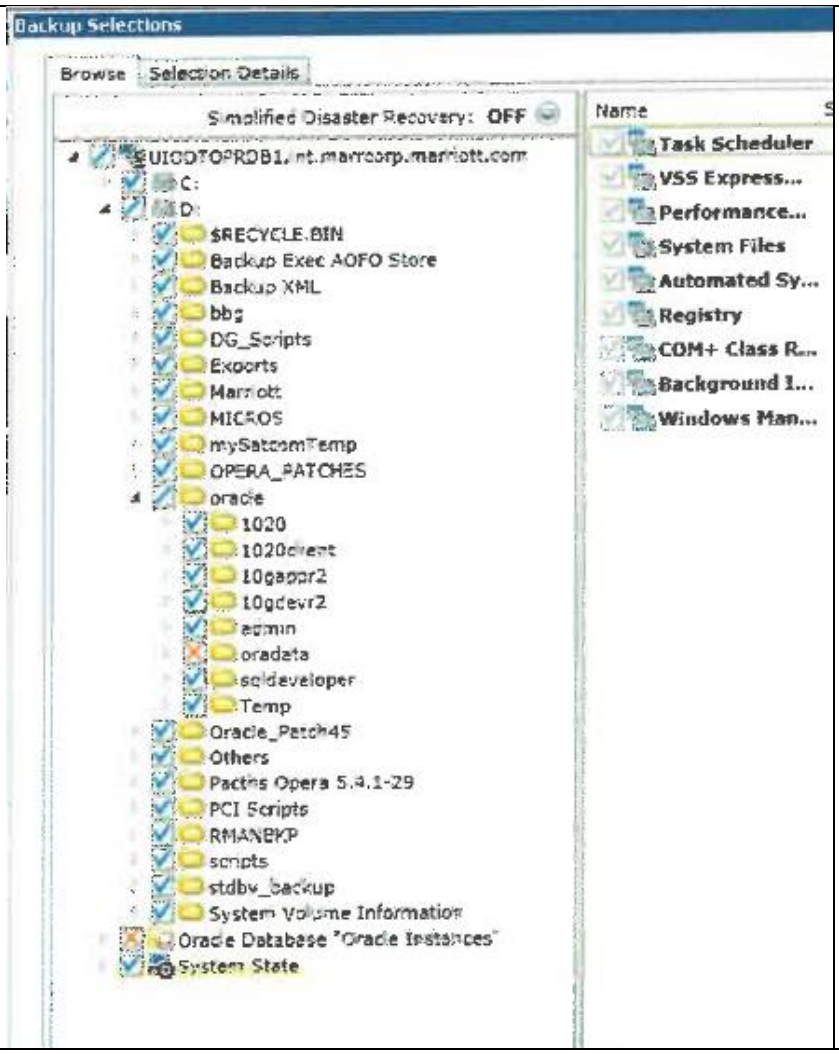
Virtual IP: 10.163.132.2

Hostname	UIODTVMOPRSS
IP Address	10.163.132.2
DNS Details	10.163.132.10 162.130.128.97 162.130.10.9
OS Installed	Windows 2019 R2
iLO License	3K9YN-4GJ99-********-*********-LM9J6
iLO IP Address	10.163.132.185
Hardware Model	DL380 G10

Serial Number	2M2435000K
RAM Installed	64GB
CPU	2CPU (2667 Mhz)
Raid Configuración	Raid 1 (HD 146GB bay 1,2) Raid 1+0 (HD 300 GB bay 3 to bay 8)
Operational Accounts	Svc-uiodt-oprdg
Software Licenses	BE Agent for DB Oracle

Configuración de Respaldos

Nombre del respaldo	Archivos para respaldar	Frecuencia del respaldo	Full / Incremental / Diferential
D50-UIODTOPRDB1 – DAILI=Y DATABASE		Diario 11:00pm	Full Oracle DB
H01 Hourly Backup Archive logs – UIODTPRDB1		Cada 4 horas	Archive logs Oracle DB
D07-Opera Daily File Backup - UIODTPRDB1		Diario 11:00pm	Full

W01 – Weekly OS Backup - UIODTPRDB1		Todos los domingos 3:00 pm	Full

Proceso de recuperación

8. Por error en el servidor ponerse en contacto con el soporte de Oracle para el levantamiento nuevamente del PMS.
9. Póngase en contacto con el proveedor de hardware para agilizar la adquisición de nuevo hardware (incluya el servidor de medios de copia de seguridad si ya no está disponible)
10. Configure el servidor según las especificaciones de hardware indicadas anteriormente.
11. Crear una imagen del servidor mediante el proceso de creación de servidores MDT.
12. Solicite al proveedor de aplicaciones que restaure la copia de seguridad o restaure el servidor desde un Backup.
13. Valide el proceso de restauración

14. Póngase en contacto con MSSC Nivel 2 para obtener los códigos de recuperación de PKI para restaurar todos los certificados PKI según la guía Opera PKI.

Opera Interfaces

Resumen

Opera PMS Interfaces proporciona el sistema de gestión de la propiedad con la información de otros sistemas vinculados, tales como la interfaz de tarjetas de crédito, POS, Key Card System, sistema de gestión de TV. La propiedad lo ha definido como "Business Critical" lo que significa que tiene que ser recuperado en 24 horas.

Support Vendor Contacts

Nombre, Teléfono, Mail, Dirección

Oracle Support

+541152997777

+5716118570

Hotel code number: 59300005

Support Identifier: 20560883

Micros POS support – SATCOM

2559275

PBX – Telalca

2988900

Guest-tek

1800000298

Saflok – DLS

Ceta del Ecuador

2265825

2436202

Hardware Vendor Contacts

Nombre, Teléfono, Mail, Dirección

HP Enterprise

1800255528 then 8448458165

Nota: Para verificar que el servidor tiene un carepack activo. Por lo general, esto tendría que ser la renovación cada año para carepack 24x7x4

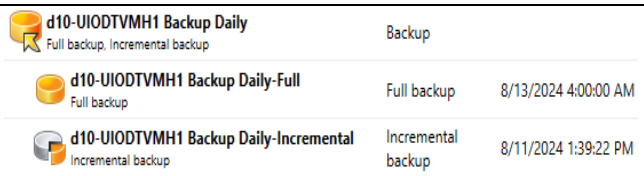
Hardware Details

Opera Database Server Details

Virtual IP: 10.163.132.3

Hostname	UIODTVMIFC1
IP Address	10.163.132.3
DNS Details	10.163.132.10 162.130.128.97 162.130.10.9
OS Installed	Windows 2019 R2
iLO License	3K9YN-4GJ99-********-*********-LM9J6
iLO IP Address	10.163.132.185
Hardware Model	DL380 G10
Serial Number	2M2435000K
RAM Installed	4GB
CPU	E5502
HDD Size	C: 40GB D: 420GB
Raid Configuration	RAID 1

Configuración de Respaldos

Nombre del respaldo	Archivos para respaldar	Frecuencia del respaldo	Full / Incremental / Diferential
D50-UIODTOPRDB1		Diario 4:00Am	Full

Proceso de recuperación

1. Ponerse en contacto con el proveedor de hardware para agilizar la adquisición de nuevo hardware (incluya el servidor de medios de copia de seguridad si ya no está disponible).
2. Configure el servidor según las especificaciones de hardware indicadas anteriormente
3. Crear una imagen del servidor mediante el proceso de creación de servidores MDT.
4. Configure el servidor de acuerdo con la guía de construcción
5. Solicite al proveedor de aplicaciones que restaure la copia de seguridad o restaure el servidor desde un Backup.

6. Realice pruebas de aceptación del usuario para validar la correcta recuperación de la funcionalidad de la aplicación.

Micros Point of Sales

Resumen

Micros Point of Sale es el POS de la propiedad y una de las aplicaciones más críticas del hotel. La propiedad lo ha definido como "Business Critical", lo que significa que debe recuperarse en 24 horas.

Support Vendor Contacts

Nombre, Teléfono, Mail, Dirección

Oracle Support

+541152997777

+5716118570

Hotel code number: 59300005

Support Identifier: 20560883

Contacto con el distribuidor local de Micros SATCOM para analizar y seleccionar la mejor forma de recuperación de las APPS y BBDD de Micros.

Una base de datos Dump se genera cada 6 horas en E:\micros_backup y se puede utilizar para recuperar las operaciones. Módulo Fiscal es necesario para procesar la facturación electrónica. Los servicios y APPs serán proporcionados por SATCOM

Micros POS support – SATCOM

2559275

Hardware Vendor Contacts

Nombre, Teléfono, Mail, Dirección

HP Enterprise

1800255528 then 8448458165

Nota: Para verificar que el servidor tiene un carepack activo. Por lo general, esto tendría que ser la renovación cada año para carepack 24x7x4

Hardware Details

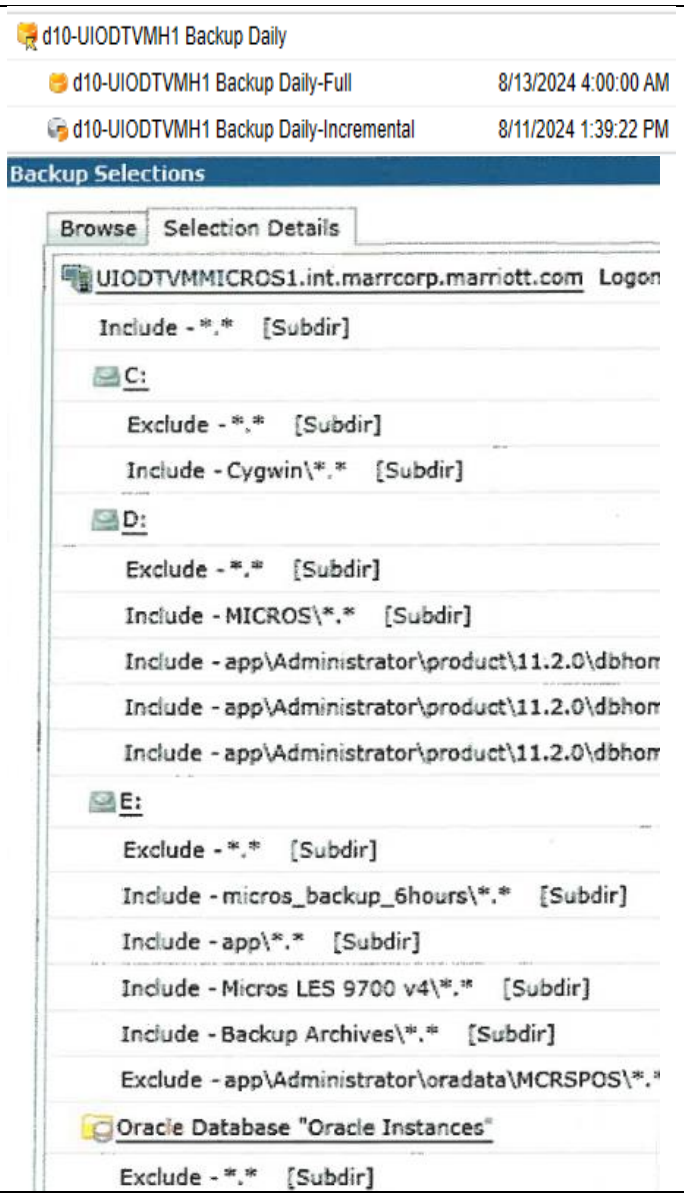
Opera Database Server Details

Virtual IP: 10.163.132.13

Hostname	UIODTVMPOS1
IP Address	10.163.132.13
DNS Details	10.163.132.10 162.130.128.97 162.130.10.9
OS Installed	Windows 2019 R2
iLO License	
iLO IP Address	10.163.132.186
Hardware Model	DL380 G10
Serial Number	2M2435000K
RAM Installed	8GB
CPU	2 virtuales sockets and 2 cores por socket
HDD Size	C: 40GB D: 100GB E: 100GB
Raid Configuration	RAID 5

Configuración de Respaldos

Nombre del respaldo	Archivos para respaldar	Frecuencia del respaldo	Full / Incremental / Diferential

D10-UIODTVMH1 Backup Daily		Diario 4:00am	Full

Proceso de recuperación

1. Ponerse en contacto con el proveedor de hardware para agilizar la adquisición de nuevo hardware (incluya el servidor de medios de copia de seguridad si ya no está disponible).
2. Configure el servidor según las especificaciones de hardware indicadas anteriormente
3. Crear una imagen del servidor mediante el proceso de creación de servidores MDT.
4. Configure el servidor de acuerdo con la guía de construcción
5. Solicite al proveedor de aplicaciones que restaure la copia de seguridad o restaure el servidor desde un Backup.

6. Realice pruebas de aceptación del usuario para validar la correcta recuperación de la funcionalidad de la aplicación.

VMware ESXi

Resumen

VMware proporciona a la propiedad infraestructura virtual para alojar máquinas virtuales como servidores. Dependiendo de la ubicación de la propiedad, es posible que este servidor tenga que restaurarse primero para proporcionar tiempos de inicio de sesión suficientes a la red, de lo contrario se producirá la autenticación externa a través de iLO o RDP. La propiedad lo ha definido como "Buisness Critical", lo que significa que debe recuperarse en un plazo de 8 horas.

Support Vendor Contacts

Marriott Systems Administration, Póngase en contacto con Global Network Operations (GNOC) +1 240-632-6000, opción 9, opción 3, y pida ayuda al SA que esté de guardia.

Hardware Vendor Contacts

Nombre, Teléfono, Mail, Dirección

HP Enterprise

1800255528 then 8448458165

Nota: Para verificar que el servidor tiene un carepack activo. Por lo general, esto tendría que ser la renovación cada año para carepack 24x7x4

Hardware Details

Opera Database Server Details

Virtual IP: 10.163.132.11

Hostname	UIODTVMDLS1
IP Address	10.163.132.1
DNS Details	10.163.132.10 162.130.128.97 162.130.10.9
OS Installed	Windows 2019
iLO License	
LO IP Address	10.163.132.189
Hardware Model	DL380 G10
Serial Number	2M2435000K
RAM Installed	4GB

CPU	Xeon Processor E5603
HDD Size	C: 40GB D: 454GB
Raid Configuration	RAID 1+0

Proceso de recuperación

1. Contratar al proveedor de hardware para agilizar el nuevo hardware
2. Ponerse en contacto con la SA para informarle de la necesidad de recuperación
3. Configure el servidor de acuerdo con la guía de construcción
4. Proceda a crear la máquina virtual invitada de acuerdo con la guía de recuperación correspondiente.
5. Una vez configurados el host y los invitados, entréguelos a SA para el acabado final.

SAFLOK

Resumen

El sistema de tarjetas llave es el sistema de llaves de la propiedad y una de las aplicaciones críticas del hotel. La propiedad lo ha definido como "Business Critical", lo que significa que debe recuperarse en 24 horas.

Support Vendor Contacts

Nombre, Teléfono, Mail, Dirección

Ceta Ecuador

2265825 / 436202

Doormakaba

http://support.saflok.com

0015143409025

Hardware Vendor Contacts

Nombre, Teléfono, Mail, Dirección

HP Enterprise

1800255528 then 8448458165

Nota: Para verificar que el servidor tiene un carepack activo. Por lo general, esto tendría que ser la renovación cada año para carepack 24x7x4

Hardware Details

Opera Database Server Details

Virtual IP: 10.163.132.15

Hostname	UIODTVMH1
IP Address	10.163.132.15
DNS Details	10.163.132.10 162.130.128.97 162.130.10.9
OS Installed	ESXi
iLO License	
LO IP Address	10.163.132.218
Hardware Model	DL380 G10
Serial Number	2M2435000K
RAM Installed	80GB
CPU	2x Xenon E5-2640V2 2.00 GHz

HDD Size	146Gb
Raid Configuration	RAID 1+0 146 GB bay 7,8 RAID 5 600 GB bay 1 a 6

Configuración de Respaldos

Nombre del respaldo	Archivos para respaldar	Frecuencia del respaldo	Full / Incremental / Diferential
D70-Daily UIODTCA1		Diario 2:00pm	Full

Proceso de recuperación

1. Contratar al proveedor de hardware para agilizar el nuevo hardware
2. Configurar el servidor según las especificaciones de hardware indicadas anteriormente
3. Cree una imagen del servidor mediante el proceso de creación de servidores MDT.
4. Solicite al proveedor de aplicaciones que restaure la copia de seguridad o restaure el servidor desde un Backup.
5. Realice pruebas de aceptación del usuario para validar la correcta recuperación de la funcionalidad de la aplicación.

Listado de proveedores

Nombre del proveedor	Sistema	Nombre de contacto	Teléfono	Mail	Dirección
Oracle	Opera	Ursula Ugaz	+562 26665098	Ursula.ugaz@oracle.com	Av. Vitacura 2939 Piso 14 Santiago de Chile
SATCOM	Symphony	Jphn Hervas	2559275 / 2559276	helpdesk@satcomec.com	Av. Colony Av 9 de Octubre Quito
Telalca	PBX		22988923	Joseluis.mosquera@telalca.com	Calle San Francisco N42-219 y Mariano
Doormakaba	Saflok		+1 (305) 7818008	David.rey@dormakaba.com	11483 NW 79 Lane
Zeus	Zeus	Danilo Reyes		Danilo.reyes@siesa.com	

Anexo 3 - Encuestas

FOOD AND BEVERAGE

Encuesta #1

1.- ¿Puede describir algún programa de formación o concienciación sobre ciberseguridad en el que haya participado en el hotel?

El año pasado asistí a una sesión de formación básica sobre ciberseguridad centrada en las estafas de phishing y la protección de contraseñas.

2.- ¿Alguna vez ha experimentado o presenciado un incidente de ciberseguridad (por ejemplo, violación de datos, ataque de malware) en el desempeño de sus funciones? En caso afirmativo, ¿puede describir lo sucedido?

Una vez fui testigo de una alerta de malware en un ordenador en la zona de la cocina. Se avisó inmediatamente a TI, que se encargó de la situación.

3.- ¿Cómo afectó el incidente de ciberseguridad a sus operaciones diarias y al funcionamiento general del hotel?

El incidente causó un pequeño retraso en las operaciones mientras se aislaba y escaneaba el computador afectado. Sin embargo, los pedidos de comida se siguieron gestionando a través de otros sistemas.

4.- ¿Cómo respondió el hotel al incidente de ciberseguridad? ¿Qué medidas inmediatas se tomaron?

El departamento de TI del hotel respondió rápidamente aislando el dispositivo y realizando una comprobación completa del sistema. También nos insistieron en la necesidad de informar inmediatamente de cualquier actividad sospechosa.

5.- ¿Cómo se comunicó la información durante y después del incidente? ¿Existía un plan de comunicación claro?

La comunicación se llevó a cabo mediante correos electrónicos y reuniones informativas con los supervisores. El departamento de TI envió instrucciones sobre los pasos a seguir y nos aseguró que la situación estaba bajo control.

6.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para su departamento y para el hotel en general?

Percibo que los mayores riesgos de ciberseguridad en nuestro departamento son el acceso no autorizado a nuestros sistemas de punto de venta.

7.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para tu departamento y para el hotel en general?

Creo que los mayores riesgos de ciberseguridad en nuestro departamento son el riesgo de ataques de phishing en dispositivos compartidos.

8.- ¿Qué medidas preventivas se aplican actualmente para protegerse contra las amenazas de ciberseguridad? ¿Hay algún aspecto que considere necesario mejorar?

Tenemos políticas estrictas de contraseñas y el departamento de TI actualiza regularmente los sistemas. Sin embargo, creo que podríamos beneficiarnos de sesiones de formación más frecuentes para mantener a todo el mundo al tanto de las nuevas amenazas.

9.- ¿Está familiarizado con las políticas del hotel y la normativa externa en materia de ciberseguridad? ¿Cómo influyen en sus operaciones diarias?

Soy consciente que existen políticas de ciberseguridad del hotel, especialmente en lo que respecta al manejo de datos y la información de los huéspedes.

10.- ¿Qué sugerencias tiene para mejorar la postura de ciberseguridad del hotel y las estrategias de respuesta?

Nuestro departamento está bastante preparado para las amenazas de ciberseguridad comunes por las charlas que hemos recibido, pero siento que en este momento nuestra mayor debilidad es el personal nuevo.

Encuesta #2

1.- ¿Puede describir algún programa de formación o concienciación sobre ciberseguridad en el que haya participado en el hotel?

He participado en cursos de concienciación sobre ciberseguridad centrados en el reconocimiento de correos electrónicos de phishing.

2.- ¿Alguna vez ha experimentado o presenciado un incidente de ciberseguridad (por ejemplo, violación de datos, ataque de malware) en el desempeño de sus funciones? En caso afirmativo, ¿puede describir lo sucedido?

Una vez tuvimos un problema en el que varios miembros del personal recibieron un correo electrónico sospechoso. Se informó al departamento de TI, que confirmó que se trataba de un intento de phishing. Afortunadamente, nadie hizo clic en el enlace.

3.- ¿Cómo afectó el incidente de ciberseguridad a sus operaciones diarias y al funcionamiento general del hotel?

No tuvo mucho impacto en nuestras operaciones diarias, pero sirvió como llamada de atención para estar más atentos a la seguridad del correo electrónico.

4.- ¿Cómo respondió el hotel al incidente de ciberseguridad? ¿Qué medidas inmediatas se tomaron?

El hotel respondió bloqueando inmediatamente al remitente y enviando una advertencia a todo el hotel para que tuviera cuidado con correos similares.

5.- ¿Cómo se comunicó la información durante y después del incidente? ¿Existía un plan de comunicación claro?

El incidente se comunicó mediante una nota interna en la reunión de novedades y la comunicación directa de los jefes de departamento.

6.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para su departamento y para el hotel en general?

El mayor riesgo es la posible vulnerabilidad de nuestros sistemas de procesamiento de pagos.

7.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para tu departamento y para el hotel en general?

El mayor riesgo es a una violación de los datos de las tarjetas de crédito de los huéspedes.

8.- ¿Qué medidas preventivas se aplican actualmente para protegerse contra las amenazas de ciberseguridad? ¿Hay algún aspecto que considere necesario mejorar?

Tenemos programas antivirus, cortafuegos y sistemas de punto de venta seguros, pero creo que también deberíamos realizar auditorías más regulares de los sistemas para asegurarnos de que todo está al día.

9.- ¿Está familiarizado con las políticas del hotel y la normativa externa en materia de ciberseguridad? ¿Cómo influyen en sus operaciones diarias?

Estoy algo familiarizado con las políticas del hotel, sobre todo las que tienen que ver con la protección de datos de los huéspedes. Estas políticas son importantes y se siguen al pie de la letra en nuestras operaciones diarias. Sería útil disponer de un proceso más rápido y ágil para informar y responder a las amenazas de ciberseguridad

10.- ¿Qué sugerencias tiene para mejorar la postura de ciberseguridad del hotel y las estrategias de respuesta?

Creo que estamos razonablemente preparados, pero la mejora continua de nuestros procesos y las actualizaciones periódicas sobre posibles amenazas reforzarían nuestra defensa.

Encuesta #3

1.- ¿Puede describir algún programa de formación o concienciación sobre ciberseguridad en el que haya participado en el hotel?

He asistido a un par de sesiones de formación en ciberseguridad, entre ellas una centrada en el manejo seguro de la información de pago y otra en el reconocimiento de las tácticas de ingeniería social.

2.- ¿Alguna vez ha experimentado o presenciado un incidente de ciberseguridad (por ejemplo, violación de datos, ataque de malware) en el desempeño de sus funciones? En caso afirmativo, ¿puede describir lo sucedido?

Personalmente no he sufrido ningún incidente de ciberseguridad, pero he oído hablar de casos en los que otros hoteles se enfrentaron a ataques de ransomware, lo que siempre es preocupante

3.- ¿Cómo afectó el incidente de ciberseguridad a sus operaciones diarias y al funcionamiento general del hotel?

Aunque no nos hemos visto directamente afectados, imagino que un incidente de este tipo perturbaría el procesamiento de los pagos y podría erosionar la confianza de los huéspedes.

4.- ¿Cómo respondió el hotel al incidente de ciberseguridad? ¿Qué medidas inmediatas se tomaron?

En una situación hipotética, creo que el hotel daría prioridad a aislar los sistemas afectados e informar a los huéspedes sobre cualquier posible compromiso de los datos.

5.- ¿Cómo se comunicó la información durante y después del incidente? ¿Existía un plan de comunicación claro?

Es probable que la comunicación se gestione a través de reuniones de departamento y actualizaciones de TI, asegurándose de que todo el mundo conoce su papel en la respuesta.

6.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para su departamento y para el hotel en general?

Los ataques de phishing y el ransomware son riesgos significativos, especialmente dado que manejamos información de pagos sensible a diario.

7.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para tu departamento y para el hotel en general?

Tenemos actualizaciones regulares de software y pasarelas de pago seguras, pero siempre hay margen para una mejor encriptación y mayor concienciación del personal.

8.- ¿Qué medidas preventivas se aplican actualmente para protegerse contra las amenazas de ciberseguridad? ¿Hay algún aspecto que considere necesario mejorar?

Estoy al tanto de la importancia de cumplir con las normativas Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago, que regulan cómo manejamos la información de pagos.

9.- ¿Está familiarizado con las políticas del hotel y la normativa externa en materia de ciberseguridad? ¿Cómo influyen en sus operaciones diarias?

Más formación basada en escenarios reales podría ayudarnos a responder de manera más efectiva a incidentes reales.

10.- ¿Qué sugerencias tiene para mejorar la postura de ciberseguridad del hotel y las estrategias de respuesta?

Nuestro departamento está preparado para manejar amenazas de ciberseguridad, pero la formación y concienciación continuas son clave para mantener esta preparación.

FINANZAS

Encuesta #1

1.- ¿Puede describir algún programa de formación o concienciación sobre ciberseguridad en el que haya participado en el hotel?

He participado en varias sesiones de formación en ciberseguridad que enfatizan la importancia de proteger los datos financieros.

2.- ¿Alguna vez ha experimentado o presenciado un incidente de ciberseguridad (por ejemplo, violación de datos, ataque de malware) en el desempeño de sus funciones? En caso afirmativo, ¿puede describir lo sucedido?

Hubo un intento de phishing dirigido a nuestro equipo financiero donde un correo electrónico pretendía ser de un proveedor solicitando un pago.

3.- ¿Cómo afectó el incidente de ciberseguridad a sus operaciones diarias y al funcionamiento general del hotel?

El incidente no interrumpió las operaciones, pero destacó la importancia de verificar doblemente la información de los proveedores y ser cautelosos con las comunicaciones por correo electrónico.

4.- ¿Cómo respondió el hotel al incidente de ciberseguridad? ¿Qué medidas inmediatas se tomaron?

El hotel bloqueó inmediatamente el correo electrónico y notificó a todo el equipo de finanzas, recordándonos ser vigilantes y reportar cualquier actividad sospechosa.

5.- ¿Cómo se comunicó la información durante y después del incidente? ¿Existía un plan de comunicación claro?

La comunicación fue clara, a través de correos electrónicos y una breve reunión para asegurarnos de que todos estuvieran al tanto de la situación y los pasos para evitar que sucediera nuevamente.

6.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para su departamento y para el hotel en general?

Los mayores riesgos son los ataques de phishing y el acceso no autorizado a los sistemas financieros.

7.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para tu departamento y para el hotel en general?

Utilizamos autenticación multifactor y auditorías regulares. Sin embargo, se necesitan actualizaciones continuas y vigilancia para evitar las amenazas potenciales.

8.- ¿Qué medidas preventivas se aplican actualmente para protegerse contra las amenazas de ciberseguridad? ¿Hay algún aspecto que considere necesario mejorar?

Cumplimos estrictamente con las normativas financieras, incluyendo aquellas relacionadas con la protección de datos, lo que a veces agrega complejidad a nuestro trabajo.

9.- ¿Está familiarizado con las políticas del hotel y la normativa externa en materia de ciberseguridad? ¿Cómo influyen en sus operaciones diarias?

Implementar un proceso de verificación de proveedores más riguroso y una formación continua sobre la concienciación ante el phishing sería beneficioso.

10.- ¿Qué sugerencias tiene para mejorar la postura de ciberseguridad del hotel y las estrategias de respuesta?

Nuestro departamento está bien preparado para las amenazas de ciberseguridad, pero la educación continua y la mejora de procesos nos ayudarán a mantener una posición sólida.

Encuesta #2

1.- ¿Puede describir algún programa de formación o concienciación sobre ciberseguridad en el que haya participado en el hotel?

Asistí a una sesión de formación sobre ciberseguridad centrada en los riesgos específicos del departamento financiero, incluido el procesamiento seguro de pagos y las técnicas de prevención del fraude.

2.- ¿Alguna vez ha experimentado o presenciado un incidente de ciberseguridad (por ejemplo, violación de datos, ataque de malware) en el desempeño de sus funciones? En caso afirmativo, ¿puede describir lo sucedido?

Hubo un intento de acceso no autorizado a nuestros sistemas financieros, que se identificó rápidamente.

3.- ¿Cómo afectó el incidente de ciberseguridad a sus operaciones diarias y al funcionamiento general del hotel?

El incidente causó preocupación temporal en el equipo, pero debido a la rápida respuesta, no hubo un impacto significativo en nuestras operaciones.

4.- ¿Cómo respondió el hotel al incidente de ciberseguridad? ¿Qué medidas inmediatas se tomaron?

El hotel respondió rápidamente asegurando los sistemas y llevando a cabo una investigación exhaustiva para asegurarse de que no se había puesto en peligro ningún dato.

5.- ¿Cómo se comunicó la información durante y después del incidente? ¿Existía un plan de comunicación claro?

La comunicación se llevó a cabo de forma profesional, con instrucciones claras de TI y la dirección sobre los pasos a seguir.

6.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para su departamento y para el hotel en general?

Los principales riesgos son las filtraciones de datos y las transacciones no autorizadas, que podrían acarrear pérdidas financieras y las consecuencias legales.

7.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para tu departamento y para el hotel en general?

Contamos cortafuegos, sistemas seguros de procesamiento de pagos y auditorías de seguridad periódicas, pero siempre hay margen de mejora en nuestros protocolos de seguridad.

8.- ¿Qué medidas preventivas se aplican actualmente para protegerse contra las amenazas de ciberseguridad? ¿Hay algún aspecto que considere necesario mejorar?

Estoy algo familiarizado con las políticas del hotel, especialmente las relativas a la protección de datos de los huéspedes.

9.- ¿Está familiarizado con las políticas del hotel y la normativa externa en materia de ciberseguridad? ¿Cómo influyen en sus operaciones diarias?

Actualizar periódicamente nuestros protocolos de seguridad y aumentar la formación del personal sobre las últimas amenazas a la ciberseguridad reforzaría nuestra defensa.

10.- ¿Qué sugerencias tiene para mejorar la postura de ciberseguridad del hotel y las estrategias de respuesta?

Nuestro departamento está preparado, pero mantenernos proactivos en la actualización de nuestras medidas de seguridad y formación garantizará que sigamos estando seguros.

Encuesta #3

1.- ¿Puede describir algún programa de formación o concienciación sobre ciberseguridad en el que haya participado en el hotel?

He asistido a la sesión de formación sobre ciberseguridad, centradas en el manejo seguro de la información financiera y la prevención del acceso no autorizado a nuestros sistemas.

2.- ¿Alguna vez ha experimentado o presenciado un incidente de ciberseguridad (por ejemplo, violación de datos, ataque de malware) en el desempeño de sus funciones? En caso afirmativo, ¿puede describir lo sucedido?

No he sufrido ningún incidente directo.

3.- ¿Cómo afectó el incidente de ciberseguridad a sus operaciones diarias y al funcionamiento general del hotel?

Un incidente de ciberseguridad podría retrasar las operaciones financieras, afectar al procesamiento de pagos y provocar la pérdida de confianza de los clientes, lo que tendría graves consecuencias para el hotel.

4.- ¿Cómo respondió el hotel al incidente de ciberseguridad? ¿Qué medidas inmediatas se tomaron?

El hotel probablemente daría prioridad a asegurar los sistemas afectados, investigar la brecha y comunicarse con las partes afectadas para mitigar cualquier daño.

5.- ¿Cómo se comunicó la información durante y después del incidente? ¿Existía un plan de comunicación claro?

La comunicación implicaría esfuerzos rápidos y coordinados entre TI, la dirección y el equipo financiero.

6.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para su departamento y para el hotel en general?

Los mayores riesgos son la suplantación de identidad, el ransomware y la violación de datos, que pueden provocar pérdidas económicas y sanciones normativas.

7.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para tu departamento y para el hotel en general?

Contamos con autenticación multifactor y el cifrado, pero es necesaria una mejora continua para hacer frente a las amenazas emergentes.

8.- ¿Qué medidas preventivas se aplican actualmente para protegerse contra las amenazas de ciberseguridad? ¿Hay algún aspecto que considere necesario mejorar?

Estoy muy familiarizado con la normativa que debemos cumplir, sobre todo la relacionada con la seguridad de los datos financieros.

9.- ¿Está familiarizado con las políticas del hotel y la normativa externa en materia de ciberseguridad? ¿Cómo influyen en sus operaciones diarias?

Actualizar periódicamente nuestros protocolos de seguridad y aumentar la formación del personal sobre las últimas amenazas a la ciberseguridad reforzaría nuestra defensa.

10.- ¿Qué sugerencias tiene para mejorar la postura de ciberseguridad del hotel y las estrategias de respuesta?

Aunque estamos bien preparados, siempre podemos mejorar nuestra formación y nuestros protocolos.

FRONT DESK

Encuesta #1

1.- ¿Puede describir algún programa de formación o concienciación sobre ciberseguridad en el que haya participado en el hotel?

Participé la charla de ciberseguridad centrada en salvaguardar la información de los huéspedes, como garantizar el procesamiento seguro de los pagos.

2.- ¿Alguna vez ha experimentado o presenciado un incidente de ciberseguridad (por ejemplo, violación de datos, ataque de malware) en el desempeño de sus funciones? En caso afirmativo, ¿puede describir lo sucedido?

Personalmente no he sufrido ningún incidente de ciberseguridad, pero soy consciente de que la recepción es un objetivo para los ataques de phishing y de ingeniería social.

3.- ¿Cómo afectó el incidente de ciberseguridad a sus operaciones diarias y al funcionamiento general del hotel?

Si se produjera un incidente, podría comprometer la información de los huéspedes y afectar a la confianza general que éstos tienen en el hotel.

4.- ¿Cómo respondió el hotel al incidente de ciberseguridad? ¿Qué medidas inmediatas se tomaron?

El hotel probablemente se centraría en proteger los sistemas afectados, informar a los clientes de la brecha y trabajar con el departamento de TI para prevenir futuros incidentes.

5.- ¿Cómo se comunicó la información durante y después del incidente? ¿Existía un plan de comunicación claro?

La comunicación sería clave, con instrucciones claras de TI y la dirección sobre cómo proceder.

6.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para su departamento y para el hotel en general?

Los mayores riesgos para la recepción son los ataques de phishing, el acceso no autorizado a la información de los huéspedes.

7.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para tu departamento y para el hotel en general?

Tenemos actualizaciones periódicas y sistemas seguros, pero creo que nos vendría bien más formación para reconocer las tácticas de ingeniería social.

8.- ¿Qué medidas preventivas se aplican actualmente para protegerse contra las amenazas de ciberseguridad? ¿Hay algún aspecto que considere necesario mejorar?

Soy consciente de las políticas que debemos seguir, sobre todo en lo que respecta al tratamiento de los datos de los huéspedes.

9.- ¿Está familiarizado con las políticas del hotel y la normativa externa en materia de ciberseguridad? ¿Cómo influyen en sus operaciones diarias?

Aumentar la frecuencia de la formación en ciberseguridad, nos ayudaría a responder mejor a las amenazas.

10.- ¿Qué sugerencias tiene para mejorar la postura de ciberseguridad del hotel y las estrategias de respuesta?

Nuestro departamento está razonablemente preparado, pero la formación continua y la vigilancia son esenciales para mantener nuestra postura de ciberseguridad.

Encuesta #2

1.- ¿Puede describir algún programa de formación o concienciación sobre ciberseguridad en el que haya participado en el hotel?

He asistido a sesiones de formación sobre la importancia de proteger la información de los huéspedes y reconocer las amenazas más comunes a la ciberseguridad, como el phishing.

2.- ¿Alguna vez ha experimentado o presenciado un incidente de ciberseguridad (por ejemplo, violación de datos, ataque de malware) en el desempeño de sus funciones? En caso afirmativo, ¿puede describir lo sucedido?

No me he encontrado directamente con ningún incidente, pero la recepción recibe a menudo correos electrónicos sospechosos que estamos formados para informar inmediatamente.

3.- ¿Cómo afectó el incidente de ciberseguridad a sus operaciones diarias y al funcionamiento general del hotel?

Un incidente de ciberseguridad podría poner en peligro los datos de los huéspedes, interrumpir los procesos de registro y salida y provocar la pérdida de confianza de los huéspedes.

4.- ¿Cómo respondió el hotel al incidente de ciberseguridad? ¿Qué medidas inmediatas se tomaron?

El hotel daría prioridad a la protección de los datos de los huéspedes, a informar a las partes afectadas y a garantizar que el incidente se contenga y se resuelva rápidamente.

5.- ¿Cómo se comunicó la información durante y después del incidente? ¿Existía un plan de comunicación claro?

La información se transmitirá por correo electrónico, reuniones de personal y comunicación directa de los responsables de TI y la dirección, para garantizar que todos conozcan su papel en la respuesta.

6.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para su departamento y para el hotel en general?

Entre los riesgos más importantes figuran los intentos de suplantación de identidad y el acceso no autorizado a la información de los huéspedes, que podrían tener graves consecuencias si no se abordan adecuadamente.

7.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para tu departamento y para el hotel en general?

Disponemos de sistemas seguros y actualizaciones periódicas, pero la formación continua del personal es crucial para adelantarnos a las posibles amenazas.

8.- ¿Qué medidas preventivas se aplican actualmente para protegerse contra las amenazas de ciberseguridad? ¿Hay algún aspecto que considere necesario mejorar?

Conozco las políticas del hotel en lo que tiene que ver con la protección de datos de los huéspedes.

9.- ¿Está familiarizado con las políticas del hotel y la normativa externa en materia de ciberseguridad? ¿Cómo influyen en sus operaciones diarias?

Implantar una formación en ciberseguridad más frecuente y detallada nos ayudaría a reconocer y responder a las amenazas con mayor eficacia.

10.- ¿Qué sugerencias tiene para mejorar la postura de ciberseguridad del hotel y las estrategias de respuesta?

La recepción está preparada para las amenazas de ciberseguridad solo recomiendo capacitar al personal que ingresa por primera vez al puesto.

Encuesta #3

1.- ¿Puede describir algún programa de formación o concienciación sobre ciberseguridad en el que haya participado en el hotel?

Participé en un programa de concienciación sobre ciberseguridad que hacía hincapié en la importancia de proteger la información de los huéspedes e identificar posibles amenazas, como el phishing.

2.- ¿Alguna vez ha experimentado o presenciado un incidente de ciberseguridad (por ejemplo, violación de datos, ataque de malware) en el desempeño de sus funciones? En caso afirmativo, ¿puede describir lo sucedido?

No me he enfrentado personalmente a ningún incidente, pero sé que la recepción suele ser objetivo de ataques de ingeniería social, lo cual es preocupante.

3.- ¿Cómo afectó el incidente de ciberseguridad a sus operaciones diarias y al funcionamiento general del hotel?

Un incidente en la recepción da lugar a una violación de la información de los huéspedes.

4.- ¿Cómo respondió el hotel al incidente de ciberseguridad? ¿Qué medidas inmediatas se tomaron?

El hotel se comunicó con los huéspedes afectados y trabajar con TI para prevenir futuros incidentes.

5.- ¿Cómo se comunicó la información durante y después del incidente? ¿Existía un plan de comunicación claro?

La comunicación implicaría instrucciones rápidas y claras por parte de los informáticos y la dirección para garantizar que el incidente se gestiona con eficiencia y eficacia.

6.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para su departamento y para el hotel en general?

Los mayores riesgos son los ataques de phishing y de ingeniería social, que podrían dar lugar a un acceso no autorizado como a los datos de los huéspedes.

7.- ¿Cuáles percibe que son los mayores riesgos de ciberseguridad para tu departamento y para el hotel en general?

Supongo que la ingeniería social.

8.- ¿Qué medidas preventivas se aplican actualmente para protegerse contra las amenazas de ciberseguridad? ¿Hay algún aspecto que considere necesario mejorar?

Hacemos uso de un proceso de cero confianzas con las llamadas telefónicas y con los correos. Por el momento pienso que se debe mejorar en que se sociabilice más los daños que puede tener el abrir un correo indebido a los nuevos usuarios por el alto nivel de rotación que tiene la propiedad.

9.- ¿Está familiarizado con las políticas del hotel y la normativa externa en materia de ciberseguridad? ¿Cómo influyen en sus operaciones diarias?

Si, me encuentro familiarizada con el proceso y las políticas que tiene Marriott internacional para el tratamiento de la información.

10.- ¿Qué sugerencias tiene para mejorar la postura de ciberseguridad del hotel y las estrategias de respuesta?

Nuestro departamento está preparado para las amenazas a la ciberseguridad, pero la mejora continua de nuestra formación y concienciación es clave para mantener una defensa sólida.

Amazonashot
Sistemas Anexo 1.xls

Disaster recovery
plan Anexo 2.docx

Encuestas
27-07-2024 Anexo 3.