FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de Carrera titulado:

Diseño de una política de seguridad de la información para los hoteles miembros de la asociación hotelera de Imbabura, basado en la norma ISO/IEC 27002:2013

Realizado por:

Ing. Christian Ricardo Estrada Ordóñez

Director del proyecto:
Ing. Verónica Rodríguez, MBA

Como requisito para la obtención del título de:

MAGISTER EN CIBERSEGURIDAD

QUITO, abril del 2020

DECLARACIÓN JURAMENTADA

Yo, Christian Ricardo Estrada Ordóñez, ecuatoriano, con Cédula de ciudadanía N° 040123651-8, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido presentado anteriormente para ningún grado o calificación profesional, y se basa en las referencias bibliográficas descritas en este documento.

A través de esta declaración, cedo los derechos de propiedad intelectual a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido en la Ley de Propiedad Intelectual, reglamento y normativa institucional vigente.

Christian Ricardo Estrada Ordóñez

040123651-8

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

Verónica Elizabeth Rodríguez Arboleda

Master in Business Administration

LOS PROFESORES INFORMANTES:

LUIS FABIÁN HURTADO VARGAS

CHRISTIAN DAVID PAZMIÑO FLORES

Después de revisar el trabajo presentado lo han calificado como apto para su defensa oral ante el tribunal examinador.

---------- ----------

Ing. Luis F. Hurtado Vargas, MGS Ing. Christian D. Pazmiño Flores, MGS

Quito, 8 de abril de 2020

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

CHRISTIAN RICARDO ESTRADA ORDÓÑEZ

CI: 040123651-8

AGRADECIMIENTO

A la Ing. Verónica Rodríguez., MBA, por la acertada dirección y revisión del presente trabajo.

Al Dr. Diego Riofrío Ph.D., por su tiempo y dedicación a este encargo.

A la Universidad Internacional SEK, por la oportuna creación de este programa y su esfuerzo por llevar a cabo con integridad el mismo, a pesar de las circunstancias.

DEDICATORIA

A mi hijo Isaac Leonardo, por haberme inspirado en la superación personal y profesional, mi esposa Daniela Paulina, quien ha sacrificado mucho para que yo pueda lograr los objetivos de vida establecidos, y a mis padres, Washington Ricardo y María Elena, quienes desde mi nacimiento han sabido guiarme por un camino de sólidos valores, rendimiento académico y desempeño profesional.

RESUMEN

Este trabajo se enfoca en desarrollar una Política de Seguridad para un grupo de hoteles, específicamente ubicados en la provincia de Imbabura - Ecuador, seleccionando controles que se encuentran en el estándar ISO/IEC 27002:2013. Entre los riesgos encontrados, existe el robo de datos, corrupción, pérdida, filtrado y más, que pueden comprometer la seguridad de la información y física de los hoteles, proveedores, clientes y huéspedes. Una vez que el riesgo se evalúa adecuadamente utilizando la metodología MAGERIT de INCIBE, las salvaguardas se determinan con base en dichos controles, luego, se propone una Política de Seguridad para los hoteles miembros, a ser adoptada. Dicha política tiene como objetivo mantener seguros los datos de hoteles, proveedores, clientes y huéspedes, asegurando que se cumplan los requisitos de Confidencialidad, Integridad y Disponibilidad para asegurar la información y la continuidad del negocio.

Palabras clave: seguridad de la información, política de seguridad en hoteles

ABSTRACT

This work focuses on developing a Security Policy for a group of hotels, specifically located in the Imbabura province of Ecuador, selecting controls found in the ISO/IEC 27002:2013 standard. Among the risk found, there is data theft, corruption, loss, breach, and more, which can compromise hotel, provider, client and guest information and physical security. Once the risk is properly assessed using INCIBE's MAGERIT methodology, safeguards are determined based in formerly said controls, then, a Security Policy for member hotels is proposed in order to be adopted. Said policy aims to keep hotel, provider, client and guest data safe, by ensuring Confidentiality, Integrity and Availability requirements for information security and business continuity are met.

Keywords: security policy, hotel information security

Índice de Contenidos

Índice de Tablas

Índice de Figuras

CAPÍTULO I

INTRODUCCIÓN

1.1. Planteamiento del problema

El extendido uso de Tecnologías de Información y Comunicación en el mundo hotelero es una tendencia sin retorno. Nunca el sector hotelero había dependido tanto de la información sistematizada. Al igual que cualquier empresa, los hoteles obedecen en gran medida de la oportuna información que manejan a diario (Santillán, 2011).

Según la entrevista realizada a Orozco (2019), los hoteles miembros de AHOTIM (Asociación Hotelera de Imbabura), utilizan una variada gama de sistemas informáticos, y no se trata de una plataforma unificada. Esto significa que cada hotel tiene su propio acuerdo de servicios con el proveedor correspondiente, con sus cláusulas y especificaciones de seguridad.

La información interna, de clientes y de huéspedes es manejada a discreción de cada funcionario en el hotel, y por tanto es susceptible de pérdida, ciberataque, manipulación o robo. También, la información sobre reservas y ventas es de manejo secreto por parte de los hoteles, quienes no desean que se revelen sus datos por razones de competencia, confidencialidad y secreto profesional (Salazar, 2020).

En ocasiones, el manejo descuidado de la información ha provocado incidentes de seguridad, tanto de la información como de la integridad física de los huéspedes. En el primer caso, ocasionando pérdida económica para la empresa y en el segundo, causando

desprestigio para el hotel y retiro de la confianza depositada en dicha empresa y en la comunidad hotelera imbabureña en general (Orozco, 2019).

Caso particular es el de los empleados despedidos intempestivamente o que han salido de la empresa por visto bueno del Ministerio del Trabajo, quienes, a modo de venganza, modificaron la información en los sistemas hoteleros, provocando el caos en una organización que depende de sus datos 24 horas al día, los 360 días del año (Salazar, 2020).

La alta rotación del personal hotelero, obliga a dichas empresas a integrar personal que a veces no tiene el conocimiento suficiente, o simplemente no hay tiempo para capacitarles en temas básicos de seguridad, por lo cual usan credenciales de otras personas, a veces con más permisos de los que deberían tener, o usuarios genéricos para los puestos clave (*e.g.* Usuario: RECEPCION para todos los recepcionistas), e incluso se permite la utilización de usuarios y claves administrativas a los empleados supuestamente de confianza.

Entonces, se deduce que los hoteles miembros de AHOTIM son propensos al robo o pérdida de información. Hecho verificado por casos pasados en que este acto sucedió. Por lo tanto, se propone la realización de una política de seguridad basada en la norma ISO 27002 que se aplique en los mencionados hoteles (Salazar, 2020).

La situación actual indica que en cualquier momento se puede suscitar un incidente de seguridad que resultaría catastrófico para el hotel víctima, puesto que, al no contar con información adecuada, habría perdido la manera de mantenerse en el negocio. También, si su información se filtra, puede comprometer la seguridad tanto del hotel como del cliente o huésped. Por último, el robo de información habría de resultar en pérdidas para el negocio (Salazar, 2020).

Para controlar que no se suscite este pronóstico, se debe diseñar e implementar una política de seguridad que permita proteger la información, tanto en aspectos de hardware como de software y garantizar la disponibilidad, integridad y confidencialidad de esta.

Los hoteles miembros de AHOTIM, por la naturaleza de su negocio, están expuestos a amenazas de seguridad informática y requieren una forma de mitigarlos (Orozco, 2019). La opción internacionalmente aceptada es la familia de normas ISO 27000, de las cuales más específicamente se requiere énfasis en los elementos que componen la norma ISO 27002.

En cuanto a seguridad informática, los hoteles miembros de AHOTIM son sujetos vulnerables y poco atendidos. Por tanto, se hace necesario la aplicación de lo establecido en esta investigación.

1.2. Formulación del problema

Los hoteles miembros de AHOTIM manejan información que debe ser íntegra, confidencial y disponible las 24 horas del día, sin embargo, no cuentan con directrices ni normas que les ayuden a proteger la información, lo que ha ocasionado incidentes de seguridad, principalmente fuga de información valiosa.

1.3. Objetivo general

Diseñar una política de seguridad de la información, que se ajuste a la realidad de los hoteles miembros de AHOTIM, mediante la aplicación de controles de la norma ISO 27002, mitigando el riesgo de seguridad de la información a los que están expuestos.

1.3.1. Objetivos específicos

- Analizar el estado actual del manejo de seguridad de la información en los hoteles miembros de AHOTIM, mediante entrevistas y encuestas a los gerentes generales

y encargados de TI en los hoteles, estableciendo la línea base de la investigación actual.

- Analizar el riesgo de seguridad de la información mediante el uso de la metodología MAGERIT, para seleccionar controles aplicables más adecuados a la realidad de los hoteles imbabureños.
- Determinar los controles de la norma ISO/IEC 27002:2013 aplicables a la realidad de los hoteles miembros de AHOTIM, mediante la lectura e investigación de trabajos similares aplicados en otros ámbitos.
- Desarrollar controles de la política de seguridad de la información para los hoteles miembros de AHOTIM, que se base en la norma ISO/IEC 27002:2013 analizada, para mitigar el riesgo de seguridad de la información identificado.

1.4. Justificación

La importancia de la integridad, confidencialidad y disponibilidad de la información es indiscutible, sobre todo en negocios de operación continua las 24 horas del día, los 360 días del año. La pérdida de una de estas características esenciales de la información podría resultar en catástrofe para los hoteles materia de estudio.

Cada vez más, los ciberataques, el malware y los atacantes internos aumentan el peligro frente a la información clave del negocio.

No existe una noción de seguridad de la información en los hoteles miembros de AHOTIM, los cuales compran sistemas y los utilizan tal como son, y sólo aplican las más mínimas reglas de seguridad que vienen embebidas en las herramientas adquiridas. Por tanto, existe riesgo de seguridad que no se está tomando en cuenta por parte de los posibles afectados (Orozco, 2019).

Esta investigación apunta a resolver la falta de una política de seguridad de la información, ayudando a los hoteles objetivo a resguardar su información y evitar incidentes nocivos que las comprometan.

1.5. Estado del arte

A nivel mundial, la investigación sobre seguridad informática en el ámbito hotelero es escasa, pero existe; ciertos trabajos se enfocan en la privacidad y seguridad física del huésped, tomando en cuenta el riesgo empresarial de exponer la información personal, como en *A Review on Privacy Issues in Hotels: A Contribution to the Definition of Information Security Policies and Marketing Strategies* (Magalhães, 2016), en donde se indica la gran superficie de ataque que exponen los hoteles, y lo poco que se hace, aparte de las regulaciones gubernamentales que normalmente tiene cada país.

Otras investigaciones se enfocan en las amenazas que la industria de hospitalidad tiene en sus manos al manejar sistemas informáticos, como en *To Be Secure or Not to Be: Isn't This the Question?A Critical Look at Hotel's Network Security* (Cobanoglu & Demicco, 2007), en donde se exploran los mecanismos que se están utilizando actualmente en los hoteles para combatir el riesgo de seguridad de la información, y que resultan poco efectivos ante los nuevos y sofisticados métodos de ataque, resaltando la utilización de software antivirus como casi única medida de prevención.

Por último, hay casos de estudio sobre la imagen que proyecta un hotel cuando ha sido atacado, como en *The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth* (Berezina, Cobanoglu, Miller, & Kwansa, 2012), en donde se investiga sobre el impacto negativo que presenta una brecha de seguridad para el activo intangible imagen, el cual al verse afectado por motivos de seguridad de la información, repercute directamente en el giro del negocio.

Estos estudios llevan a la conclusión de que la seguridad de la información es un elemento clave para el hotel, que, dependiendo de su tamaño, huéspedes e imagen, puede ser atacado en cualquier momento, recibiendo un gran impacto en su desempeño, continuidad del negocio, seguridad e incluso imagen proyectada.

Para la industria de la hospitalidad, estudios cualitativos muestran algunas características comunes entre sus establecimientos, como la disposición física de los elementos (*e.g. front desk, management, accounting*…), los cuales también dejan ver mucha similitud en los elementos de información (*i.e.* sistemas de reservas, contabilidad, aplicaciones en nube…), y por tanto, comparten ciertas vulnerabilidades y amenazas comunes, como acceso no autorizado, robo de equipos, *spoofing*, etc. (Shabani, 2017). Estas características son también visibles en el ámbito hotelero ecuatoriano.

En países como Catar, que toman muy en serio la seguridad del huésped (*i.e.* dado que la industria turística es gran soporte de la economía), se han desarrollado políticas de seguridad como la dispuesta por *The Smart Qatar Security Standard*, bajo el apartado *Security Guidelines for Hotel Information Systems*, la cual expone los lineamientos a seguir por los hoteles para mejorar la seguridad de la información (MTC-Qatar, 2018). Ecuador no dispone de algo similar.

Para el sector hotelero ecuatoriano, no existe una política de seguridad de la información, sea pública o privada, para hoteles o similares. Los entes de control del sector turístico se rigen a lo dispuesto para instituciones públicas, pero en el caso de AHOTIM, al ser una institución de derecho privado al igual que sus miembros, no cuenta con tales normas, protocolos o procedimientos para el sector turístico (Orozco, 2019).

Según Garavito (2015), se presentan las principales observaciones de seguridad de la información:

- Sistemas con protocolos no seguros
- Falta de procedimientos documentados para copias de seguridad
- Falta de capacitaciones de concientización en el tema
- Errores en el ingreso de datos al sistema
- No existen módulos de auditoría de registro de operaciones

Según los autores anteriormente citados, las instituciones con información sensible son sujetas a una alta probabilidad de ataque, es por esto que se hace necesario contar con los métodos necesarios para proteger la mencionada información y también asegurar la continuidad del negocio.

CAPÍTULO II

MARCO TEÓRICO

2.1. La información en el sector hotelero

La información es un conjunto de datos que tienen sentido, y deben cumplir con 3 características de calidad: Integridad, Disponibilidad y Confidencialidad (Vieites, 2011).

Cada vez más, la automatización de la información impacta en todos los ámbitos y el hotelero no es la excepción. Sin duda, la información es el activo más importante de la organización, especialmente de las que dependen de sus datos ininterrumpidamente (Martínez, 2012).

En el sector hotelero se maneja información de sistemas interconectados, de cada hotel, de sus clientes y de los huéspedes, la cual suele ser de alto grado de compromiso y, por tanto, debe asegurarse sus tres características de calidad en todo momento, tal como se refleja en la Figura 1. Canales de distribución de los servicios turísticos:

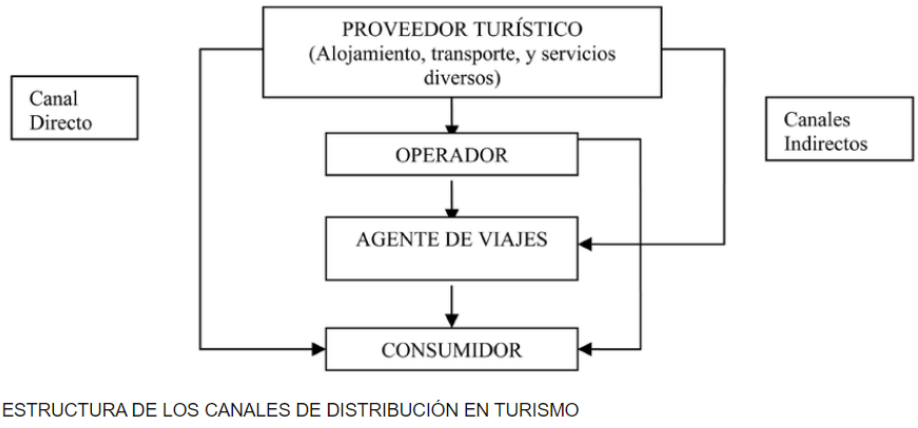

Figura 1. Canales de distribución de los servicios turísticos (Muradas, 2010)

Entonces, se puede concluir que la información debe estar segura en todo momento.

Los sistemas más comúnmente utilizados en hotelería son los *Property Management Systems - PMS*, los cuales engloban una cantidad importante de operaciones hoteleras en un solo paquete, desde el manejo de habitaciones, pasando por las reservas -en las cuales se maneja información sensible-, hasta el estado y ocupación del hotel en cualquier momento. Un *PMS* actualmente conecta con el mundo a través de Internet para mostrar la disponibilidad y vender habitaciones directamente a agencias e individuos, ya que el giro del negocio así lo demanda hoy en día.

Otros sistemas manejados en hoteles manejan la facturación, contabilidad, talento humano, etc., tal como lo demanda la regulación nacional, y, por tanto, lidian con información de carácter sensible acerca de los clientes, huéspedes, actividades, formas de pago, información crediticia, etc.

2.2. La seguridad de la información

Según Solarte (2015), la seguridad de la información es un campo de la seguridad que trata sobre cómo asegurar que la información cumpla con sus tres parámetros de calidad, Confidencialidad, Integridad y Disponibilidad:

Para asegurar la Integridad, es necesario que la información nunca sea manipulada de manera inadecuada. Para asegurar la disponibilidad, es necesario disponer de todos los mecanismos que permitan que la información llegue a quien –y sólo a quien- debe llegar. Por último, para asegurar la confidencialidad, se debe cerciorar que la información se mantenga privada en todo momento.

La información es susceptible de vulnerabilidades, amenazas y riesgos que, en caso de convertirse en ataques, pueden comprometer los tres parámetros mencionados.

2.3. Vulnerabilidad, Amenazas y Riesgos de seguridad

Las vulnerabilidades son puntos débiles en el sistema, por lo tanto, se convierten en una amenaza latente que puede ser explotada. Esto, es un riesgo que se debe analizar y mitigar para no ser víctima de ataque (Paulsen C., 2019).

En hotelería, los riesgos de seguridad son muchos, comenzando por la confidencialidad de los datos financieros, hasta el riesgo de confidencialidad de la información del huésped que podría comprometer hasta su seguridad física, dentro o fuera de las instalaciones del hotel.

2.3.1. Vulnerabilidad informática

Peligro latente que permanece de manera conocida o desconocida en un sistema informático, y que tiene la capacidad de ser explotado, comprometiendo la funcionalidad normal del mencionado sistema (INCIBE, 2015).

2.3.2. Riesgo de Seguridad Informática

Es el riesgo latente de que una amenaza de seguridad informática pueda ser ejecutada, causando problemas en sistemas informáticos (Valdéz, 1988).

2.3.3. Amenaza Informática

Es cualquier indicio de que existe una vulnerabilidad que podría ser explotada, y que pudiera significar peligro para un sistema informático.

Para atenuar el efecto de los ataques a la información, es necesario contar con una política de seguridad que permita resguardar la información y continuidad del negocio. Algo que permita y -de ser posible- obligue a los usuarios a proteger el activo más importante: la información.

2.4. Política de seguridad

Según Vieites (2011), es una declaración de cualquier medida que impida la operación indebida de un sistema informático. Esto con el fin de conservar sus tres características de calidad: Integridad, Disponibilidad y Confidencialidad.

Es un documento de alto nivel que contiene, entre varios aspectos, la definición de seguridad aplicable a la entidad en cuestión (Guayta, 2009).

Entonces, un documento de política de seguridad informática consta generalmente de secciones tales como indica Guayta (2009):

- Resumen
- Introducción
- Ámbito de aplicación
- Objetivos
- Responsabilidades

Para el desarrollo de una efectiva política de seguridad, es necesario basarse en normas y estándares establecidos que ayudan en la elaboración de instrumentos que perduren la prueba del uso y del tiempo, tales como las normas ISO 27000.

2.4.1. Normas ISO/IEC 27000

Norma internacional que dicta estándares sobre seguridad, facilitando el comercio, intercambio de información y apoyando a la transferencia de las tecnologías (MENTOR, n.d.). Es la familia de normas que mejor se ajusta a la necesidad objeto de esta investigación, por cuanto sus componentes son clave para establecer una política de seguridad que le sirva a los hoteles miembros de AHOTIM.

Dentro de esta familia de normas, la ISO 27002:2013 se ajusta a las necesidades de desarrollo de políticas de seguridad de la información.

2.4.2. Norma ISO/IEC 27002:2013

Referida también como el lenguaje común para organizaciones alrededor del mundo para la seguridad de la información (Humphreys, 2011), es una guía que sirve para estandarizar el manejo de la seguridad de la información en la organización.

Este estándar ha sido desarrollado a través de los años y en base a otros estándares para lograr una guía comprensiva o "código de práctica" a seguir, tal como se muestra en la Figura 2. Desarrollo de los estándares ISO 27000, ISO 27001 e ISO 27002.

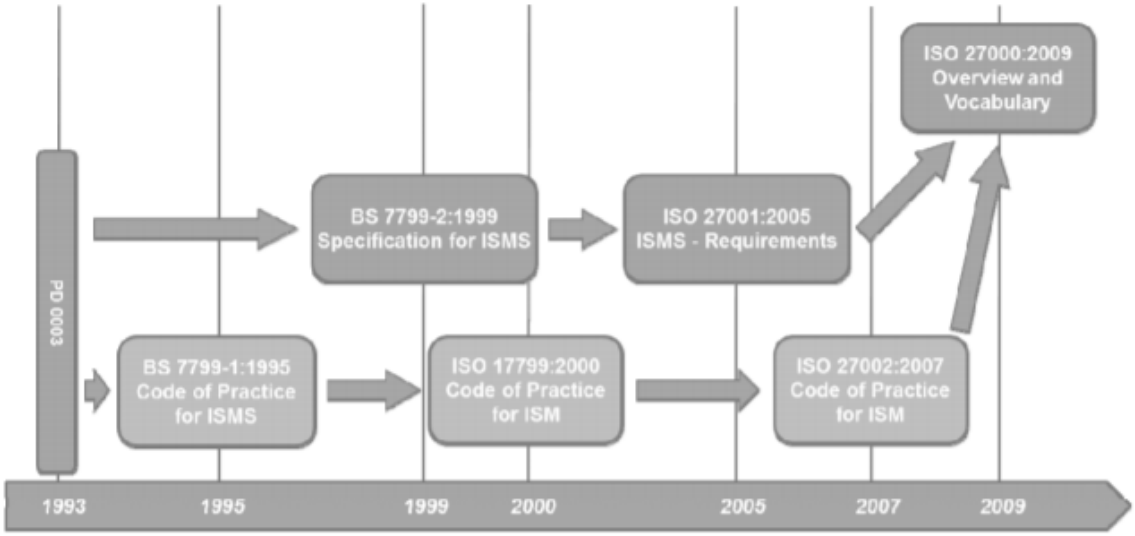

Figura 2. Desarrollo de los estándares ISO 27000, ISO 27001 e ISO 27002 (Disterer, 2013)

Las políticas de seguridad deben basarse a fuerza en un análisis de riesgo bien hecho, para lo cual existen técnicas como el Análisis de Riesgo por fórmula matemática simple (*i.e.* Riesgo = Probabilidad de Amenaza x Magnitud de daño), sin embargo, existe una metodología robusta y probada denominada MAGERIT, que se enfoca en análisis de riesgo de seguridad de la información (INCIBE, 2015).

2.5. Metodología MAGERIT

Conjunto de métodos para el análisis y gestión de riesgos en seguridad de la información, desarrollada por el Ministerio de Administraciones Públicas español (MHAP, 2012), la cual es promovida de maneral especial por el INCIBE.

Esta metodología consta de varias etapas a realizarse:

Tabla 1. Etapas de la metodología MAGERIT

Etapa	Propósito
Levantamiento de activos	Catalogar elementos que presentan riesgo
Determinar amenazas	Saber a qué se está expuesto
Estimar el impacto	Proyectar en qué grado el riesgo es dañino para la organización
Estimar la probabilidad	Calcular la oportunidad de ser impactado
Determinar las salvaguardas	Establecer los controles a implementar

Fuente. Adaptado de: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (INCIBE, 2015).

2.5.1. INCIBE

Instituto Nacional de Ciberseguridad – España. Organismo que se dedica a la educación y elaboración de materia en ciberseguridad, con el objetivo de fortalecer el uso seguro del ciberespacio (INCIBE, 2015). Promueve un análisis ordenado del riesgo al que se enfrenta la organización y permite una clasificación de los elementos, que luego se verán plasmados en la definición de la política propuesta.

2.6. Definición de políticas de seguridad

Dado que la política de seguridad es una declaración de intenciones a alto nivel (Höne & Eloff, 2012), la cual sirve como base para la elaboración de planes y procedimientos a llevar a cabo en la organización, lo cual permite cumplir el objetivo de mitigación del riesgo.

Para lograr la definición de la política, es necesario asegurar las siguientes etapas:

Tabla 2. Etapas de la elaboración de una política de seguridad

Etapa	Propósito
Planeación	Análisis de riesgo
Desarrollo	Seguimiento
Redacción	Plasmar clara y precisamente lo que se debe hacer
Aprobación	Ratificar la política y difundirla

Fuente. Adaptado de: techno-legal aspects of information society and new economy: an overview (Mendez, 2003)

CAPÍTULO III

ANÁLISIS Y SITUACIÓN ACTUAL

3.1. Situación actual

3.1.1. Antecedentes

La Asociación Hotelera de Imbabura – AHOTIM, es una organización privada que tiene como objetivo preservar el bienestar de los hoteles miembros (*i.e.* socios), mediante la elaboración de estrategias y la colaboración. Actualmente cuenta con 23 miembros y cuenta con la siguiente directiva:

Tabla 3. Directiva actual de AHOTIM

Dignidad	Nombre
Presidente	Carlos Andrés Orozco
Vicepresidente	Carlos Salazar
Secretario	Pedro Freile
Vocal	Carlos Dávila
Vocal	Graciela Domínguez
Vocal	Rubén López

Elaborado por: El autor

Los hoteles miembros cuentan con el siguiente esquema común de activos en operación:

Tabla 4. Activos comunes para los miembros de AHOTIM

Tipo	Activo
Servicios	Respaldo
	PMS en línea
	Internet

Tabla 4. Activos comunes para los miembros de AHOTIM

Tipo	Activo
	Correo Institucional
	Gestión del parque informático
Datos e Información	Bases de datos físicas
	Documentos Confidenciales
	Documentos de Uso Interno
Software	*PMS* local
	Apache
	Bases de Datos Digitales
	Sistemas operativos
	Booking apps
	WordPress
Equipos Informáticos	*Desktops/Laptops*
	Cámaras
	Servidores
	Access points
	Servidores
Redes de Comunicaciones	Red interna
	Red *Wireless* huéspedes
Soporte de Información	*Drives* externos
	Almacenamiento en Nube
Equipamiento Auxiliar	Fuentes de alimentación
	Generadores eléctricos
Instalaciones	*Datacenter*
Personal	Gerente
	Mantenimiento

Tabla 4. Activos comunes para los miembros de AHOTIM

Tipo	Activo

Fuente. Adaptado de: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (INCIBE, 2015)

El escenario común presenta un hotel dispuesto de la siguiente forma:

Tabla 5. Disposición típica de un hotel miembro de AHOTIM

Activo	Lugar	Propósito
Respaldo	*Datacenter*	Salvaguardar la información
PMS en línea	N/A	Ventas
Internet	N/A	Operación y ventas
Correo Institucional	N/A	Operación y ventas
Gestión del parque informático	N/A	Control
Bases de datos físicas	Gerencia	Operación y ventas
Documentos Confidenciales	Gerencia	Operación
Documentos de Uso Interno	Gerencia	Operación
PMS local	Recepción	Operación y ventas
Apache	N/A	Servidor web
Bases de Datos Digitales	*Datacenter*	Operación y ventas
Sistemas operativos	Estaciones de trabajo	Operación y ventas
Booking apps	N/A	Operación y ventas
WordPress	N/A	Operación y ventas
Desktops/Laptops	Recepción y gerencia	Operación y ventas
Cámaras	Todo el establecimiento	Seguridad
Servidores	*Datacenter*	Operación y ventas
Access points	*Datacenter*	Operación
Servidores	*Datacenter*	Operación y ventas
Red interna	Todo el establecimiento	Operación
Red *Wireless* huéspedes	Todo el establecimiento	Servicio
Drives externos	Datacenter	Respaldos
Almacenamiento en Nube	N/A	Respaldos
Fuentes de alimentación	*Datacenter*	Continuidad
Generadores eléctricos	Cuarto de máquinas	Continuidad
Datacenter	Cuarto de máquinas	Operación y ventas
Gerente	Gerencia	Operación
Mantenimiento	Todo el establecimiento	Operación

Fuente. Adaptado de: Entrevista a Señor Presidente de AHOTIM (Orozco, 2019)

Entonces, el escenario tecnológico de un hotel miembro se resume en la Figura 3. Esquema tecnológico típico de un hotel miembro de AHOTIM:

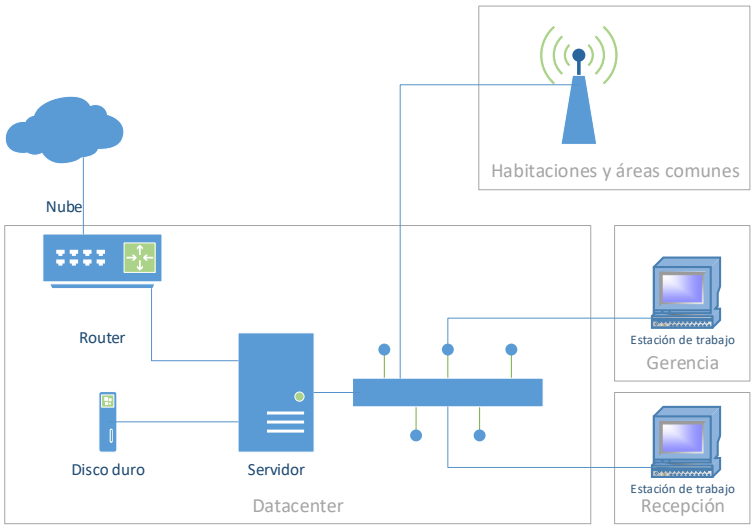

Figura 3. Esquema tecnológico típico de un hotel miembro de AHOTIM. Elaborado por el autor

Llama la atención la extrema sencillez con que se manejan los entornos de TI en los hoteles, y la falta de mecanismos de protección.

3.1.2. Seguridad actual de la información

De las entrevistas conducidas a los actores involucrados, se obtiene que los hoteles cuentan con unos pocos mecanismos de seguridad para salvaguardar la información y continuidad del negocio.

3.1.2.1. Física

Los hoteles miembros cuentan con los siguientes dispositivos de seguridad física activa y pasiva:

- Guardia de seguridad
- Cámaras de seguridad
- Rejas
- Candados

- UPS
- Generadores

3.1.2.2. Lógica

Los hoteles miembros cuentan con las siguientes medidas de seguridad lógica:

- Passwords, tanto para sistemas locales como web
- Respaldos locales, tanto de sistemas locales como web
- Respaldos en línea, tanto de sistemas locales como web
- Software antivirus

3.1.3. Información a proteger

La información que manejan los hoteles miembros corresponde a dos categorías importantes, externa e interna, de la siguiente forma:

Tabla 6. Información a proteger en los hoteles miembros

Categoría	Descripción
Interna	Facturación Contable Reservas Colaboradores Seguridad física (e.g. cámaras, accesos, etc.)
Externa	Clientes Huéspedes Colaboraciones (e.g. agencias, transporte, atracciones, etc.)

Nota. Elaborado por: El autor

3.1.4. Análisis del riesgo

Aplicando la metodología MAGERIT discutida anteriormente, mediante proceso de observación y entrevista, se procede con la primera etapa, denominada Levantamiento de Activos, en donde se categoriza y describen los mismos, tal como se muestra a continuación:

3.1.4.1. Etapa 1: Levantamiento de activos

Tabla 7. Categorización de activos

Activo	Definición	Ejemplos
Servicio	Internos cuando se producen y consumen dentro de la organización. Externos cuando se los consume desde un proveedor	Acceso a Internet, correo electrónico, servicio de certificados, etc.
Datos/información	Componentes que integran información.	Documentos, grabaciones, reportes, código, logs, etc.
Software	Aplicativos de toda clase	Programas de cualquier sistema operativo
Equipos informáticos (*hardware*)	Bienes tangibles que componen el parque informático	Computadores, servidores, *Access points*, *switches*, celulares, etc.
Redes de comunicaciones	Infraestructura que permite la comunicación entre equipos informáticos	Red cableada, red inalámbrica, red celular, etc.
Soporte de información	Dispositivos en donde se almacenan los datos	*Drives* de toda clase. *CD*, *DVD*, memorias *flash*, externos, etc.
Equipamiento auxiliar	Equipamiento que apoya el funcionamiento de los sistemas informáticos	Generadores eléctricos, UPS, aire acondicionado, etc.
Instalaciones	Lugar donde se encuentra la infraestructura	Inmuebles o muebles donde se instalan los equipos. Edificios, oficinas, locales, etc.
Personal	Personas que trabajan con los sistemas informáticos	Trabajadores, operadores, administradores, etc.

Nota. Adaptado de: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (INCIBE, 2015).

3.1.4.2. Etapa 2: Determinación de amenazas

Para la esta etapa, se sigue la metodología MAGERIT y se apoya en la siguiente tabla, denominada Criterios de Valoración:

Tabla 8. Criterios de valoración para Confidencialidad, Integridad y Disponibilidad según la metodología MAGERIT

Valor	Confidencialidad
0	De acceso público
1	De acceso a las personas de la organización, pero no al público
2	De acceso a quienes pudieran necesitarla dentro de la organización
3	De acceso exclusivo a un grupo reducido y estricto de personas
Valor	**Integridad**
0	Cuya modificación no afecta el giro del negocio
1	Cuya modificación afecta al giro del negocio o a terceros, pero puede restaurarse fácilmente
2	Cuya modificación afecta al giro del negocio o a terceros, pero puede restaurarse, aunque con mucha dificultad
3	Cuya modificación afecta gravemente al giro del negocio o a terceros, y no puede restaurarse
Valor	**Disponibilidad**
0	Cuya inaccesibilidad no afecta la actividad normal de la Institución.
1	Cuya inaccesibilidad afecta la operatividad de la institución, pero puede continuar funcionando
2	Cuya inaccesibilidad afecta gravemente la operatividad de la institución, pero puede continuar funcionando, aunque con mucha dificultad
3	Cuya inaccesibilidad no permite la operación de la institución

Nota. Adaptado de: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (INCIBE, 2015).

3.1.4.3. Etapa 3: Estimación del impacto

Entonces, se procede a estimar cual sería la severidad del impacto en caso de que un incidente suceda, según los siguientes criterios:

- **Tipo**: El tipo de activo según la categorización descrita en la Tabla 7.
- **Identificador**: Código único para referencia en otras matrices.
- **Nombre del activo**: Descripción que identifica el activo.
- **Proceso**: Departamento a cargo del activo.
- **Valoración de Confidencialidad**: Valor según consenso, tal como describe la Tabla *8*. Describe el grado de afectación si cae en manos equivocadas.
- **Valoración de Integridad**: Valor según consenso, tal como describe la Tabla *8*. Describe el grado de afectación si la información en el activo es alterada.
- **Valoración de Disponibilidad**: Valor según consenso, tal como describe la Tabla *8*. Describe el grado de afectación si el activo no está disponible.
- **Valoración de Criticidad**: Valor obtenido de una fórmula matemática que promedia los tres valores anteriores. Indica el grado general de afectación si la seguridad del activo es comprometida.

La Tabla *8* también describe mediante colores el grado de criticidad apreciado, según los siguientes criterios:

- **Verde**: El impacto es menor y no compromete la continuidad del negocio.
- **Amarillo**: El impacto es apreciable pero no compromete la continuidad del negocio.
- **Naranja**: El impacto es importante y afecta parcialmente la continuidad del negocio.
- **Rojo**: El impacto es importante y afecta totalmente la continuidad del negocio.

Tipo	Activo	Proceso	Confidencialidad	Integridad	Disponibilidad	Criticidad
Servicios	Respaldo	Mantenimiento	3	3	3	3,0
	PMS en línea	Mantenimiento	3	2	3	2,7
	Internet	Mantenimiento	3	1	3	2,3
	Correo Institucional	Mantenimiento	3	1	3	2,3
	Gestión del parque informático	Mantenimiento	3	1	3	2,3
Datos e Información	Bases de datos físicas	Mantenimiento	3	3	3	3,0
	Documentos Confidenciales	Mantenimiento	3	2	2	2,3
	Documentos de Uso Interno	Mantenimiento	3	3	1	2,3
Software	*PMS* local	Mantenimiento	3	3	3	3,0
	Apache	Mantenimiento	3	3	3	3,0
	Bases de datos digitales	Mantenimiento	3	3	3	3,0
	Sistemas operativos	Mantenimiento	3	3	2	2,7
	Booking apps	Mantenimiento	2	3	3	2,7
	WordPress	Mantenimiento	3	2	2	2,3

Tipo	Activo	Proceso	Confidencialidad	Integridad	Disponibilidad	Criticidad
Equipos Informáticos	*Desktops/Laptops*	Mantenimiento	3	3	3	3,0
	Cámaras	Mantenimiento	3	3	3	3,0
	Servidores	Mantenimiento	3	2	3	2,7
	Access Points	Redes	2	3	2	2,3
Redes de Comunicaciones	Red interna	Infraestructura	3	3	3	3,0
	Red *Wireless* huéspedes	Infraestructura	3	3	2	2,7
Soporte de Información	*Drives* externos	Mantenimiento	3	3	3	3,0
	Almacenamiento en Nube	Mantenimiento	3	3	3	3,0
Equipamiento Auxiliar	Fuentes de alimentación	Redes	3	3	3	3,0
	Generadores eléctricos	Mantenimiento	3	3	2	2,7
Instalaciones	*Datacenter*	Infraestructura	3	3	3	3,0
Personal	Gerente	Administración	3	3	3	3,0
	Mantenimiento	Administrador de datos	3	3	3	3,0

Fuente: El autor, en base a Metodología MAGERIT

Luego, se califica mediante consenso con TI en los hoteles, y se valora el impacto según las matrices descritas anteriormente, calificando cada amenaza presente.

Tabla 9. Matriz de impacto – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
1	Fuego	3	3	3	3	2										3	3	3	3	2	2	3	2	3	3	3		
2	Daños por agua	3	3	3	3	2										3	3	3	3	2	2	3	2	3	3	3		
3	Desastres naturales	3	3	3	3	2										3	3	3	3	2	2	3	2	3	3	3		
4	Corte del suministro eléctrico	3	3	3	3	2										3	3	3	3	2	2	3	2	3	3	3		
5	Condiciones inadecuadas de temperatura o humedad	1	1	1	1	1	3	1	1									1										

Tabla 9. Matriz de impacto – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos			Redes de Comunicaciones			Soporte de Información		Equipamiento Auxiliar			Instalaciones		Personal
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
6	Fallo de servicios de comunicaciones	2	2	2	2	1	3	1	1	3	1	3	3	3	1	2	2	3	2	2	2	3	2			3		
7	Desastres industriales	2	2	2	2	1	3	1	1	3	1	3	3	3	1	2	2	3	2	2	2	3	2	3	3	3		
8	Fuga de información	3	3	3	3	1	3	2	1	3	1	3	3	3	1	3	3	3	1			3	2					
9	Introducción de falsa información	3	3	3	3	1	3	3	3	3	1	3	3	3	1	3	3	3	2			3	2					
10	Acceso no autorizado	1	1	1	1	1	1	1	1	3	1	3	3	3	1	3	3	3	2			3	2					
11	Vulnerabilidad de programas (software)	3	3	3	3	3	2	2	2	3	1	3	3	3	1	3	3	3	2			3	2					
12	Corrupción de la información	3	3	3	3	3	3	3	3	3	1	3	3	3	1	3	3	3	2			3	2					
13	Destrucción de información	3	3	3	3	3	3	3	3	3	1	3	3	3	1	3	3	3	2			3	2					

Tabla 9. Matriz de impacto – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente Mantenimiento
14	Interceptación de información	1	1	1	1	2	1	1		3	1	3	3	3	1	3	3	3	2			3	1				
15	Indisponibilidad del personal	2	2	2	2	2	1	1		3	1	3	3	3	1	2	2	3	2			3	1				
16	Agotamiento de recursos	2	2	2	2	2	1	1		3	1	3	3	3	1	1	1	3	1			3	1				
17	Errores de los usuarios	2	2	2	2	2	1	1		1	1	1	1	1	1	1	1	3	2			3	2				
18	Errores del administrador	2	2	2	2	2	1	1		1	1	1	1	1	1	2	2	3	2			3	2				
19	Errores de configuración	2	2	2	2	2	1	1		3	1	3	3	3	1	3	3	3	2			3	2				
20	Degradación de los soportes de almacenamiento de la información	1	1	1	1	2	1	1		1	1	1	1	1	1	3	3	3	2			3	2				
21	Difusión de software dañino	3	3	3	3	2	1	1		3	1	3	3	3	1	3	3	3	3			3	2				

Tabla 9. Matriz de impacto – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente Mantenimiento
22	Errores de mantenimiento / actualización de programas (software)	2	2	2	2	2	1	1		3	1	3	3	3	1	3	3	3	2			3	2				
23	Errores de mantenimiento / actualización de equipos (hardware)	1	1	1	1	2	3	1		1	1	1	1	1	1	3	3	3	2			3	2				
24	Caída del sistema por sobrecarga	3	3	3	3	2	3	1		3	1	3	3	3	1	3	3	3	2			3	1				
25	Denegación de servicio	3	3	3	3	2	3	1	1	3	1	3	3	2	1	2	3	3	2	2	2	2					
26	Robo	3	3	3	3	2	3	1	1	3	1	3	3	2	1	2	3	3	2	3	3	2	1				
27	Ataques destructivos	3	3	3	3	2	3	1	1	3	1	3	3	2	1	2	3	3	2	3	3	2	1				

Tabla 9. Matriz de impacto – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente Mantenimiento
28	Extorsión	3	3	3	3	2	3	1	1	3	1	3	3	2	1	2	3	3	2			2	1				
29	Ingeniería social	3	3	3	3	2	3	1	1	3	1	3	3	2	1	2	3	3	2			2	1				
30	Manipulación de logs	3	3	3	3	2	3	1	1	3	1	3	3	2	1	2	3	3	2			2	1				
31	Abuso de privilegios de acceso	2	2	2	2	2	3	1	1	2	1	3	2	2	1	2	3	3	2	1	1	2	1				
32	Manipulación de equipos	2	2	2	2	2	3	1	1	2	1	3	2	2	1	2	3	3	2	2	2	2					
33	Manipulación de configuración	2	2	2	2	2	3	1	1	2	1	3	2	2	1	2	3	3	2	2	2	2	1				
34	Alteración de la información	2	2	2	2	2	3	1	1	2	1	3	2	2	1	2	2	3	2	2	2	2	1				

Fuente: El autor, en base a Metodología MAGERIT

3.1.4.4. Etapa 4: Estimación de la probabilidad

Luego, se procede a tomar en cuenta la observación en campo y la experiencia de TI en los hoteles. La metodología indica los valores de los cuales se puede escoger para ello, entre 0 y 3. En el caso de haber valores en blanco, es porque no aplica tal calificación a ese activo.

En la parte izquierda de la Tabla 11, la columna titulada "Amenaza" describe un catálogo común de posibles factores que pudieran comprometer al activo (INCIBE, 2015).

Tabla 10. Matriz de probabilidad del riesgo – MAGERIT

		Servicios					Datos			Aplicaciones					Equipos Informáticos					Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
1	Fuego	1					1	1	1							1	1	1	1	1	1	1		1	1			
2	Daños por agua						1	1	1							1	1	1	1	1	1	1		1	1			

Tabla 10. Matriz de probabilidad del riesgo – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente Mantenimiento
3	Desastres naturales	1					1									1	1	1	1	1	1	1		1	1		
4	Corte del suministro eléctrico	2	2	2	2	2	1			2	2	2	2	2	2	2	2	2	2	2	2	2		2	2		
5	Condiciones inadecuadas de temperatura o humedad	1	1																	1	1						
6	Fallo de servicios de comunicaciones	1	3	3	3		1									2	2	2	2	1	1						
7	Desastres industriales	3					3									1	1	1	1	1	1	1					
8	Fuga de información	2	3	3	2		3					3	3			2	2	2				1	1				
9	Introducción de falsa información		1			1	3					1	1	1													
10	Acceso no autorizado	3		3	2		2			1		1	1	1		3	2	1				1	1				

Tabla 10. Matriz de probabilidad del riesgo – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
11	Vulnerabilidad de programas (software)	1					1			1		1	1			3	3	3										
12	Corrupción de la información	1					1			2		1				3	3	3				1						
13	Destrucción de información	1								1						2	2	2				1	1					
14	Interceptación de información		3				2			1		1		1		3	1	1										
15	Indisponibilidad del personal	3					3					3	2	1	3	3	3	3		2	2	1						
16	Agotamiento de recursos	3		2													3	1				1	1					
17	Errores de los usuarios	3	3							1	1				1	3	1	1				2	2					
18	Errores del administrador	2		2								1	1	1	2	1	1	1		1	1	1	1					
19	Errores de configuración	1					1				1					1	1	1				1	1					

Tabla 10. Matriz de probabilidad del riesgo – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
20	Degradación de los soportes de almacenamiento de la información	1					1															2						
21	Difusión de software dañino	1														3		1				1						
22	Errores de mantenimiento / actualización de programas (software)	1					1			1	1	1	1	1	1	3	3	3				1						
23	Errores de mantenimiento / actualización de equipos (hardware)	1																		2	2	1						

Tabla 10. Matriz de probabilidad del riesgo – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
24	Caída del sistema por sobrecarga	1																2		1	1							
25	Denegación de servicio																											
26	Robo	2														1	1	1										
27	Ataques destructivos	1										1					1					1	1					
28	Extorsión																											
29	Ingeniería social		1																									
30	Manipulación de logs						1					1						1										
31	Abuso de privilegios de acceso	1	1	1	2		1					2	2	2				2				1	1					
32	Manipulación de equipos															2												
33	Manipulación de configuración																											

Tabla 10. Matriz de probabilidad del riesgo – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos			Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
34	Alteración de la información		1		1		1			2		1	1			3		2				2	2					

Fuente: El autor, en base a Metodología MAGERIT

De la multiplicación de la probabilidad por el impacto de cada riesgo (*i.e.* Ecuación del riesgo), se obtiene automáticamente la siguiente Matriz de Riesgos, en la que el color y el número asociado resaltan los aspectos a los que más atención debe darse para el desarrollo de la política de seguridad de la información.

Tabla 11. Matriz de Riesgos – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	Desktops/Laptops	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
1	Fuego	3	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	3	2	2	3	0	3	3	0	0	0
2	Daños por agua	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	3	2	2	3	0	3	3	0	0	0
3	Desastres naturales	3	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	3	2	2	3	0	3	3	0	0	0
4	Corte del suministro eléctrico	6	6	6	6	4	0	0	0	0	0	0	0	0	0	6	6	6	6	4	4	6	0	6	6	0	0	0
5	Condiciones inadecuadas de temperatura o humedad	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Fallo de servicios de comunicaciones	2	6	6	6	0	3	0	0	0	0	0	0	0	0	4	4	6	4	2	2	0	0	0	0	0	0	0
7	Desastres industriales	6	0	0	0	0	9	0	0	0	0	0	0	0	0	2	2	3	2	2	2	3	0	0	0	0	0	0
8	Fuga de información	6	9	9	6	0	9	0	0	0	0	9	9	0	0	6	6	6	0	0	0	3	2	0	0	0	0	0
9	Introducción de falsa información	0	3	0	0	1	9	0	0	0	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	Acceso no autorizado	3	0	3	2	0	2	0	0	3	0	3	3	3	0	9	6	3	0	0	0	3	2	0	0	0	0	0

Tabla 11. Matriz de Riesgos – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones			Soporte de Información		Equipamiento Auxiliar		Instalaciones		Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	Desktops/Laptops	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
11	Vulnerabilidad de programas (software)	3	0	0	0	0	2	0	0	3	0	3	3	0	0	9	9	9	0	0	0	0	0	0	0	0	0	0	0
12	Corrupción de la información	3	0	0	0	0	3	0	0	6	0	3	0	0	0	9	9	9	0	0	0	3	0	0	0	0	0	0	0
13	Destrucción de información	3	0	0	0	0	0	0	0	3	0	0	0	0	0	6	6	6	0	0	0	3	2	0	0	0	0	0	0
14	Interceptación de información	0	3	0	0	0	2	0	0	3	0	3	0	3	0	9	3	3	0	0	0	0	0	0	0	0	0	0	0
15	Indisponibilidad del personal	6	0	0	0	0	3	0	0	0	0	9	6	3	3	6	6	9	0	0	0	3	0	0	0	0	0	0	0
16	Agotamiento de recursos	6	0	4	0	0	0	0	0	0	0	0	0	0	0	0	3	3	0	0	0	3	1	0	0	0	0	0	0
17	Errores de los usuarios	6	6	0	0	0	0	0	0	1	1	0	0	0	1	3	1	3	0	0	0	6	4	0	0	0	0	0	0
18	Errores del administrador	4	0	4	0	0	0	0	0	0	0	1	1	1	2	2	2	3	0	0	0	3	2	0	0	0	0	0	0
19	Errores de configuración	2	0	0	0	0	1	0	0	0	1	0	0	0	0	3	3	3	0	0	0	3	2	0	0	0	0	0	0
20	Degradación de los soportes de almacenamiento de la información	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0

Tabla 11. Matriz de Riesgos – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	Desktops/Laptops	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
21	Difusión de software dañino	3	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	3	0	0	0	3	0	0	0	0	0	0
22	Errores de mantenimiento / actualización de programas (software)	2	0	0	0	0	1	0	0	3	1	3	3	3	1	9	9	9	0	0	0	3	0	0	0	0	0	0
23	Errores de mantenimiento / actualización de equipos (hardware)	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0
24	Caída del sistema por sobrecarga	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0
25	Denegación de servicio	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	Robo	6	0	0	0	0	0	0	0	0	0	0	0	0	0	2	3	3	0	0	0	0	0	0	0	0	0	0
27	Ataques destructivos	3	0	0	0	0	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	2	1	0	0	0	0	0
28	Extorsión	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	Ingeniería social	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Tabla 11. Matriz de Riesgos – MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	Desktops/Laptops	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
30	Manipulación de logs	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0
31	Abuso de privilegios de acceso	2	2	2	4	0	3	0	0	0	0	6	4	4	0	0	0	6	0	0	0	2	1	0	0	0	0	0
32	Manipulación de equipos	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0
33	Manipulación de configuración	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	Alteración de la información	0	2	0	2	0	3	0	0	4	0	3	2	0	0	6	0	6	0	0	0	4	2	0	0	0	0	0

Fuente: El autor, en base a Metodología MAGERIT

Como resultado de la matriz anterior, separando de la misma los riesgos que requieren atención, se obtiene el Resumen Final, que indica qué riesgos se debe controlar con la Política de Seguridad a proponer. Los casilleros en blanco significan riesgo nulo o no aplicable, mientras que el resto tienen la calificación correspondiente, y el color verde, amarillo y rojo, según la gravedad del impacto.

Tabla 12. Resumen Final del análisis del riesgo - MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
1	Fuego	3	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	3	2	2	3	0	3	3	0	0	0
2	Daños por agua	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	3	2	2	3	0	3	3	0	0	0
3	Desastres naturales	3	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	3	2	2	3	0	3	3	0	0	0
4	Corte del suministro eléctrico	6	6	6	6	4	0	0	0	0	0	0	0	0	0	6	6	6	6	4	4	6	0	6	6	0	0	0
5	Condiciones inadecuadas de temperatura o humedad	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Fallo de servicios de comunicaciones	2	6	6	6	0	3	0	0	0	0	0	0	0	0	4	4	6	4	2	2	0	0	0	0	0	0	0
7	Desastres industriales	6	0	0	0	0	9	0	0	0	0	0	0	0	0	2	2	3	2	2	2	3	0	0	0	0	0	0
8	Fuga de información	6	9	9	6	0	9	0	0	0	0	9	9	0	0	6	6	6	0	0	0	3	2	0	0	0	0	0

Tabla 12. Resumen Final del análisis del riesgo - MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones		Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
9	Introducción de falsa información	0	3	0	0	1	9	0	0	0	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	Acceso no autorizado	3	0	3	2	0	2	0	0	3	0	3	3	3	0	9	6	3	0	0	0	3	2	0	0	0	0	0	0
11	Vulnerabilidad de programas (software)	3	0	0	0	0	2	0	0	3	0	3	3	0	0	9	9	9	0	0	0	0	0	0	0	0	0	0	0
12	Corrupción de la información	3	0	0	0	0	3	0	0	6	0	3	0	0	0	9	9	9	0	0	0	3	0	0	0	0	0	0	0
13	Destrucción de información	3	0	0	0	0	0	0	0	3	0	0	0	0	0	6	6	6	0	0	0	3	2	0	0	0	0	0	0
14	Interceptación de información	0	3	0	0	0	2	0	0	3	0	3	0	3	0	9	3	3	0	0	0	0	0	0	0	0	0	0	0
15	Indisponibilidad del personal	6	0	0	0	0	3	0	0	0	0	9	6	3	3	6	6	9	0	0	0	3	0	0	0	0	0	0	0
16	Agotamiento de recursos	6	0	4	0	0	0	0	0	0	0	0	0	0	0	0	3	3	0	0	0	3	1	0	0	0	0	0	0
17	Errores de los usuarios	6	6	0	0	0	0	0	0	1	1	0	0	0	1	3	1	3	0	0	0	6	4	0	0	0	0	0	0

Tabla 12. Resumen Final del análisis del riesgo - MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos			Redes de Comunicaciones			Soporte de Información		Equipamiento Auxiliar		Instalaciones		Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
18	Errores del administrador	4	0	4	0	0	0	0	0	0	0	1	1	1	2	2	2	3	0	0	0	3	2	0	0	0	0	0
19	Errores de configuración	2	0	0	0	0	1	0	0	0	1	0	0	0	0	3	3	3	0	0	0	3	2	0	0	0	0	0
20	Degradación de los soportes de almacenamiento de la información	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0
21	Difusión de software dañino	3	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	3	0	0	0	3	0	0	0	0	0	0
22	Errores de mantenimiento / actualización de programas (software)	2	0	0	0	0	1	0	0	3	1	3	3	3	1	9	9	9	0	0	0	3	0	0	0	0	0	0

Tabla 12. Resumen Final del análisis del riesgo - MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones		Soporte de Información		Equipamiento Auxiliar		Instalaciones	Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
23	Errores de mantenimiento / actualización de equipos (hardware)	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0
24	Caída del sistema por sobrecarga	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0
25	Denegación de servicio	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	Robo	6	0	0	0	0	0	0	0	0	0	0	0	0	0	2	3	3	0	0	0	0	0	0	0	0	0	0
27	Ataques destructivos	3	0	0	0	0	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	2	1	0	0	0	0	0
28	Extorsión	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	Ingeniería social	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	Manipulación de logs	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0

Tabla 12. Resumen Final del análisis del riesgo - MAGERIT

		Servicios					Datos			Aplicaciones						Equipos Informáticos				Redes de Comunicaciones			Soporte de Información		Equipamiento Auxiliar		Instalaciones		Personal	
	Amenaza	Respaldo	*PMS* en línea	Internet	Correo Institucional	Gestión del parque informático	Bases de datos físicas	Documentos Confidenciales	Documentos de Uso Interno	*PMS* local	Apache	Bases de datos digitales	Sistemas operativos	*Booking apps*	*WordPress*	*Desktops/Laptops*	Cámaras	Servidores	*Access points*	Red interna	Red *Wireless* huéspedes	*Drives* externos	Almacenamiento en Nube	Fuentes de alimentación	Generadores eléctricos	*Datacenter*	Gerente	Mantenimiento
31	Abuso de privilegios de acceso	2	2	2	4	0	3	0	0	0	0	6	4	4	0	0	0	6	0	0	0	2	1	0	0	0	0	0
32	Manipulación de equipos	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0
33	Manipulación de configuración	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	Alteración de la información	0	2	0	2	0	3	0	0	4	0	3	2	0	0	6	0	6	0	0	0	4	2	0	0	0	0	0

Fuente: El autor, en base a Metodología MAGERIT

3.1.4.5. Etapa 5: Determinar las salvaguardar ante el riesgo

Una vez obtenido el resumen final de la valoración del riesgo, se procede a la siguiente etapa de la metodología, en donde se establecen los controles a aplicar, aquí se establecen las siguientes defensas para mitigar los mencionados riesgos. Los controles se escogen según la norma

ISO/IEC 27002:2013, la cual define de manera general lo que se debe hacer para mitigar cada riesgo. La Tabla 13 resume según el activo, las amenazas a las que se enfrenta el mencionado activo, la vulnerabilidad (*i.e.* debilidad encontrada), y su respectivo control que ayuda en la mitigación, aplicado a los casos calificados como Alto y Mediano Riesgo, los cuales necesitan atención inmediata. Mismo caso en la Tabla 15, pero para los calificados como bajo riesgo, los cuales se pueden poner en menor prioridad de atención.

Tabla 13. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Alto y Mediano

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
Respaldo	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.2
	Desastres industriales	Falta de sistemas de protección	11.2.1
	Fuga de información	Falta de controles	9.4.1
	Indisponibilidad del personal	Falta de personal dedicado a la seguridad	7.2.2
	Agotamiento de recursos	Falta de previsión	12.1.3
	Errores de los usuarios	Falta de procedimientos documentados	12.1.1
	Denegación de servicio	Falta de plan de respuesta	16.1.1
PMS en línea	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.2
	Fallo de servicios de comunicaciones	Falta de redundancias	15.1.3
	Fuga de Información	Falta de controles	9.4.1

Tabla 13. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Alto y Mediano

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Errores de los usuarios	Falta de procedimientos documentados	12.1.1
Internet	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.2
	Fallo de servicios de comunicaciones	Falta de redundancias	15.1.3
	Fuga de Información	Falta de controles	9.4.1
Correo Institucional	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.2
	Fallo de servicios de comunicaciones	Falta de redundancias	15.1.3
	Fuga de Información	Falta de controles	9.4.1
Gestión del Parque Informático	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.1
Bases de datos físicas	Desastres industriales	Falta de sistemas de protección	11.2.1
	Fuga de información	Falta de controles	9.4.1
	Introducción de falsa información	Falta de controles	11.1.2
PMS local	Corrupción de la información	Falta de respaldos apropiados	11.1.2
Bases de datos digitales	Fuga de información	Falta de controles	9.4.1
	Indisponibilidad del personal	Falta de personal dedicado a la seguridad	7.2.2

Tabla 13. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Alto y Mediano

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Abuso de privilegios de acceso	Demasiados privilegios a usuarios	9.2.2
Sistemas operativos	Fuga de información	Falta de controles	9.4.1
	Indisponibilidad del personal	Falta de personal dedicado a la seguridad	7.2.2
Desktops/Laptops	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.2
	Fuga de información	Falta de controles	9.2.2
	Acceso no autorizado	Falta de controles	9.4.3
	Vulnerabilidad de programas	No se analizan aspectos de seguridad	14.1.1
	Corrupción de la información	Falta de respaldos apropiados	12.3.1
	Destrucción de la información	Falta de respaldos apropiados	12.3.1
	Interceptación de la información	Falta de controles	11.1.2
	Indisponibilidad del personal	Falta de personal dedicado a la seguridad	7.2.2
	Difusión de software dañino	Falta de controles	12.2.1
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4
	Alteración de la información	Falta de controles	11.1.2

Tabla 13. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Alto y Mediano

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
Cámaras	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.2
	Fuga de información	Falta de controles	9.4.1
	Acceso no autorizado	Falta de controles	9.4.3
	Vulnerabilidad de programas	No se analizan aspectos de seguridad	14.1.1
	Corrupción de la información	Falta de respaldos apropiados	12.3.1
	Destrucción de la información	Falta de respaldos apropiados	12.3.1
	Indisponibilidad del personal	Falta de personal dedicado a la seguridad	7.2.2
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4
Servidores	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.2
	Fallo de servicios de comunicaciones	Falta de redundancias	15.1.3
	Fuga de información	Falta de controles	9.4.1
	Vulnerabilidad de programas	No se analizan aspectos de seguridad	14.1.1
	Corrupción de la información	Falta de respaldos apropiados	12.3.1
	Destrucción de la información	Falta de respaldos apropiados	12.3.1

Tabla 13. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Alto y Mediano

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Indisponibilidad del personal	Falta de personal dedicado a la seguridad	7.2.2
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4
	Caída del sistema por sobrecarga	No se gestionan las capacidades	12.1.3
	Abuso de privilegios de acceso	Demasiados privilegios a usuarios	9.2.2
	Alteración de la información	Falta de controles	11.1.2
Access points	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.2
Drives externos	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.2
	Errores de los usuarios	Falta de procedimientos documentados	12.1.1
	Degradación de los soportes de almacenamiento de la información	No se dispone de plan de renovación	11.2.4
Fuentes de alimentación	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.2
Generadores eléctricos	Corte del suministro eléctrico	Falta de sistemas de protección	11.2.2

Fuente: El autor, en base a Metodología MAGERIT

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
Respaldo	Fuego	Falta de sistemas de protección	11.2.1
	Desastres naturales	Falta de sistemas de protección	11.2.1
	Condiciones inadecuadas de temperatura o humedad	Falta de sistemas de protección	11.2.1
	Fallo de servicio de comunicaciones	Falta de redundancias	15.1.3
	Acceso no autorizado	Falta de controles	9.4.3
	Vulnerabilidad de programas	No se analizan aspectos de seguridad	14.1.1
	Corrupción de la información	Falta de respaldos apropiados	12.3.1
	Destrucción de información	Falta de respaldos apropiados	12.3.1
	Errores de configuración	Falta de conocimiento	7.2.2
	Degradación de los soportes de almacenamiento de la información	No se dispone de plan de renovación	11.2.4
	Difusión de software dañino	Falta de controles	12.2.1
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Errores de mantenimiento / actualización de equipos (hardware)	No se da mantenimiento apropiado	11.2.4
	Caída del sistema por sobrecarga	No se gestionan las capacidades	12.1.3
	Ataques destructivos	No se tienen medidas apropiadas	5.1.1
	Abuso de privilegios de acceso	Demasiados privilegios a usuarios	9.2.2
PMS en línea	Introducción de falsa información	Falta de controles	9.2.2
	Interceptación de información	Credenciales compartidas	9.3.1
	Ingeniería social	Falta de conciencia sobre el tema	7.2.2
	Abuso de privilegios de acceso	Demasiados privilegios a usuarios	9.2.2
	Alteración de la información	Falta de controles	9.2.2
Internet	Acceso no autorizado	Falta de controles	9.4.3
	Abuso de privilegios de acceso	Demasiados privilegios a usuarios	9.2.2
	Manipulación de equipos	Falta de controles	11.1.3
	Manipulación de configuración	Falta de controles	9.4.3
	Alteración de la información	Falta de controles	9.2.2

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
Gestión del Parque Informático	Introducción de falsa información	Falta de controles	9.2.2
Correo Institucional	Acceso no autorizado	Falta de controles	9.4.3
	Alteración de la información	Falta de controles	9.2.2
Bases de datos físicas	Fallo de servicios de comunicaciones	Falta de redundancias	15.1.3
	Acceso no autorizado	Falta de controles	9.4.3
	Vulnerabilidad de programas	No se analizan aspectos de seguridad	14.1.1
	Corrupción de la información	Falta de respaldos apropiados	12.3.1
	Interceptación de información	Falta de mecanismos de protección	8.1.2
	Indisponibilidad del personal	Falta de asignación de roles y delegación	7.2.1
	Errores de configuración	Falta de conocimiento	7.2.2
	Degradación de los soportes de almacenamiento de la información	No se dispone de plan de renovación	11.2.4
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Manipulación de logs	Falta de controles	9.2.2
	Abuso de privilegios de acceso	Demasiados privilegios a usuarios	9.2.2
	Alteración de la información	Falta de controles	9.2.2
PMS local	Acceso no autorizado	Falta de controles	9.4.3
	Vulnerabilidad de programas	No se analizan aspectos de seguridad	14.1.1
	Destrucción de información	Falta de respaldos apropiados	12.3.1
	Interceptación de información	Credenciales compartidas	9.3.1
	Errores de los usuarios	Falta de procedimientos documentados	12.1.1
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4
Apache	Errores de los usuarios	Falta de procedimientos documentados	12.1.1
	Errores de configuración	Falta de conocimiento	7.2.2
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4
Bases de datos digitales	Introducción de falsa información	Falta de controles	9.2.2

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Acceso no autorizado	Falta de controles	9.4.3
	Vulnerabilidad de programas	No se analizan aspectos de seguridad	14.1.1
	Corrupción de la información	Falta de respaldos apropiados	12.3.1
	Interceptación de información	Credenciales compartidas	9.3.1
	Errores del administrador	Falta de conocimiento	7.2.2
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4
	Ataques destructivos	No se tienen medidas apropiadas	5.1.1
	Manipulación de logs	Falta de controles	9.2.2
	Alteración de la información	Falta de controles	9.2.2
Sistemas operativos	Introducción de falsa información	Falta de controles	9.2.2
	Acceso no autorizado	Falta de controles	9.4.3
	Vulnerabilidad de programas	No se analizan aspectos de seguridad	14.1.1
	Errores del administrador	Falta de conocimiento	7.2.2

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4
Booking apps	Introducción de falsa información	Falta de controles	9.2.2
	Acceso no autorizado	Falta de controles	9.4.3
	Interceptación de información	Falta de mecanismos de protección	9.3.1
	Indisponibilidad del personal	Falta de asignación de roles y delegación	7.2.1
	Errores del administrador	Falta de conocimiento	7.2.2
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4
WordPress	Indisponibilidad del personal	Falta de asignación de roles y delegación	7.2.1
	Errores de los usuarios	Falta de procedimientos documentados	12.1.1
	Errores del administrador	Falta de conocimiento	7.2.2
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4
Desktops/Laptops	Fuego	Falta de sistemas de protección	11.2.1

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Daños por agua	Falta de sistemas de protección	11.2.1
	Desastres naturales	Falta de sistemas de protección	11.2.1
	Desastres industriales	Falta de sistemas de protección	11.2.1
	Errores de los usuarios	Falta de procedimientos documentados	12.1.1
	Errores del administrador	Falta de conocimiento	7.2.2
	Errores de configuración	Falta de conocimiento	7.2.2
	Robo	Falta de mecanismos antirrobo	11.1.3
Cámaras	Fuego	Falta de sistemas de protección	11.2.1
	Daños por agua	Falta de sistemas de protección	11.2.1
	Desastres naturales	Falta de sistemas de protección	11.2.1
	Desastres industriales	Falta de sistemas de protección	11.2.1
	Interceptación de información	Falta de mecanismos de protección	11.2.4
	Agotamiento de recursos	Falta de previsión	12.1.3
	Errores de los usuarios	Falta de procedimientos documentados	12.1.1

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Errores del administrador	Falta de conocimiento	7.2.2
	Errores de configuración	Falta de conocimiento	7.2.2
	Robo	Falta de mecanismos antirrobo	11.1.3
	Ataques destructivos	No se tienen medidas apropiadas	5.1.1
Servidores	Fuego	Falta de sistemas de protección	11.2.1
	Daños por agua	Falta de sistemas de protección	11.2.1
	Desastres naturales	Falta de sistemas de protección	11.2.1
	Desastres industriales	Falta de sistemas de protección	11.2.1
	Acceso no autorizado	Falta de controles	9.4.3
	Interceptación de información	Falta de mecanismos de protección	9.3.1
	Agotamiento de recursos	Falta de previsión	12.1.3
	Errores de los usuarios	Falta de procedimientos documentados	12.1.1
	Errores del administrador	Falta de conocimiento	7.2.2
	Errores de configuración	Falta de conocimiento	7.2.2

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Difusión de software dañino	Falta de controles	12.2.1
	Robo	Falta de mecanismos antirrobo	11.1.3
	Manipulación de logs	Falta de controles	9.2.2
	Alteración de la información	Falta de controles	9.2.2
Access points	Fuego	Falta de sistemas de protección	11.2.1
	Daños por agua	Falta de sistemas de protección	11.2.1
	Desastres naturales	Falta de sistemas de protección	11.2.1
	Desastres industriales	Falta de sistemas de protección	11.2.1
Red Interna	Fuego	Falta de sistemas de protección	11.2.1
	Daños por agua	Falta de sistemas de protección	11.2.1
	Desastres naturales	Falta de sistemas de protección	11.2.1
	Desastres industriales	Falta de sistemas de protección	11.2.1
	Fallo de servicios de comunicaciones	Falta de redundancias	15.1.3
	Desastres industriales	Falta de sistemas de protección	11.2.1

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
Red *Wireless* huéspedes	Fuego	Falta de sistemas de protección	11.2.1
	Daños por agua	Falta de sistemas de protección	11.2.1
	Desastres naturales	Falta de sistemas de protección	11.2.1
	Desastres industriales	Falta de sistemas de protección	11.2.1
	Fallo de servicios de comunicaciones	Falta de redundancias	15.1.3
	Fuego	Falta de sistemas de protección	11.2.1
	Daños por agua	Falta de sistemas de protección	11.2.1
	Desastres naturales	Falta de sistemas de protección	11.2.1
	Desastres industriales	Falta de sistemas de protección	11.2.1
Drives externos	Fuga de información	Falta de controles	9.2.2
	Acceso no autorizado	Falta de controles	9.4.3
	Corrupción de la información	Falta de respaldos apropiados	12.3.1
	Destrucción de información	Falta de respaldos apropiados	12.3.1
	Indisponibilidad del personal	Falta de asignación de roles y delegación	7.2.1

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Agotamiento de recursos	Falta de previsión	12.1.3
	Errores de los usuarios	Falta de procedimientos documentados	12.1.1
	Errores del administrador	Falta de conocimiento	7.2.2
	Errores de configuración	Falta de conocimiento	7.2.2
	Difusión de software dañino	Falta de controles	12.2.1
	Errores de mantenimiento / actualización de programas (software)	No se actualizan los programas	11.2.4
	Errores de mantenimiento / actualización de equipos (hardware)	No se da mantenimiento apropiado	11.2.4
	Ataques destructivos	No se tienen medidas apropiadas	5.1.1
	Abuso de privilegios de acceso	Demasiados privilegios a usuarios	9.2.2
Almacenamiento en Nube	Fuga de información	Falta de controles	9.2.2
	Acceso no autorizado	Falta de controles	9.4.3
	Corrupción de la información	Falta de respaldos apropiados	12.3.1
	Destrucción de información	Falta de respaldos apropiados	12.3.1

Tabla 14. Controles de la norma ISO/IEC 27002 a aplicarse en la Política de Seguridad de la Información. Riesgo Bajo

Activo	Amenaza	Vulnerabilidad	Control ISO/IEC 27002:2013
	Agotamiento de recursos	Falta de previsión	12.1.3
	Errores del administrador	Falta de conocimiento	7.2.2
	Errores de configuración	Falta de conocimiento	7.2.2
	Ataques destructivos	No se tienen medidas apropiadas	5.1.1
	Abuso de privilegios de acceso	Demasiados privilegios a usuarios	9.2.2
	Alteración de la información	Falta de controles	9.2.2
Fuentes de alimentación	Fuego	Falta de sistemas de protección	11.2.1
	Daños por agua	Falta de sistemas de protección	11.2.1
	Desastres naturales	Falta de sistemas de protección	11.2.1
Generadores eléctricos	Fuego	Falta de sistemas de protección	11.2.1
	Daños por agua	Falta de sistemas de protección	11.2.1
	Desastres naturales	Falta de sistemas de protección	11.2.1

Fuente: El autor, en base a Metodología MAGERIT

Con lo dispuesto en la Tabla 13 y Tabla 15, se procede a la elaboración de la Política de Seguridad de la Información para los hoteles miembros de AHOTIM, tomando en cuenta sus particularidades descritas por los hoteles miembros y observadas en campo.

CAPÍTULO IV

PROPUESTA

Una vez establecidos lo controles a aplicar en la Política de Seguridad de la Información para los hoteles miembros de AHOTIM, se procede a presentar la siguiente propuesta.

1. Política de Seguridad de la Información para los hoteles miembros de AHOTIM

1.1. Objeto y campo de aplicación

La presente política de seguridad de la información establece los mecanismos de alto nivel que se deben implementar en los hoteles miembros de AHOTIM, con el fin de salvaguardar la información.

1.2. Referencias normativas

La presente política tiene como base la norma ISO/IEC 27002:2013, internacionalmente conocida como *Information technology - Security techniques – Code of practice for information security controls* (Disterer, 2013).

1.3. Definiciones

1.3.1. Seguridad de la información

Es la disciplina que indica metodologías, métodos, prácticas y técnicas que permiten proteger la información personal u organizacional, sea de factores internos o externos.

Gracias a ella, se puede mitigar el riesgo de pérdida o robo de información, que afectaría a la potencial víctima (Bertolín, 2008).

1.3.2. Confidencialidad, Integridad y Disponibilidad

Son los pilares críticos de la seguridad de la información (Bertolín, 2008). Sin la debida atención a estos tres aspectos, la información puede ser gravemente comprometida (Disterer, 2013).

Confidencialidad se refiere a la privacidad de la información, dejando claro que sólo debe ser accedida por quienes realmente deben hacerlo, y no por otras entidades (Disterer, 2013).

Integridad se refiere a la cualidad de no ser alterada, inconsistente o duplicada. Los datos que componen la información deben estar completos y probar su integridad para no ser repudiados (INCIBE, 2015).

Disponibilidad se refiere a la cualidad de la información de estar presente cuando y en donde es necesaria. La información debe estar disponible para su uso en el momento y lugar necesarios (INCIBE, 2015).

1.3.3. Riesgo

Es un aspecto latente que puede suceder y afectar a un sistema debido a una vulnerabilidad (Bertolín, 2008).

1.3.4. Vulnerabilidad

Es una debilidad que conlleva el sistema, y puede ser aprovechada por entidades dentro y fuera de la organización para causar cualquier clase de perjuicio (Bertolín, 2008). Cuando la vulnerabilidad es aprovechada, se está enfrentando a un ataque.

1.3.5. Ataque

Es el aprovechamiento de una vulnerabilidad por parte de un actor interno o externo al entorno del sistema (Paulsen C., 2019).

1.3.6. Incidente

Es la ocurrencia de un evento en donde se compromete uno o varios de los pilares de la seguridad de la información (Bertolín, 2008), y que tiene un actor intencionado detrás del mismo.

1.3.7. Accidente

Es cuando ocurre un evento de seguridad informática de manera involuntaria y sin un actor malintencionado detrás del mismo.

1.4. Abreviaturas

- AHOTIM: Asociación Hotelera de Imbabura
- TIC: Tecnologías de la Información y comunicación
- TI: Tecnologías de la Información
- CIA: Confidencialidad Integridad Disponibilidad
- ISO: *International Organisation for Standarisation*
- IEC: *International Electrotechnical Commission*
- *SLA: Service Level Agreement*
- *PMS: Property Management System*

1.5. Política de seguridad

1.5.1. Objetivo

Establecer las directrices que garanticen la protección de la información en los hoteles miembros de AHOTIM, a través de la aplicación de controles de normas estándar internacionalmente reconocidos para el efecto.

1.5.2. Responsables

Para garantizar la correcta aplicación de la presente política, se designan los siguientes responsables:

Tabla 15. Responsabilidades de los actores involucrados

Dignidad	Responsabilidades
Presidente de AHOTIM	Aprobación y socialización de la política de seguridad de la información
Secretario de AHOTIM	Socializar la política de seguridad de la información
Gerente general de cada hotel	Recibir la política y aplicarla en su establecimiento
TI de cada hotel	Implantar los mecanismos descritos en la política de seguridad de la información
Trabajadores de cada hotel	Cumplir con la política de seguridad de la información

Elaborado por: El autor

1.5.3. Riesgo

Luego del análisis pertinente, se han encontrado los siguientes riesgos y controles que ayudará a mitigar dichos riesgos:

Tabla 16. Riesgo a mitigar y control escogido

Descripción del riesgo	Control ISO/IEC 27002:2013
Activos en lugares inadecuados, desprotegidos o a fácil alcance de agentes maliciosos	11.2.1

Tabla 16. Riesgo a mitigar y control escogido

Descripción del riesgo	Control ISO/IEC 27002:2013
Activos sin alimentación ininterrumpida, que, al cesar su funcionamiento, comprometen la continuidad del negocio	11.2.2
Activos al alcance de posibles agentes maliciosos, sin seguridad física o vigilancia, montados en la recepción u otros lugares no adecuados. Entrada prácticamente libre para cualquier persona. Llaves en armarios de informática	11.1.2
Activos fáciles de copiar, fotografiar o sustraer. Equipos desatendidos y sin bloquear. Llaves en cajoneras	11.1.3
Falta de mantenimiento a activos. Falta de licencias que permitan la actualización de estos. Falta de mantenimiento preventivo (i.e. sólo se realiza correctivo)	11.2.4
Falta de conciencia sobre importancia y seguridad de la información de huéspedes, clientes, proveedores, etc. Configuraciones estándar en los activos, sin pensar en la seguridad de la información	7.2.2
Todo activo se deduce como responsabilidad de TI, aunque fuere otro el caso. No se especifica responsables de manera escrita	7.2.1
Activos sobrecargados que no garantizan servicio. Unidades llenas en las que se sobrescribe sin criterio técnico. Almacenamiento en nube con capacidades limitadas (e.g. cuentas gratuitas)	12.1.3
Deficiencia de documentación sobre activos. Pocos y pobres manuales de operación. Falta de registro sobre procedimientos (e.g. respaldos, guardado de unidades, traslado de unidades, etc.)	12.1.1
Contratos de adhesión firmados sin revisión alguna. Falta de métodos alternativos de operación.	15.1.3
Proceso de copias de seguridad algo deficiente. No se hacen copias de seguridad con la regularidad establecida. Respaldos de información según criterio de personal no capacitado en seguridad informático.	12.3.1
Falta de software antimalware. Software irrelevante instalado en equipos. Firewalls desactivados intencionalmente. Falta de licencias, lo que impide las actualizaciones de seguridad.	12.2.1
Información al alcance de posibles agentes maliciosos. Permisos que exceden las necesidades reales de cada usuario. Activos expuestos (i.e. revelando marca, modelo, uso, etc.)	9.4.1
Permisos que exceden las necesidades reales de cada usuario. Existencia de super usuarios. Credenciales compartidas entre usuarios.	9.2.2
Credenciales compartidas entre usuarios. Contraseñas débiles. Contraseñas iguales al nombre de usuario. Credenciales que nunca	9.4.3

Tabla 16. Riesgo a mitigar y control escogido

Descripción del riesgo	Control ISO/IEC 27002:2013
caducan. Credenciales activas para trabajadores separados de la organización. Credenciales escritas y expuestas cerca de los activos.	
Falta de responsables designados en caso de incidente. Falta de planes de acción en caso de incidente.	16.1.1
Falta de política de seguridad de la información. Los incidentes se gestionan sin plan de acción. Los incidentes son atendidos por personal bien intencionado, pero poco capacitado.	5.1.1

Elaborado por: El autor

1.5.4. Desarrollo

A continuación, se describen los elementos que componen la política de seguridad de la información para los hoteles miembros de AHOTIM.

Tabla 17. Seguridad física y ambiental

Dominio	Seguridad física y ambiental
Objetivo de dominio	Asegurar el bienestar de los activos y su oportuna operación
Control ISO/IEC 27002:2013	11.2.1
Objetivo de control	Asegurar que los equipos informáticos estén debidamente protegidos
Activos a proteger	• Respaldo • Gestión del parque informático • Bases de datos físicas • *Desktops/Laptops* • Cámaras • Servidores • *Access points* • Red interna • Red *Wireless* huéspedes • *Drives* externos • Fuentes de alimentación • Generadores eléctricos
a. Los equipos informáticos estarán ubicados en un lugar seguro, protegidos de los posibles desastres industriales que pudieran ocurrir en el hotel.	

Tabla 17. Seguridad física y ambiental

<table>
<tr><td colspan="2">b. Los equipos estarán ubicados en un puesto designado, y no saldrán de él sin justificación por escrito del Gerente general.
c. Las cámaras estarán ubicadas en un lugar seguro, lejos de posibles interferencias físicas o lógicas, apuntando a los activos a proteger.
d. Los servidores residirán en armarios bajo llave, la cual estará protegida en la caja fuerte del hotel y será de uso exclusivo de TI y Gerencia.
e. Los equipos que componen las redes estarán lejos del fácil alcance de personal, huéspedes o visitantes.
f. Los drives externos que contienen los respaldos residirán diariamente en la caja fuerte del hotel, y trasladados a caja fuerte del banco al final de cada 6 meses.
g. Las fuentes de alimentación estarán ubicadas lejos del alcance de personal no autorizado.
h. Los generadores eléctricos residirán en el cuarto de máquinas, y estarán protegidos por seguridades físicas como protecciones metálicas, candados, etc.</td></tr>
<tr><td>Responsables</td><td>• Gerente general
• TI
• Seguridad del hotel</td></tr>
<tr><td>Control ISO/IEC 27002:2013</td><td>11.2.2</td></tr>
<tr><td>Objetivo de control</td><td>Asegurar que haya energía eléctrica y otras condiciones que permitan la operación ininterrumpida de los activos</td></tr>
<tr><td>Activos a proteger</td><td>• Respaldo
• PMS en línea
• Internet
• Correo institucional
• Desktops/Laptops
• Cámaras
• Servidores
• Access points
• Drives externos
• Fuentes de alimentación
• Generadores eléctricos</td></tr>
<tr><td colspan="2">a. Existirán sistemas de alimentación ininterrumpida (UPS) para todos los equipos informáticos y de seguridad.
b. Existirán generadores de electricidad que alimenten a los equipos informáticos.
c. Todos los equipos informáticos y de seguridad estarán conectados a una fuente ininterrumpida de alimentación mientras está en operación.</td></tr>
<tr><td>Responsables</td><td>• Gerente general
• TI</td></tr>
</table>

Tabla 17. Seguridad física y ambiental

	• Mantenimiento
Control ISO/IEC 27002:2013	11.1.2
Objetivo de control	Asegurar que agentes maliciosos no tengan acceso físico a los activos
Activos a proteger	• Bases de datos físicas • *PMS* local • *Desktops/Laptops* • Servidores
a. Se garantizará el acceso únicamente al personal autorizado para manejar o manipular equipos informáticos del hotel. Toda otra persona queda terminantemente prohibida de manipularlos. b. Habrá vigilancia y métodos disuasivos en las áreas restringidas, tales como cámaras de seguridad y avisos de "no tocar". c. Las personas externas no podrán ingresar con equipos informáticos a las áreas restringidas, salvo autorización expresa por escrito del Gerente general, con aprobación motivada de TI. d. Se llevará una bitácora registrada y firmada, que será responsabilidad de seguridad del hotel. En ésta, constará nombre, número de cédula y firma de quien ingresa al área restringida, sea quien fuere. e. La información impresa residirá en archivadores bajo llave y nunca sobre el escritorio de trabajador alguno.	
Responsables	• Gerente general • Seguridad • TI
Control ISO/IEC 27002:2013	11.1.3
Objetivo de control	Asegurar que los activos no estén a vista y alcance de agentes maliciosos
Activos a proteger	• Internet • *Desktops/Laptops* • Cámaras • Servidores
a. Los equipos informáticos no residirán a fácil alcance de personal no autorizado. b. Se utilizarán anclajes de seguridad en todos los equipos que admitan esta característica. c. No se dejarán desatendidos los equipos, y se bloquearán cada vez que el usuario abandone la presencia de este. d. Existirán cámaras de seguridad apuntando a los activos a proteger. e. Los servidores residirán en armarios apropiados, que posean características de seguridad física como paneles metálicos, candados, accesos biométricos, etc.	

Tabla 17. Seguridad física y ambiental

<table>
<tr><td colspan="2">f. No se permitirá el ingreso de personal no autorizado. Toda persona ajena al parea será recibida en la Recepción del hotel. Si debe ingresar, lo hará firmando en una bitácora mantenida por Seguridad, tomando datos de nombre, número de cédula, propósito y firma.</td></tr>
<tr><td>Responsables</td><td>• Gerente general
• Seguridad
• TI
• Mantenimiento</td></tr>
<tr><td>Control ISO/IEC 27002:2013</td><td>11.2.4</td></tr>
<tr><td>Objetivo de control</td><td>Asegurar que se haga el mantenimiento preventivo y correctivo a los activos</td></tr>
<tr><td>Activos a proteger</td><td>• Bases de datos físicas
• PMS local
• Apache
• Bases de datos digitales
• Sistemas operativos
• Booking apps
• WordPress
• Drives externos</td></tr>
<tr><td colspan="2">a. Habrá presupuesto para mantenimiento, reparación y renovación de equipos informáticos. Esto se hará mediante provisiones presupuestarias.
b. Se adquirirán licencias de software de protección de la información, tales como programas de respaldo, software antimalware, etc.
c. El mantenimiento será hecho por TI o un proveedor externo que garantice el servicio mediante contrato escrito.
d. Se actualizarán los elementos de protección a los equipos, tan frecuentemente como sea posible por parte de TI, al menos una vez cada 6 meses.
e. Se actualizará el software de manera periódica, buscando actualizaciones por lo menos una vez al mes.
f. Se hará comprobación del estado de drives externos de forma mensual y antes de enviar al banco, y se tomará cualquier medida correctiva o reemplazo en ese momento.</td></tr>
<tr><td>Responsables</td><td>• Gerente general
• TI
• Mantenimiento</td></tr>
</table>

Elaborador por: El autor

Tabla 18. Seguridad ligada a los recursos humanos

Dominio	Seguridad ligada a los recursos humanos
Objetivo de dominio	Involucrar a todo el personal en la cultura de seguridad de la información
Control ISO/IEC 27002:2013	7.2.2
Objetivo de control	Capacitar a los usuarios de la manera más adecuada para proteger los activos
Activos a proteger	• Respaldo • *PMS* en línea • Bases de datos físicas • Apache • Bases de datos digitales • Sistemas operativos • *Booking apps* • *WordPress* • *Desktops/Laptops* • Cámaras • Servidores • *Drives* externos • Almacenamiento en Nube
a. Habrá presupuesto y tiempo dedicado para la capacitación adecuada a los usuarios finales. Esto se hará con presupuesto indicado para capacitación. b. La capacitación en seguridad de la información será de carácter obligatorio para todos los trabajadores, y se hará con frecuencia de al menos una vez al año. c. Las capacitaciones serán conducidas por personal calificado en el área de seguridad de la información, sea interno o externo, y se dará certificado de aprobación.	
Responsables	• TI • Gerente general • Todos los trabajadores

Tabla 18. Seguridad ligada a los recursos humanos

Control ISO/IEC 27002:2013	7.2.1
Objetivo de control	Asignar responsabilidades
Activos a proteger	• Bases de datos físicas • *Booking apps* • *WordPress* • *Drives* externos
a. Se asignarán roles y responsabilidades a los trabajadores, tomando en cuenta que el personal puede ausentarse por cualquier motivo y que sus responsabilidades puedan ser cubiertas por otra persona. b. Las responsabilidades se asignarán al personal más capacitado para la tarea, o en su defecto se enviará a capacitación a la persona más idónea para el caso. c. Los proveedores de servicios, dentro de lo posible, dejarán claves de acceso a los activos, en caso de que se requiera cambiar de proveedor o éste último dejara de existir.	
Responsables	• Gerente general • TI • Todos los trabajadores

Elaborado por: El autor

Tabla 19. Seguridad en la operativa

Dominio	Seguridad en la operativa
Objetivo de dominio	Asegurar la operación de los activos
Control ISO/IEC 27002:2013	12.1.3
Objetivo de control	Asegurar que los activos y procedimientos no se detengan por falta de recursos
Activos a proteger	• Respaldo • Servidores • Cámaras • *Drives* externos • Almacenamiento en Nube
a. TI hará el respectivo monitoreo de las cuotas disponibles para respaldo de la información, informando a tiempo por escrito a Gerencia, y solicitando la adquisición o 11.2.4 involucrados. b. TI hará el monitoreo de capacidades en los servidores, y buscará soluciones preventivas ante los cuellos de botella y caída de servicios, informando por escrito a Gerencia con anticipación, para la respectiva provisión y desembolso. c. TI vigilará el buen estado de hardware, software y firmware de las cámaras de seguridad, asegurando que funcionen oportunamente en caso de un evento.	

Tabla 19. Seguridad en la operativa

<table>
<tr><td colspan="2">d. TI informará de drives externos llenos para que Gerencia coordine su envío a caja fuerte del banco.
e. TI monitoreará las capacidades del almacenamiento en nube, e informará por escrito con anticipación a Gerencia, para la provisión y desembolso que asegure más espacio de almacenamiento.</td></tr>
<tr><td>Responsables</td><td>• TI
• Gerente general</td></tr>
<tr><td>Control ISO/IEC 27002:2013</td><td>12.1.1</td></tr>
<tr><td>Objetivo de control</td><td>Documentar adecuadamente los procedimientos, especialmente los de seguridad</td></tr>
<tr><td>Activos a proteger</td><td>• Respaldo
• PMS en línea
• Drives externos</td></tr>
<tr><td colspan="2">a. Habrá manuales escritos de operación de los sistemas, aprobados con firma por TI y Gerencia.
b. La gestión del respaldo se describirá de manera escrita y firmada, con bitácora de eventos que aseguren la trazabilidad de este.
c. La gestión del PMS en línea será descrita en forma de manual de operación y entregada con firma de responsabilidad a cada usuario de este.
d. El manejo de los drives externos y su envío fuera de las premisas del hotel será documentado por escrito, asegurando la trazabilidad de su contenido y ubicación actual en todo momento.
e. Se capacitará al personal sobre el uso de los sistemas informáticos, por lo menos una vez al año, para reducir el cometimiento de errores. Esto se reflejará en un acta firmada tanto por el capacitador como por el capacitado.</td></tr>
<tr><td>Responsables</td><td>• TI
• Gerencia
• Todos los trabajadores</td></tr>
</table>

Tabla 19. Seguridad en la operativa

Control ISO/IEC 27002:2013	15.1.3
Objetivo de control	Asegurar el servicio prestado por proveedores
Activos a proteger	• Respaldo • Bases de datos físicas • Red Interna • Red *Wireless* huéspedes • *PMS* en línea • Internet • Correo institucional • Servidores
a. Se conocerá y se hará respetar el *Service Level Agreement* (SLA) que se tiene con los proveedores de software como servicio, tales como los *Property Management Systems* (*PMS).* b. Se conocerá y se hará respetar el SLA que se tiene con los proveedores de servicio de Internet. c. Las bases de datos físicas tendrán su equivalente en digital. d. Habrá equipos de respaldo para asegurar servicios críticos, éstos estarán configurados y en espera para actuar en el momento necesario. Se hará un chequeo de estos cada 6 meses. e. Habrá una lista de proveedores de Internet en espera, para el caso de que se requiera sus servicios con urgencia, o cambio inmediato de proveedor. Esta lista será elaborada y actualizada por TI cada 6 meses y aprobada por Gerencia.	
Responsables	• TI • Gerencia

Tabla 19. Seguridad en la operativa

Control ISO/IEC 27002:2013	12.3.1
Objetivo de control	Asegurar que haya respaldos oportunos
Activos a proteger	• Respaldo • *Desktops/Laptops* • Cámaras • Servidores • Bases de datos físicas • *PMS* local • Bases de datos digitales • *Drives* externos • Almacenamiento en Nube
a. Se realizarán respaldos de forma periódica, por lo menos una vez por semana. Las tareas automatizadas se verificarán manualmente al menos una vez por semana. b. Habrá presupuesto para la realización de los respaldos de la información que sean necesarios para garantizar la debida operación del hotel. c. Se harán respaldos de la información contenida en las estaciones de trabajo, servidores, cámaras, configuraciones de equipos, etc. mediante cualquier método indicado por TI. Estos respaldos residirán en los d*rives* externos asignados para el efecto. d. Las bases de datos físicas serán escaneadas y respaldadas digitalmente. e. La información de los sistemas de reservas en línea será copiada mediante reportes descargables y respaldada en las unidades asignadas para el efecto. f. El almacenamiento en nube tendrá su equivalente local y viceversa.	
Responsables	• TI • Gerencia

Tabla 19. Seguridad en la operativa

Control ISO/IEC 27002:2013	12.2.1
Objetivo de control	Proteger activos contra amenazas de software
Activos a proteger	• *Desktops/Laptops* • Respaldo • Servidores • *Drives* externos
a. Habrá presupuesto para la adquisición de software antimalware y demás mecanismos de protección contra software malicioso. b. Se prohibirá la instalación de software por parte de los usuarios finales. Esto lo hará y verificará TI mensualmente para afianzar la seguridad de la información. c. Se prohibirá la desactivación del software de seguridad por cualquier motivo. d. Los archivos se compartirán mediante correo electrónico, salvo casos especiales que requieran lo contrario. De ser el caso, TI velará por la seguridad de los activos, realizando escaneos y limpieza de los dispositivos. e. Los servidores contarán siempre con software antimalware licenciado, actualizado y activo. f. Los respaldos serán escaneados por malware una vez por semana. g. Los d*rives* externos serán escaneados por malware antes de cada envío a la caja fuerte del banco.	
Responsables	• Gerente • TI • Usuarios finales

Elaborado por: El autor

Tabla 20. Control de accesos

Dominio	Control de accesos
Objetivo de dominio	Asegurar que la confidencialidad y disponibilidad de la información
Control ISO/IEC 27002:2013	9.4.1
Objetivo de control	Asegurar que la información sea accedida sólo por quienes realmente deban hacerlo
Activos a proteger	• Todos
a. La información de los activos será conocida sólo por quienes estén autorizados por Gerencia y TI para su conocimiento. b. No se dará acceso con permisos más allá de lo estrictamente necesario para ningún activo. c. No se divulgarán detalles de ubicación, uso, contenido, etc. sobre ningún activo. d. Los activos se confiarán para reubicación o traslado, solamente al personal autorizado expresamente por TI y Gerencia.	

Tabla 20. Control de accesos

Responsables	• TI • Gerente general • Todos los trabajadores
Control ISO/IEC 27002:2013	9.2.2
Objetivo de control	Limitar permisos a los usuarios para que sólo puedan hacer lo que realmente deban hacer
Activos a proteger	• Respaldo • Bases de datos digitales • *Desktops/Laptops* • Servidores • *PMS* en línea • Internet • Bases de datos físicas • *Drives* externos • Almacenamiento en nube
a. Los usuarios de cualquier activo tendrán solamente los permisos necesarios para ejecutar su trabajo en específico, y no más. b. No habrá súper usuarios con acceso ilimitado a todas las características del activo. c. Los activos contarán con cuentas diferentes para cada usuario, en donde sea posible aplicar.	
Responsables	• Gerencia • TI • Todos los trabajadores
Control ISO/IEC 27002:2013	9.4.3
Objetivo de control	Reforzar la seguridad de las contraseñas
Activos a proteger	• *Desktops/Laptops* • Cámaras • Respaldo • Internet • Correo institucional • Bases de datos físicas • *PMS* local • Bases de datos digitales • Sistemas operativos • *Booking apps* • Servidores • *Drives* externos • Almacenamiento en Nube

Tabla 20. Control de accesos

a. Se establecerán passwords seguros con combinación de caracteres alfabéticos y numéricos. b. Los passwords serán únicos para cada usuario. c. Los passwords no serán iguales al nombre de usuario. d. Los passwords son individuales y confidenciales, no se pueden compartir bajo ninguna circunstancia. e. Es responsabilidad de cada usuario proteger su password y que no le sea sustraído. f. En caso de incidente que involucre credenciales, el dueño de las credenciales será responsable, al menos en parte, por la afectación causada. g. Las claves y pines de los dispositivos de seguridad física también serán considerados passwords. h. Las credenciales serán revocadas al momento en que un trabajador sea separado de la organización por cualquier motivo.	
Responsables	• Todos los trabajadores

Elaborado por: El autor

Tabla 21. Gestión de incidentes en la seguridad de la información

Dominio	Gestión de incidentes en la seguridad de la información
Objetivo de dominio	Asegurar que los incidentes en materia de seguridad de la información sean gestionados de manera oportuna
Control ISO/IEC 27002:2013	16.1.1
Objetivo de control	Establecer responsables de seguridad
Activos a proteger	• Todos
a. Se establecerán responsabilidades ante los incidentes de seguridad de la información, mediante la elaboración e implementación de un plan de acción y respuesta en el que se involucre a todos los trabajadores y tengan responsabilidades asignadas.	
Responsables	• TI • Gerente general • Todos los trabajadores

Elaborado por: El autor

Tabla 22. Políticas de seguridad

Dominio	Políticas de seguridad
Objetivo de dominio	Asegurar que existan, se cumplan y revisen políticas de seguridad de la información
Control ISO/IEC 27002:2013	5.1.1
Objetivo de control	Institucionalizar la política de seguridad de la información

Tabla 22. Políticas de seguridad

Activos a proteger	• Todos
a. Se conocerá, socializará y aplicará esta política de seguridad. b. La política de seguridad será actualizada cada año, a partir de un análisis de riesgo así mismo ejecutado anualmente. c. La política será aprobada por AHOTIM de forma general, y podrá ser complementada por cada hotel en particular, considerando sus especificidades. d. La política será desarrollada y actualizada por profesionales con conocimiento certificado en Seguridad de la información.	
Responsables	• Todos los trabajadores

Elaborado por: El autor

Finalmente, esta política se actualizará de manera anual, con el apoyo de los departamentos de TI de cada hotel miembro, será aprobada por AHOTIM mediante firma de su presidente, y se socializará a todos los miembros mediante reunión o canales electrónicos.

CONCLUSIONES

- El levantamiento de la información mediante entrevistas y observación de campo, juntamente con la aplicación de la metodología MAGERIT, y la investigación de otros trabajos realizados, permitió la adecuada selección de controles de la norma ISO/IEC 27002:2013 que se adaptan a la realidad y necesidades de los actores objeto de este estudio.
- El presente trabajo fue posible gracias a la meticulosa y precisa disposición de la norma ISO/IEC 27002:2013, la cual permitió un acertado análisis del estado actual y riesgo al que están expuestos los hoteles miembros de AHOTIM, en cuanto a seguridad de la información se refiere.
- Los controles escogidos corresponden a un estándar internacional (*i.e.* ISO/IEC 27002:2013), por lo cual existen definiciones universalmente aceptadas que no se prestan para malas interpretaciones o ambigüedades, lo cual facilita su entendimiento e implementación por parte de los involucrados.
- Los hoteles miembros de AHOTIM, minimizan el riesgo de seguridad de la información, pensando que, por ser empresas relativamente pequeñas, están a salvo de atacantes internos o externos, sin embargo, son ellos mismos quienes registran robo de información de negocio y lo toman como gaje del oficio, sin despertar conciencia de la pérdida que esto significa, y aceptando el riesgo como algo natural del giro del negocio.
- La aplicación de normas y metodologías probadas hizo que el trabajo sea ordenado y preciso, ahorrando tiempo y recursos en la elaboración de la política de seguridad.

RECOMENDACIONES

- Aplicar la política propuesta en los hoteles miembros de AHOTIM y desarrollar trabajos similares en otros entornos. Lo recogido en este trabajo, puede servir como base para la elaboración de políticas de seguridad en ámbitos asociados al hotelería.
- Sin el apoyo de las máximas autoridades de cada organización, las políticas de seguridad quedan en papel y no se aplican en el quehacer diario. Se recomienda conseguir el apoyo, no sólo de TI, sino de la gerencia general, o en este caso, de la presidencia de una asociación.
- Una política de seguridad de la información que no se refuerza constantemente, corre el peligro de quedar obsoleta o inaplicable. Se recomienda una actualización periódica y realista conforme a la realidad de la organización.

BIBLIOGRAFÍA

Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, *24*(7), 991–1010.

Bertolín, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Paraninfo.

Cobanoglu, C., & Demicco, F. J. (2007). To be secure or not to be: Isn't this the question? A critical look at hotel's network security. *International Journal of Hospitality & Tourism Administration*, *8*(1), 43–59.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 92–100.

Garavito, R. (2015). *Análisis y gestión de riesgo de la información en los sistemas de información misionales de una entidad del estado*. Bogotá.

Guayta, T. & I. K. (2009). *Propuesta de políticas de seguridad de la información para la CORPAIRE*. Escuela Politécnica Nacional.

Höne, K., & Eloff, J. H. P. (2012). Information security policy—what do international information security standards say? *Computers & Security*, *21*(5), 402–409.

Humphreys, E. (2011). Information Security Management System Standards. *Datenschutz Und Datensicherheit*, 7–11.

INCIBE. (2015). *Gestión de riesgos - Una guía de gestión para el empresario* (pp. 1–28).

pp. 1–28. Retrieved from https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf

Magalhães, M. J., de Magalhães, S. T., Revett, K., & Jahankhani, H. (2016). A Review on Privacy Issues in Hotels: A Contribution to the Definition of Information Security Policies and Marketing Strategies. *GOVCOPP, Universidade de Aveiro*, 205–2017. Aveiro.

Martínez, J., Majó, J., & Casadesús, M. (2012). El uso de las tecnologías de la información en el sector hotelero. *Proceedings of the VI Congress TURITEC: Turismo y Tecnologias de La Información y Las Comunicaciones*, *22*(1).

Mendez, A., Mesa, J., Zapico, F., & Guerreo, V. (2003). *Techno-Legal Aspects of Information Society and New Economy: an Overview* (p. 187). p. 187. Retrieved from http://mario.elinos.org.mx/publication/papers/2003/002.pdf

MENTOR. (n.d.). Normas ISO sobre gestión de seguridad de la información. Retrieved October 10, 2019, from http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

MHAP. (2012). MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Retrieved October 18, 2019, from https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

MTC-Qatar. (2018). Security Guidelines for Hotel Information Systems. Retrieved from https://qcert.org/sites/default/files/public/documents/security_guidelines_for_hotel_information_systems_eng_v1.0.pdf

Muradas, I. M., & Rodríguez, J. R. O. (2010). Benchmarking Interno En Una Central De Compras De Agencias De Viajes. *Cuadernos de Turismo*, (26), 177–199.

Orozco, C. (2019). *Entrevista a Señor Presidente de AHOTIM*. Ibarra.

Paulsen C., B. R. (2019). NISTIR 7298 Rev. 3. Retrieved from https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final

Salazar, C. (2020). *Entrevista a Señor Presidente (Subrogante) de AHOTIM*. Ibarra.

Santillán, G. et al. (2011). Los sistemas informáticos de gestión hotelera y los beneficios de su implementación. *TURyDES*, *4*(11). Retrieved from http://www.eumed.net/rev/turydes/11/sio.html

Shabani, N. (2017). *A study in Cyber-Security in hospitality industry - Threats and countermeasures: Case study in Reno, Nevada*. Sarasota.

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL*, *28*(5), 492–507.

Valdéz, J. (1988). *Contratos, riesgos y seguros informáticos*. México D.F.: UNAM.

Vieites, Á. G. (2011). *Enciclopedia de la seguridad informática*. Grupo Editorial RA-MA.

ANEXOS

Anexo 1: Controles de la Norma ISO/IEC 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en teonologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

Iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta. Octubre-2013

Anexo 2: Guía para la entrevista para el levantamiento de la información (Exploración inicial y concienciación)

Por favor, conteste de la manera más honesta posible, con una "X", Si o No, acerca de las siguientes preguntas relacionadas con la seguridad de la información en su hotel.

	Pregunta	Si	No
1	¿Dispone su hotel de una política de seguridad de la información?		
2	¿En su hotel se aplican principios, métodos, técnicas, etc., acerca de seguridad de la información?		
3	¿Su hotel considera importante el manejo de la información? (clientes, huéspedes, habitaciones)		
4	¿Su hotel ha sufrido robo o pérdida de información?		
5	¿Su hotel maneja información a través de un sistema?		
6	¿Su sistema está protegido con nombres de usuario y contraseñas individuales?		
7	Cuándo un trabajador termina su relación laboral con su hotel, ¿Se le revocan los permisos del sistema inmediatamente?		
8	¿Su hotel cuenta con software antivirus, antimalware, etc.?		
9	¿Su hotel tiene cláusulas contractuales sobre el manejo de la información?		
10	¿Le parece importante implementar mecanismos de seguridad de la información en su hotel?		
11	¿Hace respaldos de la información del sistema de su hotel?		
12	¿Perder la información del sistema informático, sería catastrófico para su hotel?		
13	¿Desecha los equipos informáticos en base a alguna norma que asegure la destrucción total de la información contenida?		

Por favor, conteste de la manera más honesta posible, con una “X”, en una escala de 0 a 5, donde 0 significa nulo (o nunca) y 5 es la calificación más alta posible (o alta frecuencia, diaria), acerca de las siguientes preguntas relacionadas con la seguridad de la información en su hotel.

	Pregunta	**0**	**1**	**2**	**3**	**4**	**5**
14	¿Qué tan importante considera la información en su empresa?						
15	¿Qué tan importante es que su personal no divulgue información de sus clientes, huéspedes, habitaciones, etc.?						
16	¿Qué tan frecuentemente hace el cambio de contraseñas?						
17	¿Qué tan frecuentemente hace actualizaciones de seguridad al sistema?						
18	¿Qué tan frecuentemente actualiza el software antivirus, antimalware, etc.?						
19	¿Qué tan frecuentemente sospecha que alguien ha robado información de su hotel?						
20	¿Qué tan frecuentemente sospecha que alguien ha divulgado de manera no permitida, información de su hotel?						
21	¿Qué tan frecuentemente respalda la información del sistema de su hotel?						

Christian Estrada

Entrevistador