TRABAJO DE GRADO

Opción Seminario.

Título del trabajo

Informe Técnico de Ciberseguridad – HOTEL GRAN MIRADOR & CONVENTION CENTER S.A.S

Corporación Universitaria Remington.

Nombre de la facultad: Ingenierías

Nombre del programa académico: Ingeniería de Sistemas

Nombres de los estudiantes autores del trabajo de grado.

Cristancho Santana Angel Heriberto

Jorge Leonardo Ramírez Restrepo - docente del seminario.

Seminario

2026

Tabla de Contenidos

Resumen

Este documento representa la realización de un Informe Técnico de Ciberseguridad realizado a la entidad que lleva por nombre, Hotel Gran Mirador & Convention Center S.A.S. empresa regional que por más de 12 años se ha consolidado por estar dedicada principalmente a la prestación de servicios de hospedaje, reuniones o eventos corporativos, turismo de negocios y actividades recreativas. Siendo una organización que cuenta con una gran variedad servicios como habitaciones, contando con 220 de ellas para ofrecer a sus clientes y nuevos visitantes, además de 8 salones para eventos empresariales, zonas recreativas, gimnasio y servicios complementarios para huéspedes nacionales e internacionales.

Se identifica la organización porque cuenta con una estructura organizacional y una infraestructura tecnológica, donde en estas dos se desarrollan diferentes procesos, con el propósito común, que es el de gestionar adecuadamente la prestación de los servicios antes mencionados y fortalecer el crecimiento económico de la organización.

En el Hotel Gran Mirador & Convention Center S.A.S. Se identifica una problemática en sus colaboradores con respecto a la seguridad de la información, donde el manejo se cree que solo está bajo la responsabilidad del área de tecnología, o sea de 5 personas, (1 coordinador de TIC, 2 analista de infraestructura y dos técnicos de soportes).

El propósito de presente informe es identificar claramente todas las situaciones adversas para el control y mejoramiento de la seguridad de la información de toda la entidad, para ello se clasifican los activos para facilitar su análisis, porque no todos los

activos tienen la misma importancia y no todos ellos representan el mismo valor empresarial. El informe despliega el resultado de la clasificación de sus activos más importantes, como protegerlos y la gestión de la problemática identificada, así como los resultados obtenidos en el proceso de la aplicación de una evaluación detallada a la estructura organizacional y a la infraestructura tecnológica

Palabras clave

Palabras clave: informe técnico, ciberseguridad, seguridad de la información, delitos informáticos, estructura organizacional.

Marco conceptual y normativo

Conceptos fundamentales de ciberseguridad

Ciberseguridad: el concepto de ciberseguridad está orientado a la protección de la información digital, equipos, infraestructura que la soporta y las personas de una organización cualquiera que se a la actividad, ya sea empresarial, laboral o personal.

Hoy por hoy hablar de ciberseguridad es un tema común y fundamental dado que todo tipo de información o proceso, esta digitalizado, ya sea para desarrollar trabajos, manejar información o realizar transacciones. A diferencia de 2 o 3 décadas atrás, la dependencia a la información apenas se iniciaba y la conectividad entre organizaciones era mucho menor o mayormente de manera física. Ejemplo de ello es el manejo de la facturación por medio de facturas electrónicas al realizar una compra o una venta, el departamento de impuestos y aduanas nacionales (DIAN), el comprador y el vendedor cuentan con la misma información en medios magnéticos o de forma digital. Este tipo de manejo digital es solo uno de muchos procesos que se desarrollan día a día y que requieren de confidencialidad, integridad y disponibilidad de la información.

Microsoft nos sugiere que las organizaciones estén en constate evolución o cambios en cuanto a la importancia de proteger la información manejada.

Este panorama de amenazas en constante evolución requiere que las organizaciones creen un programa de ciberseguridad dinámico y continuo para mantener la resistencia y adaptarse a los riesgos emergentes. Un programa de ciberseguridad efectivo incluye a personas, procesos y soluciones de tecnología para reducir los riesgos de interrupción de actividad comercial, robo de datos, pérdida financiera y daño de reputación a causa de un ataque. (Microsoft, https://www.microsoft.com, 2026).

Seguridad de la información: es el proceso de mantener el control tanto de acceso a la información, así como también de modificarla o utilizar la para un fin especifico. Ejemplo de seguridad de la información es la realización de pagos recibidos por clientes, brindando confianza y protección tanto en el cliente como en la organización.

La seguridad de la información, que suele abreviarse como InfoSec, es un conjunto de procedimientos y herramientas de seguridad que protegen ampliamente la información confidencial de la empresa frente al uso indebido, acceso no autorizado, interrupción o destrucción. (Microsoft, microsoft, 2026)

Confidencialidad: La confidencialidad es parte de los tres pilares de la seguridad de la información, conformando la triada CIA que está compuesta por Confidencialidad, Integridad y Disponibilidad. Siendo la confidencialidad el proceso o pilar que restringe el acceso a la

información de personas no autorizadas, garantizando el únicamente acceso al personal autorizado o a sistemas programados y por su puesto autorizados también.

La privacidad es uno de los componentes principales de InfoSec. Las organizaciones deben tomar medidas que permitan únicamente el acceso de usuarios autorizados a la información. El cifrado de datos, la Autenticación multifactor, y la prevención de pérdida de datos son algunas de las herramientas que pueden emplear las empresas para ayudar a garantizar la confidencialidad de los datos.

Integridad: se refiere a la autenticidad u originalidad de la información o información modificable única y exclusivamente de forma autorizada, de lo contrario debe permanecer completa y exactamente como se almaceno.

Las empresas con un sistema de InfoSec bien establecido reconocen la importancia de que los datos sean precisos y fiables y no permiten que los usuarios no autorizados accedan a ellos, los alteren o interfieran de cualquier otro modo en ellos. (Microsoft, microsoft, 2026)

Disponibilidad: siempre debe estar la información disponible, más aún si el acceso es restringido es porque tiene gran importancia para la organización, por lo tanto, se debe garantizar el acceso permanente al personal autorizado. De lo contrario es una falla que puede afectar todos los procesos relacionados.

InfoSec implica un mantenimiento continuo del hardware físico y la actualización habitual del sistema para garantizar que los usuarios autorizados dispongan de acceso fiable y coherente a los datos que necesiten. . (Microsoft, microsoft, 2026)

Activos de información: los activos de información representan el valor para el desarrollo de las actividades orientadas al cumplimiento de los objetivos de manera óptima. Ganando así credibilidad y confianza de manera integral tanto con sus colaboradores, como la confianza de los usuarios o clientes.

son cualquier tipo de recurso que contenga información valiosa para una organización. Estos incluyen datos, documentos, correos electrónicos, software, sistemas, redes, dispositivos y bases de datos. La protección de estos activos es crucial para garantizar la privacidad, integridad y disponibilidad de la información, y prevenir ciberataques como el robo de identidad y el fraude. (MSMK, 2024).

Amenazas: las amenazas son eventos que impactan negativamente la organización tanto en sus activos más importantes como en los que se consideran que no lo son. Pueden y en ocasiones causan daños o afectaciones no deseadas que van en contravía del cumplimiento de las metas u objetivos. Las amenazas pueden surtir efecto en cualquiera de sus activos ya sean activos digitales, activos físicos o activos humanos.

Una amenaza de ciberseguridad puede definirse como cualquier acción —intencional o no— que comprometa la seguridad de una organización o un individuo. A medida que las amenazas crecen y evolucionan, las organizaciones deben comprender a qué se enfrentan: es la única manera de defenderse de las amenazas de ciberseguridad provenientes de delincuentes que explotan vulnerabilidades para acceder a sus redes, datos e información confidencial. (Regalado, 2024)

Vulnerabilidades: son puntos susceptibles de una organización donde la amenaza puede hacer daño con mayor facilidad, dado que carecen de suficiente seguridad para responder a un ciberataque, comprometiendo negativamente los procesos, sistemas, infraestructura e inclusive personas.

En el ámbito digital, donde los datos son tan valiosos como el dinero, las vulnerabilidades representan fisuras en nuestra armadura cibernética. Estas debilidades suelen ser silenciosas e invisibles hasta que se explotan, lo que expone a las personas y a las organizaciones a muchas amenazas potenciales. Esta preocupación general impulsa los esfuerzos en materia de ciberseguridad, no solo para corregir estos fallos, sino también para comprender su origen y sus implicaciones. (proofpoint, 2026)

Riesgos y controles de seguridad: los riesgo y nuevas formas de ataques pueden ser:

Ransomware:

Se trata del secuestro de la información mediante software malicioso. El resultado suele ser la encriptación de los datos y la solicitud de un pago por su desencriptación.

Business Email Compromise:

Se trata de un tipo de suplantación de identidad mediante el envío de correos haciéndose pasar por otras personas, solicitando transferencias, contraseñas, cuentas o documentos a personas de la agenda de contactos del correo secuestrado.

Phishing o ingeniería social:

Se trata de técnicas de engaño para que se comparta información confidencial como contraseñas, datos personales o datos bancarios.

Software de gestión de riesgos de ciberseguridad:

Para la gestión de estos riesgos es necesario identificarlos, evaluarlos y asociarlos a controles que permitan mitigar cada uno de ellos, de forma que una vigilancia y monitorización constante permita a las organizaciones aumentar su seguridad.

GRCTools: facilita el Software de Gestión de Riesgos de Ciberseguridad, un completo Sistema de Gestión de Seguridad de la Información con controles precargados que facilita a las organizaciones la implementación, identificación, evaluación y monitoreo de los riesgos de ciberseguridad. (TOOLS, 2026)

Marco normativo

Tabla 1. *Normatividad aplicable.*

Norma o estándar	***Propósito***	***Aplicabilidad en la organización***

Ley 1581 de 2012. Habeas Data	Reconoce el derecho que tienen las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos y sean eliminadas cuando sea procedente.	En la organización se presenta considerable flujo de datos personales de los clientes y servidores, esto derivo en actividades sospechosas relacionadas con el uso de la tarjeta de crédito de un cliente, que se puede tipificar como intento de hurto por medios informáticos, después de usar los canales de ventas de reservas de la empresa. Aquí es donde aplicando la ley 1581 de 2012, se puede solicitar innegablemente la eliminación de todo tipo de datos por parte del Hotel Gran Mirador & Convention Center S.A.S para proteger el cliente, su nombre y sus recursos.

Ley 1273 de 2009. Ley de Delitos Informáticos	El propósito de esta ley es definir los delitos informáticos y clasificarlos según el actuar o las características del evento. Entre estas características tenemos: Acceso abusivo a sistemas informáticos. Interceptación de datos informáticos. Daño o alteración de información. Suplantación de identidad. Hurto por medios informáticos. Uso indebido de credenciales.	La organización por medio del canal de reservas maneja información de los clientes para hacer sus transacciones, en condiciones normales, estaría bien el proceso, pero dado que los movimientos sospechosos en su tarjeta, permite aplicar la ley de delitos informáticos porque se suplanto la identidad y se accedió abusivamente a l sistema. Esta ley también es aplicable es a la organización porque dada la vulnerabilidad de sus equipos al permanecer desbloqueados por durante periodos de alta ocupación

ISO 27001 Estándar internacional para implementar un Sistema de Gestión de Seguridad de la Información (SGSI)	Su propósito es proteger la información. Gestionar riesgos. Implementar controles de seguridad. Mejorar continuamente la seguridad de la organización.	La Aplicabilidad en el caso asignado se da porque las contraseñas de algunos sistemas no cumplen requisitos mínimos de complejidad. Por lo tanto, al cumplir con este estándar internacional la protección a la información aumenta de forma considerable, alejando de las amenas y reduciendo las vulnerabilidades. Con la aplicación en la organización estudiada se abre paso a realizar campañas periódicas de sensibilización en seguridad de la información, no solo por

		parte del área de sistemas, sino por todos los que trabajan para la organización.
ISO 27005 Estándar internacional que proporciona directrices para la gestión de riesgos en seguridad de la información.	El propósito de este Estándar internacional es proporcionar directrices para la gestión de riesgos en seguridad de la información. Identificar riesgos. Analizar amenazas y vulnerabilidades. Evaluar impacto y probabilidad. Priorizar riesgos. Definir tratamientos y controles.	Su aplicabilidad en la organización se debe adoptar en la implementación de un procedimiento formal para la gestión de incidentes de seguridad. Si como también aplicar este estándar internacional para la implementación y ejecución de pruebas de recuperación de información.

ENISA European Union Agency for Cybersecurity. Agencia de la Unión Europea especializada en ciberseguridad.	El propósito de la agencia de la unión europea especializada en ciberseguridad es: Fortalecer Informes sobre amenazas emergentes. Buenas prácticas de ciberseguridad. Análisis de tendencias y riesgos. Recomendaciones para fortalecer la seguridad. Referencia internacional para la toma de decisiones.	Su aplicación en esta organización es que con su aplicación se puedan reducir índices de vulnerabilidad cuando se presenten configuraciones incorrectas en el sistema de control de acceso y se vea perjudicada la asignación de habitaciones a huéspedes. Es preciso implementar el fortalecimiento que ofrece ENISA, porque algunos colaboradores desconocen los riesgos asociados al tratamiento de datos personales de huéspedes, así como tampoco se cuenta con un plan de capacitaciones generales

para todo el personal y de manera mas recurrente.

Ley Estatutaria 1581 De 2012 O Ley Habeas Data: dado el objeto principal de esta ley , el cual es desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (Calderon, 2012).

Para la organización Hotel Gran Mirador & Convention Center S.A.S. representa gran valor, ya que permite tener un acuerdo mutuo entre los usuarios y sus colaboradores, teniendo presente que toda información personal tiene instrucciones de manejo en dado caso que el titular solicite de manera general o a detalle que hacer con su información personal.

Ley 1273 de 2009. Ley de Delitos Informáticos: por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la

protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Colombia, 2026).

Esta ley o Normatividad sobre delitos informáticos permite al Hotel Gran Mirador & Convention Center S.A.S, clasificar todos los modos y formas en que un individuo ajeno a la organización o perteneciente a ella, pueda cometer un acto delictivo con la información a la que accede de forma autorizada o en el peor de los casos de forma no autorizada.

ISO 27001 Estándar internacional para implementar un Sistema de Gestión de Seguridad de la Información (SGSI): a norma ISO 27001:2022 es un estándar internacional para la gestión de la seguridad de la información, que ayuda a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de sus datos. Ofrece un marco para identificar riesgos, implementar controles y garantizar la continuidad del negocio frente a amenazas. Su certificación mejora la reputación, la competitividad y la confianza de socios y clientes, promoviendo una cultura de seguridad en la empresa. La ISO 27001 simplifica procesos, reduce requisitos documentales y adapta controles a los desafíos actuales. (ISOTOOLS, 2022).

Su implementación en la organización analizada permite implementar un verdadero sistema de gestión de seguridad de la información, porque no se tiene la cultura en ciberseguridad y esto conlleva a que no se tenga la conciencia de los diferentes riesgos a los que se exponen todos los que conforman el Hotel Gran Mirador &

Convention Center S.A.S, sus proveedores, sus clientes o huéspedes y los entes de control en caso de requerir información para efectos de impuestos o auditorias de lavado de activos.

ISO 27005 Estándar internacional que proporciona directrices para la gestión de riesgos en seguridad de la información. Su misión es clara: facilitar la aplicación de los requisitos de ISO/IEC 27001, centrándose en la identificación, análisis, evaluación y tratamiento de los riesgos. (Solutions, 2025).

Este estándar internacional es de gran importancia para la organización Hotel Gran Mirador & Convention Center S.A.S. permitiéndole, identificar cada uno de los riesgos a los que esta expuesta, que amenazas se pueden convertir en eventos n o deseados para la ella y fortalecer las áreas más vulnerable que tiene, en especial su activo humano y su concepto erróneo de la seguridad de la información, haciendo referencia al criterio que se tiene de la ciberseguridad es solo dependencia del área de las TI. Y no de todos los trabajadores del hotel.

ENISA: European Union Agency for Cybersecurity.

La Agencia Europea de Ciberseguridad (ENISA) es la agencia de la Unión dedicada a lograr un alto nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada por la Ley de Ciberseguridad de la UE, la Agencia contribuye a la política cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de las

TIC mediante esquemas de certificación de ciberseguridad, coopera con los Estados miembros y los organismos de la UE, y ayuda a Europa a prepararse para los desafíos cibernéticos del futuro. (ENISA, s.f.)

ENISA brinda a la organización estándares internacionales que permiten corregir vulnerabilidades y minimizar amenazas para poder brindar mas seguridad a sus usuarios y mayor manejo a los colaboradores, teniendo la ciberseguridad como escudo de batalla para desarrollar cada actividad o transacción de manera confiable para las dos partes que tiene acceso adecuado a los sistemas y productos del Hotel Gran Mirador & Convention Center S.A.S.

Marco contextual

Descripción de la organización

El Hotel Gran Mirador & Convention Center S.A.S. es una organización dedicada a la prestación de servicios de hospedaje, eventos corporativos, turismo de negocios y actividades recreativas. Cuenta con más de 12 años de operación y se ha consolidado como uno de los principales hoteles de la región.

La organización dispone de 220 habitaciones, 8 salones para eventos empresariales, zonas recreativas, restaurantes, gimnasio y servicios complementarios para huéspedes nacionales e internacionales.

.

Misión

Brindar experiencias de hospedaje y eventos de alta calidad mediante servicios innovadores, seguros y orientados a la satisfacción de nuestros huéspedes y clientes corporativos.

Visión

Ser reconocido como uno de los hoteles líderes del país por su excelencia operativa, innovación tecnológica y confianza en la protección de la información.

Estructura organizacional

La organización está conformada por las siguientes áreas:

- Gerencia General
- Dirección Administrativa y Financiera
- Dirección Comercial
- Gestión de Reservas
- Recepción y Atención al Cliente
- Tecnología y Sistemas
- Seguridad Física
- Alimentos y Bebidas
- Eventos y Convenciones
- Talento Humano
- Compras y Contratación
- Mantenimiento

Procesos principales

Gestión de reservas

Administra reservas realizadas mediante página web, agencias de viaje, aplicaciones móviles y atención telefónica.

Registro y atención de huéspedes

Gestiona el ingreso, permanencia y salida de huéspedes.

Gestión de eventos

Coordina eventos corporativos, capacitaciones, reuniones empresariales y actividades sociales.

Gestión financiera

Administra pagos, facturación, recaudos y control presupuestal.

Gestión de clientes

Administra información personal, historial de hospedajes y preferencias de los huéspedes.

Gestión de proveedores

Controla compras, contratos y suministros para la operación del hotel.

Recursos tecnológicos relevantes

La organización dispone de:

- 95 computadores de escritorio.
- 40 computadores portátiles.
- Sistema de gestión hotelera (PMS).
- Sistema de reservas en línea.
- Portal web corporativo.
- Plataforma de pagos electrónicos.
- Sistema CRM para clientes.
- Sistema ERP administrativo.
- Sistema de control de acceso electrónico a habitaciones.
- Correo electrónico corporativo.
- Plataforma de videovigilancia.
- Plataforma de respaldo de información.
- Infraestructura híbrida local y en la nube.
- Red WiFi corporativa.
- Red WiFi para huéspedes.
- Aplicación móvil para clientes.

Contexto de la operación:

Actualmente cuenta con aproximadamente 260 colaboradores entre personal administrativo, recepción, reservas, tecnología, mantenimiento, seguridad, alimentos y bebidas, servicio al cliente y dirección general.

El hotel atiende en promedio 4.000 huéspedes mensuales y realiza más de 300 eventos corporativos al año.

Problemática identificada:

En el caso asignado en la organización Hotel Gran Mirador & Convention Center S.A.S., se puede describir e identificar claramente varias problemáticas de seguridad de la información, pero cabe resaltar la que podría llamarse la problemática principal, y esta radica en que el crecimiento de los servicios digitales implementados ha sido más rápido que la actualización de políticas y procedimientos. Esto permite que se abra una brecha entre trabajadores y la forma adecuada de control la seguridad de la información. Los empleados en su mayoría consideran que la seguridad de la información es responsabilidad exclusivamente del área tecnológica, concepto equivocado porque la seguridad de la información depende de cada uno de los usuarios, tanto internos como externos. Adicionalmente a las problemáticas identificadas cabe mencionar que las capacitaciones sobre ciberseguridad son ocasionales y no alcanzan a todo el personal.

Esta situación actual de la organización conlleva a realizar un informe técnico de ciberseguridad para inicialmente mitigar los riesgos y fortalecer vulnerabilidades presentes.

Identificación y análisis de activos

.

Inventario de activos

Tabla 2. *Inventario de activos*

Los activos más importantes con referente a la Seguridad de la Información de la organización **Hotel Gran Mirador & Convention Center S.A.S**. son:

Activo	Tipo	Descripción	Criticidad
Sistema ERP administrativo	Digital	Es un sistema digital encargado de gestionar los procesos de la organización en una sola plataforma, permitiendo administrarla en sus distintas áreas.	Alta

Gerencia General	Humano	Representa el liderazgo de la organización y la toma de decisiones. Al representar un activo humano crítico en la organización. para la ciberseguridad es fundamental que este nivel administrativo tenga presente la importancia de la aplicabilidad y conocimiento en seguridad de la información de cada una de sus dependencias y roles que	Alta

		desempeña la organización para reducir el riesgo de daños cibernéticos de cualquier índole.	
Computadores de escritorio	Físico	Son herramientas tangibles que permiten desarrollar algunas de las actividades de la empresa	Medio

Área de tecnología y sistemas	Humano	Representa el departamento de las TIC. de la organización, también como un activo humano critico porque es allí donde se empieza a ejecutar toda la planeación hecha conjuntamente con la gerencia general. la responsabilidad del área de las tecnologías en la organización es alta, dado que debe garantizar la adaptabilidad de los colaboradores a las tecnologías	Alta

		utilizadas, así como también sensibilizar y capacitar a los trabajadores en Ciberseguridad o protección de la información para que la organización conozca y mitigue los riesgos de Ciberataques.	
Sistema de gestión hotelera (PMS)	Digital	Software integral que automatiza las operaciones diarias de un hotel.	Alta
Plataforma de pagos electrónicos	Digital	Permite adquirir servicio por medio de pagos digitales	Alto

Correo electrónico corporativo	Digital	Es el mecanismo por medio del cual se realizan confirmaciones y envió de información comercial o personal de usuarios y clientes, así como también entre funcionarios y sus distintas dependencias e instituciones externas.	Alta

La gerencia general: la gerencia general como el activo humano más importante en la toma de decisiones en la implementación de nuevas estrategias tecnológicas propuestas por el área de sistema. Es la ultima palabra en el desarrollo de proyectos a corto, mediano y largo plazo en la organización, siempre llevando la misión y la visión a

cumplimiento, sin tomar riesgos descontrolados o fuera de sus conocimientos y que se encuentren en ejecución. Al representar un activo humano crítico en la organización. para la ciberseguridad es fundamental que este nivel administrativo tenga presente la importancia de la aplicabilidad y conocimiento en seguridad de la información de cada una de sus dependencias y roles que desempeña la organización para reducir el riesgo de daños cibernéticos de cualquier índole.

Computadores de escritorio: son el activo físico importante en el desarrollo operacional de la compañía. Su disponibilidad en la organización permite a sus colaboradores contar con herramienta de acceso a la plataforma institucional y gestionar el comercio al que está dedicado el hotel. Al contar con 95 computadores de escritorio los trabajadores pueden estar permanentemente o cuando lo requieran al tanto de la información para consultar, gestionar o confirmar servicios prestados por la organización a un cliente o a otra empresa que disfruta de los servicios ofrecidos por Hotel Gran Mirador & Convention Center S.A.S.,

Área de tecnología y sistemas: esta área representa el talento humano que tiene la capacidad de integrar a todos los trabajadores, la operación y los clientes de manera practica y adecuada, teniendo la información necesaria para la gestión de cualquiera de los servicios que ofrece la organización y que es requerido por los visitantes. Al tener un

soporte tecnológico la actividad comercial de la empresa es mas confiable para las partes intervinientes en el servicio prestado, ya sea un proveedor, trabajador o cliente. también como un activo humano critico porque es allí donde se empieza a ejecutar toda la planeación hecha conjuntamente con la gerencia general. la responsabilidad del área de las tecnologías en la organización es alta, dado que debe garantizar la adaptabilidad de los colaboradores a las tecnologías utilizadas, así como también sensibilizar y capacitar a los trabajadores en Ciberseguridad o protección de la información para que la organización conozca y mitigue los riesgos de Ciberataques.

Sistema de gestión hotelera (PMS): Al contar con un activo digital muy acorde con las características de la actividad económica del negocio, este es uno de los activos más importante que tiene la organización porque permite la intercomunicación y gestión de información de los usuarios.

Los sistemas de gestión de establecimientos hoteleros (PMS) gestionan todos los aspectos de las operaciones de negocios del hotel, incluida la capacidad de ofrecer experiencias excepcionales a los huéspedes. Tradicionalmente, un PMS de hotel se definía como un software que permitía a un hotel o grupo de hoteles gestionar las capacidades de atención al público, como reservas de reservas, check-in/checkout, asignación de habitaciones, gestión de tarifas de habitaciones y facturación. Un PMS de hotel reemplazó los procesos que consumen mucho tiempo y requieren mucho papel. Hoy en día, la tecnología de hotel PMS ha evolucionado mucho más allá de la recepción. Un

PMS para hoteles es ahora un sistema de operaciones de negocio fundamental que permite a los hoteleros ofrecer experiencias increíbles a sus clientes. (ORACLE, 2026)

Plataforma de pagos electrónicos: la plataforma de pagos electrónicos es un activo digital muy importante para la organización porque permite a los usuarios asegurar sus servicios solicitados pagando de forma rápida y segura y así no perder la reserva, si este es el caso. Igualmente, a la organización le permite manejar servicios confirmados con mayor fluidez y tener inventario actualizado según los servicios que se tengan disponibles y los que no lo estén. Este activo permite a la organización agilizar sus ventas y gestionar nuevas estrategias que sean atractivas para los visitantes al momento de querer pagar un servicio pude encontrarse, por ejemplo, con bono de descuentos o mejores ofertas en la aplicación destacando y asegurando su confidencialidad en la transacción.

Correo electrónico corporativo: este activo digital es de gran importancia para la organización porque permite recibir información externa a la compañía que puede ser de gran interés, o también permite la comunicación oficial entre la organización y sus colaboradores. Es un método de confirmación de recibimiento de la información tanto del que envía como el que recibe**.**

Análisis de amenazas y vulnerabilidades

Tabla 3. *Amenazas y vulnerabilidades*

Activo	***Amenaza***	***Vulnerabilidad***
Sistema ERP	Acceso no autorizado y descontrolado permitiendo suplantación de identidad.	Contraseñas que no cumplen con el nivel mínimo de complejidad. Algunos funcionarios comparten credenciales de acceso al sistema de reservas durante cambios de turno.

	Sistema de reserva en línea	Hurto por medios informáticos	Robo de recursos económicos de los usuarios y perdida de seguridad en uso del sitio. Actividad sospechosa relacionada con el uso de su tarjeta de crédito después de realizar una reserva mediante canales digitales.

Gestión de reservas	Amenaza tecnológico ocasionada por fallas en los sistemas.	El sistema de reservas no cuenta con la capacidad de gestionar todas las solicitudes de los clientes. Puede presentar indisponibilidad durante varias horas en temporadas altas, afectando la gestión de nuevos clientes.

Correo electrónico corporativo.	Puede existir suplantación de identidad en correos fraudulentos	Algunos de los colaboradores no diferencian un correo malicioso de un correo oficial de un cliente o proveedor. Atender de manera inocente, correos fraudulentos que simulan provenir de una agencia de viajes internacional o algo por el estilo.

40 computadores portátiles	Perdida o hurto de alguno de los equipos portátiles y por lo tanto perdida de la información.	Al no mantener regularmente pruebas de recuperación de información se puede perder información de las diferentes áreas registradas. En la organización no se ejecutan pruebas de recuperación de la información.
Sistema de control de acceso electrónico a habitaciones	Fallas temporales en la asignación de habitaciones a huéspedes.	No tener un control y registro actualizado de las habitaciones disponibles, las ocupadas y las que están por desocupar. La configuración incorrecta en el sistema de control de acceso a las habitaciones.

Todas las situaciones representan riesgos para la operación de la organización, pero algunas conllevan a un nivel más agudo o alto del riesgo. una de las situaciones que representa riesgos y que esta listada en el caso de estudio es la practica de algunos funcionarios de compartir credenciales de acceso al sistema de reservas durante el cambio de turno, ya que esto se puede interpretar claramente como un delito informático de suplantación, permitiendo modificar información, sin un responsable verdadero o fácil de identificar.

Las credenciales únicas por trabajador no son de uso colectivo, por lo tanto, si algunos de los ellos hacen estas malas prácticas, carecen de capacitación en seguridad de la información y se debe concientizar a cada uno, a hacer parte de una cultura cibernética que permita mitigar cada vez los riesgos que están latentes a dañar el engranaje tecnológico de la organización.

La organización siempre debe manejar canales corporativos de información y comunicación con sus colaboradores, clientes y proveedores. En el Hotel Gran Mirador & Convention Center S.A.S existe una situación muy riesgosa que permite al trabajador o colaborador tener dominio de la información así ya no pertenezca a ella. Esta situación es el uso de correos personales para compartir información relacionadas con eventos de la organización. Esto conlleva a que la información de la empresa se exponga a casos de

información equivocada, negación de información, suplantación de imagen corporativa, y demás usos indebidos que pueden afectar el crecimiento y el comercio de la empresa. Los correos personales puede que sean un medio de comunicación usado para dar la información de determinado caso en la empresa, pero se puede mantener un buen uso mientras el trabajador hace parte de la organización, luego que ya este desvinculado, el riesgo mas pequeño al que se está, es a la perdida de comunicación con respuesta inmediata entre Organización, cliente y proveedor.

Otra situación que representa mayor riesgo es la ausencia de un procedimiento formal para la gestión de incidentes de seguridad como la pérdida del equipo portátil del área comercial que se extravió en una feria empresarial. Este equipo contaba con información de clientes corporativos y eventos programados. Esto ocurre porque no se realizan campañas de sensibilización en seguridad de la información.

La organización al contar con un numero considerable de colaboradores, muchos de ellos perciben la seguridad de la información como responsabilidad únicamente del área de tecnología, es por ello que es una situación que representa riesgo para la operación empresarial ya que ellos desconocen los riesgos asociados al tratamiento de datos y los demás delitos informáticos que puedan presentarse. Como un Hotel consolidado en el mercado y con gran enfoque de crecimiento, todo el personal debe estar en capacidad de diferenciar que actividad representa un riesgo para la seguridad de la información empresarial y cuales no lo representan.

La recepción de correos fraudulentos suplantando empresas reales o personas suplantando a otras mediante envió de correos es un riesgo presente en esta empresa, ya que no se verifica el tipo de correo que llega porque existe confianza excesiva en la legitimidad de ellos. los colaboradores del Hotel Gran Mirador & Convention Center S.A.S asumen que los correos recibidos son de agencias o de alguno de los proveedores.

Análisis y gestión de riesgos

Metodología de análisis

Para realizar la valoración del impacto y probabilidad de ocurrencia del riesgo, se realizó un análisis de que tan afectada se vería la organización en el momento de determinado evento, así como sus pérdidas económicas no solo en la organización Hotel Gran Mirador & Convention Center S.A.S, sino en sus clientes, colaboradores y nuevos usuarios.

Para calcular el riesgo cibernético, la evaluación del riesgo cibernético evalúa dos factores clave: Probabilidad de ataque: Basado en vulnerabilidades, configuraciones erróneas, actividad sospechosa y brechas de cumplimiento. Las fuentes de datos incluyen el comportamiento del usuario, los registros de seguridad y la actividad de las aplicaciones en la nube. Impacto del ataque: Considera la importancia de los activos y el valor empresarial. Una filtración de secretos comerciales o infraestructura crítica puede ser mucho más perjudicial que varios incidentes de bajo valor. (Cardoso, 2026)

Este análisis permite además identificar el tamaño del impacto en la reputación empresarial, así como también conocer la probabilidad de acuerdo a la frecuencia con que se presentan las amenazas y los puntos vulnerables, verificando que los controles existan o no, para prevenirlos, o si el riesgo se ha materializado anteriormente y que tan expuesta esta la organización a todas las amenazas y cuales son las zonas mas vulnerables que

permitan que el riesgo ocurra generando impacto negativo en sus diferentes niveles como el alto, el nivel medio o el bajo.

El proceso de evaluación comienza con la identificación de activos críticos, incluidos hardware, software, datos confidenciales, redes e infraestructura de TI, y la catalogación de posibles amenazas y vulnerabilidades. Estas amenazas pueden provenir de diversas fuentes, como hackers, malware, ransomware, amenazas internas o desastres naturales. Las vulnerabilidades pueden incluir software obsoleto, contraseñas débiles o redes no seguras. (Downie, 2024)

A medida que las ciber amenazas se vuelven cada vez más sofisticadas, las empresas de todos los tamaños deben evaluar y abordar de manera proactiva sus riesgos de ciberseguridad para proteger los datos confidenciales, mantener la confianza de los clientes y cumplir con los requisitos legales. Una comprensión integral de las posibles vulnerabilidades permite a las organizaciones tomar medidas específicas y asignar los recursos de manera eficaz, lo que minimiza las posibilidades de que se produzca un incidente perjudicial. (Warrior, 2025)

Matriz de riesgos asociados a la organización Hotel Gran Mirador & Convention Center S.A.S

Tabla 4. *Matriz de riesgos*

Riesgo	***Impacto***	***Probabilidad***	***Nivel***
Acceso descontrolado y suplantación de identidad	Alto	Alta	Alto
Robo de recursos económicos de los usuarios y perdida de seguridad en uso del sitio	Alto	Alta	Alto
Incapacidad del sistema de reservas de gestionar todas las solicitudes de los clientes.	Alto	Media	Medio

Recepción de correos fraudulentos que simulan provenir de una agencia de viajes internacionales o algo por el estilo. Y sufrir daños en la información o modificaciones no autorizadas.	Alto	Alta	Alto
Perdida de información de las diferentes áreas registradas en el sistema de la organización porque no se ejecutan pruebas de recuperación de la información.	Alto	Alto	Alto

Los riesgos prioritarios como el acceso descontrolado o no autorizado y además suplantación de identidad al utilizar credenciales correspondientes a otro trabajador, compromete la información de la organización, afectando la gestión de clientes fidelizados o los nuevos, e inclusive permite entrar en procesos legales a los autores de dicha práctica.

Se encontró también un riesgo de suma importancia que es el movimiento sospechoso de cuentas de clientes en plataforma de la organización permitiendo despertar alarma e inseguridad de parte del usuario. Representando este caso la organización como una gran posibilidad de convertirse en un sitio no seguro para los usuarios interesados en tomar los servicios ofrecidos por el Hotel Gran Mirador & Convention Center S.A.S.

Por otro lado, el riesgo de fallas por tiempos determinado en la gestión de servicios de reservas o No tener un sistema que le permita una gestión adecuada de solicitudes de servicios en altas temporadas puede ocasionar que los usuarios emigren a otras opciones de servicios en otros lugares cercanos que ofrezcan servicios similares, aunque de menor calidad.

Los riesgos identificados en la organización mediante un análisis de acuerdo a entrevista y observación, evidencia que se debe reforzar de forma urgente la mentalidad o interés referente a la seguridad de la información por parte de todos los colaboradores. De manera que toda la organización comprenda que la seguridad de la información es un

aspecto que todos deben cuidar sin que se de espacio a correos maliciosos o Ciberataques productos del desconocimiento de algún trabajador con referente a proteger los activos organizacionales.

Políticas y controles de seguridad

Políticas propuestas

Tabla 5. *Políticas de seguridad*

Política	***Objetivo***	***Riesgo asociado***
Gestión de usuarios y que cumplan requisitos mínimos de complejidad.	Proteger el acceso a los sistemas de información.	Acceso no autorizado a sistemas.
Uso seguro del correo electrónicos corporativos.	Reducir riesgos asociados al phishing y al manejo del correo institucional.	Phishing sobre correos institucionales.
Copias de seguridad de la información	Garantizar la disponibilidad y recuperación de la información	Pérdida de información por fallas técnicas.

Uso aceptable de recursos tecnológicos y actualización de software utilizado por la organización	Regular el uso de equipos, software y servicios institucionales	Uso inadecuado de memorias USB.
Clasificación y manejo de la información con copia de respaldo.	Definir cómo proteger la información según su nivel de sensibilidad	Divulgación de información confidencial

Controles propuestos

Tabla 6. *Controles de seguridad*

Riesgo	***Control***	***Justificación***
Perdida de información por desconocimiento sobre seguridad asociados al tratamiento de datos.	Capacitación y sensibilización de todo el personal.	Promover el cumplimiento de las políticas establecidas en la organización.

Recepción de correos fraudulentos que contengan información que pueda borrar o alterar el sistema	Implementación de política formal de clasificación de información.	Exceso de confianza en la legitimidad de correos electrónicos recibidos de agencias y proveedores.
Perdida de la cadena de información por la utilización de correos personales para fines de la organización.	Utilizar correos corporativos exclusivamente y que trascienda su uso así el trabajador ya no este vinculado a la empresa.	Algunos colaboradores utilizan correos personales para compartir información relacionada con eventos.
Incapacidad del sistema de reservas de gestionar todas las solicitudes de los clientes en temporadas altas.	Implementación y mejoramiento del sistema o software. realizando actualizaciones con más regularidad.	Al no tener la capacidad de gestionar eficazmente la solicitud de reservas en temporadas altas se pueden perder nuevos clientes.

Las políticas establecidas para la organización Hotel Gran Mirador & Convention Center S.A.S. permite proteger sus activos de información y orientar el comportamiento

de las personas o colaboradores frente a la seguridad de la información para disminuir los riesgos identificados de manera previa.

Las políticas y los controles identificados contribuyen a desarrollar una cultura de seguridad, tanto de trabajadores como de usuarios o clientes que frecuentemente utilizan los servicios prestados por el hotel. Permitiendo a la organización pensar en una expansión empresarial, aunque el crecimiento de los servicios digitales haya sido más rápido que la actualización de estas políticas y el planteamiento de los controles.

La organización mediante la realización de este informe técnico en Ciberseguridad pudo identificar los riesgos a los que se expone según sus amenazas y sus vulnerabilidades. De tal forma que se puede controlar con conocimiento de acuerdo al análisis realizado durante todo este tiempo. Al establecer políticas de seguridad y controles de seguridad, se reduce significativamente el impacto que cualquier evento negativo pueda causar en la organización, porque ya se tiene conocimiento de su posible ocurrencia y que hacer en este caso.

Gestión de incidentes y continuidad del negocio

Tabla 7. *Incidentes potenciales*

Incidente	***Descripción***	***Impacto***
Funcionarios se comparten credenciales de acceso al sistema de reservas durante cambio de turno.	Esta practica se realizar porque los colaboradores desconocen o no consideran importante la seguridad de la información.	Puede existir cambios de información de manera irregular o por medio de suplantación, ya que la persona que accede no es quien figura en la credencial de acceso.
El sistema de reservas presenta indisponibilidad durante varias horas.	En temporadas altas el sistema colapsa y deja de funcionar por determinadas horas.	Este funcionamiento intermitente permite que se afecte considerablemente la gestión de nuevos clientes para el Hotel Gran Mirador & Convention Center S.A.S.

Apertura de correo fraudulento simulando proceder de agencias de viajes.	Un trabajador recibió un correo fraudulento fingiendo ser una agencia de viajes internacional.	Realizar verificación en base de datos de la existencia de este correo para poder abrirlo. Como impacto se presentó intento de acceso no autorizado a cuentas institucionales.
Perdida de un computador portátil durante una feria empresarial.	Un trabajador perdió sin querer un portátil que contenía información de clientes corporativos y eventos programados.	Impacta negativamente por la pérdida de la información de dos aspectos importantes y que representan dinero para la organización: clientes corporativos y eventos programados.

Tabla 8. *Plan básico de respuesta*

Fase	***Acción***
Detección	Contraseña de algunos dispositivos no cumple con requisitos mínimos de complejidad.
Contención	Verificar el entorno donde se desarrollan las actividades y tener personal encargado del cuidado de los activos físicos en sitios de alta concurrencia. Agregar la realización de actualización de contraseñas con los requisitos mínimos de seguridad.
Erradicación	Realización de campañas periódicas de sensibilidad en acceso y seguridad de la información.
Recuperación	Utilización de contraseñas que cumplan con el mínimo de complejidad y no compartir credenciales de acceso.

Lecciones aprendidas.	La seguridad informática es un compromiso de cada uno de los integrantes de la organización, así como también de los clientes., por lo tanto, cada uno esta en la obligación de tener el conocimiento de la importancia de la confidencialidad de la información y protección de datos.

La organización Hotel Gran Mirador & Convention Center S.A.S. respondería y mantendría la continuidad operativa con enfoque al crecimiento, como la tiene en este momento, ya que después de este informe técnico se tiene claro los puntos o aspectos a mejorar. Esta herramienta técnica permite mantener identificadas las amenazas y las vulnerabilidades, para determinar los riesgos a los que se esta expuesta. De esta forma el impacto negativo disminuye significativamente hasta el punto de que no ocurra ningún evento porque ya se tiene control para mitigar el crecimiento de la probabilidad de ocurrencia de cualquier evento.

Cultura organizacional en ciberseguridad.

Tabla 9. *Hallazgos organizacionales*

Situación observada	***Riesgo asociado***
No se cumplen con las políticas establecidas en la organización.	Perdida de información por desconocimiento sobre seguridad asociados al tratamiento de datos.
Hay exceso de confianza en la legitimidad de correos electrónicos recibidos de agencias y proveedores.	Recepción de correos fraudulentos que contengan información que pueda borrar o alterar el sistema
Algunos colaboradores utilizan correos personales para compartir información relacionada con eventos.	Perdida de la información por la utilización de correos personales para fines de la organización.
No se tiene la capacidad de gestionar eficazmente la solicitud de reservas en temporadas altas.	Incapacidad del sistema de reservas de gestionar todas las solicitudes de los clientes en temporadas altas.

Tabla 10. *Recomendaciones de mejora*

Hallazgo	***Recomendación***
Funcionarios se comparten credenciales de acceso al sistema de reservas.	Utilizar credenciales de manera personal e intransferible para no incurrir en errores y delitos legales.
No existe política formal de clasificación de la información.	Se debe establecer políticas formales de clasificación y seguridad de la información en la organización.
Contraseñas no cumplen con requisitos mínimos de complejidad.	Establecer caracteres especiales para la creación de contraseñas que cumplan con requisitos minimos de complejidad.
No existe un procedimiento formal para gestión de incidentes de seguridad de la información.	Establecer de manera oficial y formal un procedimiento que permita llevar a cabo una gestión de incidentes de la seguridad de la información.

El fortalecimiento de la cultura organizacional después de las recomendaciones dadas en el informe técnico, esta dado en el instante que todos los colaboradores y clientes del Hotel Gran Mirador & Convention Center S.A.S., tengan conocimiento de la importancia de detectar situaciones que representan amenaza para la información sensible y confidencial de todos los usuarios. Por lo tanto, a medida que se recomienda corregir o agregar un aspecto, se obtiene un cambio positivo y una percepción más segura del uso de los canales digitales de la organización.

Conclusiones.

El informe técnico en ciberseguridad aplicado a la organización Hotel Gran Mirador & Convention Center S.A.S identificar sus amenazas, vulnerabilidades y de acuerdo a estos dos factores identificar también los riesgos a los que se esta inmersa. De tal forma que le permite anticiparse a cualquier evento y contar con las medidas de corrección o mitigación que le permita afectarse lo menos posible y mantener su perdurabilidad en el mercado.

Esta organización permite desarrollar la solución a diferentes hallazgos en cuanto a cultura de la seguridad de la información se refiere, así como también sensibilizar a cada dependencia o usuario que manejan datos o utilizan información para gestionar algunos de los servicios de la organización.

La identificación y el análisis de sus activos se considera un factor fundamental que permite identificar que tan afectada resulta la organización de presentarse un evento negativo. En este caso el enfoque esta dado a la importancia que tiene el adecuado manejo de la seguridad de la información por parte de cada uno de los participantes desde los diferentes roles.

La organización está proyectada a la apertura de nueva sede durante los próximos tres años, esto conlleva a que su información este realmente organizada y se cuenta con la gestión en seguridad de la misma, que permita brindar confianza a todos los usuarios.

El crecimiento de esta organización la obliga a ir a la par con el crecimiento tecnológico y las políticas de seguridad, así como los procedimientos de seguridad de la información. Creando una cultura organizacional en manejo de la información en el ámbito digital para que el crecimiento proyectado no se vea afectado por ataque, permitidos por el desconocimiento de sus alcances.

Referencias

Calderon, J. M. (17 de octubre de 2012). Ley Estatutaria 1581 De 2012 (Articulo 1°). Bogotá D.C, Colombia.

Cardoso, F. (20 de abril de 2026). *Trend Micro*. Obtenido de https://www.trendmicro.com/: https://www.trendmicro.com/es_es/what-is/attack-surface/cybersecurity-risk-assessment.html

Colombia, P. N. (2026). Normatividad sobre delitos informáticos LEY 1273 DE 2009. Bogotá, Colombia.

Downie, M. F. (9 de AGOSTO de 2024). *IBM*. Obtenido de https://www.ibm.com/: https://www.ibm.com/mx-es/think/topics/cybersecurity-risk-assessment

ENISA. (s.f.). *Nuestra visión: Una Europa segura y de confianza en materia de ciberseguridad.* Obtenido de https://www.enisa.europa.eu/about-enisa/what-we-do

ISOTOOLS. (2022). Norma ISO 27001.

Microsoft. (2026). *https://www.microsoft.com*. Obtenido de https://www.microsoft.com/es-co/security/business/security-101/what-is-cybersecurity

Microsoft. (2026). *microsoft*. Obtenido de https://www.microsoft.com/es-co/security/business/security-101/what-is-information-security-infosec

MSMK. (12 de septiembr de 2024). *MSMK*. Obtenido de https://msmk.university/activos-de-informacion/

ORACLE. (2026). *oracle.com*. Obtenido de https://www.oracle.com/latam/hospitality/what-is-hotel-pms/

proofpoint. (2026). *En el ámbito digital, donde los datos son tan valiosos como el dinero, las vulnerabilidades representan fisuras en nuestra armadura cibernética. Estas debilidades suelen ser silenciosas e invisibles hasta que se explotan, lo que expone a las personas y a* . Obtenido de https://www.proofpoint.com/es/threat-reference/vulnerability

Regalado, P. (24 de octubre de 2024). *splunk*. Obtenido de https://www.splunk.com/en_us/blog/learn/cybersecurity-threats.html

Solutions, G. (03 de 12 de 2025). Conexión entre ISO 27005 e ISO 27001: Impulsa tu gestión de riesgos en seguridad de la información.

TOOLS, G. (2026). *https://grctools.software/*. Obtenido de https://grctools.software/soluciones/riesgos/riesgos-ciberseguridad/

Warrior, S. C. (15 de octubre de 2025). *Secure Code Warrior*. Obtenido de https://www.securecodewarrior.com/: https://www.securecodewarrior.com/es/blog/cybersecurity-risk-assessment-definition-and-steps