Plan Director de Seguridad de la Información de una cadena hotelera

Nombre Estudiante: Marc Montemar Parejo

Programa: Máster Universitario en Ciberseguridad y Privacidad (MUCIP)
Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Arsenio Tortajada Gallego
Profesor responsable de la asignatura: Carles Garrigues Olivella
Centro: Universitat Oberta de Catalunya

Fecha de Entrega: 28/12/2020

FITXA DEL TREBALL FINAL

Título del trabajo:	*Plan Director de Seguridad de la Información de una cadena hotelera*
Nombre del autor:	*Marc Montemar Parejo*
Nombre del consultor/a:	*Arsenio Tortajada Gallego*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	*12/2020*
Titulación o programa:	Máster Universitario en Ciberseguridad y Privacidad (MUCIP)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Castellano*
Palabras clave	*ISO 27001, Hoteles, Seguridad de la Información*

Resumen del Trabajo:

El objetivo de este trabajo es el de desarrollar un Plan Director de Seguridad de la Información para una cadena hotelera. A pesar de haber realizado el trabajo sobre una empresa ficticia, los datos reflejados en el mismo pretenden reflejar realidades que se encuentran presentes en el sector hotelero, el cual el autor del trabajo conoce en profundidad.

La realización de este Plan Director se ha basado en el marco establecido en la norma ISO/IEC 27.001, aplicando el Modelo de Madurez de la Capacidad (CMM) sobre los controles descritos en la ISO/IEC 27.002. Con ello y con el análisis de riesgos realizado, basado en la metodología MAGERIT, conoceremos el estado actual de la organización en relación con la Seguridad de la Información.

Posteriormente, estableceremos el nivel mínimo de seguridad que la empresa está dispuesta a aceptar y se proponen los proyectos que son necesarios llevar a cabo para cubrir la brecha entre el estado inicial y el estado al que la organización quiere llegar.

Este análisis de riesgos, descripción del estado actual, definición del estado deseado y propuesta de proyectos, incorporados al marco establecido en las normas ISO de la serie 27.000 y acompañados de los criterios establecidos en el CMM, formarán el Plan Director de Seguridad de la Información, que, aplicado a una cadena hotelera, será el resultado de este trabajo.

La implantación de este Plan Director, permitirá a la empresa mejorar su gestión de la seguridad de la información e incluso certificarlo mediante la norma ISO 27.001.

Abstract:

The aim of this work is to develop an Information Security Master Plan for a hotel chain. Despite having carried out the work on a fictitious company, the data reflected in it is intended to reflect realities that are present in the hotel sector, which the author of the work knows in depth.

The development of this Master Plan has been based on the framework established in the ISO / IEC 27.001 standard, applying the Capability Maturity Model (CMM) on the controls described in ISO / IEC 27.002. Adding to this the risk analysis carried out, based on the MAGERIT methodology, we shall know the current state of the organization regarding the Information Security.

Subsequently, we will establish the minimum level of security that the company is willing to accept and the projects that need to be carried out are proposed to cover the gap between the initial state and the state the organization wants to reach.

This risk analysis, description of the current state, definition of the desired state and project proposal, incorporated into the framework established in the ISO 27,000 series standards and accompanied by the criteria established in the CMM, will form the Information Security Master Plan, which, applied to a hotel chain, will be the result of this work.

The implementation of this Master Plan will allow the company to improve its management of information security and even certify it through the ISO 27.001 standard.

Índice

Lista de tablas

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

El presente documento corresponde al TFM del Máster Universitario en Ciberseguridad y Privacidad de la UOC, cuya finalidad es la de aplicar y asentar los conocimientos adquiridos en las diferentes asignaturas cursadas en el transcurso del Máster.

La información es un activo que, con el transcurso de los años, está adquiriendo una mayor relevancia dentro de las organizaciones. Por este motivo, es imperativo que la información de las empresas se proteja de forma proporcional a la criticidad que ésta tenga para el negocio, así como a la sensibilidad de la misma.

Con la finalidad de proteger la información de forma adecuada, es necesario conocer qué activos de información forman parte de la organización, realizar una clasificación de éstos en base a las necesidades de disponibilidad, integridad y confidencialidad, así como las necesidades de autenticación y no repudio de los datos con los que va a tratar la organización, tanto de forma interna como con el resto de las partes interesadas de la empresa.

Una vez identificados y clasificados los activos, podremos realizar un análisis de riesgos de seguridad de la información de la compañía mediante el cual conoceremos el estado actual de la seguridad de la información en ésta, estableceremos la línea base, es decir, cuál es el nivel mínimo de seguridad que la empresa está dispuesta a aceptar y se propondrán los proyectos que será necesario llevar a cabo para cubrir la brecha entre el estado inicial y el estado al que la organización quiere llegar.

Este análisis de riesgos, descripción del estado actual, definición del estado deseado y propuesta de proyectos, incorporados al marco establecido en las normas ISO de la serie 27.000 y acompañados de los criterios establecidos en el Modelo de Madurez de la Capacidad (CMM), formarán el Plan Director de Seguridad de la Información, que, aplicado a una cadena hotelera, será el resultado de este trabajo.

1.2 Objetivos del Trabajo

Los principales objetivos de la realización de este plan director son los de:

- Reducir los riesgos asociados a la seguridad de la información, teniendo en cuenta los costes y daños en la imagen de la empresa que los incidentes relacionados pudieran causar, hasta unos niveles aceptables por parte de la organización.

- Asegurar el cumplimiento de la legislación vigente en materia de protección de datos personales.

- Asegurar la continuidad del negocio, reduciendo los tiempos de recuperación de los sistemas, ante posibles incidentes relacionados con la ciberseguridad.

Todo ello, siguiendo los estándares establecidos en la ISO/IEC 27001:2013 e implantando los controles necesarios para asegurar:

- La **disponibilidad** de los sistemas de información necesarios para las operaciones de la empresa.

- La **confidencialidad** de los datos, estableciendo un estricto control de acceso a los mismos para que solo pueda ser accesible a aquellos que tienen derecho a conocerla, con la finalidad de mejorar la confianza de los diferentes "stakeholders" de la organización.

- La **integridad** de los datos, utilizando los medios de protección adecuados para que la información sea protegida ante posibles modificaciones no autorizadas.

- La **autenticidad** y **no repudio**, de tal forma que se pueda confiar en las transacciones y en el intercambio de información que se produce entre las diferentes partes interesadas de la organización.

1.3 Enfoque y método seguido

Para la realización de este plan director de seguridad de la información nos basaremos en el marco establecido en la norma ISO/IEC 27.001 y aplicando el Modelo de Madurez de la Capacidad (CMM) sobre los controles descritos en la ISO/IEC 27.002. Utilizaremos también el modelo para la mejora continua PDCA (Plan-Do-Check-Act) y nos basaremos en la metodología de gestión y análisis de riesgos MAGERIT para la realización del análisis de riesgos.

En el siguiente apartado se describirán las diferentes fases que formarán parte del proyecto.

1.4 Planificación del Trabajo

A continuación, en la tabla 1, se muestran las diferentes fases, así como la planificación temporal para la realización del plan director de seguridad de la información.

Tabla 1: Planificación Plan Director

Fase	Semana														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Fase 1: Situación actual: Contextualización, objetivos y análisis diferencial Introducción al Proyecto. Enfoque y selección de la empresa que será objeto de estudio. Definición de los objetivos del Plan Director de Seguridad y Análisis diferencial de la empresa con respecto a la ISO / IEC 27001 + ISO / IEC 27002															
Fase 2: Sistema de Gestión Documental Elaboración de la Política de Seguridad. Declaración de la aplicabilidad y documentación del SGSI															
Fase 3: Análisis de riesgos Elaboración de una metodología de análisis de riesgos: Identificación y valoración de los activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.															
Fase 4: Propuesta de Proyectos Evaluación de proyectos que debe llevar a cabo la Organización para alinearse con los objetivos planteados en el Plan Director. Cuantificación económica y temporal de estos.															
Fase 5: Auditoría de Cumplimiento de la ISO / IEC 27002: 2013 Evaluación de controles, madurez y nivel de cumplimiento.															
Fase 6: Presentación de Resultados y entrega de Informes Consolidación de los resultados obtenidos durante el proceso de análisis. Realización de los informes y presentación ejecutiva a Dirección. Entrega del proyecto final.															

2. Descripción de la empresa, alcance y análisis diferencial

La empresa sobre la que se realiza este Plan Director de Seguridad de la Información se corresponde con una cadena hotelera con más de 500 trabajadores y que dispone de más de 100 hoteles en su portafolio, tanto en régimen de operación como en régimen de comercialización.

Para los hoteles en régimen de comercialización, las principales funciones de la empresa son:

- Implantación de la marca e imagen de cadena.
- Realización del marketing y la comunicación
- Responsabilidad sobre la distribución y el *revenue management* del hotel.

En cuanto a las actividades relacionadas con los hoteles en operación, además de las descritas en los hoteles en comercialización, se realizan las siguientes funciones:

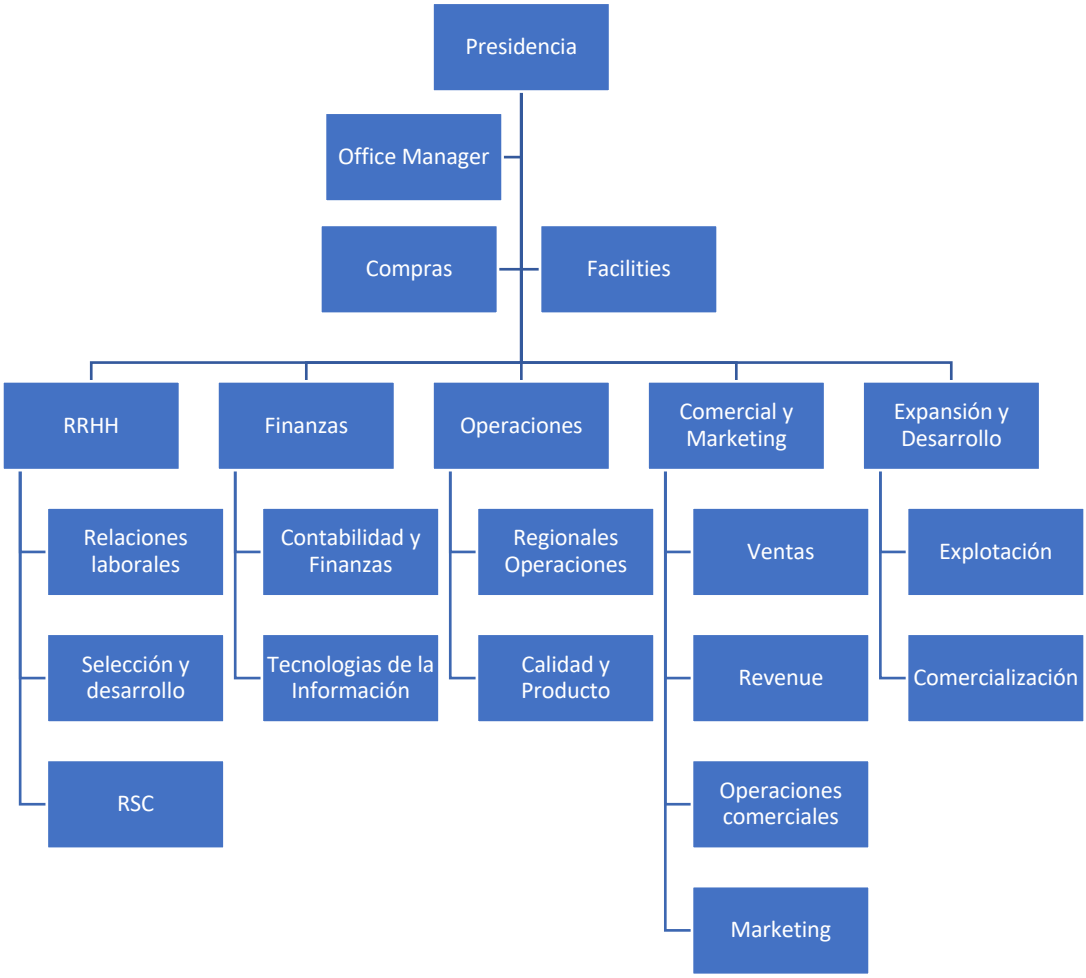
- Calidad, Procesos y formación en las áreas de:
    - Dirección hotelera
    - Recepción
    - Food & Beverage
    - Pisos
    - Mantenimiento
- Gestión en las áreas de:
    - RRHH
    - Compras
    - Finanzas
    - Legal
    - Inversiones

2.1 Estructura organizativa

2.1.1 Estructura organizativa SSCC

A continuación, en la figura 1, se muestra la estructura organizativa de la empresa en relación con los Servicios Centrales de la misma:

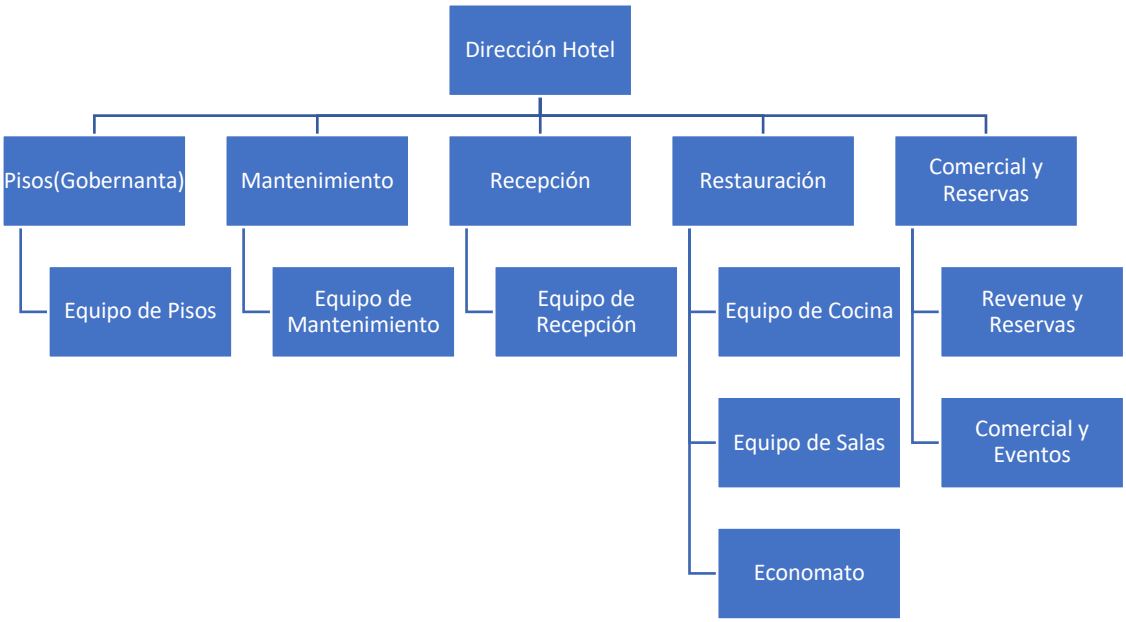
Figura 1:Estructura Organizativa SSCC



2.1.2 Estructura organizativa Hotel

La figura 2 muestra la estructura organizativa que se implanta en los diferentes hoteles del grupo:

Figura 2: Estructura Organizativa Hotel



2.2 Infraestructura Tecnológica

2.1.3 Infraestructura tecnológica en los hoteles

En el hotel existen dos redes de datos independientes, una para uso interno del hotel y la otra es la que utilizan los clientes, vía conector RJ45 o vía wifi para conectarse a internet desde sus dispositivos.

Los hoteles disponen de un servidor principal cuya conexión a la red está protegida mediante un firewall. En este servidor se aloja el programa de gestión de llaves de las habitaciones, el sistema de archivos con el que trabaja el personal interno del hotel y un aplicativo para el acceso al PMS (Property Management System) del hotel. El PMS es el principal programa de gestión del hotel, y aunque el programa en si está instalado en modo cliente, los datos a los que accede están en el cloud.

Los hoteles disponen de un Sistema de Alimentación Ininterrumpido (SAI) con capacidad de mantener durante al menos una hora tanto el servidor y resto de equipamiento ubicado en el Rack de comunicaciones, así como los dos puestos de recepción desde los que se gestionan los check-in y check-out de los clientes.

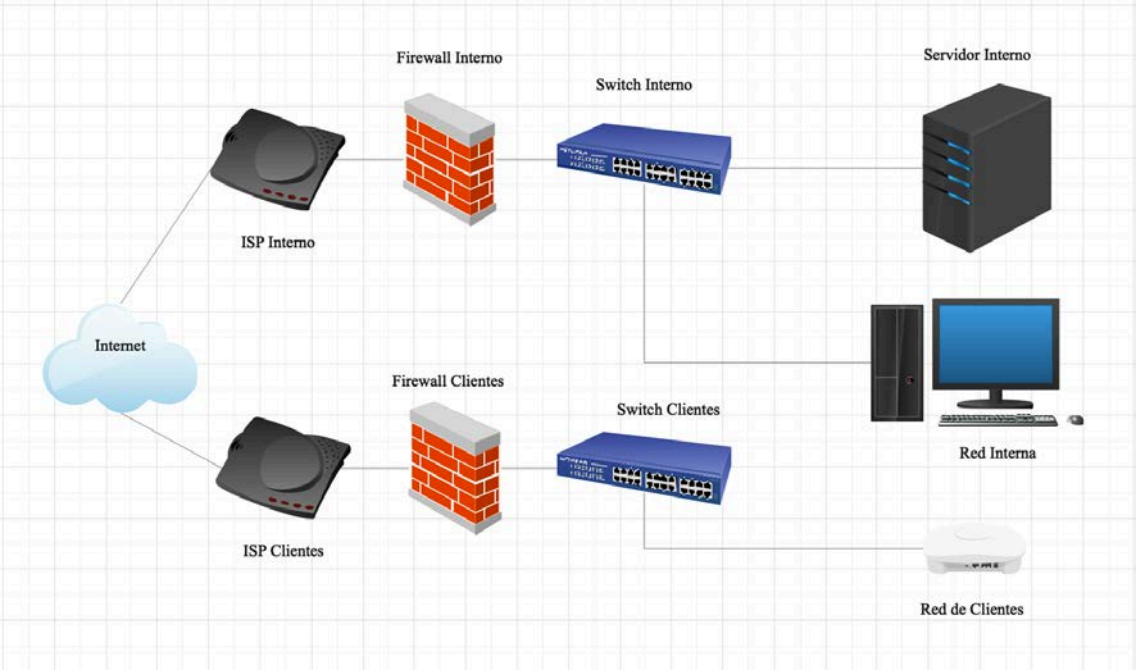
La infraestructura habitual de comunicaciones de los hoteles está compuesta por:

- Red de cableado estructurado UTP categoría 6.
- Tomas de voz y datos RJ 45 para uso interno y en habitaciones.
- Switchs Gigabit Cisco Meraki MS-225-48 de 48 puertos con DHCP snooping, detección y bloqueo.
- Puntos de acceso Wifi Cisco Meraki MR33 con firewall de capa 7 integrado.
- Cortafuegos Meraki MX84 con filtrado de contenido, filtrado de búsquedas web, prevención de intrusión, protección malware y análisis de tráfico a nivel de aplicación.

Los hoteles no disponen de personal interno de Tecnologías de la Información. La gestión de incidencias se contrata con una empresa que realiza todos los servicios relacionados con Help Desk, apoyándose en los Jefes de Mantenimiento de los hoteles.

A continuación, en la figura 3, se muestra el diagrama de red habitual de los hoteles de **Cadena Hotelera**:

Figura 3: Diagrama de red Hotel



2.1.4 Infraestructura tecnológica en SSCC

Los servicios centrales disponen de dos redes de datos independientes, una para uso del personal interno y otra para clientes, proveedores o cualquier otra persona, externa a la organización que acceda a las instalaciones. La conexión a la red interna puede realizarse mediante conector RJ45 o mediante wifi, mientras que la conexión a la red para personal externo a la organización solo está habilitada mediante wifi. Todas las conexiones hacia la red exterior están protegidas mediante un firewall.

El único servidor disponible en los servicios centrales es el que contiene el CRM, el resto de los servidores, como pueden ser el PMS, el BI, o el ERP, están ubicados en un data center externo a la organización con el cual se dispone de un contrato de servicio.

Por otro lado, existen diversos contratos con proveedores externos para diversos servicios cloud con modelos SaaS.

2.3 Alcance

El alcance de este plan director de seguridad de la información contempla todos los sistemas de información utilizados para la gestión, operación y comercialización de los hoteles de la organización, así como las infraestructuras tecnológicas de la empresa utilizadas, tanto por parte del personal interno de la compañía como por parte de clientes y proveedores de ésta.

2.3 Análisis diferencial

Para poder realizar el plan director de seguridad de la información, será necesario conocer previamente la situación inicial de la organización en esta materia, en qué punto se encuentra la empresa, así como definir el estado deseado, dónde quiere llegar. La diferencia entre ambos estados nos mostrará el gap que deberemos cubrir mediante la puesta en marcha de los diferentes proyectos que se establecerán en este plan director.

Para realizar este análisis diferencial aplicaremos el Modelo de Madurez de la Capacidad (CMM) sobre los 114 controles, organizados en 14 áreas y 35 objetivos de control que se definen en la ISO/IEC 27002:2013, lo cuál nos permitirá conocer de forma global el estado actual de la empresa en relación con la Seguridad de la Información.

En la tabla 2 se muestran los criterios que utilizaremos para la aplicación del CMM sobre cada uno de los controles:

Tabla 2: Niveles CMM

CMM - Significado	Efectividad	Descripción
L0 - Inexistente	0%	Carencia completa de cualquier proveso que reconozcamos. No se ha reconocido que exista nongún problema a resolver.
L1 - Inicial / Ad-hoc	10%	Estado inicial donde el éxito de las actividades de los procesos se basa la mayor parte de las veces en un esfuerzo personal. Los procedimientos su inexistentes o localizados en áreas concretas. No existen plantillas definidas en nivel corporativo.
L2 - Reproducible, pero intuitivo	50%	Los procesos similares se llevan a cabo de manera similar por diferentes personas con la misma tarea. Se normalizan las "buenas practicas" en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
L3 - Proceso definido	90%	La organización entera participa al proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
L4 - Gestionado y medible	95%	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tiene que tener herramientas para mejorar la calidad y la eficiencia.
L5 - Optimizado	100%	Los procesos están bajo constante mejora. base criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

En la tabla 3 se muestran los resultados de la evaluación inicial, realizada sobre el estado de la seguridad de la información de la organización, para cada uno de los 114 controles definidos en la ISO/IEC 27002:2013.

Tabla 3:Evaluación controles ISO 27002

CONTROL				Evaluación	Efectividad
A.5. Políticas de la Seguridad de la Información					**5%**
	A.5.1. Directrices de la Dirección en seguridad de la información				5%
		A.5.1.1	Políticas para la Seguridad de la Información	L1 - Inicial / Ad-hoc	10%
		A.5.1.2	Revisión de las Políticas para seguridad de la información	L0 - Inexistente	0%
A.6. Organización de la Seguridad de la Información					46%
	A.6.1. Organización Interna				42%
		A.6.1.1	Seguridad de la información Roles y Responsabilidades	L2 - Reproducible, pero intuitivo	50%
		A.6.1.2	Separación de deberes - Funciones	L2 - Reproducible, pero intuitivo	50%
		A.6.1.3	Contacto con las autoridades	L2 - Reproducible, pero intuitivo	50%
		A.6.1.4	Contacto con grupos de interés Especial	L2 - Reproducible, pero intuitivo	50%
		A.6.1.5	Seguridad de la información en la gestión de proyectos	L1 - Inicial / Ad-hoc	10%
	A.6.2. Dispositivos Móviles y Teletrabajo				50%
		A.6.2.1	Política de uso de dispositivos móviles	L2 - Reproducible, pero intuitivo	50%
		A.6.2.2	Teletrabajo	L2 - Reproducible, pero intuitivo	50%
A.7. Seguridad de los Recursos Humanos					43%
	A.7.1. Antes de la contratación				30%
		A.7.1.1	Investigación de antecedentes	L1 - Inicial / Ad-hoc	10%
		A.7.1.2	Términos y condiciones del empleo	L2 - Reproducible, pero intuitivo	50%
	A.7.2. Durante la ejecución del Empleo				50%
		A.7.2.1	Responsabilidades de la Dirección	L3 - Proceso definido	90%
		A.7.2.2	Toma de Conciencia, educación y formación en la Seg. de la inf.	L1 - Inicial / Ad-hoc	10%
		A.7.2.3	Proceso Disciplinario	L2 - Reproducible, pero intuitivo	50%
	A.7.3. Cese o cambio de puesto de trabajo				50%
		A.7.3.1	Terminación o Cambio de responsabilidades de empleo	L2 - Reproducible, pero intuitivo	50%

A.8. Gestión de Activos					27%
	A.8.1. Responsabilidad por los activos				60%
		A.8.1.1	Inventario de activos	L2 - Reproducible, pero intuitivo	50%
		A.8.1.2	Propiedad de los Activos	L2 - Reproducible, pero intuitivo	50%
		A.8.1.3	Uso aceptable de los Activos	L3 - Proceso definido	90%
		A.8.1.4	Devolución de los Activos	L2 - Reproducible, pero intuitivo	50%
	A.8.2. Clasificación de la información				10%
		A.8.2.1	Directrices de clasificación	L1 - Inicial / Ad-hoc	10%
		A.8.2.2	Etiquetado y manipulado de la información	L1 - Inicial / Ad-hoc	10%
		A.8.2.3	Manipulación de activos	L1 - Inicial / Ad-hoc	10%
	A.8.3. Manejo de medios de soporte				10%
		A.8.3.1	Gestión de medios de soporte removibles	L1 - Inicial / Ad-hoc	10%
		A.8.3.2	Eliminación de soportes	L1 - Inicial / Ad-hoc	10%
		A.8.3.3	Soportes físicos en tránsito	L1 - Inicial / Ad-hoc	10%
A.9. Control de Acceso					55%
	A.9.1. Requisitos del negocio para control de acceso				70%
		A.9.1.1	Política de control de acceso	L2 - Reproducible, pero intuitivo	50%
		A.9.1.2	Acceso a redes y a servicios en red	L3 - Proceso definido	90%
	A.9.2. Gestión de acceso de usuarios.				50%
		A.9.2.1	Gestión de altas/bajas en el registro de usuarios	L3 - Proceso definido	90%
		A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	L2 - Reproducible, pero intuitivo	50%
		A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	L1 - Inicial / Ad-hoc	10%
		A.9.2.4	Gestión de información confidencial de autentic. de usuarios	L2 - Reproducible, pero intuitivo	50%
		A.9.2.5	Revisión de los derechos de acceso de usuarios	L2 - Reproducible, pero intuitivo	50%
		A.9.2.6	Retirada o adaptación de los derechos de acceso	L2 - Reproducible, pero intuitivo	50%
	A.9.3. Responsabilidades de los usuarios				50%
		A.9.3.1	Uso de información confidencial para la autenticación	L2 - Reproducible, pero intuitivo	50%
	A.9.4. Control de Acceso a Sistemas y Aplicaciones				50%
		A.9.4.1	Restricción de acceso a información	L2 - Reproducible, pero intuitivo	50%
		A.9.4.2	Procedimientos seguros de inicio de sesión	L2 - Reproducible, pero intuitivo	50%
		A.9.4.3	Sistema de gestión de contraseñas	L2 - Reproducible, pero intuitivo	50%
		A.9.4.4	Uso de herramientas de administración de sistemas	L2 - Reproducible, pero intuitivo	50%
		A.9.4.5	Control de acceso al código fuente de los programas	L2 - Reproducible, pero intuitivo	50%
A.10 Cifrado					30%
	A.10.1 Controles criptográficos				30%
		A.10.1.1	Política de uso de los controles criptográficos	L1 - Inicial / Ad-hoc	10%
		A.10.1.2	Gestión de claves	L2 - Reproducible, pero intuitivo	50%
A.11. Seguridad física y Ambiental					53%
	A.11.1 Áreas seguras				57%
		A.11.1.1	Perímetro de seguridad física	L2 - Reproducible, pero intuitivo	50%
		A.11.1.2	Controles físicos de entrada	L2 - Reproducible, pero intuitivo	50%
		A.11.1.3	Seguridad de oficinas, despachos y recursos	L2 - Reproducible, pero intuitivo	50%
		A.11.1.4	Protección contra las amenazas externas y ambientales	L2 - Reproducible, pero intuitivo	50%
		A.11.1.5	El trabajo en áreas seguras	L3 - Proceso definido	90%
		A.11.1.6	Áreas de acceso público, carga y descarga	L2 - Reproducible, pero intuitivo	50%
	A.11.2 Seguridad de los equipos				50%
		A.11.2.1	Emplazamiento y protección de equipos	L2 - Reproducible, pero intuitivo	50%
		A.11.2.2	Instalaciones de suministro	L2 - Reproducible, pero intuitivo	50%
		A.11.2.3	Seguridad del cableado	L2 - Reproducible, pero intuitivo	50%
		A.11.2.4	Mantenimiento de los equipos	L2 - Reproducible, pero intuitivo	50%
		A.11.2.5	Salida de activos fuera de las dependencias de la empresa	L2 - Reproducible, pero intuitivo	50%
		A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	L2 - Reproducible, pero intuitivo	50%
		A.11.2.7	Reutilización o retirada segura de dispositivos de almacenam.	L2 - Reproducible, pero intuitivo	50%
		A.11.2.8	Equipo informático de usuario desatendido	L2 - Reproducible, pero intuitivo	50%
		A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	L2 - Reproducible, pero intuitivo	50%
A.12 Seguridad en la Operativa					59%
	A.12.1 Responsabilidades y procedimientos de operación				50%
		A.12.1.1	Documentación de procedimientos de operación	L2 - Reproducible, pero intuitivo	50%
		A.12.1.2	Gestión de cambios	L2 - Reproducible, pero intuitivo	50%
		A.12.1.3	Gestión de capacidades	L2 - Reproducible, pero intuitivo	50%
		A.12.1.4	Separación de entornos de desarrollo, prueba y producción	L2 - Reproducible, pero intuitivo	50%
	A.12.2 Protección contra código malicioso				50%
		A.12.2.1	Controles contra el código malicioso	L2 - Reproducible, pero intuitivo	50%
	A.12.3 Copias de seguridad				90%
		A.12.3.1	Copias de seguridad de la información	L3 - Proceso definido	90%
	A.12.4 Registro de actividad y supervisión				50%
		A.12.4.1	Registro y gestión de eventos de actividad	L2 - Reproducible, pero intuitivo	50%
		A.12.4.2	Protección de los registros de información	L2 - Reproducible, pero intuitivo	50%
		A.12.4.3	Registros de actividad del administrador y operador del sistema	L2 - Reproducible, pero intuitivo	50%
		A.12.4.4	Sincronización de relojes	L2 - Reproducible, pero intuitivo	50%
	A.12.5 Control del software en explotación				90%
		A.12.5.1	Instalación del software en sistemas en producción	L3 - Proceso definido	90%
	A.12.6 Gestión de la vulnerabilidad técnica				70%
		A.12.6.1	Gestión de las vulnerabilidades técnicas	L2 - Reproducible, pero intuitivo	50%
		A.12.6.2	Restricciones en la instalación de software	L3 - Proceso definido	90%
	A.12.7 Consideraciones de las auditorías de los sistemas de información				10%
		A.12.7.1	Controles de auditoría de los sistemas de información	L1 - Inicial / Ad-hoc	10%

A.13. Seguridad en las Telecomunicaciones					47%
	A.13.1 Gestión de la seguridad en las redes				63%
		A.13.1.1	Controles de red	L2 - Reproducible, pero intuitivo	50%
		A.13.1.2	Mecanismos de seguridad asociados a servicios en red	L2 - Reproducible, pero intuitivo	50%
		A.13.1.3	Segregación de redes	L3 - Proceso definido	90%
	A.13.2 Intercambio de información con partes externas				30%
		A.13.2.1	Políticas y procedimientos de intercambio de información	L1 - Inicial / Ad-hoc	10%
		A.13.2.2	Acuerdos de intercambio	L1 - Inicial / Ad-hoc	10%
		A.13.2.3	Mensajería electrónica	L2 - Reproducible, pero intuitivo	50%
		A.13.2.4	Acuerdos de confidencialidad y secreto	L2 - Reproducible, pero intuitivo	50%
A.14. Aquisición, desarrollo y Mantenimiento de los sistemas de información					28%
	A.14.1 Requisitos de seguridad de los sistemas de información				37%
		A.14.1.1	Análisis y especificación de los requisitos de seguridad	L2 - Reproducible, pero intuitivo	50%
		A.14.1.2	Seguridad de las comunicac. en serv. accesibles por redes públ.	L2 - Reproducible, pero intuitivo	50%
		A.14.1.3	Protección de las transacciones por redes telemáticas	L1 - Inicial / Ad-hoc	10%
	A.14.2 Seguridad en los procesos de desarrollo y soporte				37%
		A.14.2.1	Política de desarrollo seguro de software	L1 - Inicial / Ad-hoc	10%
		A.14.2.2	Procedimientos de control de cambios en los sistemas	L2 - Reproducible, pero intuitivo	50%
		A.14.2.3	Rev. técnica de las aplicaciones tras efectuar cambios en el S.O.	L1 - Inicial / Ad-hoc	10%
		A.14.2.4	Restricciones a los cambios en los paquetes de software	L2 - Reproducible, pero intuitivo	50%
		A.14.2.5	Uso de principios de ingeniería en protección de sistemas	L1 - Inicial / Ad-hoc	10%
		A.14.2.6	Seguridad en entornos de desarrollo	L2 - Reproducible, pero intuitivo	50%
		A.14.2.7	Externalización del desarrollo de software	L2 - Reproducible, pero intuitivo	50%
		A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	L2 - Reproducible, pero intuitivo	50%
		A.14.2.9	Pruebas de aceptación	L2 - Reproducible, pero intuitivo	50%
	A.14.3 Datos de prueba				10%
		A.14.3.1	Protección de los datos utilizados en prueba	L1 - Inicial / Ad-hoc	10%
A.15. Relaciones con Suministradores					50%
	A.15.1 Seguridad de la información en las relaciones con suministradores				50%
		A.15.1.1	Política de seguridad de la información para suministradores	L2 - Reproducible, pero intuitivo	50%
		A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	L2 - Reproducible, pero intuitivo	50%
		A.15.1.3	Cadena de suminist. en tecnol. de la inf. y comunicaciones	L2 - Reproducible, pero intuitivo	50%
	A.15.2 Gestión de la prestación del servicio por suministradores				50%
		A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	L2 - Reproducible, pero intuitivo	50%
		A.15.2.2	Gestión de cambios en los servicios prestados por terceros	L2 - Reproducible, pero intuitivo	50%
A.16. Gestión de Incidentes					50%
	A.16.1 Gestión de incidentes de seguridad de la información y mejoras				50%
		A.16.1.1	Responsabilidades y procedimientos	L2 - Reproducible, pero intuitivo	50%
		A.16.1.2	Notificación de los eventos de seguridad de la información	L2 - Reproducible, pero intuitivo	50%
		A.16.1.3	Notificación de puntos débiles de la seguridad	L2 - Reproducible, pero intuitivo	50%
		A.16.1.4	Valorac. de eventos de segur. de la inf. y toma de decisiones	L2 - Reproducible, pero intuitivo	50%
		A.16.1.5	Respuesta a los incidentes de seguridad	L2 - Reproducible, pero intuitivo	50%
		A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	L2 - Reproducible, pero intuitivo	50%
		A.16.1.7	Recopilación de evidencias	L2 - Reproducible, pero intuitivo	50%
A.17. Aspectos de la SI en la Gestión de la Continuidad de Negocio					30%
	A.17.1 Continuidad de la seguridad de la información				10%
		A.17.1.1	Planificación de la continuidad de la seg. de la información	L1 - Inicial / Ad-hoc	10%
		A.17.1.2	Implantación de la continuidad de la seguridad de la informac.	L1 - Inicial / Ad-hoc	10%
		A.17.1.3	Verif., rev. y evaluación de la continuidad de la seg. de la inf.	L1 - Inicial / Ad-hoc	10%
	A.17.2 Redundancias				50%
		A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la inf.	L2 - Reproducible, pero intuitivo	50%
A.18. Cumplimiento					26%
	A.18.1 Cumplimiento de los requisitos legales y contractuales				42%
		A.18.1.1	Identificación de la legislación aplicable	L2 - Reproducible, pero intuitivo	50%
		A.18.1.2	Derechos de propiedad intelectual (DPI)	L2 - Reproducible, pero intuitivo	50%
		A.18.1.3	Protección de los registros de la organización	L2 - Reproducible, pero intuitivo	50%
		A.18.1.4	Protección de datos y privacidad de la información personal	L2 - Reproducible, pero intuitivo	50%
		A.18.1.5	Regulación de los controles criptográficos	L1 - Inicial / Ad-hoc	10%
	A.18.2 Revisiones de la seguridad de la información				10%
		A.18.2.1	Revisión independiente de la seguridad de la información	L1 - Inicial / Ad-hoc	10%
		A.18.2.2	Cumplimiento de las políticas y normas de seguridad	L1 - Inicial / Ad-hoc	10%
		A.18.2.3	Comprobación del cumplimiento	L1 - Inicial / Ad-hoc	10%

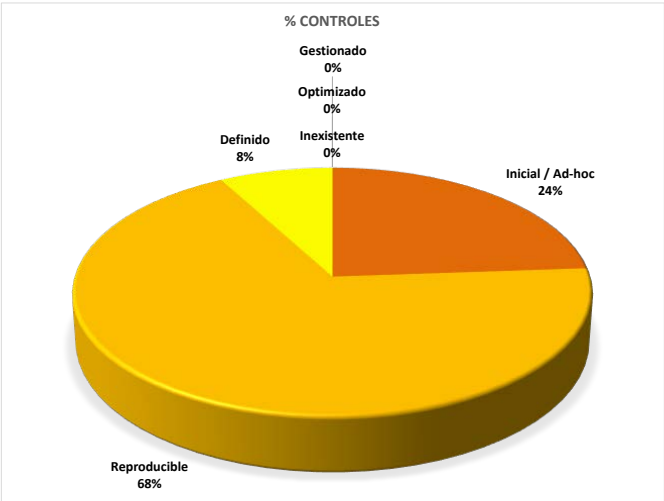
Tal y como podemos observar en la tabla 4, donde mostramos el resultado obtenido en cada una de las 14 áreas establecidas en la ISO/EC 27002:2013, existe bastante potencial de mejora en diversas de las áreas relacionadas con la gestión de la seguridad de la información. Las áreas en las que se encuentran los resultados más bajos serían la correspondiente a las políticas de la seguridad de la información, con un valor del 10%, el área de cumplimiento, con un valor del 26%, la gestión de activos, con un valor del 27% y la adquisición, desarrollo y mantenimiento de los sistemas de información, con un valor del 28%.

Tabla 4: Resultado CMM por área ISO 27002

Área	Valor
A.5. Políticas de la Seguridad de la Información	10%
A.6. Organización de la Seguridad de la Información	46%
A.7. Seguridad de los Recursos Humanos	43%
A.8. Gestión de Activos	27%
A.9. Control de Acceso	55%
A.10 Cifrado	30%
A.11. Seguridad física y Ambiental	53%
A.12 Seguridad en la Operativa	59%
A.13. Seguridad en las Telecomunicaciones	47%
A.14. Aquisición, desarrollo y Mantenimiento de los sistemas de información	28%
A.15. Relaciones con Suministradores	50%
A.16. Gestión de Incidentes	50%
A.17. Aspectos de la SI en la Gestión de la Continuidad de Negocio	30%
A.18. Cumplimiento	26%

En la figura 3 podemos observar que porcentaje de controles se encuentra en cada uno de los estados definidos en el CMM, estando un 68% de los controles en un estado "**reproducible**", un 24% en estado "**inicial/ad-hoc**" y un 8% en estado **"definido"**. Ninguno de los controles se encuentra en los estados **"inexistente"**, **"optimizado"** o **"gestionado"**

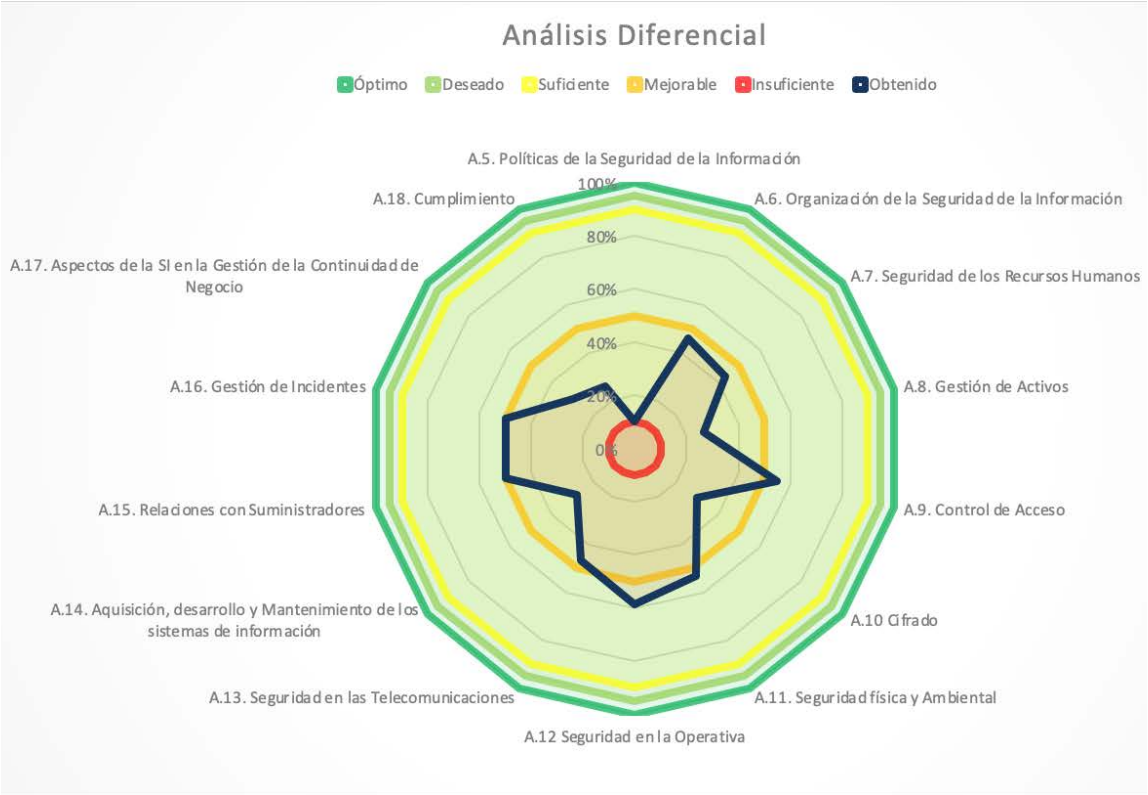
Figura 4: Porcentaje de controles por estado CMM



Nuestro objetivo, tras la implantación de los proyectos que se propondrán en este plan director, será llegar al estado que estableceremos como **“deseado”**, que se corresponderá con el estado definido como **“L4-Gestionado y medible”**, dentro del Modelo de Madurez de la Capacidad.

La figura 4 nos muestra un gráfico, en forma de “diagrama de araña”, en el que podemos ver el resultado obtenido en nuestro análisis diferencial, el cual muestra la diferencia entre el estado “actual” y el estado “deseado”, correspondiente con la gestión de la seguridad de la información, para cada uno de los capítulos descritos en la ISO/EC 27002:2013.

Figura 5: Análisis Diferencial



3. Sistema de Gestión Documental

Para cumplir con lo establecido en la norma ISO/IEC 27001:2013 y poder certificar nuestro Sistema de Gestión de Seguridad de la Información, será necesario disponer de una serie de documentos.

En los diferentes puntos de este capítulo se relacionará y desarrollará la documentación que será más relevante para poder certificar nuestro SGSI.

3.1 Política de Seguridad

La Política de Seguridad es un documento que debe ser aprobado por la Dirección General y que establece la normativa de Seguridad de la Información que deberán conocer y cumplir todos los trabajadores de la organización. En el Anexo I se muestra la política de **Cadena Hotelera**.

3.2 Procedimiento de Auditorías Internas

En el procedimiento de auditorías internas se definirá la forma en la que se llevarán a cabo las auditorías, cuya realización es necesaria durante la vigencia de la certificación. También se establecerá la planificación, así como el modelo de informe de estas auditorías. Podremos encontrar el procedimiento de **Cadena Hotelera** en el Anexo II.

3.3 Gestión de Indicadores

Una vez se hayan implementado los controles que se establezcan en el SGSI, será necesario monitorizar su eficacia. Para ello se establecen una serie de indicadores que podemos encontrar en el Anexo III.

3.4 Procedimiento de Revisión por Dirección

Otro de los aspectos que es de obligado cumplimiento si queremos mantener la certificación de nuestro SGSI es la revisión completa del sistema por parte de la Dirección de la Organización. En el Anexo IV se muestra el procedimiento que indica como se va a realizar esta revisión.

3.5 Gestión de Roles y Responsabilidades

Para poder implementar, mantener, supervisar y mejorar el Sistema de Gestión de la Seguridad de la Información de **Cadena Hotelera**, será necesario contar con un equipo de personas que se impliquen con el proyecto dentro de la organización, idealmente, toda la empresa. Cada una de las personas integrantes de la compañía deberá asumir una serie de roles y responsabilidades los cuales quedan reflejados en el Anexo V del presente documento.

3.6 Metodología de Análisis de Riesgos

Uno de los puntos más importantes, o quizás el más importante, en el desarrollo y durante todo el ciclo de vida de un Sistema de Gestión de Seguridad de la Información, es el Análisis de Riesgos. Para realizar este análisis, es necesario establecer una metodología que indique que pasos debe seguir y en que criterios se debe basar. El Anexo VI nos muestra la metodología que se va a seguir en **Cadena Hotelera**.

3.7 Declaración de Aplicabilidad

La Declaración de Aplicabilidad es un documento obligatorio para cualquier empresa que quiera obtener la certificación ISO 27001, en el que se deben identificar todos los controles de Seguridad de la Información establecidos en la empresa. En el Anexo VII podemos encontrar la Declaración de Aplicabilidad de **Cadena Hotelera**.

4. Análisis de Riesgos

Para poder proteger a la organización frente a los riesgos a los que ésta se encuentra expuesta, necesitaremos realizar previamente un análisis de riesgos. El primer paso del análisis de riesgo será el de identificar los activos de seguridad de la información de la empresa, es decir, ¿Qué debemos proteger?

Una vez dispongamos del inventario de activos, los clasificaremos en función de su tipología y del valor que éstos tienen para la organización, tanto de forma global como para cada una de las dimensiones de seguridad de la información (**A**utenticidad, **C**onfidencialidad, **I**ntegridad, **D**isponibilidad y No repudio o **T**razabilidad). Debido a la dificultad de poder establecer una valoración cuantitativa de los activos, ¿qué coste puede representar para la empresa que un potencial atacante acceda a su base de datos de clientes?, las valoraciones que se realizarán serán cualitativas.

Posteriormente realizaremos un análisis de las amenazas a las que está expuesto cada uno de los tipos de activos existentes en la organización, estableceremos el impacto que pueden tener estas amenazas sobre los activos, así como la frecuencia estimada con la que pueden producirse las mismas.

Conociendo el valor de los activos, las posibles amenazas, su impacto sobre los activos y la frecuencia con la que pueden producirse las mismas, podremos establecer los niveles de riesgo a los que están expuestos cada uno de los activos de la organización, obteniendo de esta forma el resultado del análisis de riesgos.

La metodología que se utilizará para la realización del análisis de riesgos, basada en Magerit, será la que podemos encontrar en el Anexo VI del presente documento.

4.1 Inventario de activos

En el inventario de activos se han considerado tanto los activos relacionados con la seguridad de la información correspondientes a los Servicios Centrales de la empresa como los activos de un hotel tipo.

4.1.1 Inventario activos SSCC

En la tabla 5 se muestra el inventario de los activos de los Servicios centrales de **Cadena Hotelera**. La tabla incluye también la valoración de cada uno de los activos, tanto de forma global como para cada una de las dimensiones de seguridad de la información.

Tabla 5: Inventario activos SSCC

Código	Ámbito	Activo	Valor	Aspectos críticos				
				A	C	I	D	T
CL1	Instalaciones[L]	Sala de comunicaciones SSCC	Muy Alto		9	9	9	
CL2	Instalaciones[L]	Archivo físico	Medio		7	7	7	
CL3	Instalaciones[L]	Oficinas SSCC	Muy Alto		9	9	9	
CD1	Datos[D]	Ficheros	Medio	9	8	8	8	9
CD2	Datos[D]	Datos de clientes	Muy Alto	9	9	9	8	9
CD3	Datos[D]	Datos personal (Nóminas, contratos, datos bancarios,...)	Muy Alto	9	9	9	7	9
CD4	Datos[D]	Información Financiera	Muy Alto	9	9	9	8	9
CD5	Datos[D]	Documentación legal hoteles (Licencias, permisos, legalizaciones,...)	Alto	9	9	9	7	9
CD6	Datos[D]	Contratos y Acuerdos comerciales	Alto	6	9	9	6	6
CD7	Datos[D]	Contratos alquiler	Alto	9	9	9	7	9
CD8	Datos[D]	Procedimientos operativos hoteles	Alto	8	8	9	7	8
CD9	Datos[D]	Contratos con proveedores	Medio	6	6	9	6	6
CD10	Datos[D]	Copias de respaldo (backup)	Muy Alto	9	10	10	8	9
CD11	Datos[D]	Datos de validación de credenciales (usuario, password)	Muy Alto	9	10	10	9	9
CD12	Datos[D]	Certificados de clave pública	Muy Alto	10	10	10	8	10
CD13	Datos[D]	Firmas electrónicas	Muy Alto	10	10	10	8	10
CS1	Servicios[S]	ERP Finanzas	Muy Alto	9	10	9	9	9
CS2	Servicios[S]	CRM (Customer Relationship Management)	Alto	7	10	7	7	7
CS3	Servicios[S]	Data Warehouse	Muy Alto	9	10	9	9	9
CS4	Servicios[S]	Chanel Manager	Alto	8	8	8	9	8
CS5	Servicios[S]	Redes sociales (Instagram, Twitter, Linkedin, Facebook)	Alto	9	3	9	6	9
CS6	Servicios[S]	IDS, IPS	Alto	8	5	8	10	8
CS7	Servicios[S]	Antispam y antimalware	Alto	8	8	8	9	8
CS8	Servicios[S]	CPD Externo	Muy Alto	10	10	10	10	10
CS9	Servicios[S]	Dominios	Muy Alto	9	4	9	10	9
CS10	Servicios[S]	Servidor web corporativa	Muy Alto	9	10	10	10	9
CS11	Servicios[S]	Microsoft Power BI	Muy Alto	9	10	10	9	9
CS12	Servicios[S]	Suministro de servicios de telefonía y datos compañía telefonía (ISP)	Muy Alto	7	7	7	10	7
CS13	Servicios[S]	Gestión de identidades y privilegios	Muy Alto	9	10	10	9	9
CSW1	Aplicaciones informáticas[SW]	Windows 10 ordenadores usuarios	Medio	8	4	8	7	4
CSW2	Aplicaciones informáticas[SW]	Windows Server 2012 Servidor SSCC	Muy Alto	9	9	9	9	8
CSW3	Aplicaciones informáticas[SW]	Paquete Office 365 Business (Herramientas ofimáticas)	Bajo	4	4	4	6	4
CSW4	Aplicaciones informáticas[SW]	Correo electrónico	Alto	6	6	8	8	6
CSW5	Aplicaciones informáticas[SW]	Sistema de backup	Muy Alto	9	10	10	7	9
CHW1	Equipos informáticos[HW]	Servidor principal SSCC	Muy Alto		10	10	10	
CHW2	Equipos informáticos[HW]	Servidor CRM	Alto	8	9	9	7	8
CHW3	Equipos informáticos[HW]	Ordenadores de sobremesa Finanzas	Alto		9	9	8	
CHW4	Equipos informáticos[HW]	Ordenadores de sobremesa RRHH	Alto		9	9	8	
CHW5	Equipos informáticos[HW]	Ordenadores de sobremesa Comercial, Marqueting y Reservas	Alto		7	7	8	
CHW6	Equipos informáticos[HW]	Ordenadores portátiles Operaciones, F&B, FM y Calidad	Alto		9	9	8	
CHW7	Equipos informáticos[HW]	Ordenadores portátiles Expansión	Alto		9	9	8	
CHW8	Equipos informáticos[HW]	Ordenadores portátiles Comité de Dirección	Alto		10	10	9	
CHW9	Equipos informáticos[HW]	Ordenadores portátiles Finanzas	Alto		9	9	8	
CHW10	Equipos informáticos[HW]	Ordenadores portátiles RRHH	Alto		9	9	8	
CHW11	Equipos informáticos[HW]	Ordenadores portátiles Comercial, Marqueting y Reservas	Alto		7	7	8	
CHW12	Equipos informáticos[HW]	Teléfonos móviles	Medio		7	7	9	
CHW13	Equipos informáticos[HW]	Impresoras y escáneres	Bajo		3	3	6	
CHW14	Equipos informáticos[HW]	Router	Muy Alto		9	9	9	
CHW15	Equipos informáticos[HW]	Switchs	Alto		9	9	9	
CHW16	Equipos informáticos[HW]	Firewall	Muy Alto		9	9	9	
CHW17	Equipos informáticos[HW]	Puntos de acceso wifi	Medio		5	5	9	
CHW18	Equipos informáticos[HW]	Central telefónica	Bajo		5	5	9	
CHW19	Equipos informáticos[HW]	Teléfonos IP	Muy Bajo		4	4	6	
CCOM1	Redes de comunicaciones[COM]	Red externa proveedores y clientes WIFI	Medio	5	5	5	9	5
CCOM2	Redes de comunicaciones[COM]	Red interna trabajadores SSCC conexión por cable	Muy Alto	9	9	9	9	9
CCOM3	Redes de comunicaciones[COM]	Red interna trabajadores SSCC WIFI	Muy Alto	9	9	9	9	9
CCOM4	Redes de comunicaciones[COM]	Red de fibra proveedor de servicios	Muy Alto				9	
CMedia1	Soportes de información[Media]	Memorias USB	Medio		5	5	5	
CMedia2	Soportes de información[Media]	Material impreso	Medio		5	5	5	
CMedia3	Soportes de información[Media]	Discos externos	Medio		5	5	5	
CMedia4	Soportes de información[Media]	CD-DVD	Bajo		4	4	4	
CAUX1	Equipamiento auxiliar[AUX]	Sistemas de Alimentación Ininterrumpida (SAIs)	Medio				9	
CAUX2	Equipamiento auxiliar[AUX]	Circuito Cerrado de TV (Cámaras Videovigilancia)	Alto		7	7	9	
CAUX3	Equipamiento auxiliar[AUX]	Control de accesos trabajadores	Muy Bajo		4	4	6	
CAUX4	Equipamiento auxiliar[AUX]	Climatización CPD	Bajo				7	
CAUX5	Equipamiento auxiliar[AUX]	Sistema de detección y extinción de incendios	Muy Alto				9	
CAUX6	Equipamiento auxiliar[AUX]	Cableado de red	ALto		6	6	9	
CAUX7	Equipamiento auxiliar[AUX]	Suministro electricidad	Alto				9	
CAUX8	Equipamiento auxiliar[AUX]	Equipos de destrucción de papel	Muy Bajo		4	4	4	
CP1	Personas[P]	Comité de Dirección	Muy Alto		10	10	10	
CP2	Personas[P]	Departamento relaciones laborales y administración de personal	Alto		9	9	9	
CP3	Personas[P]	Departamento RRHH Selección y formación	Medio		8	8	9	
CP4	Personas[P]	Departamento Contabilidad y Finanzas	Alto		9	9	9	
CP5	Personas[P]	Departamento Tecnologías de la Información	Alto		9	9	9	
CP6	Personas[P]	Departamento Operaciones	Alto		9	9	9	
CP7	Personas[P]	Departamento Calidad y Producto	Medio		8	8	9	
CP8	Personas[P]	Departamento RSC	Medio		8	8	9	
CP9	Personas[P]	Departamento Facility Management	Medio		8	8	9	
CP10	Personas[P]	Departamento F&B	Medio		8	8	9	
CP11	Personas[P]	Departamento de Ventas	Medio		8	8	9	
CP12	Personas[P]	Departamento de Revenue Management	Medio		8	8	9	
CP13	Personas[P]	Departamento comercial	Medio		8	8	9	
CP14	Personas[P]	Departamento de Marketing	Medio		8	8	9	
CP15	Personas[P]	Departamento Expansión y Desarrollo de Negocio	Alto		9	9	9	
CP16	Personas[P]	Proveedores	Bajo		6	6	6	
CP17	Personas[P]	Administradores de sistemas	Alto		9	9	9	

4.1.2 Inventario activos Hotel tipo

En la tabla 6 se muestra el inventario de los activos un hotel tipo de **Cadena Hotelera**. La tabla incluye también la valoración de cada uno de los activos, tanto de forma global como para cada una de las dimensiones de seguridad de la información.

Tabla 6: Inventario activos Hotel tipo

Código	Ámbito	Activo	Valor	Aspectos críticos				
				A	C	I	D	T
HL1	Instalaciones[L]	Sala de comunicaciones hoteles	Muy Alto		9	9	9	
HL2	Instalaciones[L]	Archivo físico	Medio		7	7	7	
HL3	Instalaciones[L]	Hotel	Muy Alto		9	9	9	
HD1	Datos[D]	Ficheros	Medio	9	8	8	8	9
HD2	Datos[D]	Datos de clientes	Muy Alto	9	9	9	8	9
HD3	Datos[D]	Datos personal hotel (Nóminas, contratos, datos bancarios,...)	Muy Alto	9	9	9	7	9
HD4	Datos[D]	Procedimientos operativos hotel	Medio	7	7	9	7	7
HD5	Datos[D]	Contratos con proveedores	Medio	6	6	9	6	6
HD6	Datos[D]	Copias de respaldo (backup)	Muy Alto	9	9	9	8	9
HD7	Datos[D]	Datos de validación de credenciales (usuario, password)	Muy Alto	9	9	9	9	9
HS1	Servicios[S]	PMS (Property Management System)	Muy Alto	9	10	10	10	9
HS2	Servicios[S]	APP servicios clientes hotel (Reservas, Room Service,...)	Medio	6	6	6	8	7
HS3	Servicios[S]	Software gestión de incidencias y procedimientos hotel	Medio	6	6	6	6	6
HS4	Servicios[S]	ERP Finanzas	Muy Alto	9	10	9	9	9
HS5	Servicios[S]	CRM	Alto	7	10	7	7	7
HS6	Servicios[S]	Software de feedback de clientes y reputación online	Medio	6	6	6	6	6
HS7	Servicios[S]	CRS (Computer Reservation System) - Motor de reservas	Muy Alto	9	7	9	10	9
HS8	Servicios[S]	Redes sociales (Instagram, Twitter, Linkedin, Facebook)	Alto	9	3	9	6	9
HS9	Servicios[S]	Dominios hotel	Muy Alto	9	4	9	9	9
HS10	Servicios[S]	Servidor web hotel	Muy Alto	9	10	10	10	9
HS11	Servicios[S]	Suministro de servicios de telefonía y datos compañía telefonía (ISP)	Muy Alto	7	7	7	10	7
HS12	Servicios[S]	Administración de sistemas y helpdesk externalizado	Alto	9	9	9	9	9
HS13	Servicios[S]	Gestión de identidades y privilegios	Muy Alto	9	10	10	9	9
HSW1	Aplicaciones informáticas[SW]	Windows 10 ordenadores usuarios	Medio	8	4	8	7	4
HSW2	Aplicaciones informáticas[SW]	Windows Server 2012 Servidor hotel	Muy Alto	9	9	9	9	8
HSW3	Aplicaciones informáticas[SW]	Paquete Office 365 Business (Herramientas ofimáticas)	Bajo	4	4	4	6	4
HSW4	Aplicaciones informáticas[SW]	Software gestión de llaves habitaciones	Medio	4	6	6	9	4
HSW5	Aplicaciones informáticas[SW]	Correo electrónico	Alto	6	6	8	8	6
HSW6	Aplicaciones informáticas[SW]	Servidor de ficheros	Alto	7	9	9	9	6
HSW7	Aplicaciones informáticas[SW]	Sistema de backup	Muy Alto	9	10	10	7	9
HHW1	Equipos informáticos[HW]	Servidor principal hotel	Muy Alto		10	10	10	
HHW2	Equipos informáticos[HW]	Ordenadores de sobremesa front office y back office	Alto		9	9	9	
HHW3	Equipos informáticos[HW]	Ordenador portátil dirección	Alto		9	9	7	
HHW4	Equipos informáticos[HW]	Datáfono	Alto		10	10	9	
HHW5	Equipos informáticos[HW]	Gravador de llaves habitaciones	Alto		10	10	10	
HHW6	Equipos informáticos[HW]	Ordenadores portátiles equipo comercial	Medio		6	6	7	
HHW7	Equipos informáticos[HW]	Teléfonos móviles	Medio		7	7	9	
HHW8	Equipos informáticos[HW]	Impresoras y escáneres	Bajo		3	3	6	
HHW9	Equipos informáticos[HW]	Router	Muy Alto		9	9	9	
HHW10	Equipos informáticos[HW]	Switchs	Alto		9	9	9	
HHW11	Equipos informáticos[HW]	Firewall	Muy Alto		9	9	9	
HHW12	Equipos informáticos[HW]	Puntos de acceso wifi	Medio		5	5	9	
HHW13	Equipos informáticos[HW]	Central telefónica	Bajo		5	5	9	
HHW14	Equipos informáticos[HW]	Teléfonos IP	Muy Bajo		4	4	6	
HCOM1	Redes de comunicaciones[COM]	Red externa clientes WIFI	Medio	5	5	5	9	5
HCOM2	Redes de comunicaciones[COM]	Red externa clientes conexión por cable	Medio	5	5	5	7	5
HCOM3	Redes de comunicaciones[COM]	Red interna trabajadores hotel	Muy Alto	9	9	9	9	9
HCOM4	Redes de comunicaciones[COM]	Red de fibra proveedor de servicios	Muy Alto				9	
HMedia1	Soportes de información[Media]	Memorias USB	Medio		5	5	5	
HMedia2	Soportes de información[Media]	Material impreso	Medio		5	5	5	
HMedia3	Soportes de información[Media]	Discos externos	Medio		5	5	5	
HMedia4	Soportes de información[Media]	CD-DVD	Bajo		4	4	4	
HAUX1	Equipamiento auxiliar[AUX]	Sistemas de Alimentación Ininterrumpida (SAIs)	Medio				9	
HAUX2	Equipamiento auxiliar[AUX]	Circuito Cerrado de TV (Cámaras Videovigilancia)	Alto		7	7	9	
HAUX3	Equipamiento auxiliar[AUX]	Grupo electrógeno	Medio				7	
HAUX4	Equipamiento auxiliar[AUX]	Control de accesos trabajadores	Muy Bajo		4	4	6	
HAUX5	Equipamiento auxiliar[AUX]	Climatización CPD	Bajo				7	
HAUX6	Equipamiento auxiliar[AUX]	BMS (Building Management System)- Gestión de instalaciones	Medio		4	4	9	
HAUX7	Equipamiento auxiliar[AUX]	Sistema de detección y extinción de incendios	Muy Alto				9	
HAUX8	Equipamiento auxiliar[AUX]	Cableado de red	ALto		6	6	9	
HAUX9	Equipamiento auxiliar[AUX]	Suministro electricidad	Alto				9	
HAUX10	Equipamiento auxiliar[AUX]	Equipos de destrucción de papel	Muy Bajo		4	4	4	
HP1	Personas[P]	Clientes hotel	Muy Bajo		4	4	4	
HP2	Personas[P]	Proveedores	Medio		4	4	7	
HP3	Personas[P]	Director hotel	Alto		9	9	9	
HP4	Personas[P]	Jefes de departamento hotel	Medio		7	7	8	
HP5	Personas[P]	Administradores de sistemas (empresa externa)	Alto		8	8	9	
HP6	Personas[P]	Personal recepción hotel	Alto		8	8	9	
HP7	Personas[P]	Personal administración hotel	Alto		8	8	9	

4.2 Análisis de Amenazas

Basándonos en el catálogo de amenazas que se exponen en el Libro II de Magerit, en la tabla 7 se muestran las posibles amenazas relacionadas con la seguridad de la información, a qué dimensiones afecta cada una de ellas, así como el tipo de activos al que pueden afectar las diferentes amenazas.

Tabla 7: Catálogo de Amenazas

Amenaza	Dimensión					Tipo de Activo afectado								
	A	C	I	D	T	[L]	[HW]	[SW]	[D]	[Media]	[COM]	[S]	[AUX]	[P]
[N] Desastres naturales														
[N.1] Fuego				x		x	x			x			x	
[N.2] Daños por agua				x		x	x			x			x	
[N.*] Otros desastres naturales				x		x	x			x			x	
[I] De origen industrial														
[I.1] Fuego				x		x	x			x			x	
[I.2] Daños por agua				x		x	x			x			x	
[I.*] Desastres industriales				x		x	x			x			x	
[I.4] Contaminación electromagnética				x			x			x			x	
[I.5] Avería de origen físico o lógico				x										
[I.6] Corte de suministro eléctrico				x			x			x			x	
[I.7] Condiciones inadecuadas de temperatura o humedad				x			x			x			x	
[I.8] Fallo de servicios de comunicaciones				x							x			
[I.9] Interrupción de otros servicios y suministros esenciales				x									x	
[I.10] Degradación de los soportes de almacenamiento de la información				x						x				
[E] Errores y fallos no intencionados.														
[E.1] Errores de los usuarios		x	x	x				x	x	x		x		
[E.2] Errores del administrador		x	x	x				x	x	x		x		
[E.3] Errores de monitorización (log)					x				x					
[E.4] Errores de configuración			x						x					
[E.8] Difusión de SW dañino		x	x	x				x						
[E.9] Errores de [re-]encaminamiento		x						x			x	x		
[E.15] Alteración accidental de la información			x			x		x	x	x	x	x		
[E.18] Destrucción de la información				x		x		x	x	x	x	x		
[E.19] Fugas de información		x				x		x	x	x	x	x		x
[E.20] Vulnerabilidades de los programas (SW)		x	x	x				x						
[E.21] Errores de mantenimiento / actualización de programas (SW)			x	x				x						
[E.23] Errores de mantenimiento / actualización de equipos (HW)				x			x			x			x	
[E.24] Caída del sistema por agotamiento de recursos				x			x				x	x		
[E.25] Pérdida de equipos		x		x			x			x			x	
[E.28] Indisponibilidad del personal				x										x
[A] Ataques intencionados														
[A.3]Manipulación de los registros de actividad (log)			x		x				x					
[A.4]Manipulación de la configuración	x	x	x						x					
[A.5]Suplantación de la identidad del usuario	x	x	x					x	x		x	x		
[A.6]Abuso de privilegios de acceso		x	x	x			x	x	x		x	x		
[A.7]Uso no previsto		x	x	x		x	x	x		x	x	x	x	
[A.8]Difusión de software dañino		x	x	x				x						
[A.9] [Re-]encaminamiento de mensajes		x						x			x	x		
[A.10]Alteración de secuencia			x					x			x	x		
[A.11]Acceso no autorizado		x	x			x	x	x	x	x	x	x	x	
[A.12]Análisis de tráfico		x									x			
[A.13]Repudio			x		x				x			x		
[A.14]Interceptación de información (escucha)		x									x			
[A.15]Modificación deliberada de la información			x			x		x	x	x	x	x		
[A.18]Destrucción de información				x		x		x	x	x		x		
[A.19]Divulgación de información		x				x		x	x	x	x	x		
[A.22]Manipulación de programas		x	x	x				x						
[A.23]Manipulación de los equipos		x		x			x			x			x	
[A.24]Denegación de servicio				x			x				x	x		
[A.25]Robo		x		x			x			x			x	
[A.26]Ataque destructivo				x		x	x			x			x	
[A.27]Ocupación enemiga		x		x		x								
[A.28]Indisponibilidad del personal				x										x
[A.29]Extorsión		x	x	x										x
[A.30]Ingeniería social (picaresca)		x	x	x										x

Una vez conocemos a qué activos y a qué dimensiones puede afectar cada una de las amenazas representadas en la tabla 7, haremos una valoración del impacto que pueden tener las diferentes amenazas sobre cada tipo de activo, así como la frecuencia con la que estimamos que pueden producirse. En base al impacto y la frecuencia, estableceremos una valoración base de riesgo para cada tipología de activo, que será el resultado de multiplicar ambos valores.

Valoración base de tipología de activo = Impacto x Frecuencia.

4.2.1 Valoración base de riesgo activos Instalaciones [L]

En la tabla 8 se muestra la valoración base de riesgo de los activos correspondientes a **Instalaciones [L]**.

Tabla 8: Valoración base riesgo Instalaciones

Amenaza	Frecuencia	Impacto					Impacto x Frecuencia				
		A	C	I	D	T	A	C	I	D	T
Instalaciones		**0%**	**100%**	**100%**	**100%**	**0%**	**0**	**50**	**27,5**	**2**	**0**
[N] Desastres naturales											
[N.1] Fuego	0				100%		0	0	0	0	0
[N.2] Daños por agua	0				100%		0	0	0	0	0
[N.*] Otros desastres naturales	0				50%		0	0	0	0	0
[I] De origen industrial											
[I.1] Fuego	0				100%		0	0	0	0	0
[I.2] Daños por agua	0				100%		0	0	0	0	0
[I.*] Desastres industriales	0				50%		0	0	0	0	0
[E] Errores y fallos no intencionados.											
[E.15] Alteración accidental de la información	25			10%			0	0	2,5	0	0
[E.18] Destrucción de la información	0				100%		0	0	0	0	0
[E.19] Fugas de información	25		100%				0	25	0	0	0
[A] Ataques intencionados											
[A.7]Uso no previsto	10		50%	50%	20%		0	5	5	2	0
[A.11]Acceso no autorizado	10		100%	100%			0	10	10	0	0
[A.15]Modificación deliberada de la información	10			100%			0	0	10	0	0
[A.18]Destrucción de información	0				100%		0	0	0	0	0
[A.19]Divulgación de información	10		100%				0	10	0	0	0
[A.26]Ataque destructivo	0				100%		0	0	0	0	0
[A.27]Ocupación enemiga	0		100%		100%		0	0	0	0	0

4.2.2 Valoración base de riesgo activos Hardware [HW]

En la tabla 9 se muestra la valoración base de riesgo de los activos correspondientes a **Hardware [HW]**.

Tabla 9: Valoración base riesgo Hardware

Amenaza	Frecuencia	Impacto					Impacto x Frecuencia				
		A	C	I	D	T	A	C	I	D	T
Hardware		**0%**	**100%**	**50%**	**100%**	**0%**	**0**	**50**	**5,5**	**89,25**	**0**
[N] Desastres naturales											
[N.1] Fuego	0				100%		0	0	0	0	0
[N.2] Daños por agua	0				100%		0	0	0	0	0
[N.*] Otros desastres naturales	0				100%		0	0	0	0	0
[I] De origen industrial											
[I.1] Fuego	0				100%		0	0	0	0	0
[I.2] Daños por agua	0				100%		0	0	0	0	0
[I.*] Desastres industriales	0				100%		0	0	0	0	0
[I.4] Contaminación electromagnética	10				10%		0	0	0	1	0
[I.5] Avería de origen físico o logico	25				50%		0	0	0	12,5	0
[I.6] Corte de suministro eléctrico	25				100%		0	0	0	25	0
[I.7] Condiciones inadecuadas de temperatura o humedad	50				1%		0	0	0	0,5	0
[E] Errores y fallos no intencionados.											
[E.23] Errores de mantenimiento / actualización de equipos (HW)	25				20%		0	0	0	5	0
[E.24] Caída del sistema por agotamiento de recursos	10				50%		0	0	0	5	0
[E.25] Pérdida de equipos	10		50%		100%		0	5	0	10	0
[A] Ataques intencionados											
[A.6]Abuso de privilegios de acceso	25		20%	1%	1%		0	5	0,25	0,25	0
[A.7]Uso no previsto	25		50%	1%	20%		0	12,5	0,25	5	0
[A.11]Acceso no autorizado	10		100%	50%			0	10	5	0	0
[A.23]Manipulación de los equipos	10		100%		50%		0	10	0	5	0
[A.24]Denegación de servicio	10				100%		0	0	0	10	0
[A.25]Robo	10		75%		100%		0	7,5	0	10	0
[A.26]Ataque destructivo	0				100%		0	0	0	0	0

4.2.3 Valoración base de riesgo activos Hardware [SW]

En la tabla 10 se muestra la valoración base de riesgo de los activos correspondientes a **Software [SW]**.

Tabla 10: Valoración base riesgo Software

Amenaza	Frecuencia	Impacto					Impacto x Frecuencia				
		A	C	I	D	T	A	C	I	D	T
Software		**100%**	**100%**	**100%**	**100%**	**0%**	**25**	**167,5**	**157**	**142,5**	**0**
[I] De origen industrial											
[I.5] Avería de origen físico o lógico	50				50%		0	0	0	25	0
[E] Errores y fallos no intencionados.											
[E.1] Errores de los usuarios	75		20%	20%	20%		0	15	15	15	0
[E.2] Errores del administrador	25		20%	20%	20%		0	5	5	5	0
[E.8] Difusión de SW dañino	25		100%	100%	100%		0	25	25	25	0
[E.9] Errores de [re-]encaminamiento	25		10%				0	2,5	0	0	0
[E.15] Alteración accidental de la información	25			20%			0	0	5	0	0
[E.18] Destrucción de la información	10				100%		0	0	0	10	0
[E.19] Fugas de informacion	25		50%				0	12,5	0	0	0
[E.20] Vulnerabilidades de los programas (SW)	50		50%	50%	50%		0	25	25	25	0
[E.21] Errores de mantenimiento / actualización de programas (SW)	25			20%	20%		0	0	5	5	0
[A] Ataques intencionados											
[A.5]Suplantación de la identidad del usuario	25	100%	100%	100%			25	25	25	0	0
[A.6]Abuso de privilegios de acceso	50		20%	20%	20%		0	10	10	10	0
[A.7]Uso no previsto	25		20%	20%	20%		0	5	5	5	0
[A.8]Difusión de software dañino	25		50%	100%	50%		0	12,5	25	12,5	0
[A.9] [Re-]encaminamiento de mensajes	10		50%				0	5	0	0	0
[A.10]Alteración de secuencia	10			20%			0	0	2	0	0
[A.11]Acceso no autorizado	10		100%	50%			0	10	5	0	0
[A.15]Modificación deliberada de la información	0			100%			0	0	0	0	0
[A.18]Destrucción de información	0				100%		0	0	0	0	0
[A.19]Divulgación de información	10		100%				0	10	0	0	0
[A.22]Manipulación de programas	10		50%	50%	50%		0	5	5	5	0

4.2.4 Valoración base de riesgo activos Datos [D]

En la tabla 11 se muestra la valoración base de riesgo de los activos correspondientes a **Datos [D]**.

Tabla 11: Valoración base riesgo Datos

Amenaza	Frecuencia	Impacto					Impacto x Frecuencia				
		A	C	I	D	T	A	C	I	D	T
Datos		**100%**	**100%**	**100%**	**100%**	**50%**	**25**	**87,5**	**75**	**40**	**10**
[E] Errores y fallos no intencionados.											
[E.1] Errores de los usuarios	75		20%	20%	20%		0	15	15	15	0
[E.2] Errores del administrador	25		20%	20%	20%		0	5	5	5	0
[E.3] Errores de monitorización (log)	25					20%	0	0	0	0	5
[E.4] Errores de configuración	25			20%			0	0	5	0	0
[E.15] Alteracion accidental de la información	25			20%			0	0	5	0	0
[E.18] Destrucción de la información	10				100%		0	0	0	10	0
[E.19] Fugas de información	25		50%				0	12,5	0	0	0
[A] Ataques intencionados											
[A.3]Manipulación de los registros de actividad (log)	0			20%		20%	0	0	0	0	0
[A.4]Manipulación de la configuración	0	50%	50%	50%			0	0	0	0	0
[A.5]Suplantación de la identidad del usuario	25	100%	100%	100%			25	25	25	0	0
[A.6]Abuso de privilegios de acceso	50		20%	20%	20%		0	10	10	10	0
[A.11]Acceso no autorizado	10		100%	50%			0	10	5	0	0
[A.13]Repudio	10			50%		50%	0	0	5	0	5
[A.15]Modificación deliberada de la información	0			100%			0	0	0	0	0
[A.18]Destrucción de información	0				100%		0	0	0	0	0
[A.19]Divulgación de información	10		100%				0	10	0	0	0

4.2.5 Valoración base de riesgo activos Soportes de Información [Media]

En la tabla 12 se muestra la valoración base de riesgo de los activos correspondientes a **Soportes de Información [Media]**.

Tabla 12: Valoración base riesgo Soportes de Información

Amenaza	Frecuencia	Impacto					Impacto x Frecuencia				
		A	C	I	D	T	A	C	I	D	T
Soportes de Información		**0%**	**50%**	**50%**	**100%**	**0%**	**0**	**27,5**	**13,5**	**35,5**	**0**
[N] Desastres naturales											
[N.1] Fuego	0				100%		0	0	0	0	0
[N.2] Daños por agua	0				100%		0	0	0	0	0
[N.*] Otros desastres naturales	0				100%		0	0	0	0	0
[I] De origen industrial											
[I.1] Fuego	0				100%		0	0	0	0	0
[I.2] Daños por agua	0				100%		0	0	0	0	0
[I.*] Desastres industriales	0				100%		0	0	0	0	0
[I.4] Contaminación electromagnética	10				10%		0	0	0	1	0
[I.5] Avería de origen físico o lógico	25				50%		0	0	0	12,5	0
[I.6] Corte de suministro eléctrico	25				20%		0	0	0	5	0
[I.7] Condiciones inadecuadas de temperatura o humedad	50				1%		0	0	0	0,5	0
[I.10] Degradación de los soportes de almacenamiento de la información	0				50%		0	0	0	0	0
[E] Errores y fallos no intencionados.											
[E.1] Errores de los usuarios	10		20%	20%	20%		0	2	2	2	0
[E.2] Errores del administrador	10		20%	20%	20%		0	2	2	2	0
[E.15] Alteración accidental de la información	10			20%			0	0	2	0	0
[E.18] Destrucción de la información	0				20%		0	0	0	0	0
[E.19] Fugas de información	10		20%				0	2	0	0	0
[E.23] Errores de mantenimiento / actualización de equipos (HW)	10				10%		0	0	0	1	0
[E.25] Perdida de equipos	10		20%		20%		0	2	0	2	0
[A] Ataques intencionados											
[A.7]Uso no previsto	25		10%	10%	10%		0	2,5	2,5	2,5	0
[A.11]Acceso no autorizado	10		50%	50%			0	5	5	0	0
[A.15]Modificación deliberada de la información	0			50%			0	0	0	0	0
[A.18]Destrucción de información	0				50%		0	0	0	0	0
[A.19]Divulgación de información	10		50%				0	5	0	0	0
[A.23]Manipulación de los equipos	10		20%		20%		0	2	0	2	0
[A.25]Robo	10		50%		50%		0	5	0	5	0
[A.26]Ataque destructivo	0				50%		0	0	0	0	0

4.2.6 Valoración base de riesgo activos Redes de Comunicaciones [COM]

En la tabla 13 se muestra la valoración base de riesgo de los activos correspondientes a **Redes de Comunicaciones [COM]**.

Tabla 13: Valoración base riesgo Redes de Comunicaciones

Amenaza	Frecuencia	Impacto					Impacto x Frecuencia				
		A	C	I	D	T	A	C	I	D	T
Redes de Comunicaciones		**100%**	**100%**	**100%**	**100%**	**50%**	**25**	**135**	**44,5**	**70**	**5**
[I] De origen industrial											
[I.8] Fallo de servicios de comunicaciones	25				100%		0	0	0	25	0
[E] Errores y fallos no intencionados.											
[E.9] Errores de [re-]encaminamiento	25		20%				0	5	0	0	0
[E.15] Alteración accidental de la información	25			20%			0	0	5	0	0
[E.18] Destrucción de la información	10				100%		0	0	0	10	0
[E.19] Fugas de información	25		100%				0	25	0	0	0
[E.24] Caída del sistema por agotamiento de recursos	10				100%		0	0	0	10	0
[A] Ataques intencionados											
[A.5]Suplantación de la identidad del usuario	25	100%	100%	50%			25	25	12,5	0	0
[A.6]Abuso de privilegios de acceso	50		20%	20%	20%		0	10	10	10	0
[A.7]Uso no previsto	25		20%	20%	20%		0	5	5	5	0
[A.9] [Re-]encaminamiento de mensajes	10		100%				0	10	0	0	0
[A.10]Alteración de secuencia	10			20%			0	0	2	0	0
[A.11]Acceso no autorizado	10		100%	50%			0	10	5	0	0
[A.12]Análisis de tráfico	10		100%				0	10	0	0	0
[A.13]Repudio	10			50%		50%	0	0	5	0	5
[A.14]Interceptación de información (escucha)	25		100%				0	25	0	0	0
[A.15]Modificación deliberada de la información	0			100%			0	0	0	0	0
[A.19]Divulgación de información	10		100%				0	10	0	0	0
[A.24]Denegación de servicio	10				100%		0	0	0	10	0

4.2.7 Valoración base de riesgo activos Servicios [S]

En la tabla 14 se muestra la valoración base de riesgo de los activos correspondientes a **Servicios [S]**.

Tabla 14: Valoración base riesgo Servicios

Amenaza	Frecuencia	Impacto					Impacto x Frecuencia				
		A	C	I	D	T	A	C	I	D	T
Servicios		**100%**	**100%**	**100%**	**100%**	**20%**	**10**	**71,5**	**37**	**22,95**	**0**
[E] Errores y fallos no intencionados.											
[E.1] Errores de los usuarios	25		20%	20%	10%		0	5	5	2,5	0
[E.2] Errores del administrador	10		100%	100%	100%		0	10	10	10	0
[E.9] Errores de [re-]encaminamiento	0		50%				0	0	0	0	0
[E.15] Alteración accidental de la información	10			50%			0	0	5	0	0
[E.18] Destrucción de la información	0				100%		0	0	0	0	0
[E.19] Fugas de información	10		100%				0	10	0	0	0
[E.24] Caída del sistema por agotamiento de recursos	0				100%		0	0	0	0	0
[A] Ataques intencionados											
[A.5]Suplantación de la identidad del usuario	10	100%	100%	50%			10	10	5	0	0
[A.6]Abuso de privilegios de acceso	25		50%	20%	1%		0	12,5	5	0,25	0
[A.7]Uso no previsto	20		20%	10%	1%		0	4	2	0,2	0
[A.9] [Re-]encaminamiento de mensajes	0		50%				0	0	0	0	0
[A.10]Alteración de secuencia	0			20%			0	0	0	0	0
[A.11]Acceso no autorizado	10		100%	50%			0	10	5	0	0
[A.13]Repudio	0			20%		20%	0	0	0	0	0
[A.15]Modificación deliberada de la información	0			100%			0	0	0	0	0
[A.18]Destrucción de información	0				100%		0	0	0	0	0
[A.19]Divulgación de información	10		100%				0	10	0	0	0
[A.24]Denegación de servicio	10				100%		0	0	0	10	0

4.2.8 Valoración base de riesgo activos Equipamiento Auxiliar [AUX]

En la tabla 15 se muestra la valoración base de riesgo de los activos correspondientes a **Equipamiento Auxiliar [AUX]**.

Tabla 15: Valoración base riesgo Equipamiento Auxiliar

Amenaza	Frecuencia	Impacto					Impacto x Frecuencia				
		A	C	I	D	T	A	C	I	D	T
Equipamiento auxiliar		**0%**	**50%**	**1%**	**100%**	**0%**	**0**	**18**	**0,35**	**37,85**	**0**
[N] Desastres naturales											
[N.1] Fuego	0				50%		0	0	0	0	0
[N.2] Daños por agua	0				50%		0	0	0	0	0
[N.*] Otros desastres naturales	0				50%		0	0	0	0	0
[I] De origen industrial											
[I.1] Fuego	0				50%		0	0	0	0	0
[I.2] Daños por agua	0				50%		0	0	0	0	0
[I.*] Desastres industriales	0				50%		0	0	0	0	0
[I.4] Contaminación electromagnética	10				1%		0	0	0	0,1	0
[I.5] Avería de origen físico o lógico	10				50%		0	0	0	5	0
[I.6] Corte de suministro eléctrico	25				20%		0	0	0	5	0
[I.7] Condiciones inadecuadas de temperatura o humedad	50				1%		0	0	0	0,5	0
[I.9] Interrupción de otros servicios y suministros esenciales	10				10%		0	0	0	1	0
[E] Errores y fallos no intencionados.											
[E.23] Errores de mantenimiento / actualización de equipos (HW)	25				20%		0	0	0	5	0
[E.25] Pérdida de equipos	10		20%		50%		0	2	0	5	0
[A] Ataques intencionados											
[A.7]Uso no previsto	25		20%	1%	1%		0	5	0,25	0,25	0
[A.11]Acceso no autorizado	10		10%	1%	10%		0	1	0,1	1	0
[A.23]Manipulación de los equipos	10		50%		50%		0	5	0	5	0
[A.25]Robo	10		50%		100%		0	5	0	10	0
[A.26]Ataque destructivo	0				100%		0	0	0	0	0

4.2.9 Valoración base de riesgo activos Personas [P]

En la tabla 16 se muestra la valoración base de riesgo de los activos correspondientes a **Personas [P]**.

Tabla 16: Valoración base riesgo Personas

Amenaza	Frecuencia	Impacto					Impacto x Frecuencia				
		A	C	I	D	T	A	C	I	D	T
Personas		**0%**	**100%**	**20%**	**50%**	**0%**	**0**	**105,25**	**17**	**19,5**	**0**
[E] Errores y fallos no intencionados.											
[E.19] Fugas de información	50		50%				0	25	0	0	0
[E.28] Indisponibilidad del personal	25		1%		20%		0	0,25	0	5	0
[A] Ataques intencionados											
[A.28]Indisponibilidad del personal	10				50%		0	0	0	5	0
[A.29]Extorsión	10		50%	20%	20%		0	5	2	2	0
[A.30]Ingeniería social (picaresca)	75		100%	20%	10%		0	75	15	7,5	0

4.3 Valoración de Riesgos

Una vez disponemos de la valoración base del riesgo para cada tipología de activo que hemos expuesto en el apartado 4.2, así como del valor de los diferentes activos mostrado en el apartado 4.1, solamente nos quedará multiplicar ambos valores para obtener el valor del riesgo para cada uno de los activos del inventario. Debido a que el análisis que realizamos es cualitativo, y no cuantitativo, y con la finalidad de que en el resultado del análisis destaquen los activos críticos de la organización, se le dará un mayor peso al valor de los activos que al impacto de las amenazas. Para ello, emplearemos la siguiente fórmula: **Riesgo= ((Valor activo^2) x (Valor base tipología activo)) / 10**

4.3.1 Valoración riesgo Hotel tipo

En la tabla 17 se muestra la valoración de riesgos de los activos relacionados con la seguridad de la información de un hotel tipo.

Tabla 17: Valoración Riesgo Hotel tipo

Código	Valor	Aspectos críticos					Impacto x Frecuencia					Valor de Riesgo					
		A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	TOTAL
HL1	Muy Alto		9	9	9		0	50	27,5	2	0	0	405	223	16	0	405
HL2	Medio		7	7	7		0	50	27,5	2	0	0	245	135	10	0	245
HL3	Muy Alto		9	9	9		0	50	27,5	2	0	0	405	223	16	0	405
HD1	Medio	9	8	8	8	9	25	87,5	75	40	10	203	560	480	256	81	560
HD2	Muy Alto	9	9	9	8	9	25	87,5	75	40	10	203	709	608	256	81	709
HD3	Muy Alto	9	9	9	7	9	25	87,5	75	40	10	203	709	608	196	81	709
HD4	Medio	7	7	9	7	7	25	87,5	75	40	10	123	429	608	196	49	608
HD5	Medio	6	6	9	6	6	25	87,5	75	40	10	90	315	608	144	36	608
HD6	Muy Alto	9	9	9	8	9	25	87,5	75	40	10	203	709	608	256	81	709
HD7	Muy Alto	9	9	9	9	9	25	87,5	75	40	10	203	709	608	324	81	709
HS1	Muy Alto	9	10	10	10	9	10	71,5	37	22,95	0	81	715	370	230	0	715
HS2	Medio	6	6	6	8	7	10	71,5	37	22,95	0	36	257	133	147	0	257
HS3	Medio	6	6	6	6	6	10	71,5	37	22,95	0	36	257	133	83	0	257
HS4	Muy Alto	9	10	9	9	9	10	71,5	37	22,95	0	81	715	300	186	0	715
HS5	Alto	7	10	7	7	7	10	71,5	37	22,95	0	49	715	181	112	0	715
HS6	Medio	6	6	6	6	6	10	71,5	37	22,95	0	36	257	133	83	0	257
HS7	Muy Alto	9	7	9	10	9	10	71,5	37	22,95	0	81	350	300	230	0	350
HS8	Alto	9	3	9	6	9	10	71,5	37	22,95	0	81	64	300	83	0	300
HS9	Muy Alto	9	4	9	9	9	10	71,5	37	22,95	0	81	114	300	186	0	300
HS10	Muy Alto	9	10	10	10	9	10	71,5	37	22,95	0	81	715	370	230	0	715
HS11	Muy Alto	7	7	7	10	7	10	71,5	37	22,95	0	49	350	181	230	0	350
HS12	Alto	9	9	9	9	9	10	71,5	37	22,95	0	81	579	300	186	0	579
HS13	Muy Alto	9	10	10	9	9	10	71,5	37	22,95	0	81	715	370	186	0	715
HSW1	Medio	8	4	8	7	4	25	167,5	157	142,5	0	160	268	1005	698	0	1005
HSW2	Muy Alto	9	9	9	9	8	25	167,5	157	142,5	0	203	1357	1272	1154	0	1357
HSW3	Bajo	4	4	4	6	4	25	167,5	157	142,5	0	40	268	251	513	0	513
HSW4	Medio	4	6	6	9	4	25	167,5	157	142,5	0	40	603	565	1154	0	1154
HSW5	Alto	6	6	8	8	6	25	167,5	157	142,5	0	90	603	1005	912	0	1005
HSW6	Alto	7	9	9	9	6	25	167,5	157	142,5	0	123	1357	1272	1154	0	1357
HSW7	Muy Alto	9	10	10	7	9	25	167,5	157	142,5	0	203	1675	1570	698	0	1675
HHW1	Muy Alto		10	10	10		0	50	5,5	89,25	0	0	500	55	893	0	893
HHW2	Alto		9	9	9		0	50	5,5	89,25	0	0	405	45	723	0	723
HHW3	Alto		9	9	7		0	50	5,5	89,25	0	0	405	45	437	0	437
HHW4	Alto		10	10	9		0	50	5,5	89,25	0	0	500	55	723	0	723
HHW5	Alto		10	10	10		0	50	5,5	89,25	0	0	500	55	893	0	893
HHW6	Medio		6	6	7		0	50	5,5	89,25	0	0	180	20	437	0	437
HHW7	Medio		7	7	9		0	50	5,5	89,25	0	0	245	27	723	0	723
HHW8	Bajo		3	3	6		0	50	5,5	89,25	0	0	45	5	321	0	321
HHW9	Muy Alto		9	9	9		0	50	5,5	89,25	0	0	405	45	723	0	723
HHW10	Alto		9	9	9		0	50	5,5	89,25	0	0	405	45	723	0	723
HHW11	Muy Alto		9	9	9		0	50	5,5	89,25	0	0	405	45	723	0	723
HHW12	Medio		5	5	9		0	50	5,5	89,25	0	0	125	14	723	0	723
HHW13	Bajo		5	5	9		0	50	5,5	89,25	0	0	125	14	723	0	723
HHW14	Muy Bajo		4	4	6		0	50	5,5	89,25	0	0	80	9	321	0	321
HCOM1	Medio	5	5	5	9	5	25	135	44,5	70	5	63	338	111	567	13	567
HCOM2	Medio	5	5	5	7	5	25	135	44,5	70	5	63	338	111	343	13	343
HCOM3	Muy Alto	9	9	9	9	9	25	135	44,5	70	5	203	1094	360	567	41	1094
HCOM4	Muy Alto				9		25	135	44,5	70	5	0	0	0	567	0	567
HMedia1	Medio		5	5	5		0	27,5	13,5	35,5	0	0	69	34	89	0	89
HMedia2	Medio		5	5	5		0	27,5	13,5	35,5	0	0	69	34	89	0	89
HMedia3	Medio		5	5	5		0	27,5	13,5	35,5	0	0	69	34	89	0	89
HMedia4	Bajo		4	4	4		0	27,5	13,5	35,5	0	0	44	22	57	0	57
HAUX1	Medio				9		0	18	0,35	37,85	0	0	0	0	307	0	307
HAUX2	Alto		7	7	9		0	18	0,35	37,85	0	0	88	2	307	0	307
HAUX3	Medio				7		0	18	0,35	37,85	0	0	0	0	185	0	185
HAUX4	Muy Bajo		4	4	6		0	18	0,35	37,85	0	0	29	1	136	0	136
HAUX5	Bajo				7		0	18	0,35	37,85	0	0	0	0	185	0	185
HAUX6	Medio		4	4	9		0	18	0,35	37,85	0	0	29	1	307	0	307
HAUX7	Muy Alto				9		0	18	0,35	37,85	0	0	0	0	307	0	307
HAUX8	ALto		6	6	9		0	18	0,35	37,85	0	0	65	1	307	0	307
HAUX9	Alto				9		0	18	0,35	37,85	0	0	0	0	307	0	307
HAUX10	Muy Bajo		4	4	4		0	18	0,35	37,85	0	0	29	1	61	0	61
HP1	Muy Bajo		4	4	4		0	105,25	17	19,5	0	0	168	27	31	0	168
HP2	Medio		4	4	7		0	105,25	17	19,5	0	0	168	27	96	0	168
HP3	Alto		9	9	9		0	105,25	17	19,5	0	0	853	138	158	0	853
HP4	Medio		7	7	8		0	105,25	17	19,5	0	0	516	83	125	0	516
HP5	Alto		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674
HP6	Alto		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674
HP7	Alto		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674

4.3.2 Valoración riesgo SSCC

En la tabla 18 se muestra la valoración de riesgos de los activos relacionados con la seguridad de la información de los SSCC de la organización.

Tabla 18: Valoración Riesgo SSCC

Código	Valor	Aspectos críticos					Impacto x Frecuencia					Valor de Riesgo					
		A	C	I	D	T	A	C	I	D	T	A	C	I	D	T	TOTAL
CL1	Muy Alto		9	9	9		0	50	27,5	2	0	0	405	223	16	0	405
CL2	Medio		7	7	7		0	50	27,5	2	0	0	245	135	10	0	245
CL3	Muy Alto		9	9	9		0	50	27,5	2	0	0	405	223	16	0	405
CD1	Medio	9	8	8	8	9	25	87,5	75	40	10	203	560	480	256	81	560
CD2	Muy Alto	9	9	9	8	9	25	87,5	75	40	10	203	709	608	256	81	709
CD3	Muy Alto	9	9	9	7	9	25	87,5	75	40	10	203	709	608	196	81	709
CD4	Muy Alto	9	9	9	8	9	25	87,5	75	40	10	203	709	608	256	81	709
CD5	Alto	9	9	9	7	9	25	87,5	75	40	10	203	709	608	196	81	709
CD6	Alto	6	9	9	6	6	25	87,5	75	40	10	90	709	608	144	36	709
CD7	Alto	9	9	9	7	9	25	87,5	75	40	10	203	709	608	196	81	709
CD8	Alto	8	8	9	7	8	25	87,5	75	40	10	160	560	608	196	64	608
CD9	Medio	6	6	9	6	6	25	87,5	75	40	10	90	315	608	144	36	608
CD10	Muy Alto	9	10	10	8	9	25	87,5	75	40	10	203	875	750	256	81	875
CD11	Muy Alto	9	10	10	9	9	25	87,5	75	40	10	203	875	750	324	81	875
CD12	Muy Alto	10	10	10	8	10	25	87,5	75	40	10	250	875	750	256	100	875
CD13	Muy Alto	10	10	10	8	10	25	87,5	75	40	10	250	875	750	256	100	875
CS1	Muy Alto	9	10	9	9	9	10	71,5	37	22,95	0	81	715	300	186	0	715
CS2	Alto	7	10	7	7	7	10	71,5	37	22,95	0	49	715	181	112	0	715
CS3	Muy Alto	9	10	9	9	9	10	71,5	37	22,95	0	81	715	300	186	0	715
CS4	Alto	8	8	8	9	8	10	71,5	37	22,95	0	64	458	237	186	0	458
CS5	Alto	9	3	9	6	9	10	71,5	37	22,95	0	81	64	300	83	0	300
CS6	Alto	8	5	8	10	8	10	71,5	37	22,95	0	64	179	237	230	0	237
CS7	Alto	8	8	8	9	8	10	71,5	37	22,95	0	64	458	237	186	0	458
CS8	Muy Alto	10	10	10	10	10	10	71,5	37	22,95	0	100	715	370	230	0	715
CS9	Muy Alto	9	4	9	10	9	10	71,5	37	22,95	0	81	114	300	230	0	300
CS10	Muy Alto	9	10	10	10	9	10	71,5	37	22,95	0	81	715	370	230	0	715
CS11	Muy Alto	9	10	10	9	9	10	71,5	37	22,95	0	81	715	370	186	0	715
CS12	Muy Alto	7	7	7	10	7	10	71,5	37	22,95	0	49	350	181	230	0	350
CS13	Muy Alto	9	10	10	9	9	10	71,5	37	22,95	0	81	715	370	186	0	715
CSW1	Medio	8	4	8	7	4	25	167,5	157	142,5	0	160	268	1005	698	0	1005
CSW2	Muy Alto	9	9	9	9	8	25	167,5	157	142,5	0	203	1357	1272	1154	0	1357
CSW3	Bajo	4	4	4	6	4	25	167,5	157	142,5	0	40	268	251	513	0	513
CSW4	Alto	6	6	8	8	6	25	167,5	157	142,5	0	90	603	1005	912	0	1005
CSW5	Muy Alto	9	10	10	7	9	25	167,5	157	142,5	0	203	1675	1570	698	0	1675
CHW1	Muy Alto		10	10	10		0	50	5,5	89,25	0	0	500	55	893	0	893
CHW2	Alto	8	9	9	7	8	0	50	5,5	89,25	0	0	405	45	437	0	437
CHW3	Alto		9	9	8		0	50	5,5	89,25	0	0	405	45	571	0	571
CHW4	Alto		9	9	8		0	50	5,5	89,25	0	0	405	45	571	0	571
CHW5	Alto		7	7	8		0	50	5,5	89,25	0	0	245	27	571	0	571
CHW6	Alto		9	9	8		0	50	5,5	89,25	0	0	405	45	571	0	571
CHW7	Alto		9	9	8		0	50	5,5	89,25	0	0	405	45	571	0	571
CHW8	Alto		10	10	9		0	50	5,5	89,25	0	0	500	55	723	0	723
CHW9	Alto		9	9	8		0	50	5,5	89,25	0	0	405	45	571	0	571
CHW10	Alto		9	9	8		0	50	5,5	89,25	0	0	405	45	571	0	571
CHW11	Alto		7	7	8		0	50	5,5	89,25	0	0	245	27	571	0	571
CHW12	Medio		7	7	9		0	50	5,5	89,25	0	0	245	27	723	0	723
CHW13	Bajo		3	3	6		0	50	5,5	89,25	0	0	45	5	321	0	321
CHW14	Muy Alto		9	9	9		0	50	5,5	89,25	0	0	405	45	723	0	723
CHW15	Alto		9	9	9		0	50	5,5	89,25	0	0	405	45	723	0	723
CHW16	Muy Alto		9	9	9		0	50	5,5	89,25	0	0	405	45	723	0	723
CHW17	Medio		5	5	9		0	50	5,5	89,25	0	0	125	14	723	0	723
CHW18	Bajo		5	5	9		0	50	5,5	89,25	0	0	125	14	723	0	723
CHW19	Muy Bajo		4	4	6		0	50	5,5	89,25	0	0	80	9	321	0	321
CCOM1	Medio	5	5	5	9	5	25	135	44,5	70	5	63	338	111	567	13	567
CCOM2	Muy Alto	9	9	9	9	9	25	135	44,5	70	5	203	1094	360	567	41	1094
CCOM3	Muy Alto	9	9	9	9	9	25	135	44,5	70	5	203	1094	360	567	41	1094
CCOM4	Muy Alto				9		25	135	44,5	70	5	0	0	0	567	0	567
CMedia1	Medio		5	5	5		0	27,5	13,5	35,5	0	0	69	34	89	0	89
CMedia2	Medio		5	5	5		0	27,5	13,5	35,5	0	0	69	34	89	0	89
CMedia3	Medio		5	5	5		0	27,5	13,5	35,5	0	0	69	34	89	0	89
CMedia4	Bajo		4	4	4		0	27,5	13,5	35,5	0	0	44	22	57	0	57
CAUX1	Medio				9		0	18	0,35	37,85	0	0	0	0	307	0	307
CAUX2	Alto		7	7	9		0	18	0,35	37,85	0	0	88	2	307	0	307
CAUX3	Muy Bajo		4	4	6		0	18	0,35	37,85	0	0	29	1	136	0	136
CAUX4	Bajo				7		0	18	0,35	37,85	0	0	0	0	185	0	185
CAUX5	Muy Alto				9		0	18	0,35	37,85	0	0	0	0	307	0	307
CAUX6	ALto		6	6	9		0	18	0,35	37,85	0	0	65	1	307	0	307
CAUX7	Alto				9		0	18	0,35	37,85	0	0	0	0	307	0	307
CAUX8	Muy Bajo		4	4	4		0	18	0,35	37,85	0	0	29	1	61	0	61
CP1	Muy Alto		10	10	10		0	105,25	17	19,5	0	0	1053	170	195	0	1053
CP2	Alto		9	9	9		0	105,25	17	19,5	0	0	853	138	158	0	853
CP3	Medio		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674
CP4	Alto		9	9	9		0	105,25	17	19,5	0	0	853	138	158	0	853
CP5	Alto		9	9	9		0	105,25	17	19,5	0	0	853	138	158	0	853
CP6	Alto		9	9	9		0	105,25	17	19,5	0	0	853	138	158	0	853
CP7	Medio		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674
CP8	Medio		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674
CP9	Medio		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674
CP10	Medio		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674
CP11	Medio		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674
CP12	Medio		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674
CP13	Medio		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674
CP14	Medio		8	8	9		0	105,25	17	19,5	0	0	674	109	158	0	674
CP15	Alto		9	9	9		0	105,25	17	19,5	0	0	853	138	158	0	853
CP16	Bajo		6	6	6		0	105,25	17	19,5	0	0	379	61	70	0	379
CP17	Alto		9	9	9		0	105,25	17	19,5	0	0	853	138	158	0	853

4.4 Nivel de riesgo aceptable

Tras la realización del análisis de riesgo, se establece como nivel de riesgo aceptable 700, con lo que implantaremos los controles necesarios para reducir el riesgo de cada uno de los activos a un valor igual o inferior a este nivel.

4.5 Riesgos a tratar

En las tablas 19 y 20 se muestran los activos con un valor de riesgo superior al nivel aceptable, establecido en 700, que serán los que cogeremos de base para realizar el plan de tratamiento que se llevará a cabo con la propuesta de proyectos de este plan director.

4.5.1 SSCC

Tabla 19: Riesgos a tratar SSCC

Código	Ámbito	Activo	Valor	Valor de Riesgo					
				A	C	I	D	T	TOTAL
CD2	Datos[D]	Datos de clientes	Muy Alto	203	709	608	256	81	709
CD3	Datos[D]	Datos personal (Nóminas, contratos, datos bancarios,...)	Muy Alto	203	709	608	196	81	709
CD4	Datos[D]	Información Financiera	Muy Alto	203	709	608	256	81	709
CD5	Datos[D]	Documentación legal hoteles (Licencias, permisos, legalizaciones,...)	Alto	203	709	608	196	81	709
CD6	Datos[D]	Contratos y Acuerdos comerciales	Alto	90	709	608	144	36	709
CD7	Datos[D]	Contratos alquiler	Alto	203	709	608	196	81	709
CD10	Datos[D]	Copias de respaldo (backup)	Muy Alto	203	875	750	256	81	875
CD11	Datos[D]	Datos de validación de credenciales (usuario, password)	Muy Alto	203	875	750	324	81	875
CD12	Datos[D]	Certificados de clave pública	Muy Alto	250	875	750	256	100	875
CD13	Datos[D]	Firmas electrónicas	Muy Alto	250	875	750	256	100	875
CS1	Servicios[S]	ERP Finanzas	Muy Alto	81	715	300	186	0	715
CS2	Servicios[S]	CRM (Customer Relationship Management)	Alto	49	715	181	112	0	715
CS3	Servicios[S]	Data Warehouse	Muy Alto	81	715	300	186	0	715
CS8	Servicios[S]	CPD Externo	Muy Alto	100	715	370	230	0	715
CS10	Servicios[S]	Servidor web corporativa	Muy Alto	81	715	370	230	0	715
CS11	Servicios[S]	Microsoft Power BI	Muy Alto	81	715	370	186	0	715
CS13	Servicios[S]	Gestión de identidades y privilegios	Muy Alto	81	715	370	186	0	715
CSW1	Aplicaciones informáticas[SW]	Windows 10 ordenadores usuarios	Medio	160	268	1005	698	0	1005
CSW2	Aplicaciones informáticas[SW]	Windows Server 2012 Servidor SSCC	Muy Alto	203	1357	1272	1154	0	1357
CSW4	Aplicaciones informáticas[SW]	Correo electrónico	Alto	90	603	1005	912	0	1005
CSW5	Aplicaciones informáticas[SW]	Sistema de backup	Muy Alto	203	1675	1570	698	0	1675
CHW1	Equipos informáticos[HW]	Servidor principal SSCC	Muy Alto	0	500	55	893	0	893
CHW8	Equipos informáticos[HW]	Ordenadores portátiles Comité de Dirección	Alto	0	500	55	723	0	723
CHW12	Equipos informáticos[HW]	Teléfonos móviles	Medio	0	245	27	723	0	723
CHW14	Equipos informáticos[HW]	Router	Muy Alto	0	405	45	723	0	723
CHW15	Equipos informáticos[HW]	Switchs	Alto	0	405	45	723	0	723
CHW16	Equipos informáticos[HW]	Firewall	Muy Alto	0	405	45	723	0	723
CHW17	Equipos informáticos[HW]	Puntos de acceso wifi	Medio	0	125	14	723	0	723
CHW18	Equipos informáticos[HW]	Central telefónica	Bajo	0	125	14	723	0	723
CCOM2	Redes de comunicaciones[COM]	Red interna trabajadores SSCC conexión por cable	Muy Alto	203	1094	360	567	41	1094
CCOM3	Redes de comunicaciones[COM]	Red interna trabajadores SSCC WIFI	Muy Alto	203	1094	360	567	41	1094
CP1	Personas[P]	Comité de Dirección	Muy Alto	0	1053	170	195	0	1053
CP2	Personas[P]	Departamento relaciones laborales y administración de personal	Alto	0	853	138	158	0	853
CP3	Personas[P]	Departamento RRHH Selección y formación	Medio	0	674	109	158	0	674
CP4	Personas[P]	Departamento Contabilidad y Finanzas	Alto	0	853	138	158	0	853
CP5	Personas[P]	Departamento Tecnologías de la Información	Alto	0	853	138	158	0	853
CP6	Personas[P]	Departamento Operaciones	Alto	0	853	138	158	0	853
CP15	Personas[P]	Departamento Expansión y Desarrollo de Negocio	Alto	0	853	138	158	0	853
CP17	Personas[P]	Administradores de sistemas	Alto	0	853	138	158	0	853

4.5.2 Hoteles

Tabla 20: Riesgos a tratar Hotel tipo

Código	Ámbito	Activo	Valor	Valor de Riesgo					
				A	C	I	D	T	TOTAL
HD2	Datos[D]	Datos de clientes	Muy Alto	203	709	608	256	81	709
HD3	Datos[D]	Datos personal hotel (Nóminas, contratos, datos bancarios,..	Muy Alto	203	709	608	196	81	709
HD6	Datos[D]	Copias de respaldo (backup)	Muy Alto	203	709	608	256	81	709
HD7	Datos[D]	Datos de validación de credenciales (usuario, password)	Muy Alto	203	709	608	324	81	709
HS1	Servicios[S]	PMS (Property Management System)	Muy Alto	81	715	370	230	0	715
HS4	Servicios[S]	ERP Finanzas	Muy Alto	81	715	300	186	0	715
HS5	Servicios[S]	CRM	Alto	49	715	181	112	0	715
HS10	Servicios[S]	Servidor web hotel	Muy Alto	81	715	370	230	0	715
HS13	Servicios[S]	Gestión de identidades y privilegios	Muy Alto	81	715	370	186	0	715
HSW1	Aplicaciones informáticas[SW]	Windows 10 ordenadores usuarios	Medio	160	268	1005	698	0	1005
HSW2	Aplicaciones informáticas[SW]	Windows Server 2012 Servidor hotel	Muy Alto	203	1357	1272	1154	0	1357
HSW4	Aplicaciones informáticas[SW]	Software gestión de llaves habitaciones	Medio	40	603	565	1154	0	1154
HSW5	Aplicaciones informáticas[SW]	Correo electrónico	Alto	90	603	1005	912	0	1005
HSW6	Aplicaciones informáticas[SW]	Servidor de ficheros	Alto	123	1357	1272	1154	0	1357
HSW7	Aplicaciones informáticas[SW]	Sistema de backup	Muy Alto	203	1675	1570	698	0	1675
HHW1	Equipos informáticos[HW]	Servidor principal hotel	Muy Alto	0	500	55	893	0	893
HHW2	Equipos informáticos[HW]	Ordenadores de sobremesa front office y back office	Alto	0	405	45	723	0	723
HHW4	Equipos informáticos[HW]	Datáfono	Alto	0	500	55	723	0	723
HHW5	Equipos informáticos[HW]	Gravador de llaves habitaciones	Alto	0	500	55	893	0	893
HHW7	Equipos informáticos[HW]	Teléfonos móviles	Medio	0	245	27	723	0	723
HHW9	Equipos informáticos[HW]	Router	Muy Alto	0	405	45	723	0	723
HHW10	Equipos informáticos[HW]	Switchs	Alto	0	405	45	723	0	723
HHW11	Equipos informáticos[HW]	Firewall	Muy Alto	0	405	45	723	0	723
HHW12	Equipos informáticos[HW]	Puntos de acceso wifi	Medio	0	125	14	723	0	723
HHW13	Equipos informáticos[HW]	Central telefónica	Bajo	0	125	14	723	0	723
HCOM3	Redes de comunicaciones[COM]	Red interna trabajadores hotel	Muy Alto	203	1094	360	567	41	1094
HP3	Personas[P]	Director hotel	Alto	0	853	138	158	0	853

5. Propuestas de Proyectos

En el análisis de riesgos realizado, se han detectado diversos aspectos que no cumplen con el nivel de riesgo aceptable establecido por parte de la organización.

Podemos afirmar que uno de los aspectos más críticos en cuanto a seguridad de sistemas de información se refiere, es la protección de los datos de clientes y proveedores tal y como se establece en el Reglamento General de Protección de Dados (RGPD).

En la web enforcementtracker.com, podemos ver y clasificar las sanciones, relacionadas con la RGPD, impuestas a diferentes empresas de la Unión Europea. Entre las 5 sanciones más elevadas, podemos encontrar a 2 empresas relacionadas con el sector turístico, British Airways y Marriot International, ambas han recibido sanciones de importe superior a 20 millones de euros por disponer de insuficientes medidas técnicas y organizativas que garantizaran la seguridad de la información.

Figura 6: Ranking Sanciones RGPD UE

	Country	Date	Fine [€]	Controller/Processor	Quoted Art.	Type
	Filter Column		Filter Column	Filter Column		Filter Column
ETID-23	FRANCE	2019-01-21	50,000,000	Google Inc.	Art. 13 GDPR, Art. 14 GDPR, Art. 6 GDPR, Art. 5 GDPR	Insufficient legal basis for data processing
ETID-405	GERMANY	2020-10-01	35,258,708	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
ETID-189	ITALY	2020-01-15	27,800,000	TIM (telecommunications operator)	Art. 5 GDPR, Art. 6 GDPR, Art. 17 GDPR, Art. 21 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing
ETID-58	UNITED KINGDOM	2020-10-16	22,046,000	British Airways	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security
ETID-60	UNITED KINGDOM	2020-10-30	20,450,000	Marriott International, Inc	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security

Del análisis de riesgo realizado, se establece, como otro de los aspectos cuya protección será esencial, tanto en lo relacionado con la confidencialidad como con la integridad, el correspondiente a los datos que contienen información financiera, documentación legal, contratos y acuerdos comerciales, contratos de alquiler, copias de respaldo(backup), datos de validación de credenciales, certificados de clave pública y firmas electrónicas. Para ello será necesario clasificar la información y establecer los permisos de acceso para los diferentes usuarios basándonos en el criterio de acceso exclusivo a la información imprescindible para realizar el trabajo para el que está contratado cada uno de los usuarios.

En relación con los servicios contratados con empresas externas, PMS, ERP, CRM, Servidores web, gestión de identidades y privilegios, Data Warehouse,

CPD Externo y Microsoft Power BI, en base al análisis de riesgo realizado, se establece que será necesario realizar una revisión de los contratos actuales, incorporando en las condiciones de los mismos, Acuerdos de Nivel de Servicio (SLA's) y KPI's basados en las necesidades reales de la organización.

En cuanto a las aplicaciones, como posibles puntos de entrada por parte de los atacantes que puedan conocer sus vulnerabilidades, será necesario disponer de un procedimiento adecuado para la gestión de las actualizaciones de software, así como para la revisión de los logs de los servidores. También será necesario definir e implementar un procedimiento adecuado de copias de seguridad(backup), basado en los Objetivos de Punto de Recuperación (RPO's), así como un Plan de continuidad de negocio basado en los Objetivos de Tiempo de Recuperación (RTO's) que se establezcan. Los RPO's marcarán la periodicidad con la que deben realizarse las copias de seguridad y los RTO's los tiempos que en los que deberá volver a estar operativo el sistema tras un incidente de seguridad.

En referencia a los equipos informáticos, será necesario adoptar medidas de protección frente al uso de ordenadores portátiles y teléfonos móviles, así como sobre los equipos de red, tales como Routers, Switchs, Firewalls y puntos de acceso wifi. Por otro lado, será necesario asegurar que, en todas las instalaciones, la red interna esté separada de las redes que puedan ser utilizadas tanto por clientes como por proveedores.

Finalmente, debemos considerar las personas como uno de los aspectos más críticos relacionados con la seguridad de la información, debido a la información con la que trabajan y a la que pueden obtener acceso. Será esencial que éstas tengan una formación adecuada en ciberseguridad en base al trabajo que desarrollan. Por su criticidad, será imprescindible que las personas que pertenezcan al Comité de Dirección y a los departamentos de RRHH, Finanzas, Tecnologías de la Información, Expansión y Desarrollo de Negocio y Operaciones, así como los directores de los hoteles, dispongan de esta formación.

Con la finalidad de reducir el riesgo relacionado con la Seguridad de la Información **Cadena Hotelera**, a unos niveles aceptables por parte de la organización, basándonos en los aspectos descritos con anterioridad, se propone la implantación de los siguientes proyectos:

- Auditoría cumplimiento RGPD.
- Clasificación de la información.
- Definición de política y gestión de permisos de acceso en base a roles.
- Revisión de contratos y regularización de servicios TIC prestados por terceros.
- Procedimiento actualizaciones de software y revisión de logs.
- Procedimiento de copias de seguridad (backup).
- Procedimiento de configuración de equipos.
- Procedimiento de gestión de incidentes de seguridad.
- Auditoría de seguridad de portal web de reservas.
- Auditoría de seguridad de redes y sistemas.

- Plan de formación en Seguridad de la Información.
- Plan de continuidad de negocio.

5.1 Auditoría cumplimiento RGPD

Tabla 21: Auditoría cumplimiento RGPD

PSI01-Auditoría cumplimiento RGPD					
Objetivos, descripción y alcance					
El objetivo de este proyecto es analizar si la organización cumple con todo lo establecido en la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD), que adapta la legislación española a la normativa europea, definida por el Reglamento General de Protección de Datos (RGPD).					
Solución propuesta					
Se propone contratar a una empresa externa una auditoría independiente para saber si la empresa cumple con lo establecido en la RGPD y tomar las acciones correspondientes en caso de incumplimiento.					
Fases					
Fase 1- Solicitud de presupuestos.					
Fase 2- Análisis y contratación de propuesta seleccionada.					
Fase 3- Realización de auditoría.					
Fase 4- Presentación de resultados.					
Fase 5- Propuesta de correcciones/mejoras					
Fase 6- Implementación de correcciones/mejoras					
Calendario					
2021					
Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6
Riesgos a mitigar					
Filtración datos clientes, trabajadores y terceras partes.Riesgos asociados a datos, servicios, aplicaciones, equipos, redes y personas.					
Beneficios					
Garantizar el cumplimiento de la legislación vigente para evitar posibles sanciones y evitar fugas de información que pudieran causar un gran daño reputacional para la organización.					
Controles ISO relacionados					
A 18					
Coste					10.000 €

5.2 Clasificación de la información

Tabla 22: Clasificación de la información

<table>
<tr><th colspan="4">PSI02-Clasificación de la información</th></tr>
<tr><th colspan="4">Objetivos, descripción y alcance</th></tr>
<tr><td colspan="4">Para trabajar de forma eficiente con la información disponible en la organización, es esencial que ésta se clasifique de forma adecuada. Esto permitirá protegerla frente a posibles amenazas de forma adecuada, así como establecer los permisos de acceso correspondientes en función de los diferentes roles definidos.</td></tr>
<tr><th colspan="4">Solución propuesta</th></tr>
<tr><td colspan="4">Establecer los criterios de clasificación de la información y revisión de toda la documentación de la organización clasificándola en función de los criterios definidos.</td></tr>
<tr><th colspan="4">Fases</th></tr>
<tr><td colspan="4">Fase 1- Establecer criterios de clasificación</td></tr>
<tr><td colspan="4">Fase 2- Reuniones con los diferentes departamentos para presentación proyecto</td></tr>
<tr><td colspan="4">Fase 3- Clasificación de la información</td></tr>
<tr><td colspan="4">Fase 4- Establecimiento de roles de acceso a la información</td></tr>
<tr><th colspan="4">Calendario</th></tr>
<tr><td colspan="3">2021</td><td>2022</td></tr>
<tr><td>Fase 1</td><td>Fase 2</td><td colspan="2">Fase 4</td></tr>
<tr><td></td><td></td><td colspan="2">Fase 3</td></tr>
<tr><th colspan="4">Riesgos a mitigar</th></tr>
<tr><td colspan="4">Confidencialidad, integridad y disponibilidad de la información (datos).</td></tr>
<tr><th colspan="4">Beneficios</th></tr>
<tr><td colspan="4">Una correcta clasificación de la información permitirá protegerla de forma adecuada, así como un acceso a la información con los permisos adecuados y evitar duplicidades y acceso a distintas versiones por parte de diferente personas.</td></tr>
<tr><th colspan="4">Controles ISO relacionados</th></tr>
<tr><td colspan="4">A 8.2</td></tr>
<tr><th colspan="3">Coste</th><td>Personal interno</td></tr>
</table>

5.3 Definición de política y gestión de permisos de acceso en base a roles

Tabla 23: Definición de política y gestión de permisos de acceso en base a roles

PSI03-Definición de política y gestión de permisos de acceso en base a roles			
Objetivos, descripción y alcance			
El principal objetivo de este proyecto es el de establecer quién debe acceder a qué información y con qué permisos.			
Solución propuesta			
Definición de roles de acceso y de la política de control de acceso a la información asignando los roles correspondientes a cada uno de los usuarios.			
Fases			
Fase 1- Definición de roles de acceso.			
Fase 2- Definición de política de acceso a la información en base a roles			
Fase 3- Asignación de roles a cada uno de los usuarios de la organización			
Fase 4- Asignación de permisos en base a roles			
Calendario			
2021			
Fase 1	Fase 2	Fase 3	Fase 4
Riesgos a mitigar			
Confidencialidad, integridad y disponibilidad de la información (datos).			
Beneficios			
Una correcta definición de roles y de la política de acceso a la información, permitirá protegerla de forma adecuada, así como un acceso a la información con los permisos adecuados.			
Controles ISO relacionados			
A.9			
Coste			Personal interno

5.4 Revisión de contratos y regularización de servicios TIC prestados por terceros

Tabla 24: Revisión de contratos y regularización de servicios TIC prestados por terceros

PSI04-Revisión de contratos y regularización de servicios TIC prestados por terceros							
Objetivos, descripción y alcance							
El objetivo de este proyecto es el de revisar todos los contratos relacionados con las TIC prestados por terceros con la finalidad de establecer en los mismos los KPI's necesarios para mitigar y transferir los riesgos relacionados con la Seguridad de la Información de los servicios contratados.							
Solución propuesta							
Revisión de todos los contratos de servicios TIC prestados por terceros, diseñando los KPI's correspondientes para mitigar y transferir los riesgos relativos a la Seguridad de la Información asociados a los mismos, firmando nuevos contratos o añadiendo anexos a los actuales.							
Fases							
Fase 1- Revisión de contratos							
Fase 2- Establecer KPI's							
Fase 3- Negociar inclusión de KPI's en contrato con proveedores							
Fase 4- Inclusión de KPI's en contrato							
Fase 5- Firmar nuevos contratos incluyendo los KPI's							
Calendario							
2021							
Fase 1	Fase 2	Fase 3	Fase 4	Fase 5			
Riesgos a mitigar							
Riesgo relacionado con los servicios prestados por terceros (servicios).							
Beneficios							
Los principales beneficios de este proyecto están relacionados con la mitigación y transferencia de los riesgos asociados a los servicios prestados por terceros.							
Controles ISO relacionados							
A.15							
Coste						Personal interno	

5.5 Procedimiento actualizaciones de software y revisión de logs

Tabla 25: Procedimiento actualizaciones de software y revisión de logs

PSI05-Procedimiento actualizaciones de software y revisión de logs							
Objetivos, descripción y alcance							
El objetivo de este proyecto es el de reducir los riesgos relacionados con las vulnerabilidades existentes en las versiones no actualizadas de software.							
Solución propuesta							
Implantación de procedimiento de actualización de software en el que se definan las aplicaciones afectadas así como la periodicidad de revisión de las actualizaciones.							
Fases							
Fase 1- Definición y propuesta de procedimiento							
Fase 2- Revisión y aprobación de procedimiento							
Fase 3- Publicacioón de procedimiento.							
Fase 4- Aplicación de procedimiento							
Calendario							
2021							
Fase 1	Fase 2	Fase 3	Fase 4				
Riesgos a mitigar							
Vulnerabilidades de software no actualizado (aplicaciones).							
Beneficios							
Evitar las amenazas aprovechadas por potenciales atacantes relacionadas con vulnerabilidades conocidas y originadas al no disponer del software actualizado.							
Controles ISO relacionados							
A 11.2.4, A 12.5.1, A 12.6.1							
Coste						Personal interno	

5.6 Procedimiento de copias de seguridad (backup)

Tabla 26: Procedimiento de copias de seguridad (backup)

PSI06-Procedimiento de copias de seguridad (backup)							
Objetivos, descripción y alcance							
El objetivo de este procedimiento es el de definir la información de la cual se debe realizar copias de seguridad así como la periodicidad de las copias para cada tipo de información con la finalidad de poder restaurar los sistemas en caso de ocurrencia de incidentes relacionados con la Seguridad de la Información.							
Solución propuesta							
Realización de procedimiento en el que se defina qué información debe disponer de copia de seguridad, así como la periodicidad con la que se deben realizar las copias en función de la importancia de la misma y que se basará en el Objetivo de Punto de Recuperación (RPO) que se haya establecido para cada uno de los procesos de la organización.							
Fases							
Fase 1- Definir qué información debe disponer de copia de seguridad							
Fase 2- Establecer los RPO's para cada tipo de información							
Fase 3- Definición y propuesta de procedimiento							
Fase 4- Revisión y aprobación de procedimiento							
Fase 5- Publicacioón de procedimiento.							
Fase 6- Aplicación de procedimiento							
Calendario							
2021							
Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6		
Riesgos a mitigar							
Riesgo de pérdida de información por falta de backup (datos, servicios y aplicaciones)							
Beneficios							
Permite recuperar información en base a su criticidad para el negocio.							
Controles ISO relacionados							
A 12.3.1							
Coste						Personal interno	

5.7 Procedimiento de configuración de equipos

Tabla 27: Procedimiento de configuración de equipos

PSI07-Procedimiento de configuración de equipos							
Objetivos, descripción y alcance							
El objetivo principal de la definición de un procedimiento para la configuración de equipos es el de estandarizar dichas configuraciones para disponer de la protección adecuada ante amenazas que puedan producir incidentes relacionados con la Seguridad de la Información.							
Solución propuesta							
Realización de procedimiento que establezca la configuración de los diferentes equipos, tales como ordenadores, routers, firewalls, y cualquier otro equipo relacionado con las TIC utilizando ls mejores prácticas en materia de Seguridad de la Información.							
Fases							
Fase 1- Definición y propuesta de procedimiento							
Fase 2- Revisión y aprobación de procedimiento							
Fase 3- Publicacioón de procedimiento.							
Fase 4- Aplicación de procedimiento							
Calendario							
2021							
Fase 1	Fase 2	Fase 3	Fase 4				
Riesgos a mitigar							
Riesgos relacionados con la configuración de equipos (aplicaciones, equipos y redes).							
Beneficios							
Permite la estandarización de las configuraciones para obtener una protección óptima ante las amenzas relacionadas con la Seguridad de la Información.							
Controles ISO relacionados							
A 9.4, A 11.2.4, A 12.5, A 12.6, A 14.2.4							
Coste						Personal interno	

5.8 Procedimiento de gestión de incidentes de seguridad

Tabla 28: Procedimiento de gestión de incidentes de seguridad

PSI08-Procedimiento de gestión de incidentes de seguridad							
Objetivos, descripción y alcance							
El objetivo de este proyecto es el de la implantación de un procedimiento de gestión de incidentes, que permita detectar los incidentes relacionados con la seguridad de la información de forma ágil, así como reaccionar de la forma adecuada para su mitigación.							
Solución propuesta							
Creación de procedimiento para la detección y contención de incidentes relacionados con la seguridad de la información.							
Fases							
Fase 1- Definición y propuesta de procedimiento							
Fase 2- Revisión y aprobación de procedimiento							
Fase 3- Publicacioón de procedimiento.							
Fase 4- Aplicación de procedimiento							
Calendario							
2021							
Fase 1	Fase 2	Fase 3	Fase 4				
Riesgos a mitigar							
Riesgos asociados a datos, servicios, aplicaciones, equipos, redes y personas.							
Beneficios							
Permitirá reducir los tiempos de respuesta y de contención ante los incidentes de seguridad que puedan producirse en la organización.							
Controles ISO relacionados							
A 16.1							
Coste						Personal interno	

5.9 Auditoría de seguridad de portal web de reservas

Tabla 29: Auditoría de seguridad de portal web de reservas

PSI09-Auditoría de seguridad de portal web de reservas						
Objetivos, descripción y alcance						
El principal objetivo de este proyecto es el de detectar las vulnerabilidades del portal web de reservas con la finalidad de tomar las medidas adecuadas para minimizar los riesgos, protegiendo la información contenida en el mismo, así como garantizando su disponibilidad.						
Solución propuesta						
Se propone contratar a una empresa externa una auditoría independiente de pentesting del portal web para conocer las vulnerabilidades del mismo y tomar las acciones correspondientes para minimizar los riesgos derivados de éste.						
Fases						
Fase 1- Solicitud de presupuestos.						
Fase 2- Análisis y contratación de propuesta seleccionada.						
Fase 3- Realización de auditoría.						
Fase 4- Presentación de resultados.						
Fase 5- Propuesta de correcciones/mejoras						
Fase 6- Implementación de correcciones/mejoras						
Calendario						
2021						
Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6	
Riesgos a mitigar						
iesgo de servicios y aplicaciones, concretamente de los relacionados con el portal wel						
Beneficios						
Permitirá conocer las vulnerabilidades del portal web y tomar las acciones necesarias para mitigar los riesgos existentes, protegiendo al mismo ante las potenciales amenazas.						
Controles ISO relacionados						
A 18.1.3, A.18.1.4, A.18.2						
Coste					5000	

5.10 Auditoría de seguridad de redes y sistemas

Tabla 30: Auditoría de Seguridad de redes y sistemas

PSI10-Auditoría de seguridad de redes y sistemas						
Objetivos, descripción y alcance						
El principal objetivo de este proyecto es el de detectar las vulnerabilidades en la infraestructura de red de la organización con la finalidad de tomar las medidas adecuadas para minimizar los riesgos asociados a la información que se transmite sobre la misma.						
Solución propuesta						
Se propone contratar a una empresa externa una auditoría independiente para conocer las vulnerabilidades de las infraestructuras de red y de los sistemas de la organización y tomar las acciones correspondientes para minimizar los riesgos relacionados con ello.						
Fases						
Fase 1- Solicitud de presupuestos.						
Fase 2- Análisis y contratación de propuesta seleccionada.						
Fase 3- Realización de auditoría.						
Fase 4- Presentación de resultados.						
Fase 5- Propuesta de correcciones/mejoras						
Fase 6- Implementación de correcciones/mejoras						
Calendario						
2021						
Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6	
Riesgos a mitigar						
Riesgos de infraestructura de red y sistemas.						
Beneficios						
Permitirá conocer las vulnerabilidades de las redes existentes y protegerlas ante las potenciales amenazas.						
Controles ISO relacionados						
A 18.1.3, A.18.1.4, A.18.2						
Coste						5000

5.11 Plan de formación en Seguridad de la Información

Tabla 31: Plan de formación en Seguridad de la Información

PSI11-Plan de formación en Seguridad de la Información					
Objetivos, descripción y alcance					
Formar a la dirección de la organización en materia de ciberseguridad para que tome conciencia de las vulnerabilidades de la empresa, así como de las amenazas a la que ésta está expuesta y al mismo tiempo se convierta en promotora de la aplicación de las medidas necesarias para protegerse en el ciberespacio.					
Solución propuesta					
Contratación de formación especializada en ciberseguridad que impartirá un experto en la materia.					
Fases					
Fase 1- Búsqueda de formadores y solicitud de presupuestos.					
Fase 2- Análisis y contratación de propuesta seleccionada.					
Fase 3- Impartición de la formación					
Calendario					
2021					
Fase 1	Fase 2	Fase 3			
Riesgos a mitigar					
Riesgo de uso indebido de la información y de los sistemas que la soportan por falta de conocimiento (Personas).					
Beneficios					
Concienciar a la dirección de la necesidad de protegerse frente a las amenazas a las que está sometida la organización en materia de ciberseguridad, lo que ayudará a transmitir al resto de personas de la empresa la necesidad de protección ante estas amenazas .					
Controles ISO relacionados					
A 7.2.2					
Coste					10000

5.12 Plan de continuidad de negocio

Tabla 32: Plan de continuidad de negocio

PSI12-Plan de continuidad de negocio			
Objetivos, descripción y alcance			
El objetivo de este proyecto es el de poder garantizar que la organización pueda continuar y/o restablecer sus procesos en forma, tiempo y coste adecuados ante la ocurrencia de incidentes que afecten a la seguridad de la información.			
Solución propuesta			
Realización de un plan de continuidad de negocio en base al análisis de impacto en el negocio realizado para cada uno de los procesos críticos de la organización y establecimiento de las medidas a tomar ante la materialización de amenazas que puedan afectar a los mismos definiendo los Objetivos de Tiempo de Recuperación (RTO) y el Objetivo del Punto de Recuperación de los datos (RPO).			
Fases			
Fase 1- Revisión con los responsables de departamento de los procesos críticos.			
Fase 2- Realización de Análisis de Impacto en el Negocio (BIA)			
Fase 3- Definición de RTO y RPO			
Fase 4- Definición del plan de respuesta a incidentes			
Fase 5- Realización del Plan de Continuidad de Negocio.			
Calendario			
2021			
Fase 1			Fase 4
	Fase 2	Fase 3	Fase 5
Riesgos a mitigar			
Riesgos asociados a datos, servicios, aplicaciones, equipos, redes y personas.			
Beneficios			
Permitirá continuar o restablecer las operaciones de la organización en un tiempo óptimo teniendo en cuenta la relación coste/beneficio de las medidas a tomar.			
Controles ISO relacionados			
A 17			
Coste			Personal interno

5.13 Resumen de proyectos

Tabla 33: Resumen de proyectos

Id	Proyecto	2021				2022				Coste
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
PSI01	Auditoría cumplimiento RGPD									10.000 €
PSI02	Clasificación de la información									Personal interno
PSI03	Definición de política y gestión de permisos de acceso en base a roles									Personal interno
PSI04	Revisión de contratos y regularización de servicios TIC prestados por terceros									Personal interno
PSI05	Procedimiento actualizaciones de software y revisión de logs									Personal interno
PSI06	Procedimiento de copias de seguridad (backup)									Personal interno
PSI07	Procedimiento de configuración de equipos									Personal interno
PSI08	Procedimiento de gestión de incidentes de seguridad									Personal interno
PSI09	Auditoría de seguridad de portal web de reservas									5.000 €
PSI10	Auditoría de seguridad de redes y sistemas									5.000 €
PSI11	Plan de formación en Seguridad de la Información									10.000 €
PSI12	Plan de continuidad de negocio									Personal interno
									Coste Total	30.000 €

5.14 Evolución cumplimiento dominios ISO/IEC 27002

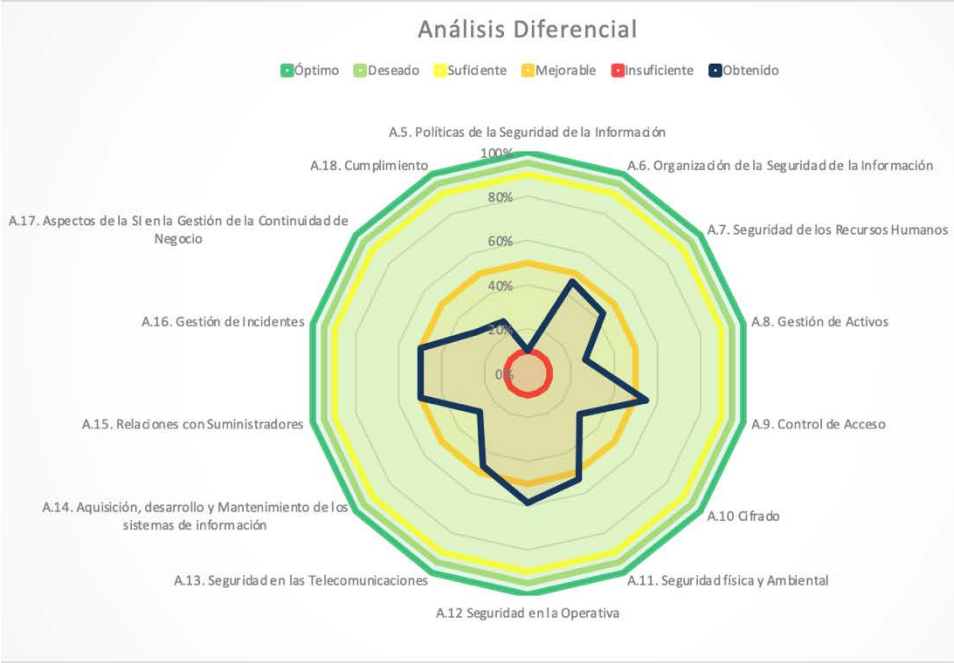
Tras la implementación de los proyectos propuestos, obtendremos una importante mejora en cuanto a la gestión de la Seguridad de la Información dentro de la Organización, avanzando hacia el objetivo que nos habíamos marcado inicialmente, el de llegar al estado definido como **"L4-Gestionado y medible"**, dentro del Modelo de Madurez de la Capacidad(CMM).

Dentro de los proyectos propuestos, los correspondientes a auditoría nos permitirán conocer con mayor profundidad nuevas necesidades no detectadas en esta fase inicial, que siguiendo un modelo de mejora continua (Plan, Do, Check, Act), con toda seguridad, nos permitirá llegar al estado CMM deseado en un par de años.

La figura 8 nos muestra cual será el estado de los dominios definidos en la ISO 27002 tras la implementación de los proyectos propuestos. En ella podremos ver la notable mejora respecto al estado inicial representado en la figura 7.

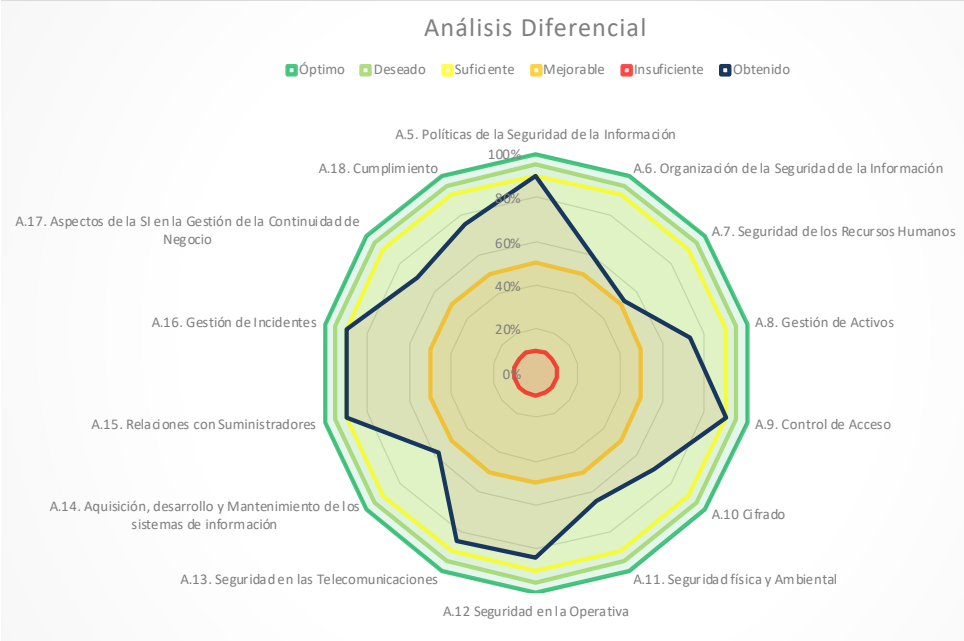
5.14.1 Estado Inicial

Figura 7: Estado inicial dominios ISO 27002



5.14.2 Estado tras implementación proyectos

Figura 8: Estado tras implantación proyectos dominios ISO 27002

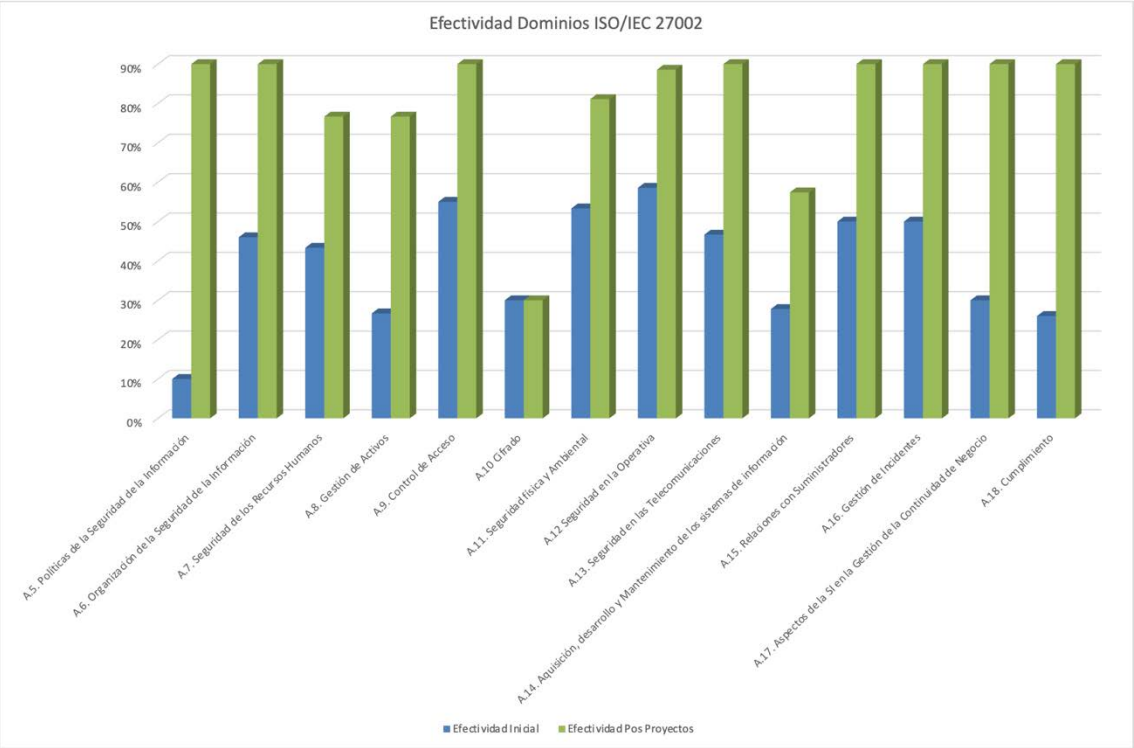


6. Auditoría de cumplimiento

Una vez han sido implementados los proyectos descritos en el capítulo 4, es el momento de realizar una auditoría para conocer el estado de la seguridad de la información de la organización. Para ello, la auditoría se basará en realizar una revisión del estado en el que se encuentran, dentro del modelo CMM, cada uno de los dominios que se establecen en la ISO/IEC 27002:2013.

En el Anexo VIII, podemos ver el informe de auditoría, en cuyos resultados, que también se muestran de forma gráfica en la figura 9, podemos observar la mejora producida sobre cada uno de los dominios establecidos en la ISO 27002 tras la implementación de los proyectos definidos en el Plan Director.

Figura 9: Evolución dominios ISO/IEC 27002



A pesar de haberse producido importantes mejoras en cada uno de los dominios, durante la auditoria se han detectado algunas no conformidades, las cuales se muestran en la tabla 34. En el Anexo VIII podemos encontrar el detalle de las mismas, así como las acciones correctivas a aplicar para la resolución de éstas.

Tabla 34: Controles ISO 27002 con No Conformidades

CONTROL				Cumplimiento
A.7. Seguridad de los Recursos Humanos				
	A.7.1. Antes de la contratación			
		A.7.1.1	Investigación de antecedentes	No
A.8. Gestión de Activos				
	A.8.3. Manejo de medios de soporte			
		A.8.3.1	Gestión de medios de soporte removibles	No
		A.8.3.2	Eliminación de soportes	No
		A.8.3.3	Soportes físicos en tránsito	No
A.10 Cifrado				
	A.10.1 Controles criptográficos			
		A.10.1.1	Política de uso de los controles criptográficos	No
		A.10.1.2	Gestión de claves	No
A.11. Seguridad física y Ambiental				
	A.11.1 Áreas seguras			
		A.11.1.1	Perímetro de seguridad física	No
		A.11.1.6	Áreas de acceso público, carga y descarga	No
	A.11.2 Seguridad de los equipos			
		A.11.2.7	Reutilización o retirada segura de dispositivos de almacenam.	No
A.12 Seguridad en la Operativa				
	A.12.1 Responsabilidades y procedimientos de operación			
		A.12.1.4	Separación de entornos de desarrollo, prueba y producción	No
A.14. Aquisición, desarrollo y Mantenimiento de los sistemas de información				
	A.14.2 Seguridad en los procesos de desarrollo y soporte			
		A.14.2.1	Política de desarrollo seguro de software	No
		A.14.2.6	Seguridad en entornos de desarrollo	No
		A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	No
	A.14.3 Datos de prueba			
		A.14.3.1	Protección de los datos utilizados en prueba	No

7. Conclusiones

El trabajo realizado ha conseguido que se lograran los objetivos iniciales planteados en el mismo, los cuales se fundamentaban en la realización de un Plan Director de Seguridad de la Información para una cadena hotelera con la finalidad de:

- Reducir los riesgos asociados a la seguridad de la información, teniendo en cuenta los costes y daños en la imagen de la empresa que los incidentes relacionados pudieran causar, hasta unos niveles aceptables por parte de la organización.

- Asegurar el cumplimiento de la legislación vigente en materia de protección de datos personales.

- Asegurar la continuidad del negocio, reduciendo los tiempos de recuperación de los sistemas, ante posibles incidentes relacionados con la ciberseguridad.

La metodología seguida, comprendida de, análisis de situación inicial, elaboración de documentación requerida en el sistema de gestión documental, identificación de activos de información, clasificación de los mismos en base a las necesidades de disponibilidad, integridad, confidencialidad, autenticación y no repudio de los datos, análisis de riesgos de seguridad de la información, definición del estado deseado, propuesta de proyectos para cubrir la brecha entre estado inicial y estado deseado y realización de auditoría de cumplimiento, considero que ha sido la adecuada para poder realizar el trabajo con éxito.

En relación con la planificación, estimada inicialmente en 15 semanas, si bien es cierto que se ha conseguido cumplir con las fechas establecidas en la misma, el número de horas dedicadas al proyecto ha sido bastante superior a las previstas inicialmente.

Uno de los aspectos más reveladores del trabajo realizado, ha sido el de poner de manifiesto la importancia que realmente tiene la realización de una auditoría de cumplimiento tras la implementación de los proyectos propuestos. Ésta ha permitido conocer nuevas acciones a realizar y en consecuencia entrar en un ciclo de mejora continua que permitirá poder certificar la Gestión de la Seguridad de la Información de la Organización en base a la norma ISO/IEC 27.001.

El Plan Director de Seguridad de la Información se ha realizado en base a los conocimientos que el autor tiene sobre el sector hotelero y puede ser de aplicación para la mayoría de las cadenas hoteleras. No obstante, es importante destacar que existe un trabajo especialmente relevante en la elaboración de un Plan Director de Seguridad de la Información, el cual no se ha tratado en este trabajo debido a la importante cantidad de tiempo y recursos que requiere, y que es clave para adaptar el Plan a cualquier empresa. Este trabajo es el de realizar entrevistas con todos los departamentos y resto de partes implicadas, tanto

internas como externas, con la finalidad de conocer en detalle tanto el estado inicial de la seguridad de la información como el estado deseado.

8. Glosario

Análisis de riesgos: Proceso mediante el cual se analiza el valor de los activos de una organización, se identifican las amenazas a la que están expuestos estos activos y se evalúan las vulnerabilidades de cada uno de los activos hacia las amenazas identificadas, evaluando la probabilidad de que los activos sean afectados por cada una de las amenazas, así como su impacto en la organización.

Autenticación: Verificar que la identidad de alguien corresponde realmente a quien dice ser.

Confidencialidad: Corresponde a la no divulgación de información privada o sensible.

Disponibilidad: La información y los sistemas tendrán disponibilidad cuando estén accesibles siempre que sea requerido.

Enterprise Resource Planning (ERP): Es un aplicativo con el se planifican y gestionan los principales procesos de la Organización. En el sector hotelero, su principal función es la gestión financiera.

Integridad: Se dice que los datos tienen integridad cuando se puede confiar en que estos son fiables y no han sido alterados.

ISO 27001: Norma que recoge los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información. Esta norma es certificable.

ISO 27002: Código de buenas prácticas para la gestión de la Seguridad de la Información. Recoge un amplio catálogo de controles y buenas prácticas en la materia. Se utiliza de referencia para seleccionar los controles de seguridad.
Línea Base

Magerit: Metodología elaborada por el Consejo Superior de Administración Electrónica (CSAE) utilizada para realizar análisis y gestión de riesgos de los sistemas de información.
Modelo de Madurez de la Capacidad (CMM)
No repudio

Plan-Do-Check-Act (PDCA): Conocido también como ciclo de Deming, es una metodología iterativa que se utiliza para implementar la mejora continua de procesos o productos.

Property Management System (PMS): Software utilizado en los hoteles para gestionar la operativa del hotel (reservas, check in y check out, asignación de habitaciones y facturación entre otros)
Revenue Management

Riesgo aceptable: Indica el nivel de riesgo que está dispuesto a asumir la organización. Será necesario la toma de las medidas oportunas para cualquier riesgo que esté por encima de este nivel

Recovery Point Objective (RPO): Los Objetivos de Punto de Recuperación marcarán desde que momento temporal se quiere recuperar la información una vez se ha producido un incidente y dependerá de las necesidades operativas de la organización. Cuantifica la cantidad de información que la empresa está dispuesta a perder y se utiliza pa establecer la periodicidad de las copias de seguridad.

Recovery Time Objective (RTO): Define el tiempo establecido por la organización para recuperar un determinado proceso o sistema tras la ocurrencia de un incidente.

9. Bibliografía

1. CRUZ ALLENDE, Daniel, GARRE GUI, Silvia, SEGOVIA HENARES, Antonio José y TORTAJADA GALLEGO, Arsenio. *Sistema de gestión de la seguridad de la información* [en línea]. Barcelona: UOC, 2018. Disponible en: http://materials.cv.uoc.edu.biblioteca-uoc.idm.oclc.org/daisy/Materials/PID_00253134/pdf/PID_00253134.pdf

2. CRUZ ALLENDE, Daniel, SEGOVIA HENARES, Antonio José y TORTAJADA GALLEGO, Arsenio. *Análisis de riesgos* [en línea]. Barcelona: UOC, (s/f). Disponible en: http://materials.cv.uoc.edu.biblioteca-uoc.idm.oclc.org/daisy/Materials/PID_00253143/pdf/PID_00253143.pdf

3. CRUZ ALLENDE, Daniel, SEGOVIA HENARES, Antonio José y TORTAJADA GALLEGO, Arsenio. *Planes de continuidad de negocio* [en línea]. Barcelona: UOC, (s/f). Disponible en: http://materials.cv.uoc.edu.biblioteca-uoc.idm.oclc.org/daisy/Materials/PID_00253144/pdf/PID_00253144.pdf

4. ESTEVAN DE QUESADA, Rafael. *Introducció a l'auditoria TIC i de seguretat TIC* [en línea]. Barcelona: UOC, (s/f). Disponible en: http://materials.cv.uoc.edu.biblioteca-uoc.idm.oclc.org/daisy/Materials/PID_00239294/pdf/PID_00239291.pdf

5. ESTEVAN DE QUESADA, Rafael. *Auditoria de certificació ISO 27001* [en línea]. Barcelona: UOC, (s/f). Disponible en: http://materials.cv.uoc.edu.biblioteca-uoc.idm.oclc.org/daisy/Materials/PID_00239297/pdf/PID_00239288.pdf

6. GARRE GUI, Silvia, SEGOVIA HENARES, Antonio José y TORTAJADA GALLEGO, Arsenio. *Introducción a la seguridad de la información* [en línea]. Barcelona: UOC, (s/f). Disponible en: http://materials.cv.uoc.edu.biblioteca-uoc.idm.oclc.org/daisy/Materials/PID_00253141/pdf/PID_00253141.pdf

7. GARRE GUI, Silvia, SEGOVIA HENARES, Antonio José y TORTAJADA GALLEGO, Arsenio. *Implantación de un sistema de gestión de la seguridad de la información (SGSI)* [en línea]. Barcelona: UOC, (s/f). Disponible en: http://materials.cv.uoc.edu.biblioteca-uoc.idm.oclc.org/daisy/Materials/PID_00253140/pdf/PID_00253140.pdf

8. GARRE GUI, Silvia, SEGOVIA HENARES, Antonio José y TORTAJADA GALLEGO, Arsenio. *Desarrollo de algunos objetivos de control del SGSI* [en línea]. Barcelona: UOC, (s/f). Disponible en: http://materials.cv.uoc.edu.biblioteca-uoc.idm.oclc.org/daisy/Materials/PID_00253142/pdf/PID_00253142.pdf

9. GDPR Enforcement Tracker [en línia] [fecha de consulta: 18 de noviembre de 2020]. Disponible en: https://enforcementtracker.com

10. *INCIBE-Plan Director de Seguridad* [en línia] [fecha de consulta: 15 de noviembre de 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

11. *INCIBE-SECtoriza2 Turismo y ocio* [en línia] [fecha de consulta: 15 de noviembre de 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/SECtoriza2/turismo_ocio.pdf

12. *ISACA* [en línia] [fecha de consulta: 10 de octubre de 2020]. Disponible en: https://www.isaca.org

13. ISO/IEC 27001:2013. *Tecnología de la información.Técnicas de seguridad.Sistemas de Gestión de la Seguridad de la Información. Requisitos.*

14. ISO/IEC 27002:2013. *Tecnología de la Información.Técnicas de seguridad.Código de prácticas para los controles de seguridad de la información.*

15. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [en línia] [fecha de consulta: 25 de octubre de 2020]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.X-NgIS1Q28V

16. *ODS-La Ciberseguridad en la industria Hotelera* [en línia] [fecha de consulta: 20 de noviembre de 2020]. Disponible en: https://opendatasecurity.io/wp-content/uploads/2019/04/Ciberseguridad-en-la-industria-hotelera-_compressed.pdf

17. *WIKI: Sistemas de Gestión de Seguridad de la Información* [en línia] [fecha de consulta: 25 de octubre de 2020]. Disponible en: http://cv.uoc.edu/webapps/xwiki/wiki/matm1709/view/Main/Creación+del+SGSI

10. Anexos

Anexo I: Política de Seguridad

SGSI-PL01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Política de Seguridad	16/10/2020	Marc Montemar	Aprobado

POLÍTICA DE SEGURIDAD

Página 1 de 5

SGSI-PL01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Política de Seguridad	16/10/2020	Marc Montemar	Aprobado

0.- Índice

1.- Introducción

La dirección de **Cadena Hotelera** ha tomado la decisión de adoptar una serie de medidas con la finalidad de proteger los activos estratégicos de la organización. Dentro de estos activos se contempla la información, los documentos, las plataformas y los diferentes sistemas de información necesarios para su tratamiento, almacenamiento, comunicación y explotación, esenciales para que las actividades de negocio puedan desarrollarse, así como asegurar el futuro de la organización.

Dentro del actual entorno de transformación digital, no es concebible poder alcanzar los **objetivos estratégicos** de la empresa sin tener en consideración una adecuada gestión de la seguridad de la información. Ésta permite la adopción de las medidas adecuadas para asegurar unos niveles aceptables y medibles de disponibilidad, confidencialidad e integridad de la información cuyo tratamiento se realice en **Cadena Hotelera**, con la finalidad de velar de la forma más adecuada por los intereses y derechos de los usuarios y prevenir que cualquier incidencia relacionada con la seguridad de la información pueda comprometer la operativa o imagen de la organización.

2.- Objetivos

Los principales objetivos perseguidos con esta política de seguridad de la información son los de:

- Implementar un marco de referencia que permita asegurar la protección efectiva de la información de **Cadena Hotelera**.

- Concienciar a todo el personal de la empresa de la importancia de la seguridad de la información y de la necesidad de que éste comprenda de forma adecuada sus responsabilidades.

- Establecer las principales medidas de seguridad de la información que se deben implementar con la finalidad de proteger a la organización de forma adecuada contra las potenciales amenazas a las que la organización está expuesta y que podrían poner en riesgo la disponibilidad, confidencialidad e

integridad de la información, pudiendo causar la pérdida o determinados daños tanto en los activos de información (datos, equipos, documentación, impresa) como en el negocio y en la reputación e imagen de **Cadena Hotelera**. Estas medidas servirán como guía que facilitará a todo el personal de la empresa una toma de decisiones adecuada en los aspectos relacionados con la seguridad de la información.

3.- Alcance

Esta política se aplica a:

- Todos y cada uno de los trabajadores de la organización, tanto si son empleados, contratistas, consultores o mantienen cualquier otro tipo de relación con la empresa que implique la realización de trabajos para la misma.

- Todos y cada uno de los activos de información de la organización, cualquiera que sea su formato (electrónico, impreso o escrito sobre papel, transmitido en una conversación, …) así como todos los medios utilizados para su almacenamiento y transporte.

4.- Normas de Seguridad de la Información

Es responsabilidad de todos los trabajadores de la empresa proteger la información de forma proporcional al valor que esta proporciona a la organización, el cuál será otorgado por el propietario de dicha información. Este valor viene representado por los diferentes niveles mediante los cuales se clasifica la información, que estarán relacionados con los niveles de sensibilidad y criticidad de la información. Para cada uno de estos niveles se definirán diferentes controles que quedarán documentados en normativas asociadas a este documento.

Dentro de la organización se establecen 3 tipologías de información, “Pública”, “De uso interno” y “Confidencial”.

El acceso a cualquier información no considerada como “Pública” debe ser autorizado por los responsables de departamento y propietarios de la misma, bajo el criterio de acceso exclusivo a aquello que realmente sea necesario para realizar las funciones de cada uno de los puestos de trabajo y deshabilitando todo acceso no necesario.

Las contraseñas de acceso tanto a la información como a las tecnologías de la información son para uso individual, no pueden compartirse con terceras personas y de responsabilidad única de su propietario.

Cualquier incidente que atente contra lo establecido en la presente política debe ser notificado obligatoriamente y de forma inmediata por parte del trabajador que lo detecte al responsable de su departamento. Éste último analizará cada caso y lo

reportará al departamento de Tecnologías de la Información para que se tomen las medidas oportunas con la finalidad de evitar que se pueda repetir un incidente similar.

Los responsables de departamento procurarán que todo el personal reciba formación en materia de seguridad de la información, acorde a las necesidades y al rol que cada trabajador ejerza en la compañía.
En los casos en los que sea estrictamente necesario compartir con terceros información "Confidencial" o "De uso interno", se deberán suscribir acuerdos de confidencialidad con éstos.
Queda completamente prohibida la divulgación de cualquier información "Confidencial" o "De uso interno", salvo que se disponga de previa autorización del propietario de dicha información, el cuál se hará responsable de esta divulgación.

Cualquier incumplimiento de la presente política y de las normativas que la desarrollan por parte de cualquier empleado podrá llevar a la apertura de procedimientos disciplinarios.

De forma anual o ante cambios relevantes en los Sistemas de Información, el responsable de seguridad revisará y o adecuará la política de Seguridad a las condiciones contemporáneas de la organización.

Correo electrónico: Los trabajadores de **Cadena Hotelera** deberán conocer que las cuentas de correo electrónico proporcionadas por la empresa no son privadas, con lo que **Cadena Hotelera** podrá supervisar, sin necesidad de comunicación previa, cualquier mensaje que sea enviado, guardado o recibido a través del sistema de correo electrónico de la organización.

No podrá utilizarse el sistema de correo de la organización para la creación o distribución de mensajes que incluyan mensajes ofensivos sobre raza, color de la piel, edad, orientación sexual, pornografía, creencias y prácticas religiosas, políticas o de nacionalidad y en general cualquier mensaje que pueda ser ofensivo o perjudicial hacia terceras personas o que pueda dañar la imagen de la empresa.

El correo de empresa no debe ser utilizado para cuestiones de carácter personal.

Servicios de red: Cualquier dispositivo informático que contenga información confidencial y que vaya a conectarse tanto a redes internas de la organización, como a redes externas, deberá contar con un sistema, aprobado por el Responsable de Tecnologías de la Información, que controle el acceso al mismo mediante contraseña.

Protección de pantallas: Los ordenadores deberán disponer de protector de pantalla, protegido mediante contraseña, que bloquee la pantalla tras detectar un periodo de inactividad superior a 15 minutos, no pudiendo desbloquearse sin introducir contraseña.

Instalación de software en los equipos: No estará permitida la instalación de nuevo software en los equipos informáticos proporcionados por la empresa. En caso de ser

imprescindible la instalación de algún software adicional en los equipos, se deberá realizar una solicitud al responsable de departamento correspondiente, quién en caso de autorizar el cambio realizará solicitud posterior al departamento de Tecnologías de la Información.

Dispositivos móviles: Todo el personal al que se le haya hecho entrega de dispositivos móviles de la empresa, tales como ordenadores portátiles, teléfonos móviles, tabletas o similares, deberá responsabilizarse de su cuidado y devolución en las mismas condiciones en los que la organización se lo entregó. Estos dispositivos, en la medida de lo posible, no deberán mostrarse en espacios públicos y en ningún caso deberán dejarse desatendidos.

Todos los dispositivos deberán disponer de clave de acceso que los proteja ante accesos no autorizados. En el caso de los ordenadores portátiles, estos deberán disponer de software antivirus y anti-espía que los pueda proteger ante posibles ataques.

D. XXXXXXXXXXX
CARGO

Barcelona, a XX de XXXX de 2020

Anexo II: Procedimiento de Auditorías Internas

SGSI-PR01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Auditorías Internas	16/10/2020	Marc Montemar	Aprobado

AUDITORÍAS INTERNAS

Página 1 de 4

SGSI-PR01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Auditorías Internas	16/10/2020	Marc Montemar	Aprobado

0.- Índice

1.- Objetivos

El objetivo del presente procedimiento es el de documentar los procesos, planificar y definir las auditorías internas necesarias para asegurar que el SGSI se adecua a lo establecido en las normas de referencia, así como definir las responsabilidades de los procesos con la finalidad de mejorar de forma continua la eficacia del sistema.

2.- Alcance

Este procedimiento aplica a la realización de las auditorías internas del Sistema de Gestión de la Seguridad de la Información.

3.- Documentación de referencia

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

4.- Requisitos generales del SGSI

Las auditorías se realizarán de forma que anualmente cubran la totalidad del Sistema de Gestión de Seguridad de la Información, salvo casos excepcionales, como aquellos en los que se hayan producido cambios relevantes en la organización, estrategia o política o bien hayan aparecido importantes incidentes de seguridad o se hayan detectado en auditorías previas deficiencias en el sistema de gestión, en los que se podrán realizar con una periodicidad menor.

El alcance, objetivo y duración de cada una de las auditorías, así como el equipo auditor que las realice, serán definidos por el Comité de Seguridad de la Información. El equipo auditor podrá estar compuesto tanto por personal interno como externo a la organización

Para que el trabajo del auditor sea completamente imparcial y objetivo, es imprescindible que se cumpla con el principio de independencia. Esto significa que el auditor debe ser completamente independiente de la actividad auditada, no puede haber participado de forma directa o indirecta con ningún aspecto relacionado con esta actividad, y no puede existir ningún tipo de conflicto de intereses, bien sea de forma directa o indirecta, entre el auditor y la actividad a auditar.

5.- Procedimiento de actuación de las auditorías internas

Cualquier auditoría interna que se pretenda llevar a cabo, deberá ser planificada con anterioridad. De forma anual, el líder del equipo auditor, que generalmente será el responsable de seguridad de la información, realizará el Plan de Auditoría, en el que se detallarán los Objetivos y alcance de la auditoría, los documentos de referencia, el equipo auditor y las responsabilidades de cada uno de sus miembros, así como una planificación detallada de las fechas, lugares y duración estimada de las actividades a realizar en cada una de las áreas afectadas. Este Plan de Auditoría deberá ser aprobado por el Comité de Seguridad de la Información y distribuido con posterioridad a los responsables de las áreas afectadas y a los integrantes del equipo auditor.

Cuando vayan a realizarse las auditorías, teniendo en cuenta la planificación llevada a cabo, el equipo auditor realizará una reunión previa con las personas asignadas de las áreas afectadas informándoles del objetivo de la auditoría, así como de la forma en la que esta se va a llevar a cabo y de la documentación y registros que se van a revisar en la misma, con la finalidad de optimizar los tiempos dedicados.

En base a la documentación revisada, a las entrevistas realizadas a las personas correspondientes de las diferentes áreas, así como al resto de las evidencias encontradas durante la auditoría, el equipo auditor se reunirá para intercambiar información y estará en condiciones de sacar conclusiones y proceder con la redacción del informe de auditoría.

El informe de auditoría deberá contener al menos los siguientes apartados:

- Fecha de realización de la auditoría.
- Objetivo y alcance de la auditoría.
- Controles auditados.
- Equipo auditor.
- Documentación de referencia sobre la que se basa la auditoría.
- Resumen ejecutivo.
- Metodología empleada.
- Conclusiones generales sobre el grado de cumplimiento de los requisitos del SGSI.
- Detalle de las No conformidades y observaciones encontradas.

SGSI-PR01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Auditorías Internas	16/10/2020	Marc Montemar	Aprobado

Una vez elaborado el informe, el equipo auditor lo enviará al responsable de seguridad de la información y se reunirá con éste para realizar una presentación de los resultados del informe.

El responsable de seguridad de la información compartirá el informe de Auditoría con el Comité de Seguridad de la Información y enviará los resultados obtenidos en cada una de las áreas a sus respectivos responsables de forma segregada. Los responsables de cada área deberán enviar, en el plazo de una semana tras la recepción de los resultados, propuestas de implantación de medidas correctivas para cada una de las no conformidades detectadas.

Anexo III: Gestión de Indicadores

SGSI-IND01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Gestión de Indicadores	16/10/2020	Marc Montemar	Aprobado

GESTIÓN DE INDICADORES

Página 1 de 4

SGSI-IND01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Gestión de Indicadores	16/10/2020	Marc Montemar	Aprobado

0.- Índice

1.- Objetivos

La definición de indicadores es necesaria para poder medir la eficacia de los controles de seguridad implantadas.

2.- Alcance

Este procedimiento aplica a los indicadores que ayudan a medir la eficiencia del Sistema de Gestión de la Seguridad de la Información.

3.- Documentación de referencia

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- ISO/IEC 27004:2016

4.- Indicadores

Formación en seguridad de la información	
Descripción	Se medirá la cantidad de formación impartida en materia de seguridad de la información.
Control de seguridad	A 7.2.2 - Toma de Conciencia, educación y formación en la Seg. de la inf.
Fórmula de medición	Número de horas de formación anuales impartidas / Número de trabajadores.
Unidades de medida	horas por trabajador / año
Frecuencia de medición	Anual
Valor objetivo	8 horas por trabajador / año
Valor umbral	4 horas por trabajador / año
Responsable de la medida	Responsable de formación

SGSI-IND01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Gestión de Indicadores	16/10/2020	Marc Montemar	Aprobado

Control registro de entrada	
Descripción	Mediante el software de registro de entrada, se extraerán de forma mensual los datos del número de días en que se ha marcado registro de entrada para cada uno de los trabajadores y se sacará una media por trabajador.
Control de seguridad	A 11.1.2 - Controles físicos de entrada
Fórmula de medición	Suma (Número de días con registro de entrada para cada uno de los trabajadores) / (Número de días laborables * Número de trabajadores)
Unidades de medida	% registro de entrada
Frecuencia de medición	Mensual
Valor objetivo	90%
Valor umbral	70%
Responsable de la medida	Técnico de RRHH

Incidencias por uso indebido de activos	
Descripción	Se medirá el número de incidencias producidas por un uso indebido de los activos.
Control de seguridad	A 8.1.3 - Uso aceptable de los Activos
Fórmula de medición	Número de incidencias anuales producidas por un uso indebido de los activos / año
Unidades de medida	Número incidencias / año
Frecuencia de medición	Anual
Valor objetivo	5 incidencias / año
Valor umbral	10 incidencias / año
Responsable de la medida	Responsable Tecnologías de la Información

Revisión de vulnerabilidades en equipos	
Descripción	De forma mensual se realizarán pruebas con el fin de detectar vulnerabilidades técnicas en una muestra de equipos de la organización.
Control de seguridad	A 12.6.1 - Gestión de las vulnerabilidades técnicas
Fórmula de medición	Número de vulnerabilidades detectadas / Número de items evaluados
Unidades de medida	% vulnerabilidades
Frecuencia de medición	Mensual
Valor objetivo	5%
Valor umbral	15%
Responsable de la medida	Responsable administración de sistemas

SGSI-IND01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Gestión de Indicadores	16/10/2020	Marc Montemar	Aprobado

Cumplimiento Sistema Gestión de la Seguridad de la Información	
Descripción	Para verificar que se están implementando los procedimientos necesarios para garantizar la continuidad de la seguridad de la información se verificará con el responsable de seguridad de la información si están definidos los procedimientos e implementados los controles correspondientes para garantizar la continuidad de la seguridad de la información ante situaciones adversas. Se pedirán evidencias que garanticen que se cumple con lo descrito anteriormente.
Control de seguridad	A 17.1.3 - Verificación, revisión y evaluación de la continuidad de la seguridad de la información
Fórmula de medición	Cumplimiento (SI / NO)
Unidades de medida	1-cumplan; 0-No Cumple.
Frecuencia de medición	Anual
Valor objetivo	1-Cumple
Valor umbral	1-Cumple
Responsable de la medida	Dirección General

Disponibilidad web de reservas	
Descripción	Se revisará mensualmente el tiempo de inactividad de la web de reservas
Control de seguridad	A 12.4.1 - Registro y gestión de eventos de actividad
Fórmula de medición	Horas de inactividad / mes
Unidades de medida	horas de inactividad
Frecuencia de medición	Mensual
Valor objetivo	4 horas
Valor umbral	10 horas
Responsable de la medida	Responsable Tecnologías de la Información

Disponibilidad PMS	
Descripción	Se revisará mensualmente el tiempo de inactividad del Property Management System (PMS)
Control de seguridad	A 12.4.1 - Registro y gestión de eventos de actividad
Fórmula de medición	Horas de inactividad / mes
Unidades de medida	horas de inactividad
Frecuencia de medición	Mensual
Valor objetivo	4 horas
Valor umbral	10 horas
Responsable de la medida	Responsable Tecnologías de la Información

Anexo IV: Procedimiento de Revisión por Dirección

SGSI-PR02		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Revisión Dirección SGSI	16/10/2020	Marc Montemar	Aprobado

REVISIÓN DIRECCIÓN SGSI

Página 1 de 3

SGSI-PR02		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Revisión Dirección SGSI	16/10/2020	Marc Montemar	Aprobado

0.- Índice

1.- Objetivos

En este procedimiento se establecen los aspectos del SGSI que deben ser revisados por parte de la alta dirección, así como la planificación de esta revisión, con la finalidad de asegurar la conveniencia, adecuación y eficacia continuas del SGSI.

2.- Alcance

Este procedimiento aplica a las revisiones del Sistema de Gestión de la Seguridad de la Información por parte de la alta dirección de la empresa.

3.- Documentación de referencia

- ISO/IEC 27001:2013

4.- Descripción de la metodología

La Dirección General de **Cadena Hotelera** revisará el Sistema de Gestión de Seguridad de la Información de la organización con una frecuencia mínima anual, así como cuando se produzcan cambios de relevancia en el propio SGSI. Todo ello con la finalidad de asegurar la conveniencia, adecuación y eficiencia continuas del mismo.

La Dirección general deberá revisar los siguientes aspectos del SGSI:

- El estado de las acciones que se hayan implementado desde las anteriores revisiones realizadas por la dirección.
- Cambios en cuestiones, tanto externas como internas, que sean de afectación al SGSI.
- Información relevante sobre el comportamiento de la seguridad de la información tal como:
    - Los resultados de las auditorías realizadas, así como las no conformidades detectadas en las mismas y las acciones correctivas aplicadas y/o propuestas.

  - Seguimiento y resultados de mediciones y de los indicadores clave de riesgo.
  - El cumplimiento de los objetivos de seguridad de la información.
- Las observaciones y comentarios que provengan de las diferentes partes interesadas, como puedan ser proveedores, accionistas y clientes.
- Los resultados de las evaluaciones de riesgos, así como el estado del plan de tratamiento de riesgos.
- Las oportunidades de mejora continua

Tras realizar la revisión, la dirección deberá tomar decisiones que tengan relación con las oportunidades de mejora continua del sistema de gestión de seguridad de la información y de cualquier necesidad de cambio en éste. Los resultados de la revisión deberán quedar reflejados en el acta de la reunión, que servirá como evidencia de la revisión realizada.

Anexo V: Gestión de Roles y Responsabilidades

SGSI-PR03		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Roles y Responsabilidades	16/10/2020	Marc Montemar	Aprobado

GESTIÓN DE ROLES Y RESPONSABILIDADES

Página 1 de 6

SGSI-PR03		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Roles y Responsabilidades	16/10/2020	Marc Montemar	Aprobado

0.- Índice

1.- Objetivos

El objetivo de este documento es el de describir los roles y responsabilidades que tienen diferentes trabajadores de la organización sobre la seguridad de la información.

2.- Alcance

Este documento aplica sobre todos los activos relacionados con la seguridad de la información.

3.- Documentación de referencia

- ISO/IEC 27001:2013

SGSI-PR03		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Roles y Responsabilidades	16/10/2020	Marc Montemar	Aprobado

4.- Roles y Responsabilidades

4.1.- Comité de Dirección

El Comité de Dirección de la Organización es el responsable de evaluar y aprobar las medidas estratégicas en materia de Seguridad e la Información, las cuales deberán estar alineadas con la estrategia global de la organización.

Las principales funciones del Comité de Dirección relacionas con la Seguridad de la Información son:

- Incluir la Seguridad de la Información en la agenda del comité como uno de los aspectos a tratar.
- Nombrar a los miembros del Comité de Seguridad de la Información, dándole soporte y dotando a éste de los recursos necesarios.
- Aprobar las políticas relacionadas con la Seguridad de la Información.
- Determinar los niveles de riesgo aceptables por parte de la organización.
- Aprobar el plan director de Seguridad de la Información en el que se reflejan los principales proyectos e iniciativas relacionados con la materia.
- Realizar seguimiento de los indicadores clave de la seguridad de la información.

Las decisiones tomadas por el Comité de Dirección quedarán reflejadas en acta.

4.2.- Comité de Seguridad de la Información

El Comité de Seguridad de la Información estará formado por responsables de diferentes departamentos de la organización. Formarán parte de este comité, representantes de las áreas de RRHH, Tecnologías de la Información, Finanzas, Operaciones, Comercial/Marketing y expansión y desarrollo, así como el responsable de Seguridad Física y el responsable de Seguridad de la Información. Uno de los miembros del comité formará parte del Comité de Dirección.

Las principales funciones del Comité de Seguridad de la Información son:

- Tomar decisiones de forma consensuada sobre los aspectos relacionados con la seguridad de la información.
- Presentar las políticas, normas y responsabilidades en materia de seguridad de la información al comité de dirección para su aprobación, así como implantar las directrices marcadas por el mismo.
- Asignar los diferentes roles y funciones en materia de seguridad de la información.
- Validar el plan de seguridad de la información para presentarlo al comité de dirección y realizar seguimiento de la implantación del mismo.

- Fomentar la concienciación y formación de los trabajadores de la organización.
- Revisar los incidentes de seguridad de la información más relevantes que se hayan producido.

4.3.- Responsable de seguridad de la información

El Responsable de Seguridad de la Información tiene un papel fundamental en la definición e implementación de una metodología que ayude a la organización a identificar, evaluar y minimizar los riesgos relacionados con la Seguridad de la Información para proteger esta información en cuanto a la confidencialidad, disponibilidad, integridad, autenticidad, autenticidad y trazabilidad.

Entre sus principales funciones destacan:

- Implementar las directrices del comité de seguridad de la información.
- Elaborar las políticas de seguridad de la información.
- Desarrollar, de forma conjunta con cada una de las áreas implicadas, el marco normativo de seguridad controlando su cumplimiento, gestionando la seguridad de la información de forma global y siendo el punto de referencia dentro de la organización.
- Proponer acciones de mejora para mitigar los riesgos existentes.
- Monitorizar el estado de la seguridad de la información de forma periódica.
- Definir los indicadores clave de seguimiento.
- Gestionar de forma adecuada el presupuesto destinado a la seguridad de la información, contratando los recursos necesarios.
- Elaborar, juntamente con el área de RRHH, los planes de formación relacionados con la seguridad de la información.
- Realizar análisis de los riesgos en materia de seguridad de la información.
- Coordinar con el resto de las áreas de negocio el plan de continuidad de negocio de la organización en base a los análisis de impacto sobre el negocio (BIA).

4.4.- Delegado de protección de datos

Sus funciones vienen definidas en el artículo 39 del Reglamento General de Protección de Datos. Entre sus funciones están el asesoramiento, información y supervisión del cumplimiento del RGPD por parte de la Organización.

4.5.- Responsables funcionales de la información

Las principales funciones relacionadas con la seguridad de la información que deberán realizar los responsables funcionales de la información, a los que también mencionaremos como propietarios de les datos, serán las de clasificar la información bajo su responsabilidad en función de su confidencialidad, disponibilidad, integridad, autenticidad y no repudio, así como determinar el uso que se tiene que hacer de esta

información y conceder las pertinentes autorizaciones de acceso a la misma. También colaborar, cuando se les requiera, a realizar revisiones y auditorías de seguridad.

4.6.- Área de Tecnología de la Información

Es una de las áreas que mayor peso tiene en relación con la seguridad de la información, ya que administra los sistemas sobre la que reside y se transmite la mayor parte de la información. Su principal responsabilidad es la de custodio de la información.
Sus principales funciones son:

- Colaborar con el responsable de seguridad de la información en la definición de las políticas, estándares y procedimientos, así como asegurar su cumplimiento.

- Gestionar las vulnerabilidades e implantar los controles de seguridad y acciones correctoras que se establezcan.

- Implicar al responsable de seguridad de la información en la implantación de los cambios que se quieran producir en los sistemas requiriendo su participación.

- Adoptar las medidas necesarias para proteger la información en base a la clasificación de la misma que ha hecho su propietario.

4.7.- Área de seguridad física

Esta área deberá proporcionar los medios técnicos adecuados para la protección física de la información ante amenazas físicas como puedan ser inundaciones, incendios o cortes de suministro eléctrico entre otras. También deberá proteger los accesos no autorizados, así como disponer de las medidas de recuperación de la situación normal de operación en base a los requisitos que se establezcan en los planes de continuidad de negocio.

Previamente a la construcción o rehabilitación de hoteles u oficinas, el responsable del área de seguridad física deberá implicar al responsable de seguridad de la información para tener en consideración la ubicación de elementos de red y comunicaciones, así como la protección de los diferentes equipos relacionados con la seguridad de la información.

4.8.- Área de RRHH

El área de RRHH deberá informar a las áreas responsables de gestionar los recursos de la información sobre las altas, bajas y cambios de posición o categoría de los empleados para que éstas puedan gestionar el acceso a los recursos de información de forma adecuada. También deberá trabajar de forma conjunta con el responsable

de seguridad de la información en la elaboración de la política de seguridad sobre los aspectos que afecten al personal.

4.9.- Área de asesoría jurídica

Deberá colaborar con el Responsable de Seguridad de la Información, informándole y asesorándole sobre la aplicación en la organización de la nueva legislación que pueda afectar a la seguridad de la información, ayudándole a definir las cláusulas específicas de seguridad de la información que se deben incorporar en los contratos con terceras partes o con personal externo a la compañía, así como a investigar y resolver incidencias de seguridad en el momento que estas puedan derivar en acciones legales por parte de terceros.

4.10.- Directores de departamento

Deberán colaborar con el Responsable de Seguridad de la Información dentro de su ámbito de actuación, con la finalidad de que toda la organización trabaje de forma segura.

4.11.- Todo el personal

Cualquier persona que trabaje para la organización, tanto de forma directa como a través de terceros, con acceso a información de la empresa deberá mantener la confidencialidad de la información, hacer un uso adecuado de los activos de la información a los que tiene acceso para protegerlos de accesos no autorizados, cumplir con las políticas de seguridad de la compañía y notificar las incidencias de seguridad que detecte y que puedan poner en peligro la seguridad de la información.

Anexo VI: Metodología de Análisis de Riesgos

SGSI-PR04		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Metodología Análisis de Riesgos	16/10/2020	Marc Montemar	Aprobado

METODOLOGÍA ANÁLISIS DE RIESGOS

Página 1 de 5

SGSI-PR04		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Metodología Análisis de Riesgos	16/10/2020	Marc Montemar	Aprobado

0.- Índice

1.- Objetivos

El objetivo de este procedimiento es el de establecer una metodología para analizar los riesgos relacionados con la Seguridad de la Información.

2.- Alcance

Este procedimiento se aplicará a los activos relacionados con la seguridad de la información.

3.- Documentación de referencia

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- ISO/IEC 27005:2018
- MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
    - Libro I: Método
    - Libro II: Catálogo de Elementos
    - Libro III: Guía de Técnicas

4.- Descripción de la metodología

Para realizar el análisis de riesgos, nos basaremos en la metodología Magerit.

Inicialmente se realizará un **Inventario de Activos**, que consistirá en detallar todos los activos de la organización relacionados con la información que vamos a incluir en nuestro análisis de riesgos. Una vez tengamos la relación de activos, clasificaremos cada uno ellos dentro de alguno de los siguientes grupos:

- Instalaciones
- Equipos informáticos (Hardware)
- Aplicaciones informáticas (Software)

- Datos
- Soportes de información (dispositivos de almacenamiento de datos)
- Redes de comunicaciones
- Servicios
- Equipamiento auxiliar
- Personas

Será importante tener en consideración las dependencias entre activos. Un activo de un nivel superior depende del activo del nivel inferior, es decir que las necesidades de seguridad del activo de nivel superior quedarán reflejadas en el activo de nivel inferior. En consecuencia, una amenaza sobre un activo de nivel inferior afectará también en el activo de nivel superior, con lo que se deberá mostrar esta relación entre activos en forma de árbol. A modo de ejemplo, un fallo en un activo de nivel inferior (Aire Acondicionado) podría dañar un activo de nivel superior (Servidor).

Una vez realizado el inventario de activos, habiéndolos clasificado por grupos y establecida su dependencia, se procederá a realizar una **Valoración de** estos **Activos**. Debido a la dificultad de establecer valoraciones cuantitativas para determinados activos, se procederá a realizar una valoración cualitativa, que completaremos con una estimación cuantitativa, según diferentes categorías, con lo que el valor de los activos podrá ser:

Valoración	Rango en €
Muy Alto	valor > 50.000
Alto	25.000 < valor > 50.000
Medio	10.000 < valor > 25.000
Bajo	3.000 < valor > 10.000
Muy Bajo	valor < 3.000

También, con la finalidad de conocer el aspecto más crítico relacionado con la seguridad de cada uno de los activos, se deberán valorar de forma independiente cada una de las 5 **dimensiones de** la **seguridad** de la información (**A**utenticidad, **C**onfidencialidad, **I**ntegridad, **D**isponibilidad y No repudio o **T**razabilidad).

La escala que se utilizará para valorar cada una de las dimensiones es la siguiente:

Valor	Criterio
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importantea la organización
1-3	Daño menor a la organización
0	Daño irrelevante a la organización

Aplicando todo lo detallado con anterioridad, el resultado final de la tabla de activos será el siguiente

Ámbito	Activo	Valor	Aspectos críticos				
			A	C	I	D	T
Instalaciones	Activo XX	MUY ALTO	8	6	5	6	8

Otro de los aspectos que debemos incluir en el Análisis de Riesgos es el **Análisis de Amenazas**

Para realizar el análisis de amenazas, basándonos en la metodología Magerit, clasificaremos las amenazas en 4 grandes bloques, que serán los siguientes:

- Desastres naturales
- De origen industrial
- Errores y fallos no intencionados
- Ataques intencionados

Para cada tipo de activo analizaremos la frecuencia con la que se puede producir una amenaza determinada, así como su impacto en las diferentes dimensiones de seguridad del activo.
Los valores que estableceremos para la frecuencia serán los siguientes:

Frecuencia	Rango	Valor
Muy frecuente	Diario	100
Frecuente	Quincenal	75
Frecuencia Media	Mensual	50
Poco frecuente	Trimestral	25
Baja	Semestral	10
Muy baja	Anual	0

En cuanto a los valores del impacto para cada una de las dimensiones serán:

Impacto	Valor
Muy alto	100%
Alto	50%
Medio	20%
Bajo	10%
Muy bajo	1%

Aplicando todo lo expuesto anteriormente, el resultado final del análisis de amenazas mostrará una tabla como la siguiente:

Activo	Frecuencia	Impacto				
		A	C	I	D	T
Activo XX		100%	50%	20%	100%	50%
Amenaza 1	10	50%	50%	10%	100%	50%
Amenaza 2	25	100%	20%	20%	20%	20%

En la tabla podemos observar como el valor de la fila que identifica el activo, se corresponde con el valor del impacto máximo que puede provocar cada una de las diferentes amenazas.

Llegados a este punto, podemos obtener el resultado del **Impacto Potencial**, que será el resultado de multiplicar el valor de cada una de las dimensiones del activo por el porcentaje de impacto y que podemos ver en la siguiente tabla.

Ámbito	Activo	Valor	Aspectos críticos					Impacto					Impacto Potencial				
			A	C	I	D	T	A	C	I	D	T	A	C	I	D	T
Instalaciones	Activo XX	MUY ALTO	8	6	5	6	8	100%	50%	20%	100%	50%	8	3	1	6	4

Multiplicando el Impacto potencial por la frecuencia, obtendremos el **Riesgo Intrínseco**, que será el nivel de riesgo de cada uno de los activos antes de aplicar cualquier medida de mitigación. Este resultado nos permitirá priorizar el plan de acción.

Será necesario establecer un nivel límite de riesgo, todo lo que quede por debajo de este nivel estará dentro de lo que organización considera **riesgo aceptable** y no supondrá una amenaza grave para la organización. A todo activo que tenga un valor que esté por encima de este nivel de riesgo aceptable deberán aplicarse controles para reducirlo. Este nivel de riesgo aceptable debe ser aprobado por la dirección de la Organización.

Una vez se hayan implementado todos los controles el riesgo disminuirá, pero no se eliminará. El nivel de riesgo que permanecerá tras la implementación de los controles será el **riesgo residual**.

Anexo VII: Declaración de Aplicabilidad

SGSI-DOA01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Declaración de aplicabilidad	16/10/2020	Marc Montemar	Aprobado

DECLARACIÓN DE APLICABILIDAD

Página 1 de 6

SGSI-DOA01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Declaración de aplicabilidad	16/10/2020	Marc Montemar	Aprobado

0.- Índice

1.- Objetivos

El objetivo de este documento es el de identificar qué controles, de los que se relacionan en la ISO 27001 se aplican a la organización, incluyendo el detalle de su aplicabilidad.

2.- Alcance

El alcance serán todos los controles de seguridad de la información establecidos en la ISO 27001 y que son de aplicación a la organización.

3.- Documentación de referencia

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

SGSI-DOA01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Declaración de aplicabilidad	16/10/2020	Marc Montemar	Aprobado

4.- Declaración de aplicabilidad

SGSI-DOA01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Declaración de aplicabilidad	16/10/2020	Marc Montemar	Aprobado

CONTROL				Aplicación	Justificación	Documentación relacionada
A.5. Políticas de la Seguridad de la Información						
	A.5.1. Directrices de la Dirección en seguridad de la información					
		A.5.1.1	Políticas para la Seguridad de la Información	Sí	Se dispone de política de seguridad, aprobada por la dirección y disponible en la intranet de la organización.	SGSI-PL01
		A.5.1.2	Revisión de las Políticas para seguridad de la información	Sí	Todavía no se ha realizado ninguna revisión, pero se ha definido el procedimiento para ello.	SGSI-PR02
A.6. Organización de la Seguridad de la Información						
	A.6.1. Organización Interna					
		A.6.1.1	Seguridad de la información Roles y Responsabilidades	Sí	Existe documento en el que se definen las responsabilidades.	SGSI-PR03
		A.6.1.2	Separación de deberes - Funciones	Sí	Se deberá desarrollar procedimiento para establecer la separación de deberes en determinadas funciones, como pueda ser compras-pago de facturas	
		A.6.1.3	Contacto con las autoridades	Sí	Se realizan por parte del departamento de comunicación.Se deberá desarrollar procedimiento.	
		A.6.1.4	Contacto con grupos de interés Especial	Sí	Se realizan por parte del departamento de comunicación.Se deberá desarrollar procedimiento.	
		A.6.1.5	Seguridad de la información en la gestión de proyectos Proyectos Seguridad de la información en gestión de Proyectos	Sí	Se deberá desarrollar procedimiento para incluir la seguridad de la información en la gestión de proyectos.	
	A.6.2. Dispositivos Móviles y Teletrabajo					
		A.6.2.1	Política de uso de dispositivos móviles	Sí	Se dispone de política de seguridad, aprobada por la dirección y disponible en la intranet de la organización.	SGSI-PL01
		A.6.2.2	Teletrabajo	Sí	Diversos trabajadores realizan teletrabajo, actualmente se está desarrollando la política.	
A.7. Seguridad de los Recursos Humanos						
	A.7.1. Antes de la contratación					
		A.7.1.1	Investigación de antecedentes	Sí	No existe un procedimiento para ello, se deberá desarrollar.	
		A.7.1.2	Términos y condiciones del empleo	Sí	No existe un procedimiento para ello, se deberá desarrollar.	
	A.7.2. Durante la ejecución del Empleo					
		A.7.2.1	Responsabilidades de la Dirección	Sí	Existe documento en el que se definen las responsabilidades.	SGSI-PR03
		A.7.2.2	Toma de Conciencia, educación y formación en la Seg. de la inf.	Sí	Se deberá realizar un plan de formación en materia de seguridad de la información.	
		A.7.2.3	Proceso Disciplinario	Sí	Se deberá establecer el procedimiento por parte de RRHH.	
	A.7.3. Cese o cambio de puesto de trabajo					
		A.7.3.1	Terminación o Cambio de responsabilidades de empleo	Sí	No existe un procedimiento para ello, se deberá desarrollar.	
A.8. Gestión de Activos						
	A.8.1. Responsabilidad por los activos					
		A.8.1.1	Inventario de activos	Sí	No existe un procedimiento para ello, se deberá desarrollar.	
		A.8.1.2	Propiedad de los Activos	Sí	No existe documento detallado donde se establezca con detalle la propiedad de todos los activos de la información. Se deberá desarrollar.	
		A.8.1.3	Uso aceptable de los Activos	Sí	El uso aceptable de activos está incluído en las politicas de seguridad	SGSI-PL01
		A.8.1.4	Devolución de los Activos	Sí	No existe procedimiento definido de devolución de bactivos. Se deberá desarrollar.	
	A.8.2. Clasificación de la información					
		A.8.2.1	Directrices de clasificación	Sí	Se deberá definir procedimiento.	
		A.8.2.2	Etiquetado y manipulado de la información	Sí	Se deberá definir procedimiento.	
		A.8.2.3	Manipulación de activos	Sí	Se deberá definir procedimiento.	
	A.8.3. Manejo de medios de soporte					
		A.8.3.1	Gestión de medios de soporte removibles	Sí	Se deberá definir procedimiento.	
		A.8.3.2	Eliminación de soportes	Sí	Se deberá definir procedimiento.	
		A.8.3.3	Soportes físicos en tránsito	Sí	Se deberá definir procedimiento.	

SGSI-DOA01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Declaración de aplicabilidad	16/10/2020	Marc Montemar	Aprobado

A.9. Control de Acceso					
	A.9.1. Requisitos del negocio para control de acceso				
	A.9.1.1	Política de control de acceso	Sí	La política de control de acceso está incluida en las políticas de seguridad	SGSI-PL01
	A.9.1.2	Acceso a redes y a servicios en red	Sí	Existe un procedimiento para autorizar los accedos a redes y servicios de red cuando se incorporá una persona a la organización.	Procedimiento de RRHH.
	A.9.2. Gestión de acceso de usuarios.				
	A.9.2.1	Gestión de altas/bajas en el registro de usuarios	Sí	Existe un procedimiento de altas y bajas cuando una persona se incorpora o abandona a la organización.	Procedimiento de RRHH.
	A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	Sí	Se deberá establecer un procedimiento para asignar los diferentes derechos de acceso a los usuarios.	
	A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	Sí	Se deberá establecer un procedimiento para solicitar y autorizar privilegios especiales.	
	A.9.2.4	Gestión de información confidencial de autentic. de usuarios	Sí	Se deberá documentar procedimiento.	
	A.9.2.5	Revisión de los derechos de acceso de usuarios	Sí	Se deberá documentar procedimiento.	
	A.9.2.6	Retirada o adaptación de los derechos de acceso	Sí	Se deberá documentar procedimiento.	
	A.9.3. Responsabilidades de los usuarios				
	A.9.3.1	Uso de información confidencial para la autenticación	Sí	Se deberá documentar procedimiento.	
	A.9.4. Control de Acceso a Sistemas y Aplicaciones				
	A.9.4.1	Restricción de acceso a información	Sí	Se deberá documentar procedimiento.	
	A.9.4.2	Procedimientos seguros de inicio de sesión	Sí	Se deberá documentar procedimiento.	
	A.9.4.3	Sistema de gestión de contraseñas	Sí	Se deberá documentar procedimiento.	
	A.9.4.4	Uso de herramientas de administración de sistemas	Sí	Se deberá documentar procedimiento.	
	A.9.4.5	Control de acceso al código fuente de los programas	Sí	Se deberá documentar procedimiento.	
A.10 Cifrado					
	A.10.1 Controles criptográficos				
	A.10.1.1	Política de uso de los controles criptográficos	Sí	Se deberá definir la política.	
	A.10.1.2	Gestión de claves	Sí	Se deberá documentar procedimiento.	
A.11. Seguridad física y Ambiental					
	A.11.1 Áreas seguras				
	A.11.1.1	Perímetro de seguridad física	Sí	Se deberá documentar procedimiento.	
	A.11.1.2	Controles físicos de entrada	Sí	Se deberá documentar procedimiento.	
	A.11.1.3	Seguridad de oficinas, despachos y recursos	Sí	Se deberá documentar procedimiento.	
	A.11.1.4	Protección contra las amenazas externas y ambientales	Sí	Se deberá documentar procedimiento.	
	A.11.1.5	El trabajo en áreas seguras	Sí	Se deberá documentar procedimiento.	
	A.11.1.6	Áreas de acceso público, carga y descarga	Sí	Se deberá documentar procedimiento.	
	A.11.2 Seguridad de los equipos				
	A.11.2.1	Emplazamiento y protección de equipos	Sí	Se deberá definir procedimiento.	
	A.11.2.2	Instalaciones de suministro	Sí	Se deberá definir procedimiento.	
	A.11.2.3	Seguridad del cableado	Sí	Se deberá definir procedimiento.	
	A.11.2.4	Mantenimiento de los equipos	Sí	Se deberá definir procedimiento.	
	A.11.2.5	Salida de activos fuera de las dependencias de la empresa	Sí	Se deberá definir procedimiento.	
	A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Sí	Se deberá definir procedimiento.	
	A.11.2.7	Reutilización o retirada segura de dispositivos de almacenam.	Sí	Se deberá definir procedimiento.	
	A.11.2.8	Equipo informático de usuario desatendido	Sí	Se deberá definir procedimiento.	
	A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	Sí	Incorporado es política de seguridad	SGSI-PL01
A.12 Seguridad en la Operativa					
	A.12.1 Responsabilidades y procedimientos de operación				
	A.12.1.1	Documentación de procedimientos de operación	Sí	Se deberá documentar procedimiento.	
	A.12.1.2	Gestión de cambios	Sí	Se deberá documentar procedimiento.	
	A.12.1.3	Gestión de capacidades	Sí	Se deberá documentar procedimiento.	
	A.12.1.4	Separación de entornos de desarrollo, prueba y producción	Sí	Se deberá documentar procedimiento.	
	A.12.2 Protección contra código malicioso				
	A.12.2.1	Controles contra el código malicioso	Sí	Se dispone de servicio contratado con terceros, para el bloqueo de correos sospechosos. Se deberá definir procedimiento.	
	A.12.3 Copias de seguridad				
	A.12.3.1	Copias de seguridad de la información	Sí	Aunque el proceso esté definido, se deberá docuemntar dentro de los procedimientos de Seguridad de la Información.	
	A.12.4 Registro de actividad y supervisión				
	A.12.4.1	Registro y gestión de eventos de actividad	Sí	Se deberá documentar procedimiento.	
	A.12.4.2	Protección de los registros de información	Sí	Se deberá documentar procedimiento.	
	A.12.4.3	Registros de actividad del administrador y operador del sistema	Sí	Se deberá documentar procedimiento.	
	A.12.4.4	Sincronización de relojes	Sí	Se deberá documentar procedimiento.	
	A.12.5 Control del software en explotación				
	A.12.5.1	Instalación del software en sistemas en producción	Sí	Se deberá incorporar documentación	
	A.12.6 Gestión de la vulnerabilidad técnica				
	A.12.6.1	Gestión de las vulnerabilidades técnicas	Sí	Se deberá documentar procedimiento.	
	A.12.6.2	Restricciones en la instalación de software	Sí	Aunque el proceso esté definido, se deberá docuemntar dentro de los procedimientos de Seguridad de la Información.	
	A.12.7 Consideraciones de las auditorías de los sistemas de información				
	A.12.7.1	Controles de auditoría de los sistemas de información	Sí	Se ha definido el procedimiento para la realización de las auditorías relacionadasd con el Sistema de Gestión de la Seguridad de la Información.	SGSI-PR01

SGSI-DOA01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Declaración de aplicabilidad	16/10/2020	Marc Montemar	Aprobado

A.13. Seguridad en las Telecomunicaciones					
	A.13.1 Gestión de la seguridad en las redes				
	A.13.1.1	Controles de red	Sí	Se deberá documentar procedimiento.	
	A.13.1.2	Mecanismos de seguridad asociados a servicios en red	Sí	Se deberá documentar procedimiento.	
	A.13.1.3	Segregación de redes	Sí	Se aplica para separar las redes internas de las de proveedores o clientes. Aunque está definido se deberá incorporar a los procedimientos de seguridad de la información.	Procedimiento de IT.
	A.13.2 Intercambio de información con partes externas				
	A.13.2.1	Políticas y procedimientos de intercambio de información	Sí	Definido en política de seguridad.	SGSI-PL01
	A.13.2.2	Acuerdos de intercambio	Sí	Se deberá definir procedimiento.	
	A.13.2.3	Mensajería electrónica	Sí	Se deberá definir procedimiento.	
	A.13.2.4	Acuerdos de confidencialidad y secreto	Sí	Se deberá definir procedimiento.	
A.14. Aquisición, desarrollo y Mantenimiento de los sistemas de información					
	A.14.1 Requisitos de seguridad de los sistemas de información				
	A.14.1.1	Análisis y especificación de los requisitos de seguridad	Sí	Se deberá definir procedimiento.	
	A.14.1.2	Seguridad de las comunicac. en serv. accesibles por redes públ.	Sí	Se deberá definir procedimiento.	
	A.14.1.3	Protección de las transacciones por redes telemáticas	Sí	Se deberá definir procedimiento.	
	A.14.2 Seguridad en los procesos de desarrollo y soporte				
	A.14.2.1	Política de desarrollo seguro de software	Sí	Se deberá definir política.	
	A.14.2.2	Procedimientos de control de cambios en los sistemas	Sí	Se deberá definir procedimiento.	
	A.14.2.3	Rev. técnica de las aplicaciones tras efectuar cambios en el S.O.	Sí	Se deberá definir procedimiento.	
	A.14.2.4	Restricciones a los cambios en los paquetes de software	Sí	Se deberá definir procedimiento.	
	A.14.2.5	Uso de principios de ingeniería en protección de sistemas	Sí	Se deberá definir procedimiento.	
	A.14.2.6	Seguridad en entornos de desarrollo	Sí	Se deberá definir procedimiento.	
	A.14.2.7	Externalización del desarrollo de software	Sí	Se deberá definir procedimiento.	
	A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	Sí	Se deberá definir procedimiento.	
	A.14.2.9	Pruebas de aceptación	Sí	Se deberá definir procedimiento.	
	A.14.3 Datos de prueba				
	A.14.3.1	Protección de los datos utilizados en prueba	Sí	Se deberá definir procedimiento.	
A.15. Relaciones con Suministradores					
	A.15.1 Seguridad de la información en las relaciones con suministradores				
	A.15.1.1	Política de seguridad de la información para suministradores	Sí	Se deberá definir procedimiento.	
	A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	Sí	Se deberá definir procedimiento.	
	A.15.1.3	Cadena de suminist. en tecnol. de la inf. y comunicaciones	Sí	Se deberá definir procedimiento.	
	A.15.2 Gestión de la prestación del servicio por suministradores				
	A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	Sí	Se deberá definir procedimiento.	
	A.15.2.2	Gestión de cambios en los servicios prestados por terceros	Sí	Se deberá definir procedimiento.	
A.16. Gestión de Incidentes					
	A.16.1 Gestión de incidentes de seguridad de la información y mejoras				
	A.16.1.1	Responsabilidades y procedimientos	Sí	Se deberá definir procedimiento.	
	A.16.1.2	Notificación de los eventos de seguridad de la información	Sí	Se deberá definir procedimiento.	
	A.16.1.3	Notificación de puntos débiles de la seguridad	Sí	Se deberá definir procedimiento.	
	A.16.1.4	Valorac. de eventos de segur. de la inf. y toma de decisiones	Sí	Se deberá definir procedimiento.	
	A.16.1.5	Respuesta a los incidentes de seguridad	Sí	Se deberá definir procedimiento.	
	A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Sí	Se deberá definir procedimiento.	
	A.16.1.7	Recopilación de evidencias	Sí	Se deberá definir procedimiento.	
A.17. Aspectos de la SI en la Gestión de la Continuidad de Negocio					
	A.17.1 Continuidad de la seguridad de la información				
	A.17.1.1	Planificación de la continuidad de la seg. de la información	Sí	Se deberá definir procedimiento.	
	A.17.1.2	Implantación de la continuidad de la seguridad de la informac.	Sí	Se deberá definir procedimiento.	
	A.17.1.3	Verif., rev. y evaluación de la continuidad de la seg. de la inf.	Sí	Se deberá definir procedimiento.	
	A.17.2 Redundancias				
	A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la inf.	Sí	Se deberá documentar procedimiento.	
A.18. Cumplimiento					
	A.18.1 Cumplimiento de los requisitos legales y contractuales				
	A.18.1.1	Identificación de la legislación aplicable	Sí	Se deberá documentar procedimiento.	
	A.18.1.2	Derechos de propiedad intelectual (DPI)	Sí	Se deberá documentar procedimiento.	
	A.18.1.3	Protección de los registros de la organización	Sí	Se deberá documentar procedimiento.	
	A.18.1.4	Protección de datos y privacidad de la información personal	Sí	Se deberá documentar procedimiento.	
	A.18.1.5	Regulación de los controles criptográficos	Sí	Se deberá definir procedimiento.	
	A.18.2 Revisiones de la seguridad de la información				
	A.18.2.1	Revisión independiente de la seguridad de la información	Sí	No se han realizado revisiones independientes pero se ha definido el procedimiento de auditoría	SGSI-PR01
	A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Sí	No se ha realizado todavía pero se ha definido procedimiento.	SGSI-PR02
	A.18.2.3	Comprobación del cumplimiento	Sí	No se ha realizado todavía pero se ha definido procedimiento.	SGSI-PR02

Anexo VIII: Informe de Auditoría

SGSI-AUD01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Equipo Auditor	Fecha
1.0	Auditoría de cumplimiento	26/11/2020	Marc Montemar	26/11/2020

AUDITORÍA DE CUMPLIMIENTO

Página 1 de 11

SGSI-AUD01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Equipo Auditor	Fecha
1.0	Auditoría de cumplimiento	26/11/2020	Marc Montemar	26/11/2020

0.- Índice

1.- Objetivos

El objetivo de la presente auditoría es el de evaluar el grado de madurez de la seguridad de la información de la organización sobre cada uno de los dominios descritos en la ISO/IEC 27002:2013.

2.- Alcance

Esta auditoría se realizará sobre los controles definidos en la declaración de aplicabilidad que, en el caso de Cadena Hotelera, corresponde con los 114 controles, organizados en 14 áreas y 35 objetivos de control, referenciados en la ISO/IEC 27002:2013.

3.- Documentación de referencia

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

4.- Metodología empleada

Para la realización de esta auditoría se ha realizado una reunión previa con representantes de las áreas de Tecnologías de la Información, Finanzas, Recursos Humanos, Operaciones, Expansión y Comercial de la Organización, a quienes se ha solicitado también documentación relacionada con los diferentes controles descritos en la Declaración de Aplicabilidad de la compañía.

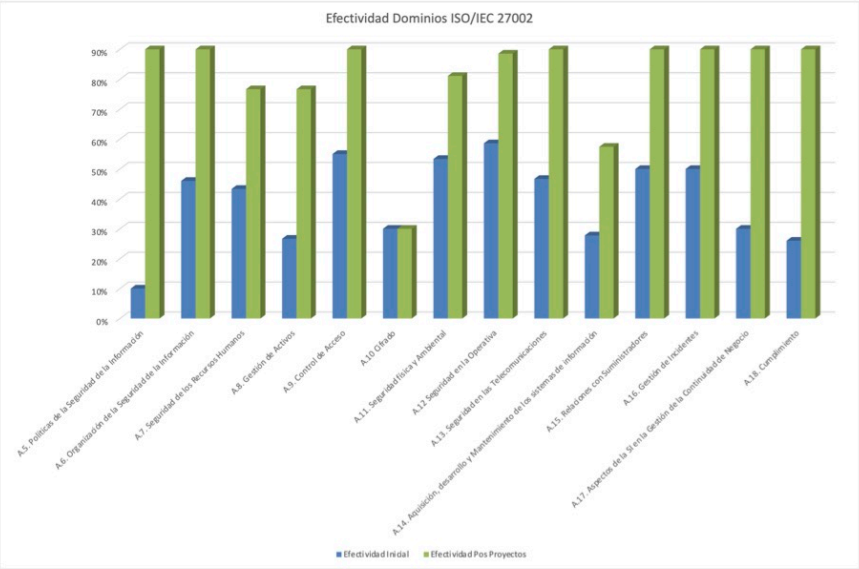
En base a la documentación recopilada y a las entrevistas realizadas a las personas correspondientes de las diferentes áreas, así como al resto de las evidencias encontradas durante la auditoría, se ha contrastado el grado de cumplimiento para cada uno de los controles definidos en la ISO/IEC 27002:2013.

SGSI-AUD01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Equipo Auditor	Fecha
1.0	Auditoría de cumplimiento	26/11/2020	Marc Montemar	26/11/2020

5.- Resumen ejecutivo

La auditoría se ha realizado con la finalidad de conocer el grado de madurez de la seguridad de la información basándonos en el estado de implementación de cada uno de los controles definidos en la ISO/IEC 27002.

Tras la implementación de los proyectos establecidos en el Plan Director de Seguridad de la Información, tal y como se muestra en el siguiente gráfico, se detecta una evolución muy favorable sobre los dominios descritos en la ISO 27002, debido a las mejoras producidas sobre cada uno de los controles.



A pesar de las mejoras producidas en cada uno de los dominios, durante la auditoría se han detectado algunas no conformidades debido a la falta de implementación de diversos controles que en la declaración de aplicabilidad se establecen como aplicables a la organización.

SGSI-AUD01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Equipo Auditor	Fecha
1.0	Auditoría de cumplimiento	26/11/2020	Marc Montemar	26/11/2020

El siguiente cuadro muestra los controles sobre los que se han detectado las No Conformidades, cuyo detalle se podrá observar en el capítulo 7 del presente informe.

CONTROL				Cumplimiento
A.7. Seguridad de los Recursos Humanos				
	A.7.1. Antes de la contratación			
		A.7.1.1	Investigación de antecedentes	No
A.8. Gestión de Activos				
	A.8.3. Manejo de medios de soporte			
		A.8.3.1	Gestión de medios de soporte removibles	No
		A.8.3.2	Eliminación de soportes	No
		A.8.3.3	Soportes físicos en tránsito	No
A.10 Cifrado				
	A.10.1 Controles criptográficos			
		A.10.1.1	Política de uso de los controles criptográficos	No
		A.10.1.2	Gestión de claves	No
A.11. Seguridad física y Ambiental				
	A.11.1 Áreas seguras			
		A.11.1.1	Perímetro de seguridad física	No
		A.11.1.6	Áreas de acceso público, carga y descarga	No
	A.11.2 Seguridad de los equipos			
		A.11.2.7	Reutilización o retirada segura de dispositivos de almacenam.	No
A.12 Seguridad en la Operativa				
	A.12.1 Responsabilidades y procedimientos de operación			
		A.12.1.4	Separación de entornos de desarrollo, prueba y producción	No
A.14. Aquisición, desarrollo y Mantenimiento de los sistemas de información				
	A.14.2 Seguridad en los procesos de desarrollo y soporte			
		A.14.2.1	Política de desarrollo seguro de software	No
		A.14.2.6	Seguridad en entornos de desarrollo	No
		A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	No
	A.14.3 Datos de prueba			
		A.14.3.1	Protección de los datos utilizados en prueba	No

6.- Conclusiones

Esta ha sido la primera auditoría realizada sobre el estado del Sistema de Gestión de Seguridad de la Información en base a los controles definidos en la ISO/IEC 27002. Se ha detectado una destacable mejora de la implementación de los controles tras la implementación del Plan Director, aunque se han detectado algunas no conformidades al no haber implementado todos los controles establecidos en la declaración de aplicabilidad.

SGSI-AUD01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Equipo Auditor	Fecha
1.0	Auditoría de cumplimiento	26/11/2020	Marc Montemar	26/11/2020

7.- Detalle de No conformidades y Observaciones

REGISTRO DE NO CONFORMIDAD Y/O MEJORA				
Fecha de apertura:	26/11/2020	**No conformidad**	AUD01-NC01	
Descripción	No se cumple con lo indicado en el control "A 7.1.1-Investigación de antecedentes" de la ISO/IEC 27002.			
Evidencias	No se muestran evidencias de la realización de investigación de antecedentes a ninguno de los trabajadores contratados por la empresa en los últimos 5 años.			
Acciones correctivas/preventivas	Será necesario determinar si la organización pretende cumplir con el control A.7.1.1 y en caso contrario indicarlo en la Declaración de Aplicabilidad.			
	Responsable	Dirección RRHH	**Fecha límite**	26/02/2021
	Estado	Pendiente	**Fecha de cierre**	

REGISTRO DE NO CONFORMIDAD Y/O MEJORA				
Fecha de apertura:	26/11/2020	**No conformidad**	AUD01-NC02	
Descripción	No se cumple con lo indicado en los controles relacionados con el "Manejo de medios de soporte", A.8.3 de la ISO/IEC 27002.			
Evidencias	No se muestran evidencias de la existencia de procedimientos relacionados con la gestión de medios de soporte removibles, la eliminación de soportes ni el manejo de los soportes físicos en tránsito.			
Acciones correctivas/preventivas	Será necesario definir procedimientos para la gestión, eliminación y manejo de los dispositivos de almacenamiento de información.			
	Responsable	Responsable de IT	**Fecha límite**	26/02/2021
	Estado	Pendiente	**Fecha de cierre**	

SGSI-AUD01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Equipo Auditor	Fecha
1.0	Auditoría de cumplimiento	26/11/2020	Marc Montemar	26/11/2020

REGISTRO DE NO CONFORMIDAD Y/O MEJORA				
Fecha de apertura:	26/11/2020	**No conformidad**	AUD01-NC03	
Descripción	No se cumple con lo indicado en los controles relacionados con los "A 10.1-Controles criptográficos", de la ISO/IEC 27002.			
Evidencias	No se muestran evidencias del desarrollo e implementación de políticas sobre el uso de controles criptográficos para proteger la información así como sobre el uso, protección y duración de las claves de cifrado durante su ciclo de vida.			
Acciones correctivas/preventivas	Será necesario definir las políticas relacionadas con el uso de controles criptográficos para proteger la información así como sobre el uso, protección y duración de las claves de cifrado durante su ciclo de vida.			
	Responsable	Responsable de Seguridad de la Información	**Fecha límite**	26/02/2021
	Estado	Pendiente	**Fecha de cierre**	

SGSI-AUD01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Equipo Auditor	Fecha
1.0	Auditoría de cumplimiento	26/11/2020	Marc Montemar	26/11/2020

REGISTRO DE NO CONFORMIDAD Y/O MEJORA				
Fecha de apertura:	26/11/2020	**No conformidad**	AUD01-NC04	
Descripción	No se cumple con lo indicado en los controles relacionados con las Áreas seguras, "A 11.1.1 -Perímetro de seguridad física" y "A 11.1.6 - Áreas de acceso público, carga y descarga", establecidos en la ISO/IEC 27002.			
Evidencias	Tras visita a las instalaciones, se detecta que no existen dispositivos que bloqueen el control de acceso a las salas donde se encuentran los servidores y tampoco existe un control sobre las áreas de acceso público, carga y descarga.			
Acciones correctivas/preventivas	Se deberán instalar mecanismos de control de acceso a las salas de servidores, tales como teclado, cerradura con llave o similar para restringir el acceso a dichas salas de personal no autorizado. Será necesaria también la instalación de cámaras de videovigilancia mediante sistema CCTV en las zonas de carga y descarga que puedan visualizarse desde la recepción de los hoteles.			
	Responsable	Facility Manager	**Fecha límite**	26/05/2021
	Estado	Pendiente	**Fecha de cierre**	

SGSI-AUD01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Equipo Auditor	Fecha
1.0	Auditoría de cumplimiento	26/11/2020	Marc Montemar	26/11/2020

REGISTRO DE NO CONFORMIDAD Y/O MEJORA				
Fecha de apertura:	26/11/2020	**No conformidad**	AUD01-NC05	
Descripción	No se cumple con lo indicado en el control relacionado con la Seguridad de los equipos "A 11.2.7 -Reutilización o retirada segura de dispositivos de almacenamiento", establecido en la ISO/IEC 27002.			
Evidencias	No se muestra evidencia la existencia de un procedimiento de revisión de los soportes de almacenamiento cuando se recibe o se retira un equipo de circulación, de tal forma que se asegure que se ha eliminado de forma segura cualquier dato sensible o software bajo licencia antes de su retirada definitiva.			
Acciones correctivas/preventivas	Se deberá redactar e implementar un procedimiento que asegure la revisión de los soportes de almacenamiento de cualquier equipo que reciba el equipo de IT antes de su retirada de circulación.			
	Responsable	Responsable de IT	**Fecha límite**	26/02/2021
	Estado	Pendiente	**Fecha de cierre**	

SGSI-AUD01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Equipo Auditor	Fecha
1.0	Auditoría de cumplimiento	26/11/2020	Marc Montemar	26/11/2020

REGISTRO DE NO CONFORMIDAD Y/O MEJORA				
Fecha de apertura:	26/11/2020	**No conformidad**	AUD01-NC06	
Descripción	No se cumple con lo descrito en el control "A 12.1.4 -Separación de entornos de desarrollo, prueba y producción", establecido en la ISO/IEC 27002.			
Evidencias	No se evidencia la existencia de un procedimiento que establezca la separación, tanto a nivel de redes, como a nivel de equipos, de los entornos de producción con los de desarrollo y pruebas .			
Acciones correctivas/preventivas	Se deberá realizar un procedimiento que establezca la separación de los recursos de desarrollo, pruebas y operación, con la finalidad de reducir los riesgos de acceso no autorizado así como posibles cambios del sistema en producción.			
	Responsable	Responsable de IT	**Fecha límite**	26/02/2021
	Estado	Pendiente	**Fecha de cierre**	

SGSI-AUD01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Equipo Auditor	Fecha
1.0	Auditoría de cumplimiento	26/11/2020	Marc Montemar	26/11/2020

REGISTRO DE NO CONFORMIDAD Y/O MEJORA				
Fecha de apertura:	26/11/2020	**No conformidad**	AUD01-NC07	
Descripción	No se cumple con lo indicado en los controles relacionados con la Seguridad en los procesos de desarrollo y soporte, "A 14.2.1 - Política de desarrollo seguro de software", "A 14.2.6 -Seguridad en entornos de desarrollo" y "A 14.2.8 - Pruebas de funcionalidad durante el desarrollo de los sistemas", establecidos en la ISO/IEC 27002.			
Evidencias	No se evidencia la existencia de políticas ni procedimientos que establezcan de qué forma debe tenerse en cuenta la seguridad de la información en los desarrollos de software y sistemas dentro de la organización, así como en las pruebas de los mismos.			
Acciones correctivas/preventivas	Se deberán desarrollar e implementar políticas y procedimientos para que los desarrollos y pruebas de software y sistemas consideren las seguridad de la información durante todo el ciclo de vida (diseño, desarrollo, implementación y mantenimiento).			
	Responsable	Responsable de Seguridad de la Información	**Fecha límite**	26/02/2021
	Estado	Pendiente	**Fecha de cierre**	

SGSI-AUD01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Equipo Auditor	Fecha
1.0	Auditoría de cumplimiento	26/11/2020	Marc Montemar	26/11/2020

REGISTRO DE NO CONFORMIDAD Y/O MEJORA				
Fecha de apertura:	26/11/2020	**No conformidad**	AUD01-NC08	
Descripción	No se cumple con lo indicado en el control relacionado con los Datos de prueba, "A 14.3.1 -Protección de los datos utilizados en prueba", establecido en la ISO/IEC 27002.			
Evidencias	No se evidencia la existencia de procedimientos que establezcan de qué forma deben seleccionarse, protegerse y controlarse los datos utilizados en los entornos de prueba.			
Acciones correctivas/preventivas	Se deberán desarrollar e implementar procedimientos para la selección, protección y control de los datos de prueba.			
	Responsable	Responsable de Seguridad de la Información	**Fecha límite**	26/02/2021
	Estado	Pendiente	**Fecha de cierre**	