SGSI-RE01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Resumen Ejecutivo	26/12/2020	Marc Montemar	Aprobado

RESUMEN EJECUTIVO

SGSI-RE01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Resumen Ejecutivo	26/12/2020	Marc Montemar	Aprobado

0.- Índice

1.- Introducción

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 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.

2.- Objetivos

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, cuyos principales objetivos 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.

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.

4.- Resultados

4.1.- 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 siguiente tabla se muestran los criterios que se han utilizado para la aplicación del CMM sobre cada uno de los controles:

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.

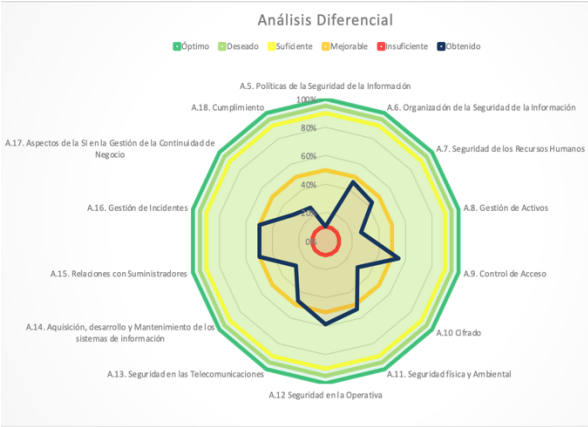
En la siguiente tabla, donde se muestra el resultado obtenido en cada una de las 14 áreas establecidas en la ISO/EC 27002:2013.

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%

Se puede observar como existe un importante 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%.

Nuestro objetivo, tras la implantación de los proyectos que se proponen en el 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.

En el siguiente gráfico, en forma de "diagrama de araña", podemos ver el resultado obtenido en nuestro análisis diferencial, el cual muestra la diferencia entre el estado "actual", en color azul, y el estado "deseado", en color verde claro, correspondiente con la gestión de la seguridad de la información, para cada uno de los capítulos descritos en la ISO/EC 27002:2013.



4.2.- 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 el Plan Director se han desarrollado estos documentos, correspondientes a:

- **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.

- **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.

- **Gestión de Indicadores:** Una vez se hayan implementado los controles que se establezcan en el SGSI, será necesario monitorizar su eficacia. Para ello se han desarrollado los indicadores pertinentes.

- **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.

- **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 Plan Director.

- **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, se ha establecido la metodología que indica que pasos debe seguir y en que criterios se debe basar.

- **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.

4.3.- 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.

Los activos que se han considerado en el análisis de riesgos son 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.

4.3.1 Resultados del Análisis de Riesgos

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).

Ya son varias 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.

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.

4.4.- Propuesta de Proyectos

Con la finalidad de reducir el riesgo relacionado con la Seguridad de la Información de nuestra organización, a unos niveles aceptables por parte de la misma, basándonos en los aspectos descritos con anterioridad, en el Plan Director, se propone la implantación de los siguientes 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 €

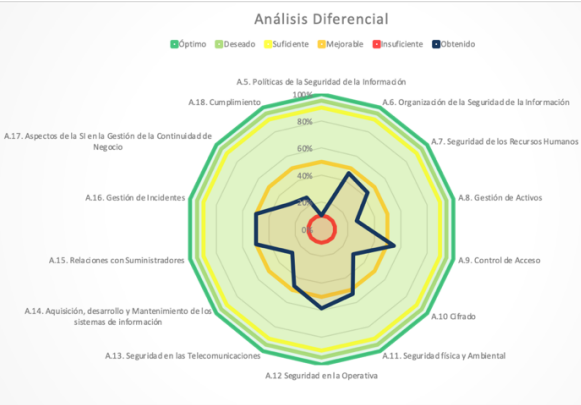
4.5.- Evolución cumplimiento dominios ISO/IEC 27002

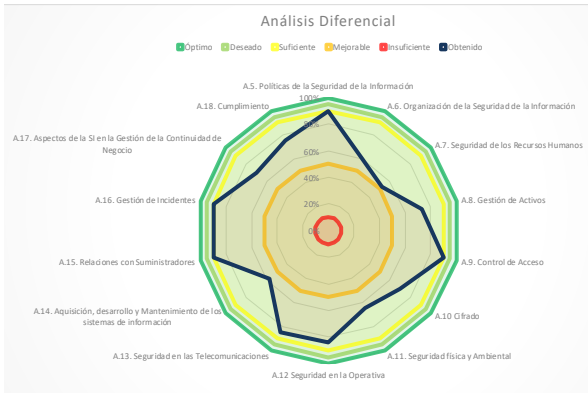
Tras la implementación de los proyectos propuestos, obtendremos una importante mejora en cuanto a la gestión de la Seguridad de la Información dentro de la Organización, avanzando hacia el objetivo que nos habíamos marcado inicialmente, el de llegar al estado definido como **"L4-Gestionado y medible"**,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

En los siguientes diagramas, se muestra la evolución del estado de los dominios definidos en la ISO 27002, con anterioridad y tras la implementación de los proyectos propuestos respectivamente. En ellos podemos ver la notable mejora producida.

SGSI-RE01		Histórico de cambios		
Versión	Descripción	Fecha de modificación	Autor	Estado
1.0	Resumen Ejecutivo	26/12/2020	Marc Montemar	Aprobado





4.6. Auditoría de cumplimiento

Una vez han sido implementados los proyectos descritos anteriormente, 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.

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 siguiente tabla:

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

5.- 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 realización de una auditoría de cumplimiento, tras la implementación de los proyectos propuestos, 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.