Anexo B – Procedimiento de Auditoría

1. Alcance

El presente documento será de aplicación a todas las áreas de la empresa que realicen procesos comprendidos dentro del alcance del SGSI.

2. Equipo Auditor

El equipo que realice las auditorías internas de la empresa debe cumplir una serie de requisitos que se describe a continuación.

2.1 Formación

El equipo auditor deberá estar compuesto por personal que cuente con la siguiente formación:

- Título universitario en Ingeniería Informática o Telecomunicaciones.
- Experiencia mínima de dos años en los sistemas y procedimientos a auditar.
- Curso en auditoria interna ISO/IEC 27001

2.2 Habilidades

- Independencia en las actuaciones de auditoria.
- Persistencia y tenacidad orientada a la consecución de los objetivos de la auditoria.
- Buenas habilidades sociales
- Tener una actitud positiva y abierta que le permita considerar ideas o puntos de vistas alternativas.
- Capacidad de trabajo en equipo.
- Dotes de gestión.

2.3 Composición del equipo auditor

El equipo auditor estará compuesto por los siguientes roles:

- **Un Auditor Jefe:** Persona del grupo que atesora la mayor experiencia y es capaz de coordinar a un equipo auditor. Debe tener conocimiento de todos los sistemas y procesos a auditar.
- **Dos Auditores:** Personas del grupo que cuentan con la formación y habilidades anteriormente descritas.
- **Expertos técnicos**: Gente experta en determinados procesos y sistemas que asesoran al auditor jefe y a los auditores donde no lleguen sus conocimientos técnicos.

3. Plan de auditoría

Una vez que la empresa obtenga la certificación ISO/IEC 27001 se deben llevar a cabo distintas auditorías internas con el objetivo de satisfacer la mejora continua y por consiguiente la renovación de la certificación.

Se revisarán al menos una vez al año casa unos de los procesos y sistemas dentro del ámbito del SGSI dividido en 4 auditorías trimestrales.

3.1 Primer Trimestre

- Auditoría de los accesos físicos a los edificios.
- Auditoría de la seguridad física de los sistemas.
- Auditoría de la seguridad física de las dependencia críticas o restringidas
- Auditoría de la seguridad física de la información
- Supervisión las acciones llevadas a cabo para corregir las no conformidades detectadas en auditorías previas.
- Revisión de la política de seguridad de la organización.

3.2 Segundo Trimestre

- Auditoría de la seguridad de la red de la empresa
- Auditoría del acceso y uso de Internet
- Auditoría de conexiones con terceros
- Auditoría de Correo Electrónico corporativo.
- Supervisión las acciones llevadas a cabo para corregir las no conformidades detectadas en auditorías previas.
- Revisión de la política de seguridad de la organización.

3.3 Tercer Trimestre

- Auditoría de configuración de los sistemas
- Auditoría de proceso de adquisición de Hardware y Software
- Auditoría de administración hardware y software
- Auditoría de desarrollo software.
- Supervisión las acciones llevadas a cabo para corregir las no conformidades detectadas en auditorías previas.
- Revisión de la política de seguridad de la organización.

3.4 Cuarto Trimestre

- Auditoría de almacenamiento de la información
- Auditoría de acceso lógico
- Supervisión las acciones llevadas a cabo para corregir las no conformidades detectadas en auditorías previas.
- Revisión de la política de seguridad de la organización.

4. Modelo de informe de auditoría

PAG. 1 de 2	**INFORME DE AUDITORÍA INTERNA**	**[Membrete de la empresa]**
[Versión del Documento]		
[Código de Auditoría]		

1. Datos	
Trimestre y año de Auditoría	
Norma de referencia	
Lugar de la auditoría	
Componentes del equipo auditor	

2. Alcance	
a. Exclusiones	

3. Definiciones

PAG. 2 de 2	INFORME DE AUDITORÍA INTERNA	[Membrete de la empresa]
[Versión del Documento]		
[Código de Auditoría]		

4. Objetivos

5. Resultados

b. No conformidades

En la presente auditoría de han encontrado __ No conformidades(NC). Se muestran a continuación

Nº	Área o Proceso	Descripción	Responsable	Auditor

6. Observaciones y Oportunidades de Mejora

7. Conclusiones