Máster Universitario en Ciberseguridad y Privacidad (MUCIP)

ANEXO 6
ESQUEMA DOCUMENTAL

Universitat Oberta de Catalunya

Natividad García Lacárcel

INDICE

En este anexo se desarrollan los documentos necesarios para poder certificar el sistema.

POLÍTICA DE SEGURIDAD

La Política de Seguridad tiene por objeto proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normas pertinentes (Norma ISO/IEC 27002:2013). Constituye la normativa interna que todo el personal afectado por el alcance del Sistema de Gestión de Seguridad de la información debe conocer y cumplir.

Política de Seguridad de la Información

Objetivo

La Política de Seguridad de la Información de la empresa está orientada a garantizar la protección de todos los activos de información y la tecnología utilizada para su tratamiento, de las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar su integridad, disponibilidad y confidencialidad, favoreciendo el eficiente cumplimiento de los objetivos estratégicos de la organización.
Para ello, la empresa se compromete a desarrollar un Sistema de Gestión de la Seguridad (SGSI) impulsado por la Dirección, siguiendo el estándar internacional para la gestión de la seguridad de la información ISO/IEC 27001 como referencia para establecer, implantar, mantener y mejorar.

Alcance

La política afectará a la totalidad de las actividades que desarrolla la empresa y será aplicable a todo el ámbito de la organización, a sus recursos y a la totalidad de los procesos internos. Así como de conocimiento y aplicación por parte de todos los empleados y empresas externas vinculadas a través de contratos de prestación de servicios o acuerdos con terceros.

Política General de Seguridad de la Información

Los principios que rigen la política son los siguientes:

- Implementar las medidas de seguridad.
- Promover medios y prácticas que aseguren la continuidad de la actividad.
- Garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.
- Principio de confidencialidad, integridad y disponibilidad.
- Mantener las políticas, normativas y procesos actualizados, con el fin de asegurar su vigencia y nivel de eficacia.
- Promover una cultura en toda la organización orientada a la protección de los activos de información.
- Difusión, consolidación y cumplimiento de la política.
- Principio de mejora continua.

Revisión

Para la evaluación del cumplimiento de la política, la empresa se compromete a un programa de auditorías interno. Así como a someterse anualmente a auditorías de seguimiento exigidas por el ISO/IEC 27001 y realizada por el organismo de acreditación, así como a una auditoría externa, previa a la anterior, para la revisión del sistema de gestión e implantación de las políticas y medidas de seguridad.

Divulgación

Existen procesos y documentos técnicos derivados de la política, al alcance de todos

los empleados, que aclaran las obligaciones y las medidas de seguridad para proceder al tratamiento de la información y el cumplimiento de la normativa de protección de datos de carácter personal.

Política de Alto Nivel

Esta Política tendrá difusión, por parte de la Dirección, siendo accesible a todos los empleados de la organización, así como otras partes interesadas y se entiende implantada y mantenida en todos los niveles del Sistema de Gestión de la empresa, contando con el total compromiso de la Dirección.

PROCEDIMIENTO DE AUDITORÍAS INTERNAS DE SEGURIDAD

El procedimiento de auditorías internas permite realizar el seguimiento del Sistema de Gestión de Seguridad de la Información. El documento incluirá una planificación de las auditorías que se llevarán a cabo durante la vigencia de la certificación (una vez se obtenga), requisitos que se establecerán a los auditores internos y se definirá el modelo de informe de auditoría.

Procedimiento de auditorías internas

La comprobación de la conveniencia del diseño e implantación del SGSI se efectúa mediante auditorías. Además de vigilar el correcto mantenimiento de la documentación generada. (Revisiones, políticas de seguridad, marco normativo, objetivos, análisis de riesgos e indicadores, etc.)
Deben estar suficientemente planificadas y contar con la implicación de todo el personal necesario. Se procurará la realización de una auditoría interna de forma anual con personal propio especializado de la organización o por un tercero idóneo contratado para la ejecución. Además, queda abierta la posibilidad de realización de auditorías excepcionales.
Se incluirá la frecuencia, métodos, responsabilidades, requisitos e informes. Deberá hacer especial hincapié en la objetividad e imparcialidad del proceso para que los resultados den información pertinente y real.
El informe de auditoría incluirá información sobre la fecha, nombre de los auditores, alcance, controles, conformidad del SGSI con la norma, no conformidades detectadas y recomendaciones.

OBJETIVO
El objetivo de la auditoría es conocer el nivel de cumplimiento del SGSI en la empresa, con el fin de evaluar la conformidad con los requisitos de la norma ISO 27001:2013 e ISO 27002:2013, los requisitos legales, de la organización y sus partes interesadas. Para conseguir estos objetivos, se establecerá un procedimiento a través del cual se planifiquen y ejecuten periódicamente las auditorías internas del SGSI.

Este programa de auditoría interna observará el cumplimiento de los siguientes objetivos marcados:

- El análisis de riesgos de la organización, riesgos y criterio empleado para determinar si un riesgo es significativo.
- El método por el que se monitoriza y mide.
- La forma que se informa y mejora el SGSI.
- Las revisiones realizadas sobre el SGSI.
- El nivel de implicación de la Dirección.
- La declaración de aplicabilidad.
- Los objetivos que procura la empresa.

ALCANCE Y ÁREAS AUDITADAS
El alcance incluirá a todas las áreas de la empresa ya que todas realizan procesos comprendidos dentro SGSI.

Los ámbitos de auditoria para la realización de este proceso serán los siguientes:
- Administración
- Recursos humanos
- Sistemas
- Tecnología

- Redes

REQUISITOS EQUIPO AUDITOR
El auditor encargado de ejecutar la auditoría ya sea contratado como personal propio de la empresa o por medio de una empresa externa debe demostrar como mínimo y sin limitarse una serie de requisitos.

- Título profesional como Ingeniero de Sistemas, Electrónico, de Telecomunicaciones o afines.
- Experiencia de 2 años mínimo en auditorías de sistemas.
- Participación en al menos 2 auditorías de Sistemas de Gestión de Seguridad con respecto a la norma ISO 27001 en el rol de auditor o auditor líder.
- Demostrar experiencia en consultoría, asesoría y/o auditoría en temas relacionados con Seguridad de la Información.
- Ser independientes en los procesos que se auditaran.
- Capacidad de trabajo en equipo.
- Dotes de comunicación y gestión.

Funciones:
- Coordinar al equipo auditor.
- Preparar las auditorías.
- Verificar si se efectúa el cumplimiento del SGSI respecto a la norma y se mantiene actualizado.
- Analizar los resultados de las auditorías.
- Elaborar los informes con los resultados.

COMPOSICIÓN EL EQUIPO AUDITOR
El equipo auditor suele estar formado por un jefe auditor, diversos auditores de apoyo y técnicos que asesoran a éstos.

- Auditor jefe: Responsable de la auditoría, persona con la mayor experiencia y capaz de coordinar al equipo.
- Dos auditores: Personal de apoyo al auditor jefe que cuenta con la formación adecuada.
- Expertos técnicos: Personal con conocimientos técnicos y experiencia para asesorar a los auditores.

ACTIVIDADES DEL PROCEDIMIENTO
Las actividades que deberán tenerse en cuenta para la ejecución de las auditorías son las siguientes:

1. **PLAN DE LA AUDITORÍA**

La Auditoría completa se realizará tres años, dividida anualmente con el fin de revisar por lo menos, una vez cada tres años cada uno de los procesos y sistemas de la organización.

Primera anualidad:
- Auditoría de las Políticas de Seguridad
- Auditoría de la Organización de la Seguridad de la Información.
- Auditoría de la Seguridad relacionada con Recursos Humanos.
- Auditoría de la Gestión de Activos
- Auditoría del Control de acceso

Segunda anualidad:
- Auditoría del Cifrado
- Auditoría de la Seguridad Física y Ambiental

- Auditoría de la Seguridad de la Operativa
- Auditoría de la Seguridad de las Comunicaciones TIC.

Tercera anualidad:

- Auditoría de la Adquisición y Mantenimiento de los Sistemas de Información.
- Auditoría de las Relaciones con Proveedores.
- Auditoría de la Gestión de Incidentes en la Seguridad de la Información.
- Auditoría de la Gestión de la Continuidad de Negocio en relación con la Seguridad de la Información.
- Auditoría de cumplimiento.

La planificación a tres años se muestra de forma detallada a continuación:

CONTROL	RECURSO	INICIO
5 - Políticas de seguridad de la información	Responsable SGSI y Dirección.	1er Año – 1er Trimestre
5.1 – Directrices de gestión de la seguridad de la información	Responsable SGSI y Dirección.	1er Año – 1er Trimestre
6 - Organización de la seguridad de la información	Responsable SGSI y Dirección.	1er Año – 1er Trimestre
6.1 – Organización interna	Responsable SGSI y Dirección.	1er Año – 1er Trimestre
6.2 – Los dispositivos móviles y el teletrabajo	Responsable SGSI y Dirección.	1er Año – 2º Trimestre
7 – Seguridad relativa a los recursos humanos	Responsable SGSI	1er Año – 2º Trimestre
7.1 – Antes del empleo	Responsable SGSI	1er Año –2º Trimestre
7.2 – Durante el empleo	Responsable SGSI	1er Año – 2º Trimestre
7.3 – Finalización del empleo o cambio en el puesto de trabajo	Responsable SGSI	1er Año – 3er Trimestre
8 - Gestión de activos	Responsable SGSI	1er Año – 3er Trimestre
8.1 – Responsabilidad sobre los activos	Responsable SGSI	1er Año – 3er Trimestre
8.2 – Clasificación de la información	Responsable SGSI	1er Año – 3er Trimestre
8.3 – Manipulación de los soportes	Responsable SGSI	1er Año – 3er Trimestre
9 - Control de acceso	Responsable SGSI	1er Año – 4º Trimestre
9.1 – Requisitos de negocio para el control de acceso	Responsable SGSI	1er Año – 4º Trimestre
9.2 – Gestión de acceso de usuario	Responsable SGSI	1er Año – 4º Trimestre
9.3 – Responsabilidad del usuario	Responsable SGSI	1er Año – 4º Trimestre

9.4 – Control de acceso a sistemas y aplicaciones	Responsable SGSI	1er Año – 4º Trimestre
10 - Criptografía	Responsable SGSI	2º Año – 1er Trimestre
10.1 – Controles criptográficos	Responsable SGSI	2º Año – 1er Trimestre
11 – Seguridad física y del entorno	Responsable SGSI	2º Año – 1er Trimestre
11.1 – Áreas seguras	Responsable SGSI	2º Año – 1er Trimestre
11.2 – Seguridad de los equipos	Responsable SGSI	2º Año – 2º Trimestre
12. Seguridad de las operaciones	Responsable SGSI	2º Año – 2º Trimestre
12.1 – Procedimientos y responsabilidades operacionales	Responsable SGSI	2º Año – 2º Trimestre
12.2 – Protección contra el software malicioso	Responsable SGSI	2º Año – 2º Trimestre
12.3 – Copias de seguridad	Responsable SGSI	2º Año – 3er Trimestre
12.4 – Registros y supervisión	Responsable SGSI	2º Año – 3er Trimestre
12.5 – Control de software en explotación	Responsable SGSI	2º Año – 3er Trimestre
12.6 – Gestión de la vulnerabilidad técnica	Responsable SGSI	2º Año – 3er Trimestre
12.7 –Consideraciones sobre la auditoria de sistemas de información	Responsable SGSI	2º Año – 4º Trimestre
13 – Seguridad de las comunicaciones	Responsable SGSI	2º Año – 4º Trimestre
13.1 – Gestión de la seguridad de redes	Responsable SGSI	2º Año – 4º Trimestre
13.2 – Intercambio de información	Responsable SGSI	2º Año – 4º Trimestre
14 – Adquisición, desarrollo y mantenimiento de los sistemas de información	Responsable SGSI	3er Año – 1er Trimestre
14.1 – Requisitos de seguridad en los sistemas de información	Responsable SGSI	3er Año – 1er Trimestre
14.2 – Seguridad en el desarrollo y en los procesos de soporte	Responsable SGSI	3er Año – 1er Trimestre
14.3 – Datos de prueba	Responsable SGSI	3er Año – 1er Trimestre
15 - Relación con los proveedores	Responsable SGSI	3er Año – 2º Trimestre
15.1 – Seguridad en las relaciones con proveedores	Responsable SGSI	3er Año – 2º Trimestre
15.2 – Gestión de la provisión de servicios del proveedor	Responsable SGSI	3er Año – 2º Trimestre

16 – Gestión de incidentes de seguridad de la información	Responsable SGSI	3er Año – 3er Trimestre
16.1 – Gestión de incidentes de seguridad de la información y mejoras	Responsable SGSI	3er Año – 3er Trimestre
17 – Aspectos de seguridad de la información para la gestión de la continuidad del negocio	Responsable SGSI	3er Año – 3er Trimestre
17.1 – Continuidad de la seguridad de la información	Responsable SGSI	3er Año – 3er Trimestre
17.2 - Redundancias	Responsable SGSI	3er Año – 4º Trimestre
18 – Cumplimiento	Responsable SGSI	3er Año – 4º Trimestre
18.1 – Cumplimiento de los requisitos legales y contractuales	Responsable SGSI	3er Año – 4º Trimestre
18.2 – Revisiones de la seguridad de la información	Responsable SGSI	3er Año – 4º Trimestre

Planificación auditoría interna

El plan de auditorías internas deberá tener la siguiente información:

- Objetivo, alcance y proceso por auditar
- Nombre del auditor jefe y del equipo.
- Criterios de la auditoría
- Fecha, hora y lugar de la auditoría
- Normativa

Seguidamente se adjunta el modelo que se utiliza para documentar el Plan de Auditoría.

2. EJECUCIÓN DE LA AUDITORÍA

Para efectuar las auditorías internas se deben seguir estos pasos:

- Reunión de inicio.
- Revisión de la documentación de la empresa a auditar.
- Planeación y programación de entrevistas.
- Ejecución auditoría.
- Generación del Informe
- Presentación de resultados.

3. HALLAZGOS

Los tipos de hallazgos que se pueden identificar durante la ejecución de la auditoría interna son: no conformidades, conformidades, oportunidades de mejora u observaciones relacionadas con temas de interés.

- No conformidad: Es un incumplimiento de un requerimiento estipulado por la norma estándar. Pueden darse:
    - No conformidad mayor: Se incumple un apartado completo del estándar, o se detecta una situación que presenta un riesgo crítico para el SGSI.
    - No conformidad menor: Es una no conformidad detectada de menor gravedad que la anterior. Debe procurarse solventarla y cerrarla en un tiempo correcto.
- Conformidad: Van asociadas al cumplimiento de un requisito de la norma.

En el proceso de auditoría también pueden descubrirse hallazgos como:

- Observaciones: La observación es menos crítica en comparación con la conformidad menor. Este hallazgo no es obligatorio tratarlo para obtener la certificación, se entiende como una sugerencia.

- Oportunidades de mejora: Se tratan de un apoyo al sistema, no son incumplimientos a la norma, ni no conformidades, simplemente se trata de propuestas dirigidas a la organización para su mejora.

RESULTADO

Finalmente se obtendrá un informa de auditoría y será entregado a las partes interesadas y a la alta dirección. Esta información servirá para poder ser contrastada con pasadas auditorías y poder comprobar la evolución y mejora del sistema de gestión de seguridad de la información.
Cuando ha finalizado el proceso de auditoría se remitirán los informes al comité de seguridad donde estarán miembros de la dirección de la empresa y responsable de todas las áreas. De este modo se podrá evaluar de forma efectiva el resultado de las auditorías y generar si hiciesen falta proyectos de evolución para reducir los problemas encontrados. En caso de no conformidad se establecerán nuevas citas con el grupo auditor para poder tratarlas.

El informe de auditoría contendrá la siguiente información:
- Fecha de auditoría
- Equipo auditor
- Identificación de la compañía
- Objetivos de la auditoría
- El alcance y la norma de referencia
- Conformidad del SGSI con la norma
- No conformidades detectadas en el proceso

Ofrecerá información de:
- Causas que provoca los hallazgos.
- Acciones correctivas que se pueden efectuar.
- Análisis de la efectividad de las acciones correctivas de anteriores auditorías.

A continuación, se muestra en forma de cuadro resumen el procedimiento.

ACTIVIDADES
Planificar y programar las auditorías internas
Publicar la programación de las auditorías internas
Controles a auditar
Diseñar plan de auditoría
Reunión de inicio
Revisión documentación
Realizar entrevistas y visitas de verificación
Documentar hallazgos
Reunión de cierre
Desarrollar el plan de acción y mejora

Actividades de la auditoría

FORMATO MODELO PARA EL PLAN DE AUDITORÍA INTERNA

Objetivo de la auditoría:

Alcance:

Auditores:

Fecha de inicio de la auditoría (dd/mm/aa):

Fecha de finalización de la auditoría (dd/mm/aa):

Normatividad relacionada:

Listado actividades						
Fecha	**Hora**	**Lugar**	**Auditor**	**Actividad**	**Documentación relacionada**	**Responsable**

FORMATO MODELO INFORME DE AUDITORÍA INTERNA

INFORME DE AUDITORIA INTERNA SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

<FECHA>
<EMPRESA>

1. INTRODUCCIÓN

- Objetivo de la Auditoría
- Alcance de la Auditoría
- Fecha de la auditoría (dd/mm/aa)
- Lugar
- Áreas auditadas
- Equipo auditor

2. HALLAZGOS DE AUDITORÍA

Hallazgos de la auditoría				
ID	**Hallazgo**	**Norma Relacionada**	**Descripción**	**Tipo de hallazgo (No conformidad, Recomendación)**

3. CONCLUSIONES

GESTIÓN DE INDICADORES

En esta fase se produce el seguimiento continuado de la evolución de los indicadores, ya que son muy importantes para poder valorar su eficacia. Debe procurarse la automatización de los procedimientos. Con ello se consigue obtener informes más fáciles y seguros, así como alarmas que permitan denunciar incidencias o situaciones de seguridad deficiente que urja solucionar.

La ISO/IEC 27001:2013 establece en su apartado 9.1 que la organización debe evaluar el desempeño de la seguridad y la eficacia del sistema de gestión de la seguridad de la información.
Los controles de seguridad implantados deben ser medidos. A través de ellos se podrá evaluar la implantación del SGSI en la organización y su seguimiento.
Los indicadores más apropiados y que interesan a la organización, son aquellos vinculados a los dominios establecidos en el Anexo A de la norma.

OBJETIVOS
Los objetivos son:

- Evaluar la implantación y efectividad de los controles de seguridad.
- Comunicar valores de seguridad a la dirección de la organización.
- Mejorar los indicadores que sirvan de guía en las revisiones del SGSI.
- Servir como entrada al plan de análisis y tratamiento de riesgos.

ALCANCE
Esta política cubre a todos los empleados y procesos de la organización.

INDICADORES
Los indicadores implantados a realizar para revisar los diferentes controles que aplican de los dominios de la ISO 27001:2013

5. Políticas de Seguridad	
Indicador	IC1 - Nº de revisiones de la política de seguridad por parte de la dirección.
Objetivo	Verificar que el documento es revisado por Dirección.
Control	5.1.2
Fórmula medición	Revisiones / año
Periodicidad	Anual
Valor objetivo	3
Valor umbral	1

6. Organización de la seguridad de la información	
Indicador	IC2 - Verificar si los roles y responsabilidades relativos a seguridad de la información están definidos
Control	6.1.1
Fórmula medición	(Nº tareas seguridad con responsable / Nº tareas seguridad totales) *100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	80%
Indicador	IC3 - Revisión de la seguridad en los proyectos

Control	6.1.5
Fórmula medición	(Nº de proyectos revisados / Total proyectos) * 100
Periodicidad	Semestre
Valor objetivo	100%
Valor umbral	80%
Indicador	IC4 - Revisión de política de teletrabajo
Control	6.2.2
Fórmula medición	(Nº de proyectos revisados / Total proyectos) * 100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	80%

7. Seguridad relativa a los recursos humanos	
Indicador	IC5 - Revisiones de antecedentes de nuevo personal contratado
Control	7.1.1
Fórmula medición	(Nº de revisados / Total nuevos contratados) * 100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	80%
Indicador	IC6 - Cursos de formación relativos a seguridad
Control	7.2.2
Fórmula medición	(Total valoración cursos) * 10 /Encuestas
Periodicidad	Anual
Valor objetivo	80%
Valor umbral	60%

8. Gestión de activos	
Indicador	IC7 - Control de activos
Control	8.1.1
Fórmula medición	(Nº de activos inventariados) / (Total de activos) * 100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	90%
Indicador	IC8 - Devolución de activos
Control	8.1.4
Fórmula medición	(Nº de activos devueltos / Nº de activos deberían ser devueltos) * 100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	90%
Indicador	IC9 - Eliminación correcta soportes
Control	8.3.2
Fórmula medición	(Nº de soportes eliminados / Nº de activos deberían ser eliminados) * 100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	90%

9.Contro de Acceso	
Indicador	IC10 - Accesos no autorizados a la red de la

	empresa
Control	9.1.2
Fórmula medición	(Nº de accesos no autorizados) / (Nº total de accesos) * 100
Periodicidad	Trimestral
Valor objetivo	0%
Valor umbral	1%
Indicador	IC11 - Control de privilegios de empleados
Control	9.2.1; 9.2.2; 9.2.3; 9.2.5; 9.2.6
Fórmula medición	(Nº de soportes eliminados / Nº de activos deberían ser eliminados) * 100
Periodicidad	Trimestral
Valor objetivo	100%
Valor umbral	90%
Indicador	IC12 - Empleados con rol administradores
Control	9.4.4
Fórmula medición	(Nº de empleados con privilegios / Nº de empleados) * 100
Periodicidad	Anual
Valor objetivo	5%
Valor umbral	10%

10.Criptografía	
Indicador	IC13 - Envío información encriptada
Control	10.1.1;
Fórmula medición	(Total envío información encriptada/ Total envío información) *100
Periodicidad	Trimestral
Valor objetivo	90%
Valor umbral	85%

11.Seguridad física y del entorno	
Indicador	IC14 - Medidas de seguridad físicas
Control	11.1.2;11.1.3
Fórmula medición	(Nº de intrusiones evitadas) / (Nº total de intrusiones) * 100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	95%
Indicador	IC15 - Revisión de sistemas contra incendios
Control	11.1.4
Fórmula medición	(Nº de revisiones) / (Nº objetivo de revisiones) * 100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	95%
Indicador	IC16 - Eficacia del sistema de suministro continuo de electricidad del CPD
Control	11.2.2
Fórmula medición	(Nº de equipos que sufren apagado) / (Total de los equipos) * 100
Periodicidad	Anual

Valor objetivo	0%
Valor umbral	5%
Indicador	IC17 - Eficacia parcheado de los sistemas
Control	11.2.4
Fórmula medición	(Nº de sistemas con último parche) / (Nº total de sistemas) * 100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	95%

12.Seguridad de las operaciones	
Indicador	IC18 - Sistemas sin antivirus
Control	12.2.1
Fórmula medición	(Nº de sistemas sin antivirus) / (Nº de sistemas que precisan antivirus) * 100
Periodicidad	Trimestral
Valor objetivo	0%
Valor umbral	5%
Indicador	IC19 - Eficacia del antivirus corporativo
Control	12.2.1
Fórmula medición	(Nº de amenazas detectadas) / (Nº de amenazas) * 100
Periodicidad	Trimestral
Valor objetivo	100%
Valor umbral	95%
Indicador	IC20 - Eficacia del sistema de backup
Control	12.3.1
Fórmula medición	(Nº de backup satisfactorios) / (Número de Backup) * 100
Periodicidad	Trimestral
Valor objetivo	100%
Valor umbral	95%
Indicador	IC21 - Eficacia del sistema de control de vulnerabilidades
Control	12.6.1
Fórmula medición	(Vulnerabilidades convertidas en amenazas) / (Nº de vulnerabilidades) * 100
Periodicidad	Trimestral
Valor objetivo	0%
Valor umbral	3%
Indicador	IC22 - Instalación de software no permitido
Control	12.6.2
Fórmula medición	(Equipos con software no permitido) / (Nº de equipos) * 100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	95%
Indicador	IC23 - Cumplimiento auditorías internas
Control	12.7.1
Fórmula medición	(Auditorías realizadas) / (Auditorías planificadas) * 100
Periodicidad	Anual

Valor objetivo	100%
Valor umbral	95%

13.Seguridad de las comunicaciones	
Indicador	IC24 - Eficacia de los equipos de seguridad de red
Control	13.1.2
Fórmula medición	(Nº de acceso a la red no permitidos) / (Nº de accesos) * 100
Periodicidad	Trimestral
Valor objetivo	0%
Valor umbral	5%

14.Adquisición, desarrollo y mantenimiento de los sistemas de información	
Indicador	IC25 - Cambios en entornos de desarrollo
Control	14.2.2
Fórmula medición	(Nº Cambios efectuados) / (Nº Cambios totales) * 100
Periodicidad	Trimestral
Valor objetivo	100%
Valor umbral	95%

15.Relación con proveedores	
Indicador	IC26 - Accesos sistemas empresa subcontratada
Control	15.1.2
Fórmula medición	Número accesos sin autorización
Periodicidad	Trimestral
Valor objetivo	0
Valor umbral	1
Indicador	IC27 - Cumplimiento sistemas de seguridad en el entorno de desarrollo contratado a un proveedor externo
Control	15.1.3
Fórmula medición	Número de intrusiones
Periodicidad	Trimestral
Valor objetivo	0
Valor umbral	1

16.Gestión de incidentes de seguridad de la información	
Indicador	IC28 - Debilidades notificadas por los usuarios
Control	16.1.2
Fórmula medición	Número notificaciones
Periodicidad	Trimestral
Valor objetivo	0
Valor umbral	1
Indicador	IC29 - Eficacia respuesta a incidentes
Control	16.1.5
Fórmula medición	(Nº incidentes resueltos tiempo establecido) / (Nº de incidentes)
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	95%

17.Seguridad física y del entorno	
Indicador	IC30 - Procesos forman parte del plan de continuidad de negocio
Control	17.1.2
Fórmula medición	(Nº de procesos que funcionan correctamente) / (Nº de procesos) * 100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	95%

18.Cumplimiento	
Indicador	IC31 - Incumplimiento legislativo
Control	18.1.1
Fórmula medición	(Nº Incumplimientos de obligaciones legales) / (Nº de obligaciones legales)
Periodicidad	Anual
Valor objetivo	0%
Valor umbral	5%
Indicador	IC32 - Verificación de ejecución de auditorias
Control	18.2.1
Fórmula medición	(Nº de auditorías realizadas) / (Nº de auditorías planeadas) *100
Periodicidad	Anual
Valor objetivo	100%
Valor umbral	90%
Indicador	IC33 - Cumplimiento de las políticas de seguridad
Control	18.2.2
Fórmula medición	Nº Infracciones
Periodicidad	Anual
Valor objetivo	0
Valor umbral	5

REVISIÓN POR PARTE DE LA DIRECCIÓN

La ISO/IEC 27001:2013 establece la obligación de efectuar por parte de la alta dirección la revisión periódica del SGSI con la finalidad de asegurarse de su conveniencia, adecuación y eficacia continuas. Define tanto los puntos de entrada, como los puntos de salida que se deben obtener de las revisiones. De manera que la dirección puede verificar y monitorizar el sistema y establecer compromisos para realizar las mejoras necesarias.

- Valora los cambios en la empresa que afecten al SGSI.
- El compromiso de la dirección de gestionar la información de forma detallada y documentada.
- Revisar el cumplimiento de los objetivos de seguridad de la información.
- Revisar el cumplimiento de la implementación de los controles para el tratamiento de los riesgos identificados, así como de las vulnerabilidades y amenazas.
- Valorar la retroalimentación del desempeño de la seguridad de la información y la aplicación de las acciones correctivas resultado de las auditorías y revisiones realizadas.

Revisión por parte de la dirección

El Sistema de Gestión de Seguridad de la Información de MASIAG contempla una evaluación periódica, sistemática y estructurada del SGSI de la organización a cargo de la Alta Dirección que permite asegurar una adecuada planeación y la corrección de posibles incumplimientos.

OBJETIVOS

- Revisión de la política de seguridad de la información
- Revisión de los objetivos de seguridad de la información.
- Documentación y registro de los resultados obtenidos

ALCANCE

El proceso comienza con la programación de la fecha de revisión por la dirección y finaliza con el seguimiento, compromisos establecidos en el Plan de Mejoramiento.

INFORMACIÓN ENTRADAS

La revisión por la Dirección a intervalos planificados para asegurar la conveniencia, adecuación y eficacia continuas debe contemplar las siguientes entradas:

- **El estado de las acciones de las revisiones de gestión anteriores.** Resultados de mediciones realizadas, auditorías y revisiones del SGSI. Efectuar la revisión sobre los compromisos que adquirieron para en base a ello, tomar decisiones adecuadas.
- Revisiones tanto de la política como de los objetivos del Sistema. Análisis del cumplimiento de las políticas y objetivos, en base a los indicadores considerados en el estudio.
- Desempeño del Sistema de Seguridad. Revisión el SGSI, con respecto a las metas planeadas y las acciones, con las cuales modificar las desviaciones que surjan y aprovechar la conformidad en los procesos.
- **Cambios en asuntos externos e internos que son relevantes para el sistema de gestión de seguridad de la información.** Es decir, cambios que influyen al Sistema de Gestión y puedan alterar a los sistemas que conforman el SGSI.

- **La retroalimentación sobre el desempeño de la seguridad de la información.** Retroalimentación de los usuarios y de los clientes, para detectar aspectos relevantes que pueda afectar al servicio y ayude, en las acciones para mejorar el incremento. **Incluyendo la información referente a no conformidades y acciones correctivas; resultados de seguimiento y medición; resultados de la auditoría; y cumplimiento de los objetivos de seguridad de la información.** Identificar el estado de las acciones para en base a los resultados poder tomar decisiones al respecto.
- **Comentarios de las partes interesadas.**
- **Resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos y oportunidades de mejora continua.**
- **Decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el SGSI.** Propuestas de mejora obtenidas por personal o por responsables de departamento. Precisar las necesidades en la mejora constante del Sistema de Gestión.
- **La organización debe retener información documentada como evidencia de los resultados de las revisiones por la dirección.**

Dichas entradas deben de ser revisadas por Dirección para en base al actual estado del negocio, impacto en clientes y planes de proyección de futuro puedan establecer distintos elementos de salida que activen planes de mejora del SGSI. Al finalizar la reunión se realiza un resumen de ella y se levanta el acta.

Cuadro resumen de las entradas:

ENTRADAS PARA LA REVISIÓN
1. Revisión compromisos de revisiones anteriores.
2. Estado y actualización del contexto de la organización.
3. Desempeño de los procesos y conformidad del servicio ofrecido
4. Resumen ejecutivo de indicadores - Auditorías realizadas al SGSI - Efectividad de las acciones correctivas - Gestión de hallazgos de auditorías - Impartición de concienciación personal - Resultados de las pruebas de concienciación - Incidentes atendidos - Retroalimentación con el cliente. - Idoneidad de los procesos y conformidad del servicio. - Información de las no conformidades y acciones correctivas del período analizado.
5. Resumen ejecutivo de Hallazgos de Auditoría.
6. Resumen ejecutivo de la Gestión de Incidentes de Seguridad.
7. Legalidad vigente
8. Oportunidades de mejora del SGSI

Resumen entradas

PROCEDIMIENTO

1. Recoger información. El encargado de seguridad de la información deberá recoger la siguiente información previa a la revisión por la alta dirección.

- Resultado de las auditorías internas.
- Métricas de desempeño del SGSI.
- Resultado del tratamiento de no conformidades.
- Resumen de incidentes de seguridad en el último año.
- Estado de los planes de tratamiento de la información.

2. Preparar el Informe de entrada. El encargado de seguridad de la información elaborará el informe de entrada previo a la revisión por parte de la dirección.

3. Convocar la reunión de Revisión. El encargado de seguridad de la información convocará a la alta dirección y a los propietarios del riesgo para la revisión anual.

Los propietarios de un riesgo son aquellos individuos, miembros del equipo del proyecto, responsables de la gestión, el seguimiento y el control de un riesgo identificado que se les ha asignado, incluida la implementación de las respuestas seleccionadas. Es decir, la persona o grupo de individuos que están en las mejores condiciones para comprender e implementar las acciones necesarias para la gestión del riesgo.

Estos propietarios de riesgos evalúan e informan periódicamente al director del proyecto sobre el estado del riesgo y las actualizaciones pertinentes a través de reuniones.

4. Iniciar la reunión. Se analizan los resultados de la información con el objetivo de determinar las acciones de mejora continua adecuadas para el SGSI. Más concretamente:

- Definir el plan de acción para los compromisos no cerrados.
- Presentar los cambios en las partes externas e internas
- Definir los ajustes y el plan de acción necesarios
- Revisar los resultados de no conformidades y acciones correctivas
- Revisar los resultados de la auditoría interna
- Discutir el avance en el cumplimiento de los objetivos de seguridad
- Revisar la retroalimentación de las partes interesadas
- Revisar los resultados de la valoración de riesgos y el avance del plan de tratamiento de riesgos
- Discutir las oportunidades de mejora del SGSI
- Definir y planear las acciones de mejora identificadas

5. Generación de Informe de Salida: Los temas tratados y decisiones acordadas en la reunión de revisión se registrarán en un informe de salida.

FORMATO MODELO PARA EL INFORME DE ENTRADA

INFORME DE ENTRADA
1. Resumen compromisos de la Revisión Anterior
2. Estado y actualización contexto organización
3. Desempeño de los procesos y conformidades
2. Resumen Ejecutivo de Indicadores
2.1. Auditorías realizadas al SGSI
2.2. Efectividad de las Acciones Correctivas
2.3 Gestión de Hallazgos de Auditorías

2.4. Impartición de concienciación personal
2.5. Resultados de las pruebas de concienciación
2.6 Incidentes atendidos
2.7. Retroalimentación con el cliente.
2.8. Idoneidad de los procesos y conformidad del servicio.
2.9. Información de las no conformidades y acciones correctivas del período analizado.
3. Resumen ejecutivo de Hallazgos de Auditoría

4. Resumen ejecutivo de la Gestión de Incidentes de Seguridad

5.Legalidad vigente

6. Oportunidades de mejora del SGSI

FORMATO MODELO PARA EL INFORME DE SALIDA

INFORME DE SALIDA
1. Fecha de Reunión:
2. Asistentes a la Reunión de Revisión:
3.Resultados de la Revisión de Indicadores:
4. Resultados de la Revisión de la Política de Seguridad de la Información:
5. Resultados de la Revisión del Alcance del SGSI:

6. Resultados de la Revisión del Nivel de Riesgo Aceptable:
7. Conclusiones:

GESTIÓN DE ROLES Y RESPONSABILIDADES

La norma ISO 27001 establece los roles, responsabilidades y autoridades en la organización. Se caracteriza por:

- La Dirección es la encargada de la comunicación y asignación de roles dentro de la organización.
- La Dirección asigna las responsabilidades para asegurar la conformidad del SGSI con la normativa ISO 27001.

OBJETIVO

Identificar los roles que tienen alguna responsabilidad en el mantenimiento y/o mejora continua del SGSI de la organización.

ALCANCE

Cargos administrativos y técnicos.

ESTRUCTURA JERÁRQUICA

Estructura jerárquica

COMITÉ DE DIRECCIÓN

El comité de dirección es el más alto órgano de gobierno en la organización.
Está constituido por:

- Director general
- Director de sistemas TI
- Director financiero
- Director comercial
- Director de proyectos

Sus funciones son las siguientes:

- Priorizar la seguridad de la información por parte de la compañía.
- Nombrar a los miembros del Comité de Seguridad de la Información y dotarles de recursos.
- Aprobar la política, normas y responsabilidades generales en materia de seguridad de la información.

- Determinar el umbral de riesgo aceptable en materia de seguridad.
- Analizar posibles riesgos introducidos por cambios en las funciones o funcionamiento de la compañía para adoptar las medidas de seguridad más adecuadas.
- Aprobar el Plan de seguridad de la información.
- Realizar el seguimiento del cuadro de mando de la seguridad de la información

COMITÉ DE SEGURIDAD

El comité de seguridad se trata de un equipo compuesto por al menos una persona de Dirección, para que de esta manera las decisiones que se tomen pueden estar respaldadas por alguien de Dirección. Se encargarán de crear, mantener, supervisar y mejorar el sistema. En el caso de la empresa a analizar el comité de seguridad está formado por el mismo personal que el comité de dirección.

Comité de seguridad

Lo formará el siguiente personal:

- Director general
- Director de sistemas TI
- Director financiero
- Director comercial
- Director de proyectos

Tiene como funciones:

- Revisar los procedimientos de la Auditoría Interna.
- Propiciar la comunicación con los responsables de las diferentes áreas.
- Generar las políticas generales y específicas de la seguridad de la información.
- Aprobar la metodología de análisis de riesgos o los cambios en ella
- Asesorar a la alta dirección en la toma de decisiones con respecto al nivel de riesgo aceptable.
- Analizar la gestión de incidentes de seguridad de la información.
- Medir la eficacia del cumplimiento de los objetivos de seguridad de la información.
- Controlar el cumplimiento en materia de legalidad.
- Promover la concienciación y formación de los usuarios.
- Asignar roles y funciones en materia de seguridad.

DIRECTOR GENERAL

El director general es la persona investida de máxima autoridad en la gestión y dirección administrativa en la empresa.

Funciones en materia de seguridad de la información son las siguientes:

- Garantizar los recursos para el funcionamiento del SGSI.
- Liderar la toma de decisiones estratégicas relacionadas con la gestión de seguridad de la Información.
- Revisar y aprobar la Política de Seguridad de la Información de la empresa.
- Designar a la persona que ocupe la función de Oficial de Seguridad de la Información.
- Establecer junto con el comité de seguridad los controles y auditorías necesarias para el seguimiento del desempeño del SGSI.
- Evaluar, al menos una vez al año, la gestión de la Seguridad de la Información e implantar las acciones necesarias para el cumplimiento de los objetivos.
- Formar parte del comité de seguridad.

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

La empresa MASIAG cuenta con un responsable entre su personal para coordinar los esfuerzos de los distintos órganos establecidos en el SGSI.

El responsable de seguridad de la información tiene una larga lista de funciones:

- Implantar las directrices acordadas por el Comité de Seguridad de la Información.
- Elaborar, promover y mantener las políticas de seguridad de la información de la empresa.
- Colaborar con otros departamentos para velar por el cumplimiento de las políticas de seguridad. Actuar como punto de unión para coordinación de otras unidades y funciones.
- Desarrollar el marco normativo de seguridad y controlar su cumplimiento, con el apoyo del resto de áreas.
- Definir la arquitectura de seguridad de los sistemas de información, monitorizar la seguridad a nivel tecnológico.
- Hacer seguimiento y revisar los incidentes de seguridad, poniéndolo en conocimiento del CSI si fuera necesario.
- Concienciar y formar en seguridad de la información al personal.
- Controlar la gestión de riesgos de nuevos proyectos y velar por el desarrollo seguro de aplicaciones.
- Velar por el cumplimiento legal de las normativas que le son de aplicación, coordinando las actuaciones necesarias con las unidades responsables.
- Coordinar acciones con las áreas de negocio para elaborar y gestionar un Plan de continuidad de negocio de la compañía.
- Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas. Para actualizar el mejorar el Plan de seguridad del a información.
- Revisar periódicamente el estado de la seguridad en cuestiones organizativas, técnicas o metodológicas.
- Promover y coordinar entre las áreas de negocio el análisis de riesgos de los procesos más críticos e información más sensible, y proponer acciones de mejora y mitigación del riesgo, de acuerdo con el umbral aceptable definido por el Comité de Dirección.

DIRECTOR DE SISTEMAS TI

Se trata de la persona responsable del correcto uso y administración de los recursos informáticos de la compañía. Así como ocuparse de los mantenimientos preventivos, solucionar problemas relacionados con hardware y software, mantener equipos actualizados, controlar y configurar las copias de seguridad, así como responder a consultas relacionadas con el manejo de aplicaciones.

Funciones:

- Definir el inventario de activos
- Informar e identificar condiciones inseguras durante el desarrollo de las actividades.
- Cumplir con el plan de capacitación definido en el SGSI
- Implementar las mejoras identificadas, acciones correctivas y preventivas.
- Participación y elaboración del plan programa del SGSI.

DIRECTOR FINANCIERO

Responsable de control de recursos financieros. Se encarga de efectuar el control financiero, aprobar los recursos financieros para inversión o gastos. Así como elaborar el presupuesto anual y velar por su correcta ejecución con referencia a lo planeado. Además efectúa los informes de activos/pasivos del a empresa.

Funciones:

- Proveer los recursos necesarios para el cumplimiento del SGSI.
- Informar e identificar condiciones inseguras en el desarrollo de las actividades.
- Cumplir con el plan de capacitación y concienciación.
- Participar y elaborar el plan del programa de SGSI.

EMPLEADOS INVOLUCRADOS EN LOS PROCESOS

El personal que no está incluido en los comités también tiene que cumplir una serie de obligaciones con respecto al SGSI. Hay una serie de funciones aplicables a todos ellos:

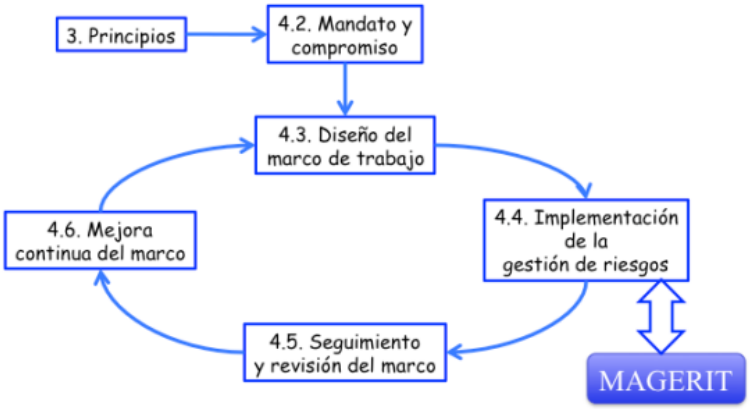
- Hacer un buen uso de los equipos informáticos y tratar adecuadamente la información a la cual se tiene acceso, protegiéndola de accesos no autorizados.
- Respetar las normas y procedimientos en materia de seguridad de la información impulsados por la organización.
- Utilizar adecuadamente las credenciales de acceso a los sistemas informáticos.
- Velar por la confidencialidad de la información.
- Respetar la RGPD.
- Notificar cualquier sospecha o incidente de seguridad que pueda poner en peligro la seguridad de la información.

METODOLOGÍA DE ANÁLISIS DE RIESGOS

El objeto del análisis de riesgos es identificar de manera clara los riesgos a los cuales está expuesta la organización, y determinar las medidas de seguridad más adecuadas para los diferentes activos de seguridad de la información. De igual forma permite establecer los planes de contingencia.

Algunas de las metodologías utilizadas para realizar el análisis de riesgos exigido por la norma ISO 27001 en el marco de la implementación de los SGSI son: Octave, Magerit, Mehari, NIST SP 800:30, Coras, Cramm y Ebios. Cada una de ellas cuenta con ventajas y desventajas, pueden ser de aplicación cualquiera de ellas en la actividad del análisis de riesgos, conforme a lo establecido por la norma ISO 31000 (estándar para la gestión de riesgos) dentro de los SGSI en las organizaciones.

Pero en el caso que tratamos se procederá a utilizar la metodología MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información y recomienda las medidas apropiadas que deberían adoptarse para controlar estos riesgos. El método será adaptado a las características de la empresa que tratamos.



ISO 3100 – Marco de trabajo para la gestión de riesgos

MAGERIT persigue los siguientes objetivos:
Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.
- También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos

Las ventanas e inconvenientes de este método son:

METODOLOGIA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
MAGERIT	Gobierno, compañías grandes comerciales y no comerciales, Pymes.	Alcance completo en el análisis y gestión de riesgos. Está bien documentada en cuanto a recursos de información, amenazas y tipos de activos. Utiliza un completo análisis para su uso. Divide los activos de la organización en diferentes grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier riesgo. Se centra en tres objetivos: concientizar sobre la existencia de los riesgos y de la necesidad de atajarlos a tiempo, ofrecer un método sistemático para analizar tales riesgos, ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación. Permite que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión de riesgos efectiva. Posee una buena base documental en tres libros: El método, Catálogo de elementos y Guías de técnicas, que son de acceso público. Posee herramientas para el análisis de riesgos como PILAR.	En su modelo no involucra los procesos, recursos, ni vulnerabilidades. Se considera una metodología costosa en su aplicación.

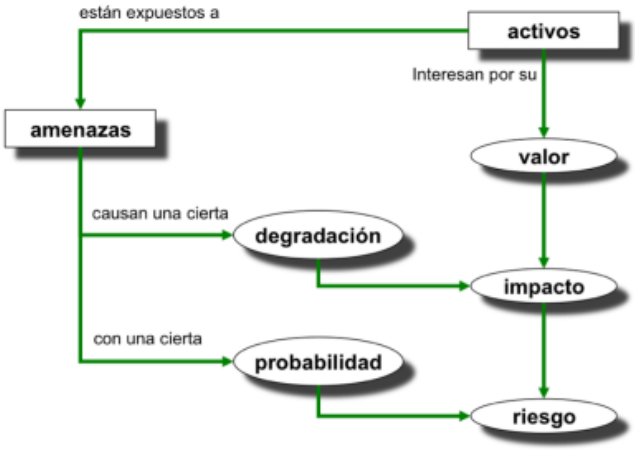
Ventajas e inconvenientes MAGERIT

El análisis de riesgos estima los siguientes componentes:

- Activos: Elementos del sistema de información, o relacionados con el mismo y son de apoyo, para cumplir los objetivos de la organización.
- Amenazas: Hechos que afectan a los activos de la empresa.
- Protección: Medidas para preservar los activos de las amenazas.

Con los componentes anteriores se considera:

- Vulnerabilidades: Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo de la información.
- Impacto: Relación sucesos que pueden ocurrir.
- Riesgo: Peligro al que están expuestos.
- Salvaguardas: Mecanismo de protección frente a las amenazas.



Elementos del análisis de riesgos potenciales

El método para determinar el riesgo sigue los siguientes pasos:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Paso 1: Caracterización de los activos

En esta primera fase se realiza la identificación y agrupación de los activos para valorarlos. Se busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

Una vez los activos han sido inventariados, es decir, los activos son listados, inventariados e identificado el propietario, deben clasificarse de acuerdo a las siguientes categorías:

TIPOS DE ACTIVOS	DESCRIPCIÓN
Activos esenciales	En un sistema de información hay 2 cosas esenciales: la información que se maneja y los servicios que prestan.
Arquitectura del Sistema	Elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.
Datos/Información[D]	El activo que permite a la organización prestar sus servicios.
Claves criptográficas[K]	La criptografía se emplea para proteger el secreto o autenticar a las partes.
Servicios[S]	Funciones que satisfacen las necesidades de los usuarios prestados por el sistema.
Software-Aplicaciones informáticas [SW]	Soporte lógico que permite gestionar, analizar y transformar los datos permitiendo la explotación de la información para la prestación de los servicios
Equipamiento informático [HW]	Recursos materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.

Redes de comunicaciones [COM]	Instalaciones dedicadas como servicios de comunicaciones para medios de transporte que llevan datos de un sitio a otro.
Soportes de información [Media]	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.
Equipamiento auxiliar [AUX]	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
Instalaciones[L]	Lugares donde se alojan los sistemas de información y comunicaciones.
Personal[P]	Las personas relacionadas con los sistemas de información.

Tipos de activos

La tipificación de los activos proporciona información de interés como criterio de identificación de amenazas potenciales y salvaguardas apropiadas a la naturaleza del activo.

El rango de la valoración económica:

El rango de la valoración económica:	RANGO	VALOR
Muy alta	Valor>50.000€	100.000€
Alta	10.000€<valor>50.000€	25.000€
Media	5.000€<valor>10.000€	7.500€
Baja	1.000€<valor>5.000€	2.500€
Muy baja	Valor<1.000€	1.000€

Valoración económica

La dependencia entre los activos se tendrá en cuenta según la definición de la metodología Magerit que indica “los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura depende de los activos que se encuentran más abajo”. Es decir, la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior.

Por último, se debe proceder asignar un valor para cada activo. Mediante las dimensiones se valorará las consecuencias de la materialización de una amenaza. Dicha valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

La valoración de los activos se realizará en función:

Disponibilidad: Un activo tiene un gran valor desde el punto de vista de disponibilidad cuando si una amenaza afectara a su disponibilidad, las consecuencias serían graves.
Integridad: Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización.
Confidencialidad: Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización.
Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

VALOR	CRITERIO
10 extremo	daño extremadamente grave
9 muy alto	daño muy grave
6-8 alto	daño grave
3-5 medio	daño importante
1-2 bajo	daño menor
0 despreciable	irrelevante a efectos prácticos

Valoración daño

La caracterización de los activos utilizará los siguientes campos:

- Identificador: Código que permite identificar de manera unívoca el activo.
- Nombre: Nombre del activo
- Descripción: Breve descripción del activo
- Tipo: Clasificación.
- Responsable: Persona responsable del activo utilizado.
- Valor: Número equivalente a la definición, de acuerdo al criterio estipulado en la escala para valoración de activos.

2. Caracterización de las amenazas.

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación). Engloba las tareas de identificación de las amenazas, así como la valoración de ellas.
El listado de amenazas que pueden sufrir los activos puede ser:

[N] Desastres naturales. Amenazas naturales que pueden ocurrir.
- [N.1] Fuego
- [N.2] Daños por agua
- [N.3] Desastres naturales

[I] De origen industrial. Sucesos que pueden ocurrir en el desempeño de la actividad industrial. Pueden producirse de forma accidental o deliberada.
- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios y suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados
- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de re-encaminamiento
- [E.10] Errores de secuencia
- [E.14] Escapes de información

[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento/ actualización de programas
[E.23] Errores de mantenimiento/ actualización de software
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal

[A] Ataques intencionados
[A.3] Manipulación de los registros de actividad
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] Re- encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

Se pueden dar casos de errores y amenazas, o de los dos casos juntos:
- Amenazas que sólo pueden ser errores, nunca ataques deliberados
- Amenazas que nunca son errores: siempre son ataques deliberados.
- Amenazas que pueden producirse tanto por error como deliberadamente.

Valoración de las amenazas en función de la probabilidad de ocurrencia.

VALOR		CRITERIO	
Muy Alta [MA]	100	Una vez al día	Muy frecuente
Alta [A]	10	Una vez al mes	Frecuente
Media [M]	1	Una vez al año	Normal
Baja [B]	1/10	Una vez cada varios años	Poco frecuente
Muy baja [MB]	1/100	Cada muchos años.	Muy poco frecuente

Valoración amenazas

3. Salvaguardas

Hasta este punto se han tenido en cuenta los impactos y riesgos a que estarían

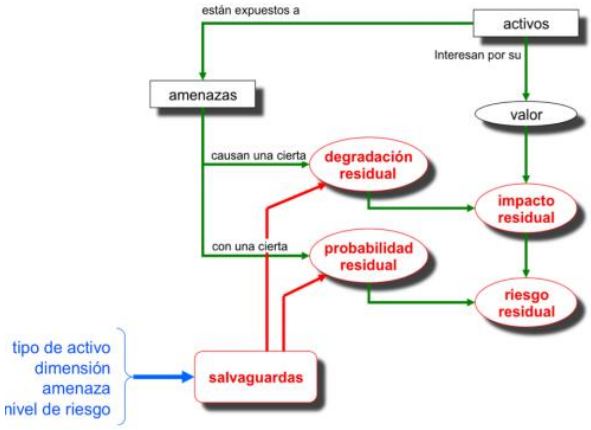
expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes. Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo

Las salvaguardas permiten hacer frente a las amenazas. Las salvaguardas, especialmente las técnicas, varían con el avance tecnológico

- porque aparecen tecnologías nuevas,
- porque van desapareciendo tecnologías antiguas,
- porque cambian los [tipos de] activos a considerar,
- porque evolucionan las posibilidades de los atacantes o
- porque evoluciona el catálogo de salvaguardas disponibles.

Las salvaguardas entran en el cálculo del riesgo de dos formas:

- Reduciendo la probabilidad de las amenazas. Procuran impedir completamente que la amenaza se materialice.
- Limitando el daño causado. Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye.



Elementos de análisis del riesgo residual

Tipos de salvaguardas:

EFECTO	TIPO
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[M] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Tipos de salvaguardas

La valoración de las salvaguardas se efectúa mediante la escala de madurez, recoge en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda. La eficacia y madurez de las salvaguardas:

FACTOR	NIVEL	SIGNIFICADO
0%	L0	Inexistente
	L1	Inicial/ad hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso definido
	L4	Gestionado y medible
100%	L5	Optimizado

Salvaguardas

4. Estimación del Impacto

Esta actividad procesa todos los datos recopilados en las actividades anteriores. El impacto residual es aquel está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

Impacto = valor del activo x degradación (%)

Escala para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:
MB: muy bajo
B: bajo
M: medio
A: alto
MA: muy alto

La tabla para calcular el impacto:

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Impacto

La estimación del impacto:

CONCEPTO	DESCRIPCIÓN	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
MA	Si el hecho se materializará tendría consecuencias o efectos desastrosos en la organización.	Afecta a toda la organización. Multas por incumplimiento de la legislación. Suspensión de las actividades misionales de la organización.
A	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la organización.	Afecta varios conjuntos de datos personales o procesos de la organización.
M	Si el hecho llegara a presentarse tendría	Afecta un conjunto de datos personales

	medianas consecuencias o efectos sobre la organización.	o el proceso.
B	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.	Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso.
MB	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización.	Afecta a una actividad del proceso.

Estimación del impacto

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata.

5. Estimación del Riesgo

El riesgo residual es aquel está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

Riesgo = Impacto x Probabilidad

La escala cualitativa que modela impacto, probabilidad y riesgo es la siguiente:

escalas		
Impacto	Probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Escala impacto, probabilidad y riesgo

Pudiendo combinarse impacto y frecuencia en una tabla para calcular el riesgo:

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Cálculo riesgo

DIMENSIÓN RIESGO	ACCIÓN REQUERIDA
MA	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.

A	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
M	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor. Compartir el riesgo.
B	Mitigar el riesgo mediante de medidas momentáneas y efectivas del proceso que permitan prevenirlo o llevarlo a la zona de riesgo bajo. Asumir el riesgo.
MB	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectivas y preventivas.

Acciones requeridas según el riesgo

6. Umbral de riesgo

Una vez valorado el nivel de riesgo existente para cada activo, se deben comparar los resultados con el umbral del riesgo, es decir, cuándo considera que el nivel de riesgo obtenido es aceptable, y cuándo es necesario actuar sobre el mismo. Este umbral se determina teniendo en cuenta la criticidad del activo y el riesgo calculado. Mediante los siguientes rangos de puntuación se puede determinar los activos sobre los que hay que implementar mejoras:

Rango puntuación riesgo:

Si la dimensión del Riesgo es [MB], [B] o [M]	Riesgo aceptable	Asumir el Riesgo: Riesgos para los cuales se determina que el nivel de exposición es adecuado y por lo tanto se acepta.
	Riesgo tolerable	Mitigar el Riesgo: Riesgos que se puede permitir gestionar, que en caso de materialización la entidad se encuentra en la capacidad de asumirlo.
	Riesgo moderado	Mitigar o Evitar el Riesgo: Riesgos para los cuales se requiere fortalecer los controles existentes y/o agregar nuevos controles.
Si la dimensión del Riesgo es [A]o [MA]	Riesgo importante	Mitigar o Evitar el Riesgo: Implementación de controles adicionales como parte del fortalecimiento de los actuales o como resultado de haberlo compartido o transferido.
	Riesgo inaceptable	Evitar el Riesgo: Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

Umbral de riego

Se deberá de disminuir todos los riesgos por debajo del umbral de riesgos que es el punto en que una organización considera que los riesgos a los que se encuentra expuesta no son aceptables. Para gestionar los riesgos en una empresa pueden tomarse tres decisiones:

- Reducirlos
- Transferirlos
- Aceptarlos

Para ello debe de gestionarse un plan de acción que debería de contener la siguiente información:

- Establecer prioridades, asignar prioridad a los riesgos que deben de reducirse en primer lugar.

- Planteamiento del análisis de coste / beneficio, para cada medida comprobar si el coste de la misma supera el beneficio.
- Selección de controles definitivos
- Asignación de responsabilidades, asignar responsable para la implantación de los controles.
- Implantación de controles

DECLARACIÓN DE APLICABILIDAD

Documento que incluye todos los controles de Seguridad establecidos en la Organización, con el detalle de su aplicabilidad, estado y documentación relacionada.

CONTROL				APLICA	JUSTIFICACIÓN
A.5 Política de seguridad de la información					
	A.5.1 Directrices de la dirección en seguridad de la información				
		A.5.1.1	Conjunto de políticas para la seguridad de la información	SI	Se ha identificado la necesidad de contar con políticas de seguridad de la información para establecer las normas de seguridad dentro de la empresa.
		A.5.1.2	Revisión de las políticas para la seguridad de la información	SI	Se reconoce la necesidad de revisar periódicamente las políticas de seguridad de la información como un factor de éxito en la mejora continua del SGSI.
A.6 Organización de la seguridad de la información					
	A.6.1 Organización interna				
		A.6.1.1	Asignación de responsabilidades para la segur. de la información	SI	Requerido para norma. Necesario para definición de roles. Existen algunas responsabilidades pero es necesario formalizarlos.
		A.6.1.2	Segregación de tareas	SI	Requerido para norma. Necesario para definición de roles y tareas. Debido a la sensibilidad de la información que se trata es necesario realizar segregación de tareas.
		A.6.1.3	Contacto con las autoridades	SI	Requerido para la norma y establecer procedimientos internos. Debido a la sensibilidad de la información debe estar en contacto con las autoridades, grupos de respuesta a emergencias, etc.
		A.6.1.4	Contacto con grupo de especial interés	SI	Requerido para la norma y establecer procedimientos internos. Es necesario pertenecer a grupos de interés especial para estar al tanto de novedades.
		A.6.1.5	Seguridad de la información en la gestión de proyectos.	SI	Requerido para norma. En el desarrollo de software, deben tenerse en cuenta los aspectos de seguridad de la información en la gestión de proyectos.
	A.6.2 Dispositivos móviles y teletrabajo				
		A.6.2.1	Políticas de dispositivos móviles	SI	Requerido para norma y gestionar accesos a información. Auditoría interna. Se ha identificado la necesidad de contar con políticas de seguridad de la información para establecer las normas de seguridad dentro de la empresa.
		A.6.2.2	Teletrabajo	SI	Requerido para norma y gestionar accesos a información. Auditoría interna. El teletrabajo está autorizado e incluye el acceso a activos de información que hacen parte del SGSI, se requiere establecer una política que soporte las medidas de seguridad que se requieren para proteger la información.
A.7 Seguridad de recursos humanos					
	A.7.1 Antes de empleo				
		A.7.1.1	Investigación de antecedentes	SI	Requerido para norma y mejor en procesos selectivos internos. Los empleados y contratistas tendrán acceso a información confidencial por lo cual este control es necesario.

	A.7.1.2	Términos y condiciones de empleo	SI	Requerido para norma y mejor en procesos selectivos internos. Los empleados y contratistas tendrán acceso a información confidencial por lo que este control es necesario.
A.7.2 Durante el empleo				
	A.7.2.1	Responsabilidades de gestión	SI	Requerido por norma y mejora de procedimientos.
	A.7.2.2	Conciencia de seguridad de la información y entrenamiento	SI	Requerido por norma y mejora de formación del personal en seguridad. Planificación de formaciones. Se entiende necesario generar conciencia en el personal para tener éxito en la protección de la seguridad.
	A.7.2.3	Procedimiento disciplinario	SI	Requerido por norma y procedimientos internos para personal. Necesario para mantener protegida la información.
A.7.3 Finalización del empleo o cambio en el puesto de trabajo				
	A.7.3.1	Responsabilidades ante la finalización o cambio	SI	Requerido por norma. Generación de procedimientos de gestión de personal en alta/baja/cambio.
A.8 Gestión de activos				
A.8.1 Responsabilidad de los activos				
	A.8.1.1	Inventario de activos	SI	Requerido por norma. Correcta gestión de activos. Con el fin de controlar la información debido a su sensibilidad y alto valor.
	A.8.1.2	Propiedad de los activos	SI	Requerida por norma. Establecer responsabilidades.
	A.8.1.3	Uso aceptable de los activos	SI	Requerida por norma. Procedimiento de uso de bienes y activos de la empresa. Necesario establecer reglas para el uso aceptable de activos.
	A.8.1.4	Retorno de los activos	SI	Requerida por norma. Procedimiento de uso de bienes y activos de la empresa. Los activos deben ser utilizados solamente para fines laborales y en caso de terminación de contrato laboral deben ser devueltos a la organización.
A.8.2 Clasificación de la información				
	A.8.2.1	Clasificación de la información	SI	Requerida por norma. Documento de clasificación de información. Al tratar información sensible, debe ser clasificada con el fin de poder determinar adecuadamente el manejo que debe dársele.
	A.8.2.2	Etiquetado de la información	SI	Requerida por norma. Documento de clasificación de información. La información debe ser etiquetada de acuerdo a los niveles de clasificación definidos en la política de clasificación de la información.
	A.8.2.3	Manipulado de la información	SI	Requerida por norma. Documento de clasificación de información. Procedimiento que aclare el uso de debe tener la información por parte del personal.
A.8.3 Manejo de los soportes				
	A.8.3.1	Gestión de soportes extraíbles	SI	Requerida por norma. Procedimiento de uso de bienes de la empresa. El uso de dispositivos extraíbles está autorizado por lo cual es indispensable proteger de manera adecuada la información que contiene.

	A.8.3.2	Eliminación de soportes	SI	Requerida por norma. Procedimiento de uso de bienes de la empresa. Se requiere un procedimiento formal para la disposición segura de los medios.
	A.8.3.3	Soportes físicos en tránsito	SI	Requerida por norma. Procedimiento de uso de bienes de la empresa. Debido a la sensibilidad de la información que maneja.
A.9 Control de acceso				
A.9.1 Requisitos empresariales de control de acceso				
	A.9.1.1	Política de control de acceso	SI	Requerida por norma. Gestión de acceso de personal. Se ha identificado la necesidad de contar con políticas de seguridad de la información para establecer las normas de seguridad dentro de la organización.
	A.9.1.2	Acceso a las redes y servicios de red	SI	Requerida por norma. Gestión de acceso de personal. Debido a la sensibilidad de la información que se maneja en los equipos y la red.
A.9.2 Gestión de acceso de usuario				
	A.9.2.1	Registro y baja de usuario	SI	Requerida por norma. Procedimiento de gestión de usuarios. Existe una alta rotación de personal en las áreas.
	A.9.2.2	Provisión de acceso de usuario	SI	Requerida por norma. Procedimiento de gestión de usuarios. Los usuarios tienen distintos niveles de acceso a la información, este control es requerido para proteger la información.
	A.9.2.3	Gestión de privilegiados de acceso	SI	Requerida por norma. Procedimiento de gestión de usuarios. Se gestionan los derechos de acceso privilegiado.
	A.9.2.4	Gestión de la información secreta de autentificación de los usuarios	SI	Requerida por norma. Procedimiento de gestión de usuarios. Reconoce como información secreta de autenticación como un activo crítico.
	A.9.2.5	Revisión de los derechos de acceso de usuario	SI	Requerida por norma. Procedimiento de gestión de usuarios. Este control requiere una segunda validación al proceso de registro y cancelación de usuarios.
	A.9.2.6	Retirada o reasignación de los derechos de acceso	SI	Requerida por norma. Procedimiento de gestión de usuarios. Una vez terminar un contrato laboral deben retirarse los derechos de acceso a la información por parte de ese usuario.
A.9.3 Responsabilidades del usuario				
	A.9.3.1	Uso de información secreta de autenticación	SI	Requerida por norma. Asignación de roles y procedimiento de gestión de usuarios. Reconoce como información secreta de autenticación como un activo crítico.
A.9.4 Control de sistemas y acceso a las aplicaciones				
	A.9.4.1	Restricción del acceso a la información	SI	Requerida por norma. Clasificación de la información. Se requiere para proteger los activos de información dentro del alcance del SGSI.
	A.9.4.2	Procedimiento de inicio de sesión seguro	SI	Requerida por norma. Clasificación de la información. Reconoce este control para una implantación válida para proteger la información de accesos no autorizados.

		A.9.4.3	Sistema de gestión de contraseñas	SI	Requerida por norma. Clasificación de la información. Es necesario el uso de un sistema de gestión de contraseñas con el fin de garantizar la calidad de las mismas.
		A.9.4.4	Uso de programas de servicios públicos privilegiados	SI	Requerida por norma. Clasificación de la información. Reconoce como indispensable este control para proteger la información y los registros de acceso.
		A.9.4.5	Control de acceso al código fuente del programa	SI	Requerida por norma. Clasificación de la información. Realiza desarrollos internos para sistemas de información que hacen parte del alcance del SGSI.
A.10 Criptografía					
	A.10.1 Controles criptográficos				
		A.10.1.1	Políticas sobre el uso de controles criptográficos	SI	Requerida por norma. Se aplica ya que usa el protocolo https para el acceso seguro a las aplicaciones web.
		A.10.1.2	Gestión de claves.	SI	Requerida por norma. Se aplican controles criptográficos para la protección de la información.
A.11 Seguridad física y del entorno					
	A.11.1 Áreas seguras				
		A.11.1.1	Perímetro de seguridad física	SI	Requerida por norma. Gestión de accesos. Las operaciones de los procesos son realizadas en áreas que deben ser aseguradas físicamente.
		A.11.1.2	Controles de entrada físicas	SI	Requerida por norma. Gestión de accesos. Las operaciones de los procesos son realizadas en áreas que deben ser aseguradas físicamente.
		A.11.1.3	Seguridad de oficina, despachos y recursos	SI	Requerida por norma. Gestión de accesos. Las operaciones de los procesos son realizadas en áreas que deben ser aseguradas físicamente.
		A.11.1.4	Protección contra amenazas externas y ambientales	SI	Requerida por norma. Gestión de accesos. Se encuentran en las instalaciones equipos importantes para la empresa.
		A.11.1.5	El trabajo en áreas seguras	SI	Requerida por norma. Gestión de accesos. Los procesos se realizan en áreas que deben ser aseguradas físicamente.
		A.11.1.6	Zonas de entrega y carga	SI	Requerida por norma. Gestión de accesos. Se han identificado áreas donde se carga y descarga equipos.
	A.11.2 Seguridad de los equipos				
		A.11.2.1	Emplazamiento y protección del equipo	SI	Requerida por norma. Gestión de activos, bienes. Los equipos tecnológicos deben ser protegidos.
		A.11.2.2	Instalación de suministro	SI	Requerida por norma. Gestión de activos, bienes. Los equipos tecnológicos deben ser protegidos.

	A.11.2.3	Seguridad del cableado	SI	Requerida por norma. Gestión de activos, bienes. El cableado es importante para la empresa, así que debe ser protegido.
	A.11.2.4	Mantenimiento de los equipos	SI	Requerida por norma. Gestión de activos, bienes. Los equipos son activos importantes para la organización que deben ser mantenidos adecuadamente.
	A.11.2.5	Retirada de materiales propiedad de la empresa	SI	Requerida por norma. Gestión de activos, bienes. Los equipos son un activo especialmente importante que debe ser controlada su retirada.
	A.11.2.6	Seguridad de los equipos fuera de las instalaciones	SI	Requerida por norma. Gestión de activos, bienes. Hay equipos tecnológicos que pueden ser utilizados fuera de las instalaciones.
	A.11.2.7	Reutilización o eliminación segura de equipos	SI	Requerida por norma. Gestión de activos, bienes. Los equipos almacenan información importante, deben ser protegidos.
	A.11.2.8	Equipos de usuario desatendidos	SI	Requerida por norma. Gestión de activos, bienes. Los equipos almacenan información importante, deben ser protegidos.
	A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	SI	Requerida por norma. Gestión de activos, bienes. Los equipos almacenan información importante, deben ser protegidos.
A.12 Operaciones de seguridad				
A.12.1 Procedimientos y responsabilidades en las operaciones				
	A.12.1.1	Procedimientos operativos documentales	SI	Requerido por norma. Procedimientos y operativas de personal. Todas las operaciones son ejecutadas por personal.
	A.12.1.2	Gestión de cambios	SI	Requerido por norma. Procedimientos y operativas de personal. Deben efectuarse labores de mantenimiento, etc. para proteger la disponibilidad.
	A.12.1.3	Gestión de la capacidad	SI	Requerido por norma. Procedimientos y operativas de personal. Debe ser gestionado el posible crecimiento en cuanto a clientes, etc.
	A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	SI	Requerido por norma. Procedimientos y operativas de personal. Se efectúan desarrollos internos por lo que la norma es aplicable.
A.12.2 Protección contra malware				
	A.12.2.1	Controles contra el malware	SI	Requerido por norma. Seguridad lógica. Los sistemas pueden susceptibles a código malicioso, por lo tanto es requerido el control.
A.12.3 Copias de seguridad				
	A.12.3.1	Copia de seguridad de la información	SI	Requerido por norma. Plan de continuidad de negocio. Se reconoce como indispensable ante la respuesta a posibles incidentes de seguridad de la información.
A.12.4 Registro y seguimiento				

	A.12.4.1	Registro de eventos	SI	Requerido por norma. Gestión de acceso a información. La trazabilidad de la actividad de los usuarios sobre sus activos de información.
	A.12.4.2	Protección de la información de los registros	SI	Requerido por norma. Gestión de acceso a información. La trazabilidad de la actividad de los usuarios sobre sus activos de información.
	A.12.4.3	Registros de administración y operación	SI	Requerido por norma. Gestión de acceso a información. La trazabilidad de la actividad de los usuarios sobre sus activos de información.
	A.12.4.4	Sincronización del reloj	SI	Requerido por norma. Gestión de acceso a información. La hora de los dispositivos informáticos debe estar sincronizada.
A.12.5 Control de software en explotación				
	A.12.5.1	Instalación de software en explotación	SI	Requerido por norma. Seguridad lógica. Los sistemas operativos deben protegerse para evitar malware, virus, etc.
A.12.6 Técnico de gestión de vulnerabilidades				
	A.12.6.1	Gestión de vulnerabilidades técnicas	SI	Requerido por norma. Seguridad lógica. Equipos que están expuestos a vulnerabilidades.
	A.12.6.2	Restricciones de instalación de software	SI	Requerido por norma. Seguridad lógica. Es necesario el control del software que se instala que puede ocasionar daños de malware, etc.
A.12.7 Consideraciones sobre la auditoria de sistemas de información				
	A.12.7.1	Controles de auditoría de sistemas de información	SI	Requerido por normal. Evolución del sistema de gestión de la seguridad. Las auditorías técnicas son necesarias para prevenir la indisponibilidad.
A.13 Seguridad de las comunicaciones				
A.13.1 Gestión de la seguridad de la red				
	A.13.1.1	Controles de red	SI	Requerido por norma. Seguridad lógica. Asegurar la red interna de datos de la empresa.
	A.13.1.2	Seguridad de los servicios de red	SI	Requerido por norma. Seguridad lógica. Asegurar la red interna de datos de la empresa.
	A.13.1.3	Segregación en redes	SI	Requerido por norma. Seguridad lógica. Es necesario implementar una infraestructura tecnológica con segregación de redes, varias capas de seguridad.
A.13.2 Intercambio de información				
	A.13.2.1	Políticas y procedimientos de intercambio de información	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Hay necesidad de contar con políticas de seguridad de la información para establecer las normas de seguridad dentro de la compañía.
	A.13.2.2	Acuerdos de intercambio de información	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.

	A.13.2.3	Mensajería electrónica	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.
	A.13.2.4	Acuerdos de confidencialidad o de no revelación	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información				
A.14.1 Requisitos de seguridad en los sistemas de información				
	A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	SI	Requerido por norma. Procedimiento de seguridad de sistemas de información. Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida.
	A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	SI	Requerido por norma. Procedimiento de seguridad de sistemas de información. Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida.
	A.14.1.3	Protección de las transacciones de servicios de aplicaciones	SI	Requerido por norma. Procedimiento de seguridad de sistemas de información. Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida.
A.14.2 Seguridad en el desarrollo y en los procesos de soporte				
	A.14.2.1	Políticas de desarrollo seguro	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.
	A.14.2.2	Procedimientos de control de cambio del sistema	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.
	A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.
	A.14.2.4	Restricciones a los cambios en los paquetes de software	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.
	A.14.2.5	Principios de ingeniería de sistemas seguros	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.
	A.14.2.6	Entorno de desarrollo seguro	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información.
	A.14.2.7	Externalización del desarrollo de software	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Preparar el sistema para la posible externalización del desarrollo del software.
	A.14.2.8	Pruebas funcionales de seguridad del sistema	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Preparar el sistema para posibles desarrollos software en los procesos incluidos en el alcance SGSI.
	A.14.2.9	Pruebas de aceptación del sistema	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Preparar el sistema para posibles desarrollos software en los procesos incluidos en el alcance SGSI.

A.14.3 Datos de prueba				
	A.14.3.1	Protección de datos de prueba	SI	Requerido por norma. Procedimiento de protección de datos y uso de los mismos. Preparar el sistema para posibles desarrollos software en los procesos incluidos en el alcance SGSI.
A.15 Relación con proveedores				
A.15.1 Seguridad en las relaciones con proveedores				
	A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Con el fin de proteger la información que se intercambia con terceros.
	A.15.1.2	Requisitos de seguridad en contratos con terceros	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Con el fin de proteger la información que se intercambia con terceros.
	A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Con el fin de proteger la información que se intercambia con terceros.
A.15.2 Gestión de la provisión de servicios del proveedor				
	A.15.2.1	Control y revisión de la provisión de servicios del proveedor	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Con el fin de proteger la información que se intercambia con terceros.
	A.15.2.2	Gestión de cambios en la provisión del servicio de proveedor	SI	Requerido por norma. Seguridad lógica. Procedimientos de protección de datos. Con el fin de proteger la información que se intercambia con terceros.
A.16 Gestión de incidentes de seguridad de la información				
A.16.1 Gestión de incidentes de seguridad de la información y mejoras				
	A.16.1.1	Responsabilidades y procedimientos	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades. Gestionar las responsabilidades y procedimientos en caso de situaciones adversas.
	A.16.1.2	Informar eventos de seguridad de la información	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades. Gestionar e informar de los eventos que pudieran producirse en materia de seguridad.
	A.16.1.3	Informar las debilidades de seguridad de la información	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades. Gestionar e informar de las debilidades que pudieran producirse en materia de seguridad.
	A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades. Asegurar la gestión de incidentes de seguridad.
	A.16.1.5	Respuesta a incidentes de seguridad de la información	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades. Procedimiento de contingencia. Asegurar la gestión de incidentes de seguridad.
	A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades. Aprendizaje de situaciones generadas por incidentes de seguridad de la información.

	A.16.1.7	Recopilación de evidencias	SI	Requerido por norma. Continuidad de negocio y asignación de roles, responsabilidades. Protección de datos. La gestión de la seguridad de la información debe tener en cuenta la recopilación de evidencias que ayuden a mejorar el SGSI.
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio				
A.17.1 Continuidad de la seguridad de la información				
	A.17.1.1	Planificación de la continuidad de la seguridad de la información	SI	Requerido por norma. Seguridad lógica, política de seguridad. La continuidad de la seguridad de la información debería formar parte de los sistemas de gestión de continuidad de negocio de la organización.
	A.17.1.2	Implementación de la continuidad de la seguridad de la información	SI	Requerido por norma. Seguridad lógica, política de seguridad. La continuidad de la seguridad de la información debería formar parte de los sistemas de gestión de continuidad de negocio de la organización.
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	Requerido por norma. Seguridad lógica, política de seguridad. La continuidad de la seguridad de la información debería formar parte de los sistemas de gestión de continuidad de negocio de la organización.
A.17.2 Redundancias				
	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	SI	Requerido por normal. Continuidad del negocio. Asegurar la disponibilidad de los recursos de tratamiento de la información.
A.18 Cumplimiento				
A.18.1 Cumplimiento de requisitos legales y contractuales				
	A.18.1.1	Identificación de la legislación aplicable y los requisitos contractuales.	SI	Requerido por norma. Protección de datos y LSSIE. Las operaciones deben realizarse de acuerdo a los requisitos legales que le apliquen.
	A.18.1.2	Derechos de propiedad intelectual	SI	Requerido por norma. Protección de datos y LSSIE. Lo exige la ley.
	A.18.1.3	Protección de los registros de la organización	SI	Requerido por norma. Protección de datos y LSSIE. Este control es necesario de cara a posibles incidentes de seguridad.
	A.18.1.4	Protección y privacidad de la información de carácter personal	SI	Requerido por norma. Protección de datos y LSSIE. Debe preservarse la privacidad de la información de carácter personal.
	A.18.1.5	Regulación de controles criptográficos	SI	Requerido por norma. Protección de datos y LSSIE. La regulación de los controles criptográficos es de obligación para el cumplimiento legal.
A.18.2 Revisiones de seguridad de la información				
	A.18.2.1	Revisión independiente de seguridad de la información	SI	Requerido por norma. Protección de datos y LSSIE. Identificar las fallas y oportunidades de mejora del sistema y garantizar que se opera según las políticas y procedimientos de la organización.
	A.18.2.2	Cumplimiento de políticas y estándares de seguridad	SI	Requerido por norma. Protección de datos y LSSIE. Identificar las fallas y oportunidades de mejora del sistema y garantizar que se opera según las políticas y procedimientos de la organización.

		A.18.2.3	Revisión de cumplimiento técnico	SI	Requerido por norma. Protección de datos y LSSIE. Identificar las fallas y oportunidades de mejora del sistema y garantizar que se opera según las políticas y procedimientos de la organización.