Proyecto SGSI

Garantía y Seguridad de la Información

Grupo G4
Jhon Steeven Cabanilla Alvarado
Pablo Muñoz Hernández
Javier Rodríguez Martín

Fase I: Análisis de la organización

- Empresa dedicada a la topografía y geodesia, que se encuentra en crecimiento.
- Necesidad mayor de seguridad informática debido a este crecimiento.
- Dispone de una sede de 150 m2 (oficinas, áreas de trabajo, servidores...)
- Servidores: 2 servidores Blade, y almacenamiento tanto en disco como en NAS
- Acceso internet con router doméstico ISP, sin firewall ni proxy.
- Objetivos generales relacionados con la seguridad (Entre otros):
  - **Garantizar que la información sólamente es accedida por las personas o procesos autorizados para ello.**
  - Asegurar que la información solamente puede ser modificada por las personas o los procesos autorizados para ello, sin que se produzca corrupción en ella.
  - Garantizar que la información es accesible en el momento y las condiciones preestablecidas.

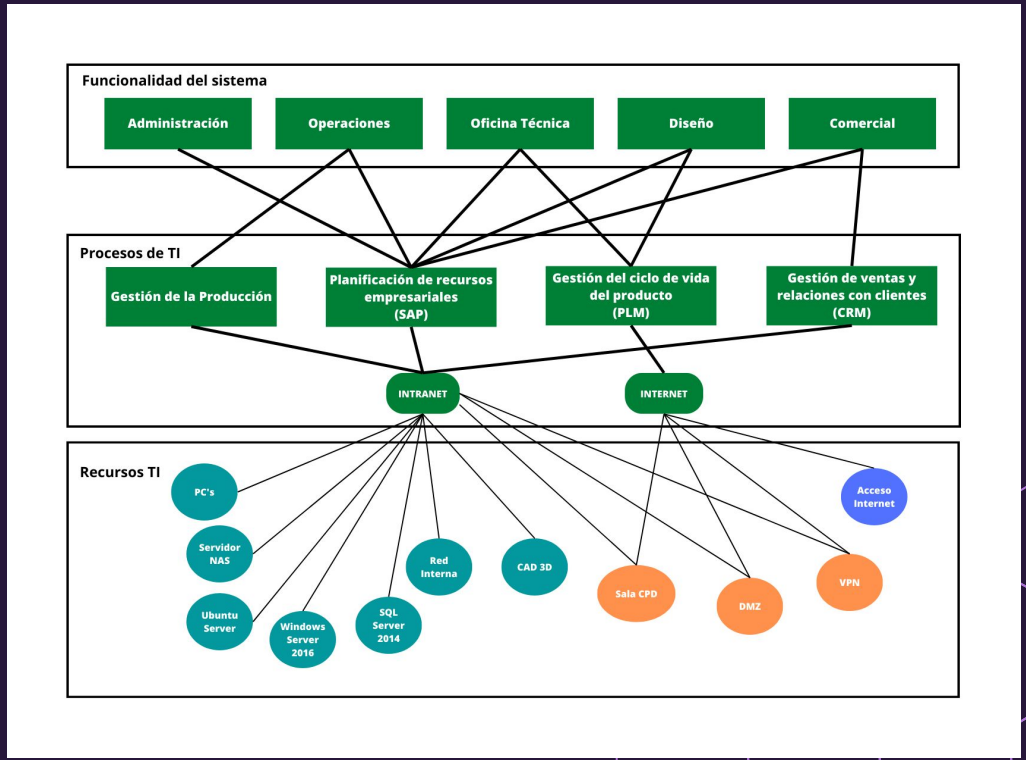
Fase I: Análisis de la organización

- Agentes implicados:
    - Dirección general
    - Comité de seguridad
    - Responsables de la información servicios
    - Responsable de sistemas y telecomunicaciones.
    - Responsable de seguridad
    - Usuario
- La empresa también cuenta con diversas funcionalidades, distintos recursos de TI, y una arquitectura que cuenta con ciertas normas y medidas de seguridad.

Se va a realizar un sistema de seguridad informática para proteger la información importante con la que cuenta esta empresa.

Fase II: Elaboración del catálogo de activos

Diferentes activos con los que cuenta la empresa y sus relaciones:



Catálogo de activos

La empresa cuenta con diferentes activos, obtenidos del MAGERIT, que se dividen en diferentes categorías:

1. Servicio
2. Datos e información
3. Aplicaciones software
4. Personal
5. Redes de comunicaciones
6. Soportes de información
7. Equipamiento auxiliar
8. Instalaciones
9. intangibles

Todos estos activos se valoran en función de su importancia en la empresa

Inventario de activos

Ejemplo de un activo, con su descripción, características y dependencias:

[HW]Equipos Informáticos	
Código: HW.1	Nombre: Equipos Informáticos
Descripción: Los equipos de sobremesa o portátiles son dispositivos informáticos que se utilizan por los profesionales de campo, técnicos y administrativos de la empresa. Cada puesto de trabajo dispone de un equipo de sobremesa o portátil que incluye un monitor, un teclado y un ratón conectados a través de un concentrador.	
Propietario: Responsable de sistemas y telecomunicaciones	
Crítico: Sí	
Localización: Oficina técnica	
Dependencias	
Activos: COM.3	Grado: Alto
¿Por qué? Los equipos informáticos necesitan acceder a Internet para realizar muchas de sus funciones.	
Dependencias	
Activos: COM.5, Media.1, Media.2	Grado: Alto
¿Por qué? Los equipos informáticos pueden necesitar acceder a servidores para realizar ciertas tareas, como el almacenamiento de datos o la ejecución de aplicaciones.	
Dependencias	
Activos: SW.1, SW.2, SW.3	Grado: Alto
¿Por qué? Los equipos informáticos necesitan aplicaciones de software para realizar muchas de sus funciones.	
Dependencias	
Activos: COM.1, COM.2, COM.4	Grado: Medio
¿Por qué? Los equipos informáticos pueden funcionar sin una red de comunicaciones.	

Otro ejemplo de tabla de activos con sus características y dependencias:

[Media]Soportes de la información	
Código: Media.1	Nombre: Dispositivos de almacenamiento
Descripción: Los dispositivos de almacenamiento son aquellos en los que se guarda la información de la empresa. En este caso, se dispone de almacenamiento tanto en disco dedicado como en NAS. Esto significa que tiene servidores con discos duros exclusivos para el almacenamiento de la información y un dispositivo de almacenamiento en red (NAS) que permite a los usuarios acceder a los datos de forma centralizada a través de la red. Estos dispositivos son fundamentales para la empresa ya que en ellos se guardan todos los datos y la información necesarias para el funcionamiento del negocio.	
Propietario: Responsable de la información y de los servicios	
Crítico: Sí	
Localización: Sala CPD	
Código: Media.2	Nombre: Servidores y sistema de almacenamiento en red (NAS)
Descripción: Los servidores y el sistema de almacenamiento en red (NAS) son dispositivos informáticos que se utilizan para guardar y gestionar la información de la empresa. Los servidores están especialmente diseñados para procesar y gestionar grandes cantidades de datos y permitir el acceso a ellos a través de la red. En el caso de esta empresa, tiene dos servidores Blade y un sistema de almacenamiento en red NAS, que se encuentran ubicados en la sala de servidores.	
Propietario: Responsable de la información y de los servicios	
Crítico: Sí	
Localización: Sala CPD	
Dependencias	
Activos: COM.5	Grado: Alto
¿Por qué? Sin estos servidores, los dispositivos de almacenamiento no serían accesibles y no se podría utilizar la información almacenada en ellos. Es importante garantizar que ambos activos estén siempre disponibles y en buen estado para evitar interrupciones en el funcionamiento de la empresa.	
Dependencias	
Activos: L.1	Grado: Medio
¿Por qué? Los soportes de la información dependen de las instalaciones de la empresa, debido a que el lugar físico en el que se encuentren debe contar con una serie de condiciones específicas, como por ejemplo, temperaturas óptimas o refrigeración adecuada.	

Valoración de activos

Dos activos de ALTA IMPORTANCIA:

Datos de clientes y proyectos: Los datos de clientes y proyectos son de alta importancia para la empresa, ya que son esenciales para la actividad principal de la empresa y para cumplir con sus objetivos. Estos datos incluyen información sobre los clientes de la empresa, como sus datos de contacto y sus preferencias, así como información sobre los proyectos en los que está trabajando la empresa, como los plazos, presupuestos y requerimientos específicos de cada proyecto.

Servicio de gestión de proyectos: alta importancia debido a que la gestión adecuada de los proyectos es esencial para la correcta ejecución de la actividad de la empresa y para cumplir con los plazos y presupuestos establecidos.

ACTIVOS DE MEDIA IMPORTANCIA:

Equipos de sobremesa o portátiles: Los equipos de sobremesa o portátiles utilizados por los profesionales de campo, técnicos y administrativo son de media importancia para la empresa de topografía y geodesia, ya que, aunque son necesarios para el desempeño de sus tareas, no son esenciales para la realización de su actividad principal.

Servicio de atención al cliente: media importancia, ya que, aunque el servicio de atención al cliente es importante para la satisfacción del cliente y para mantener una buena relación con ellos, no es esencial para la actividad principal de la empresa.

ACTIVOS DE BAJA IMPORTANCIA:

Cerraduras electrónicas: Las cerraduras electrónicas son importantes para proteger el acceso a la empresa, pero su valor es bajo, ya que se pueden utilizar otras medidas de seguridad físicas para protegerlas.

Aire acondicionado: Bajo. El aire acondicionado es un activo necesario para garantizar un ambiente idóneo, pero no es un activo fundamental para la empresa.

Fase III: Elaboración del listado de amenazas

Para llevar a cabo el listado de amenazas hemos utilizado el catálogo de amenazas que establece **Magerit** de amenazas posibles sobre los activos de un sistema de información. Para cada amenaza se ha incluido la siguiente información:

- Código de la amenaza.
- Su descripción.
- La probabilidad de que se materialice y por qué.
- Activos a los que afecta y el nivel de impacto sobre la Confidencialidad, Integridad, Disponibilidad, Autenticación y Trazabilidad.

Nivel de impacto		Nivel de Probabilidad	
Impacto	**Descripción**	**Probabilidad**	**Descripción**
Alto	Degradación total	Alta	Mensualmente
Medio	Degradación perceptible	Media	Una vez al año
Bajo	Degradación inapreciable	Baja	Cada varios años

Categoría de amenaza	Descripción
[N] Desastres naturales	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
[I] De origen industrial	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial y que pueden darse de forma accidental o deliberada.
[E] Errores y fallos no intencionados	Fallos no intencionales causados de forma directa por la actividad de personas que tienen acceso al sistema de información. Muchas se producen por error u omisión.
[A] Ataques intencionados	Fallos deliberados causados por la actividad humana con el objetivo o bien de beneficiarse indebidamente o de causar daños a la organización.

AMENAZA [N.1] FUEGO

[N.1] Fuegos					
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema					
Probabilidad: Baja Los incendios son eventos relativamente infrecuentes en un entorno de oficinas y se pueden tomar medidas preventivas para minimizar el riesgo de incendios.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
HW.1 - Equipos de sobremesa o portátiles	-	-	A	-	B
Media.1- Dispositivos de almacenamiento	-	-	A	-	B
Media.2 - Servidores y sistemas de almacenamiento	-	-	A	-	B
AUX.1 – Cerraduras electrónicas	-	-	A	-	B
AUX.2 – Aire acondicionado	-	-	A	-	B
L.1 – Sede de la empresa	-	-	A		B

AMENAZA [E.8] DIFUSIÓN DE SOFTWARE DAÑINO

[E.8] Difusión de software dañino.					
Descripción: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.					
Probabilidad: Media En general, la probabilidad de que ocurra esta amenaza puede variar dependiendo de diversos factores, como la seguridad del sistema, la calidad de las medidas de protección contra el malware, y la actividad de los usuarios en línea. En general, se puede decir que la probabilidad de que ocurra esta amenaza puede ser media.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
SW.1 – Aplicaciones de topografía y geodesia.	A	A	M	A	B
SW.2 - Aplicaciones de planificación de recursos y de gestión de la producción.	A	A	M	A	B
SW.3 - Aplicaciones de gestión de relaciones con clientes.	A	A	M	A	B

Fase IV: Evaluación y gestión de Riesgos

- Análisis de los activos con mayor importancia.
- Tablas empleadas:

TABLA PARA ESTIMAR LA PROBABILIDAD	
VALOR	**DESCRIPCIÓN**
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Medio (2)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (3)	La amenaza se materializa a lo sumo una vez cada semana.

(1)

TABLA PARA ESTIMAR EL IMPACTO	
VALOR	**DESCRIPCIÓN**
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

(2)

CRITERIOS DE ACEPTACIÓN DEL RIESGO	
RANGO	**DESCRIPCIÓN**
Riesgo <= 4	La organización considera el riesgo poco reseñable.
Riesgo > 4	La organización considera el riesgo reseñable y debe proceder a su tratamiento.

(3)

Ejemplo I

D.4 - Información financiera de la empresa			
Amenazas	**Probabilidad**	**Impacto**	**Riesgo**
[E.1] Errores de los usuarios	3	2	6
[E.2] Errores del administrador.	2	3	6
[A.5] Suplantación de la identidad del usuario	2	3	6

Ejemplo II

SW.1 - Aplicaciones de topografía y geodesia			
Amenazas	**Probabilidad**	**Impacto**	**Riesgo**
[I.5] Avería de origen físico o lógico	2	1	2
[E.1] Errores de los usuarios	3	1	3
[E.2] Errores del administrador	2	3	6
[E.8] Difusión de software dañino	2	3	6
[E.9] Errores de [re-]encaminamiento	1	2	2
[E.20] Vulnerabilidades de los programas (software)	2	3	6
[E.21] Errores de mantenimiento/actualización de programas (software)	2	2	4
[A.5] Suplantación de la identidad del usuario	2	2	4
[A.8] Difusión de software dañino	2	3	6

Fase V: Propuesta de salvaguardas

Criterio — Riesgo > 4: Riesgo reseñable y procedemos al correspondiente tratamiento

SW.1 - Aplicaciones de topografía y geodesia		
Amenazas	**Salvaguardas**	**Probabilidad**
[E.2] Errores del administrador	Capacitación y formación del personal responsable	Alta
	Revisión y validación de cambios	Media
	Copias de seguridad y recuperación	Media

Tabla de salvaguardas – Explicaciones

S.1 - Procesos de negocio		
Amenazas	**Salvaguardas**	**Probabilidad**
[A.5] Suplantación de la identidad del usuario	Autenticación fuerte	Muy Alta
	Monitoreo del acceso	Alta
	Uso de contraseñas seguras	Muy Alta

Autenticación fuerte: como la autenticación de dos factores, que implica utilizar dos métodos diferentes para verificar la identidad del usuario.

Monitoreo del acceso: se pueden implementar medidas para monitorear el acceso a los sistemas, de manera que se pueda detectar y prevenir intentos de suplantación de la identidad del usuario.

Referencias

- MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [Libro I - Método]
- MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [Libro II - Catálogo de Elementos]
- SGSI - Implantación de un SGSI en la empresa
- Tablas extraídas de las Plantillas proporcionadas para realizar cálculos.