Informe de seguridad del sistema

GARANTÍA y SEGURIDAD DE LA INFORMACIÓN
Curso 22/23

Grupo G4

Jhon Steeven Cabanilla Alvarado
Pablo Muñoz Hernández
Javier Rodríguez Martín

1. Características del Sistema

1.1. Panorámica del Sistema

Se trata de una empresa pequeña del sector Topografía y Geodesia, con 3 profesionales de campo, 2 técnicos y 1 administrativo. Se ha ido dotando a lo largo de los años de infraestructura y sistemas de almacenamiento de la información a medida que han ido surgiendo las necesidades de negocio y/o la plantilla ha ido creciendo.

Este modelo de crecimiento ha propiciado que actualmente no se cuente con una infraestructura totalmente estandarizada ni con unos medios técnicos bien dimensionados para el funcionamiento de los sistemas.

La actividad diaria de la empresa se desarrolla con normalidad, pero soporta un nivel de riesgo en el ámbito de la seguridad informática que resulta peligroso para una empresa de sus características, que cuenta, en la actualidad, con unas cifras de negocio y plantilla que en nada se parecen a las iniciales.

La empresa dispone de despachos individuales para cada uno de los técnicos, administrativos y directivos. El resto comparte oficina abierta. Cada puesto de trabajo dispone de un equipo de sobremesa o portátil con monitor, teclado y ratón conectables a través de un concentrador.

1.1.1. Dependencias

La empresa dispone de una sede con unos 150 m2 distribuidos en varias zonas: oficina, área de trabajo, sala de servidores, almacén, zona de café/reuniones. La puerta de acceso a la empresa, al almacén y a la sala de máquinas se controlan con cerraduras electrónicas activadas desde una aplicación móvil. Se dispone de sistema de aire acondicionado estándar en toda la instalación, pero ni la sala de máquinas ni el almacén cuentan con refrigeración o adaptación técnica específica.

1.1.2. Servidores

El departamento dispone de dos servidores Blade y de almacenamiento tanto en disco dedicado como en NAS, todos ellos en la sala de servidores en un armario rack de 21” de capacidad suficiente. La compañía tiene en su poder dos servidores y un NAS que se encuentran ubicados en la sala del CPD.

1.1.3. Comunicaciones

El servicio de acceso a internet se realiza mediante un router doméstico proporcionado por el ISP que da servicio actualmente a las instalaciones, y con ausencia de firewall y proxy.

Por otro lado, la distribución del cable a los equipos se realiza a través de un switch de 24 bocas sin gestión.

La comunicación vía wifi se realiza directamente al router que cuenta con una clave WPA2.

1.2. Política

Las directrices y objetivos generales que en relación con la seguridad guían a la compañía son:

- Garantizar que la información solamente 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.
- Establecer sistemas enfocados a la mejora continua que se adapten y se actualicen en función de unos objetivos claros, concisos y medibles que establece la estrategia marcada por la Dirección.
- Instruir, motivar e implicar a todo el personal en la gestión y desarrollo del sistema de seguridad, fomentando la autorresponsabilidad.
- Dotar de los recursos necesarios para el logro de la satisfacción de todas las partes interesadas, tanto internas como externas.

Para aplicar esta política, se lleva a cabo la implantación de un SGSI basado en la norma ISO/IEC 27001.

1.3. Agentes implicados

1.3.1. Dirección general

Las funciones atribuidas a la dirección estratégica de la organización consistirán en proporcionar medios para los planes de seguridad, nombrar al resto de los responsables e impulsar la política de seguridad.

1.3.2. Comité de seguridad

El comité de seguridad estará compuesto por directivos con capacidad de decisión que cubran varias áreas de la organización. Este comité estará formado por (*varios roles pueden estar desempeñados por la misma persona*):

Rol	Persona a desempeñarlo
Responsable de sistemas y telecomunicaciones	Director de IT
Responsable de asesoría legal	Subcontratado. Bajo control de Director de IT
Responsable de línea de negocio	Director de Operaciones Director Técnico (I+D+i) Director de Diseño

Sus funciones son la aprobación de la política de seguridad y los proyectos de mejoras relacionados con la misma.

1.3.3. Responsables de la información y de los servicios

Generalmente se establecen por líneas de negocio o departamentos. Se define como responsable el respectivo director del departamento, para cada una de las líneas departamentales existentes en la empresa que son:

- Administración (Finanzas/RR.HH.)
- Operaciones (trabajos de campo)
- Oficina Técnica
- Comercial

Sus funciones serán las de definir los requisitos de seguridad de su servicio o departamento y asegurarse de que las personas a su cargo usan adecuadamente, y acorde a normativa, los medios de los que disponen.

1.3.4. Responsable de sistemas y telecomunicaciones

El director de IT, apoyándose en el personal técnico a su cargo, será el responsable de que funcionen correctamente los sistemas informáticos.

Las funciones serán configurar y mantener los sistemas informáticos, aplicar la política de respaldo y recuperación, monitorizar y supervisar los posibles incidentes de seguridad y aplicar los procedimientos de operación y administración con controles de seguridad.

1.3.5. Responsable de seguridad

El director de IT será el responsable de la seguridad de la organización. Sus funciones serán coordinar y asegurar que se toman las medidas de seguridad adecuadas. Para ello debe conocer el estado de la seguridad, plantear y coordinar el Plan Director de Seguridad y plantear y coordinar el Plan de Continuidad de Negocio.

1.3.6. Usuario

Debe usar los sistemas siguiendo las normas y directrices definidas por la compañía.

1.4. Funcionalidad del sistema

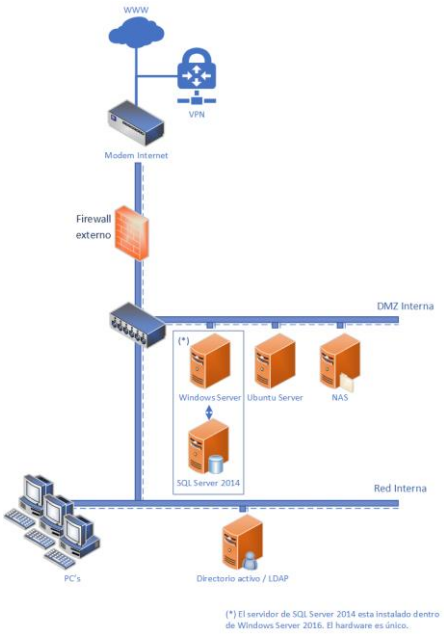
- Administración (Finanzas/RR.HH.): SAP, software de planificación de recursos empresariales.
- Operaciones: Software para la gestión de la producción.
- Oficina Técnica: PLM, software de gestión del ciclo de vida del producto.
- Diseño: PLM, software de gestión del ciclo de vida del producto.
- Comercial: Software para la gestión de las ventas y las relaciones con los clientes.

1.5. Recursos de TI

- PC 's.
- Servidor NAS. Se almacenan los diseños de los productos, los catálogos comerciales, las fotometrías, …
- Ubuntu Server. En este servidor están todas las aplicaciones internas que dan soporte a Operaciones y Gestión de Proyectos, desarrolladas en Java y Python. Aquí está el servidor Web.
- Windows Server 2016. Está aquí el servidor de correo, Exchange, y el Directorio Activo.
- Estaciones de trabajo (4) para diseño asistido por computador, aplicaciones de gestión de datos de estaciones topográficas, …
- SQL Server 2014.
- Red Interna.
- Programas específicos de CAD y de reconstrucción 3D.
- VPN: tecnología de red que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.
- DMZ: red aislada que se encuentra dentro de la red interna de la organización. En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet, como el servidor web o de correo.
- Acceso a Internet.

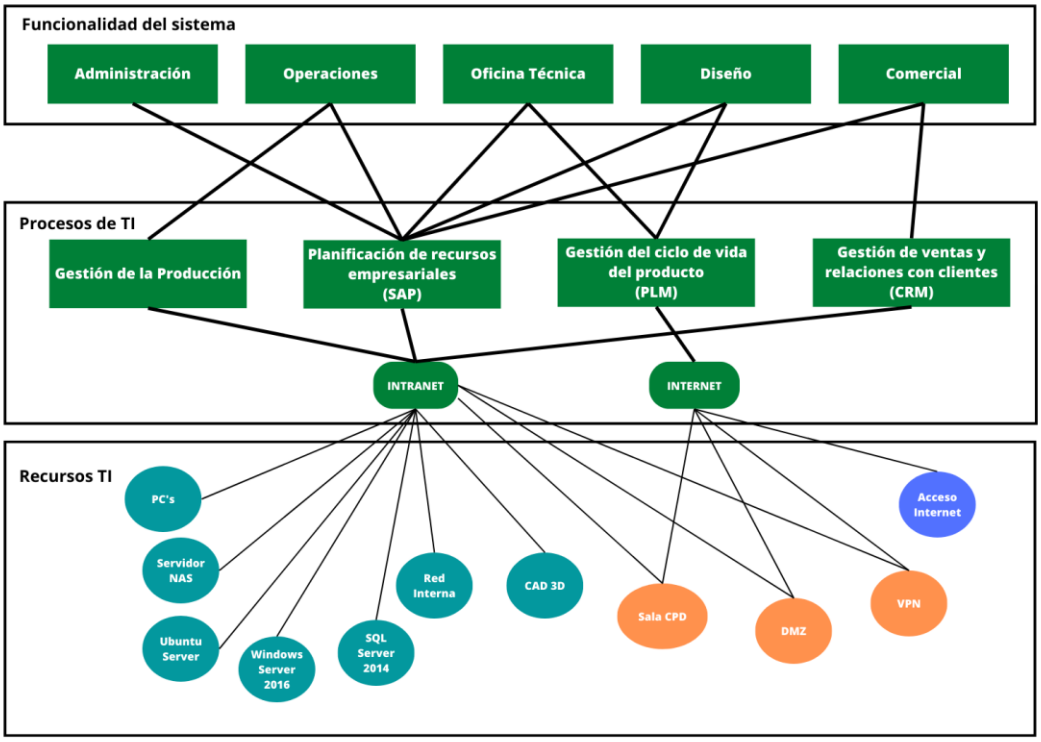
1.6. Arquitectura

Para implementar la ISO/IEC 27001 es necesario disponer de una arquitectura que cumpla ciertas normas y medidas de seguridad. La que se propone implantar inmediatamente es la siguiente:



Se trata de una arquitectura con una red interna, un switch de cabecera, un firewall y un modem profesional de fibra óptica simétrica con doble canal de respaldo. Los servidores estarán conectados con los ordenadores a través de la red interna y el acceso a la red estará controlado por el directorio activo. Hay tres servidores disponibles uno con Windows Server 2016 y SQL Server 2014, otro con Ubuntu Server 18.04 LTS y un NAS Synology. Para las conexiones desde el exterior, se instalará un servicio VPN que proporcionará acceso seguro a los recursos internos de la empresa.

1.7. Mapa de activos



2. Análisis de Riesgos y Medidas de Seguridad

2.1. Bienes de Información valiosos (catálogo de activos)

Como bien sabemos, los activos pueden dividirse en diferentes grupos según su naturaleza. Por este motivo, utilizaremos la **metodología de Magerit** para agrupar activos. A continuación, se presenta un catálogo de activos en función de la metodología comentada:

1. Servicios

- Procesos de negocio relacionados con la actividad de la empresa de topografía y geodesia.
- Servicio de atención al cliente.
- Servicio de gestión de proyectos.

2. Datos e información

- Datos e información relacionados con el trabajo de campo y la gestión de proyectos.
- Datos e información relacionados con la gestión de la empresa, como clientes, proveedores y empleados.
- Datos de clientes y proyectos.
    - Información relacionada con el personal o procesos, garantizando su accesibilidad en todo momento y evitando modificaciones no acreditadas.
- Información financiera de la empresa.

3. Aplicaciones de Software

- Aplicaciones de topografía y geodesia utilizadas en el trabajo de campo.
- Aplicaciones de planificación de recursos y de gestión de la producción.
- Aplicaciones de gestión de relaciones con clientes (CRM) utilizadas en la oficina.

4. Equipos informáticos

- Equipos de sobremesa o portátiles utilizados por los profesionales de campo, técnicos y administrativos.
    - Cada puesto de trabajo dispone de un equipo de sobremesa o portátil con monitor, teclado y ratón conectables a través de un concentrador.

5. Personal

- Personal interno de la empresa, incluyendo profesionales de campo, técnicos y administrativos.
    - Responsable de sistemas y telecomunicaciones.
    - Responsable de la información y de los servicios.
    - Responsable de línea de negocio.
    - Responsable de seguridad.
- Personal subcontratado que pueda tener acceso a la información de la empresa.
    - Responsable de asesoría legal.

6. Redes de comunicaciones

- Router doméstico que da acceso a Internet.
    - Proporcionado por el ISP que da servicio a las instalaciones, y con ausencia de firewall y proxy.
- Switch de 24 bocas sin gestión utilizado para distribuir el cable a los equipos.
- Red wifi protegida por clave WPA2.

- Arquitectura:
    - Arquitectura formada por una red interna, un switch de cabecera, un firewall y un modem profesional de fibra óptica simétrica con doble canal de respaldo.
- Tres servidores disponibles:
    - Windows Server 2016 y SQL Server 2014.
        - Windows Server 2016: contiene el servidor de correo, Exchange, y el Directorio Activo.
    - Ubuntu Server 18.04 LTS.
        - Contiene todas las aplicaciones internas que dan soporte a Operaciones y Gestión de Proyectos, desarrolladas en Java y Python, además de contener también el servidor Web.
    - NAS Synology.
        - En él se almacenan los diseños de los productos, los catálogos comerciales y las fotometrías.

7. Soportes de información

- Dispositivos de almacenamiento utilizados para guardar la información de la empresa.
- Servidores y sistema de almacenamiento en red (NAS) ubicados en la sala de servidores.
    - Dos servidores Blade y de almacenamiento tanto en disco dedicado como en NAS.

8. Equipamiento auxiliar

- Cerraduras electrónicas utilizadas para controlar el acceso a la empresa.
- Sistema de aire acondicionado estándar en toda la instalación.

9. Instalaciones

- Sede de la empresa con diferentes áreas de trabajo.
  - Dispone de una sede con unos 150 m2.
  - Oficina, área de trabajo, sala de servidores, almacén y zona de café/reuniones.

10. Intangibles

- Imagen y reputación de la empresa.
- Políticas y procedimientos de seguridad de la información.

2.1.1. Inventario de activos

[S]Servicios	
Código: S.1	Nombre: Procesos de negocio
Descripción: Los procesos de negocio relacionados con la actividad de la empresa de topografía y geodesia son el conjunto de actividades y tareas que se llevan a cabo en la empresa para desempeñar su actividad principal. Estos procesos pueden incluir, por ejemplo, la adquisición de datos en el campo o la elaboración de informes y diseños.	
Propietario: Responsable de la información y de los servicios	
Crítico: Sí	
Localización: Departamento comercial	
Código: S.2	Nombre: Servicio de atención al cliente
Descripción: El servicio de atención al cliente es el conjunto de actividades y tareas que se llevan a cabo en la empresa para brindar una respuesta eficiente y satisfactoria a las necesidades y demandas de los clientes. Este servicio puede incluir, por ejemplo, el atender y resolver las consultas y solicitudes de los clientes, brindar información sobre los productos y servicios de la empresa, y gestionar y solucionar posibles problemas o incidencias.	
Propietario: Responsable de la información y de los servicios	
Crítico: Sí	
Localización: Departamento comercial	
Código: S.3	Nombre: Servicio de gestión de proyectos
Descripción: El servicio relacionado con la gestión de proyectos es el conjunto de actividades y tareas que se llevan a cabo en la empresa para planificar, organizar y controlar los diferentes proyectos que se desarrollan. Este servicio puede incluir la definición de los objetivos y requisitos del proyecto, y la evaluación y mejora continua del mismo.	
Propietario: Comité de seguridad	
Crítico: Sí	
Localización: Oficina técnica	
Dependencias	
Activos: D1, D2, D3, D4	Grado: Alto
¿Por qué? Los procesos de negocio, el servicio de atención al cliente y el servicio de gestión de proyectos de la empresa dependen profundamente de la información y datos que se manipulan.	
Dependencias	
Activos: SW.1, SW.2, SW.3	Grado: Alto
¿Por qué? Estos activos son necesarios para llevar a cabo los procesos de negocio, el servicio de atención al cliente y el servicio de gestión de proyectos. La dependencia es alta ya que sin estas aplicaciones, estos procesos no podrían realizarse.	
Dependencias	
Activos: HW.1	Grado: Alto
¿Por qué? Estos activos son necesarios para acceder a los servidores y utilizar las aplicaciones	

[S]Servicios	
Código: S.1	Nombre: Procesos de negocio
Descripción: Los procesos de negocio relacionados con la actividad de la empresa de topografía y geodesia son el conjunto de actividades y tareas que se llevan a cabo en la empresa para desempeñar su actividad principal. Estos procesos pueden incluir, por ejemplo, la adquisición de datos en el campo o la elaboración de informes y diseños.	
Propietario: Responsable de la información y de los servicios	
de software que se utilizan en los procesos de negocio, el servicio de atención al cliente y el servicio de gestión de proyectos.	
Dependencias	
Activos: COM.1, COM.2, COM.3, COM.4, COM.5	Grado: Alto
¿Por qué? Estos activos son necesarios para conectar los equipos informáticos a los servidores y permitir el acceso a la información necesaria para realizar los procesos en cuestión. La dependencia es alta ya que, sin una red de comunicaciones adecuada, estos procesos no podrían realizarse.	
Dependencias	
Activos: Media.1, Media.2	Grado: Alto
¿Por qué? Los procesos de negocio, el servicio de atención al cliente y el servicio de gestión de proyectos dependen de los servidores ya que son los encargados de almacenar y procesar la información necesaria para realizar estos procesos. La dependencia es alta ya que, sin estos servidores, los procesos no podrían realizarse.	

[D]Datos e información	
Código: D.1	Nombre: Datos e información relacionados con el trabajo de campo y gestión de proyectos
Descripción: Conjunto de datos e información que se generan y utilizan en la empresa para llevar a cabo el trabajo de campo y la gestión de proyectos. Estos datos pueden incluir información sobre los equipos y herramientas utilizadas en el trabajo de campo, los resultados de las mediciones y análisis realizados, la información de los clientes y proyectos, y los datos de gestión de la empresa relacionados con la producción y la planificación.	
Propietario: Responsable de la información y los servicios	
Crítico: Sí	
Localización: Departamento de operaciones	
Código: D.2	Nombre: Datos e información relacionados con la gestión de la empresa.
Descripción: Conjunto de datos e información que se utilizan para llevar a cabo las actividades de gestión de la empresa, como la gestión de clientes, proveedores y empleados. Estos datos pueden incluir, por ejemplo, información sobre los clientes y sus preferencias, los proveedores y sus condiciones comerciales y los empleados y sus habilidades y competencias.	
Propietario: Dirección general	
Crítico: Sí	
Localización: Departamento de administración	
Código: D.3	Nombre: Datos de clientes y proyectos
Descripción: Los datos de clientes y proyectos son el conjunto de datos e información que se utilizan para gestionar y desarrollar los proyectos de los clientes. Estos datos pueden incluir, por ejemplo, información sobre los requisitos y objetivos del proyecto, los plazos y presupuestos y los resultados y entregables del proyecto.	
Propietario: Responsables de la información y los servicios	
Crítico: Sí	
Localización: Departamento de administración	

Código: D.4	Nombre: Información financiera de la empresa.
Descripción: La información financiera de la empresa es el conjunto de datos e información relacionados con las finanzas de la empresa. Esta información puede incluir, por ejemplo, el balance general, el estado de resultados, el estado de flujos de efectivo y el informe de gestión. Además, es necesaria para cumplir con las obligaciones fiscales y contables de la empresa.	
Propietario: Responsables de la información y los servicios	
Crítico: Sí	
Localización: Departamento de la información	
Dependencias	
Activos: COM.5, Media.1, Media.2	Grado: Alto
¿Por qué? Los datos e información mencionados dependen de los servidores ya que son los encargados de almacenar y procesar esta información. La dependencia es alta ya que sin servidores, estos datos y esta información no estarían disponibles.	
Dependencias	
Activos: SW.1, SW.2, SW.3	Grado: Alto
¿Por qué? Estos activos son necesarios para acceder a los datos e información mencionados y utilizarlos en los procesos de negocio y en la gestión de la empresa. La dependencia es alta ya que, sin aplicaciones de software adecuadas, estos datos e información no podrían utilizarse.	
Dependencias	
Activos: COM.1, COM.2, COM.3, COM.4	Grado: Alto
¿Por qué? Estos activos son necesarios para conectar los equipos informáticos a los servidores y permitir el acceso a los datos e información mencionados.	
Dependencias	
Activos: P1	Grado: Alto
¿Por qué? Los datos e información mencionados dependen del personal interno ya que son las personas encargadas de generar, procesar y utilizar esta información en los procesos de negocio y en la gestión de la empresa. La dependencia es alta ya que sin personal capacitado y con acceso autorizado, estos datos no podrían utilizarse adecuadamente.	

[SW]Software	
Código: SW.1	Nombre: Aplicaciones de topografía y geodesia
Descripción: Herramientas informáticas que se utilizan en el trabajo de campo de la empresa. Estas aplicaciones pueden incluir programas de medición y análisis de datos, herramientas de dibujo y diseño y programas de gestión de proyectos.	
Propietario: Responsable de sistemas y telecomunicaciones	
Crítico: Sí	
Localización: Departamento de operaciones	
Código: SW.2	Nombre: Aplicaciones de planificación de recursos y de gestión de la producción.
Descripción: Herramientas informáticas que se utilizan para gestionar y planificar los recursos y la producción de la empresa. Felicidades. Pueden incluir, por ejemplo, programas de gestión de proyectos, herramientas de seguimiento y control de la producción y programas de gestión de Recursos Humanos.	
Propietario: Responsable de sistemas y telecomunicaciones	
Crítico: Sí	
Localización: Departamento de operaciones	
Código: SW.3	Nombre: Aplicaciones de gestión de relaciones con clientes (CRM) utilizadas en la oficina.
Descripción: Herramientas informáticas que se utilizan para gestionar las relaciones con los	

clientes de la empresa. Estas aplicaciones pueden incluir programas de gestión de clientes, herramientas de seguimiento y análisis de la satisfacción del cliente y programas de gestión de la relación con el cliente.
Propietario: Responsable de sistemas y telecomunicaciones
Crítico: Sí
Localización: Departamento de operaciones
Dependencias
Activos: COM.3 | Grado: Alto
¿Por qué? Las aplicaciones de software necesitan acceder a Internet para funcionar correctamente.
Dependencias
Activos: COM.5 | Grado: Alto
¿Por qué? Las aplicaciones de software se ejecutan en los servidores y requieren de ellos para funcionar.
Dependencias
Activos: HW.1 | Grado: Media
¿Por qué? Las aplicaciones de software se utilizan en los equipos informáticos para ser ejecutadas y realizar su trabajo.
Dependencias
Activos: P.1 | Grado: Medio
¿Por qué? El personal interno utiliza las aplicaciones de software para llevar a cabo su trabajo, pero algunas aplicaciones pueden funcionar sin la presencia del personal.

[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.	

[P]Personal	
Código: P.1	Nombre: Personal interno de la empresa,
Descripción: El personal interno de la empresa incluye a los profesionales del campo, técnicos y administrativos que trabajan en la empresa. Además, hay varios responsables que se encargan de diferentes áreas de la empresa, como el responsable de sistemas y telecomunicaciones, el	

responsable de la información y de los servicios, el responsable de líneas de negocio y el responsable de seguridad.	
Propietario: Dirección general	
Crítico: Sí	
Localización: Departamento de administración	
Dependencias	
Activos: HW.1	Grado: Alta
¿Por qué? Debido a que el personal interno necesita de equipos informáticos para llevar a cabo su trabajo, y además estos equipos pueden mejorar su rendimiento y capacidad.	
Dependencias	
Activos: COM.1, COM.2, COM.3, COM.4, COM.5	Grado: Alta
¿Por qué? El personal interno puede necesitar acceder a la red para realizar sus tareas o comunicarse con otros trabajadores.	
Dependencias	
Activos: L.1	Grado: Media
¿Por qué? Dependencia media con las instalaciones, como despachos o áreas de trabajo, ya que el personal interno necesita un lugar adecuado donde realizar sus labores.	
Código: P.2	Nombre: Personal subcontratado que pueda tener acceso a la información de la empresa.
Descripción: El personal subcontratado es aquel que no forma parte de la plantilla de la empresa, pero que puede tener acceso a la información de la empresa. Esto puede incluir, por ejemplo, a proveedores, consultores externos o personal de limpieza o mantenimiento. Es importante garantizar que estas personas sólo tengan acceso a la información que necesitan para realizar su trabajo, y que se les apliquen las medidas de seguridad adecuadas para proteger la información de la empresa.	
Propietario: Dirección general	
Crítico: Sí	
Localización: Departamento de administración	
Dependencias	
Activos: In.2	Grado: Alta
¿Por qué? Estas políticas establecen las normas y regulaciones que deben seguirse para proteger la información de la empresa, y deben ser comprendidas y seguidas por todo el personal subcontratado que tenga acceso a la información de la empresa.	

[COM]Redes de Comunicaciones	
Código: COM.1	Nombre: Router doméstico que da acceso a Internet.
Descripción: Dispositivo que se utiliza para conectar las instalaciones de la empresa. Este router es proporcionado por el ISP que da servicio a las instalaciones y no cuenta con un firewall ni un proxy, lo que puede representar un riesgo para la seguridad en la red. Es importante considerar la posibilidad de implementar un firewall y un proxy para proteger la red y evitar posibles ataques externos.	
Propietario: Responsable de sistemas y telecomunicaciones	
Crítico: Sí	
Localización: Oficina técnica	
Código: COM.2	Nombre: Switch de 24 bocas
Descripción: El Switch de 24 bocas es un dispositivo de red que se utiliza para conectar los equipos de la empresa. Se conecta a la red interna y se utiliza para distribuir el cable a los diferentes equipos, lo que permite a estos equipos comunicarse entre sí y acceder a los recursos compartidos de la red. Sin embargo, el switch no está gestionado, lo que significa que no se puede controlar de manera centralizada. Esto puede representar un riesgo para la seguridad y el correcto funcionamiento de la red. Es importante considerar la posibilidad de implementar	

un switch gestionado para mejorar la gestión y seguridad de la red.	
Propietario: Responsable de sistemas y telecomunicaciones	
Crítico: Sí	
Localización: Oficina técnica	
Código: COM.3	Nombre: Red wifi protegida por clave WPA2.
Descripción: La red wifi es una red inalámbrica que permite a los dispositivos conectarse a Internet y a la red interna de la empresa sin necesidad de cables. La red wifi está protegida por una clave WPA2, que es un estándar de seguridad utilizado en redes wifi para proteger la comunicación entre dispositivos y habilitar accesos no autorizados. La utilización de una clave WPA2 protege la red wifi de posibles ataques externos, pero es importante garantizar que la clave utilizada sea segura y no sea fácilmente adivinable. Además, es recomendable actualizar la clave de forma regular para evitar que sea descubierta por posibles atacantes.	
Propietario: Responsable de sistemas y telecomunicaciones	
Crítico: Sí	
Localización: Oficina técnica	
Dependencias	
Activos: In.2	Grado: Alta
¿Por qué? Estas políticas establecen las normas y regulaciones que deben seguirse para proteger la información de la empresa, y deben ser comprendidas y seguidas por todo el personal subcontratado que tenga acceso a la información de la empresa.	
Código: COM.4	Nombre: Arquitectura
Descripción: La arquitectura del sistema se compone de diferentes elementos que trabajan en conjunto para proporcionar acceso a Internet y a la red interna de la empresa. La red interna permite a los diferentes equipos de la empresa comunicarse entre sí y acceder a los recursos compartidos de la red. El switch de cabecera se encarga de distribuir el tráfico de la red entre los diferentes equipos, permitiendo una comunicación fluida y rápida. El firewall protege la red interna de posibles ataques externos filtrando el tráfico entrante y permitiendo solamente el tráfico utilizado. Por último, el módem de fibra óptica simétrica proporciona una conexión de alta velocidad y fiabilidad, permitiendo a los equipos de la empresa acceder a Internet y a los recursos en línea. La arquitectura está diseñada para proporcionar un buen rendimiento y seguridad en la red de la empresa.	
Propietario: Responsable de sistemas y telecomunicaciones	
Crítico: Si	
Localización: Oficina técnica	
Dependencias	
Activos: COM.4	Grado: Alta
¿Por qué? Las principales dependencias del sistema de arquitectura son el switch de cabecera, el firewall y el módem de fibra óptica simétrica. El grado de dependencia es alto ya que estos elementos son fundamentales para el correcto funcionamiento de la red interna de la empresa y su ausencia puede afectar la composición y acceso a los recursos de la red.	
Código: COM.5	Nombre: Servidores disponibles
Descripción: Los servidores son equipos informáticos que proporcionan servicios y recursos a los diferentes equipos de la red interna de la empresa. La empresa cuenta con tres servidores diferentes, cada uno con funcionalidades y usos distintos. El primer servidor utiliza Windows Server 2016 y SQL Server 2014 y se utiliza principalmente para almacenar y gestionar el correo electrónico de la empresa. El segundo servidor utiliza Ubuntu Server 18.04 LTS y aloja todas las aplicaciones internas que se utilizan en las operaciones y en la gestión de proyectos de la empresa. Por último, el tercer servidor es un Synology que se utiliza para almacenar y gestionar archivos importantes de la empresa. Todos estos servidores son cruciales para el funcionamiento adecuado de la empresa.	
Propietario: Responsable de sistemas y telecomunicaciones	
Crítico: Sí	

Localización: Sala CPD	
Dependencias	
Activos: Media.1, Media.2	Grado: Media
¿Por qué? Los servidores almacenan información importante de la empresa, por lo que es importante contar con soportes de almacenamiento seguros y confiables para asegurar la disponibilidad y seguridad de esta información.	
Dependencias	
Activos: COM.4	Grado: Media
¿Por qué? Los servidores necesitan estar conectados a la red interna para poder ofrecer sus servicios y recursos a los equipos de la empresa.	

[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.	

[AUX]Equipamiento auxiliar	
Código: AUX.1	Nombre: Cerraduras electrónicas
Descripción: Las cerraduras electrónicas son dispositivos utilizados para controlar el acceso a la empresa y garantizar que solo las personas autorizadas puedan entrar. Estas cerraduras pueden ser activadas a través de una aplicación móvil y ofrecen una mayor seguridad que las cerraduras tradicionales.	
Propietario: Responsable de seguridad	

Crítico: No	
Localización: Puerta de acceso a la empresa, almacén, y sala máquinas	
Dependencias	
Activos: SW.2	Grado: Alto
¿Por qué? Depende del software de gestión de accesos que se utiliza para controlar el acceso a la empresa y autorizar el acceso a cada usuario.	
Dependencias	
Activos: COM.3	Grado: Alto
¿Por qué? Depende de la red wifi de la empresa para comunicarse y enviar y recibir información.	
Dependencias	
Activos: P.1	Grado: Medio
¿Por qué? Depende del personal interno de la empresa que utiliza las cerraduras y puede requerir soporte en caso de problemas o dificultades.	
Código: AUX.2	Nombre: Sistema de aire acondicionado
Descripción: El sistema de aire acondicionado estándar es un sistema de climatización que se utiliza en toda la instalación de la empresa. Proporciona una temperatura agradable y una buena calidad del aire en todas las instalaciones, lo que contribuye a mejorar el confort y la productividad del personal.	
Propietario: Responsable de la información y de los servicios	
Crítico: No	
Localización: Toda la instalación	
Dependencias	
Activos: L.1	Grado: Alto
¿Por qué? El sistema de aire acondicionado se utiliza en toda la instalación de la empresa, por lo que su funcionamiento es crucial para el confort y la productividad del personal en el trabajo.	
Dependencias	
Activos: P.2	Grado: Alto
¿Por qué? El sistema de aire acondicionado requiere de un mantenimiento regular para garantizar su correcto funcionamiento y prolongar su vida útil.	

[L]Instalaciones	
Código: L.1	Nombre: Sede de la empresa
Descripción: La sede de la empresa es un espacio físico con diferentes áreas de trabajo, como una oficina, un área de trabajo, una sala de servidores, un almacén y una zona de café/reuniones. Tiene un tamaño aproximado de 150 m2.	
Propietario: Dirección general	
Crítico: Sí	
Localización: Todas las instalaciones	
Dependencias	
Activos: P.2	Grado: Medio
¿Por qué? Depende de la contratación de un servicio de limpieza y mantenimiento para garantizar que el espacio esté en buenas condiciones y se mantenga limpio y ordenado.	

[In]Intangibles	
Código: In.1	Nombre: Imagen y reputación de la empresa.
Descripción: La imagen y reputación de la empresa se refiere a la percepción que tienen los clientes, proveedores y otros interesados sobre la empresa. La buena reputación de una empresa puede ser un factor importante en su éxito, ya que puede ayudar a ganar confianza y credibilidad en el mercado. Por otro lado, una mala reputación puede perjudicar a la empresa y afectar su rentabilidad y desempeño en el mercado.	
Propietario: Responsables de la información y de los servicios	

Crítico: Sí	
Localización: Departamento comercial	
Dependencias	
Activos: S.1, S.2, S.3	Grado: Alto
¿Por qué? Los clientes son cruciales para la imagen y reputación de la empresa, ya que su satisfacción y fidelización pueden influir en la percepción que tienen otros potenciales clientes de la empresa. Además, la calidad de los productos o servicios ofrecidos es fundamental para mantener una buena reputación y evitar problemas que puedan dañar la imagen de la empresa.	
Dependencias	
Activos: P.1, P.2	Grado: Alto
¿Por qué? Los empleados también son importantes, ya que su comportamiento y actitud pueden afectar la imagen de la empresa.	
Código: In.2	Nombre: Políticas y procedimientos de seguridad de la información.
Descripción: Los activos de información valiosos se refieren a las políticas y procedimientos que se han establecido en la empresa para proteger la información y garantizar su confidencialidad, integridad y disponibilidad. Estos activos incluyen las normas y medidas de seguridad que se han establecido para el acceso y uso de la información, la protección física y lógica de los sistemas y la formación y concienciación del personal sobre las medidas de seguridad. Estos activos son esenciales para garantizar la seguridad de la información y evitar cualquier tipo de amenaza o ataque que puedan afectar a la empresa.	
Propietario: Dirección general	
Crítico: Sí	
Localización: Departamento de administración	
Dependencias	
Activos: P.1, P.2	Grado: Alta
¿Por qué? El personal de la empresa es responsable de cumplir con las políticas y procedimientos de seguridad de la información, por lo que su cumplimiento es fundamental para garantizar la seguridad de la información.	
Dependencias	
Activos: COM.5, Media.1, Media.2	Grado: Alta
¿Por qué? Estos activos almacenan y gestionan la información de la empresa, por lo que es fundamental que se cumplan las políticas y procedimientos de seguridad para proteger esta información y evitar posibles pérdidas o daños.	
Dependencias	
Activos: SW.1, SW.2, SW.3	Grado: Alta
¿Por qué? Las aplicaciones de la empresa utilizan y gestionan la información, por lo que es importante que se cumplan las políticas y procedimientos de seguridad para proteger la información y garantizar su integridad y confidencialidad.	

2.1.2. Valoración de activos

No todos los activos tienen la misma importancia para la organización, ni generan los mismos problemas si son atacados. Por ello, procedemos a realizar una valoración de los activos que hemos considerado en función de la relevancia que tengan para el negocio y del impacto que una incidencia sobre el mismo pueda causar a la entidad.
Para ello utilizaremos una **valoración cualitativa** con los siguientes valores: Alto, Medio y Bajo.

Activos de alta importancia

Procesos de negocio relacionados con la actividad de la empresa de topografía y geodesia: alta importancia, ya que son los procesos que permiten a la empresa realizar su actividad principal y generar ingresos.

Servicio de gestión de proyectos: alta importancia, ya 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.

Datos e información relacionados con el trabajo de campo y la gestión de proyectos: Los datos e información relacionados con el trabajo de campo y la gestión de proyectos son de alta importancia para la empresa de topografía y geodesia, ya que son los datos y la información que permiten realizar su actividad principal y cumplir con sus objetivos. Estos datos e información incluyen información sobre los proyectos en los que está trabajando la empresa, los datos recogidos en el trabajo de campo, los diseños y planos de los proyectos, y cualquier otra información relevante para la correcta ejecución de los proyectos.

Datos de clientes y proyectos: Los datos de clientes y proyectos son de alta importancia para la empresa de topografía y geodesia, 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.

Información financiera de la empresa: La información financiera de la empresa es de alta importancia para la empresa de topografía y geodesia, ya que es esencial para la correcta gestión de la empresa y para tomar decisiones adecuadas. La información financiera incluye datos como los ingresos y gastos de la empresa, el balance general, el estado de resultados y otros datos relevantes para la gestión financiera de la empresa.

Aplicaciones de topografía y geodesia utilizadas en el trabajo de campo: Las aplicaciones de topografía y geodesia utilizadas en el trabajo de campo son de alta importancia para la empresa, ya que son esenciales para la realización de su actividad principal y para cumplir con sus objetivos. Estas aplicaciones incluyen programas de diseño, cálculo y análisis utilizados en el trabajo de campo, así como otras aplicaciones específicas para la topografía y la geodesia.

Personal interno de la empresa, incluyendo profesionales de campo, técnicos y administrativos: El personal interno de la empresa, incluyendo profesionales de campo, técnicos y administrativos, es de alta importancia para la empresa de topografía y geodesia, ya que son esenciales para la realización de su actividad principal y para cumplir con sus objetivos. Los empleados de la empresa son los responsables de llevar a cabo las tareas relacionadas con la topografía y la geodesia, así como de realizar las tareas administrativas necesarias para el correcto funcionamiento de la empresa.

Red wifi protegida: La red wifi es de alta importancia para la empresa, ya que permite a los usuarios conectarse a la red de forma inalámbrica. En la actualidad, es fundamental contar con una red wifi de alta calidad para ofrecer una buena experiencia de usuario y una conexión estable y segura. Además, la red wifi también puede ser utilizada por los profesionales de campo para acceder a la información y aplicaciones de la empresa de forma remota. Por lo tanto, se podría valorar la importancia de la red wifi como alta, ya que es un componente clave para la conectividad de la empresa y para la productividad de los usuarios.

Arquitectura: La arquitectura del sistema es de alta importancia para la empresa, ya que es el diseño y la estructura que define la forma en que se organizan y se conectan los diferentes componentes del sistema. Una buena arquitectura de sistema permite que la empresa tenga un funcionamiento eficiente y seguro, con un buen rendimiento y una adecuada gestión de la información.

Dispositivos de almacenamiento utilizados para guardar la información de la empresa: Los dispositivos de almacenamiento utilizados para guardar la información de la empresa son de alta importancia para la empresa de topografía y geodesia, ya que son esenciales para la correcta gestión y protección de la información de la empresa. Los dispositivos de almacenamiento, como discos duros, discos externos, servidores y NAS, son utilizados para guardar la información de la empresa y permiten que esta información esté disponible en todo momento y en caso de necesidad.

Imagen y reputación de la empresa: La imagen y reputación de la empresa son activos de alta importancia para la empresa. Una buena imagen y reputación pueden ayudar a atraer y retener a clientes, mejorar las relaciones con los proveedores y empleados, y aumentar la confianza de los inversores y otros grupos de interés. Por otro lado, una mala imagen y reputación pueden afectar negativamente el negocio y la reputación de la empresa, y causar pérdidas financieras. Por lo tanto, es importante proteger y cuidar la imagen y reputación de la empresa.

Políticas y procedimientos de seguridad de la información: La política y los procedimientos de seguridad de la información son un activo de alto valor para la empresa. Estos son esenciales para garantizar la confidencialidad, integridad y disponibilidad de la información, lo que puede tener un impacto directo en la imagen y reputación de la empresa. Además, una política y procedimientos de seguridad bien diseñados y ejecutados pueden ayudar a reducir el riesgo de sufrir ataques informáticos y otros tipos de amenazas que pueden afectar el funcionamiento de la empresa y su rentabilidad.

Activos de media importancia

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.

Datos e información relacionados con la gestión de la empresa: Los datos e información relacionados con la gestión de la empresa son de media importancia para la empresa de topografía y geodesia, ya que, aunque son importantes para el correcto funcionamiento de la empresa y para tomar decisiones adecuadas, no son esenciales para la actividad principal de esta. Estos datos e información incluyen información sobre los clientes, proveedores y empleados de la empresa, así como información financiera y de otro tipo que se utiliza en la gestión de la empresa.

Aplicaciones de planificación de recursos y de gestión de la producción: Las aplicaciones de planificación de recursos y de gestión de la producción son de media importancia para la empresa de topografía y geodesia, ya que, aunque son importantes para el correcto funcionamiento de la empresa y para maximizar su eficiencia, no son esenciales para la realización de su actividad principal. Estas aplicaciones incluyen programas utilizados para planificar el uso de los recursos de la empresa, como el tiempo y los recursos materiales, así como programas utilizados para gestionar la producción, como el seguimiento de los proyectos y la monitorización de su avance. Por lo tanto, se podría valorar la importancia de estas aplicaciones como media, ya que son importantes para la gestión de la empresa, pero no son esenciales para la realización de su actividad principal.

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. Estos equipos incluyen computadoras de escritorio o portátiles, así como otros dispositivos como monitores, teclados y ratones, que son utilizados por los trabajadores para realizar sus tareas diarias.

Router doméstico: El router doméstico es de mediana importancia para la empresa, ya que es un componente fundamental para la conexión a Internet de la empresa. El router es el dispositivo que se encarga de gestionar la conexión a Internet y de distribuirla a todos los dispositivos de la empresa. Sin embargo, en el caso de la empresa, este router es un dispositivo doméstico y no cuenta con un firewall o un proxy, lo que puede suponer un riesgo en términos de seguridad. Por lo tanto, se podría valorar la importancia del router como mediana, ya que es esencial para la conexión a Internet de la empresa, pero no cuenta con las medidas de seguridad adecuadas.

Switch de 24 bocas: El switch de 24 bocas es de mediana importancia para la empresa de topografía y geodesia, ya que es un componente fundamental para la conexión de los equipos de la empresa. El switch es el dispositivo que se encarga de distribuir la señal de red a todos los equipos de la empresa, permitiendo la comunicación entre ellos. Sin embargo, en el caso de la empresa de topografía y geodesia, se menciona que el switch no cuenta con gestión, lo que puede suponer un riesgo en términos de gestión y seguridad de la red.

Sede de la empresa: La sede de la empresa es de importancia media, ya que es el lugar físico donde se desarrolla la actividad de la empresa y donde se almacenan y gestionan los datos e información importantes. Sin embargo, en el caso de la empresa, no se menciona ninguna característica especial o particular de la sede que pueda influir en la importancia de esta para la empresa. Por lo tanto, se podría valorar la importancia de la sede de la empresa como media, ya que es un elemento necesario para el funcionamiento de la empresa, pero no tiene una influencia determinante en su actividad.

Activos de baja importancia

Personal subcontratado que pueda tener acceso a la información de la empresa: El personal subcontratado que pueda tener acceso a la información de la empresa es de baja importancia para la empresa, ya que, aunque pueden tener acceso a algunos datos y documentos de la empresa, no son esenciales para la realización de su actividad principal. Los empleados subcontratados suelen ser contratados para realizar tareas específicas y temporalmente, y por lo general no tienen acceso a toda la información de la empresa.

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.

2.2. Listado de amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. **Amenaza**: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008].

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.

En la siguiente tabla se muestran las medidas utilizadas para medir el nivel de probabilidad de que ocurra la amenaza y el nivel de impacto de dicha amenaza sobre los activos en cuestión.

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

Por último, antes de mostrar el listado de amenazas, se incluye una tabla en donde se muestran las categorías de las amenazas utilizadas y sus respectivas descripciones.

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.

[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

[N.2] Daños por agua					
Descripción: inundaciones: posibilidad de que el agua acabe con los recursos del sistema.					
Probabilidad: Baja Las inundaciones son eventos relativamente infrecuentes en un entorno de oficinas y se pueden tomar medidas preventivas para minimizar el riesgo de inundaciones.					
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

[N.*] Desastres naturales					
Descripción: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ...					
Probabilidad: Baja La probabilidad de que ocurra un desastre natural en el sistema dependerá de la ubicación de la sede de la empresa y de la frecuencia de desastres naturales en la zona. Sin embargo, en general, se puede considerar que la probabilidad de que ocurra un desastre natural en el sistema es baja, ya que los desastres naturales son eventos relativamente infrecuentes en un entorno de oficinas y se pueden tomar medidas preventivas para minimizar el riesgo de desastres naturales.					
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

[I.5] Avería de origen físico o lógico					
Descripción: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.					
Probabilidad: Media La probabilidad de que ocurra una avería de origen físico o lógico en el sistema es media, ya que es normal que los equipos y los programas experimenten fallos o errores durante su uso.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
HW.1 - Equipos de sobremesa o portátiles	B	M	M	-	B
Media.1-Dispositivos de almacenamiento	B	M	M	-	B
Media.2 - Servidores y sistemas de almacenamiento	B	M	M	-	B
AUX.1 – Cerraduras electrónicas	-	-	A	-	M
AUX.2 – Aire acondicionado	-	-	A	-	M
SW.1 – Aplicaciones de topografía y geodesia.	B	B	M	-	B
SW.2 - Aplicaciones de planificación de recursos y de gestión de la producción.	B	B	M	-	B
SW.3 - Aplicaciones de gestión de relaciones con clientes.	B	B	M	-	B

[I.6] Corte del suministro eléctrico					
Descripción: cese de la alimentación de potencia					
Probabilidad: Baja En general, se puede considerar que la probabilidad de que ocurra un corte del suministro eléctrico en el sistema es baja, ya que en la mayoría de las zonas el suministro eléctrico suele ser fiable y no suele haber cortes frecuentes.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
HW.1 - Equipos de sobremesa o portátiles	-	A	A	-	M
Media.1- Dispositivos de almacenamiento	-	A	A	-	M
Media.2 - Servidores y sistemas de almacenamiento	-	A	A	-	M
AUX.1 – Cerraduras electrónicas	-	-	A	-	M
AUX.2 – Aire acondicionado	-	-	A	-	M

[I.7] Condiciones inadecuadas de temperatura o humedad					
Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...					
Probabilidad: Media En general, se podría considerar como una amenaza de probabilidad media, ya que es un problema que puede ocurrir en cualquier lugar y en cualquier momento, y puede causar daños significativos en los equipos y la información.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
HW.1 - Equipos de sobremesa o portátiles	-	A	A	-	B
Media.1- Dispositivos de almacenamiento	-	A	A	-	B
Media.2 - Servidores y sistemas de almacenamiento	-	A	A	-	B
AUX.1 – Cerraduras electrónicas	-	-	M	-	B
AUX.2 – Aire acondicionado	-	-	A	-	B

[I.8] Fallo de servicios de comunicaciones					
Descripción: cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.					
Probabilidad: Media Probabilidad media de esta amenaza ya que, aunque no es muy común, no es completamente improbable que ocurra un fallo en los servicios de comunicaciones.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
COM.1 - Router doméstico que da acceso a Internet.	-	A	A	-	M
COM.2 - Switch de 24 bocas sin gestión utilizado para distribuir el cable a los equipos.	–	A	A	–	M
COM.3 - Red wifi protegida por clave WPA2.	-	A	A	-	M
COM.4 - Arquitectura	-	A	A	-	M
COM.5 - Servidores disponibles: Windows Server 2016 y SQL Server 2014, Ubuntu Server 18.04 LTS y NAS Synology.	-	A	A	-	M

[I.10] Degradación de los soportes de almacenamiento de la información					
Descripción: como consecuencia del paso del tiempo					
Probabilidad: Baja La probabilidad de que ocurra esta amenaza en el sistema es baja, ya que la degradación de los soportes de almacenamiento de la información suele ser un proceso lento y gradual. Sin embargo, dependiendo de las condiciones de almacenamiento y de la calidad de los soportes utilizados, la probabilidad de esta amenaza puede variar. Por lo tanto, es importante tener en cuenta las condiciones de almacenamiento y utilizar soportes de calidad para minimizar la probabilidad de esta amenaza.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
Media.1- Dispositivos de almacenamiento	-	M	M	-	B
Media.2 - Servidores y sistemas de almacenamiento	-	M	M	-	B

[E.1] Errores de los usuarios					
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc.					
Probabilidad: Alta En general, se puede decir que la probabilidad de que ocurra esta amenaza es alta, ya que es común que los usuarios comentan errores al usar un sistema, incluso si han recibido una buena formación y el sistema es sencillo de usar.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
S.1 - Procesos de negocio relacionados con la actividad de la empresa de topografía y geodesia.	-	B	B	-	B
S.2 – Servicio de atención al cliente.	-	B	B	-	B
S.3 - Servicio de gestión de proyectos.	-	B	B	-	B
Media.1- Dispositivos de almacenamiento	-	B	B	-	B
Media.2 - Servidores y sistemas de almacenamiento	-	B	B	-	B
D.1 - Datos e información relacionados con el trabajo de campo y la gestión de proyectos.	-	B	B	-	B
D.2 - Datos e información relacionados con la gestión de la empresa, como clientes, proveedores y empleados.	-	B	B	-	B
D.3 - Datos de clientes y proyectos.	-	B	B	-	B
D.4 - Información financiera de la empresa.	-	B	B	-	B
SW.1 – Aplicaciones de topografía y geodesia.	-	B	B	-	B
SW.2 - Aplicaciones de planificación de recursos y de gestión de la producción.	-	B	B	-	B
SW.3 - Aplicaciones de gestión de relaciones con clientes.	-	B	B	-	B

[E.2] Errores del administrador.					
Descripción: equivocaciones de personas con responsabilidades de instalación y operación					
Probabilidad: Media Depende de varios factores, como la capacitación y experiencia del administrador, la complejidad del sistema y la disponibilidad de recursos para supervisar y monitorear el sistema. En general, se podría considerar que la probabilidad de ocurrencia de esta amenaza es media.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
S.1 - Procesos de negocio relacionados con la actividad de la empresa de topografía y geodesia.	M	A	-	-	M
S.2 – Servicio de atención al cliente.	M	A	-	-	M
S.3 - Servicio de gestión de proyectos.	M	A	-	-	M
Media.1- Dispositivos de almacenamiento	A	A	A	-	M
Media.2 - Servidores y sistemas de almacenamiento	A	A	A	-	M
D.1 - Datos e información relacionados con el trabajo de campo y la gestión de proyectos.	A	A	A	–	M
D.2 - Datos e información relacionados con la gestión de la empresa, como clientes, proveedores y empleados.	A	A	A	-	M
D.3 - Datos de clientes y proyectos.	A	A	A	-	M
D.4 - Información financiera de la empresa.	A	A	A	-	M
SW.1 – Aplicaciones de topografía y geodesia.	M	A	A	-	M
SW.2 - Aplicaciones de planificación de recursos y de gestión de la producción.	M	A	A	-	M
SW.3 - Aplicaciones de gestión de relaciones con clientes.	M	A	A	-	M
COM.1 - Router doméstico que da acceso a Internet.	B	A	A	-	M
COM.2 - Switch de 24 bocas sin gestión utilizado para distribuir el cable a los equipos.	B	A	A	-	M
COM.3 - Red wifi protegida por clave WPA2.	B	A	A	-	M
COM.4 - Arquitectura	B	A	A	-	M
HW.1 - Equipos de sobremesa o portátiles	B	M	M	-	M

[E.7] Deficiencias en la organización					
Descripción: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.					
Probabilidad: Media En muchas ocasiones y más si se trata de una empresa de un tamaño medio considerable, es difícil ponerse de acuerdo o coordinarse en ciertos aspectos.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
P.1 - Personal interno de la empresa, incluyendo profesionales de campo, técnicos y administrativos.	-	M	M	-	B
P.2 - Personal subcontratado que pueda tener acceso a la información de la empresa.	-	B	B	-	B

[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

[E.9] Errores de [re-]encaminamiento					
Descripción: envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.					
Probabilidad: Baja En general, se puede decir que la probabilidad de que ocurra esta amenaza puede ser baja si se tienen medidas de seguridad adecuadas en el sistema y se lleva a cabo una gestión adecuada de las comunicaciones en la red. Sin embargo, si estas medidas no están en su lugar o no se llevan a cabo de manera adecuada, la probabilidad de que ocurra esta amenaza puede ser más alta.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
S.1 - Procesos de negocio relacionados con la actividad de la empresa de topografía y geodesia.	A	B	-	B	B
S.2 – Servicio de atención al cliente.	A	B	-	B	B
S.3 - Servicio de gestión de proyectos.	A	B	-	B	B
SW.1 – Aplicaciones de topografía y geodesia.	M	M	B	-	B
SW.2 - Aplicaciones de planificación de recursos y de gestión de la producción.	M	M	B	-	B
SW.3 - Aplicaciones de gestión de relaciones con clientes.	M	M	B	-	B
COM.1 - Router doméstico que da acceso a Internet.	B	M	B	-	B
COM.2 - Switch de 24 bocas sin gestión utilizado para distribuir el cable a los equipos.	B	M	B	-	B
COM.3 - Red wifi protegida por clave WPA2.	M	M	B	-	B
COM.4 - Arquitectura	B	M	B	-	B

[E.20] Vulnerabilidades de los programas (software).					
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.					
Probabilidad: Media En general, todos los sistemas informáticos tienen vulnerabilidades y es importante estar constantemente buscando y corrigiendo estos defectos para minimizar el riesgo de ser afectado por ellos. Por lo tanto, es posible que la probabilidad de que ocurra esta amenaza sea Media o Alta, dependiendo de la complejidad del sistema y de la cantidad de esfuerzo que se dedique a buscar y corregir vulnerabilidades.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
SW.1 – Aplicaciones de topografía y geodesia.	A	A	M	B	B
SW.2 - Aplicaciones de planificación de recursos y de gestión de la producción.	A	A	M	B	B
SW.3 - Aplicaciones de gestión de relaciones con clientes.	A	A	M	B	B

[E.21] Errores de mantenimiento / actualización de programas (software)					
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.					
Probabilidad: Media La probabilidad de que esta amenaza se materialice dependerá de factores como la calidad del software, la frecuencia y eficacia de las actualizaciones, y la habilidad y cuidado del personal encargado del mantenimiento. En general, es importante tener buenas prácticas de mantenimiento y actualización de software para minimizar el riesgo de errores.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
SW.1 – Aplicaciones de topografía y geodesia.	B	A	M	B	B
SW.2 - Aplicaciones de planificación de recursos y de gestión de la producción.	B	A	M	B	B
SW.3 - Aplicaciones de gestión de relaciones con clientes.	B	A	M	B	B

[E.23] Manipulación o errores de mantenimiento / actualización de equipos (hardware)					
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.					
Probabilidad: Baja La probabilidad de que ocurra este suceso es baja, debido a que hoy en día hay gran facilidad para realizar actualizaciones en los equipos y aplicaciones software, siendo incluso en algunos casos automático.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
HW.1 - Equipos de sobremesa o portátiles	B	M	A	-	-
Media.1- Dispositivos de almacenamiento	B	M	A	-	-
Media.2 - Servidores y sistemas de almacenamiento	B	M	A	-	-
AUX.1 – Cerraduras electrónicas	-	-	A	-	-
AUX.2 – Aire acondicionado	-	-	A	-	-

[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos					
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.					
Probabilidad: Media La probabilidad podría ser baja si el sistema cuenta con recursos suficientes para manejar la carga de trabajo, media si el sistema tiene recursos limitados pero suficientes para manejar la carga de trabajo en la mayoría de las situaciones, o alta si el sistema tiene recursos limitados y es susceptible a caídas debido al agotamiento de estos recursos.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
S.1 - Procesos de negocio relacionados con la actividad de la empresa de topografía y geodesia.	-	M	A	-	B
S.2 – Servicio de atención al cliente.	-	M	A	-	B
S.3 - Servicio de gestión de proyectos.	-	M	A	-	B
HW.1 - Equipos de sobremesa o portátiles	-	-	A	-	B
COM.1 - Router doméstico que da acceso a Internet.	-	-	A	-	B
COM.2 - Switch de 24 bocas sin gestión utilizado para distribuir el cable a los equipos.	-	-	A	-	B

COM.3 - Red wifi protegida por clave WPA2.	-	M	A	-	B
COM.4 - Arquitectura	-	M	A	-	B

[E.25] Robo o Pérdida de equipos					
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.					
Probabilidad: Baja En general, la pérdida de equipos puede tener una probabilidad baja, media o alta dependiendo de las circunstancias. Por ejemplo, si se implementan medidas de seguridad adecuadas y se realiza un seguimiento regular de los equipos, la probabilidad de pérdida de equipos podría ser baja. En cambio, si no se toman medidas de seguridad adecuadas o no se lleva un seguimiento regular de los equipos, la probabilidad de pérdida de equipos podría ser más alta.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
HW.1 - Equipos de sobremesa o portátiles	M	M	A	M	M
Media.1- Dispositivos de almacenamiento	A	A	A	A	M
Media.2 - Servidores y sistemas de almacenamiento	A	A	A	A	M
AUX.1 – Cerraduras electrónicas	-	-	A	-	M
AUX.2 – Aire acondicionado	-	-	A	-	M

[E.28] Indisponibilidad del personal					
Descripción: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ...					
Probabilidad: Baja La probabilidad de que el personal de la empresa no esté disponible es baja ya que por ejemplo las personas en general no suelen enfermar muchas veces al año de media, aunque puede ir por rachas: puede que un personal no enferme durante años y luego en un año enferma 3 veces.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
P.1 - Personal interno de la empresa, incluyendo profesionales de campo, técnicos y administrativos.	-	-	A	-	-
P.2 - Personal subcontratado que pueda tener acceso a la información de la empresa.	-	-	A	-	-

[A.5] Suplantación de la identidad del usuario					
Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.					
Probabilidad: Media La probabilidad de que ocurra esta amenaza puede variar ampliamente dependiendo de factores como la seguridad del sistema, la forma en que se protege la información de acceso y el nivel de conciencia de seguridad entre los usuarios autorizados.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
S.1 - Procesos de negocio relacionados con la actividad de la empresa de topografía y geodesia.	A	A	M	A	B
S.2 – Servicio de atención al cliente.	A	A	M	A	B
S.3 - Servicio de gestión de proyectos.	A	A	M	A	B
SW.1 – Aplicaciones de topografía y geodesia.	A	M	M	A	B
SW.2 - Aplicaciones de planificación de recursos y de gestión de la producción.	A	M	M	A	B
SW.3 - Aplicaciones de gestión de relaciones con clientes.	A	M	M	A	B
COM.1 - Router doméstico que da acceso a Internet.	M	M	-	M	B
COM.2 - Switch de 24 bocas sin gestión utilizado para distribuir el cable a los equipos.	M	M	-	M	B
COM.3 - Red wifi protegida por clave WPA2.	M	A	-	M	B
COM.4 - Arquitectura	M	A	-	M	B
D.1 - Datos e información relacionados con el trabajo de campo y la gestión de proyectos.	A	A	M	A	B
D.2 - Datos e información relacionados con la gestión de la empresa, como clientes, proveedores y empleados.	A	A	M	A	B
D.3 - Datos de clientes y proyectos.	A	A	M	A	B
D.4 - Información financiera de la empresa.	A	A	M	A	B

[A.8] Difusión de software dañino					
Descripción: propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.					
Probabilidad: Media En general, la probabilidad de que ocurra esta amenaza depende de varios factores, como la seguridad y las medidas de protección implementadas en el sistema, la sensibilidad de los datos que almacena el sistema, y el nivel de actividad de los ciberdelincuentes en el área geográfica en la que se encuentra el sistema.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
SW.1 – Aplicaciones de topografía y geodesia.	M	A	A	A	B
SW.2 - Aplicaciones de planificación de recursos y de gestión de la producción.	M	A	A	A	B
SW.3 - Aplicaciones de gestión de relaciones con clientes.	M	A	A	A	B

[A.25] Robo					
Descripción: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.					
Probabilidad: Media En general, se podría decir que la probabilidad de que ocurra esta amenaza puede ser considerada media ya que, aunque en algunos casos la seguridad puede ser alta, siempre existe un riesgo de que un delincuente pueda acceder a los equipos de alguna manera.					
Activos Afectados					
Nombre	**Degradación**				
	C	I	D	A	T
HW.1 - Equipos de sobremesa o portátiles	M	M	A	-	M
Media.1- Dispositivos de almacenamiento	M	A	M	-	M
Media.2 - Servidores y sistemas de almacenamiento	A	A	M	-	M
AUX.1 – Cerraduras electrónicas	-	-	A	-	M
AUX.2 – Aire acondicionado	-	-	A	-	M

2.3. Riesgos

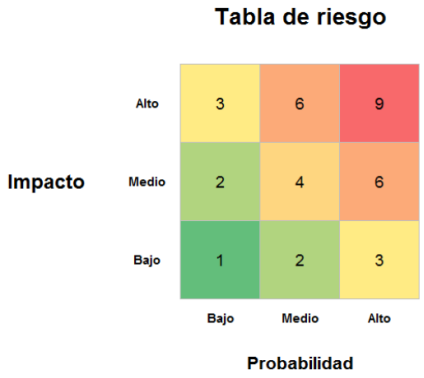
El análisis de riesgos es un proceso que consiste en identificar los riesgos de seguridad de la empresa, determinar su magnitud e identificar las áreas que requieren implantar salvaguardas. Para llevar a cabo este análisis nos centraremos en los **activos que hemos considerado más importantes** en función de la relevancia que tienen para el negocio y del impacto que una incidencia sobre el mismo pueda causar a la entidad **[2.1.2]**.

Para realizar el análisis utilizaremos las siguientes tablas donde se señalan los valores que emplearemos para indicar las probabilidades e impactos de las amenazas. También usaremos una tabla con rangos como criterio de aceptación del riesgo.

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.

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.

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.



S.1 - Procesos de negocio			
Amenazas	**Probabilidad**	**Impacto**	**Riesgo**
[E.1] Errores de los usuarios	3	1	3
[E.2] Errores del administrador.	2	2	4
[E.9] Errores de [re-]encaminamiento	1	2	2
[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos	2	2	4
[A.5] Suplantación de la identidad del usuario	2	3	6

S.3 - Servicio de gestión de proyectos			
Amenazas	**Probabilidad**	**Impacto**	**Riesgo**
[E.1] Errores de los usuarios	3	1	3
[E.2] Errores del administrador.	2	2	4
[E.9] Errores de [re-]encaminamiento	1	2	2
[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos	2	2	4
[A.5] Suplantación de la identidad del usuario	2	3	6

D.1 - Datos e información relacionados con el trabajo de campo y gestión de proyectos			
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

D.3 - Datos de clientes y proyectos			
Amenazas	**Probabilidad**	**Impacto**	**Riesgo**
[E.1] Errores de los usuarios	3	3	9
[E.2] Errores del administrador.	2	3	6
[A.5] Suplantación de la identidad del usuario	2	3	6

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

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

P.1 - Personal interno de la empresa			
Amenazas	**Probabilidad**	**Impacto**	**Riesgo**
[E.1] Errores de los usuarios	3	1	3
[E.7] Deficiencias de la organización	2	2	4
[E.9] Errores de [re-]encaminamiento	1	1	1
[E.28] Indisponibilidad del personal	2	3	6

COM.3 - Red Wifi protegida por clave WPA2			
Amenazas	**Probabilidad**	**Impacto**	**Riesgo**
[I.8] Fallo de servicios de comunicaciones	2	3	6
[E.2] Errores del administrador.	2	3	6
[E.9] Errores de [re-]encaminamiento	1	2	2
[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos	2	3	6
[A.5] Suplantación de la identidad del usuario	2	1	2

COM.4 - Arquitectura del Sistema			
Amenazas	**Probabilidad**	**Impacto**	**Riesgo**
[I.8] Fallo de servicios de comunicaciones	2	2	4
[E.2] Errores del administrador.	2	3	6
[E.9] Errores de [re-]encaminamiento	1	2	2
[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos	2	3	6
[A.5] Suplantación de la identidad del usuario	2	1	2

Media.1 - Dispositivos de almacenamiento			
Amenazas	**Probabilidad**	**Impacto**	**Riesgo**
[N.1] Fuegos	1	2	2
[N.2] Daños por agua	1	2	2
[N.*] Desastres naturales	1	2	2
[I.5] Avería de origen físico o lógico	2	3	6
[I.6] Corte del suministro eléctrico	1	1	1
[I.7] Condiciones inadecuadas de temperatura o humedad	2	2	4
[I.10] Degradación de los soportes de almacenamiento de la información	1	1	1
[E.1] Errores de los usuarios	3	1	3
[E.2] Errores del administrador	2	3	6
[E.23] Manipulación o errores de mantenimiento / actualización de equipos (hardware)	1	2	2
[E.25] Robo o Pérdida de equipos	1	3	3
[A.25] Robo	2	3	6

2.4. Salvaguardas (contramedidas)

Se definen las salvaguardas o contramedidas de seguridad como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Estas pueden actuar disminuyendo el impacto o la probabilidad.

Tal y como se indicó en el apartado anterior, para aquellas amenazas con un **Riesgo > 4**, consideraremos el riesgo reseñable y procederemos a su correspondiente tratamiento. Para realizar el análisis de salvaguardas o medidas de seguridad se ha incluido la siguiente información:

- Nombre de los activos más críticos.
- Las amenazas que afectan a dichos riesgos.
- Una serie de salvaguardas para reducir el riesgo.
- Una probabilidad que indica en qué medida la salvaguardas reduciría el impacto de la amenaza tratada sobre el activo que se está analizando.
- Tras estas tablas se incluye una breve explicación de las salvaguardas que se han elegido.

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

S.3 - Servicio de gestión de proyectos		
Amenazas	**Salvaguardas**	**Probabilidad**
[A.5] Suplantación de la identidad del usuario	Uso de contraseñas seguras	Muy Alta
	Restricciones de acceso	Alta
	Formación del personal	Alta

Explicación salvaguardas elegidas:

Autenticación fuerte: se pueden utilizar métodos de autenticación fuertes como la autenticación de dos factores, que implica utilizar dos métodos diferentes (como una contraseña y un código enviado a un dispositivo móvil) para verificar la identidad del usuario.

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

Uso de contraseñas seguras: se pueden establecer políticas de contraseñas seguras que requieran que los usuarios utilicen contraseñas complejas y difíciles de adivinar.

Restricciones de acceso: se pueden implementar restricciones de acceso que limiten el acceso a los sistemas y aplicaciones a solo los usuarios autorizados.

Formación del personal: se puede ofrecer formación al personal sobre cómo detectar y evitar intentos de suplantación de la identidad del usuario, así como sobre buenas prácticas de seguridad informática en general.

D.1 - Datos e información relacionados con el trabajo de campo y gestión de proyectos		
Amenazas	**Salvaguardas**	**Probabilidad**
[E.1] Errores de los usuarios	Formación y capacitación periódica	Media
	Sistemas de validación y verificación de datos	Alta
	Realizar copias de seguridad	Media
	Sistemas de control de acceso	Media
[E.2] Errores del administrador	Capacitación y formación del personal responsable	Alta
	Copias de seguridad y recuperación	Media
	Monitoreo y alertas	Baja

[A.5] Suplantación de la identidad del usuario	Autenticación fuerte	Alta
	Implementar sistemas de control de acceso	Alta
	Verificación y autorización	Alta
	Medidas de protección de la información	Media

D.3 - Datos de clientes y proyectos		
Amenazas	**Salvaguardas**	**Probabilidad**
[E.1] Errores de los usuarios	Sistemas de validación y verificación de datos	Alta
	Políticas y procedimientos claros y sencillos	Baja
	Realizar copias de seguridad	Media
	Sistemas de control de acceso	Media
[E.2] Errores del administrador.	Capacitación y formación del personal responsable	Alta
	Revisión y validación de cambios	Media
	Copias de seguridad y	Baja

	recuperación	
	Acceso controlado y autorización	Alta
	Monitoreo y alertas	Baja
[A.5] Suplantación de la identidad del usuario	Políticas para el uso y la gestión de las credenciales	Alta
	Protección de la información	Alta

D.4 - Información financiera de la empresa		
Amenazas	**Salvaguardas**	**Probabilidad**
[E.1] Errores de los usuarios	Sistemas de validación y verificación de datos	Alta
	Políticas y procedimientos claros y sencillos	Baja
	Realizar copias de seguridad	Media
	Sistemas de control de acceso	Media
[E.2] Errores del administrador.	Capacitación y formación del personal responsable	Alta
	Revisión y validación de cambios	Media
	Copias de seguridad y	Baja

	recuperación	
	Acceso controlado y autorización	Alta
	Monitoreo y alertas	Baja
[A.5] Suplantación de la identidad del usuario	Políticas para el uso y la gestión de las credenciales	Alta
	Protección de la información	Alta
	Implementar sistemas de control de acceso	Alta

Explicación salvaguardas elegidas:

Realizar formación y capacitación periódica a los empleados sobre el uso correcto de los sistemas y la importancia de la precisión y la seguridad en el manejo de datos.

Implementar sistemas de validación y verificación de datos que permitan detectar y corregir errores antes de que se produzcan o se difundan.

Establecer políticas y procedimientos claros y sencillos para el manejo de datos, y asegurarse de que los empleados las conozcan y las cumplan.

Realizar copias de seguridad periódicas de los datos, para poder recuperarlos en caso de pérdida o corrupción.

Implementar sistemas de control de acceso que permitan restringir el acceso a los datos sólo a las personas autorizadas, y que registren y supervisen el acceso y la modificación de los datos.

Implementar sistemas de autenticación fuertes y seguros que permitan verificar la identidad de los usuarios de manera fiable y evitar que terceros se hagan pasar por ellos. Por ejemplo, se podrían utilizar contraseñas seguras, tokens de acceso, o autenticación de dos factores.

Establecer políticas y procedimientos para el uso y la gestión de las credenciales de acceso, como contraseñas y tokens, y asegurarse de que los usuarios las protejan y cambien periódicamente.

Implementar sistemas de control de acceso y supervisión que permitan registrar y monitorear el acceso y la actividad de los usuarios, y detectar y bloquear intentos de suplantación de identidad.

Realizar una verificación y autorización adecuadas de las personas que tienen acceso a los sistemas y datos, y establecer una política de rotación y eliminación de los accesos innecesarios o inactivos.

Implementar medidas de protección de la información, como cifrado de datos y redes, para evitar que los atacantes puedan acceder a ellos en caso de suplantación de identidad.

Capacitación y formación del personal responsable: proporcionar a las personas responsables de instalación y operación la formación y capacitación necesarias para realizar su trabajo de manera eficiente y evitar errores.

Revisión y validación de cambios: establecer procesos de revisión y validación de cambios para asegurar que los cambios realizados en el sistema sean correctos y no causen problemas.

Copias de seguridad y recuperación: realizar copias de seguridad periódicas de los datos y establecer un plan de recuperación de desastres para garantizar que se puedan recuperar los datos en caso de pérdida.

Acceso controlado y autorización: establecer medidas de control de acceso para garantizar que solo las personas autorizadas tengan acceso a los datos e información relevantes.

Monitoreo y alertas: implementar sistemas de monitoreo y alertas para detectar posibles problemas o errores de manera rápida y tomar medidas de corrección.

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
[E.8] Difusión de software dañino	Implementar software antivirus	Alta
	Copias de seguridad periódicas	Media
	Políticas y procedimientos para la descarga y la instalación de software	Media
[E.20] Vulnerabilidades de los programas (software)	Mantener actualizadas las aplicaciones y los sistemas operativos	Alta

	Software de protección de la información	Alta
	Establecer políticas para la gestión de vulnerabilidades	Alta
	Medidas de protección de la información	Alta
	Copias de seguridad periódicas	Media
[A.8] Difusión de software dañino	Implementar un software antivirus	Alta
	Políticas y procedimientos para la descarga y la instalación de software	Media
	Sistemas de control de acceso y supervisión	Baja

Explicación salvaguardas elegidas:

Capacitación y formación del personal responsable: proporcionar a las personas responsables de instalación y operación la formación y capacitación necesarias para realizar su trabajo de manera eficiente y evitar errores.

Revisión y validación de cambios: establecer procesos de revisión y validación de cambios para asegurar que los cambios realizados en el sistema sean correctos y no causen problemas.

Copias de seguridad y recuperación: realizar copias de seguridad periódicas de los datos y establecer un plan de recuperación de desastres para garantizar que se puedan recuperar los datos en caso de pérdida.

Implementar un software antivirus y un sistema de protección en línea para detectar y eliminar malware y otras amenazas informáticas.

Establecer políticas y procedimientos para la descarga y la instalación de software, y asegurarse de que los usuarios sólo instalen y ejecuten aplicaciones de fuentes confiables y verificadas.

Realizar copias de seguridad periódicas de las aplicaciones y la información que contienen, para poder recuperarlas en caso de pérdida o daño.

Implementar medidas de protección de la información, como cifrado de datos y redes, para evitar que los atacantes puedan acceder a ellos en caso de difusión de malware.

Establecer sistemas de control de acceso y supervisión que permitan restringir el acceso a las aplicaciones solo a las personas autorizadas y que registren y supervisen el acceso y la actividad de los usuarios.

Mantener actualizadas las aplicaciones y los sistemas operativos a las últimas versiones disponibles, que suelen incluir parches y correcciones de vulnerabilidades conocidas.

Utilizar software de protección de la información y de monitoreo de vulnerabilidades que permita detectar y mitigar riesgos de seguridad en las aplicaciones.

Establecer políticas y procedimientos para la gestión de vulnerabilidades, que incluyan la evaluación y priorización de los riesgos y la implementación de medidas de mitigación adecuadas.

Implementar medidas de protección de la información, como cifrado de datos y redes, que puedan ayudar a proteger los datos y la información de posibles ataques o accesos no autorizados.

Realizar copias de seguridad periódicas de las aplicaciones y la información que contienen, para poder recuperarlas en caso de pérdida o daño.

P.1 - Personal interno de la empresa		
Amenazas	**Salvaguardas**	**Probabilidad**
[E.28] Indisponibilidad del personal	Políticas y procedimientos de gestión de la contingencia	Media
	Planes de contingencia	Alta
	Desarrollar y mantener programas de formación y actualización del personal	Alta
	Establecer sistemas de comunicación y coordinación	Alta
	Contratar seguros de responsabilidad civil y de protección de la salud	Media

Explicación salvaguardas elegidas:

Implementar políticas y procedimientos de gestión de la contingencia que permitan identificar los riesgos de indisponibilidad del personal y definir medidas para minimizar sus efectos.

Realizar planes de contingencia para cada área y puesto de trabajo, que incluyan la designación de personal de respaldo y la definición de protocolos de actuación en caso de ausencia del titular.

Desarrollar y mantener programas de formación y actualización del personal, que permitan mejorar las habilidades y el conocimiento de los empleados y aumentar su capacidad para hacer frente a situaciones de contingencia.

Establecer sistemas de comunicación y coordinación efectivos entre los diferentes departamentos y áreas de la empresa, para garantizar la continuidad del trabajo en caso de ausencia del personal.

Contratar seguros de responsabilidad civil y de protección de la salud de los empleados, que cubran los riesgos de enfermedad, accidente o fallecimiento.

COM.3 - Red Wifi protegida por clave WPA2		
Amenazas	**Salvaguardas**	**Probabilidad**
[I.8] Fallo de servicios de comunicaciones	Medidas de protección física	Media
	Medidas de protección lógica	Alta
	Implementar un plan de continuidad del negocio	Alta
	Acuerdos con proveedores de servicios de comunicaciones	Alta
	Contratar seguros de protección de la actividad	Media
[E.2] Errores del administrador	Medidas de seguridad y políticas de acceso y uso de la red wifi	Alta
	Procedimientos de gestión de cambios y de configuración de la red wifi	Alta

	Medidas de protección de la información y de la confidencialidad	Media
	Medidas de formación y capacitación	Bajo
[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos	Dimensionamiento adecuado de los recursos de la red wifi	Alta
	Medidas de gestión de rendimiento y monitoreo	Alta
	Políticas y procedimientos de uso y gestión de la red wifi	Media
	Medidas de seguridad para proteger la red wifi de ataques externos	Media

COM.4 - Arquitectura del Sistema		
Amenazas	**Salvaguardas**	**Probabilidad**
[E.2] Errores del administrador.	Planes de contingencia y planes de recuperación	Alta
	Medidas de formación y capacitación	Baja
[E.24] Denegación del servicio o caída del sistema por agotamiento de recursos	Planes de contingencia y planes de recuperación	Media

Explicación salvaguardas elegidas:

Implementar medidas de protección física para los equipos de comunicaciones y de red, como proteger los cables de red y los dispositivos de acceso a la red de posibles daños o alteraciones.

Implementar medidas de protección lógica para los equipos de comunicaciones y de red, como la utilización de firewalls y sistemas de detección y prevención de intrusiones para proteger la red de posibles ataques externos.

Diseñar e implementar un plan de continuidad del negocio que incluya la identificación de puntos críticos y la definición de medidas de protección y de respuesta ante posibles fallos de servicios de comunicaciones.

Establecer acuerdos y contratos con proveedores de servicios de comunicaciones para garantizar el suministro de servicios de alta disponibilidad y la prestación de servicios de mantenimiento y soporte en caso de fallo.

Contratar seguros de protección de la actividad que cubran los riesgos de interrupción o cese de los servicios de comunicaciones.

Implementar medidas de seguridad y políticas de acceso y uso de la red wifi para protegerla de posibles errores o acciones no autorizadas por parte del administrador o de cualquier otro usuario.

Establecer procedimientos de gestión de cambios y de configuración de la red wifi para asegurar que cualquier cambio o modificación realizada en la red sea revisada y autorizada por un responsable autorizado.

Establecer medidas de protección de la información y de la confidencialidad de los datos transmitidos a través de la red wifi, para evitar que sean accedidos de forma no autorizada por el administrador o por cualquier otro usuario.

Contar con planes de contingencia y planes de recuperación ante posibles fallos o errores del administrador, para minimizar el impacto en el negocio y garantizar la continuidad del servicio.

Implementar medidas de formación y capacitación para el personal de administración, para asegurar que cuentan con los conocimientos y habilidades necesarios.

Realizar un dimensionamiento adecuado de los recursos de la red wifi en función de las necesidades de la empresa y el volumen de tráfico que se espera en la red.

Implementar medidas de gestión de rendimiento y monitoreo de los recursos de la red wifi para detectar posibles problemas de rendimiento o agotamiento de recursos a tiempo y poder tomar medidas correctivas.

Establecer políticas y procedimientos de uso y gestión de la red wifi para evitar el consumo excesivo de recursos y el colapso de la red.

Implementar medidas de seguridad para proteger la red wifi de ataques externos que puedan consumir excesivamente los recursos de la red.

Contar con planes de contingencia y planes de recuperación ante posibles fallos o agotamiento de recursos, para minimizar el impacto en el negocio y garantizar la continuidad del servicio.

Media.1 - Dispositivos de almacenamiento		
Amenazas	**Salvaguardas**	**Probabilidad**
[I.5] Avería de origen físico o lógico	Realizar copias de seguridad periódicas y almacenarlas	Alta
	Dispositivos de almacenamiento de alta calidad y mantenimiento	Media
	Sistema de detección y reparación de errores en los dispositivos de almacenamiento	Media
[E.2] Errores del administrador.	Realizar copias de seguridad regulares	Alta
	Establecer políticas y procedimientos de seguridad	Media
	Implementar medidas de monitoreo y supervisión	Alta
	Proporcionar capacitación y formación adecuada a los administradores	Media
[A.25] Robo	Cajas fuertes o sistemas de almacenamiento	Alta
	Sistemas de alarma y vigilancia	Alta
	copias de seguridad de los datos almacenados	Media

	Políticas de acceso y uso de los dispositivos de almacenamiento	Media
	Medidas de seguridad física en la sede	Media

Explicación salvaguardas elegidas:

Realizar copias de seguridad periódicas y almacenarlas en un lugar seguro: esta medida ayuda a proteger la información y a minimizar la pérdida de datos en caso de una avería.

Utilizar dispositivos de almacenamiento de alta calidad y con un mantenimiento adecuado: la utilización de dispositivos de alta calidad y el mantenimiento adecuado pueden ayudar a prevenir fallos y aumentar la confiabilidad del sistema.

Implementar un sistema de detección y reparación de errores en los dispositivos de almacenamiento: este sistema puede ayudar a detectar y corregir errores en los dispositivos de almacenamiento, minimizando el impacto de una avería.

Utilizar cajas fuertes o sistemas de almacenamiento seguros para guardar los dispositivos de almacenamiento.

Implementar sistemas de alarma y vigilancia para proteger la sede de la empresa.

Realizar copias de seguridad de los datos almacenados en los dispositivos de forma regular para minimizar el impacto en caso de robo.

Establecer políticas de acceso y uso de los dispositivos de almacenamiento para minimizar el riesgo de robo por parte de personal interno.

Implementar medidas de seguridad física en la sede de la empresa, como cerraduras de alta seguridad y sistemas de vigilancia.

Realizar copias de seguridad regulares de los datos almacenados en los dispositivos de almacenamiento: Esto permitiría recuperar los datos en caso de pérdida debido a errores del administrador.

Establecer políticas y procedimientos de seguridad y buenas prácticas para el uso de los dispositivos de almacenamiento: Esto incluiría medidas como el uso de contraseñas seguras y la no compartición de cuentas de usuario.

Implementar medidas de monitoreo y supervisión del uso de los dispositivos de almacenamiento: Esto podría incluir el uso de herramientas de monitoreo de actividad y registros de acceso para detectar y prevenir errores del administrador.

Proporcionar capacitación y formación adecuada a los administradores de los dispositivos de almacenamiento: Esto podría incluir cursos de formación en seguridad de la información y buenas prácticas de administración.