Informe de seguridad del sistema

GARANTÍA y SEGURIDAD DE LA INFORMACIÓN
Curso 22/23

Grupo 02

Carlos Martín Sanz
Alejandro Pulido Sánchez
Héctor Toribio González

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 y administrativo 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 concentrador.

1.1.1. Dependencias

La empresa dispone de una sede con unos 150 m2 distribuídos 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 medias 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

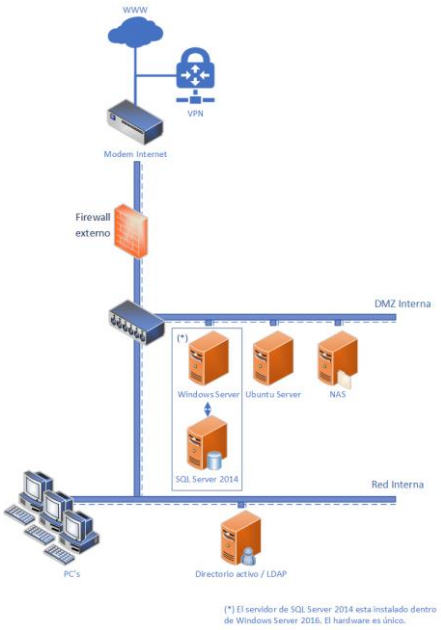
- Administración (Finanzas/RR.HH.): SAP, software de planificación de recursos empresariales.
- Operaciones: Software para la gestión de la producción.
- Oficina Técnica: PLM, software de gestión del ciclo de vida del producto.
- Diseño: PLM, software de gestión del ciclo de vida del producto.
- Comercial: 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: **(puede / debe modificarla como desee, argumentando lo hecho)**



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

Primero numeremos los activos y después realizaremos el mapa:

1. PC’s: Son recursos de la empresa e implicaría un riesgo bastante importante que fallasen o que alguien comprometiese estos equipos.

2. NAS: Dispositivo de almacenamiento conectado a la red encargado de la realización de copias de seguridad de ciertos datos importantes.

3. Ubuntu Web: Web OS que utilizan ciertas líneas de negocio dentro de la empresa.

4. Programas Java o Python

5. Windows Server 2016: Web OS de Windows que ofrece ciertas capas de seguridad inspiradas en Azure. Importante en la empresa ya que aloja servicios cruciales como el de correo.

6. SQL Server 2014: Sistema de administración de datos utilizado por la empresa. Un sujeto que desee comprometer o robar información puede usarlo para obtener datos de la empresa.

7. Red Interna: Si alguien externo accede puede causar problemas.

8. VPN.

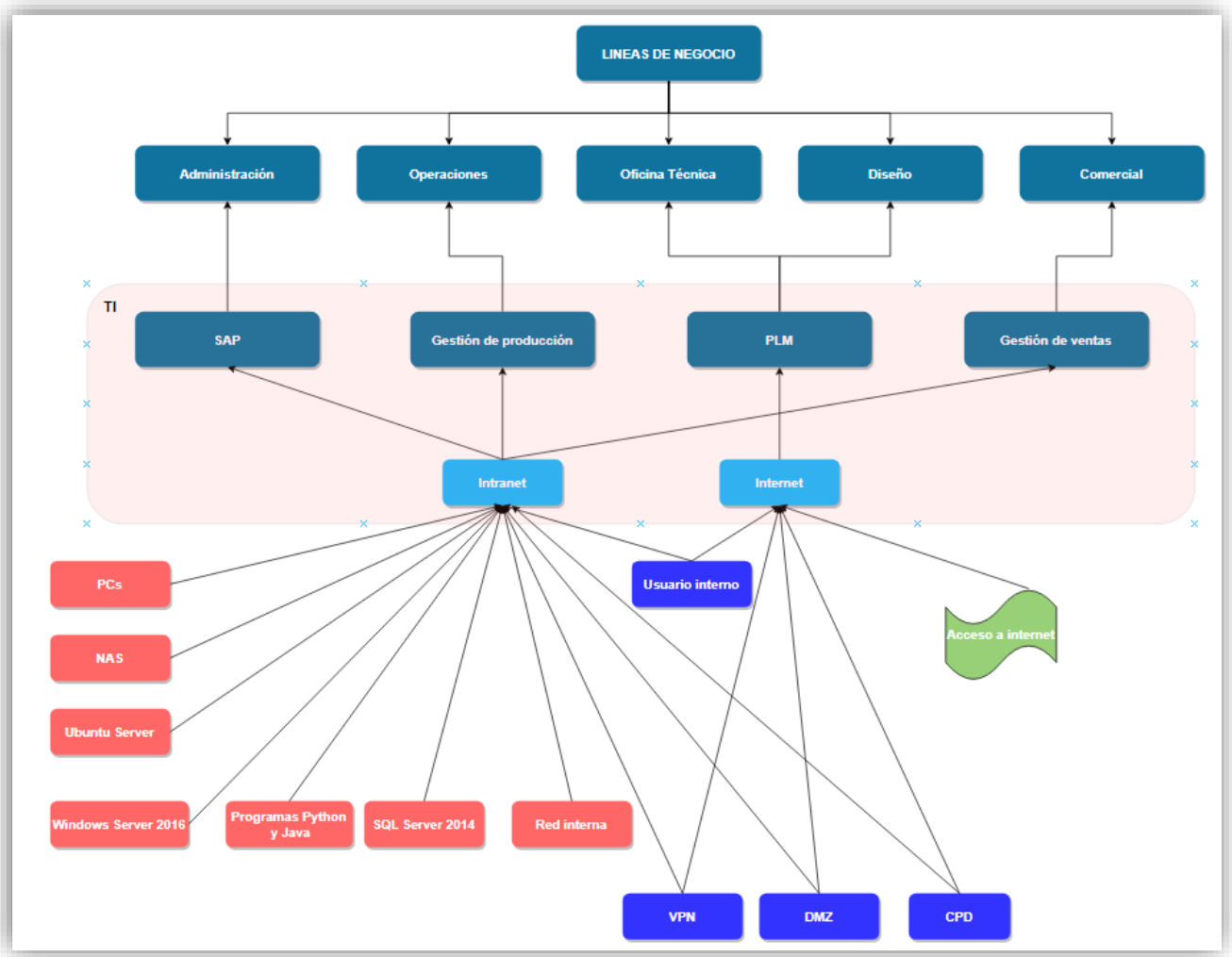
9. DMZ: Activo importante.

10. Acceso a internet: El sitio menos seguro que hay y a través del que pueden llegar la gran mayoría de ataques.

11. CPD: Centro de Procesamiento de Datos en el que se aloja parte de la información de la empresa. Estos sitios suelen tener un altísimo nivel de seguridad… a pesar de esto, es posible atacar y comprometer servidores en estos lugares.

12. Usuario interno.

Mapa de activos a considerar en la empresa y sus dependencias:



2. Análisis de Riesgos y Medidas de Seguridad

2.1. Bienes de Información valiosos (catálogo de activos)

Para realizar la clasificación de los bienes de información valiosos dentro del catálogo de activos, vamos a realizar una clasificación acorde a la realizada por la metodología Magerit. Dicha metodología a la cual hemos tenido acceso gracias a los materiales de trabajo proporcionados, toda la información se recoge en el siguiente enlace MAGERIT 3.0

Identificamos los activos en nuestro caso concreto en el orden que aparecen en el documento anteriormente mencionado:

- **Datos e información manejada.**
  - **Datos de los trabajadores de la empresa.**
  - **Datos de los clientes.**
  - **Datos de los proveedores.**
  - **Políticas de empresa.**
  - **Modelos y arquitecturas de seguridad.**
  - **Diagrama de red de la organización.**

- **Servicios internos y externos**

En este punto recopilamos los servicios tanto internos como externos que son necesarios para poder organizar el sistema.

- **Ubuntu Server:** en este servidor están todas las aplicaciones internas que dan soporte a Operaciones y Gestión de Proyectos, desarrolladas en Java y Python.
  - Garantizar y asegurar el control de accesos HTTP (CORS).
  - Asegurar que este servidor Ubuntu tiene acceso a la intranet de la empresa/organización durante todo su ciclo de vida.
    - Minimizar las posibles desconexiones o problemas.
  - Asegurar que esté actualizado con todos los parches y actualizaciones de seguridad pertinentes.
    - Comprobar que el firewall del servidor está configurado de forma correcta. Para controlar los servicios expuestos en la red.

- **Windows Server 2016:** aquí es donde reside el servidor de correo, Exchange y el Directorio Activo.
  - Garantizar y asegurar el control de accesos HTTP (CORS)
  - Asegurar que este servidor tiene acceso a la intranet de la empresa/organización durante todo su ciclo de vida
    - Minimizar las posibles desconexiones o problemas
  - Asegurar que esté actualizado con todos los parches y actualizaciones de seguridad pertinentes.
    - Comprobar que el firewall del servidor está configurado de forma correcta. Para controlar los servicios expuestos en la red.

Dentro del Windows Server como ya hemos dicho residen:

- *Servidor de Correo:*
  - Garantizar y asegurar el control de accesos HTTP (CORS)

- Garantiza y asegurar la disponibilidad y accesibilidad.
- Asegurar que esté actualizado con los últimos parches y actualizaciones de seguridad pertinentes.

- *Exchange:*
  - Permitir a los usuarios acceder a la plataforma de mensajería desde otros dispositivos.
  - Garantiza y asegurar la disponibilidad y accesibilidad.
  - Asegurar que esté actualizado con los últimos parches y actualizaciones de seguridad pertinentes.

- *Directorio Activo:*
  - Garantizar y asegurar el control de accesos HTTP (CORS).
  - Garantiza y asegurar la disponibilidad y accesibilidad.
  - Tener un mecanismo robusto ante posibles ataques de Phishing
  - Tener un mecanismo robusto y una política de contraseñas segura.
  - Documentación de las políticas de seguridad del Directorio Activo.
  - Modelo de Menor Privilegio (PoLP)
    - Concepto de seguridad de la información en que se da a un usuario los permisos de acceso mínimos necesarios para desempeñar sus funciones laborales.

- **SQL Server 2014:**
  - Encargado de asegurar y garantizar que todos los permisos del servidor están configurados correctamente.
  - Asegurar que esté actualizado con todos los parches y actualizaciones de seguridad pertinentes.

- **Aplicaciones informáticas (software)**

Estas aplicaciones informáticas son las que permiten manejar todos los datos dentro del sistema.

- **Programas Java y Python, para garantizar la gestión del ciclo de vida del producto.**
  - Ha de tener conexión con la intranet de la organización.
  - Garantizar la eficiencia del código.
  - Garantizar que los códigos estén probados y testeados de forma correcta y completa para evitar futuros problemas de seguridad.
  - Comprobar que se está utilizando la versión más actualizada tanto de Java como de Python en tema de seguridad.
  - Garantizar y asegurar que, en entornos productivos, los programas no sean legibles.

Soportes de información

- **Equipos informáticos (hardware)**

Dentro de estos dispositivos que permiten hospedar datos, aplicaciones y servicios podríamos realizar una pequeña subdivisión entre los que consideramos principales o de un nivel superior de importancia o prioridad, y los secundarios menos prioritarios o no tan necesarios, pero nos ceñimos a la clasificación Magerit. En esta clasificación los

"secundarios" se denominan equipamiento auxiliar.

- **PC's**
  - Comprobar que el firewall de cada PC está configurado de forma correcta. Para controlar los servicios expuestos en la red.
  - Asegurar que cada PC únicamente está siendo utilizado por aquella persona o personas que disponen de los permisos para ello.
  - Asegurar que todos los PC tienen acceso constante a la intranet de la organización.
  - Asegurar que todos los PC están utilizando su última versión de software, en caso de lo contrario, instalar la versión más actualizada.
- **Modem.**
- **Switch.**
- **Servidores blade y Armarios Rack (CPD).**
- **Máquinas refrigeradoras de ambiente.**
- **Bombonas Gas Novec 1230 (Extinción de inciendo)**

- **Soportes de información**

Son los dispositivos encargados de todo el almacenamiento de datos dentro del sistema

- **Servidor NAS:** donde se almacenan los diseños de los productos, los catálogos comerciales, las fotometrías …
  - Garantizar y asegurar que únicamente pueden acceder a este servidor las personas que tengan permiso o autorización.
  - Relacionado con el punto anterior, que cada persona que tiene acceso únicamente realice las acciones permitidas o correspondientes.
  - Asegurar que el servidor tiene acceso constante a la intranet de la organización.
  - Asegurar que está utilizando su última versión de software, en caso de lo contrario, instalar la versión más actualizada.
  - Asegurar y garantizar que todos los dispositivos físicos que utiliza el servidor NAS están en buen estado, con el fin de que la información que este contiene es siempre accesible.

- **Disco dedicado:** donde se almacena información adicional.
  - Asegurar su correcto funcionamiento.
  - Garantizar y asegurar que únicamente pueden acceder a la información que contiene este disco las personas que tengan permiso o autorización.

- **Equipamiento auxiliar**

Son dispositivos que complementan el material informático.

- **Teclados y ratones para los PC's.**
- **Repetidores de conexión.**
- **Dispositivos electrónicos para los empleados (Únicamente utilizables en el ámbito de la organización).**

- **Redes y comunicación**

Recopilamos las redes que van a ser necesarias para la organización, y que van a permitir el intercambio de datos dentro de esta.

- **Acceso a Internet: t**odos los dispositivos relacionados con la organización tanto PC's de la oficina, así como dispositivos de los empleados proporcionados por la organización han de poder conectarse a Internet, independientemente de donde se encuentren dentro de la oficina.

- **VPN**: una Red privada virtual, que permita la extensión segura de la red ya cifran su tráfico en internet y disfrazan su identidad en línea. Con el fin de evitar a terceros el seguimiento de sus actividades en línea y el robo de datos.
  - Asegurar el acceso y disponibilidad a esta.
  - Asegurar que toda la organización tenga acceso seguro a Internet externo.

- **DMZ:** una zona desmilitarizada, es decir, red aislada que se encuentra dentro de la red interna de la organización. Dentro de esta se encuentran ubicados los recursos de la organización que son accesibles desde Internet, como son el servidor de correo y el Exchange.
  - Asegurar que toda la organización tenga acceso seguro a Internet externo.

- **Instalaciones**

Son los lugares físicos donde se van a encontrar los equipos informáticos y de comunicaciones de la organización.

- **CPD**
  - Garantizar el control de acceso.
  - Condiciones idóneas de temperatura y espacio para el funcionamiento y conservación de este.
- **Oficina**
  - Garantizar el control de acceso.
  - Tener los recursos físicos localizados en una zona.
  - División en despachos para cada empleado.

- **Personal**

Las personas encargadas de explotar y operar todos los elementos/activos anteriormente mencionados.

- **Profesionales de campo**
  - Compromiso de trabajo con la organización.
  - Fomentar responsabilidad dentro de la organización.

- **Técnicos**
  - Compromiso de trabajo con la organización.
  - Fomentar responsabilidad dentro de la organización.

- **Administrativo**
  - Compromiso de trabajo con la organización.
  - Fomentar responsabilidad dentro de la organización.

Una vez que ya hemos clasificado los activos según la metodología Magerit, vamos a marcar los requerimientos necesarios para cada activo en base a los principales pilares de la seguridad “CIDAN” vistos en clase. También asignamos un responsable al activo, así como un tipo, la ubicación donde se encuentra y si este activo es crítico (realmente importante o no). Las celdas marcadas de color verde son los requerimientos necesarios en esos activos.

LISTADO DE ACTIVOS

							Confidencialidad	Integridad	Disponibilidad	Autenticidad	No repudio
ID	Grupo	Nombre	Responsable	Tipo	Ubicación	Crítico	C	I	D	A	N
ID_0001	Servicios internos y externos	Ubuntu Server	Responsables de la información y de los servicios	Servidor (físico)	Sala de servidores	SI					
ID_0002	Servicios internos y externos	Windows Server 2016	Responsables de la información y de los servicios	Servidor (físico)	Sala de servidores	SI					
ID_0003	Servicios internos y externos	Servidor de Correo	Responsables de la información y de los servicios	Servidor (físico)	Sala de servidores	SI					
ID_0004	Servicios internos y externos	Directorio Activo	Responsables de la información y de los servicios	Directorio (físico)	Sala del CPD1	SI					
ID_0005	Servicios internos y externos	SQL Server 2014	Responsables de la información y de los servicios	Servidor (físico)	Sala de servidores	SI					
ID_0006	Servicios internos y externos	Exchange	Responsables de la información y de los servicios	Servidor (físico)	Sala de servidores	SI					
ID_0007	Datos e información manejada	Datos de los trabajadores de la empresa	Responsable de seguridad y Responsables de la información	Información (online)	En los servidores de la organización	SI					
ID_0008	Datos e información manejada	Datos de los clientes	Responsable de seguridad y Responsables de la información	Información (online)	En los servidores de la organización	SI					
ID_0009	Datos e información manejada	Datos de los proveedores	Responsable de seguridad y Responsables de la información	Información (online)	En los servidores de la organización	SI					
ID_0010	Datos e información manejada	Políticas de la empresa	Responsable de seguridad y Responsables de la información	Información (online)	En los servidores de la organización	SI					
ID_0011	Datos e información manejada	Modelos y arquitecturas de la seguridad	Responsable de seguridad y Responsables de la información	Información (online)	En los servidores de la organización	SI					
ID_0012	Datos e información manejada	Diagrama de red de la organización	Responsable de seguridad y Responsables de la información	Información (online)	En los servidores de la organización	SI					
ID_0013	Aplicaciones informáticas (software)	Programas Python	Responsable de operaciones	Software	En los PC's	SI					
ID_0014	Aplicaciones informáticas (software)	Programas Java	Responsable de operaciones	Software	En los PC's	SI					
ID_0015	Equipos informáticos (hardware)	PC's	Responsable de Administración y Comercial	Dispositivos (físico)	Oficina y despachos o almacén	SI					
ID_0016	Equipos informáticos (hardware)	Modem	Responsable de Administración y Comercial	Dispositivos (físico)	Oficina y despachos o almacén	SI					
ID_0017	Equipos informáticos (hardware)	Switch	Responsable de Administración y Comercial	Dispositivos (físico)	Oficina y despachos o almacén	SI					
ID_0018	Equipos informáticos (hardware)	Bombonas Gas Novec 1230	Responsable de seguridad	Bombonas (físico)	Salas del CPD	SI					
ID_0019	Equipos informáticos (hardware)	Servidores Blade y armarios Rack (CPD)	Responsable de Administración y Comercial	Dispositivos (físico)	Salas del CPD	SI					
ID_0020	Equipos informáticos (hardware)	Máquinas refrigeradoras de ambiente	Responsable de seguridad	Dispositivos (físico)	Salas del CPD	SI					
ID_0021	Soportes de información	Servidor NAS	Responsable de seguridad y Responsables de la información	Servidor (físico)	Salas del CPD	SI					
ID_0022	Soportes de información	Disco dedicado	Responsable de seguridad y Responsables de la información	Servidor (físico)	Salas del CPD	SI					
ID_0023	Equipamiento auxiliar	Teclados y ratones	Responsable comercial y administración	Dispositivos (físico)	Oficina y despachos o almacén	NO					
ID_0024	Equipamiento auxiliar	Repetidores	Responsable comercial y administración	Dispositivos (físico)	Oficina y despachos o almacén	NO					
ID_0025	Equipamiento auxiliar	Dispositivos para empleados	Responsable comercial y administración	Dispositivos (físico)	Oficina y despachos o almacén	NO					
ID_0026	Redes y comunicaciones	Acceso a internet	Responsable de sistemas y telecomunicaciones	Redes y dispositivos (físicos)	Toda la oficina y zonas de ella	SI					
ID_0027	Redes y comunicaciones	VPN	Responsable de sistemas y telecomunicaciones	Online	Toda la oficina y zonas de ella	SI					
ID_0028	Redes y comunicaciones	DMZ	Responsable de sistemas y telecomunicaciones	Online	Toda la oficina y zonas de ella	SI					
ID_0029	Instalaciones	CPD	Responsable de servicios	Lugar (físico)	Local externo a la oficina	SI					
ID_0030	Instalaciones	Oficina	Responsable de oficina	Lugar (físico)	Zona de 150 m2	SI					
ID_0031	Personal	Profesionales de campo	Responsable de Administración	Personas físicas	Área de trabajo o zona de café	SI					
ID_0032	Personal	Técnicos	Responsable de Administración	Personas físicas	Área de trabajo o zona de café	SI					
ID_0033	Personal	Administrativos	Responsable de Administración	Personas físicas	Área de trabajo o zona de café	SI					

2.2. Listado de amenazas

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

Vamos a analizar las amenazas que hemos considerado más importantes por separado y ver a que activos afecta, con que impacto y con que probabilidad, pero, antes de esto, realizaremos una tabla para ver que dimensiones (CIDAT) tiene cada amenaza que vamos a tratar. De esta manera primero veremos a que principios fundamentales de la seguridad afectará cada amenaza y, tras esto, como afecta en concreto a cada activo.

Tabla de dimensión de amenazas:

LEYENDA DIMENSIÓN	
	AFECTA
	NO AFECTA

DIMENSION DE AMENAZAS						
ID_amenaza	Nombre amenaza	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
A.18	DESTRUCCIÓN DE INFORMACIÓN					
A.24	DENEGACIÓN DE SERVICIO					
E.1	ERRORES DE LOS USUARIOS					
E.2	ERRORES EN LA ADMINISTRACIÓN					
E.7	DFICIENCIAS EN LA ORGANIZACIÓN					
E.19	FUGAS DE INFORMACIÓN					
E.20	VULNERABILIDADES EN LOS PROGRAMAS					
E.21	ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS					
E.22	ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE EQUIPOS					
E.24	CAIDA DE SISTEMAS POR AGOTAMIENTO DE RECURSOS					
I.6	CORTE DE SUMINISTRO ELÉCTRICO					
I.10	DEGRADACIÓN DE LOS SOPORTES DE ALMACENANMIENTO DE LA INFORMACIÓN					
N.1	FUEGO					
N.2	AGUA					

A continuación, analizaremos a que activos y en qué medida afectan las amenazas seleccionadas. Algunas de las amenazas las hemos unido en una tabla ya que consideramos que afectan a los mismos activos y de una forma parecida:

Posibilidad de que el fuego acabe con recursos del sistema

FUEGO [N.1]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0001	Ubuntu Server	Alto	Bajo
ID_0002	Windows Server 2016	Alto	Bajo
ID_0003	Servidor de correo	Alto	Bajo
ID_0004	Directorio Activo	Alto	Bajo
ID_0005	SQL Server 2014	Alto	Bajo
ID_0006	Exchange	Alto	Bajo
ID_0015	PC's	Alto	Bajo
ID_0016	Modem	Alto	Bajo
ID_0017	Switch	Alto	Bajo
ID_0019	Servidores Blade y Armarios Rack	Alto	Bajo
ID_0021	Servidor NAS	Alto	Bajo
ID_0022	Disco dedicado	Medio	Bajo
ID_0024	Repetidores	Medio	Bajo
ID_0029	CPD	Medio	Bajo
ID_0030	Oficina	Medio	Bajo

Posibilidad de que el agua acabe con recursos del sistema.

AGUA [N.2]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0001	Ubuntu Server	Alto	Bajo
ID_0002	Windows Server 2016	Alto	Bajo
ID_0003	Servidor de correo	Alto	Bajo
ID_0004	Directorio Activo	Alto	Bajo
ID_0005	SQL Server 2014	Alto	Bajo
ID_0006	Exchange	Alto	Bajo
ID_0015	PC's	Alto	Bajo
ID_0016	Modem	Alto	Bajo
ID_0017	Switch	Alto	Bajo
ID_0019	Servidores Blade y Armarios Rack	Alto	Bajo
ID_0021	Servidor NAS	Alto	Bajo
ID_0022	Disco dedicado	Medio	Bajo
ID_0024	Repetidores	Medio	Bajo
ID_0029	CPD	Medio	Bajo
ID_0030	Oficina	Medio	Bajo

Cese de la alimentación de potencia

CORTE DE SUMINISTRO ELÉCTRICO [I.6]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0001	Ubuntu Server	Alto	Media
ID_0002	Windows Server 2016	Alto	Media
ID_0003	Servidor de Correo	Alto	Media
ID_0004	Directorio Activo	Alto	Media
ID_0005	Exchange	Alto	Media
ID_0006	SQL Server 2014	Alto	Media
ID_0007	Datos de los trabajadores de la empresa	Alto	Media
ID_0008	Datos de los clientes	Alto	Media
ID_0009	Datos de los proveedore	Alto	Media
ID_0010	Modelos de arquitectura y seguridad	Alto	Media
ID_0011	Modelos y arquitecturas de la seguridad	Alto	Media
ID_0012	Diagrama de red de la organización	Alto	Media
ID_0013	Programas Python	Bajo	Media
ID_0014	Programas Java	Bajo	Media
ID_0018	PC's	Alto	Media
ID_0019	Modem	Alto	Media
ID_0020	Switch	Alto	Media
ID_0021	Servidores Blade y armarios Rack (CPD)	Alto	Media
ID_0022	Máquinas refrigeradoras de ambiente	Alto	Media
ID_0023	Gas Novec 1230 (Extinción de Incendio dentro del CPD)	Bajo	Bajo
ID_0024	Teclados y ratones	Bajo	Media
ID_0025	Repetidores	Alto	Media
ID_0027	Acceso a internet	Alto	Media
ID_0028	VPN	Alto	Media
ID_0029	DMZ	Alto	Media

Consecuencia del paso del tiempo

Degradación de los soportes de almaecnamiento de la información[I.10]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0001	Ubuntu Server	Alto	Media
ID_0002	Windows Server 2016	Alto	Media
ID_0003	Servidor de correo	Medio	Bajo
ID_0004	Directorio Activo	Medio	Bajo
ID_0005	SQL Server 2014	Alto	Bajo
ID_0006	Exchange	Bajo	Bajo
ID_0015	PC's	Bajo	Bajo
ID_0016	Servidores Blade y Armarios Rack	Alto	Media
ID_0019	CPD	Alto	Alto
ID_0021	Servidor NAS	Alto	Media
ID_0022	Disco dedicado	Alto	Media

Equivocaciones de las personas cuando usan los servicios, datos, etc.
Equivocaciones de personas con responsabilidades de instalación y operación

ERRORES EN LOS USUARIOS Y EN LA ADMINISTRACIÓN [E.1 y E.2]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0001	Ubuntu Server	Medio	Bajo
ID_0002	Windows Server 2016	Medio	Bajo
ID_0003	Servidor de Correo	Medio	Bajo
ID_0004	Directorio Activo	Medio	Bajo
ID_0005	Exchange	Medio	Bajo
ID_0006	SQL Server 2014	Alto	Bajo
ID_0007	Datos de los trabajadores de la empresa	Medio	Medio
ID_0008	Datos de los clientes	Medio	Medio
ID_0009	Datos de los proveedore	Medio	Medio
ID_0010	Modelos d arquitectura y seguridad	Alto	Medio
ID_0015	Profesionales	Medio	Alto
ID_0016	Tecnicos	Medio	Alto
ID_0017	Administrativos	Medio	Alto
ID_0026	Dispositivos para empleados	Medio	Medio
ID_0030	CPD	Alto	Medio
ID_0031	Oficina	Medio	Medio

Acciones descoordinadas, errores por omisión, etc.

DEFICIENCIAS EN LA ORGANIZACIÓN [E.7]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0001	Ubuntu Server	Medio	Bajo
ID_0002	Windows Server 2016	Medio	Bajo
ID_0003	Servidor de Correo	Medio	Bajo
ID_0004	Directorio Activo	Medio	Bajo
ID_0005	Exchange	Medio	Bajo
ID_0006	SQL Server 2014	Medio	Bajo

Incontinencia verbal, medios electrónicos, soporte papel, etc

FUGAS DE INFORMACIÓN [E.19]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0003	Servidor de correo	Medio	Bajo
ID_0007	Datos de los trabajadores de la empresa	Medio	Bajo
ID_0008	Datos de los clientes	Alto	Medio
ID_0009	Datos de los proveedores	Alto	Medio
ID_0011	Modelos y arquitecturas de la seguridad	Alto	Medio
ID_0012	Diagrama de red de la organización	Medio	Bajo
ID_0029	DMZ	Alto	Bajo
ID_0030	CPD	Alto	Bajo

Defectos en el código que propician a una operación defectuosa sin intención por parte del usuario.

VULNERABILIDADES DE LOS PROGRAMAS [E.20]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0013	Programas Python	Medio	Bajo
ID_0014	Programas Java	Medio	Bajo

Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE LOS PROGRAMAS (SOFTWARE) [E.21]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0013	Programas Python	Alto	Medio
ID_0014	Programas Java	Alto	Medio

Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.

ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE EQUIPOS (HARDWARE) [E.22]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0001	Ubuntu Server	Alto	Bajo
ID_0002	Windows Server 2016	Alto	Bajo
ID_0003	Servidor de Correo	Alto	Bajo
ID_0004	Directorio Activo	Alto	Bajo
ID_0005	Exchange	Alto	Bajo
ID_0006	SQL Server 2014	Alto	Bajo
ID_0018	PC's	Medio	Media
ID_0019	Modem	Alto	Media
ID_0020	Switch	Alto	Media
ID_0021	Servidores Blade y armarios Rack (CPD)	Medio	Media
ID_0022	Máquinas refrigeradoras de ambiente	Alto	Media
ID_0023	Gas Novec 1230 (Extinción de Incendio dentro del CPD)	Alto	Media
ID_0024	Teclados y ratones	Bajo	Media
ID_0025	Repetidores	Bajo	Media
ID_0026	Dispositivos para empleados	Alto	Media

Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.

DESTRUCCION DE INFORMACIÓN [A.18]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0001	Ubuntu Server	Medio	Bajo
ID_0002	Windows Server 2016	Medio	Bajo
ID_0003	Servidor de Correo	Medio	Bajo
ID_0004	Directorio Activo	Medio	Bajo
ID_0005	Exchange	Medio	Bajo
ID_0006	SQL Server 2014	Alto	Bajo
ID_0007	Datos de los trabajadores de la empresa	Alto	Bajo
ID_0008	Datos de los clientes	Alto	Bajo
ID_0009	Datos de los proveedore	Alto	Medio
ID_0010	Modelos d arquitectura y seguridad	Alto	Medio
ID_0026	Dispositivos para empleados	Medio	Medio
ID_0030	CPD	Alto	Medio

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

DENEGACIÓN DEL SERVICIO O CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECUERSOS [A.24]			
Id.Activo	Nombre Activo	Impacto	Probabilidad
ID_0001	Ubuntu Server	Alto	Medio
ID_0002	Windows Server 2016	Alto	Medio
ID_0003	Servidor de Correo	Alto	Medio
ID_0004	Directorio Activo	Alto	Medio
ID_0005	Exchange	Alto	Medio
ID_0006	SQL Server 2014	Alto	Medio
ID_0018	PC's	Bajo	Bajo
ID_0027	Acceso a internet	Bajo	Bajo
ID_0029	DMZ	Alto	Bajo

2.3. Riesgos

Ahora para cada amenaza detectada anteriormente, vamos a elaborar una tabla de riesgos, en la cual analizaremos la probabilidad e impacto, así como el riesgo total que representa para cada uno de los activos. Para este último campo usamos la tabla inferior.

Nivel de Riesgo			
Probabilidad	**Impacto**		
	Bajo	**Medio**	**Alto**
Alta	Bajo	Medio	Alto
Media	Bajo	Medio	Medio
Baja	Bajo	Bajo	Bajo

Vamos a seguir el mismo orden que en el apartado de amenazas, empezando con la amenaza de fuego y terminando con la denegación del servicio o caida del sistema por agotamiento de recursos.

Probabilidad de que una amenaza de daños por fuego se materialice y provoque daños en un activo o sistema.

ANÁLISIS DE RIESGOS - RIESGO FUEGO [ID_0001]				
ID Activo	Activo	Probabilidad	Impacto	Riesgo
ID_0001	Ubuntu Server	Baja	Alto	Bajo
ID_0002	Windows Server 2016	Baja	Alto	Bajo
ID_0003	Servidor de correo	Baja	Alto	Bajo
ID_0004	Directorio Activo	Baja	Alto	Bajo
ID_0005	SQL Server 2014	Baja	Alto	Bajo
ID_0006	Exchange	Baja	Alto	Bajo
ID_0015	PC's	Baja	Alto	Bajo
ID_0016	Modem	Baja	Alto	Bajo
ID_0017	Switch	Baja	Alto	Bajo
ID_0019	Servidores Blade y Armarios Rack	Baja	Alto	Bajo
ID_0021	Servidor NAS	Baja	Alto	Bajo
ID_0022	Disco dedicado	Baja	Medio	Bajo
ID_0024	Repetidores	Baja	Medio	Bajo
ID_0029	CPD	Baja	Medio	Bajo
ID_0030	Oficina	Baja	Medio	Bajo

Probabilidad de que una amenaza de daños por agua se materialice y provoque daños en un activo o sistema.

ANÁLISIS DE RIESGOS - AGUA [ID_0002]				
Id.Activo	Nombre Activo	Impacto	Probabilidad	Riesgo
ID_0001	Ubuntu Server	Alto	Bajo	Bajo
ID_0002	Windows Server 2016	Alto	Bajo	Bajo
ID_0003	Servidor de correo	Alto	Bajo	Bajo
ID_0004	Directorio Activo	Alto	Bajo	Bajo
ID_0005	SQL Server 2014	Alto	Bajo	Bajo
ID_0006	Exchange	Bajo	Bajo	Bajo
ID_0015	PC's	Bajo	Bajo	Bajo
ID_0016	Modem	Bajo	Bajo	Bajo
ID_0017	Switch	Bajo	Bajo	Bajo
ID_0019	Servidores Blade y Armarios Rack	Alto	Bajo	Bajo
ID_0021	Servidor NAS	Alto	Bajo	Bajo
ID_0022	Disco dedicado	Medio	Bajo	Bajo
ID_0024	Repetidores	Medio	Bajo	Bajo
ID_0029	CPD	Medio	Bajo	Bajo
ID_0030	Oficina	Medio	Bajo	Bajo

Probabilidad de que se produzcan daños en los equipos y sistemas debido al corte del suministro eléctrico.

ANÁLISIS DE RIESGOS - RIESGO CORTE SUMINISTRO ELECTRICO [ID_0003]				
ID Activo	Activo	Probabilidad	Impacto	Riesgo
ID_0001	Ubuntu Server	Media	Alto	Medio
ID_0002	Windows Server 2016	Media	Alto	Medio
ID_0003	Servidor de Correo	Media	Alto	Medio
ID_0004	Directorio Activo	Media	Alto	Medio
ID_0005	Exchange	Media	Alto	Medio
ID_0006	SQL Server 2014	Media	Alto	Medio
ID_0007	Datos de los trabajadores de la empresa	Media	Alto	Medio
ID_0008	Datos de los clientes	Media	Alto	Medio
ID_0009	Datos de los proveedores	Media	Alto	Medio
ID_0010	Modelos de arquitectura y seguridad	Media	Alto	Medio
ID_0011	Modelos y arquitecturas de la seguridad	Media	Alto	Medio
ID_0012	Diagrama de red de la organización	Media	Alto	Medio
ID_0013	Programas Python	Media	Bajo	Bajo
ID_0014	Programas Java	Media	Bajo	Bajo
ID_0018	PC's	Media	Alto	Medio
ID_0019	Modem	Media	Alto	Medio
ID_0020	Switch	Media	Alto	Medio
ID_0021	Servidores Blade y armarios Rack (CPD)	Media	Alto	Medio
ID_0022	Máquinas refrigeradoras de ambiente	Media	Alto	Medio
ID_0023	Gas Novec 1230 (Extinción de Incendio c	Bajo	Bajo	Bajo
ID_0024	Teclados y ratones	Media	Bajo	Bajo
ID_0025	Repetidores	Media	Alto	Medio
ID_0027	Acceso a internet	Media	Alto	Medio
ID_0028	VPN	Media	Alto	Medio
ID_0029	DMZ	Media	Alto	Medio

Probabilidad de que se produzcan daños en los sistemas y perdidas de información debido a la degradación de los soportes de almacenamiento de información.

ANÁLISIS DE RIESGOS - DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE INFORMACIÓN [ID_0004]				
ID Activo	Activo	Probabilidad	Impacto	Riesgo
ID_0001	Ubuntu Server	Alto	Medio	Medio
ID_0002	Windows Server 2016	Alto	Medio	Medio
ID_0003	Servidor de correo	Medio	Bajo	Bajo
ID_0004	Directorio Activo	Medio	Bajo	Bajo
ID_0005	SQL Server 2014	Alto	Bajo	Bajo
ID_0006	Exchange	Bajo	Bajo	Bajo
ID_0015	PC's	Bajo	Bajo	Bajo
ID_0016	Servidores Blade y Armarios Rack	Alto	Medio	Medio
ID_0019	CPD	Alto	Alto	Alto
ID_0021	Servidor NAS	Alto	Medio	Medio
ID_0022	Disco dedicado	Alto	Medio	Medio

Probabilidad de que se produzcan daños en los sistemas y perdidas de información debido a errores de los trabajadores de la empresa.

ANÁLISIS DE RIESGOS - ERROR EN LOS USUARIOS Y ADMINISTRACIÓN [ID_0005]				
ID Activo	Activo	Probabilidad	Impacto	Riesgo
ID_0001	Ubuntu Server	Bajo	Medio	Bajo
ID_0002	Windows Server 2016	Bajo	Medio	Bajo
ID_0003	Servidor de Correo	Bajo	Medio	Bajo
ID_0004	Directorio Activo	Bajo	Medio	Bajo
ID_0005	Exchange	Bajo	Medio	Bajo
ID_0006	SQL Server 2014	Bajo	Alto	Bajo
ID_0007	Datos de los trabajadores de la empresa	Medio	Medio	Medio
ID_0008	Datos de los clientes	Medio	Medio	Medio
ID_0009	Datos de los proveedore	Medio	Medio	Medio
ID_0010	Modelos d arquitectura y seguridad	Medio	Alto	Medio
ID_0015	Profesionales	Alto	Medio	Medio
ID_0016	Tecnicos	Alto	Medio	Medio
ID_0017	Administrativos	Alto	Medio	Medio
ID_0026	Dispositivos para empleados	Medio	Medio	Medio
ID_0030	CPD	Medio	Alto	Medio
ID_0031	Oficina	Medio	Medio	Medio

Probabilidad de que se produzcan daños en los equipos y sistemas debido a acciones descoordinadas, errores por omisión...

ANÁLISIS DE RIESGOS - DEFICIENCIAS EN LA ORGANIZACIÓN [ID_0006]				
ID.Activo	Nombre Activo	Impacto	Probabilidad	Riesgo
ID_0001	Ubuntu Server	Medio	Bajo	Bajo
ID_0002	Windows Server 2016	Medio	Bajo	Bajo
ID_0003	Servidor de Correo	Medio	Bajo	Bajo
ID_0004	Directorio Activo	Medio	Bajo	Bajo
ID_0005	Exchange	Medio	Bajo	Bajo
ID_0006	SQL Server 2014	Medio	Bajo	Bajo

Probabilidad de que se produzcan daños a la empresa debido a Incontinencia verbal, medios electrónicos, soporte papel, etc.

ANÁLISIS DE RIESGOS - FUGA INFORMACION [ID_0007]				
ID Activo	Activo	Probabilidad	Impacto	Riesgo
ID_0003	Servidor de correo	Bajo	Medio	Bajo
ID_0007	Datos de los trabajadores de la empresa	Bajo	Medio	Bajo
ID_0008	Datos de los clientes	Medio	Alto	Medio
ID_0009	Datos de los proveedores	Medio	Alto	Medio
ID_0011	Modelos y arquitecturas de la seguridad	Medio	Alto	Medio
ID_0012	Diagrama de red de la organización	Bajo	Medio	Bajo
ID_0029	DMZ	Bajo	Alto	Bajo
ID_0030	CPD	Bajo	Alto	Bajo

Probabilidad de que se produzcan daños en los sistemas debido a defectos en el código.

ANÁLISIS DE RIESGOS - VULNERABILIDADES DE LOS PROGRAMAS [ID_0008]				
ID.Activo	Nombre Activo	Impacto	Probabilidad	Riesgo
ID_0013	Programas Python	Medio	Bajo	Bajo
ID_0014	Programas Java	Medio	Bajo	Bajo

Probabilidad de que se produzcan daños en los sistemas debido defectos en los procedimientos.

ANÁLISIS DE RIESGOS - ERROR MANTENIMIENTO/ACTUALIZACION [ID_0009]				
ID Activo	Activo	Probabilidad	Impacto	Riesgo
ID_0013	Programas Python	Medio	Medio	Medio
ID_0014	Programas Java	Medio	Medio	Medio

Probabilidad de que se produzcan daños en los sistemas debido defectos en los procedimientos.

ANÁLISIS DE RIESGOS - ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE EQUIPOS (HARDWARE) [ID_0010]				
ID.Activo	Nombre Activo	Impacto	Probabilidad	Riesgo
ID_0001	Ubuntu Server	Alto	Bajo	Bajo
ID_0002	Windows Server 2016	Alto	Bajo	Bajo
ID_0003	Servidor de Correo	Alto	Bajo	Bajo
ID_0004	Directorio Activo	Alto	Bajo	Bajo
ID_0005	Exchange	Alto	Bajo	Bajo
ID_0006	SQL Server 2014	Alto	Bajo	Bajo
ID_0018	PC's	Medio	Medio	Medio
ID_0019	Modem	Alto	Medio	Medio
ID_0020	Switch	Alto	Medio	Medio
ID_0021	Servidores Blade y armarios Rack (CPD)	Medio	Medio	Medio
ID_0022	Máquinas refrigeradoras de ambiente	Alto	Medio	Medio
ID_0023	Gas Novec 1230 (Extinción de Incendio dentro del CPD)	Alto	Medio	Medio
ID_0024	Teclados y ratones	Bajo	Medio	Bajo
ID_0025	Repetidores	Bajo	Medio	Bajo
ID_0026	Dispositivos para empleados	Alto	Medio	Medio

Probabilidad de que se produzcan daños en los sistemas debido a la eliminación intencional de información.

ANÁLISIS DE RIESGOS - DESTRUCCIÓN INFORMACIÓN [ID_0011]				
ID Activo	Activo	Probabilidad	Impacto	Riesgo
ID_0001	Ubuntu Server	Bajo	Medio	Bajo
ID_0002	Windows Server 2016	Bajo	Medio	Bajo
ID_0003	Servidor de Correo	Bajo	Medio	Bajo
ID_0004	Directorio Activo	Bajo	Medio	Bajo
ID_0005	Exchange	Bajo	Medio	Bajo
ID_0006	SQL Server 2014	Bajo	Alto	Bajo
ID_0007	Datos de los trabajadores de la empresa	Bajo	Alto	Bajo
ID_0008	Datos de los clientes	Bajo	Alto	Bajo
ID_0009	Datos de los proveedore	Medio	Alto	Medio
ID_0010	Modelos d arquitectura y seguridad	Medio	Alto	Medio
ID_0026	Dispositivos para empleados	Medio	Medio	Medio

Probabilidad de que se produzcan daños en los equipos e información debido a la caída del sistema.

ANÁLISIS DE RIESGOS - DENEGACIÓN DEL SERVICIO O CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECUERSOS [ID_0012]				
ID.Activo	Nombre Activo	Impacto	Probabilidad	Riesgo
ID_0001	Ubuntu Server	Alto	Medio	Medio
ID_0002	Windows Server 2016	Alto	Medio	Medio
ID_0003	Servidor de Correo	Alto	Medio	Medio
ID_0004	Directorio Activo	Alto	Medio	Medio
ID_0005	Exchange	Alto	Medio	Medio
ID_0006	SQL Server 2014	Alto	Medio	Medio
ID_0018	PC's	Bajo	Bajo	Bajo
ID_0027	Acceso a internet	Bajo	Bajo	Bajo
ID_0029	DMZ	Alto	Bajo	Bajo

2.4. Salvaguardas (contramedidas)

Definir las salvaguardas entendidas como "aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo de un sistema de información". Habrá que tener en cuenta que existen salvaguardas que buscan reducir el impacto, es decir, limitar la degradación causada por una amenaza sobre un activo, mientras que otras se centran en reducir la probabilidad de que una amenaza se materialice y así reducir su riesgo.

SALVAGUARDAS:

1. RIESGO POR FUEGO [ID_0001]:

1.1. Reducción de impacto:

1.1.1. Instalación de detectores de humo y alarma en las instalaciones.

1.1.2. Proveer al personal con una pequeña formación sobre qué hacer en caso de incendio y con material de extinción de estos.

1.1.3. Asegurarse de que los productos y materiales que puedan ser inflamables estén almacenados en lugares preparados para que el impacto sea el menor posible.

1.1.4. Establecer un plan de respuesta, asignando responsables y protocolos a seguir.

1.2. Prevención del riesgo:

1.2.1. Hacer inspecciones periódicas de las instalaciones eléctricas y del gas.

1.2.2. Contratar una empresa de mantenimiento que controle la probabilidad de estos riesgos.

1.2.3. Tras estudiar los riesgos y activos, realizar un plan de prevención adecuado estableciendo responsables y protocolos a seguir para poder evitar estos incendios.

2. RIESGO POR AGUA [ID_0002]:

2.1. Reducción de impacto:

2.1.1. Instalar detectores de humedad por el/los edificios de la empresa para, en caso de inundación o goteras, poder enterarnos lo antes posible y reducir al máximo el impacto.

2.1.2. Establecer un plan de reducción de impacto en el caso de inundación. Este plan podrá incluir protocolos como una desactivación escalada y controlada de la electricidad, un protocolo de actuación para los empleados y un plan de contingencia para proteger los equipos y datos presentes en las instalaciones y poder retomar la actividad normal de la empresa cuanto antes.

2.1.3. Contratar una empresa que asegure los posibles daños causados por una amenaza de este tipo (aplicable también al riesgo con ID_0001).

2.1.4. Tener toda la información de la empresa guardada en un lugar externo a esta ya sea un CPD, nube o cualquier instalación preparada para almacenar esas cantidades de datos. De esta manera, si ocurre un incidente por agua tendremos toda la información en un lugar seguro.

2.2. Prevención:

2.2.1. Realizar pruebas periódicamente de los sistemas de alarma de agua, instalaciones de tuberías y cualquier estructura que tenga riesgo de provocar una inundación.

3. RIESGO DE CORTE DE SUMINISTRO ELÉCTRICO [ID_0003]

3.1. Reducción de impacto:

3.1.1. Tener un SAI (Sistema de Alimentación Interrumpida). Con uno de estos no conseguiremos un impacto de 0 ya que, normalmente, están preparados para suministrar energía a un número limitado de dispositivos. Por lo tanto, le usaremos para suministrar energía a los dispositivos, servidores o PCs que más pérdidas pueden provocar a la empresa. Con esto reduciremos el impacto bastante.

3.1.2. Tener un plan de contingencia para que, en caso de corte del suministro eléctrico, podamos salvar el máximo número de datos y servicios en el menor tiempo posible.

3.1.3. Realizar pruebas periódicas para “observar y entrenar” el comportamiento de los servidores y dispositivos y poder armar un procedimiento que debe seguir la red de dispositivos cuando ocurra un corte de este estilo. Este procedimiento dictaría, por ejemplo, de qué manera tienen que migrar la información unos servidores a otros para perder el menor número de esta o nada de info. Realizar un simulacro de este cada cierto tiempo para observar que se sigue este procedimiento planificado.

3.2. Prevención:

3.2.1. Comprobación cada poco tiempo del estado de las terminales físicas del suministro eléctrico con su correspondiente mantenimiento para evitar este tipo de cortes.

3.2.2. Contratación de una empresa externa que se encargue de suministrar electricidad a toda la empresa en caso de que ocurra un corte en la fuente principal. Además, podríamos combinar esta mediad con anteriores

comentadas como un SAI que, durante el periodo en el que está cortada la fuente de electricidad principal y se activa la secundaria (empresa comentada en este apartado) suministre electricidad hasta que llegue la proporcionada por esta fuente secundaria. Esto se podría considerar como mediad de reducción de impacto, pero al hacer 0 impacto y que parezca que no ha habido ningún corte, la pondremos en este apartado.

4. DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE INFORMACIÓN [ID_0004]

4.1. Reducción de impacto:

4.1.1. Realizar copias de seguridad a menudo en lugares seguros para evitar la pérdida de estos datos.

4.1.2. Utilizar herramientas de recuperación de datos que nos ayuden a recuperar parte de la información.

4.1.3. Un sistema de almacenamiento en red sería buena opción para reducir el impacto en caso de fallo de alguno de estos soportes. De esta manera, tendremos parte de la información almacenada en la nube. Esto trae más ventajas como la posibilidad de acceder a la información desde cualquier dispositivo cuando queramos.

4.2. Prevención:

4.2.1. Si utilizamos soportes de almacenamiento de alta calidad y con las últimas tecnologías, podremos evitar que ocurran estos errores a menudo.

4.2.2. De la misma manera que en anteriores riesgos, si realizamos un mantenimiento periódico de estos soportes, podremos evitar o ver venir un error de este tipo.

4.2.3. El lugar en el que almacenemos estos soportes debe ser un lugar adecuado. Un sitio fresco, seco y lejos de fuentes de calor.

5. ERROR EN LOS USUARIOS Y ADMINISTRACIÓN [ID_0005]

5.1. Reducción de impacto:

5.1.1. Una vez ha ocurrido el error, deberíamos identificada la causa del error, implementar medidas para minimizar el impacto y asegurarse de que no vuelve a ocurrir.

5.1.2. Al igual que en el anterior riesgo, es adecuado tener un sistema de recuperación de datos o un protocolo de seguridad que consigue recuperar

parte de los datos que pueden haberse perdido en ese error.

5.1.3. Es adecuado notificar a las personas afectadas por el error para que tengan conocimiento de lo que está ocurriendo y tranquilizar en la mayor medida a estas personas.

5.1.4. Es importante revisar y mejorar los procedimientos existentes para evitar que se produzcan errores en el futuro y reducir el riesgo de que se produzcan daños similares en el futuro.

5.2. Prevención:

5.2.1. Lo mejor para evitar estos errores es asegurarse de que las personas que usan los servicios estén capacitadas y conozcan cómo utilizarlos correctamente puede reducir el riesgo de equivocarse.

5.2.2. Conseguir un diseño más intuitivo y sencillo de los servicios para que los usuarios entiendan mejor la interfaz y les sea más complicado cometer este tipo de errores.

5.2.3. Implementar un sistema de validación de datos para las contraseñas y correos de los usuarios.

5.2.4. Los controles de acceso son muy importantes para evitar que personas no autorizadas o inadecuadamente capacitadas tengan acceso a los servicios y cometan errores.

5.2.5. Monitorización del estado de los usuarios y supervisión para comprobar los errores que puedan ocurrir.

6. DEFICIENCIAS EN LA ORGANIZACIÓN [ID_0006]

6.1. Reducción de impacto:

6.1.1. Realizar un estudio del alcance del daño causado junto con la magnitud de este. Con esto podremos determinar las medidas necesarias para reducir el impacto.

6.1.2. Una vez hecho este estudio, debemos realizar un plan de acción con diferentes medidas para mitigar el impacto.

6.1.3. Tener rapidez a la hora de tomar las medidas. Podríamos tener un horario para indicar cuando se deberían realizar las medidas, intentando realizarlas lo antes posible.

6.1.4. Monitorización del progreso de las medias habladas anteriormente.

6.1.5. Derivado de la monitorización, actualización del plan cuando sea necesario. A veces no vemos las cosas igual al principio que cuando llevamos ciertas medidas implementadas y es necesario cambiar el plan.

6.2. Prevención:

6.2.1. Establecer roles en el personal y un sistema o soporte de comunicación estable.

6.2.2. Monitorizar las acciones de los miembros en el equipo y dar feedback sobre correcciones que se podrían llevar a cabo y actualizaciones de los procedimientos del personal.

6.2.3. Relacionado también con el establecimiento de roles, debemos implementar un sistema de escalado de decisiones. De esta manera se repartirá la responsabilidad de las distintas tareas o decisiones.

6.2.4. Debemos proporcionar a todos los miembros del equipo la capacitación y el adiestramiento necesario para que sepan cómo cumplir con sus responsabilidades y tomar decisiones de manera efectiva y eficiente.

7. FUGA DE INFORMACIÓN [ID_0007]

7.1. Reducción de impacto:

7.1.1. De nuevo, lo más adecuado al principio es estudiar y analizar el alcance de la filtración para la elaboración de un plan de acción con medidas específicas para mitigar el impacto. Tras analizar este alcance, si estamos hablando de un impacto potencialmente peligroso tomaríamos medidas inmediatas. Monitorear y actualizar estas medidas es algo fundamental.

7.2. Prevención:

7.2.1. Establecer políticas de seguridad que restrinjan el acceso a la información cierto tipo de perfiles y permitan el acceso a otros. Con esto conseguiremos tener un mayor control de la información.

7.2.2. Es necesario implementar medidas de seguridad física y lógica para proteger la información confidencial, como cifrado, autenticación de usuarios, control de acceso y registro de actividades.

7.2.3. Entrenar y capacitar al personal con técnicas o procedimientos de seguridad para proteger la información.

7.2.4. Realizar pruebas y auditorías periódicas de seguridad de la información para identificar posibles vulnerabilidades y tomar medidas para corregirlas.

Estas pruebas pueden ser de pentesting, pruebas de penetración, auditorías (pruebas de caja negra, gris y blanca) o incluso de ingeniería social con los propios empleados.

8. VULNERABILIDADES DE LOS PROGRAMAS [ID_0008]

8.1. Reducción de impacto:

8.1.1. De nuevo lo primero que hay que hacer es el análisis del alcance, el plan de acción y la monitorización y actualización de este.

8.1.2. Tener una herramienta o contratar a una empresa que se encargue de la posible recuperación de los datos perdidos en el ataque. Por ejemplo, si nos han introducido un ransomware por una vulnerabilidad de uno de estos programas, poder frenar el ataque y recuperar la información secuestrada.

8.2. Prevención:

8.2.1. Realizar pruebas y validaciones del código, utilizando técnicas y herramientas adecuadas para detectar y corregir posibles errores.

8.2.2. Establecer un proceso de revisión y aprobación riguroso para garantizar que el código cumpla con todos los estándares y requisitos, y que, en el caso de violar alguno de estos estándares, se corrija antes de su implementación.

8.2.3. Proporcionar a todos los miembros del equipo la capacitación y el adiestramiento para que sepan cómo escribir y revisar código y cumplir con los estándares y requisitos necesarios.

8.2.4. Utilizar software seguro en su última versión. Asegurarse de que todos los programas utilizados son de marcas reconocidas, de confianza y tienen las ultimas actualizaciones.

9. ERROR MANTENIMIENTO/ACTUALIZACIÓN [ID_0009]

9.1. Reducción de impacto:

9.1.1. Primero, determinaremos la causa raíz del problema mediante la documentación del software, pruebas y hacer preguntas al fabricante.

9.1.2. Si hay una vulnerabilidad en el software, toma medidas inmediatas para proteger los datos y el sistema. Esto puede incluir desconectar el software de la red, deshabilitar cualquier función vulnerable, cerrar sesiones de los usuarios o deshabilitar todas las funciones durante periodos medios/cortos de tiempo.

9.1.3. Si el problema afecta a varios usuarios o a una parte importante del sistema, es importante notifícales y asegurarse de que están al tanto de la situación, informarles de lo que se va a hacer con tranquilidad y de cómo se está manejando.

9.1.4. Una vez localizado el error/vulnerabilidad que nos está causando tantos problemas, de debe parchear. Esto, de nuevo, puede incluir deshabilitar ciertos servicios para poder parchear bien el error y que no vuelva a ocurrir. Tras aplicar el parche debe monitorearse el funcionamiento del servicio y realizarse ciertas pruebas para comprobar que realmente hemos arreglado el problema.

9.2. Prevención:

9.2.1. Tener un control de versiones de calidad. Esto implica la creación de un registro de todas las versiones del software y la documentación de cualquier actualización o parche aplicado. Esto nos permite controlar el uso de versiones obsoletas o defectuosas del software.

9.2.2. Antes de actualizar, asegurarse de que todo funciona bien y la actualización no va a provocar problemas en otras partes del sistema mediante numerosas pruebas.

9.2.3. Utilizar medidas de seguridad adicionales como firewalls, prevención de intrusiones, encriptar los datos, contraseñas seguras, etc. Esto también es aplicable al riesgo anterior (ID_0009).

9.2.4. Asegurarse de que los usuarios saben cómo usar correctamente el software.

9.2.5. Mantenerse en contacto con el fabricante del software y asegurarse de que estén al tanto de cualquier problema o problema que hayas identificado. Esto puede ayudar a que el fabricante se dé cuenta de problemas conocidos y les parchee.

10. ERROR MANTENIMIENTO/ACTUALIZACIÓN EQUIPOS HARDWARE[ID_0010]

10.1. Reducción de impacto:

10.1.1. Es importante realizar copias de seguridad de los datos antes de intentar solucionar el problema para minimizar el riesgo de pérdida de información.

10.1.2. Implementar un plan de contingencia para minimizar el impacto del fallo en la organización y garantizar la continuidad del negocio.

10.1.3. Si es posible, intentar reparar el equipo para recuperar la información y

poder seguir usándole si es posible. Si no es posible repararle, lo más conveniente es reemplazarle tras intentar extraer la información que había en el anterior.

10.2. Prevención:

10.2.1. Realizar mantenimientos periódicos para evitar que los equipos estén en malas condiciones. Un buen ejemplo es extraer el polvo o partículas atrapadas dentro de los PCs una vez cada año/dos años.

10.2.2. Dentro de la capacidad adquisitiva de la empresa, es importante utilizar equipos de alta calidad que hayan sido probados y certificados por el fabricante para garantizar su confiabilidad y durabilidad.

11. DESTRUCCIÓN INFORMACIÓN[ID_0011]

11.1. Reducción de impacto:

11.1.1. Básicamente lo más importante y lo que va a reducir el impacto en mayor medida es la realización de copias de seguridad de la información. Si el riesgo se ha producido, lo que mejor te puede salvar es tener una copia de todo en otra máquina o en la nube.

11.1.2. De nuevo, se puede utilizar software de recuperación de datos para intentar recuperar parte de los datos o la totalidad de estos. Si no se dispone de estas herramientas, se puede llamar a un experto especializado en este tipo de casos de recuperación de información.

11.2. Prevención:

11.2.1. Establecer políticas de seguridad de la información que prohíban la eliminación intencional de información y establezcan consecuencias para las personas que no cumplan con estas políticas.

11.2.2. Utilizar software o monitorizar a mano el acceso a la información para asegurarse de que todos los individuos que accedan a ella sean de fiar y, si alguno de los empleados destruye información intencionalmente, saber quien ha sido y como lo ha hecho.

11.2.3. Utilizar contraseñas seguras y cambiarlas regularmente puede proteger la información contra el acceso no autorizado y evitar la eliminación intencional de ella.

12. DENEGACIÓN DE SERVICIO O CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOSID_0012]

12.1. Reducción de impacto:

12.1.1. Es importante encontrar la causa raíz del problema. Esto puede incluir un análisis de distintas partes como la carga de trabajo, los recursos y la configuración.

12.1.2. Si es posible, se pueden aumentar temporalmente los recursos del sistema, como la memoria o el ancho de banda, para ayudar a manejar la carga de trabajo y tener un margen para mitigar el ataque, en el caso de que el problema sea causado por esto.

12.1.3. Intentar equilibrar la carga de trabajo para liberar los dispositivos que están saturados.

12.1.4. Estudiar los límites de los dispositivos y establecer un límite de carga de trabajo para que el sistema no llegue a la sobrecarga.

12.1.5. Es importante comunicar a los usuarios lo sucedido y proporcionarles información sobre cómo se está abordando el problema y cuándo se espera que el sistema vuelva a estar disponible. Esto se debe hacer con tranquilidad e intentando evitar que cunda el pánico.

12.2. Prevención:

12.2.1. Al igual que se puede hacer cuando se ha producido la sobrecarga, el se puede equilibrar la carga de trabajo antes de que se produzca esta. Para esto sería adecuado armar un protocolo de actuación que prevea esta sobrecarga e inmediatamente equilibre la carga de trabajo.

12.2.2. Utilizar más a menudo las cachés ya que nos permiten obtener datos rápidamente sin tener que estar constantemente accediendo al servicio.

12.2.3. Se puede dividir una aplicación en múltiples microservicios pequeños y autónomos. De esta manera cada uno de ellos puede ser escalado de forma independiente, lo que permite una mejor gestión de la carga de trabajo.

12.2.4. Utilizar la nube proporciona una gran cantidad de recursos a disposición y permite aumentar o disminuir la cantidad de recursos utilizados según sea necesario para manejar la carga de trabajo. Además, proporciona varias ventajas ya habladas anteriormente.

12.2.5. Utilizar diferentes técnicas de optimización para que el rendimiento mejore. Pueden ser cambios en el código, ayudas a la paralelización, etc.

12.2.6. Monitorizar los posibles cuellos de botella que puedan surgir y tomar medidas para abordarlos antes de que se conviertan en un problema grave.