MEMORIA

Análisis de Riesgos como parte de un SGSI

Laura Bezanilla

GARANTÍA Y SEGURIDAD DE LA INFORMACIÓN

18 de diciembre de 2022

Universidad de Valladolid

Índice

1. Características del Sistema

1.1. Panorámica del Sistema

Se trata de una empresa pequeña del sector Topografía y Geodesia, con tres profesionales de campo, dos técnicos y un 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 distribuidos en varias zonas: oficina, área de trabajo, sala de servidores, almacén, zona de café o 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 un 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 otro de almacenamiento tanto en disco dedicado como en NAS, todos ellos se ubican 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 todas las instalaciones. Sin embargo, no tiene programado ni firewall, ni proxy.

Por otro lado, la distribución del cable a los equipos se realiza a través de un switch de 24 puertos, el cual no tiene ningún tipo de gestión.

Finalmente, la comunicación vía wifi se realiza directamente al router que está protegido con una clave de tipo WPA2.

1.2. Política

A continuación, se describen las diferentes directrices y objetivos generales, que en relación con la seguridad, guían a la compañía:

- 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 de la empresa 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 toda 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 los medios necesarios para los planes de seguridad, nombrar al resto de los responsables e impulsar la política de seguridad en toda la empresa.

1.3.2. Comité de seguridad

El comité de seguridad estará compuesto por diferentes directivos con una buena capacidad de decisión con el objetivo de cubrir 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 del Director de IT
Responsable de línea de negocio	Director de Operaciones Director Técnico (I+D+i) Director de Diseño

Entre sus funciones están la aprobación de la política de seguridad propuesta 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, además de 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 principal responsable de que funcionen correctamente los diferentes sistemas informáticos dentro de la empresa.

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

Todos los usuarios deben usar los diferentes sistemas informáticos a su disposición 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 de los trabajadores.
- Servidor NAS. Se almacenan los diseños de los productos, los catálogos comerciales, las fotometrías, etc.
- 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 es donde se encuentra el servidor Web.
- Windows Server 2016. Aquí está el servidor de correo, Exchange, y el Directorio Activo.
- Estaciones de trabajo para el diseño asistido por computador, aplicaciones de gestión de datos de estaciones topográficas, etc.
- 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 norma 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:

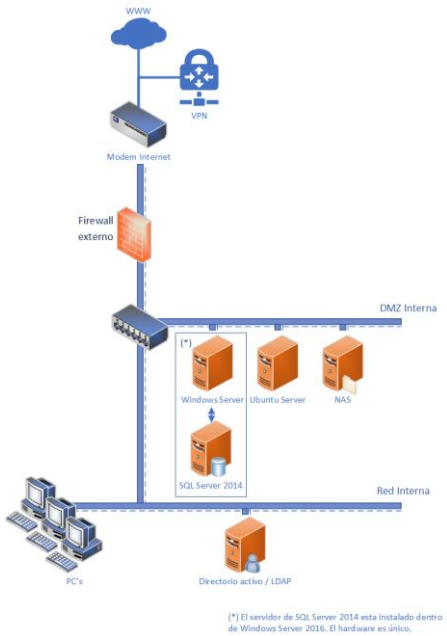

Figura 1. Arquitectura propuesta para la empresa

Se trata de una topología 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.

Por otro lado, existen 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 ha decidido instalar un servicio VPN que proporcionará a los teletrabajadores acceso seguro a los recursos internos de la empresa.

1.7. Mapa de activos

Teniendo en cuenta la situación actual de la empresa, se ha realizado un mapa de activos a considerar incluyendo sus dependencias. Ver *Tabla 1*.

2. Análisis de Riesgos y Medidas de Seguridad

2.1. Bienes de Información valiosos

2.1.1. Activos de Hardware

La empresa posee una estructura de red sencilla con un router, switch, servidores y PCs en la que prima la disponibilidad y confidencialidad frente a los datos de los servidores, a los cuales accederán los trabajadores dentro de la red interna. Por tanto, se requerirá configurar listas de acceso a los servidores para garantizar un acceso seguro a la información crítica de la compañía.

2.1.2. Activos de Servicios

La empresa aloja varios servicios. Entre ellos están un servidor NAS, un servidor SQL 2014, un Windows Server 2016, un Ubuntu Server, un servidor de correo, un servidor Exchange, un directorio activo, un servidor Web y el acceso a Internet. En todos estos servidores se prioriza la disponibilidad, aunque en el servidor SQL y NAS priman la integridad y la autenticidad. En el servidor de correo y NAS también es importante la confidencialidad. Teniendo en cuenta esta situación, un posible plan de actuación en cuanto a la disponibilidad es instalar SAIs en los servidores más importantes de la organización.

2.1.3. Activos de Datos

Entre los diferentes datos de la empresa se encuentran los diseños de productos, catálogos comerciales, fotometrías, correos electrónicos de los empleados y el historial de ventas. En todos ellos se antepone la disponibilidad y, en los diseños de productos y correos electrónicos, también la confidencialidad. Para asegurar la disponibilidad se deberán crear distintos backup de los datos para poder usarlos en caso de pérdida debido a un ataque malicioso.

INVENTARIO DE ACTIVOS								
Identificador	Código	Nombre	Tipo	Descripción	Responsable	Ubicación	Dependencias	Valor
ID_001	HW.1	PCs	Hardware	Ordenadores de los puestos de trabajo y despachos	Sistemas y Telecomunicaciones	Despachos / Oficina abierta		Medio
ID_002	HW.2	Servidores Blade	Hardware	Servidores con almacenamiento en disco dedicado y NAS	Sistemas y Telecomunicaciones	Sala Servidores		Muy Alto
ID_003	HW.3	Router doméstico	Hardware	Proporciona servicio de acceso a Internet. No cuenta ni con proxy ni con un firewall activos	Sistemas y Telecomunicaciones	Área de Trabajo		Muy Alto
ID_004	HW.4	Switch	Hardware	Switch de 24 puertos	Sistemas y Telecomunicaciones	Área de Trabajo		Alto
ID_005	HW.5	Equipos moviles de empresa	Hardware	Equipos de los empleados, que pueden llevarse a casa y traer a la oficina	Sistemas y Telecomunicaciones			Alto
ID_006	S.1	Servidor NAS	Hardware	Servidor de almacenamiento de los datos importantes de la empresa conectado a la red	Sistemas y Telecomunicaciones	Sala del CPD	HW.2	Muy Alto
ID_007	S.2	Servidor Windows Server 2016	Servicio	Servidor basado en Windows	Sistemas y Telecomunicaciones	Sala de Servidores	HW.2	Muy Alto
ID_008	S.3	Servidor SQL 2014	Servicio	Base de datos de la empresa	Sistemas y Telecomunicaciones	Sala de Servidores	HW.2	Muy Alto
ID_009	S.4	Servidor Ubuntu Server	Servicio	Servidor basado en Linux con un gran rendimiento	Sistemas y Telecomunicaciones	Sala de Servidores	HW.2	Alto
ID_010	S.5	Servidor de correo	Servicio	Ofrece soporte a los correos electrónicos de los empleados	Sistemas y Telecomunicaciones	Sala de Servidores	S.1	Alto
ID_011	S.6	Servidor Exchange	Servicio	Servidor de Microsoft Exchange	Sistemas y Telecomunicaciones	Sala de Servidores	S.1	Alto
ID_012	S.7	Directorio Activo	Servicio	Servicio de directorios en la red distribuida de ordenadores	Sistemas y Telecomunicaciones	Sala de Servidores	S.1	Medio
ID_013	S.8	Acceso a internet	Servicio	Proporcionado por el ISP	Sistemas y Telecomunicaciones	Sala de Servidores	HW.3	Alto
ID_014	S.9	Servidor Web	Servicio	Servidor web de la empresa	Sistemas y Telecomunicaciones	Sala de Servidores	S.3	Medio
ID_015	D.1	Diseños de Productos	Datos	Archivos que representan productos creados por la empresa	Responsable de línea de negocio	Sala de Servidores	S.1	Muy Alto
ID_016	D.2	Catálogos comerciales	Datos	Archivos que contienen un listado de los productos en venta	Comercial	Sala de Servidores	S.1	Bajo
ID_017	D.3	Fotometrías	Datos	Datos de mediciones de luz de objetos	Operaciones	Sala de Servidores	S.1	Medio
ID_018	D.4	Correos electrónicos	Datos	Conjunto de correos electrónicos de los trabajadores, junto con los mensajes recibidos y enviados	Sistemas y Telecomunicaciones	Sala del CPD	S.5	Muy Alto
ID_019	D.5	Historial de ventas	Datos	Información sobre las ventas efectuadas por la empresa	Administración	Sala de Servidores	S.3	Medio
ID_020	SW.1	Programas CAD / Reconstrucción 3D	Software	Porgramas instalados en los PCs de la empresa a disposición de los trabajadores		PCs	HW.1	Bajo
ID_021	SW.2	Aplicaciones de Gestión	Software	Aplicaciones que dan soporte a Operaciones y Gestión de proyectos, desarrolladas en Java y Python	Operaciones	PCs	S.4	Alto
ID_022	SW.3	VPN	Software	Permite la extension de la red local sobre una red pública	Responsable de Seguridad		HW.3	Alto
ID_023	SW.4	Aplicación de apertura de puertas	Software	Permite controlar las cerraduras electrónicas de las puertas de acceso a la empresa, almacén y sala de máquinas	Responsable de Seguridad	Móvil personal		Alto
ID_024	SW.5	Aplicaciones PLM	Software	Aplicaciones para la gestión del ciclo de vida del producto	Oficina Técnica	PCs	HW.1	Medio
ID_025	SW.6	Aplicaciones SAP	Software	Aplicaciones para la planificación de recursos empresariales	Administración	PCs	HW.1	Alto
ID_026	SW.7	Aplicaciones topográficas	Software	Aplicaciones de gestión de datos de estaciones topográficas	Operaciones	PCs	HW.1	Bajo
ID_020	P.1	Director General	Personal	Director de la empresa				Muy Alto
ID_021	P.2	Responsable de sistemas y telecom.	Personal	Forma parte del comité de seguridad, responsable del funcionamiento correcto de los sistemas informáticos	Director General			Alto
ID_022	P.3	Responsable de asesoría legal	Personal	Forma parte del comité de seguridad	Director General			Bajo
ID_023	P.4	Responsable de línea de negocio	Personal	Forma parte del comité de seguridad	Director General			Bajo
ID_024	P.5	Responsables de info / servicios	Personal	Son los directores de los departamentos de Administración, Operaciones, Oficina Técnica y Comercial	Director General			Medio
ID_026	P.6	Responsable de Seguridad	Personal	Coordina y asegura que se toman las medidas de seguridad adecuadas	Director General			Medio

Tabla 1. Mapa de activos de la empresa

2.1.4. Activos de Software

Entre los activos de software se encuentran programas CAD y de reconstrucción 3D, aplicaciones de gestión de proyectos, una VPN, una aplicación de apertura de puertas, aplicaciones PLM, aplicaciones SAP y aplicaciones topográficas. En todas ellas, lo más importante para la empresa es la disponibilidad. Mientras que en la VPN, es la confidencialidad y autenticidad. Por tanto, se deberá crear diferentes backup para todos aquellos programas implicados.

2.1.5. Activos de Personal

Director General, Comité de seguridad (formado por el responsable de sistemas y telecomunicaciones, responsable de asesoría legal y responsable de línea de negocio), responsables de la información y de los servicios (que son los directores de cada uno de los cuatro departamentos de la empresa), el responsable de sistemas y telecomunicaciones y el responsable de seguridad.

2.2. Listado de amenazas

Una amenaza es cualquier probabilidad de que ocurra una violación de la seguridad de la empresa. En otras palabras, es un peligro probable asociado a la posibilidad real de que un atacante malicioso se aproveche de una vulnerabilidad. Para esta empresa se ha elaborado un listado de las posibles amenazas existentes actualmente. Ver *Tabla 3*.

Además, para esta organización se ha considerado pertinente realizar también un estudio y análisis de las vulnerabilidades del sistema.

En el mundo de la seguridad en las empresas, una vulnerabilidad es una debilidad en un sistema de información que pone en riesgo la seguridad de la información, pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de los datos, así como otras dimensiones de seguridad importantes para la empresa, como la trazabilidad o la autenticidad. Ver *Tabla 4*.

2.3. Riesgos

Un riesgo es la posibilidad de que una de las amenazas descritas anteriormente se produzca, ocasionando un ataque que puede generar una pérdida de valor en uno o varios de los activos de la empresa. Ver *Tabla 2.*

Riesgos	Valoración (10 = máx)	Activos
Acceso no autorizado a los datos	7	Datos
Perdida de eficiencia en negocio	7	Personal
Perdida de clientes	7	Servicios
Pérdida del material de trabajo	6	Hardware, Datos
Perdida de datos	6	Datos
Media de riesgos	6,6	

Tabla 2. Valoración de los riesgos de la empresa

	Amenazas	Valoración (máx = 10)
1	Servidores no disponibles	8
2	Error en la página web	2
3	SW defectuoso	6
4	Fallo de router/switch	6
5	Fallo de ordenadores/portatiles	7
6	Fallo de teléfonos	7
7	Fallo de impresora	2
8	Cerradura averiada	4
9	Trabajador enfermo	7
10	Corte de servicio electricidad	9
11	Corte de servicio agua	4
12	Corte de servicio gas	2
13	Corte de servicio Internet	7
14	Crisis económica	7
15	Incendio, inundación, etc	7
16	Robo	7
17	Pandemia	7
18	Acceso al drive o a los ordenadores por personas no autorizad	10
19	Incumplimiento de relaciones contractuales.	8
20	Infracción legal.	8
21	Comprometer información confidencial.	10
22	Destrucción de registros.	7
23	Accidentes laborales	7
24	Divulgación de contraseñas.	10
25	Malversación y fraude.	7
26	Errores en mantenimiento.	6
27	Falsificación de registros.	8
28	Fuga de información.	8
29	Código malicioso.	8
30	Uso indebido de los sistemas de información.	6
31	Errores de contabilidad.	6
32	Huelgas o paros.	7
33	Cambio involuntario de datos en un sistema de información.	6
34	Cambios no autorizados de registros.	6
35	Instalación no autorizada de software.	5
36	Acceso físico no autorizado.	8
37	Uso no autorizado de material con copyright.	7
38	Uso no autorizado de software.	7
39	Error de usuario.	6

Tabla 3. Valoración de las amenazas actuales de la empresa

Vulnerabilidades	Impacto	Probabilidad	Valoración (máx = 10)	Activos	Relación Amenazas
Contraseñas predeterminadas no modificadas.	Medio	Media	6	HW	18, 24
Eliminación de medios de almacenamiento sin eliminar datos.	Medio	Media	6	D	16, 20 , 24, 28
Gestión inadecuada del cambio.	Bajo	Media	5	S.1, S.2, S.3, S.4, S.6, HW.1, HW.2	5, 26, 33
Clasificación inadecuada de la información.	Medio	Media	7	D	21,22,39
Control inadecuado del acceso físico.	Medio	Baja	5	HW	18, 20, 21,28, 34, 36
Inadecuada gestión de red.	Bajo	Baja	1	HW.3, HW.4	4, 16, 18, 20, 21, 28, 36
Inadecuada gestión y protección de contraseñas.	Alto	Alta	8	HW, SW	18,21,24,28
Protección física no apropiada.	Alto	Media	7	P, HW	8,21,36
Falta de formación y conciencia sobre seguridad.	Alto	Alta	8	D, P	18,21,24,28,36
Falta de política de acceso o política de acceso remoto.	Bajo	Baja	3	D	
Ausencia de política de escritorio limpio y pantalla clara.	Bajo	Alta	5	HW.1	23
Carencia o mala implementación de la auditoría interna.	Alto	Media	7	D	27,25,20
Desprotección en equipos móviles.	Alto	Alta	8	HW.1, HW.5	18, 21, 22, 24, 29, 30
Falta de redundancia, copia única.	Alto	Alta	8	D	1, 4, 5, 10, 13, 22, 33, 34
Ubicación vulnerable a inundaciones.	Bajo	Baja	3	HW, D	15
Copia no controlada de datos.	Alto	Media	7	D	3, 18, 28, 30, 33, 34
Descarga no controlada de Internet.	Alto	Alta	8	HW.1, HW.5	18, 21, 24, 29, 30
Uso incontrolado de sistemas de información.	Medio	Alta	7	HW	1, 2, 5, 18, 20, 21, 22, 24, 28, 20, 30, 31, 33, 34, 35, 37, 38, 39
Empleados desmotivados.	Medio	Media	6	P, D	9, 21, 23, 24, 27, 28, 30, 31, 33, 35, 37, 38, 39
Conexiones a red pública desprotegidas.	Medio	Alta	7	D	6, 18, 21, 24, 28, 29, 30

Tabla 4. Valoración de las vulnerabilidades de la empresa

2.4. Salvaguardas. Contramedidas

Una salvaguarda es un procedimiento o mecanismo tecnológico que tiene como objetivo reducir el riesgo de un sistema de información. Teniendo en cuenta todo lo detallado en este documento, se ha llevado a cabo una lista con las diferentes contramedidas propuestas que la empresa deberá implementar para aumentar su seguridad frente a los posibles ataques del futuro.

ID	Task Name	Duración	Predecesores
1	Formación y concienciación en seguridad: Búsqueda de empleados para impartir cursos	1 día	
2	Formación y concienciación en seguridad: Impartir cursos	2,5 días	1
3	Reglas de uso aceptable de los activos: Implantar normas de seguridad para portátiles	2 días	
4	Reglas de uso aceptable de los activos: Protección con candados para quipos personales	1 día	3
5	Log-onSeguro: Implenentación de la verificación en dos pasos	12 horas	
6	Log-onSeguro: Desconexión automática	1 hora	5
7	Copias de seguridad: Aumentar espacio de servidores	8 horas	
8	Copias de seguridad: Configurar backups semanales	4 horas	7
9	Verificación, revisión y evaluación de la Continuidad: Establecer un método de evaluación de la seguridad periódico	2 días	2;4;5;8

Tabla 5. Listado de las contramedidas propuestas

Finalmente, existen determinados riesgos que es imposible, o simplemente no rentable para la organización, intentar evitar. Por ello, los riesgos aceptados están listados a continuación:

Riesgo Aceptado	Comentario
Inundación de las oficinas	La aceptación de este riesgo será de tipo pasiva, ya que no se destinarán recursos a realizar un plan por si se llega a producir.
Incendio en las oficinas	La aceptación de este riesgo será de tipo activa, ya que se contará con un plan detallado por si dicho riesgo se materializa en algún momento. Pero no se llevarán a cabo controles del mismo.
Perdida de empleados hacia la competencia	La aceptación de este riesgo será de tipo pasiva, ya que no se destinarán recursos a realizar un plan por si se llega a producir.
Atentados terroristas	La aceptación de este riesgo será de tipo pasiva, ya que no se destinarán recursos a realizar un plan por si se llega a producir.
Perdida eléctrica en la instalación	La aceptación de este riesgo será de tipo activa, ya que se contará con un plan detallado por si dicho riesgo se materializa en algún momento. Pero no se llevarán a cabo controles del mismo.
Perdida funcional de los equipos personales	La aceptación de este riesgo será de tipo activa, ya que se contará con un plan detallado por si dicho riesgo se materializa en algún momento. Pero no se llevarán a cabo controles del mismo.
Pandemias	La aceptación de este riesgo será de tipo pasiva, ya que no se destinarán recursos a realizar un plan por si se llega a producir.
Crisis económicas	La aceptación de este riesgo será de tipo pasiva, ya que no se destinarán recursos a realizar un plan por si se llega a producir.
Cambios en las normativas que no aplican al negocio	La aceptación de este riesgo será de tipo pasiva, ya que no se destinarán recursos a realizar un plan por si se llega a producir.
Subida exagerada del precio del alquiler	La aceptación de este riesgo será de tipo activa, ya que se contará con un plan detallado por si dicho riesgo se materializa en algún momento. Pero no se llevarán a cabo controles del mismo.

Tabla 6. Listado de los riesgos aceptados por la empresa