Universidad de **Valladolid**

Escuela de Ingeniería Informática

TRABAJO DE FIN DE GRADO

Grado en Ingeniería Informática

Mención de Tecnologías de la información

ASEGURAEMPRESA: DESARROLLO DE UN SISTEMA QUE PERMITA ENSEÑAR A GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN DE UNA EMPRESA

Autor:

Adrián Muñoz Rojo

Universidad de **Valladolid**

Escuela de Ingeniería Informática

TRABAJO DE FIN DE GRADO

Grado en Ingeniería Informática

Mención de Tecnologías de la información

ASEGURAEMPRESA: DESARROLLO DE UN SISTEMA QUE PERMITA ENSEÑAR A GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN DE UNA EMPRESA

Autor:

Adrián Muñoz Rojo

Tutora:

Margarita Gonzalo Tasis

Resumen

Vivimos en un mundo globalizado y competitivo donde las empresas se encuentran diariamente con desafíos, como amenazas de seguridad, ataques cibernéticos o fraudes electrónicos. Por tanto, cada vez es más importante gestionar la seguridad de la información de la empresa y así, proteger el activo más valioso de ésta, los datos.

Índice de contenidos

Índice de figuras

Índice de tablas

Parte 1. Contexto

Capítulo 1

Introducción y contexto

1.1. Introducción y objetivo

1.1.1. Introducción

La información es el activo más valioso del que depende el buen funcionamiento de una empresa. Mantener su integridad, confidencialidad y disponibilidad es esencial para conseguir los objetivos de esa organización.

Por esa razón, desde hace mucho tiempo, todas las organizaciones han puesto los medios necesarios para proteger su información.

En la actualidad, se han ido desarrollando nuevas tecnologías y se han aumentado cada vez más los riesgos para las empresas que se exponen a nuevas amenazas.

Lamentablemente, ahora mismo, es relativamente fácil acceder a herramientas que permiten a personas no autorizadas a llegar a una información no autorizada, sin mucha necesidad de esfuerzo o conocimientos, con lo que puede causar graves perjuicios a la empresa.

La mayor parte de la información está en equipos informáticos o redes de datos, que se conocen como sistemas de información, que está sujeto a riesgos y amenazas que pueden generarse dentro o fuera de la empresa. Existen riesgos físicos como incendios, terremotos… y riesgos lógicos relacionados con la propia tecnología de la empresa.

Para proteger a las empresas, es necesario conocer bien todos estos conceptos de los que estamos hablando y establecer unos procedimientos adecuados, implementado controles de seguridad basados cada uno de ellos en la evaluación de cada riesgo y amenaza. [1]

1.1.2. Objetivo

El objetivo del proyecto es la realización de una aplicación web que ayude a cualquier empresario a conocer todas las vulnerabilidades, amenazas y riesgos de pérdida de información de datos que pueda tener su empresa y darle así, un plan de medidas para reducir todos los supuestos riesgos que pueda tener. En resumen, explicarle cómo llevar a cabo un sistema gestor de seguridad de la información.

1.2. Estructura de la memoria

Esta memoria está dividida en cuatro partes y, a su vez, en subsecciones, abarcando así los distintos documentos que se van a explicar:

1. Parte I. Introducción y objetivos: Incluye una breve introducción y objetivos del tema en cuestión. Finalmente, contiene un análisis profundo del contexto del proyecto, lo que vamos a estudiar y cómo vamos a calcular el proceso de riesgos de una empresa, con un ejemplo práctico que implementaremos en la aplicación web.
2. Parte II. AseguraEmpresa: Es una parte fundamental ya que incluye documentos como el plan de desarrollo de software, el documento de análisis, de diseño, planificación del proyecto y los riesgos. También se explican detalles importantes de la implementación del proyecto.
3. Parte III. Conclusión y trabajo futuro.
4. Webgrafía y bibliografía.

1.3. Contexto

El proyecto está destinado, como bien hemos explicado antes, a que cualquier empresario entienda qué es un sistema gestor de seguridad de la información, a partir de ahora, SGSI y, además, ayudarle a realizarlo en su empresa. Un SGSI es una herramienta o metodología sencilla que cualquier empresa pueda tener. Consiste en establecer procedimientos y controles con objeto de disminuir los riesgos de su empresa. Los beneficios de utilizar un SGSI son bastante claros:

-En primer lugar, obtenemos una reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. Con ello lograremos reducir las amenazas hasta alcanzar un nivel asumible en cada empresa. Así, si se produce cualquier incidencia, los daños se minimizan y la continuidad del negocia está asegurada.

-En segundo lugar, se produce ahorro de costes innecesarios por la racionalización de los recursos, ya que se eliminan las inversiones innecesarias como las producidas por desestimar o sobreestimar riesgos.

-Por último, el uso de un SGSI contribuye a mejorar la competitividad de las empresas en el mercado, viéndose así, a la empresa más fiable y con mejor imagen que otras que no han conseguido implementarlo.

Para implementar el SGSI, hace falta conocer que es la gestión de los riesgos, conocer todos los conceptos y señalar cuál son las etapas de éste. La Gestión de Riesgos es la "*identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo"* [1].

La gestión de los riesgos está presente en distintos ámbitos de la sociedad y de las empresas. Todas las personas debemos ser conscientes de que existen amenazas que suponen un peligro para conseguir cada uno de los objetivos que nos proponemos.

Para realizar la gestión de los riesgos, lo primero que hay que comprender, son todos los términos con los que vamos a trabajar de aquí en adelante. [2][3]

- **Activo:** Se trata de cualquier recurso de la empresa necesario para poder desempeñar las actividades diarias y cuya no disponibilidad o deterior supone un agravio o coste a la empresa. Su protección es el fin último de la gestión de los riesgos ya que los activos son susceptibles a ser atacados deliberada o accidentalmente. Ejemplos de activos son: información, datos, servicios, aplicaciones, equipos, comunicaciones, recursos administrativos, recursos físicos y recursos humanos. Lo más importante es saber que en una organización hay dos cosas esenciales: la información que se maneja y los servicios que se prestan. Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes de la empresa. Estos activos esenciales dependen de otros activos como pueden ser los equipos hardware o instalaciones y sobre todo las personas que trabajan con ellos.

  Una parte fundamental del activo es su **valoración**, ya que un activo interesa por lo que vale. El valor de cada activo suele estar en la información que maneja o los servicios que presta.

  Los activos se suelen valorar y pueden interesar por las dimensiones que abarca:

  - Confidencialidad: La información solo tiene que ser accesible o divulgada por aquellos que están autorizados. Respecto a esta dimensión hay que hacerse la pregunta ¿qué daño causaría que la información que el activo posee lo conociese quien no debe? Esta valoración suele aplicarse a los datos.
  - Integridad: La información debe permanecer correcta y como el emisor la originó sin manipulaciones de terceros. Sobre esta dimensión la pregunta crítica sería ¿qué perjuicio causaría que estuviese dañado o corrupto? Esta valoración también es típica de los datos ya que se pueden modificar o dañar.

- Disponibilidad: La información debe estar siempre accesible para aquellos que están autorizados. Para la valoración de esta dimensión la pregunta sería ¿qué perjuicio causaría no tener este activo disponible para su utilización?

Figura 1. Dimensiones de los activos

Nunca hay que olvidar también otras dimensiones como la autenticidad y la trazabilidad que se suelen usar en servicios dedicados a la administración electrónica o comercio electrónico. Nosotros añadiremos estas dos últimas dimensiones a la hora de mantener la integridad y confidencialidad de ciertos activos como firmas digitales o registros de actividad.

Una vez determinadas qué dimensiones interesan en cada activo de la empresa, hay que proceder a la valoración de éstos. Se realiza esta valoración para calcular el coste que supondría la recuperación del activo que se viese afectado. Hay muchos factores: costes de reposición del activo, pérdida de ingresos, sanciones por incumplimiento de ley, pérdida de imagen de la empresa, etc.

Esta valoración puede ser cuantitativa o cualitativa.

-Cualitativas: Estas escalas permiten posicionar el valor de cada activo en un orden respecto a los demás

-Cuantitativas: Son valoraciones numéricas que permiten sumar valores para posicionar los activos que más riesgo tienen.

- **Amenazas:** Se trata de una circunstancia desfavorable que puede ocurrir y cuando sucede tiene consecuencias negativas sobre los activos, provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Las amenazas hay que determinarlas, para poder conocer lo que puede ocurrir a nuestro activo. Las amenazas típicas pueden ser [3]:

- De origen natural: Hay accidentes naturales (incendios, terremoto...), en los que la información es una víctima pasiva, pero de todas formas debemos saber lo que puede pasar.
- Del entorno: Desastres naturales como fallos eléctricos o contaminación, en los que la información es una víctima pasiva, pero hay que saber lo que puede suceder.
- Causadas por las personas de forma accidental: acciones no intencionadas por error u omisión.
- Causadas por las personas de forma deliberada: Ataques deliberados para beneficiarse indebidamente, para causar daños y perjuicios a la organización.
- Defectos en las aplicaciones: errores que nacen del equipamiento propio en su diseño o implementación.

Al igual que a los activos, a las amenazas hay que valorarlas. Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar la influencia de la amenaza en el activo por dos formas:

- Degradación: cuál sería la pérdida de valor del activo.
- Probabilidad: es la medida de la certidumbre de que la amenaza se materialice.

La degradación de valor se modela cualitativamente con escalas nominal similares a (siendo el 1 el valor más bajo y el 5 el más alto):

5	Muy alta	Casi seguro	Fácil
4	Alta	Muy alto	Medio
3	Media	Posible	Difícil
2	Baja	Poco probable	Muy difícil
1	Muy baja	Muy raro	Extremadamente difícil

Tabla 1. Degradación de valor

La probabilidad de ocurrencia es algo más complejo de determinar. A veces se modela numéricamente utilizando un porcentaje:

100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco frecuente	Cada varios años
1/100	Muy poco frecuente	Siglos

Tabla 2. Probabilidad de ocurrencia

- **Impacto:** Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos, y la degradación que causan las amenazas, es fácil calcular el impacto que éstas tendrían sobre el sistema.
    - Impacto acumulado: Es el calculado sobre un activo teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto. Al calcularse sobre los activos permite determinar salvaguardas que hay que proponer. El valor de un ordenador no es el valor en si de éste propi, sino también de lo que almacena.
    - Impacto repercutido: Es el calculado sobre un activo teniendo en cuenta su valor propio y las amenazas a las que está expuesto.

- **Riesgo:** Se denomina riesgo a la medida del daño probable sobre el sistema. Se calcula con el producto del impacto y la probabilidad de que se materialice la amenaza. Por tanto, el riesgo crece con el impacto y la probabilidad. Se pueden distinguir zonas a tener en cuenta a tratar los riesgos.
    - Zona 1: Riesgos muy probables y con poco impacto.
    - Zona 2: Desde riesgos improbables y medio impacto hasta riesgos muy probables con impacto bajo.
    - Zona 3: Riesgos improbables y de bajo impacto.
    - Zona 4: Riesgos improbables, pero de muy alto impacto.

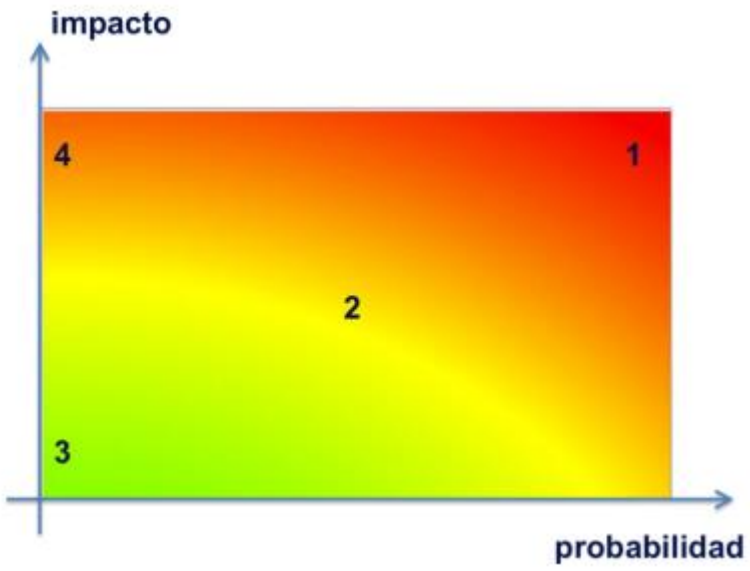


Figura 2. Riesgos en función del impacto y la probabilidad

Después de conocer las zonas de los riesgos, hay que tomar una serie de decisiones por diversos factores: gravedad del impacto u obligaciones por ley.

Todas las consideraciones finalmente terminan en una calificación de cada riesgo:

- Crítico: requiere atención urgente.
- Grave: requiere atención.
- Apreciable: Tiene que ser objeto de estudio.
- Asumible: No se van a tomar acciones. Ya sea porque el impacto o riesgo son asumibles o porque las salvaguardas son muy costosas.

Una vez que hemos valorado los riesgos, el siguiente paso es el **tratamiento** de éstos:

- **Aceptación de riesgo**: Se asume el riesgo, ya que está por debajo del umbral de riesgo de cada empresa, o como hemos explicado antes, la probabilidad es muy baja y los costes, de las salvaguardas que evitan la amenaza, son muy elevados.
- **Evitar o eliminar el riesgo**: Es una opción frente a un riesgo que no es aceptable. Más viable que prescindir de la información, es sustituir los activos por otros que no se vean afectados por esas amenazas.
- **Reducir el riesgo**: Se toman medidas necesarias para que el riesgo se sitúe por debajo del umbral de riesgos de cada

empresa. Hay dos opciones, reducir la degradación que pueda causar la amenaza o reducir la probabilidad de que la amenaza se materialice.

- **Asignarlo a terceros**: Transferir el riesgo o compartir el riesgo si no se transfiere en su totalidad. Hay dos formas: se comparten por medio de componentes del sistema que se reparten las responsabilidades o se comparten por medio de una contratación de seguros, y por medio de dinero, el tomador reduce el impacto de las amenazas.

- **Salvaguardas:** Son los procedimientos o mecanismos que reducen los riesgos. Hay que realizar una selección de salvaguardas para cada tipo de activo, ya que hay amenazas que se solventan simplemente organizándose bien, pero otras requieren elementos técnicos o seguridades físicas.

  Hay dos tipos de salvaguardas:

  - Reducen la probabilidad o salvaguardas preventivas que impiden que la amenaza se materialice.
  - Limitan el daño causado. La amenaza se materializa, pero las consecuencias se limitan.

- **Vulnerabilidades:** Son todas las debilidades que presentan los activos y pueden ser aprovechadas por una amenaza. Son vulnerabilidades, todas las ausencias de las salvaguardas sobre un activo.

Capítulo 2

Ejemplo práctico

Ahora que ya nos hemos puesto en contexto con el tema del que se va a tratar en el proyecto, a continuación, vamos a mostrar un ejemplo práctico que seguiremos en la aplicación web:

2.1. Identificación de los activos

Como bien hemos explicado antes, el primer paso es identificar los activos que tienen las empresas, empleando la metodología MAGERIT [3], la cual propone el siguiente modelo de clasificación:

Categoría de activos	Descripción de los activos	Activos
Datos/Información	Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información o será trasferido de un lugar a otro por medios de transmisión.	Copias de respaldo; Código fuente; Código ejecutable; Credenciales y contraseñas; Datos en papel; Datos de control de acceso.
Servicios	Función que satisface una necesidad de los usuarios	Accesos remotos; Correo electrónico; Servicios de File Systems. Servidores
Software	Tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos la explotación de la información para la prestación de los servicios.	Sistemas operativos; Antivirus; Aplicaciones ofimáticas; Máquinas virtuales; Sistema gestor de Bases de datos;

Hardware	Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.	Grandes equipos (Hosts); Equipos medios; Informática personal; Equipos móviles; Agendas electrónicas; Soporte de la red (Switch, routers.);
Redes de comunicación	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.	Red telefónica; Red de área local (LAN); Red de área inalámbrica (WLAN);
Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o, por lo menos, durante largos periodos de tiempo.	Discos duros; Discos virtuales; Almacenamiento en la red; USBs; CD-DVD; Tarjetas de memoria; Disquetes.
Equipamiento auxiliar	Otros equipos que sirven de soporte a los sistemas de información.	Fuentes de alimentación; Sistemas de alimentación interrumpida; Generadores eléctricos; Equipos de climatización; Cableado eléctrico; Fibra óptica; Equipos de destrucción; Cajas fuertes;
Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones.	Edificios; Mobiliario y cuartos; Instalaciones de respaldo
Personal	Personas relacionadas con los sistemas de información.	Usuarios internos; Usuarios externos; Operadores; Administradores; Desarrolladores; Proveedores; Subcontratas.

Tabla 3. Identificación de activos

2.1.1. Valoración de los activos

Una vez identificado los activos, hay que comenzar a valorarlos en términos de las dimensiones explicadas anteriormente: Disponibilidad, Integridad y Confidencialidad.

Vamos a utilizar una valoración que abarque las dimensiones con los temas más importantes de una empresa: Económico, Legal e Imagen.

Dimensiones	Temas	Descripción
Disponibilidad	Económico	La indisponibilidad del activo afecta económicamente a la empresa
	Obligaciones legales	La indisponibilidad del activo genera sanciones legales
	Imagen	La indisponibilidad del activo afecta a la imagen de la empresa
Integridad	Económico	Los datos modificados no autorizados generan pérdidas de dinero en la empresa
	Obligaciones legales	Los datos modificados no autorizados generan sanciones legales
	Imagen	Los datos modificados no autorizados afectan negativamente a la imagen de la empresa
Confidencialidad	Económico	La información conocida por personas no autorizadas afecta a la estrategia de negocio
	Obligaciones legales	La información conocida por personas no autorizadas ocasiona el incumplimiento de la normativa de la empresa
	Imagen	La información conocida por personas no autorizadas afecta al nombre de la empresa

Tabla 4. Relación de las dimensiones con los temas importantes

Para valorar los activos vamos a utilizar una escala cuantitativa de cinco valores de menor a mayor:

Valor	Criterio	Número identificativo
Despreciable	Daño irrelevante	1
Bajo	Daño menor	2
Medio	Daño importante	3
Alto	Daño grave	4
Extremo	Daño extremadamente grave	5

Tabla 5. Escala cuantitativa

Una vez explicada la escala que vamos a utilizar, procedemos a valorar los temas más importantes que consideramos de una empresa asignando a cada tema el número identificativo correspondiente de la escala:

Temas	Criterio de valoración	Número identificativo
Económico	No supondría perdidas económicas	1
	Supondría pérdidas económicas mínimas	2
	Supondría pérdidas de cierto interés para la competencia	3
	Supondría pérdidas de alto interés para la competencia y graves pérdidas económicas para la empresa	4
	Pérdidas económicas excepcionalmente elevadas y de enorme interés para la competencia	5
Obligaciones legales	No se incumple ninguna ley de confidencialidad	1
	Probablemente cause incumplimiento leve de una ley	2
	Probablemente cause incumplimiento de una ley o regulación	3
	Probablemente cause incumplimiento grave de una ley o regulación	4
	Probablemente cause un incumplimiento excepcionalmente grave de una ley y regulación	5
Imagen	No afecta a la imagen de la empresa ni daño a la reputación	1
	Puede causar una pérdida de confianza dentro de la organización	2
	Probablemente cause una cierta publicidad negativa para afectar negativamente a las relaciones con el público y organizaciones	3
	Probablemente cause publicidad negativa generalizada por afectar gravemente a las relaciones con el público y organizaciones	4
	Probablemente cause una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con otras organizaciones y con el público en general	5

Tabla 6. Criterio de valoración de los temas

Valoramos los activos y finalmente los ponemos un nivel de criticidad:

Activo	Confidencialidad			Integridad			Disponibilidad			Promedio	Criticidad
	Económ	Legal	Imagen	Económ	Legal	Imagen	Económ	Legal	Imagen		
Código fuente	5	5	5	5	5	5	5	5	5	5	Extremo
Código ejecutable	5	5	5	5	5	5	5	5	5	5	Extremo
Backups	5	5	5	5	5	5	5	5	5	5	Extremo
Contraseñas y Credenciales	5	5	5	4	4	4	5	5	5	5	Extremo
Correo electrónico	4	4	4	4	4	4	4	4	4	4	Alto
File Systems	5	5	5	5	5	5	5	5	5	5	Extremo
Servidores	5	5	5	5	5	5	5	5	5	5	Extremo
Accesos remotos	4	4	4	4	4	4	3	5	5	4	Alto
Antivirus	4	2	5	2	2	3	4	4	4	4	Alto
Sistemas operativos	1	1	1	1	2	1	1	2	2	2	Bajo
Aplicaciones escritorio	3	3	3	3	3	3	4	4	4	3	Medio
IDEs / MV	4	4	4	4	4	4	4	4	4	4	Alto
SGBD	4	4	4	4	4	4	4	4	4	4	Alto
Hosts	5	5	5	5	5	5	5	5	5	5	Extremo
Ordenadores	4	4	4	3	3	3	4	4	4	4	Alto
Móviles	3	3	3	3	3	3	3	3	3	3	Medio
Soportes de red	4	4	4	4	4	4	4	4	4	4	Alto
LAN	4	4	3	4	2	3	4	2	3	4	Alto
WLAN	4	4	3	4	2	3	4	2	3	4	Alto

Activo	Confidencialida			Integridad			Disponibilidad			Promedio	Criticidad
	Económi	Legal	Imagen	Económi	Legal	Imagen	Económi	Legal	Imagen		
Red teléfono	3	3	3	2	2	2	3	3	3	3	Medio
Almacenamiento externo	3	4	4	1	2	2	1	1	1	3	Medio
Equipamiento auxiliar	3	3	3	3	3	3	3	3	3	3	Medio
Instalaciones	5	5	5	5	5	5	5	5	5	5	Extremo
Personal	5	5	5	5	5	5	4	4	4	5	Extremo

Tabla 7. Valoración de los activos

2.2. Estudio de las amenazas de cada activo

El siguiente paso es estudiar las amenazas que tienen los activos. Entre corchetes, se pondrá las dimensiones o propiedades que puede perjudicar cada amenaza, [D], [C], [I], Disponibilidad, Confidencialidad e Integridad respectivamente.

Activos afectados	**Amenazas**
Instalaciones Cuartos de equipos Cuarto de archivos Equipamientos auxiliares	-Posibilidad de que un incendio o una inundación (de origen natural o industrial) acabe con los recursos del sistema. [D] -Incidentes que se producen por un desastre natural. [D] -Corte de suministro eléctrico. [D] -Degradación de los equipamientos auxiliares que pueden afectar a su uso. [D] -Ocupación enemiga. [D] -Acceso no autorizado. [C] [I] -Modificación deliberada de la información. [I] -Destrucción de la información [D] -Robo de equipamiento auxiliar. [D] [C] -Ataques destructivos. [D]
Personal Talento humano	-Exempleados descontentos todavía con privilegios. (Fuga de información) [C] -Indisponibilidad de personal. [D] -Extorsión. [D] [C] [I] -Abusos de buena fe. [D] [C] [I] -Terceros interesados en generar ataques que provoquen la indisponibilidad de los servicios de la empresa. [D] [C] [I] -Deficiencias en la organización [D]

Datos e información. Código fuente y ejecutable. Contraseñas y credenciales.	-Errores de usuarios no intencionados. [D] [C] [I] -Errores de los administradores no intencionados. [D] [C] [I] -Errores de monitorización (log). [I] -Manipulación de los registros de actividad. [I] -Errores de configuración [I] -Manipulación de la configuración [I] -Alteración accidental de la información. [I] -Alteración deliberada de la información. [I] -Divulgación de la información. [C] -Destrucción de la información. [D] -Fugas de información. [C] -Suplantación de la identidad [C][I] -Abuso de privilegios de acceso. [D] [C] [I] -Acceso no autorizado. [C] [I]
Redes de comunicación LAN WLAN	-Fallo de servicios de comunicaciones [D] -Errores de los administradores. [D][C][I] -Errores de re-encaminamiento. [C] -Errores de secuencia [I] -Alteración o destrucción de información en su tránsito [I] -Caída del sistema por agotamiento de recursos [D] -Uso no previsto [D][C][I] -Alteración de secuencia. [I] -Análisis de tráfico [C] -Interceptación de información [C] -Denegación de servicio. [D]
	-Avería de origen lógico. [D]

Software Antivirus S.O Aplicaciones Sgbd	-Errores de los usuarios. [D] [C] [I] -Errores de configuración de los administradores. [D][C][I] -Difusión de software dañino. [D] [C] [I] -Errores de re-encaminamiento. [C] -Errores de secuencia [I] -Alteración accidental de las aplicaciones. [I] -Destrucción de las aplicaciones. [D] -Errores de mantenimiento o actualización de los programas. [D][I] -Abuso de privilegios de acceso. [D] [C] [I] -Acceso no autorizado. [C] [I] -Ataques de inyección. [D] [C] [I] -Uso no previsto. [D] [C] [I] -Manipulación de programas. [D] [C] [I] -Ataques deliberados. [D] [C] [I] -Auditorías débiles. [D] [C] [I] -Denegación de servicio. [D]
Hardware Hosts Ordenadores Móviles/Pda Equipamiento informático	-Posibilidad de que un incendio o una inundación (de origen natural o industrial) acabe con los recursos del sistema. [D] -Incidentes que se producen por un desastre natural. [D] -Corte de suministro eléctrico. [D] -Errores de los administradores. [D][C][I] -Errores de mantenimiento y actualización de equipos. [D] -Caída del sistema por agotamiento de recursos. [D] -Pérdida de equipos. [D][C] -Abuso de privilegios de acceso. [D] [C] [I] -Uso no previsto [D][C][I] -Acceso no autorizado [C][I] -Manipulación de los equipos. [C][D] -Denegación de servicio. [I]

	-Robo. [D][C] -Ataque destructivo. [D]
Servicios Correo electrónico Servidores File Systems	-Errores de usuarios no intencionados. [D] [C] [I] -Errores de los administradores no intencionados. [D] [C] [I] -Errores de re-encaminamiento. [C] -Errores de secuencia [I] -Alteración accidental de la información. [I] -Destrucción de la información. [D] -Fugas de información. [C] -Caída del sistema por agotamiento de recursos [D] -Abuso de privilegios de acceso. [D] [C] [I] -Uso no previsto [D][C][I] -Denegación de servicio. [I] -Puertos abiertos. [D] [C] [I] -Servicios inutilizados. [D] [C] [I] -Ataques deliberados. [D] [C] [I] -Ingeniería Social. [D] [C] [I]
Medios de almacenamiento Medios de	-Posibilidad de que un incendio o una inundación (de origen natural o industrial) acabe con los recursos del sistema. [D] -Incidentes que se producen por un desastre natural. [D] -Degradación de los soportes de almacenamiento. [D] -Errores de usuarios no intencionados. [D] [C] [I] -Errores de los administradores no intencionados. [D] [C] [I] -Alteración accidental de la información. [I] -Alteración deliberada de la información. [I] -Divulgación de la información. [C] -Destrucción de la información. [D] -Fugas de información. [C] -Errores de mantenimiento y actualización. [D]

almacenamiento (cont.)	-Uso no previsto. [D] [C] [I] -Robo. [D][C] -Ataques dirigido [D] [C] [I]

Tabla 8. Amenazas

2.2.1. Riesgo de cada amenaza

El siguiente paso de la gestión de riesgos es estudiar el riesgo de cada amenaza. Como hemos explicado anteriormente, el riesgo se calcula de la siguiente manera:

Riesgo= Probabilidad x Impacto

Mostramos la matriz en la que calculamos el riesgo:

Probabilidad	**Impacto**				
	Muy bajo (1)	**Bajo (2)**	**Medio (3)**	**Alto (4)**	**Muy alto (5)**
Muy bajo (1)	1	2	3	4	5
Bajo (2)	2	4	6	8	10
Medio (3)	3	6	9	12	15
Alto (4)	4	8	12	16	20
Muy alto (5)	5	10	15	20	25

Tabla 9. Matriz de riesgo

A continuación, valoramos el riesgo que hemos calculado en la matriz con una escala cuantitativa de valores:

Valoración del riesgo	Calificación
Muy bajo	1-2
Bajo	3-4
Medio	5-9
Alto	10-15
Crítico	16-25

Tabla 10. Escala cuantitativa de los riesgos

Siguiendo las anteriores valoraciones, valoramos todas amenazas en función del riesgo que puede tener que se lleven a cabo:

Activos afectados	Amenazas	Valoración del riesgo		
		Probabil.	Impacto	Calificación
Instalaciones Cuartos de equipos Cuarto de archivos Equipamientos auxiliares	-Posibilidad de que un incendio o una inundación (de origen natural o industrial) acabe con los recursos del sistema. [D]	1	5	5
	-Incidentes que se producen por un desastre natural. [D]	1	5	5
	-Corte de suministro eléctrico. [D]	2	5	10
	-Degradación de los equipamientos auxiliares que pueden afectar a su uso. [D]	3	3	9
	-Ocupación enemiga. [D]	1	5	5
	-Acceso no autorizado. [C] [I]	2	5	10
	-Modificación deliberada de la información. [I]	2	5	10
	-Destrucción de la información [D]	2	5	10

	-Robo de equipamiento auxiliar. [D] [C]	1	3	3
	-Ataques destructivos. [D]	2	5	10
Personal Talento humano	-Exempleados descontentos todavía con privilegios. (Fuga de información) [C]	1	5	5
	-Indisponibilidad de personal. [D]	1	4	4
	-Extorsión. [D] [C] [I]	1	5	5
	-Abusos de buena fe. [D] [C] [I]	2	4	8
	-Terceros interesados en generar ataques que provoquen la indisponibilidad de los servicios de la empresa. [D] [C] [I]	4	4	16
	-Deficiencias en la organización [D]	3	3	9
Datos e información. Código fuente y ejecutable. Contraseñas y credenciales.	-Errores de usuarios no intencionados. [D] [C] [I]	4	4	16
	-Errores de configuración [I]	3	4	12
	-Errores de los administradores no intencionados. [D] [C] [I]	3	5	15
	-Errores de monitorización (log). [I]	3	4	12
	-Manipulación de los registros de actividad. [I]	2	5	10
	-Manipulación de la configuración [I]	2	5	10
	-Alteración accidental de la información. [I]	4	4	16
	-Alteración deliberada de la información. [I]	2	5	10
	-Divulgación de la información. [C]	2	4	8
	-Destrucción de la información. [D]	4	5	20
	-Fugas de información. [C]	3	5	15
	-Suplantación de la identidad [C][I]	3	5	15
	-Abuso de privilegios de acceso. [D] [C] [I]	4	5	20
	-Acceso no autorizado. [C] [I]	3	5	15

Redes de comunicación LAN WLAN	-Fallo de servicios de comunicaciones [D]	2	5	10
	-Errores de los administradores. [D][C][I]	3	5	15
	-Errores de re-encaminamiento. [C]	2	5	10
	-Errores de secuencia [I]	3	4	12
	-Alteración o destrucción de formación en su tránsito [I]	3	5	15
	-Caída del sistema por agotamiento de recursos [D]	4	5	20
	-Uso no previsto [D][C][I]	4	4	16
	-Alteración de secuencia. [I]	3	4	12
	-Análisis de tráfico [C]	4	3	12
	-Interceptación de información [C]	4	5	20
	-Denegación de servicio. [D]	4	5	20
Software Antivirus S.O Aplicaciones SGBD	-Avería de origen lógico. [D]	2	2	4
	-Errores de los usuarios. [D] [C] [I]	4	3	12
	-Errores de los administradores. [D][C][I]	4	4	16
	-Difusión de software dañino. [D] [C] [I]	5	5	25
	-Errores de re-encaminamiento. [C]	2	2	4
	-Errores de secuencia [I]	2	2	4
	-Alteración accidental de la información aplicaciones. [I]	2	2	4
	-Destrucción de las aplicaciones. [D]	2	2	4
	-Errores de mantenimiento o actualización de los programas. [D][I]	4	3	12
	-Abuso de privilegios de acceso. [D] [C] [I]	4	4	16
	-Acceso no autorizado. [C] [I]	4	4	16
	-Ataques de inyección	4	4	16
	-Uso no previsto. [D] [C] [I]	4	4	16
	-Manipulación de programas. [D] [C] [I]	3	4	12

Hardware Hosts Ordenadores Móviles/Pda Equipamiento informático	-Posibilidad de que un incendio o una inundación (de origen natural o industrial) acabe con los recursos del sistema. [D]	1	5	5
	-Incidentes que se producen por un desastre natural. [D]	1	5	5
	-Corte de suministro eléctrico. [D]	2	3	6
	-Errores de los administradores. [D][C][I]	3	4	12
	-Errores de mantenimiento y actualización de equipos. [D]	4	4	16
	-Caída del sistema por agotamiento de recursos. [D]	3	4	12
	-Pérdida de equipos. [D][C]	2	4	12
	-Abuso de privilegios de acceso. [D] [C] [I]	4	3	12
	-Uso no previsto [D][C][I]	4	2	8
	-Acceso no autorizado [C][I]	4	3	12
	-Manipulación de los equipos. [C][D]	2	4	8
	-Denegación de servicio. [I]	3	5	15
	-Robo. [D][C]	2	4	8
	-Ataque destructivo. [D]	2	5	10
Servicios Correo electrónico Servidores File Systems	-Errores de usuarios no intencionados. [D] [C] [I]	3	3	9
	-Errores de los administradores no intencionados. [D] [C] [I]	3	4	12
	-Errores de re-encaminamiento. [C]	2	4	8
	-Errores de secuencia [I]	2	4	8
	-Alteración accidental de la información. [I]	2	5	10
	-Destrucción de la información. [D]	2	5	10
	-Fugas de información. [C]	3	5	15
	-Caída del sistema por agotamiento de recursos [D]	3	5	15
	-Abuso de privilegios de acceso. [D] [C] [I]	4	3	12

	-Uso no previsto [D][C][I]	4	3	12
	-Denegación de servicio. [I]	3	5	15
Medios de almacenamiento	-Posibilidad de que un incendio o una inundación (de origen natural o industrial) acabe con los recursos del sistema. [D]	1	3	3
	-Incidentes que se producen por un desastre natural. [D]	1	3	3
	-Degradación de los soportes de almacenamiento. [D]	4	2	8
	-Errores de usuarios no intencionados. [D] [C] [I]	4	3	12
	-Errores de los administradores no intencionados. [D] [C] [I]	3	4	12
	-Alteración accidental de la información. [I]	3	3	9
	-Alteración deliberada de la información. [I]	2	4	8
	-Divulgación de la información. [C]	3	4	12
	-Destrucción de la información. [D]	3	4	12
	-Fugas de información. [C]	3	3	9
	-Errores de mantenimiento y actualización. [D]	2	2	4
	-Uso no previsto. [D] [C] [I]	4	1	4
	-Robo. [D][C]	2	3	6

Tabla 11. Valoración del riesgo de cada amenaza

2.3. Elección de estrategias de cada riesgo

Uno de los últimos pasos de la gestión de riesgos es tratar cada riesgo. A continuación, se muestran las estrategias que hemos seleccionado a cada riesgo:

Activos	Amenazas	Calificación	Estrategia
Instalaciones Cuartos de equipos Cuarto de archivos Equipamientos auxiliares	-Posibilidad de que un incendio o una inundación (de origen natural o industrial) acabe con los recursos del sistema. [D]	5	Reducir
	-Incidentes que se producen por un desastre natural. [D]	5	Aceptar
	-Corte de suministro eléctrico. [D]	10	Reducir
	-Degradación de los equipamientos auxiliares que pueden afectar a su uso. [D]	9	Reducir
	-Ocupación enemiga. [D]	5	Reducir
	-Acceso no autorizado. [C] [I]	10	Reducir
	-Modificación deliberada de la información. [I]	10	Reducir
	-Destrucción de la información [D]	10	Reducir
	-Robo de equipamiento auxiliar. [D] [C]	3	Aceptar
	-Ataques destructivos. [D]	10	Reducir
Personal Talento humano	-Exempleados descontentos todavía con privilegios. (Fuga de información) [C]	5	Reducir
	-Indisponibilidad de personal. [D]	4	Aceptar
	-Extorsión. [D] [C] [I]	5	Reducir
	-Abusos de buena fe. [D] [C] [I]	8	Reducir
	-Terceros interesados en generar ataques que provoquen la indisponibilidad de los servicios de la empresa. [D] [C] [I]	16	Reducir
	-Deficiencias en la organización [D]	9	Reducir

Datos e información. Código fuente y ejecutable. Contraseñas y credenciales.	-Errores de usuarios no intencionados. [D] [C]	16	Reducir
	-Errores de configuración [I]	12	Reducir
	-Errores de los administradores no intencionados. [D] [C] [I]	15	Reducir
	-Errores de monitorización (log). [I]	12	Reducir
	-Manipulación de los registros de actividad. [I]	10	Reducir
	-Manipulación de la configuración [I]	10	Reducir
	-Alteración accidental de la información. [I]	16	Reducir
	-Alteración deliberada de la información. [I]	10	Reducir
	-Divulgación de la información. [C]	8	Reducir
	-Destrucción de la información. [D]	20	Reducir
	-Fugas de información. [C]	15	Reducir
	-Suplantación de la identidad [C][I]	15	Reducir
	-Abuso de privilegios de acceso. [D] [C][I]	20	Reducir
	-Acceso no autorizado. [C] [I]	15	Reducir
Redes de comunicación LAN WLAN	-Fallo de servicios de comunicaciones [D]	10	Reducir
	-Errores de los administradores. [D][C][I]	15	Reducir
	-Errores de re-encaminamiento. [C]	10	Reducir
	-Errores de secuencia [I]	12	Reducir
	-Alteración o destrucción de información en su tránsito [I]	15	Reducir
	-Caída del sistema por agotamiento de recursos [D]	20	Reducir
	-Uso no previsto [D][C][I]	16	Reducir
	-Alteración de secuencia. [I]	12	Reducir
	-Análisis de tráfico [C]	12	Reducir
	-Interceptación de información [C]	20	Reducir
	-Denegación de servicio. [D]	20	Reducir

Software Antivirus S.O Aplicaciones SGBD	-Avería de origen lógico. [D]	4	Aceptar
	-Errores de los usuarios. [D] [C] [I]	12	Reducir
	-Errores de los administradores. [D][C][I]	16	Reducir
	-Difusión de software dañino. [D] [C] [I]	25	Reducir
	-Errores de re-encaminamiento. [C]	4	Aceptar
	-Errores de secuencia [I]	4	Aceptar
	-Alteración accidental de la información aplicaciones. [I]	4	Aceptar
	-Destrucción de las aplicaciones. [D]	4	Aceptar
	-Errores de mantenimiento o actualización de los programas. [D][I]	12	Reducir
	-Abuso de privilegios de acceso. [D] [C] [I]	16	Reducir
	-Acceso no autorizado. [C] [I]	16	Reducir
	-Uso no previsto. [D] [C] [I]	16	Reducir
	-Manipulación de programas. [D] [C] [I]	12	Reducir
Hardware Hosts Ordenadores Móviles/Pda Equipamiento informático	-Posibilidad de que un incendio o una inundación (de origen natural o industrial) acabe con los recursos del sistema. [D]	5	Reducir
	-Incidentes que se producen por un desastre natural. [D]	5	Aceptar
	-Corte de suministro eléctrico. [D]	6	Reducir
	-Errores de los administradores. [D][C][I]	12	Reducir
	-Errores de mantenimiento y actualización de equipos. [D]	16	Reducir
	-Caída del sistema por agotamiento de recursos. [D]	12	Reducir
	-Pérdida de equipos. [D][C]	12	Reducir
	-Abuso de privilegios de acceso. [D] [C] [I]	12	Reducir
	-Uso no previsto [D][C][I]	8	Reducir
	-Acceso no autorizado [C][I]	12	Reducir

	-Manipulación de los equipos. [C][D]	8	Reducir
	-Denegación de servicio. [I]	15	Reducir
	-Robo. [D][C]	8	Reducir
	-Ataque destructivo. [D]	10	Reducir
Servicios Correo electrónico Servidores File Systems	-Errores de usuarios no intencionados. [D] [C] [I]	9	Reducir
	-Errores de los administradores no intencionados. [D] [C] [I]	12	Reducir
	-Errores de re-encaminamiento. [C]	8	Reducir
	-Errores de secuencia [I]	8	Reducir
	-Alteración accidental de la información. [I]	10	Reducir
	-Destrucción de la información. [D]	10	Reducir
	-Fugas de información. [C]	15	Reducir
	-Caída del sistema por agotamiento de recursos [D]	15	Reducir
	-Abuso de privilegios de acceso. [D] [C] [I]	12	Reducir
	-Uso no previsto [D][C][I]	12	Reducir
	-Denegación de servicio. [I]	15	Reducir
Medios de almacenamiento	-Posibilidad de que un incendio o una inundación (de origen natural o industrial) acabe con los recursos del sistema. [D]	3	Aceptar
	-Incidentes que se producen por un desastre natural. [D]	3	Aceptar
	-Degradación de los soportes de almacenamiento. [D]	8	Reducir
	-Errores de usuarios no intencionados. [D] [C] [I]	12	Reducir
	-Errores de los administradores no intencionados. [D] [C] [I]	12	Reducir
	-Alteración accidental de la información. [I]	9	Reducir
	-Alteración deliberada de la información. [I]	8	Reducir
	-Divulgación de la información. [C]	12	Reducir

	-Destrucción de la información. [D]	12	Reducir
	-Fugas de información. [C]	9	Reducir
	-Errores de mantenimiento y actualización. [D]	4	Aceptar
	-Uso no previsto. [D] [C] [I]	4	Aceptar
	-Robo. [D][C]	6	Reducir

Tabla 12. Selección de estrategia de tratamiento de riesgos

2.4. Elección de salvaguardas

Por último, se plantean los siguientes controles o salvaguardas enfocados a reducir y controlar los riesgos que pueden ocurrir:

Activos	Amenazas	Salvaguardas
Instalaciones Cuartos de equipos Cuarto de archivos Equipamientos auxiliares	-Posibilidad de que un incendio o una inundación (de origen natural o industrial) acabe con los recursos del sistema. [D]	-Extintores de agua pulverizada en cuartos con documentos en papel -Extintores de anhídrido carbónico para fuegos originados en instalaciones eléctricas. -Bocas de incendios -Columnas hidratantes exteriores -Detectores de incendios/humo -Rociadores automáticos de agua -Pulsadores de alarma
	-Corte de suministro eléctrico. [D]	-Generadores eléctricos
	-Degradación de los equipamientos auxiliares que pueden afectar a su uso. [D]	-Revisión del estado de los equipamientos auxiliares -Protección del cableado -Climatización
	-Ocupación enemiga. [D]	-Control de acceso físico
	-Acceso no autorizado. [C] [I]	-Control de acceso físico -Control de acceso lógico -Herramientas de monitoreo de accesos.
	-Modificación deliberada de la información. [I]	-Control de acceso físico
	-Destrucción de la información [D]	-Control de acceso físico

Personal Talento humano	-Exempleados descontentos todavía con privilegios. (Fuga de información) [C]	-Gestión de cancelación de cuentas de exempleados y sus privilegios. -Establecer acuerdos de confidencialidad.
	-Extorsión. [D] [C] [I]	-Establecer acuerdos de confidencialidad. -Establecer programas de capacitación y sensibilización al personal de la empresa en temas relacionados con la seguridad de la información. -Capacitar al personal que en caso de extorsión contar todo a sus superiores directos
	-Abusos de buena fe. [D] [C] [I]	-Establecer acuerdos de confidencialidad. -Establecer programas de capacitación y sensibilización al personal de la empresa en temas relacionados con la seguridad de la información
	-Deficiencias en la organización [D]	-Formación de personal en organización -Planificación correcta -Gestión de riesgos -Inspecciones de seguridad
Datos e información. Código fuente y ejecutable. Contraseñas y credenciales.	-Errores de usuarios no intencionados. [D] [C] [I]	-Copias de seguridad
	-Errores de configuración [I]	-Monitoreo de la configuración
	-Errores de los administradores no intencionados. [D] [C] [I]	-Control de acceso lógico -Copias de seguridad -Detención y recuperación

Datos e información. Código fuente y ejecutable. Contraseñas y credenciales (cont.)	-Errores de monitorización. [I]	-Revisión permanente de los archivos de monitorización y su configuración.
	-Manipulación de los registros de actividad. [I]	-Detención y recuperación -Copias de seguridad de los registros de actividad
	-Manipulación de la configuración [I]	-Control de acceso lógico -Copias de seguridad -Detención y recuperación
	-Alteración accidental de la información. [I]	-Copias de seguridad
	-Alteración deliberada de la información. [I]	-Detención y recuperación -Copias de seguridad -Cifrado de la información -Uso de firmas electrónicas -Uso de servicios de fechado electrónico
	-Divulgación de la información. [C]	-Cifrado de la información
	-Destrucción de la información. [D]	-Copias de seguridad -Gestión de privilegios para borrar información -Control de acceso lógico
	-Fugas de información. [C]	-Cifrado de información
	-Suplantación de la identidad [C][I]	-Usar herramientas que permita utilizar contraseñas robustas -Herramienta que obligue a cambiar contraseñas cada cierto periodo de tiempo. -Autenticación de dos factores
	-Abuso de privilegios de acceso. [D] [C] [I]	-Definir una política de control de acceso que se aplique no sólo

Datos e información. Código fuente y ejecutable. Contraseñas y credenciales (cont.)		a los datos que sean accesibles para que sea posible identificar a usuarios que abusen de sus privilegios -Control de acceso por niveles
	-Acceso no autorizado. [C] [I]	-Cifrado de información -Usar herramientas que permita utilizar contraseñas robustas
	-Errores de los administradores. [D][C][I]	-Copias de seguridad
	-Errores de re-encaminamiento. [C]	-Revisión y controles para asegurar la integridad del mensaje
	-Errores de secuencia [I]	-Revisión y controles para asegurar la integridad del mensaje
	-Caída del sistema por agotamiento de recursos [D]	-Monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el uso
	-Uso no previsto [D][C][I]	-Establecer reglas de uso -Control de acceso a internet a páginas web ajenas a la empresa.
	-Alteración de secuencia. [I]	-Revisión y controles para asegurar la integridad del mensaje
	-Análisis de tráfico [C]	-Monitorear el tráfico que puede soportar la red de la empresa.
	-Interceptación de información [C]	-Cifrado de información -Codificación de mensajes -Protección criptográfica
	-Denegación de servicio. [D]	-Establecer router entre la red y ISP

		-Capas de seguridad como ACL -Cortafuegos -Cantidad alta de ancho de banda -Instalación de un proxy inverso que apunten a varios servidores de la red de la empresa que tienen copias de los servicios que ofrece
Software Antivirus S.O Aplicaciones SGBD	-Avería de origen lógico. [D]	-Revisión y detención -Copias de seguridad
	-Errores de los usuarios. [D] [C] [I]	-Revisión y detención -Copias de seguridad
	-Errores de los administradores. [D][C][I]	-Revisión y detención -Copias de seguridad -Uso de contraseñas para asegurar cambios en las aplicaciones
	-Difusión de software dañino. [D] [C] [I] -Ataques de inyección [D] [C] [I]	-Chequeos de validación de aplicaciones para detectar cualquier corrupción de la información -Cifrar bases de datos
	-Errores de re-encaminamiento. [C]	-Revisión y controles para asegurar la integridad del mensaje
	-Errores de secuencia [I]	-Revisión y controles para asegurar la integridad del mensaje
	-Alteración accidental de la información aplicaciones. [I]	-Revisión y detención -Copias de seguridad
	-Destrucción de las aplicaciones. [D]	-Revisión y detención -Copias de seguridad -Uso de contraseñas de administrador para realizar cambios

	-Errores de mantenimiento o actualización de los programas. [D][I]	-Mejorar las aplicaciones existentes -Revisión y actualización continua
	-Abuso de privilegios de acceso. [D] [C] [I]	-Control de acceso a aplicaciones por niveles.
	-Acceso no autorizado. [C] [I]	-Contraseñas y credenciales
	-Uso no previsto. [D] [C] [I]	-Establecer reglas de uso
	-Denegación de servicio [D] [C] [I]	-Utilización de firewalls
	-Auditorías débiles. [D] [C] [I]	-Registro de auditoría detallada
	-Manipulación de programas. [D] [C] [I]	-Chequeos de validación de aplicaciones para detectar cualquier corrupción de la información -Contraseñas y credenciales
Hardware Hosts Ordenadores Móviles/Pda Equipamiento informático	-Posibilidad de que un incendio o una inundación (de origen natural o industrial) acabe con los recursos del sistema. [D]	-Extintores de agua pulverizada en cuartos con documentos en papel -Extintores de anhídrido carbónico para fuegos originados en instalaciones eléctricas. -Bocas de incendios -Columnas hidratantes exteriores -Detectores de incendios/humo -Rociadores automáticos de agua -Pulsadores de alarma
	-Corte de suministro eléctrico. [D]	-Generadores eléctricos
	-Errores de configuración los administradores. [D][C][I]	-Copias de seguridad
	-Errores de mantenimiento y actualización de equipos. [D]	-Revisión, actualización y mantenimiento de equipos

	-Pérdida de equipos. [D][C]	-Copias de seguridad -Contraseñas y credenciales
	-Abuso de privilegios de acceso. [D] [C] [I]	-Establecer reglas de uso -Control de acceso por niveles
	-Uso no previsto [D][C][I]	-Establecer reglas de uso -Control de acceso a páginas web ajenas a la que se trabaja en la empresa
	-Acceso no autorizado [C][I]	-Contraseñas y credenciales
	-Manipulación de los equipos. [C][D]	-Copias de seguridad -Detención y recuperación -Contraseñas y credenciales
	-Denegación de servicio. [I]	-Cortafuegos -Desactivar todos los puertos no necesarios
	-Robo. [D][C]	-Contraseñas y credenciales -Copias de seguridad
Servicios Correo electrónico Servidores File Systems	-Errores de usuarios no intencionados. [D] [C] [I]	-No iniciar sesión en ordenadores públicos -No enviar información sensible
	-Errores de los administradores no intencionados. [D] [C] [I]	-Copias de seguridad
	-Alteración accidental de la información. [I]	-Copias de seguridad
	-Fugas de información. [C]	-Cifrado de la información -Auditoría de archivos -Sistemas de detección de intrusos -IPS
	-Abuso de privilegios de acceso. [D] [C] [I]	-Definir una política de control de acceso que se aplique no sólo a los datos que sean accesibles para que sea posible identificar a

		usuarios que abusen de sus privilegios
	-Uso no previsto [D][C][I]	-Establecer reglas de uso -Concienciar al personal del peligro que tiene el uso indebido de aplicaciones como el correo eléctronico.
	-Denegación de servicio. [I]	-Monitorear tráfico -Desactivar puertos no necesarios -Configurar registros Windows o linux -Firewalls -Instalación de un proxy inverso que apunten a varios servidores de la red de la empresa que tienen copias de los servicios que ofrece -Servidores aislados
Medios de almacenamiento	-Degradación de los soportes de almacenamiento. [D]	-Revisión y cambio de medios de almacenamiento
	-Errores de usuarios no intencionados. [D] [C] [I]	-Detención y recuperación -Copias de seguridad
	-Errores de los administradores no intencionados. [D] [C] [I]	-Detención y recuperación -Copias de seguridad
	-Alteración accidental de la información. [I]	-Detención y recuperación -Copias de seguridad
	-Divulgación de la información. [C]	-Cifrado en la información -Contraseñas en medios de almacenamiento
	-Destrucción de la información. [D]	-Contraseñas para borrar información

	-Fugas de información. [C]	-Cifrado en la información -Contraseñas en medios de almacenamiento
	-Robo. [D][C]	-Contraseñas en medios de almacenamiento -Copias de seguridad

Tabla 13. Salvaguardas

Parte 2. AseguraEmpresa

Capítulo 3

Planificación

3.1. Plan de desarrollo software

3.1.1. Evolución del plan de desarrollo software

3.1.1.1. Metodología

Para desarrollo del software, utilizaremos un proceso de desarrollo de software que defina detalladamente las fases del proyecto. Hay varios tipos de procesos de desarrollo de software para abordar este problema, sin embargo, el que más se adapta a este caso es Proceso Unificado.

El Proceso Unificado es una metodología de desarrollo de software que está basado en componentes e interfaces bien definidas, y junto con el Lenguaje Unificado de Modelado (UML), constituye la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos. [4]

El proceso unificado es un modelo de fases que identifica cuatro fases diferentes en el proceso de software:

I. Inicio: En esta fase se define la visión, los objetivos y el alcance del proyecto. En esta fase se obtiene una lista de los factores de riesgo del proyecto y un análisis de los requerimientos de este. No se tiene todavía una versión ejecutable.
II. Elaboración: Tiene como principal finalidad completar el análisis de los casos de uso y definir la arquitectura del sistema. Se obtiene la visión refinada del proyecto y se ajustan los requisitos y riesgos.
III. Construcción: Se van incorporando sucesivamente los casos de uso, de acuerdo con los factores de riesgo del proyecto. Esto permite contar en forma temprana con versiones del sistema que satisfagan los principales casos de uso.
IV. Transición: Es la fase final, la aplicación debe estar lista para ser probada, instalada y utilizada por el cliente.

3.1.1.2. Plan de fases

Según la evolución del plan de desarrollo anteriormente explicado, seguiremos el modelo de Proceso Unificado y sus fases. Cada fase tendrá sus propias iteraciones o tareas a realizar:

En la fase de Inicio se desarrollará el contexto y el objetivo del proyecto, y se tendrán definidos los principales riesgos del proyecto para poder gestionarles. También explicaremos el plan de desarrollo del software que hemos elegido y se sacará una principal lista de los requisitos, tanto funcionales como no funcionales del sistema.

En la fase de elaboración se seguirá realizando el documento de análisis, en el que se completará los requisitos del sistema, si faltase alguno, y seguiríamos con la realización de la lista de los casos de uso. Una vez que tengamos la lista de los casos de uso, se empezará con la realización del modelo de dominio. Hay que meditar si vamos a utilizar una base de datos para realizar su diseño. En esta fase también realizaremos la arquitectura de software. Es necesario explicar que esta fase se realizará junto a la de construcción porque puede que mientras se implemente el sistema, se encuentre algún otro requisito o caso de uso.

En la fase de construcción se documentará todo relacionado con la implementación del sistema. Se pondrá en prueba todo el funcionamiento. También se elaborará el manual de usuario e instalación. Durante estas tres fases se realizará la documentación del sistema.

En la fase de transición todo estará listo para ser probado, instalado y utilizado por el cliente sin ningún problema. Quizá se hagan más tipos de pruebas hasta los días antes de la defensa del proyecto para evitar cualquier tipo de problema, pero en este punto el proyecto debería estar terminado.

3.1.2. Gestión del proyecto

3.1.2.1. Planificación

Saber estimar y planificar es fundamental a la hora de encarar este proyecto. Por eso, una vez identificadas las actividades del proyecto anteriormente, definiremos la fecha de inicio y fin estimadas de cada una de ellas y trataremos de cumplirlas. [5]

La planificación será de unas horas fijas a la semana que será de **18 horas.**

3.1.2.2. Hitos

Para poder cumplir la planificación establecida se marcan unos hitos para que sirvan de ayuda para desarrollar el proyecto. Cuando se finalicen los siguientes hitos, estarán acabadas sus actividades y se revisará el estado del proyecto.

Hito	Fase	Iteración	Duración	Fecha comienzo	Fecha final
1	Inicio	Primera	38 horas	18/03/19	01/04/19
2	Elaboración	Segunda	42 horas	02/04/19	18/04/19
3	Construcción	Tercera	120 horas	19/04/19	03/06/19
4	Transición	Cuarta	16 horas	04/06/19	10/06/19

Tabla 14. Hitos del proyecto

3.1.2.3. Plan de trabajo

En la siguiente tabla presentamos la planificación ideal, más detallada de las actividades del proyecto, representándolos en tareas y siguiendo un orden de tareas que realizar para poder hacer las siguientes, también con una fecha estimada de realización.

Tarea	Nombre	Duración	Comienzo	Final	Predecesora
	Inicio	38 horas	18/03/19	01/04/19	
1	Plan desarrollo software	6 horas	18/03/19	20/03/19	-
2	Planificación	2 horas	21/03/19	22/03/19	-
3	Gestión de riesgos	14 horas	22/03/19	26/03/19	-
4	Especificación de requisitos	16 horas	27/03/19	01/04/19	-
	Elaboración	42 horas	02/04/19	18/04/19	
5	Casos de uso	6 horas	02/04/19	04/04/19	4
6	Modelo de dominio y Bases de datos	32 horas	05/04/19	16/04/19	4;5
7	Arquitectura de sistema	4 horas	17/04/19	18/04/19	3;4;5
	Construcción	120 horas	19/04/19	03/06/19	
8	Prototipo	2 horas	19/04/19	19/04/19	
9	Usabilidad y guías de diseño	2 horas	20/04/19	20/04/19	
10	Implementación	116 horas	21/04/19	03/06/19	7;8;9
	Transición	16 horas	04/06/19	10/06/19	
11	Pruebas	2 horas	04/06/19	04/06/19	10
12	Manual de usuario	8 horas	04/06/19	07/06/19	11
13	Manual de instalación	6 horas	04/06/19	06/06/19	12

Tabla 15. Plan de trabajo

Presentamos a continuación las tareas para cada una de las fases y sus diagramas de Gantt realizados con la herramienta Project.

Fase de inicio:

Nombre de tarea	Duración	Comienzo	Fin	Predec
Plan desarrollo software	6 horas	lun 18/03/19	mié 20/03/19	
Planificación	2 horas	jue 21/03/19	jue 21/03/19	
Gestión de riesgos	14 horas	vie 22/03/19	mar 26/03/19	
Especificación de requisitos	16 horas	mié 27/03/19	lun 01/04/19	

Figura 3. Fase de inicio ideal

Fase de elaboración

Casos de uso	6 horas	mar 02/04/19	jue 04/04/19	4
Modelo de dominio y de bases de datos	32 horas	vie 05/04/19	mar 16/04/19	4;5
Arquitectura de sistema	4 horas	mié 17/04/19	jue 18/04/19	3;4;5

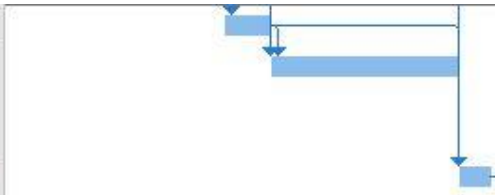


Figura 4. Fase de elaboración ideal

Fase de construcción

Prototipo	2 horas	vie 19/04/19	vie 19/04/19	
Usabilidad y guias de diseño	2 horas	sáb 20/04/19	sáb 20/04/19	
Implementación	116 horas	dom 21/04/19	lun 03/06/19	7;8;9

Figura 5. Fase de construcción ideal

	Pruebas	2 horas	mar 04/06/19	mar 04/06/19	10
	Manual de usuario	8 horas	mié 05/06/19	sáb 08/06/19	11
	Manual de instalación	6 horas	dom 09/06/19	dom 09/06/19	12

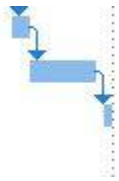


Figura 6. Fase de transición ideal

3.1.3. Plan de gestión de riesgos

El PM-BOK [6] proporciona la siguiente definición "un riesgo en un proyecto es un evento o una condición inciertos que, si ocurren, tienen un efecto positivo o negativo sobre los objetivos del proyecto". Los riesgos se relacionan con posibles problemas futuros. Implican, por tanto, una posible causa y efecto. Genéricamente un riesgo es algo que puede ocurrir o no, por lo tanto, los riesgos hay que gestionarlos.

La gestión de riesgos va a servir como una inversión de futuro, ahorrándonos costes de corrección de problemas que ya se han producido y mejorando el control del proyecto.

En resumen, ayudan a identificar y mitigar los problemas con antelación para prevenir el impacto adverso en factores del proyecto como presupuesto, planificación, recursos y coste y sobre las funcionalidades del proyecto y atributos de calidad.

Existen principalmente tres tipos de riesgos que son los que se tendrán en cuenta:

- Riesgos de Proyecto: Restricciones de recursos, interfaces externas, relaciones con los proveedores etc.
- Riesgos de Proceso: proceso software no documentado, proceso de diseño pobre, planificación ineficaz etc.
- Riesgos de Producto: diseño complejo, requisitos incompletos etc.

Así mismo, el riesgo tiene un impacto cuya gravedad se puede dividir en cuatro niveles (de mayor a menor gravedad):

- Catastrófico: de producirse el riesgo, el objetivo del proyecto fracasaría.
- Crítico: tanto el rendimiento del proceso como del proyecto se ven afectados.
- Marginal: se trata de un problema que afecta a objetivos secundarios.
- Despreciable: se trata de problemas menores.

Nombre del riesgo	**Incumplimiento de la planificación**
Categoría	Riesgo de proceso
Probabilidad	60%
Consecuencias	Critico
Fase	Todas
Enunciado	Este riesgo se puede producir cuando se ha realizado una planificación ineficaz que pueden causar retrasos y otras situaciones no acordes con lo previsto
Contexto	A lo largo del proyecto
Análisis	Se retrasaría las fechas previstas de entrega de fases del proyecto
Plan de acción	Revisión y modificación de la planificación

Tabla 16. Riesgo 1: Incumplimiento de la planificación.

Nombre del riesgo	**Falta de experiencia en proyecto similares**
Categoría	Riesgo de producto
Probabilidad	60%
Consecuencias	Critico
Fase	Todas
Enunciado	Debido a la falta de experiencia en la elaboración de proyectos, este podría verse afectado, incluso con retrasos
Contexto	A lo largo del proyecto
Análisis	Desarrollo de las actividades más lento
Plan de acción	Adquirir más experiencia a través de documentación, formación.

Tabla 17. Riesgo 2: Falta de experiencia

Nombre del riesgo	Errores en la etapa del diseño
Categoría	Riesgo de proceso
Probabilidad	75%
Consecuencias	Critico
Fase	Diseño
Enunciado	Pueden existir muchos errores en la etapa de diseño, por falta de experiencia en proyectos similares o falta de familiaridad con las herramientas usadas.
Contexto	Fase de diseño
Análisis	Puede ser que surja la necesidad de revisar más en profundidad la etapa de diseño, retrasando las etapas siguientes
Plan de acción	Comprobar en la etapa de diseño que todo que se va realizando esta correctamente siguiendo los requisitos de los documentos de análisis

Tabla 18. Riesgo 3: Errores en la etapa de diseño

Nombre del riesgo	Cambios en los requisitos o requisitos mal definidos
Categoría	Riesgo de producto
Probabilidad	30%
Consecuencias	Marginal
Fase	Análisis
Enunciado	Pueden existir muchos errores en la etapa de análisis, y a la hora de elegir los requisitos necesarios. Pueden aparecer mas requisitos
Contexto	Fase de análisis
Análisis	Si el análisis no es correcto se deberá repetir total o parcial. Puede suponer un retraso en las demás etapas
Plan de acción	Comprobaciones periódicas de la etapa de análisis.

Tabla 19. Riesgo 4: Errores en los requisitos

Nombre del riesgo	Baja temporal
Categoría	Riesgo de proyecto
Probabilidad	1%
Consecuencias	Catastrófico
Fase	Todas
Enunciado	Puedo causar baja por diversos motivos durante un periodo de tiempo.
Contexto	A lo largo del proyecto
Análisis	Se retrasaría las fechas previstas de entrega de fases del proyecto, pudiendo llegar a no cumplir el objetivo final.
Plan de acción	Se modificaría la planificación. La carga de trabajo aumentaría considerablemente.

Tabla 20. Riesgo 5: Baja temporal

Nombre del riesgo	Falta de revisión y actualización del proyecto
Categoría	Riesgo de proceso
Probabilidad	10%
Consecuencias	Marginal
Fase	Todas
Enunciado	Se debe realizar revisiones al final de cada interacción del proyecto
Contexto	A lo largo del proyecto
Análisis	Si las revisiones no son correctas, se arrastrarán errores por las siguientes fases del proyecto.
Plan de acción	Se revisará todo el trabajo después de realizar una interacción

Tabla 21. Riesgo 6: Falta de revisión de las etapas del proyecto

Nombre del riesgo	Desarrollo de interfaces poco usables o que no cumplan los atributos de usabilidad
Categoría	Riesgo de proceso
Probabilidad	20%
Consecuencias	Marginal
Fase	Diseño/Implementación
Enunciado	El diseño incorrecto de las interfaces puede afectar negativamente al proceso de diseño y de implementación
Contexto	Diseño / implementación
Análisis	Si se produce errores, puede llevar al rediseño de las interfaces
Plan de acción	Se revisará las interfaces y se realizará un seguimiento de estas

Tabla 22. Riesgo 7: Desarrollo de interfaces incorrectas

Nombre del riesgo	Ausencia de familiaridad de las herramientas a usar en el desarrollo del proyecto
Categoría	Riesgo de proceso
Probabilidad	20%
Consecuencias	Marginal
Fase	Todas
Enunciado	Posibilidad de que no se tenga experiencia con alguna herramienta que se vaya a emplear
Contexto	Todas las fases
Análisis	Si se produce este riesgo, cabe la posibilidad de que se tarde más en realizar las fases.
Plan de acción	Formación de las tecnologías a usar

Tabla 23. Riesgo 8: Ausencia de familiaridad de herramientas desarrolladas en el proyecto

Nombre del riesgo	Caída de la máquina virtual
Categoría	Riesgo de proyecto
Probabilidad	5%
Consecuencias	Crítico
Fase	Implementación
Enunciado	Posibilidad de que la máquina virtual deje de funcionar por diversas causas
Contexto	Fase de implementación
Análisis	Si se produce este riesgo, no se podrá realizar la implementación del proyecto durante el tiempo que la máquina no esté operativa
Plan de acción	Restauración del sistema en otra máquina virtual, a partir de una copia de seguridad realizada anteriormente

Tabla 24. Riesgo 9: Caída de máquinas virtuales

Nombre del riesgo	Rotura del ordenador con el que se trabaja
Categoría	Riesgo de proyecto
Probabilidad	5%
Consecuencias	Crítico
Fase	Todas
Enunciado	Posibilidad de que el ordenador con el que se trabaje se rompa o deje de funcionar
Contexto	Todas
Análisis	Si se produce este riesgo, no se podrá realizar el proyecto hasta que no se consiga otro ordenador
Plan de acción	Copias de seguridad para no perder el trabajo realizado

Tabla 25. Riesgo 10: Rotura de equipo

3.1.4. Seguimiento del proyecto

A continuación, se va a describir el tiempo real empleado para cada una de las fases que fueron planificadas anteriormente.

Las fases de Inicio y Elaboración se realizaron en el tiempo estimado de la planificación ideal, en 38 y 42 horas respectivamente.

En la planificación real solo modificamos la fase de Construcción y Transición ya que hemos sufrido los siguientes riesgos:

-Incumplimiento de la planificación.

-Falta de experiencia en proyectos similares

-Errores en la etapa de diseño

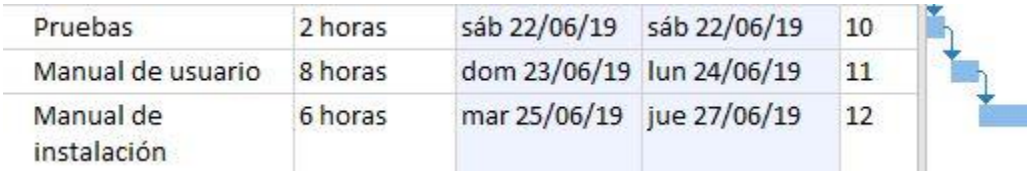
- Desarrollo de interfaces poco usables o que no cumplan los atributos de usabilidad

Por tanto, en la fase de Construcción sufrimos un retraso de 44 horas, por tanto, el diagrama de Gannt quedaría:

	Prototipo	4 horas	vie 19/04/19	sáb 20/04/19	
	Usabilidad y guias de diseño	6 horas	sáb 20/04/19	dom 21/04/19	
	Implementación	154 horas	lun 22/04/19	vie 21/06/19	7;8;9

Figura 7. Fase de construcción real

Por consecuente, la fase de transición, aunque se realizó en el tiempo estimado, sufrió un retraso de tiempo:



Pruebas	2 horas	sáb 22/06/19	sáb 22/06/19	10
Manual de usuario	8 horas	dom 23/06/19	lun 24/06/19	11
Manual de instalación	6 horas	mar 25/06/19	jue 27/06/19	12

Figura 8. Fase de transición real

Capítulo 4

Análisis

4.1. Análisis

Este apartado tiene como objetivo realizar un análisis del dominio del problema a resolver.

4.1.1. Requisitos

Un requisito es una condición o capacidad que necesita el usuario para resolver un problema o conseguir un objetivo determinado. Se presentan los requisitos del problema, tanto los funcionales, como no funcionales. [7]

4.1.1.1. Requisitos funcionales

Son una definición de los servicios que el sistema debe proporcionar, cómo debe reaccionar a una entrada particular y cómo se debe comportar ante situaciones particulares.

FRQ-001	El sistema deberá mostrar información acerca de AseguraEmpresa
Descripción	El sitio web deberá mostrar información acerca de lo que realiza y como lo realiza
FRQ-002	Disponer de un encabezado con secciones
Descripción	El sitio web tendrá que tener un menú encuadrado con todas las secciones bien definidas
FRQ-003	Disponer de una lista de activos
Descripción	El sistema deberá mostrar una lista de los activos que puede tener una empresa
FRQ-004	El sistema deberá permitir seleccionar los activos
FRQ-005	Disponer de una tabla de vulnerabilidades/amenazas
Descripción	El sistema deberá mostrar una tabla de vulnerabilidades/amenazas de todos activos o de los activos seleccionados
FRQ-006	El sistema deberá mostrar una tabla con salvaguardas
Descripción	El sistema deberá mostrar una tabla de salvaguardas de todos activos o de los activos seleccionados
FRQ-007	El sistema deberá permitir seleccionar las salvaguardas
FRQ-008	El sistema deberá ser capaz de calcular el riesgo de pérdida de información, en porcentaje, que puede sufrir la empresa
FRQ-009	El sistema deberá ser capaz de mostrar la cifra de riesgo que tiene la empresa, diciendo así, si esta es alta, media o baja.
FRQ-010	El sistema deberá permitir realizar un tratamiento de los riesgos

Tabla 26. Requisitos funcionales

4.1.1.2. Requisitos no funcionales

Restricciones que afectan a los servicios o funciones del sistema, tales como restricciones de tiempo, sobre el proceso de desarrollo, estándares, etc.

NFR-001	Facilidad de uso
Descripción	El sitio web deberá mostrar una buena interfaz en la que su uso sea intuitivo y fácil de usar
NFR-002	Rendimiento
Descripción	El sitio web deberá mostrar fluidez
NFR-003	Disponibilidad
Descripción	El sitio web deberá tener disponibilidad 24 horas los 7 días de la semana
NFR-004	Rápida respuesta del servidor
Descripción	El servidor deberá cargar rápido todo el contenido que el usuario solicita
NFR-005	Calidad de imágenes
Descripción	El sitio web deberá mostrar buena calidad de imágenes
NFR-006	Buen diseño adaptativo
Descripción	El sitio web deberá seguir un diseño adaptativo, que se adapte correctamente a cualquier navegador
NFR-007	La base de datos será en lenguaje MariaDB
NFR-008	La página web será dinámica y estará implementada con PHP.
NFR-009	El servidor estará alojado con Sistema operativo Ubuntu
NFR-010	El acceso al sistema será a través de HTTP.

Tabla 27. Requisitos no funcionales

4.1.2. Casos de uso

4.1.2.1. Actores

Se le llama actor a toda entidad externa al sistema que guarda una relación con éste y que le demanda una funcionalidad.

En la aplicación web solo existe un tipo de actor que es el usuario. Es el que visitará la página web y se informará de todas vulnerabilidades, amenazas y posibles soluciones que puede tener su empresa para garantizar la seguridad de la información. [8]

4.1.2.2. Diagramas de casos de uso

A continuación, mostramos el diagrama de casos de uso:

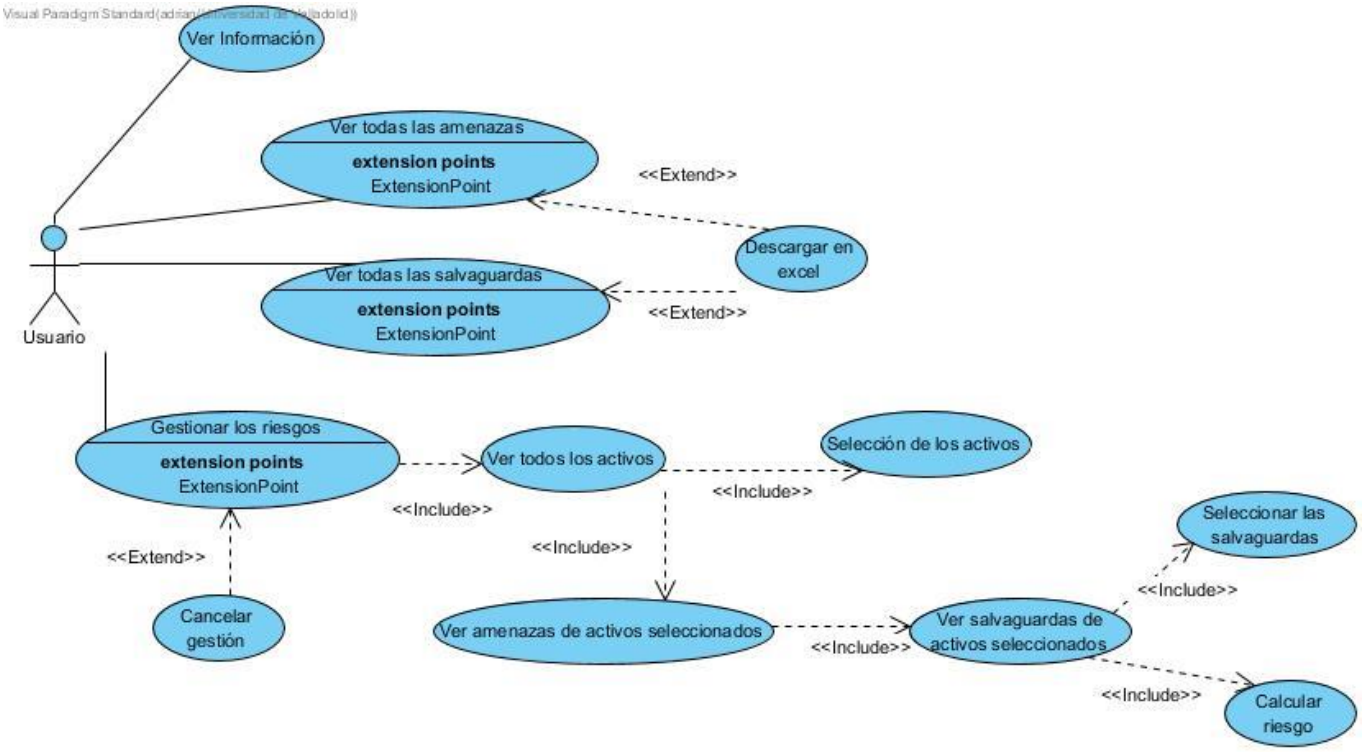


Figura 9. Diagrama de casos de uso

4.1.2.3. Especificación de casos de uso

A continuación, mostramos el paso a paso de cada uno de los casos de uso:

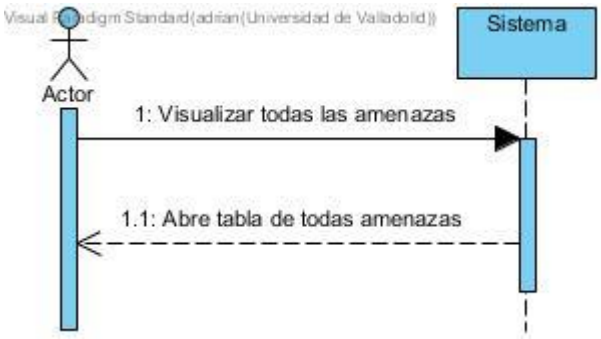


Figura 10. Diagrama de secuencia de caso de uso 1

UC-001	**Ver todas amenazas**	
Descripción	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario desea ver todas amenazas que pueden tener cualquier activo	
Precondición	El usuario se encuentra navegando por el sitio web	
Secuencia Normal	Paso	Acción
	1	El actor Usuario (ACT-0001) pulsa sobre la sección "*Ver todas amenazas"* en el navigation bar.
	2	El sistema redirige a la página donde se muestra la información que desea ver el usuario
Postcondición	El sistema muestra correctamente la información que el usuario ha pulsado para ver	

Tabla 28. Caso de uso 1: Ver todas las amenazas

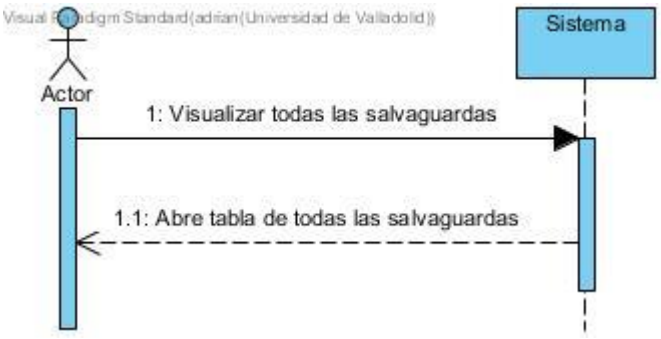


Figura 11. Diagrama de secuencia de caso de uso 2

UC-002	**Ver todas salvaguardas**	
Descripción	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario desea ver todas las salvaguardas que pueden tener cualquier activo	
Precondición	El usuario se encuentra navegando por el sitio web	
Secuencia Normal	Paso	Acción
	1	El actor Usuario (ACT-0001) pulsa sobre la sección "*Ver todas salvaguardas"* en el navigation bar.
	2	El sistema redirige a la página donde se muestra la información que desea ver el usuario
Postcondición	El sistema muestra correctamente la información que el usuario ha pulsado para ver	

Tabla 29. Caso de uso 2: Ver todas las salvaguardas

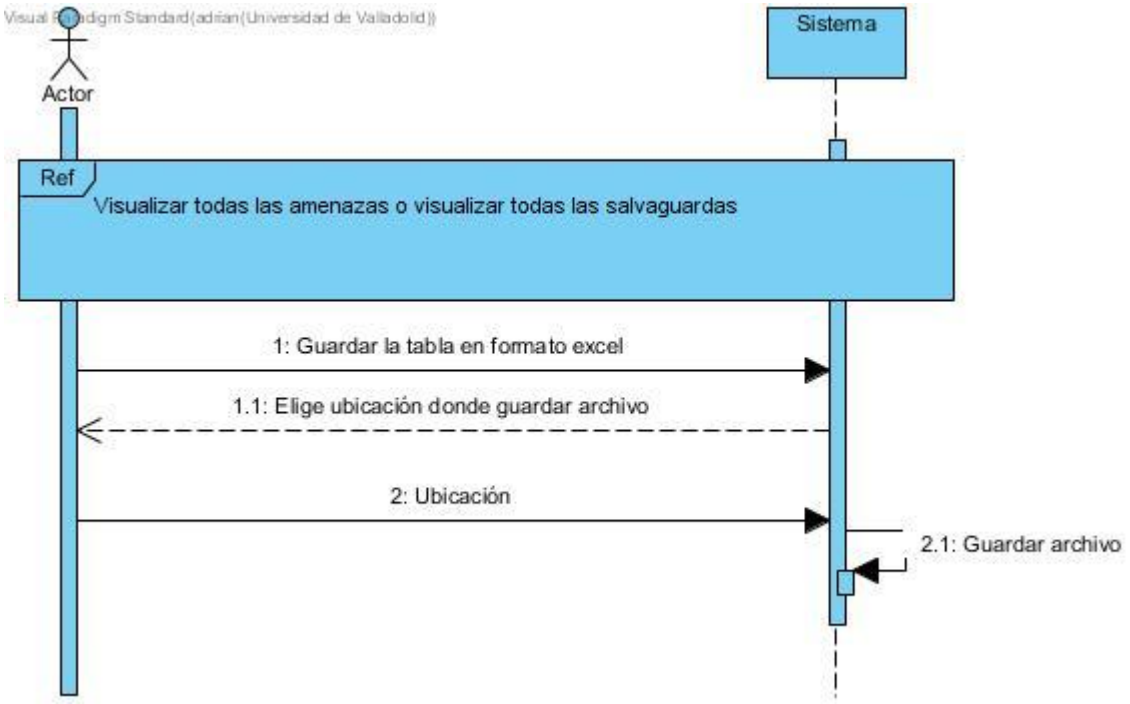


Figura 12. Diagrama de secuencia caso de uso 3

UC-003	**Descargar en Excel las tablas**	
Descripción	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario desea descargar en formato Excel las tablas de todas amenazas o salvaguardas	
Precondición	El actor Usuario (ACT-0001) se encuentra navegando en la sección de ver todas las amenazas o ver todas las salvaguardas	
Secuencia Normal	Paso	Acción
	1	El actor Usuario (ACT-0001) pulsa sobre el botón de descargar en excel
	2	El sistema pregunta al actor Usuario (ACT-0001) dónde desea guardar el archivo
	3	El actor Usuario (ACT-0001) elige donde guardar el archivo
	4	El sistema guarda el archivo
Postcondición	El sistema guarda correctamente el archivo en la ubicación elegida por el actor Usuario (ACT-0001)	

Tabla 30. Caso de uso 3. Descargar en Excel las tablas

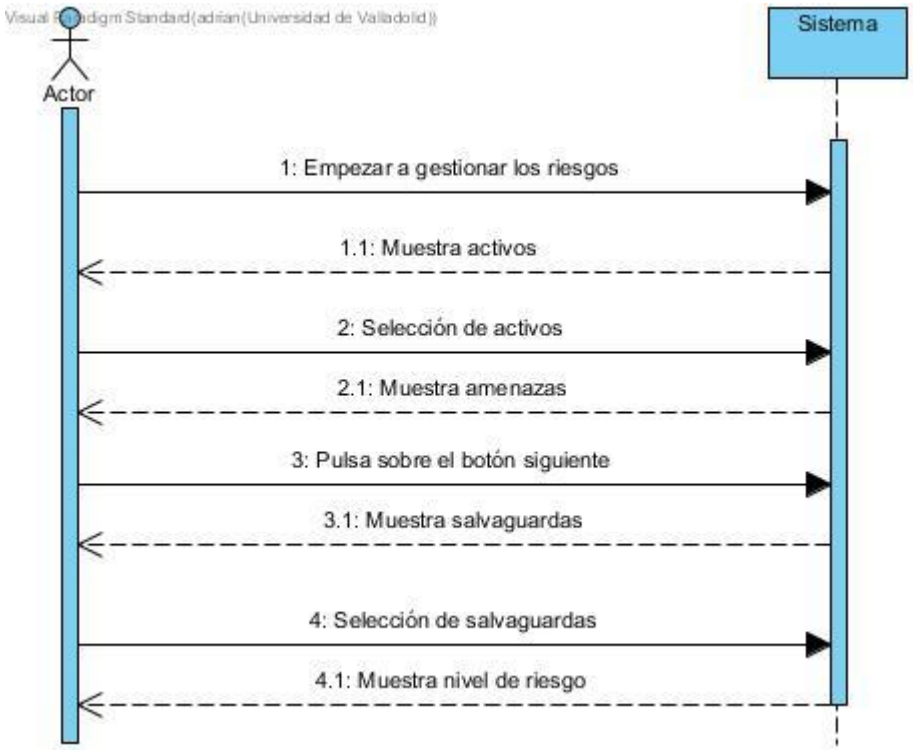


Figura 13. Diagrama de secuencia caso de uso 4

UC-004	**Gestionar riesgos**	
Descripción	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario comienza a gestionar los riesgos que puede tener su empresa	
Precondición	El usuario debe de estar navegando por la página web	
Secuencia Normal	Paso	Acción
	1	El actor Usuario (ACT-0001) pulsa sobre el botón de empezar a gestionar los riesgos
	2	El sistema redirige al actor Usuario (ACT-0001) a la página dónde se muestran todos activos que nosotros consideramos que puede tener una empresa
	3	El actor Usuario (ACT-0001) selecciona los activos que tiene en su empresa
	4	El sistema redirige al actor Usuario (ACT-0001) a la página donde se muestran todas amenazas que pueden tener los activos seleccionados.
	5	El actor Usuario (ACT-0001) pulsa sobre el botón siguiente
	6	El sistema redirige al actor Usuario (ACT-0001) a la página donde se muestra las salvaguardas que deben tener los activos seleccionados
	7	El actor Usuario (ACT-0001) selecciona las salvaguardas que dispone en su empresa para sus activos
	8	El sistema calcula y muestra el riesgo de pérdida de información que tiene la empresa del actor Usuario (ACT-0001)
Postcondición	El sistema muestra correctamente la información que el usuario ha pulsado para ver	

Tabla 31. Caso de uso 4: Gestionar riesgos

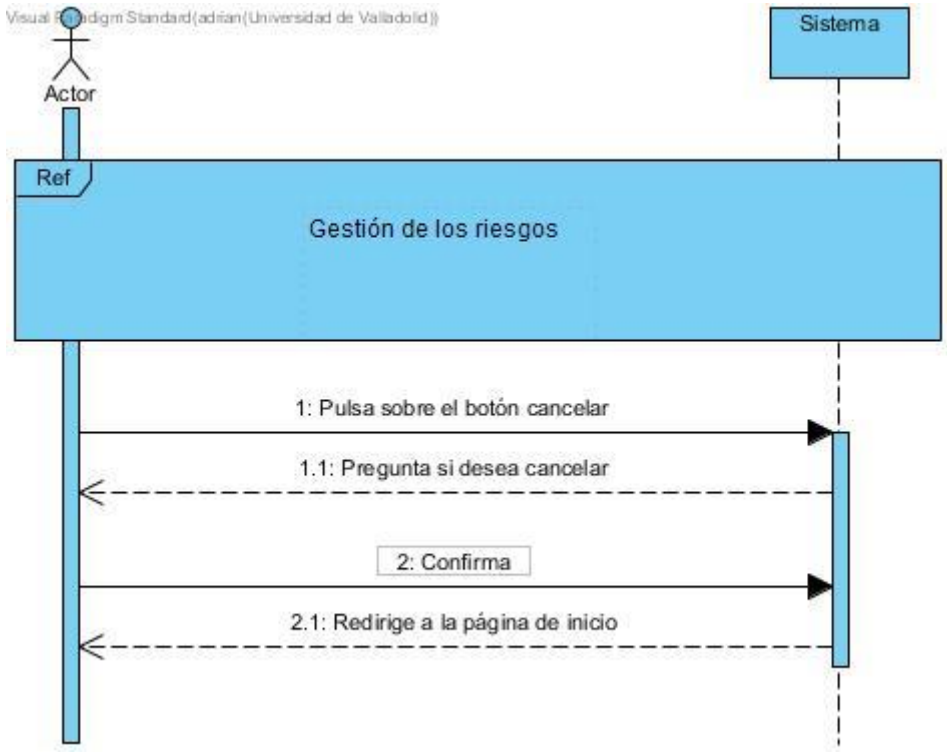


Figura 14. Diagrama de caso de uso 5. Cancelar gestión de los riesgos

UC-005	**Cancelar gestión**	
Descripción	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario desea cancelar la gestión de sus riesgos.	
Precondición	El actor Usuario (ACT-0001) se encuentra en el caso de uso "Gestión de riesgos"	
Secuencia Normal	Paso	Acción
	1	El actor Usuario (ACT-0001) pulsa sobre el botón cancelar
	2	El sistema pregunta al actor Usuario (ACT-0001) qué si quiere cancelar la gestión de sus riesgos
	3	El actor Usuario (ACT-0001) confirma
	4	El sistema cancela la gestión y redirige al usuario a la página de inicio

Tabla 32. Caso de uso 5. Cancelar gestión de los riesgos

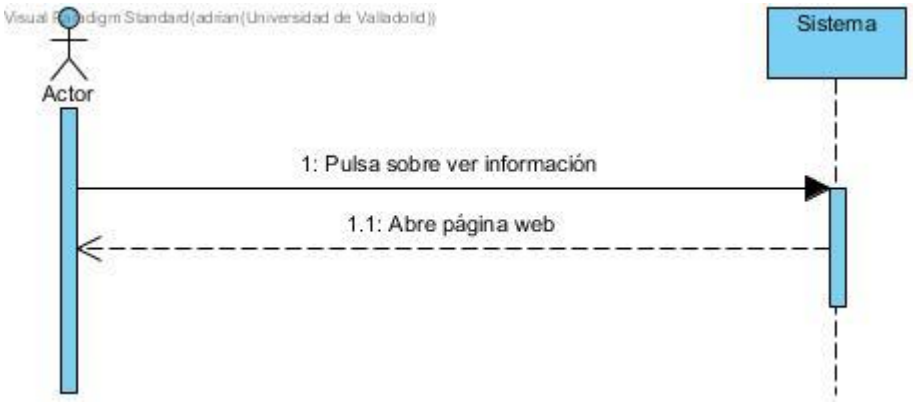


Figura 15. Diagrama de secuencia caso de uso 6

UC-006	**Ver información**	
Descripción	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario desea ver información de la página web	
Precondición	El actor Usuario (ACT-0001) se encuentra navegando en la página web	
Secuencia Normal	Paso	Acción
	1	El actor Usuario (ACT-0001) pulsa sobre el botón de "Información" del navigation web.
	2	El sistema redirige al actor Usuario (ACT-0001) a la página.
Postcondición	El sistema muestra correctamente la información	

Tabla 33. Caso de uso 6. Ver información

4.1.3. Modelo de dominio

A continuación, se muestra el diagrama de dominio de la aplicación:

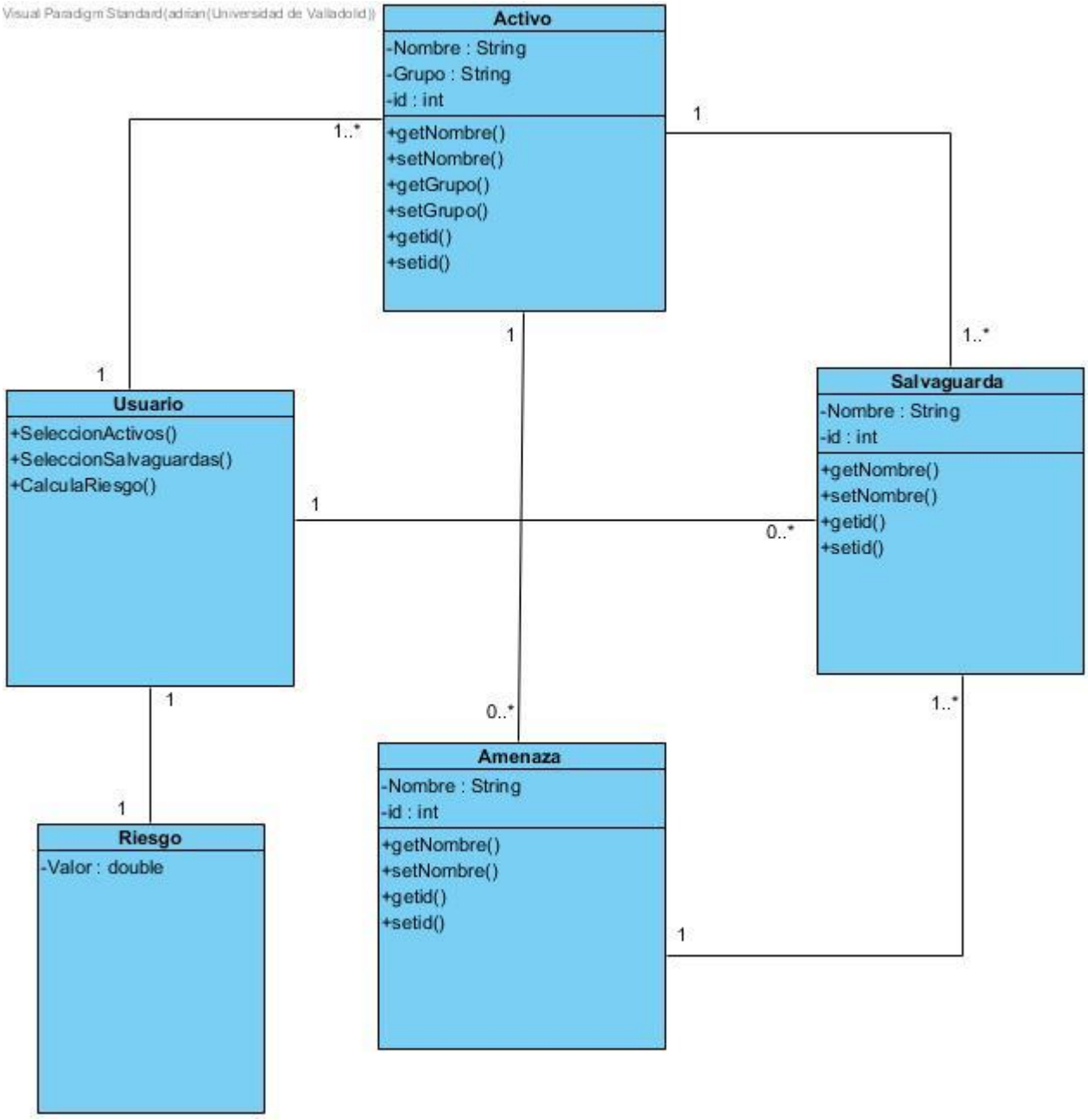


Figura 16. Modelo de dominio

Capítulo 5

Diseño

5.1. Arquitectura del sistema

5.1.1. Patrones arquitectónicos

5.1.1.1. Patrón MVC

La web estará diseñada principalmente bajo el patrón Modelo-Vista-Controlador. MVC es un patrón de arquitectura de las aplicaciones software que separa la lógica de negocio de la interfaz de usuario. Los tres componentes de este patrón son: [8]

- Modelo: Es la representación específica de la información con la que se opera. Incluye los datos y lógica para operar con ellos.

- Controlador: Responde a eventos de la interfaz de usuario e invoca cambios en el modelo y en la vista.

- Vista: Es la presentación del modelo de forma adecuada para interactuar con ella, normalmente a través de una interfaz de usuario.

El MVC que utilizamos es el MVC Pasivo que, a diferencia del activo, es el controlador el que manipula el modelo exclusivamente e informa a la vista que éste ha cambiado y debe ser refrescada.

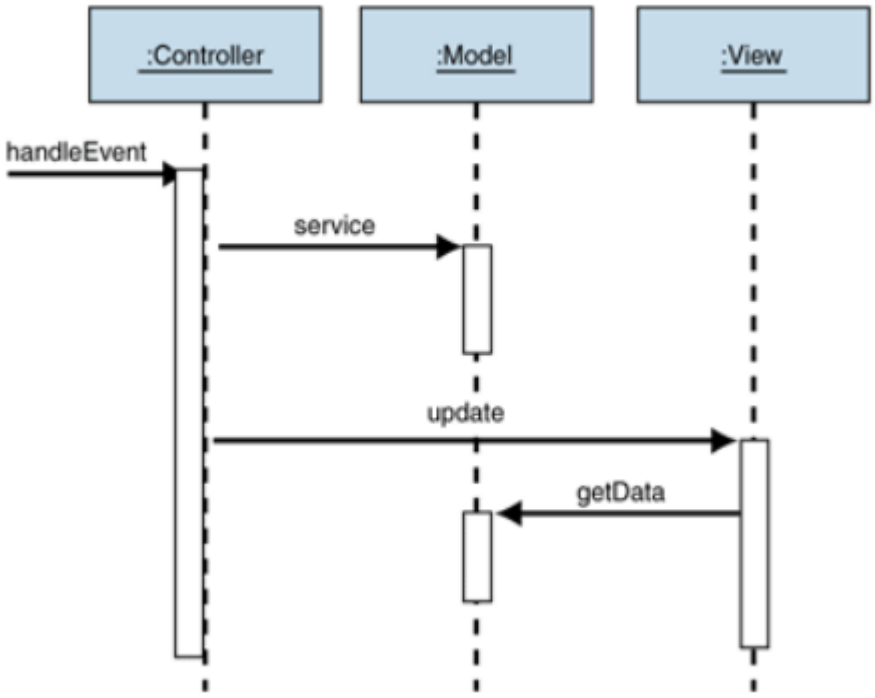


Tabla 34. Patrón MVC

5.1.1.2. Otros patrones

5.1.1.2.1. Patrón Data Mapper

Utilizamos el patrón Data Mapper para interaccionar con la base de datos.

Mapper: es un objeto que establece una comunicación entre dos objetos independientes.

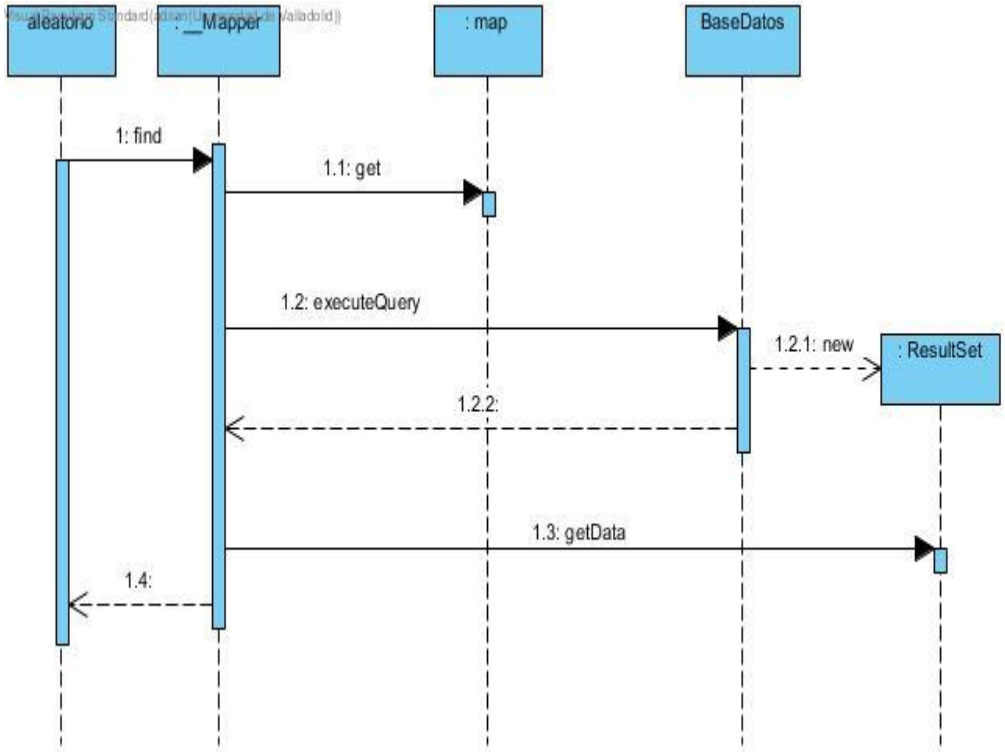


Figura 17. Patrón Data Mapper

5.1.2. Arquitectura y diagrama arquitectónico

El estilo arquitectónico que utilizaremos es la arquitectura de capas. En la arquitectura por capas se definen las capas que se utilizan en la aplicación de manera que sólo se comunican entre si las capas adyacentes. Las capas que vamos a utilizar son: [9] [10]

- Capa de presentación: Es la interfaz de usuario. Hace la información accesible al usuario. Mostrará la información al usuario, recuperará los datos del modelo e inicializará los controladores. En esta capa se encuentra la vista del patrón MVC. Se define el diseño de la web.

- Capa de dominio: Coordina la aplicación, procesa los comandos, toma decisiones y realiza los cálculos. Recibe las entradas del usuario como eventos, lo traslada al modelo y muestra las vistas. En esta capa se encuentra la mayor parte de la funcionalidad del sistema.

- Capa de acceso a datos: Mueve los datos entre las capas.

- Capa de almacenamiento de datos: Es de donde se obtiene la información y los datos. Suele ser una base de datos como MariaDB.

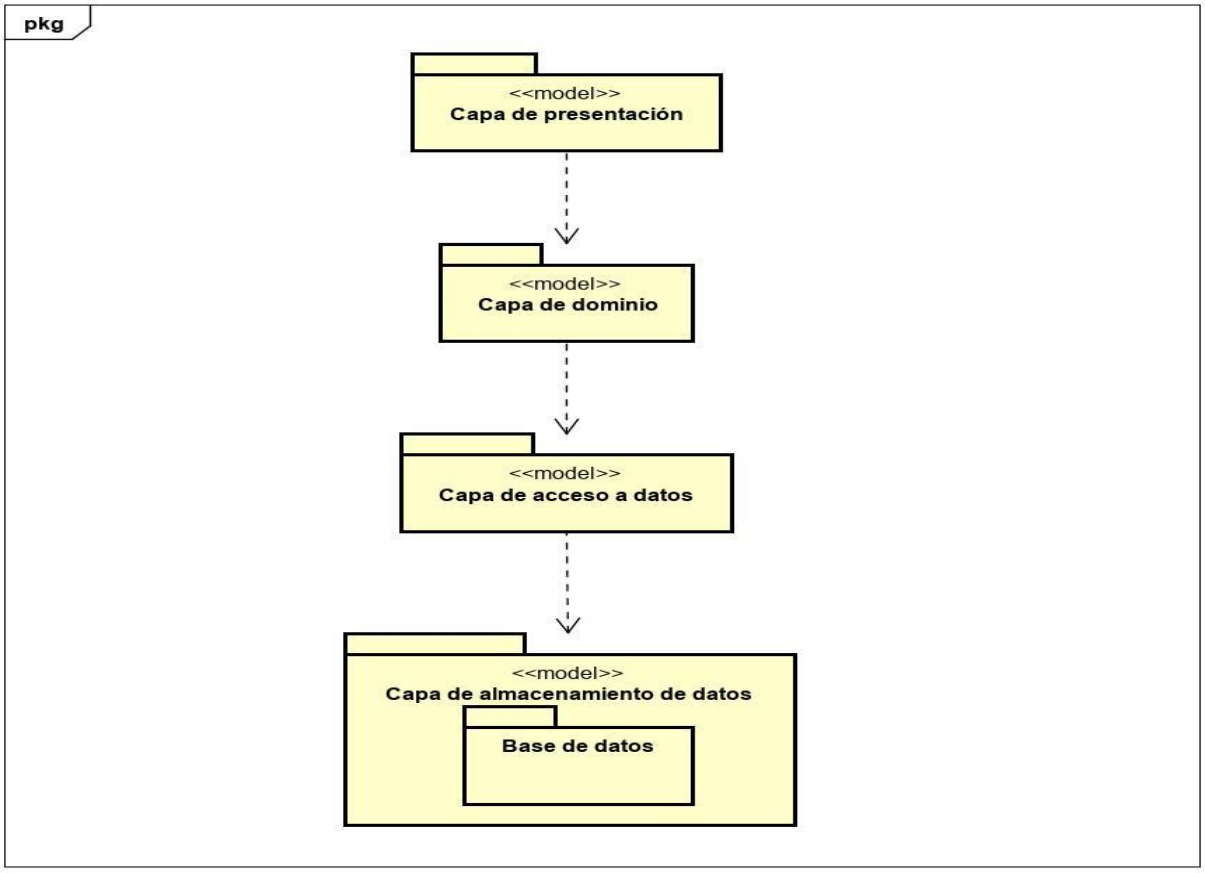


Figura 18. Modelado de la arquitectura

5.1.3. Diagrama de despliegue

Un diagrama de despliegue modela la arquitectura en tiempo de ejecución del sistema. Esto muestra la configuración de elementos de hardware (nodos) y muestra cómo los elementos y artefactos del software se trazan en esos nodos. [17]

En nuestro caso, se compone de un dispositivo, que será el dispositivo del usuario con el que acceden al sitio web. El dispositivo contiene un navegador web para comunicarse con nuestro servidor web mediante un protocolo HTTP.

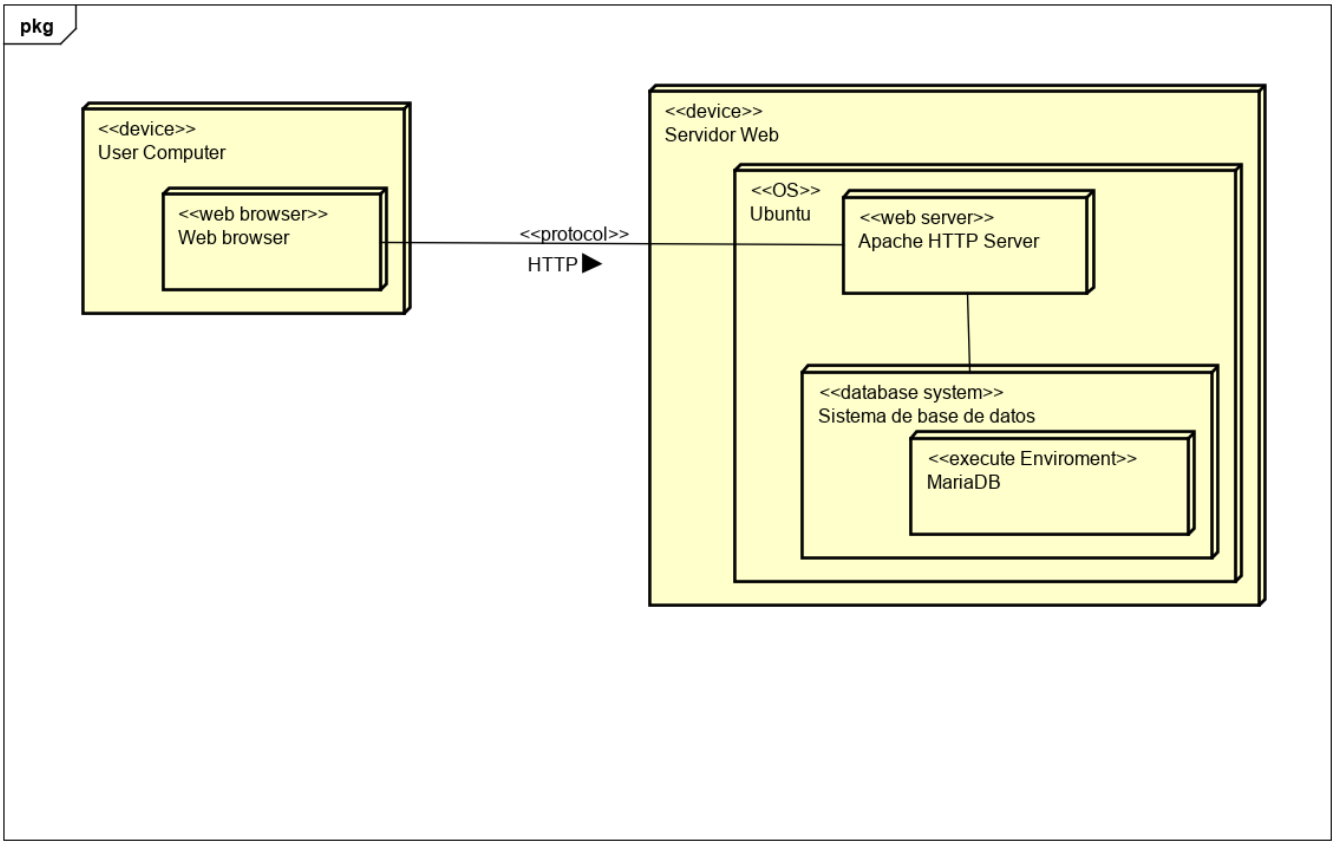


Figura 19. Diagrama de despliegue

5.1.4. Diagramas de secuencia

A continuación, mostramos los diagramas de secuencia de los casos de uso:

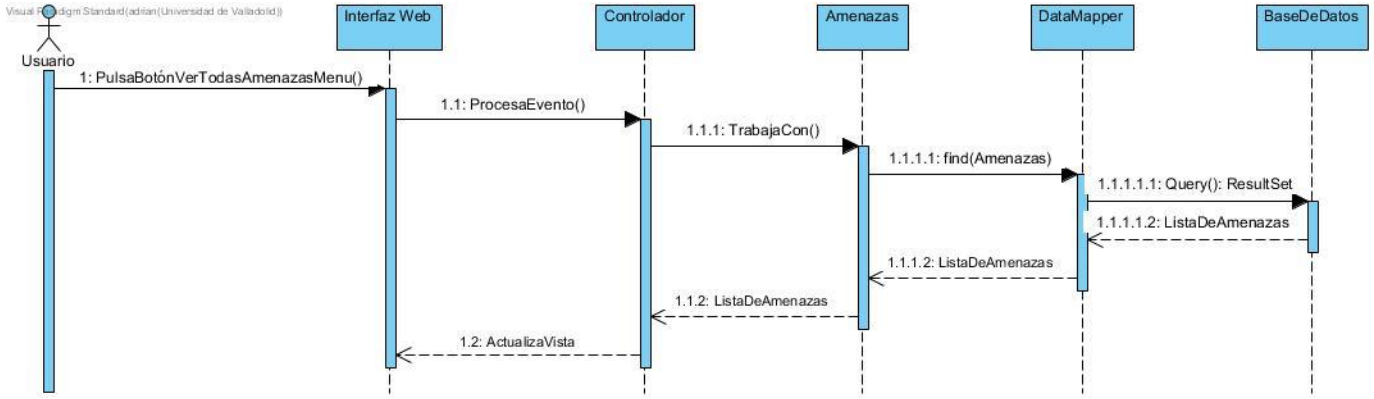


Figura 20. Diagrama de secuencia. Ver todas las amenazas

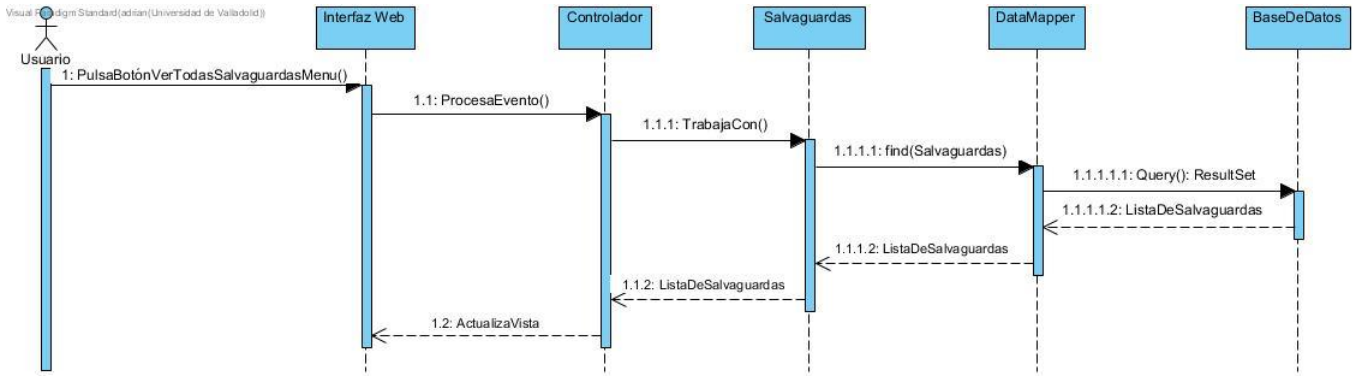


Figura 21. Diagrama de secuencia. Ver todas las salvaguardas

El siguiente caso de uso también es válido para el caso de uso: Ver todas las salvaguardas.

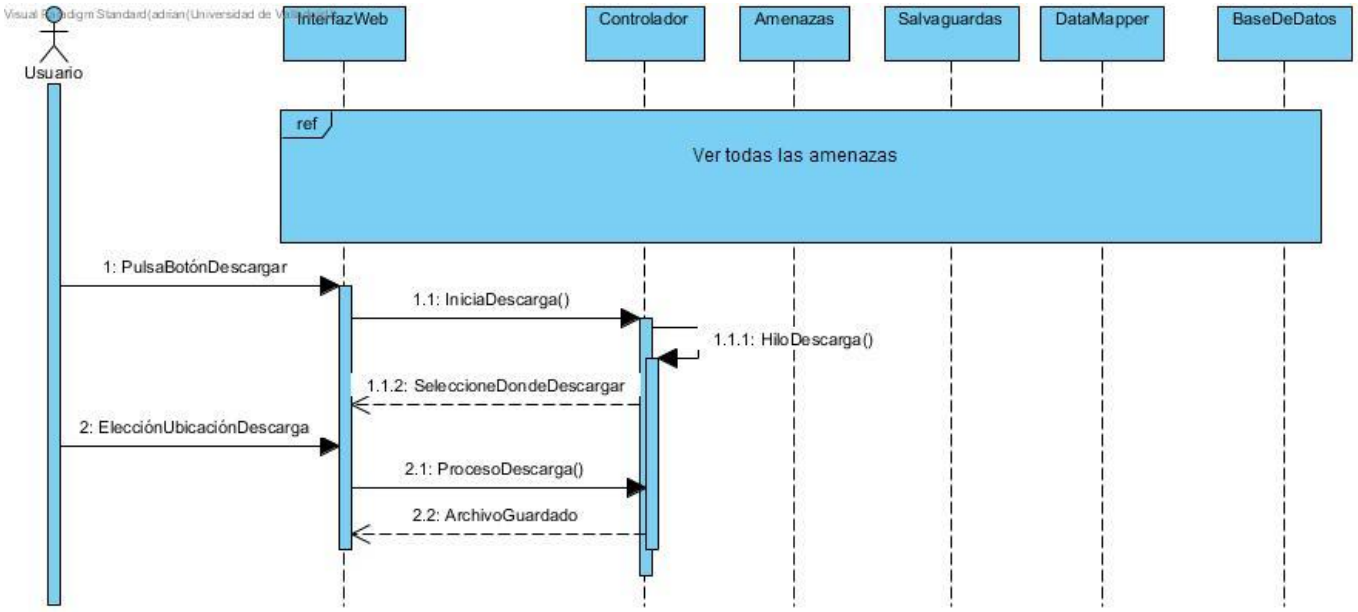


Figura 22. Diagrama de secuencia. Descargar en Excel

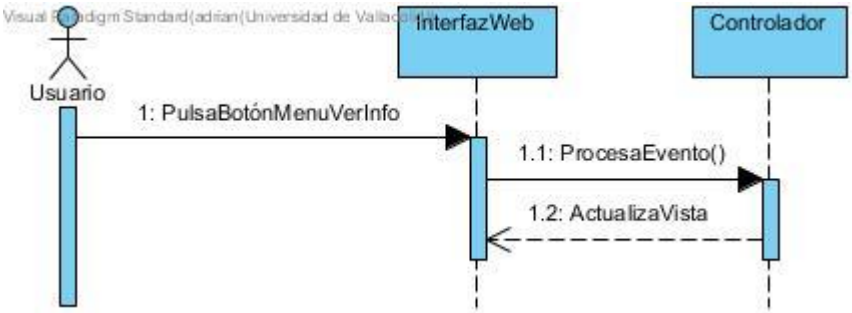


Figura 23. Diagrama de secuencia. Ver información

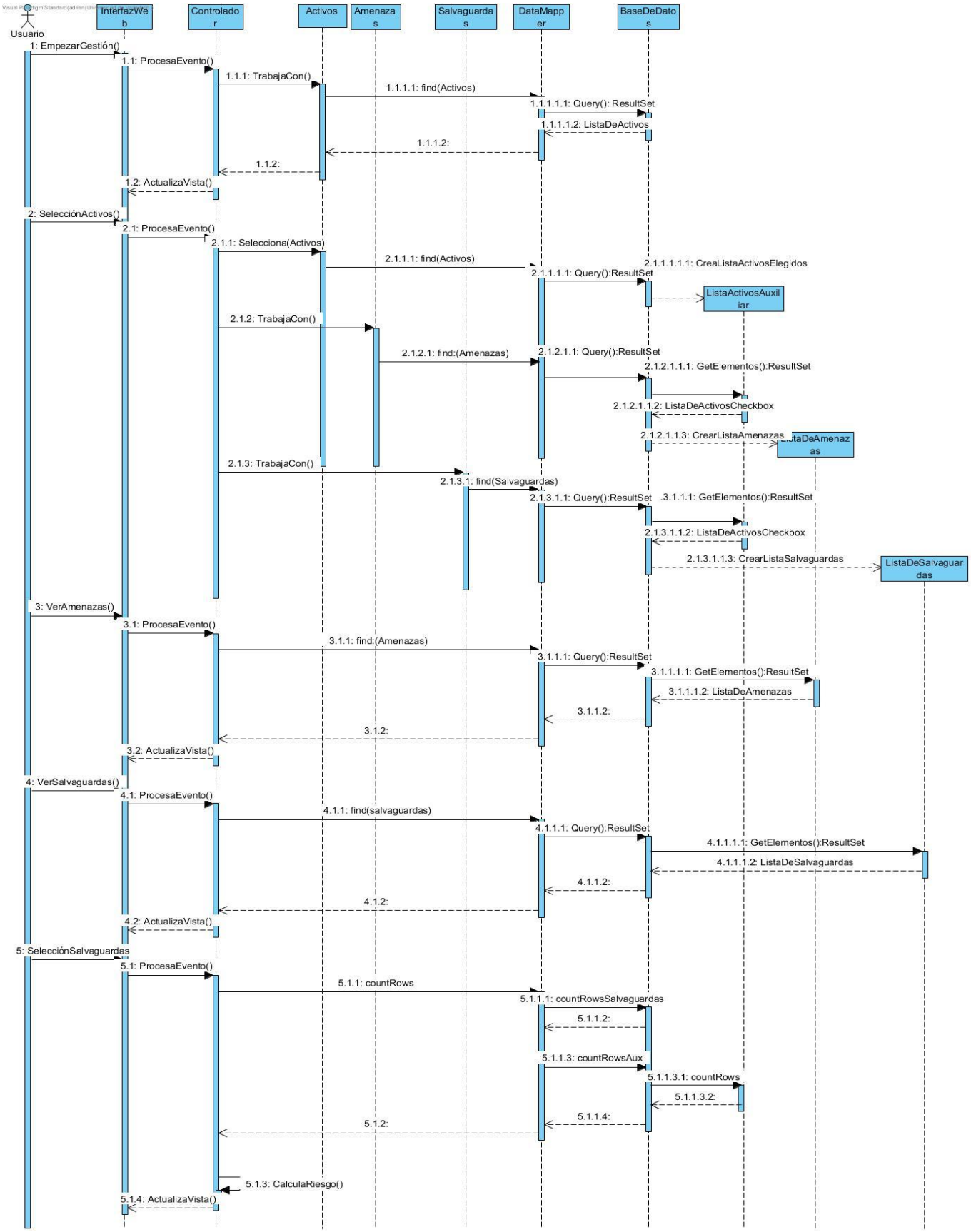


Figura 24. Diagrama de secuencia. Gestión de riesgos

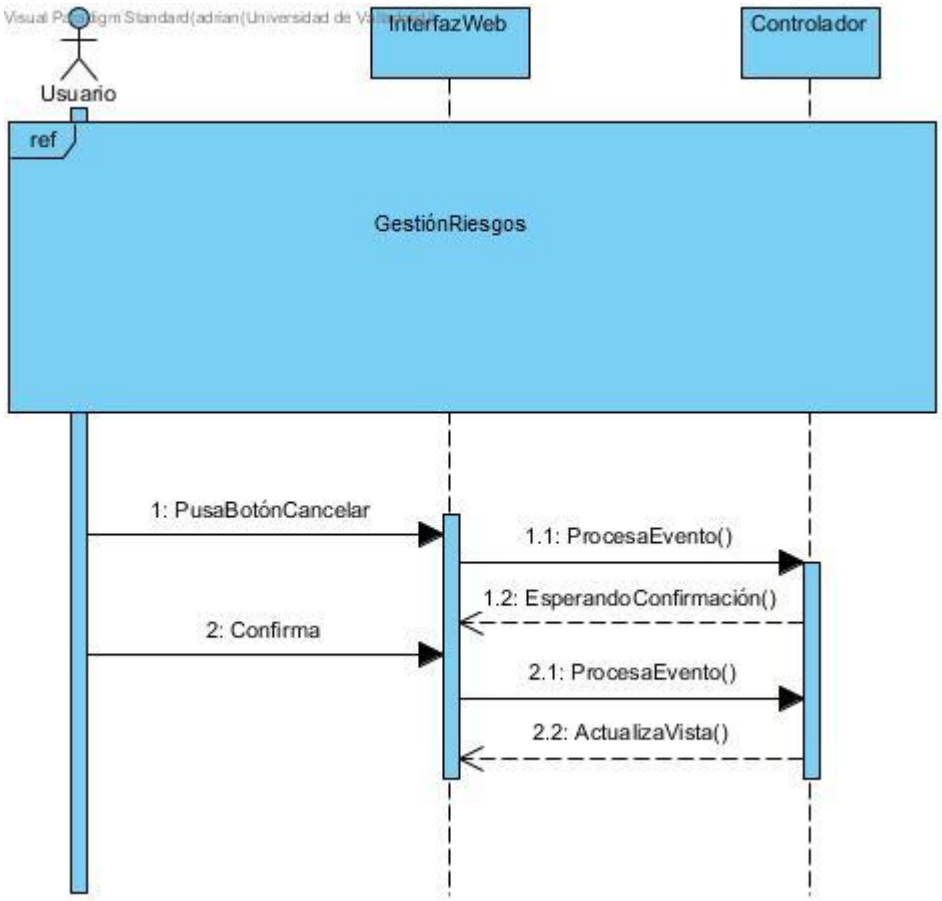


Figura 25. Diagrama de secuencia. Cancelar Gestión de riesgos

5.1.5. Modelo relacional de datos

En nuestra base de datos podemos diferenciar cuatro tablas:

- Tabla Activos: Hemos insertado todos los activos que hemos considerado antes que puede contener una empresa cualquiera. Consta de dos columnas: grupo de activos que meten a varios activos en un mismo grupo y la segunda columna que son todos los activos que tienen los grupos de activos. Como clave primaria hemos elegido las dos columnas existentes ya que no puede haber dos mismos activos en un grupo de activos.
- Tabla Amenazas: Hemos insertado todas las amenazas que hemos considerado que puede tener un activo de una empresa. Consta también de dos columnas: activos, que son los mismos que la tabla Activos y la segunda columna es amenazas, en la que se inserta cada amenaza que tiene un activo. Como clave primara hemos elegido las dos columnas, ya que un activo puede tener varias amenazas, pero no pueden repetirse.
- Tabla Salvaguardas: Esta tabla contiene todas las salvaguardas que hemos considerado para cada amenaza. Consta de tres columnas: activos, amenazas y salvaguarda. Al principio pensamos en eliminar una de las tablas entre Amenazas y Salvaguardas, pero no podíamos implementar el hecho de que un activo puede tener varias amenazas y varias salvaguardas para cada amenaza. Como clave primaria hemos elegido las tres columnas.
- Tabla Aux: Es una tabla auxiliar, en los que se eliminan los registros y se vuelven a introducir cada vez que se hace una nueva gestión de riesgos. La idea de esta tabla es recoger los POST que hace el usuario al seleccionar los activos que tiene en su empresa con los checkbox, que se introduzcan los activos seleccionados en los registros de la tabla, para luego realizar operaciones entre las tablas Amenazas y Salvaguardas solo de los activos seleccionados. Solo tiene una columna y se llama activos.

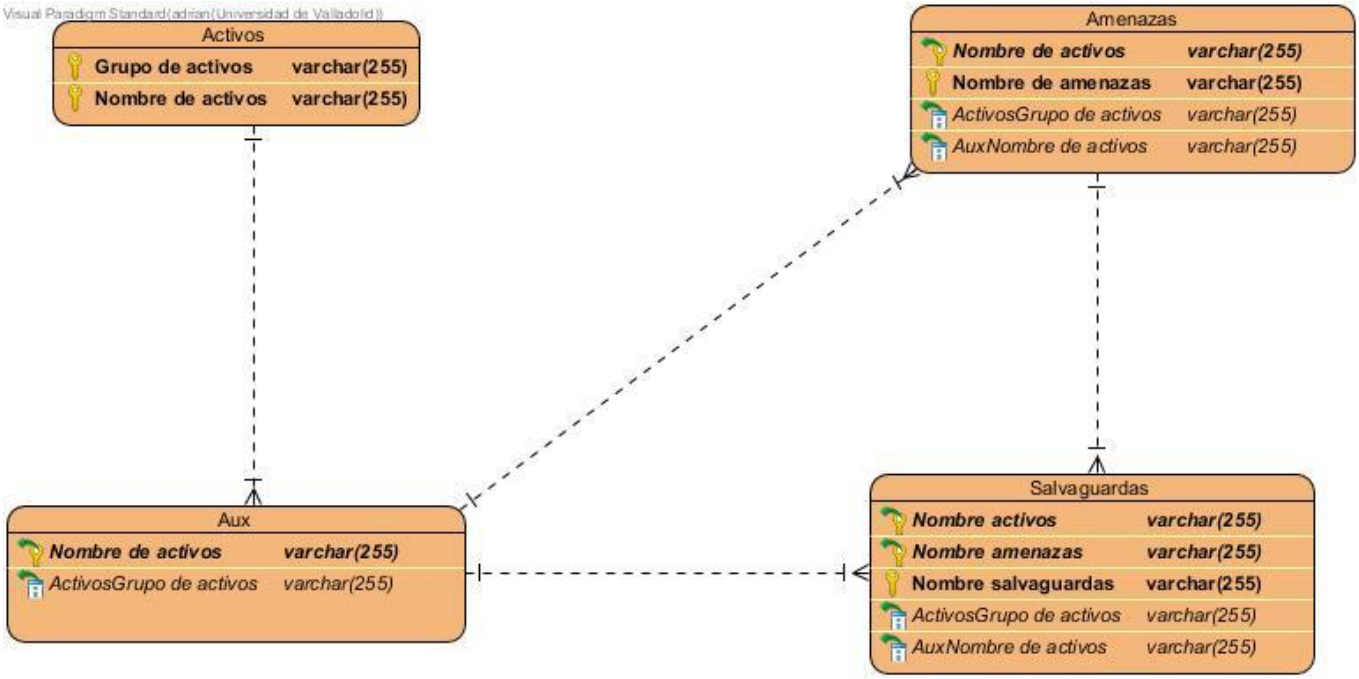


Figura 26. Diagrama modelo relacional de datos E-R

Capítulo 6

Implementación

6.1. Implementación

6.1.1. Prototipo

6.1.1.1. Usabilidad

La usabilidad es la facilidad con que los usuarios que utilizan la aplicación web pueden usarla. Para conseguir esto, hay que hacer la interfaz de la aplicación web usable, es decir, de fácil manejo para el usuario. Para ello, en la implementación de la aplicación web se van a tener en cuenta los siguientes **atributos de usabilidad**: [11]

- Facilidad de aprendizaje: La aplicación tiene que ser sencilla a la hora de usarse, ya que eso influirá en que los clientes no dejen de utilizarla.
- Facilidad de recuerdo: Es la facilidad que tiene el usuario para poder recordar cómo se usa la aplicación.
- Gestión de errores: Evitar los errores al introducir datos en la interfaz, informándolo de ello.

Por otro lado, también se ha basado el diseño en determinados **patrones visuales** [12] [13]:

- Table filter: Utilizamos un filtro de tablas ya que, en nuestra aplicación web, hay tablas con un conjunto de datos muy grande. Se usa cuando una o más columnas se pueden resumir en diferentes categorías.
- Alternative row colors: Se utiliza para diferenciar mejor una columna de otra, ya que tenemos muchas filas y varias columnas en las tablas y cada fila puede ser de diferente tamaño.

- Vertical Menú: Se usa un menú vertical cuando el usuario debe navegar entre las secciones de un sitio web, pero el espacio de ésta es limitado.
- Home link: El usuario debe poder navegar fácilmente hasta el punto de inicio o la página principal del sitio web.

6.1.1.2. Prototipo

A continuación, mostramos un prototipo de bajo coste del caso de uso principal. [14]

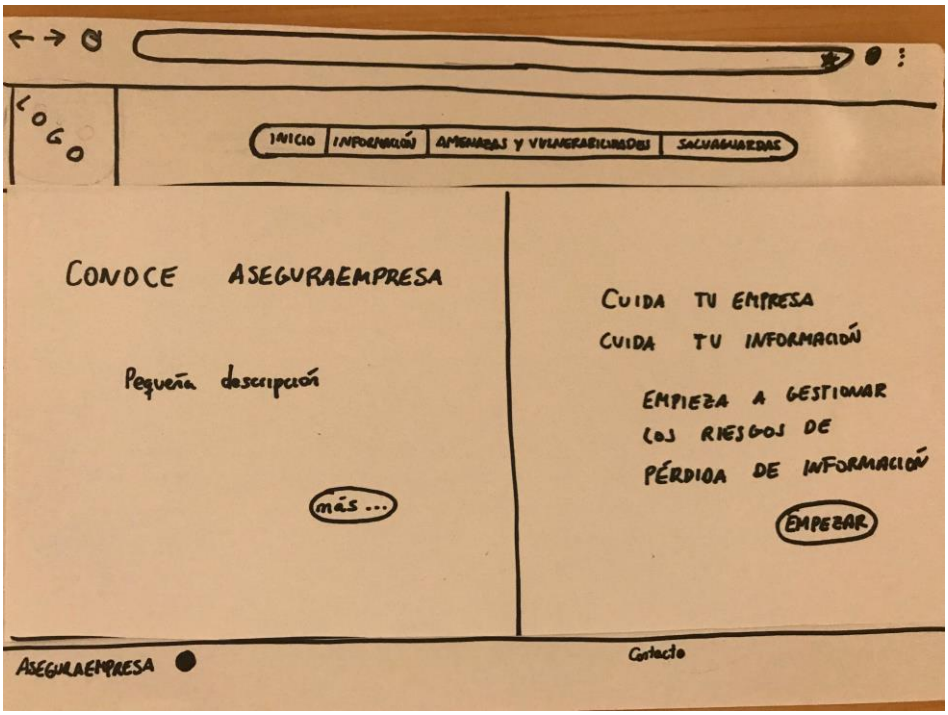


Figura 27. Pantalla de inicio

La pantalla de inicio consta de una breve explicación de lo que la aplicación web hace, mostrando el usuario los botones vivibles, para que pueda realizar la gestión de los riesgos. También dispondrá del menú vertical fijo en todas las páginas de la aplicación para que pueda navegar por ésta cuando le apetezca al usuario.

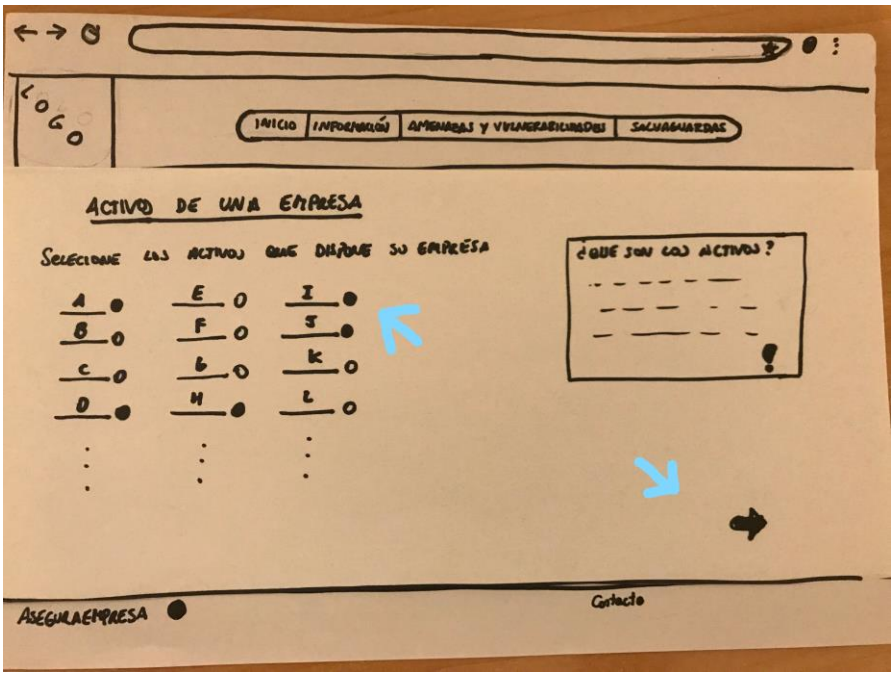


Figura 28. Pantalla selección de los activos

Se muestran los activos en una especie de tabla con un checkbox al lado de cada uno para que se pueda seleccionar. También se ira explicando al usuario qué es cada uno de los términos con los que está trabajando.

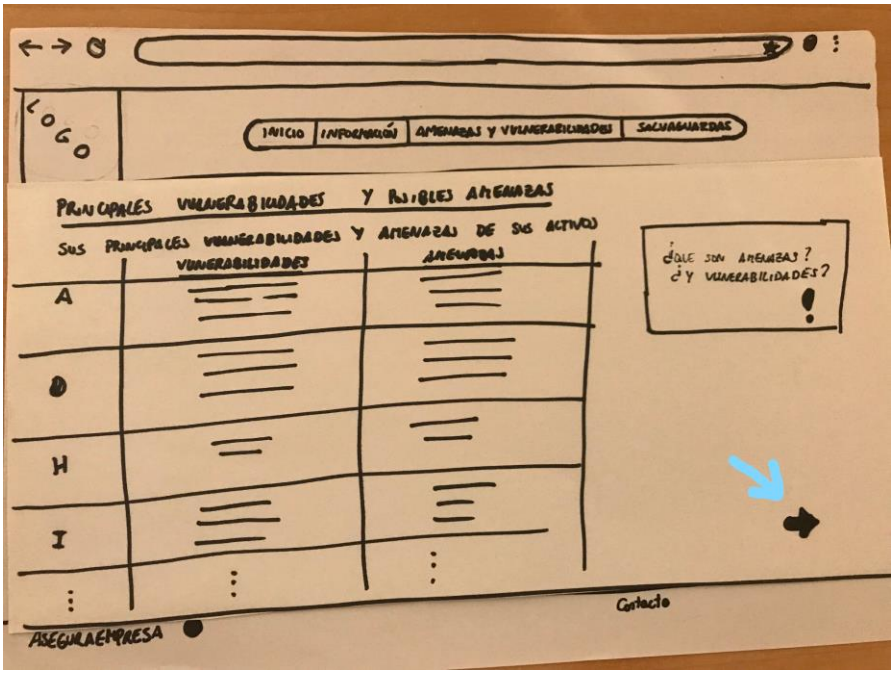


Figura 29. Pantalla donde se muestran las amenazas

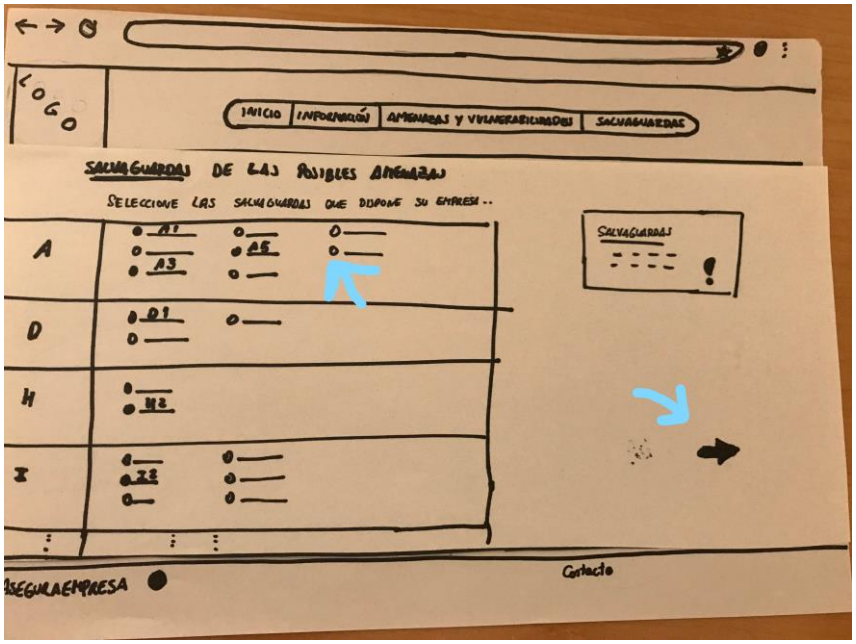


Figura 30. Pantalla de selección de salvaguardas

Se irá guiando al usuario visiblemente hasta que pueda llegar al final de la gestión,

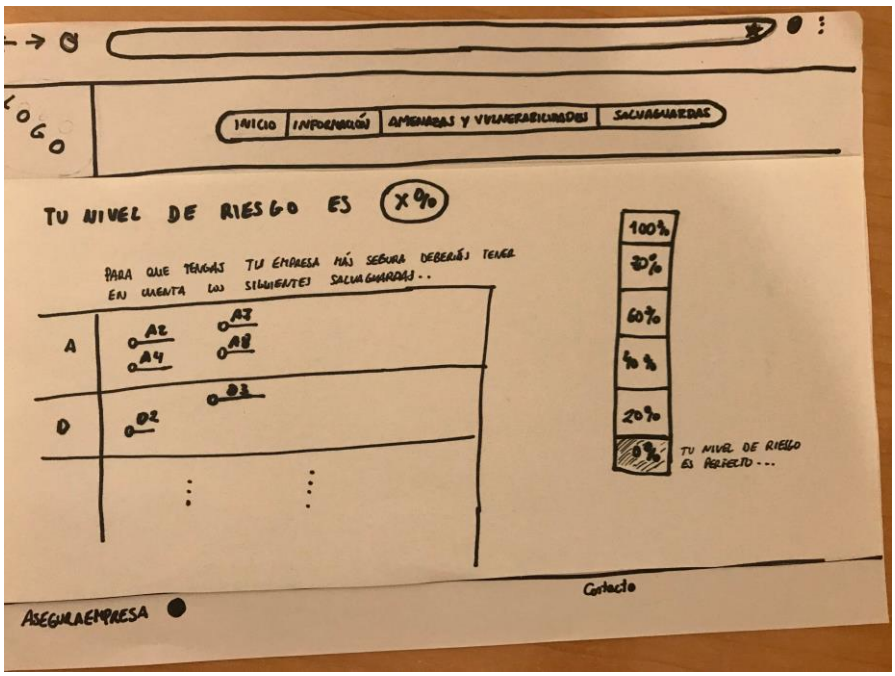


Figura 31. Pantalla donde se muestra el nivel de riesgo

Capítulo 7

Pruebas

7.1. Pruebas de caja negra

A continuación, se va a explicar el conjunto de pruebas que se han llevado a cabo a lo largo del desarrollo del proyecto. La realización de pruebas es un proceso necesario, ya que, podemos descubrir y eliminar posibles errores que se hayan podido cometer en la etapa de desarrollo. Vamos a centrarnos en las pruebas de caja negra.

Las pruebas de caja negra son pruebas funcionales donde se evalúa el funcionamiento del software, que hemos definido en requisitos y casos de uso. Se limitan a que nosotros que somos el tester, probamos con datos de entrada y comprobamos que sale lo que nosotros queremos que salga. [15]

Prueba de caja negra-001	Botón Inicio
Descripción	El usuario desea regresar a la pantalla inicial desde cualquier pantalla pulsando sobre la sección Inicio del menú
Resultado esperado	Redirigir a la pantalla inicial
Salida	Correcto

Tabla 35. Prueba de caja negra 1. Botón de inicio

Prueba de caja negra-002	Menú despegable
Descripción	El usuario desea ir a las páginas del menú
Resultado esperado	Redirección a la pantalla que pulse del menú
Salida	Correcto

Tabla 36. Prueba de caja negra 2. Menú despegable

Prueba de caja negra-003	No selección de checkbox en la selección de activos
Descripción	El usuario desea pasar a la pantalla de visualización de las amenazas en la gestión de riesgo sin seleccionar ningún activo
Resultado esperado	Alerta al usuario de que no se ha seleccionado ningún activo.
Salida	Incorrecto. Error de base de datos

Tabla 37. Prueba de caja negra 3. No selección de checkbox en la selección de activos

Prueba de caja negra-004	Paso a la pantalla de amenazas con checkbox seleccionados
Descripción	El usuario desea pasar a la pantalla de visualización de las amenazas en la gestión de riesgo seleccionando al menos un activo.
Resultado esperado	El usuario visualiza las amenazas de los activos que ha seleccionado previamente.
Salida	Correcto

Tabla 38. Prueba de caja negra 4. Paso a la pantalla de amenazas con checkbox seleccionados

Prueba de caja negra-005	Utilización de los filtros de tablas
Descripción	El usuario desea filtrar la tabla y pone parte del nombre que desea buscar
Resultado esperado	La tabla se acorta y muestra sólo los datos que coinciden con lo que ha puesto el usuario
Salida	Correcto

Tabla 39. Prueba de caja negra 5. Filtro de tablas

Prueba de caja negra-006	Visualización de salvaguardas
Descripción	El usuario quiere ver las salvaguardas de sus activos previamente seleccionados
Resultado esperado	Se muestran las salvaguardas de los activos que ha seleccionado el usuario.
Salida	Correcto

Tabla 40. Prueba de caja negra 6. Visualización de salvaguardas

Prueba de caja negra-007	Pasar al cálculo del riesgo sin seleccionar ninguna salvaguarda
Descripción	El usuario quiere calcular su riesgo de pérdida de información y no se ha seleccionado ninguna salvaguarda.
Resultado esperado	Se muestra que el riesgo de pérdida de información es del 100%
Salida	Incorrecto. No deja pasar a la página de cálculo del riesgo ya que te obliga a seleccionar al menos una salvaguarda.

Tabla 41. Prueba de caja negra 7. Pasar al cálculo del riesgo sin seleccionar ninguna salvaguarda

Prueba de caja negra-008	Cálculo del riesgo de pérdida de información
Descripción	El usuario quiere calcular su riesgo de pérdida de información
Resultado esperado	Se muestra el riesgo de pérdida de información
Salida	Correcto

Tabla 42. Prueba de caja negra 8. Cálculo del riesgo de pérdida de información

Prueba de caja negra-009	Visualización del resumen de la gestión de riesgos
Descripción	Se muestra el resumen de la gestión de riesgos del usuario
Resultado esperado	Se muestra el resumen de la gestión de riesgo del usuario correctamente
Salida	Correcto

Tabla 43. Prueba de caja negra 9. Visualización del resumen de la gestión de riesgos

Prueba de caja negra-010	Cancelar la gestión de los riesgos
Descripción	El usuario desea cancelar la gestión de los riesgos
Resultado esperado	Se pregunta si de verdad quiere cancelar la gestión de los riesgos y si confirma se redirige a la página principal.
Salida	Incorrecto. Se redirige a la pantalla principal directamente

Tabla 44. Prueba de caja negra 10. Cancelar la gestión de los riesgos

Prueba de caja negra-011	Visualización de las tablas de todas las amenazas y salvaguardas
Descripción	El usuario desea echar un vistazo a las tablas de todas amenazas o salvaguardas
Resultado esperado	Se muestran las tablas correctamente
Salida	Correcto

Tabla 45. Prueba de caja negra 11. Visualización de las tablas de todas las amenazas y salvaguardas

Prueba de caja negra-012	Descargar en formato Excel las tablas
Descripción	El usuario desea descargar las tablas de todas amenazas o salvaguardas
Resultado esperado	Se descargan en la ubicación que el usuario desee y en formato Excel.
Salida	Correcto

Tabla 46. Prueba de caja negra 12. Descargar en formato Excel las tablas

Capítulo 8

Tecnologías utilizadas

En este apartado se explicará la tecnología utilizada para la implementación del proyecto, el lenguaje de programación utilizado y los IDE.

8.1. Lenguajes de programación

- PHP
- JAVASCRIPT
- HTML
- CSS

8.2. IDE

- Visual Studio Code
- Visual Paradigm
- Astah*
- Microsoft Project
- Navicat for MySQL
- Filezilla

Parte 3

Capítulo 9

Conclusión y trabajo futuro

9.1. Conclusión

Una vez finalizado el presente Trabajo de Fin de Grado, puedo concluir con que se han cumplido todos los objetivos marcados desde el principio.

Se ha desarrollado una aplicación web con las funcionalidades presentadas, en la que ayudamos a cualquier empresario a realizar un Sistema Gestor de Seguridad de la Información. También, contamos con una interfaz guiada y fácil de usar para el usuario, tras haber realizado un estudio de usabilidad.

Además, se han aprendido todos los conceptos relacionados de la seguridad de la información en cualquier empresa y la importancia qué es protegerla y la peligrosidad que conlleva no hacerlo.

Por último, hemos aprendido cuál es el proceso de creación de un proyecto nuevo, pasando por todas las fases y tomando posición en todos los roles.

9.2. Trabajo futuro

Después de haber cumplido con los objetivos, proponemos una serie de mejoras que se pueden desarrollar para mejorar y añadir nuevas funcionalidades para la herramienta:

- Realización de aplicación web a aplicación móvil.

- Permitir al usuario añadir nuevos activos que nosotros no hemos considerado, así como amenazas que hayan podido tener anteriormente y salvaguardas con lo que lo hayan solventado.
- Traducción de la aplicación web a diferentes idiomas. Contar con botones para la traducción del sitio.
- Añadir más activos, amenazas y salvaguardas.

ANEXOS

ANEXO I: Manual de instalación

En el siguiente manual se explicará el proceso de instalación del software necesario que utilizaremos en la aplicación. Aunque es una aplicación web, en el que el usuario no tiene que instalar nada, solo disponer de un navegador web en el dispositivo que utilice la aplicación, se explicará el proceso de instalación del software en el servidor.

1.1. Instalación y configuración de LAMP

Lo primero que realizamos es instalar en nuestro servidor LINUX, la infraestructura LAMP. Esta infraestructura consta de un servidor web Apache para las aplicaciones web, gestor de base de datos MariaDB y el lenguaje de programación PHP. [16]

1.1.1. Instalación de Apache

Para instalar el servidor web Apache, solo es necesario descargarlo desde el gestor de paquetes de Ubuntu, apt.

```
sudo apt-get update
sudo apt-get install apache2
```

Comprobamos que apache está funcionando ejecutando

```
service apache2 status
```

Deberíamos ver:

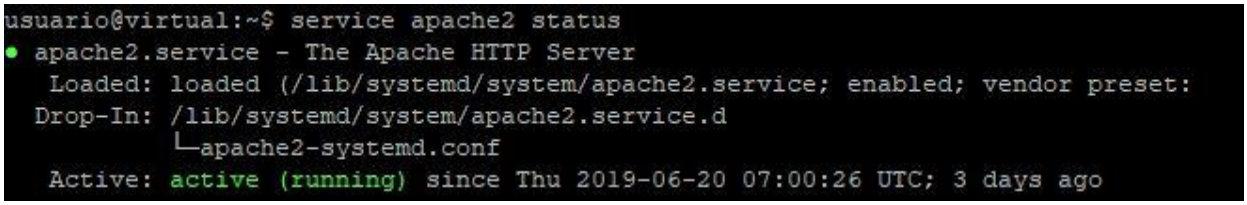


Figura 32. Servidor apache corriendo

Una vez hecho esto, si entramos en un navegador y ponemos la IP de nuestro servidor (virtual.lab.inf.uva.es:30132) deberíamos ver la página:

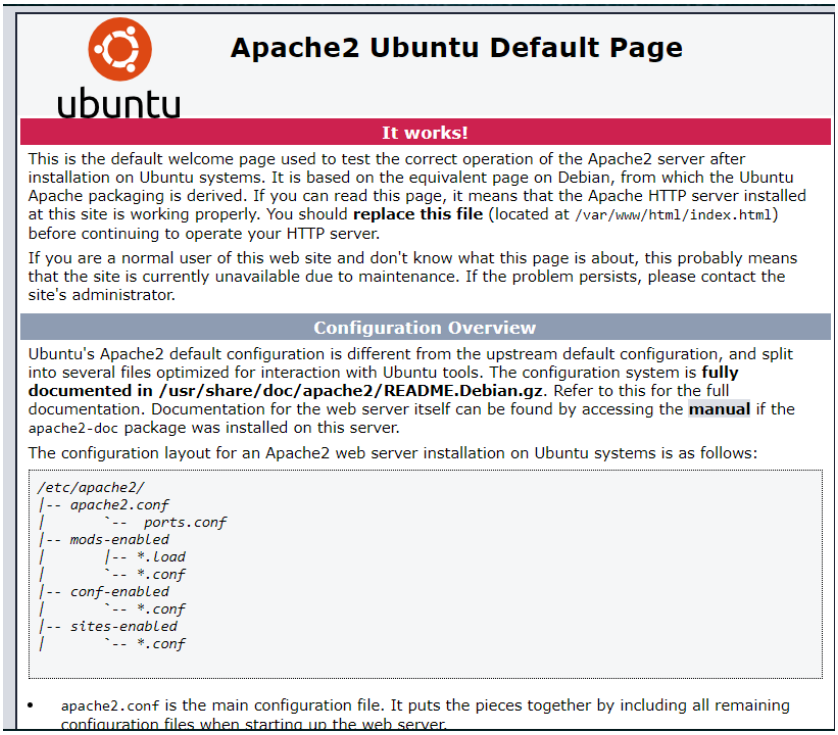


Figura 33. Apache funciona

1.1.2. Instalación MariaDB

Para instalar la base de datos, ejecutamos el siguiente comando:

```
apt-get install mariadb-server mariadb-client
```

Para comprobar si funciona, igual que antes, ejecutamos:

```
service mysql status
```

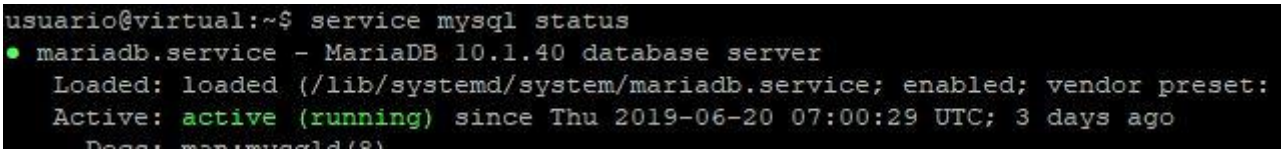


Figura 34. Mysql corriendo correctamente

Configuramos MariaDB ejecutando:

```
/usr/bin/mysql_secure_installation
```

En el primer paso nos preguntará por la contraseña de “root” para MariaDB, pulsaremos la tecla enter ya que no hay contraseña definida. Luego nos preguntará si queremos asignar una contraseña para el usuario “root”. Es recomendable usar contraseña. El siguiente paso nos preguntará si queremos

eliminar usuario anónimo, aquí indicaremos que Sí queremos borrar los datos. Luego nos preguntará si queremos desactivar que el usuario "root" se conecte remotamente, aquí indicaremos que No queremos desactivar acceso remoto para usuario "root". El siguiente paso nos preguntará si queremos eliminar la base de datos "test", aquí indicaremos que Sí queremos borrar las base de datos "test". El siguiente paso nos preguntará si queremos recargar privilegios, aquí indicaremos que Sí.

1.1.3. Instalación PHP

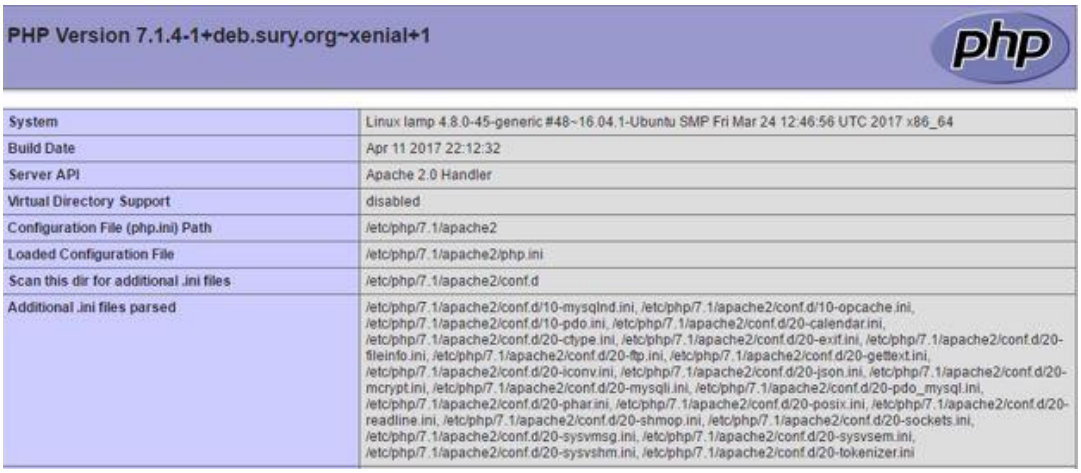
Para instalar el lenguaje de programación web que vamos a utilizar, ejecutamos los siguientes comandos:

```
apt install php php-cli php-mysql libapache2-mod-php
service apache2 restart
```

Para comprobar que funciona PHP crearemos un fichero /var/www/html/test.php con el código:

```
<?php
phpinfo();
?>
```

Al entrar en un navegador https://virtual.lab.inf.uva.es:20132/test.php deberíamos ver algo como:



PHP Version 7.1.4-1+deb.sury.org~xenial+1

System	Linux lamp 4.8.0-45-generic #48~16.04.1-Ubuntu SMP Fri Mar 24 12:46:56 UTC 2017 x86_64
Build Date	Apr 11 2017 22:12:32
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.1/apache2
Loaded Configuration File	/etc/php/7.1/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.1/apache2/conf.d
Additional .ini files parsed	/etc/php/7.1/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.1/apache2/conf.d/10-opcache.ini, /etc/php/7.1/apache2/conf.d/10-pdo.ini, /etc/php/7.1/apache2/conf.d/20-calendar.ini, /etc/php/7.1/apache2/conf.d/20-ctype.ini, /etc/php/7.1/apache2/conf.d/20-exif.ini, /etc/php/7.1/apache2/conf.d/20-fileinfo.ini, /etc/php/7.1/apache2/conf.d/20-ftp.ini, /etc/php/7.1/apache2/conf.d/20-gettext.ini, /etc/php/7.1/apache2/conf.d/20-iconv.ini, /etc/php/7.1/apache2/conf.d/20-json.ini, /etc/php/7.1/apache2/conf.d/20-mcrypt.ini, /etc/php/7.1/apache2/conf.d/20-mysqli.ini, /etc/php/7.1/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.1/apache2/conf.d/20-phar.ini, /etc/php/7.1/apache2/conf.d/20-posix.ini, /etc/php/7.1/apache2/conf.d/20-readline.ini, /etc/php/7.1/apache2/conf.d/20-shmop.ini, /etc/php/7.1/apache2/conf.d/20-sockets.ini, /etc/php/7.1/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.1/apache2/conf.d/20-sysvsem.ini, /etc/php/7.1/apache2/conf.d/20-sysvshm.ini, /etc/php/7.1/apache2/conf.d/20-tokenizer.ini

Figura 35. PHP instalado correctamente

ANEXO 2: Manual de usuario

En este manual se pretende proporcionar una ayuda al usuario de la aplicación web.

En la siguiente ilustración, podemos ver la página inicial del sitio web. Podemos ver un encabezado que está siempre presente

Figura 36. Página principal

El menú servirá para navegar a las distintas secciones y subsecciones de la página web. Cuando el ratón se sitúe sobre las secciones del menú que tienen subsecciones, éstas se situarán debajo de la sección padre. La sección INICIO, servirá como enlace de la página principal.

Para comenzar la gestión de riesgos, el usuario tiene dos opciones, la primera, si selecciona la sección del menú Gestión de tus riesgos, desde cualquier página de la aplicación web, o desde la página principal, pinchando al botón Empezar.

La primera página que aparece al empezar a gestionar los riesgos es la de selección de los activos que el usuario tenga en su empresa. Se explica al usuario que tiene que seleccionar los activos que tiene en su empresa junto a una breve explicación sobre lo que son éstos.

Figura 37. Página selección de activos parte 1

Figura 38. Página selección de activos parte 2

Como vemos en las figuras, el usuario podrá seleccionar cada uno de los activos que disponga. Después, tendrá que pulsar sobre el botón siguiente para seguir con la gestión de los riesgos. En cualquier momento, el usuario podrá cancelar la gestión pulsando sobre el botón Cancelar, que le redirigirá a la pantalla principal.

Si el usuario, da al botón siguiente sin seleccionar al menos un checkbox, saltará una alerta, avisándole de que tiene que seleccionar al menos uno.

La segunda pantalla con la que se encontraría el usuario es la de visualizar las posibles amenazas que tienen los activos que anteriormente seleccionó.

Al igual que antes, la aplicación web muestra información sobre qué es una amenaza, para entender lo que pueda suceder al activo en cuestión.

Figura 39. Página visualización de amenazas de la gestión de riesgos

Cuando el usuario haya acabado de visualizar las amenazas que tienen los activos de su empresa, pulsaría sobre el botón siguiente.

La siguiente pantalla con la que se encuentra el usuario es la selección de salvaguardas que tiene para tratar de solucionar las amenazas que tienen sus activos. Se explica lo qué es una salvaguarda antes, para que el usuario se ponga en situación.

Figura 40. Página de selección de salvaguardas

El usuario, seleccionará las salvaguardas que tiene en su empresa, si es que tiene alguna de las que hay en la tabla y en cuanto termine deberá pulsar sobre el botón siguiente.

A continuación, se le mostrará al usuario un resumen de su gestión de riesgos, diciéndole el nivel de riesgo de pérdida de información que tiene en su empresa. Habrá tres opciones: Riesgo menor del 30%, la caja de riesgo aparecerá en verde, riesgo entre un 30-60% en la que la caja se pondrá en amarillo, y cuando el riesgo supere el 60% la caja se pondrá en rojo. Se le recomendará al usuario visitar la página dónde mostramos todas las salvaguardas posibles para todos los activos.

Figura 41. Página dónde se muestra el nivel de riesgo

Por último, mostramos, las dos últimas páginas de nuestra aplicación web. Consisten en dos tablas informativas, en las que ayudamos al usuario a tener una ayuda sobre todas amenazas y sus salvaguardas si quiere ampliar los activos de su empresa.

El usuario tiene dos caminos para llegar a estas dos páginas. Pinchando sobre el menú, la sección PARA TÚ INTERÉS, mostramos la siguiente página:

Figura 42. Página dónde se muestran las tablas informativas

Pulsando en cada una de las imágenes, nos llevará a la página dónde se muestran o todas amenazas de los activos o todas las salvaguardas.

La segunda opción para llegar a cualquiera de estas dos páginas es, pulsando directamente sobre el menú despegable de la sección PARA TÚ INTERÉS.

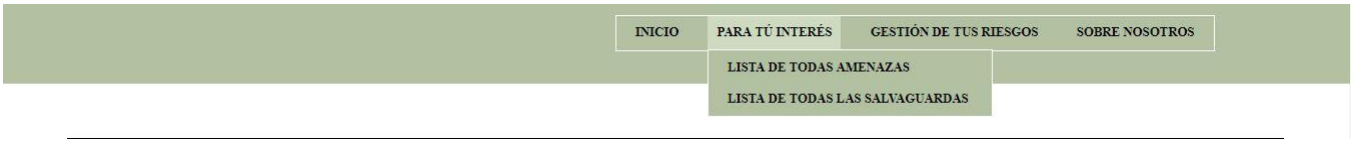


Figura 43. Menú despegable

Dentro de estas dos páginas, tenemos la opción de descargar en formato Excel las tablas informativas. El usuario solo tendría que pulsar el botón de descargar y guardarlo en su dispositivo físico.

Figura 44. Botón de descargar en Excel

ANEXO 3: Contenido del CD

En el CD entregado, podemos encontrar varias carpetas entre las que se encuentran los siguientes archivos:

- Código fuente: Todos los archivos (HTML, PHP, JS) que componen la aplicación web. Readme con el link de acceso a la página web y usuarios y contraseñas de la máquina virtual.
- Manuales: Manuales tanto de usuario como de instalación para una mejor lectura
- Planificación: El archivo de planificación .mpp, que es visible con la aplicación WINDOWS PROJECT.
- Memoria.pdf

Webgrafía y Bibliografía

7.1. Webgrafía

[1] Instituto Nacional de Ciberseguridad de España.

Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

[Último acceso:05/05/2019]

[2] Instituto Nacional de Ciberseguridad de España.

Disponible en: https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf

[Último acceso:20/05/2019]

[7] Requisitos. Apuntes de la asignatura Ingeniería del software I. Escrito por Miguel Ángel Laguna

Disponible en: https://www.infor.uva.es/~mlaguna/is1/apuntes/2-requisitos.pdf

[Último acceso:30/05/2019]

[8] Casos de uso. Actores

Disponible en: https://es.wikipedia.org/wiki/Caso_de_uso

[Último acceso:15/05/2019]

[12] Patterns in interaction design

Disponible en: http://www.welie.com/patterns/

[Último acceso:06/06/2019]

[13] User Interface Design patterns

Disponible en: http://ui-patterns.com/

[Último acceso:10/06/2019]

[15] Pruebas de caja negra

Disponible en: https://www.globetesting.com/2012/08/pruebas-de-caja-negra/

[Último acceso:25/06/2019]

[16] Instalación LAMP

Disponible en https://clouding.io/kb/como-instalar-en-linux-apache-mariadb-y-php-lamp/

[Último acceso:10/04/2019]

[17] Diagrama de despliegue

Disponible en: http://www.sparxsystems.com.ar/resources/tutorial/uml2_deploymentdiagram.html

[Último acceso:10/05/2019]

7.2. Bibliografía

[3] Magerit- versión 3.0- Metodología de Análisis y Gestión de Riesgos de los Ssitemas de Información.

"Libro II-Catálogo de elementos." Ministerio de Hacienda y Administración, 2012.

[4] Ingeniería del software, Ian Sommerville Séptima edición. Editorial Addison Wesley,2012

[5] "Planificación de un proyecto", tema de la asignatura Planificación y gestión de plataformas informáticas. Cuarto curso del grado de ingeniería informática. Escrito por Pablo de la Fuente Redondo.

[6] "Gestión de riesgos", tema de la asignatura Planificación y gestión de plataformas informáticas. Cuarto curso del grado de ingeniería informática. Escrito por Pablo de la Fuente Redondo.

[8] UML y Patrones, Craig Larman. Editorial Pearson,1999.

[9]" Diseño de la arquitectura del software", tema de la asignatura Diseño, Integración y adaptación del software. Tercer curso del grado de ingeniería informática. Escrito por José Manuel Marqués Corral.

[10] "Diseño Software. Patrones", tema de la asignatura Diseño, Integración y Adaptación del Software Tercer curso del grado de ingeniería informática. Escrito por José M. Marqués Corral.

[11] "Usabilidad", tema 2 de la asignatura IPC. Segundo curso del grado de ingeniería informática. Escrito por Alejandra Martínez Monés.

[14] "Prototipos", tema de la asignatura IPC. Segundo curso del grado de ingeniería informática. Escrito por Alejandra Martínez Monés.