***Imagen que contiene Logotipo

Descripción generada automáticamente***

10/6/2021

Trabajo 6

Plan de Contingencia

Seguridad Informática

Alejandro Ortega Martínez

Grado en Ingeniería Informática

Contenido

[1. Introducción 4](#_Toc74260724)

[¿Qué es un plan de contingencia? 4](#_Toc74260725)

[Elección del plan de contingencia 5](#_Toc74260726)

[2. Tipos de planes de Contingencia 6](#_Toc74260727)

[2.1. Plan de Continuidad de Negocio (PCN) 6](#_Toc74260728)

[2.2. Plan de Continuidad TIC (PCTIC) 6](#_Toc74260729)

[2.3. Plan de Recuperación ante Desastres (PRD) 6](#_Toc74260730)

[3. Herramienta de Análisis de Riesgos: PILAR 7](#_Toc74260731)

[4. Esquema Nacional de Seguridad 7](#_Toc74260732)

[4.1. ¿Qué es el Esquema Nacional De Seguridad? 8](#_Toc74260733)

[4.2. Objetivos 8](#_Toc74260734)

[4.3. Elementos del Esquema Nacional de Seguridad 9](#_Toc74260735)

[4.4. Indicaciones en el modo de actuar 10](#_Toc74260736)

[Notificación de Incidentes 10](#_Toc74260737)

[Auditoría de la Seguridad 10](#_Toc74260738)

[4. Plan de contingencia: Fases 11](#_Toc74260739)

[Plan de Contingencia Fase 0: Determinación del Alcance 11](#_Toc74260740)

[Plan de Contingencia Fase 1: Análisis de la organización 12](#_Toc74260741)

[Reuniones 12](#_Toc74260742)

[Análisis de Impacto sobre el negocio 13](#_Toc74260743)

[Análisis de riesgo 15](#_Toc74260744)

[Plan de Contingencia Fase 2: Determinación de la Estrategia de Continuidad 17](#_Toc74260745)

[Plan de contingencia Fase 3: Respuesta a la Contingencia 19](#_Toc74260746)

[Plan de Crisis (O de incidentes) 19](#_Toc74260747)

[Planes Operativos de Recuperación de Recursos 20](#_Toc74260748)

[Procedimientos Técnicos de Trabajo (O de Incidentes) 20](#_Toc74260749)

[Plan de Contingencia Fase 4: Prueba, Mantenimiento y Revisión 21](#_Toc74260750)

[Plan de mantenimiento 22](#_Toc74260751)

[Plan de Pruebas 22](#_Toc74260752)

[Plan de Contingencia Fase 5: Concienciación 23](#_Toc74260753)

[4. Plan de Contingencia: Hacienda 24](#_Toc74260754)

[4.1. Fase 0: Alcance 24](#_Toc74260755)

[Datos Relevantes 24](#_Toc74260756)

[Alcance del plan 25](#_Toc74260757)

[4.2. Fase 1: Análisis 25](#_Toc74260758)

[Reuniones 25](#_Toc74260759)

[Análisis de Impacto 30](#_Toc74260760)

[Análisis de Riesgos 32](#_Toc74260761)

[4.3. Fase 2: Determinación de la estrategia de Continuidad 35](#_Toc74260762)

[Inundación 36](#_Toc74260763)

[Incendio 36](#_Toc74260764)

[Robo (presencial) 37](#_Toc74260765)

[Ciberataque 37](#_Toc74260766)

[Caída del suministro eléctrico 38](#_Toc74260767)

[Caída de red 38](#_Toc74260768)

[Malfuncionamiento de equipos 38](#_Toc74260769)

[4.4. Fase 3: Respuesta a la contingencia 39](#_Toc74260770)

[Plan de Crisis y planes operativos de Recuperación de Entornos 39](#_Toc74260771)

[Procedimientos tecnicos de trabajos 44](#_Toc74260772)

[4.5. Fase 4: Prueba, Mantenimiento y Revisión 47](#_Toc74260773)

[Plan de pruebas 48](#_Toc74260774)

[Plan de Mantenimiento 49](#_Toc74260775)

[4.6. Fase 5: Concienciación 50](#_Toc74260776)

[7. Conclusión 51](#_Toc74260777)

[8. Bibliografía 53](#_Toc74260778)

# Introducción

## ¿Qué es un plan de contingencia?

Según la (EAE Business School, s.f.), podemos definir un plan de contingencia, como un **plan B,**  aunque también se le llama **Plan de continuidad de negocio**.

Para ser más exactos, definimos plan de contingencia como la **planificación que nos indica Los pasos que toma una organización cuando se produce una situación o evento inesperado**.

Esta situación puede ser positiva, como por ejemplo, que tengamos un superávit de ventas. Sin embargo, la mayor parte de las veces se refiere a los eventos negativos.

Por lo tanto, la motivación para crear este Plan B es prepararse ante los posibles eventos que puedan afectar a una empresa, ya sea, por ejemplo, financieramente hablando, respecto a su reputación, o en cuanto la continuidad de sus operaciones se refiere.

Puede considerarse que definir un plan de contingencia es adoptar un **enfoque proactivo**, en comparación con la gestión de crisis, que es más un enfoque reactivo. Tener un plan de contingencia asegura que el negocio siempre esté preparado para cualquier eventualidad. Por el contrario, un plan para la gestión de crisis permite a la organización controlar la respuesta después de que ocurran los hechos.

## Estructura del trabajo

Primero se hará una breve introducción. A continuación se hablarán de elementos interesantes, como son la herramienta PILAR o el Esquema Nacional de Seguridad. Después, se tratará de forma teórica las fases de un plan de contingencia para, por último, aplicarlas a nuestro ejemplo practico

## Elección del plan de contingencia

En mi caso, he decidido hacer el plan de contingencia sobre el edificio de Hacienda de Burgos.

He tomado esta decisión ya que, con respecto a las TIC se refiere, y más en concreto, a su seguridad, es un edificio muy propenso a ser objetivo de ataques informáticos, ya que se trata de un edificio gubernamental en el que se lleva a cabo muchas operaciones en cuanto a registros y dinero se refiere.

Es por esto por lo que opino que es un edificio interesante de hacer un plan de contingencia.

NOTA: Cabe destacar que, como es obvio, no se ha ido a recopilar datos a la institución ya que ni la situación lo permite, ni los empleados los proporcionan por temas de seguridad.

Por esto, me inventaré los datos de la forma más precisa posible, ya que el objetivo de este trabajo no es realizar un plan de contingencia preciso, sino el aprender a realizarlos.



# 2. Tipos de planes de Contingencia

Normalmente un plan de contingencia completo engloba los varios tipos de planes, aunque es interesante destacar los siguientes para tenerlos claros:

## 2.1. Plan de Continuidad de Negocio (PCN)

Es, por así decirlo, el plan de contingencia global. Establece la continuidad de la organización desde todas las perspectivas posibles: Infraestructuras TIC, recursos humanos, comunicación, logística, etc.

Cada uno de estos ámbitos tiene a su vez su plan de contingencia más específico.

## 2.2. Plan de Continuidad TIC (PCTIC)

Es uno de los planes de contingencia que forman parte del general, y en el que más nos vamos a centrar durante la realización de este trabajo.

Este es un plan de contingencia que se centra, en particular, en el ámbito tecnológico.

## 2.3. Plan de Recuperación ante Desastres (PRD)

Otro plan de contingencia que forma parte del general.

En este también nos centraremos algo (aunque en menor medida), ya que, por ejemplo, un terremoto, o una inundación, puede afectar a nuestros servicios TIC.

# 3. Herramienta de Análisis de Riesgos: PILAR

PILAR es un conjunto de herramientas EAR (Entorno de Análisis de Riesgos) cuya función es el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y está desarrollada y financiada parcialmente por el CCN (CCN, s.f.).

La herramienta PILAR permite analizar los riesgos en varias dimensiones: **confidencialidad, integridad, disponibilidad, autenticidad** y **trazabilidad**.

También permite realizar análisis **cuantitativos** y **cualitativos**; y **análisis de Impacto** y **Continuidad de Operaciones** (CCN, s.f.).

Se ha decidido usar esta herramienta, ya que cumple los estándares del centro criptológico nacional, y nos permite aplicar la metodología Magerit, que es una metodología teórica, de manera práctica.

Las organizaciones públicas, como es nuestro caso, disponen de licencias con todos las ventajas de esta aplicación. Sin embargo, como no es posible hacerse con una licencia, se usará la versión para PYME y Administración local.

# 4. Esquema Nacional de Seguridad

Aunque vayamos a hacer un plan de contingencia, como objetivo del trabajo, cabe mencionar al esquema nacional de seguridad, que se ocupa de este tipo de temas, y que, al ser el objetivo del trabajo la delegación de Hacienda de Burgos es amparada por dicho esquema.

## 4.1. ¿Qué es el Esquema Nacional De Seguridad?

Debido a la transformación digital del sector público, se han de dar también unas medidas y técnicas de seguridad que protejan la información utilizada, ya que es material muy vulnerable que trata con gran cantidad de datos personales.

Teniendo en mente también la Ley del Procedimiento Administrativo Común de las Administraciones Públicas (Ley 39/2015), en el artículo 13 se dicta el derecho “relativo a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas”.

Debido a todo esto, y a causa de esta existente necesidad de seguridad, nace el **Esquema Nacional de Seguridad,** cuyo objetivo es **establecer la política de seguridad en la utilización de medios electrónicos**.

Las instrucciones de seguridad amparadas en el ENS son **de obligatorio cumplimiento**, ya que se consideran esenciales para una adecuada, homogénea y coherente implantación de los requisitos.

## 4.2. Objetivos

El Esquema Nacional de Seguridad tiene como principales los siguientes objetivos:

* **Crear las condiciones de seguridad necesarias en el uso de los medios electrónicos**, a través de medidas que garanticen la seguridad de sistemas, datos, etc. que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios electrónicos.
* **Promover la gestión continuada de la seguridad.**
* **Promover la prevención, detección y corrección**¸ con respecto a ciberamenazas y ciberataques.
* **Promover un tratamiento homogéneo de la seguridad** que facilite la cooperación en la prestación de servicios públicos digitales cuando participan diversas entidades.
* **Servir de modelo de buenas practicas**

## 4.3. Elementos del Esquema Nacional de Seguridad

Los principales elementos del ENS son:

* **Los principios básicos** a considerar en las decisiones en materia de seguridad (artículos 4-10).
* **Los requisitos mínimos** que permitan una protección adecuada de la información (artículos 11-26).
* **El mecanismo para lograr el cumplimiento de los principios básicos y de los requisitos mínimos**, mediante la adopción de **medidas de seguridad proporcionadas** a la naturaleza de la información y los servicios a proteger (artículos 27, 43, 44, Anexo 1 y Anexo 2).
* **El uso de infraestructuras y servicios comunes** (artículo 28)
* **Las guías de seguridad** (artículo 29).
* **Las instrucciones técnicas de seguridad** (artículo 29).
* **Las comunicaciones electrónicas** (artículos 31-33).
* **La auditoría de la seguridad** (artículo 34 y anexo 3).
* **La respuesta ante incidentes de seguridad** (artículos 36 y 37).
* **El uso de productos certificados** (artículo 18, Anexo 2 y Anexo 4).
* **La conformidad** (Articulo 41).
* **La formación y la concienciación.**

## 4.4. Indicaciones en el modo de actuar

En el ENS se recogen también algunas indicaciones de cómo actuar en aspectos concretos. A continuación veremos algunos de ellos.

### Notificación de Incidentes

Con respecto a la notificación de incidentes, deberemos primero determinar los niveles de impacto con respecto a unos criterios recogidos en el BOE (ver bibliografía). Si los incidentes son Alto, Muy Alto, o Critico, se deberán notificar obligatoriamente dichos incidente, junto con una serie de evidencias. También es de obligado cumplimiento remitir una serie de estadísticas, así como los impactos recibidos.

Para llevar a cabo estas tareas, el cnn ha desarrollado una herramienta llamada **LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas)**, con el fin de automatizar estos mecanismos de notificación.

### Auditoría de la Seguridad

En el BOE se ha dictaminado la **instrucción técnica de Seguridad de auditoria de la seguridad de los sistemas de información**.

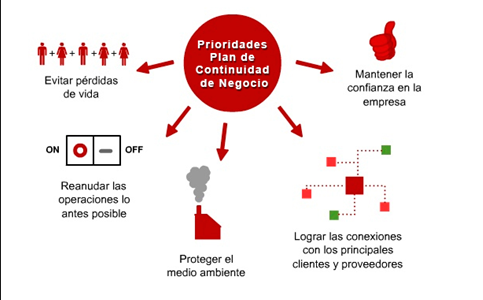
Dentro de esta instrucción, hay puntos como el **ámbito de la aplicación** que se refiere a todos los sistemas de la información a los que nos hemos referido anteriormente.

También se habla de su **obligatoriedad** y la **normativa que lo regula**. Otros puntos que trata es su **alcance**, o **como se debe ejecutar y el informe que se debe presentar**.

# 4. Plan de contingencia: Fases

En este apartado veremos las fases teóricas que puede tener un plan de contingencia, para posteriormente desarrollarlas y ejecutarlas en nuestro caso concreto

## Plan de Contingencia Fase 0: Determinación del Alcance



Esta es la primera fase de un plan de contingencia, y la que menor número de recursos consume.

En esta fase, se determinan que elementos de nuestra empresa van a ser el foco crítico del plan de contingencia. En nuestro caso, nos centraremos en los elementos informáticos, aunque estos van de la mano con el personal, que, personalmente, considero un eslabón en la informática (y posiblemente el más débil, por eso los tendremos muy en cuenta).

Normalmente el alcance son los **sistemas de mayor criticidad**, es decir, estos sistemas que, si fallaran, tendría un gran impacto en nuestra organización.

Esta determinación del alcance la podemos plantear desde dos enfoques:

* **Enfoque por activo:** Asume que la continuidad de la organización reside en un conjunto de activos (por ejemplo, los servidores, o los equipos personales).
* **Enfoque por proceso:** Pretende mejorar la continuidad enfocándose en los procesos, sin tener en cuenta los activos que le den soporte.

Podríamos pensar que un enfoque por proceso en una empresa sea la seguridad, mientras que un enfoque por activo podrían ser las cámaras de vigilancia.

El alcance que escojamos va a determinar el volumen de trabajo de nuestro proyecto. En nuestro caso, como vamos a hacer un plan de contingencia orientado a TIC, nos vamos a **centrar más en enfoque por proceso.** Es decir, vamos a coger nuestros procesos más críticos y mejorar su continuidad.

## Plan de Contingencia Fase 1: Análisis de la organización

La tarea a realizar en esta fase es recoger todos los datos posibles sobre la organización en cuestión (**circunstancias**, **tecnologías**, **procesos** y **recursos**).

Esto nos sirve para crear una base sólida sobre la que construir nuestro plan de contingencia, y llevar a cabo las siguientes fases de una manera más precisa.

Algunas de las tareas importantes de esta fase son las siguiente:

### Reuniones

Una de las primeras tareas debe ser **reunirnos con los usuarios** implicados en nuestro plan de contingencia. Gracias a estas reuniones, deberíamos ser capaces de sacar información muy valiosa, como pueden ser información sobre los empleados, sobre la distribución de las instalaciones, inventarios e información sobre todos los equipos informáticos, etc.

Después de esta reunión, lo que tenemos que hacer es recopilar toda la información sobre las aplicaciones que hemos obtenido en el paso anterior, para detallar su funcionamiento, proveedores, etc. Esto lo podemos hacer reuniéndonos con el personal encargado de dichas aplicaciones.

Tras estas reuniones, tendremos una **visión general de los procesos de los que queremos mejorar su continuidad.**

### Análisis de Impacto sobre el negocio

El siguiente paso será el **Análisis de Impacto sobre el Negocio** o **BIA** (Bussiness Impact Analysis), a partir de la información recogida anteriormente.

Este análisis es uno de los más importantes del plan de contingencia, por lo que es de vital importancia que lo hagamos correctamente. Además, gracias a él, podemos categorizar los procesos obtenidos en anteriores fases según sean más o menos importantes.

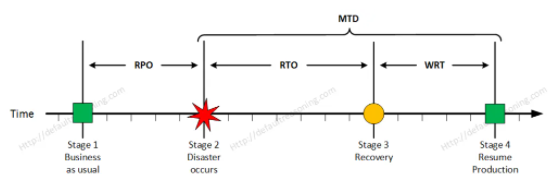
Este documento contiene los **requisitos temporales y de recursos** de los procesos recopilados, y conjunto al Análisis de Riesgos, que veremos en el siguiente punto, define las iniciativas a implantar para recuperar los procesos en situación de contingencia.

Para cada uno de los procesos analizados, tenemos que obtener los siguientes datos:



* **Tiempo de recuperación** (RTO- recovery Time Objective): Es el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado. Este valor tiene un gran componente de seguridad. Por así decirlo, es el máximo tiempo tolerable que necesitamos para que dicho proceso vuelva a estar activo.
* **Recursos humanos y tecnológicos empleados en el proceso**: En este apartado, determinamos que recursos necesitan nuestros procesos para funcionar en una situación de contingencia, así como los tiempos de recuperación de cada uno de ellos. Por ejemplo, debemos determinar si un determinado proceso va a necesitar de impresoras, acceso a la red, o un operario entendido en el proceso.
* **Tiempo máximo tolerable de caída** (MTD-Maximum Tolerable Downtime): Es el máximo tiempo que un proceso puede permanecer inoperativo antes de que se vuelva desastroso para la organización. Se diferencia del RTO en que el RTO nos dice cuanto tiempo tarda en recuperarse un proceso, y a esto hay que sumarle el tiempo que tarda esta caída en ser fatal para el negocio. Por lo general, **el RTO debe ser menor que el MTD.**
* **Niveles mínimos de recuperación** (ROL-Revised Operating Level): Es el nivel mínimo de recuperación que debe tener una actividad para considerarla como recuperada, aunque no esté trabajando todavía a todo el potencial necesario. Aquí se debe tener en cuenta el público objetivo destinatario de la actividad del servicio, compromisos con terceras partes, etc.
* **Dependencias de otros procesos internos o proveedores externos:** El objetivo es verificar que nuestros proveedores de recursos y actividades dispongan de algún tipo de plan de recuperación, para que sus situaciones de desastre no se trasladen a nuestra organización.
* **Grado de dependencia de la actualidad de los datos** (RPO-Recovery Point Objective): Determina el impacto que tiene sobre la actividad la perdida de datos, y va muy de la mano con el tema de las copias de seguridad.

Para hacernos una idea más general, lo podemos ver en la siguiente línea de tiempo sacada de (Default Reasoning, s.f.)



Por lo tanto, después de realizar este BIA, nos tiene que quedar claro lo siguiente:

* Que **procesos debemos recuperar antes**, en función de su MTD. Lo ordenaremos **en una escala por MTD**, lo normal es hacer una escala dividida en tres rangos de valores, por ejemplo, menos de un día, entre uno y dos días, más de dos días.
* Que **aplicaciones debemos recuperar antes**, en función de los procesos en los que intervengan.
* Las **necesidades de copias de seguridad**.

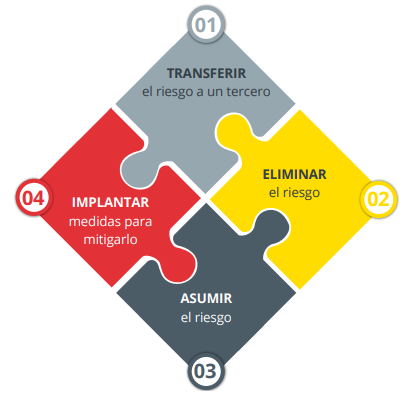
Hay que tener en cuenta que, a mayores exigencias, mayor número de recursos necesitaremos destinar a cubrirlas, por lo que tendremos que evaluar a ver si alguna exigencia que se nos da la consideramos demasiado elevada. Por tanto, debemos trasladar a los usuarios las implicaciones de los requerimientos que nos indican e instarles a considerar incidencias en el pasado, ausencias por enfermedad, etc.

### Análisis de riesgo

Tras obtener la anterior información, procederemos a estudiar que amenazas pueden acechar a los procesos del alcance, con que probabilidad, y que impacto tendrían. Para ello, seguiremos los siguientes pasos:

1. **Determinar las amenazas** a las que está expuesta la organización, como pueden ser robos o ciberataques, desastres naturales, caídas de red, etc. Nos centraremos en las amenazas que implican una indisponibilidad de los procesos del alcance.
2. Una vez identificadas las amenazas, **determinaremos su probabilidad de que ocurra, y el impacto que podría ocasionar.** La manera más extendida de hacerlo es con una escala de valores, por ejemplo del uno al cinco, donde uno es “Muy poco probable”, y cinco es “casi seguro”. En general, **nos interesan** **los riesgos con un mayor impacto, y una probabilidad no despreciable**, ya que son los que realmente pueden poner en peligro la organización.
3. Por último, realizaremos el **producto de la probabilidad por el impacto**. Gracias a esto, obtendremos una escala de los riesgos, ordenados en función a la urgencia con la que los tenemos que tratar. De este paso sacaremos un listado con los riesgos, un valor de impacto, y un valor de probabilidad.

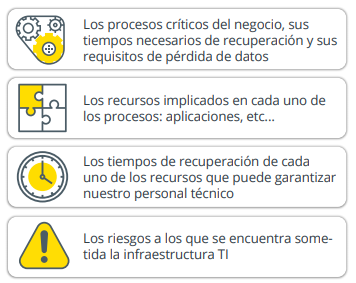
Hay que tener en cuenta que, al igual que el punto anterior, evaluar los riesgos vuelve a ser un proceso subjetivo.

Una vez determinados los principales riesgos, hay que decidir cómo tratarlos, conforme a una de las cuatro medidas:

Para cada riesgo que consideremos importante, realizaremos un **plan de tratamiento de riesgos**. Para cada medida de este plan de tratamiento, determinaremos:

* Descripción de la medida o iniciativa.
* Riesgo o riesgos que mitiga.
* Fecha de implantación limite.
* Responsable de la implantación.
* Recursos necesarios para su implantación.

## Plan de Contingencia Fase 2: Determinación de la Estrategia de Continuidad

Tras las fases anteriores, tendremos la siguiente información:

A partir de esta información, podemos identificar si los recursos actuales y sus estrategias de recuperación permitirían cubrir el MTD establecido para cada proceso.

Por ejemplo, si el proceso de contratación tiene un MTD de 24 horas, y usa el correo electrónico, la aplicación de contabilidad, y el acceso a un directorio departamental. El correo electrónico y el directorio departamental tienen un RTO de 8 horas, pero la aplicación de contabilidad de 48. Esto quiere decir que si cae la aplicación de contabilidad, el proceso de contratación estará caído 48 horas, el doble que su MTD. Por tanto, nuestro propósito es **implantar medidas que reduzcan este tiempo de recuperación** por debajo de 24h.

En resumen, lo que tenemos que hacer es **determinar cómo recuperar un sistema para evitar que una contingencia lo degrade de manera irreversible para nuestra empresa.**

Algunos elementos potencialmente afectables por una contingencia son:

* **Personal**: Según el personal critico identificado en el BIA, debemos evaluar las opciones para evitar lo máximo posible que no se encuentren disponibles.
* **Locales**: Deben evaluarse también situaciones en las que no se disponga de ubicación para trabajar.
* **Tecnología**: Se deben valorar alternativas o medidas complementarias para las diferentes tecnologías implicadas en los activos.
* **Información**: Considerar los aspectos relacionados con la disponibilidad y salvaguarda de la información.
* **Proveedores**: Debemos garantizar que los proveedores críticos tienen unos tiempos de respuesta acordes con los que necesitamos.

Como resultado de esta fase, determinaremos las estrategias de recuperación más adecuadas en cada caso, teniendo en cuenta que algunos procesos pueden requerir varias estrategias de recuperación.

Estas estrategias se implantarán en una fase posterior, y para cada una de ellas deberemos valorar el coste y viabilidad de su implantación, recursos necesarios, etc.

## Plan de contingencia Fase 3: Respuesta a la Contingencia

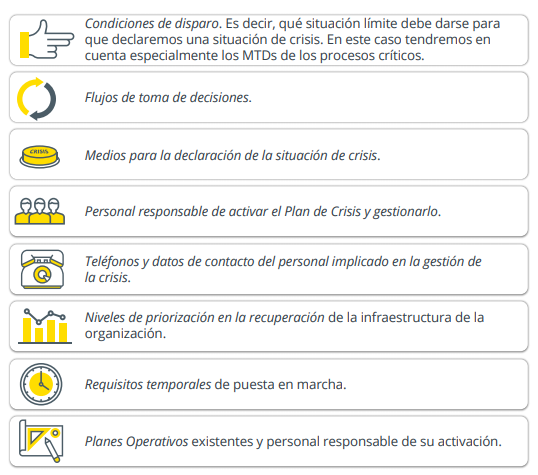
En este punto trataremos la **implantación de las iniciativas** identificadas en la anterior fase. Durante esta implantación, podemos abordar la fase de documentación de respuesta a la contingencia, y a partir de este punto nos centraremos en los elementos más relacionados con la tecnología.

Esta documentación se ejecuta en forma de árbol jerárquico, donde el elemento superior gestiona el momento crítico inmediatamente posterior a la crisis, los elementos intermedios ponen las bases para la recuperación de la infraestructura, y los nodos inferiores establecen los procedimientos tecnicos detallados para dicha recuperación.

Este proceso se organiza en torno a los siguientes elementos:

### Plan de Crisis (O de incidentes)

Este documento es el **elemento central en la gestión de la situación de crisis**, cuyo objetivo es **evitar que tomemos decisiones improvisadas** que puedan empeorar la crisis. Este plan de crisis contiene todos los elementos necesarios para la gestión de la crisis:



Tras la ejecución de este plan de crisis, habremos podido **gestionar el momento crítico de la crisis** y puesto en marcha todos los procesos necesarios para la recuperación de la infraestructura afectada a través de los Planes Operativos de Recuperación de Recursos.

### Planes Operativos de Recuperación de Recursos

Una vez hemos contenido el momento inicial de la crisis, debemos **evaluar su alcance y determinar qué Planes Operativos de Recuperación se activan**.

Tras el disparo de los diferentes Planes Operativos, cada una de las infraestructuras afectadas comenzará su proceso de recuperación, tomando como base los Procedimientos Tecnicos de Trabajo.

### Procedimientos Técnicos de Trabajo (O de Incidentes)

Con Procedimientos Tecnicos de Trabajo entendemos a la **documentación que describe como debemos de llevar las tareas necesarias para la gestión y recuperación de una aplicación, sistema, infraestructura o entorno.**

En realidad no son parte del plan de contingencia, sino de la operación diaria, pero en una situación de crisis se vuelven más importantes.

Por tanto, estos documentos contienen gran cantidad de información específica a cada uno de los entornos: Direcciones IP, versiones de programas, listados de comandos, recuperación de copias de bases de datos, puesta en marcha de aplicaciones, etc.

## Plan de Contingencia Fase 4: Prueba, Mantenimiento y Revisión

El objetivo de nuestro plan de contingencia TIC es **gestionar de la manera más optima en tiempo y forma una crisis no prevista**. Por tanto, es imperativo que lo mantengamos actualizado en todo momento y que su vigencia sea comprobada regularmente.

Para esto, realizaremos una serie de **pruebas** sobre los entornos definidos en el alcance. Entre todas las pruebas, debemos realizar pruebas de cada uno de los entornos al menos una vez al año.

En la ejecución de las pruebas, es necesario llevar a cabo una planificación previa que tenga en cuenta:

* Personal técnico implicado
* Personal externo implicado
* Descripción de la prueba
* Descripción del resultado esperado.
* Hora y fecha de realización: debemos tener en cuenta que durante la prueba, se implica una parada parcial o total del servicio.

Tras la prueba, deberá **elaborarse un informe que recoja los resultados y describa posibles incidencias**. Cualquier incidencia que se haya producido debe analizarse para la aplicación de medidas correctoras.

Algunas posibles pruebas que pueden realizarse son:

* Qué pasaría si cae el servicio eléctrico, comprobar si el sistema de alimentación secundario entra en acción.
* Verificar los tiempos de recuperación de los posibles repositorios documentales de la organización en una máquina de pruebas.
* Recuperación de las aplicaciones críticas del negocio.
* Acceso remoto a la infraestructura desde una ubicación remota.

En el plan de mantenimiento se recogen los eventos que nos dicen que debemos hacer una modificación o revisión del sistema, y en el plan de pruebas recogemos las diversas pruebas a llevar a cabo.

### Plan de mantenimiento

Su propósito es **mantener actualizada toda la documentación cada vez que se produzca un cambio**, ya sea a nivel de infraestructura TIC, de personal, o de cualquier otro aspecto implicado en los procesos críticos.

Gracias a esto, conseguiremos que nuestro plan de contingencia refleje fielmente los recursos que tenemos en la actualidad, para no tener que depender de recursos obsoletos, o que ya no se encuentran disponibles.

### Plan de Pruebas

Su objetivo es **mostrar los distintos tipos de pruebas de contingencia que podemos llevar a cabo**. Esto permite:

* Garantizar que la información del plan se mantiene actualizada.
* Garantizar que en situación de contingencia, la organización podrá recuperarse en los tiempos establecidos.
* Incrementar la cohesión del personal implicado en una potencial contingencia.
* Mejorar el conocimiento de los usuarios en relación con las pruebas de continuidad.
* Incrementar la confianza de los usuarios en la organización.

## Plan de Contingencia Fase 5: Concienciación

Como última fase de la implantación del plan de contingencia, debemos **realizar tareas para concienciar al personal sobre la continuidad**.

En concreto, debemos plantear un proceso de concienciación que contemple la descripción de los elementos que utilizamos en la continuidad. Además de considerarse aspectos como las responsabilidades, pruebas que debemos realizar, etc.

El público objetivo en este caso deberá ser tanto el personal técnico como el personal de negocio que tenga algún tipo de relación con los procesos críticos dentro del alcance.

# 4. Plan de Contingencia: Hacienda

Por último, en este apartado vamos a desarrollar nuestro plan de contingencia, orientado al edificio de Hacienda de Burgos.

Como se ha mencionado anteriormente, se trata de un plan de contingencia ficticio, cuyos datos e información serán inventados, y operaciones como, por ejemplo, las reuniones, serán emuladas.

Para seguir este plan de contingencia, tomaremos el modelos resumido anteriormente (INCIBE, s.f.).

## 4.1. Fase 0: Alcance

En este Plan de Continuidad, nos centraremos en la delegación de Haciendo de la ciudad de Burgos.

Antes de embarcarnos con el alcance del plan, veremos unos pequeños datos relevantes sobre esta delegación de Hacienda, a la que, a partir de ahora, nos referiremos únicamente como “Hacienda”.

### Datos Relevantes

Dicha delegación se corresponde con un único edificio, situado en la Calle Vitoria, Nº 39, en la ciudad de Burgos, provincia de Burgos, con código postal 09071.

El teléfono de atención al cliente es el 947 47 73 00, y la dirección de fax es 947 27 03 42.

El código de la delegación es 09600.

### Alcance del plan

En este apartado veremos el alcance del plan propiamente dicho. Como hemos dicho anteriormente, determinaremos que elementos de Hacienda son el foco de la mejora de la continuidad. Dichos elementos los podemos reconocer como los más críticos, los que, sin su operatividad, Hacienda correría un grave peligro.

En nuestro caso, elegiremos un **alcance por proceso**, en el que primero veremos que procesos son críticos para la continuidad de esta organización, y posteriormente indagaremos en los activos implicados.

Por petición de la empresa, hemos decidido que el alcance de nuestro plan de contingencia sea el mencionado anteriormente, es decir, **un alcance que abarque todos los procesos críticos**. Sin embargo, nos referiremos **solo a la delegación de Burgos**, y no a la institución de Hacienda en general.

En cuanto a los procesos críticos, hemos identificado principalmente los siguientes:

* Telecomunicaciones
* Contabilidad
* Seguridad Informática
* Seguridad Física

## 4.2. Fase 1: Análisis

Tras ver el alcance que va a tener nuestro plan de contingencia, llevaremos a cabo el análisis.

### Reuniones

El primer paso es reunirnos con los usuarios finales. Debido a esto, hemos tenido una serie de reuniones con las siguientes personas:

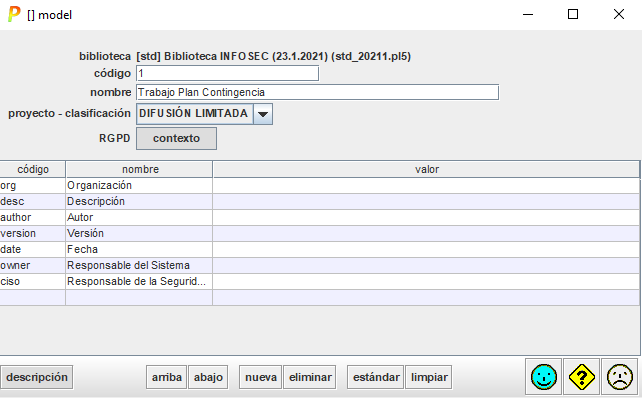
**Reunión 1: Director de Hacienda**

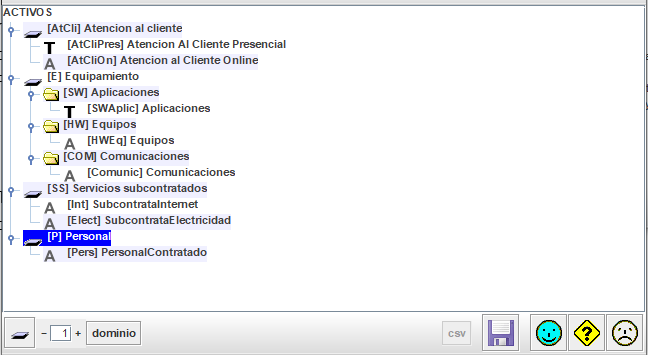
En esta primera reunión, nos hemos reunido con el director de la sucursal de hacienda.

Se ha hablado de la necesidad de tener un plan de contingencia, y de los ámbitos que son interesantes tratar.

Tras llevar a cabo la reunión, se ha llegado a la conclusión de que se usará la herramienta PILAR, proporcionada por el centro criptológico nacional, para detectar los procesos a tener en cuenta para nuestro plan de contingencia. Posteriormente se detalla el uso de esta herramienta:

Primero se creará un proyecto, como viene a continuación



Posteriormente, seleccionaremos los activos, como se observa en la siguiente captura de pantalla:

Tras identificar los procesos críticos con el director, se procede a realizar una reunión con cada uno de los jefes de departamento implicados para poder identificar cada uno de los activos.

**Reunión con el director de departamento de Atención Al Cliente**

En esta ocasión, nos hemos reunido con el director del departamento de atención al cliente.

En dicha reunión, se nos ha informado de que este departamento divide la atención al cliente en dos subgrupos: el presencial y el online.

En cuanto al presencial, se nos ha comunicado que son todos los operarios que actúan en la recepción, o recibiendo a personas que van a hacer alguna consulta o encargo. También se incluyen consultas telefónicas. Estos se encargan de realizar o analizar perfiles personales, así como gestionarlos, por lo que podemos considerar que tratan con datos personales. Son personal interno (funcionarios), que trabajan de cara al público.

Con respecto al online, nos referimos a la atención al cliente que se hace por medio de la página web de la delegación. Debido a esto, a parte de los activos mencionados antes, hay que añadir todos los referidos a la informática, como pueden ser los ficheros de datos, datos de validación de credenciales, mensajes cifrados para la información sensible, y todos los términos de redes inalámbricas e informática, que se verá con más detalle en otra de las reuniones.

Así en la aplicación PILAR, nos quedaría el siguiente resumen de los dos:



**Reunión con el jefe de departamento de Informática**

A continuación nos hemos reunido con el jefe del departamento de informática.

Nos ha comentado que este departamento es el que lleva todos los equipos, por lo que hemos podido ser informados sobre todos los equipos con los que operan.

Para empezar, tienen una sala de servidores en la planta -1, donde almacenan y centralizan toda la información. Estos servidores se corresponden con servidores IBM 8335-GTA, y son 6 servidores de este modelo. Tienen un voltaje de entre 200 y 240 V y un consumo máximo de alimentación de 1875W. Se han decidido almacenar en el sótano debido a la cantidad de ruido y de calor que originan. Su sistema operativo es un Ubuntu Server 21.04, la última actualización a fecha del análisis.

También disponen de ordenadores personales, uno por cada empleado, más el de recepción. Esto hace una suma de 21 ordenadores personales. Todos están conectados a la red interna del departamento, aunque esta red interna también tiene salida al exterior vía internet. Los ordenadores tienen como sistema operativo Windows 7, y vienen con pocas aplicaciones instaladas, las justas para que los funcionarios puedan realizar su trabajo. Cabe destacar que dichos funcionarios solo tienen permisos normales, no de administrador.

A estos 21 ordenadores hay que sumarles 7 del departamento de informática, con prestaciones más potentes, y cuyo sistema operativo es Ubuntu 20.04. Dichos equipos tienen acceso a la red.

Todos los equipos, y el servidor, tienen un sistema de backup automático, que se guarda en otro servidor en otra localización, gestionado por el gobierno.

Por último, cabe destacar que el proveedor de internet es Movistar, debido a que es el que más velocidad de conexión ofrecía, y el proveedor de energía es Iberdrola.

Todo esto queda reflejado en una tabla en el apartado [Procedimientos tecnicos de trabajo](#_Procedimientos_tecnicos_de)

Al finalizar la reunión, se ha mencionado que se dispone de una SAI, por si hay cortes de luz.

Todo esto se ve reflejado en PILAR en los siguientes apartados:

Software:



Hardware:



Internet:



Electricidad:



**Reunión con el jefe de Departamento de Personal**

En esta reunión se ha hablado con el jefe de personal, que es quien lleva todas las contrataciones de la delegación.

Nos ha informado que en la actualidad hay 32 trabajadores, contando los jefes de personal y el director. A ellos, hay que sumarles 7 trabajadores del departamento de informática.

Los 32 trabajadores principales tienen acceso a todos los equipos menos a los de informática y al servidor, pero, como nos mencionó anteriormente el jefe de informática, sin permisos de administrador. Los informáticos, por el contrario, sí que tienen acceso de administrador tanto a todos los equipos del edificio, como a la sala de servidores.

Todos estos datos se ven reflejados en el activo “Personal Contratado” de la herramienta PILAR:



**Reunión con el director de Contabilidad**

Por último, nos hemos reunido con el director de contabilidad.

Nos ha dicho que este es el departamento más importante, ya que, como es lógico, la subdelegación de Hacienda no puede permitir que ningún tema de contabilidad vaya mal.

En cuanto a temas de personal o de comunicaciones, no nos ha dicho nada remarcable con respecto a lo que se nos ha comentado en anteriores reuniones.

Sin embargo, sí que nos ha destacado la importancia de que este departamento funcione correctamente, ya que tienen que estar siempre actualizados con los nuevos datos de cualquier persona, y no pueden permitir que nadie los modifique.

En el activo PILAR ha quedado reflejado de la siguiente manera:

Una vez realizadas las reuniones, se procederá al Análisis de Impacto.

### Análisis de Impacto

El siguiente paso es realizar el análisis de impacto sobre el negocio o BIA.

Para ello, nos ayudaremos de la herramienta PILAR, que hemos estado usando anteriormente para recoger los activos importantes.

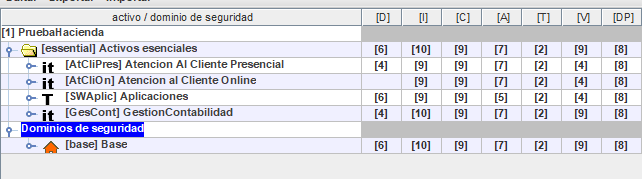
Lo primero que tenemos que hacer es una valoración de los activos, para ello, nos ayudaremos de la herramienta PILAR.

Nos iremos a Análisis de riesgos>Activos>Valoración de los dominios, en los que **valoraremos los niveles de seguridad** desde el 0 (despreciable, no nos preocupa), hasta el 10 (máxima preocupación).

Primero vamos a valorar los activos conforme al tipo de información que usan. Para esto, pilar nos ofrece las siguientes opciones:



Disponibilidad (D), Integridad de los datos (I), Confidencialidad de los datos (C), Autenticidad de los usuarios y la información (A), Trazabilidad del servicio y de los datos (T), Valor (V) y Datos Personales (DP). Así, la tabla, tras discutirlo con el equipo, nos queda de la siguiente manera:



Con la herramienta PILAR, se hace de la manera vista anteriormente. Sin embargo, si quisiéramos hacerlo de manera teórica, haríamos lo siguiente:

Primero, estableceríamos una escala, que sería la siguiente:

[30min][1 hora][12 horas][1 día][2 días]

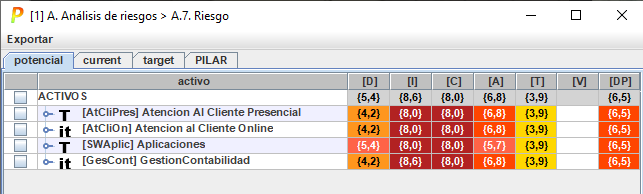
Ahora, procederemos a valorar los recursos:

* **Atención al cliente presencial**
  + RTO: 1 hora
  + MTD: 1 día
  + RPO: 2 días
* **Atención al cliente presencial**
  + RTO: 1 hora
  + MTD: 1 hora
  + RPO: 1 hora
* **Aplicaciones**
  + RTO: 1 hora
  + MTD: 1 hora
  + RPO: 12 horas
* **Equipos**
  + RTO: 30 min
  + MTD: 12 horas
  + RPO: 12 horas
* **Internet y Electricidad:** Van por subcontrata, por lo que solo podremos sacar el MTD:
  + MTD: 1 hora
* **Contabilidad**
  + RTO: 30 min
  + MTD: 30 min
  + RPO: 30 min

### Análisis de Riesgos

Como en el punto anterior, realizaremos dos medidas de riesgos, las expuestas en la teoría anteriormente descrita, por el INCIBE; y las que nos da PILAR.

Empezaremos con el análisis que nos otorga PILAR, en la pestaña de riesgos:



Los colores y los números significan lo siguiente:



Como podemos observar, se le añade un nivel muy crítico tanto a la confidencialidad como a la integridad, y un poco menos a la autenticidad y a la disponibilidad.

Para continuar, haremos el análisis de riesgos como se detalla de forma teórica en la guía del INCIBE:

Primero, **determinaremos las amenazas**, posteriormente **determinaremos su probabilidad y su impacto**, y posteriormente realizaremos el producto de estos para ver el **nivel de la amenaza**.

Tras buscar las posibles amenazas, y analizarlas, nos queda la siguiente tabla:

|  |  |  |  |
| --- | --- | --- | --- |
| **Amenaza** | **Probabilidad** | **Impacto** | **nivel** |
| Inundación | 2 | 6 | 12 |
| Incendio | 3 | 6 | 18 |
| Robo (presencial) | 3 | 10 | 30 |
| Ciberataque | 5 | 10 | 50 |
| Caída de suministro eléctrico | 4 | 4 | 16 |
| Caída de red | 6 | 1 | 6 |
| Malfuncionamiento de equipos | 6 | 4 | 24 |

A continuación, se explicarán los valores decididos, y que estrategia vamos a seguir para tratar dichos riesgos:

* **Inundación:** Aunque nunca se ha producido, la delegación de hacienda no se encuentra muy distante del rio, tan solo a un bloque de edificios, es por esto por lo que se le ha dado una probabilidad de 2. El impacto seria notable, pero no muy alto, ya que todos los equipos están en lugares elevados. Como no se puede evitar, hemos decidido tomar una estrategia de Asumir el riesgo.
* **Incendio:** Al igual que la inundación, es probable que ocurra. No nos preocuparía la perdida de la información de los equipos, ya que todo se almacena en los servidores, de los que se hace una copia en espejo por sistema RAID en servidores en otra ubicación. Como no se puede evitar, hemos decidido tomar una estrategia de Asumir el riesgo.
* **Robo (presencial):** Es también poco probable, pero no imposible. Además, si el robo se lleva a cabo con éxito, supondría un grave problema para la administración pública, por lo que se le ha asignado el mayor impacto posible. La estrategia que vamos a tomar para enfrentarnos a este riesgo es la de eliminarlo. Esta estrategia de eliminación supondrá la instalación de todas las cámaras de seguridad necesarias, así como la contratación de una empresa de seguridad para que vigile el edificio tanto de día como de noche.
* **Ciberataque:** Consideramos que es mucho más probable que el robo, debido al anonimato que supone y a la dependencia de la administración de las TIC. Aun así, el impacto sería el mayor, por las razones anteriormente vistas. La estrategia a seguir es la de eliminarlo. Esta estrategia supondrá tanto una formación básica de ciberseguridad a todos los empleados, como una formación superior para el departamento de informática. Además, se adquirirán licencias de antivirus para empresas, eligiendo un antivirus cuyas características estén acordes con la magnitud de esta delegación.
* **Caída de suministro eléctrico:** No es algo extraño que haya un corte eléctrico, ya puede ser por diferentes factores: tormenta, problemas con el cableado, accidentes, problemas del proveedor. Como no está a nuestro alcance, decidimos transferir el riesgo a un tercero, en este caso, al proveedor de energía.
* **Caída de red:** Similar a la caída de suministro eléctrico. También decidimos transferir el riesgo a un tercero, en este caso, al proveedor de internet.
* **Malfuncionamiento de equipos:** Es bastante habitual que haya equipos que dejen de funcionar, ya sea por errores de los operarios, problemas con algún programa, o simplemente mala suerte. Aunque no tiene mucho riesgo, es algo que puede ocurrir con bastante frecuencia. Esta amenaza hemos decidido implantar medidas para mitigarla.

## 4.3. Fase 2: Determinación de la estrategia de Continuidad

En esta fase, nos ocuparemos de determinar una estrategia de continuidad para cada amenaza vista en la fase anterior, es decir, elaboraremos un plan para saber cómo recuperarnos de estas amenazas, y no actuar improvisadamente.

### Inundación

Si hemos sufrido una inundación, lo primero que haremos será drenar todo el agua que pueda quedar en el edificio, antes de poner en marcha cualquier actividad.

Posteriormente, se revisarán los equipos: se hará un inventario de cuantos continúan operativos, y cuáles no. Dicho informe se enviará al departamento de informática, para que lo puedan evaluar, y decidan con que prioridad comprar los equipos faltantes. Ante duda, la prioridad será:

1. Servidores
2. Equipos del departamento de informática
3. Impresoras y equipos comunes
4. Equipos personales del resto de departamentos

Paralelamente a este procedimiento, se realizará lo mismo para el archivo en físico de documentos, se hará un inventario de que documentos han sido destruidos. Sin embargo, este inventario se trasladará a la oficina general de Hacienda, desde donde se nos informará que hacer.

Por último, se comprobará el mobiliario, viendo que ha quedado en desuso, y que hace falta renovar.

Después de todas estas fases, que durarán un máximo de 2 días hábiles, se reabrirá al público.

Mientras tanto, mediante teletrabajo, debemos procurar que la atención al cliente online se reanude el mismo día de la inundación o, como muy tarde, al día siguiente a primera hora.

### Incendio

Al igual que con la inundación, se harán paralelamente dos inventarios:

Primero, se revisarán los equipos: se hará un inventario de cuantos continúan operativos, y cuáles no. Dicho informe se enviará al departamento de informática, para que lo puedan evaluar, y decidan con que prioridad comprar los equipos faltantes. Ante duda, la prioridad será:

1. Servidores
2. Equipos del departamento de informática
3. Impresoras y equipos comunes
4. Equipos personales del resto de departamentos

Mientras tanto, otro equipo se encargará de revisar los documentos calcinados, para ver cuales quedan en un estado aceptable y cuáles no. Dicho inventario se enviará a la sede central de hacienda.

Al igual que con las inundaciones, mediante teletrabajo, debemos procurar que la atención al cliente online se reanude el mismo día de la inundación o, como muy tarde, al día siguiente a primera hora.

### Robo (presencial)

Dividiremos el robo presencial en dos variantes:

Robo de bienes materiales: Aquí incluiremos el dinero, mobiliario, etc. es decir, material que consideramos **remplazable**. La única estrategia aquí es hacer inventario de lo robado y dar parte a la policía nacional. También se revisarán las cámaras de seguridad, cuyo contenido se incluirá en el parte a la policía para facilitarles su labor.

Robo de información: Aquí, aunque sean también bienes materiales, incluiremos tanto equipos informáticos como documentos de texto, es decir, robos que suponen una **fuga de información**. Al igual que la anterior, se intentará hacer un inventario de la información robada, el alcance de dicha brecha de datos, y se dará parte a la policía. Es importante también tener en cuenta que hay que dar parte a las personas cuya información se ha visto comprometida, como dictamina la Ley Orgánica de Protección de Datos.

### Ciberataque

Una vez ocurrido el ciberataque, si no hemos podido mitigarlo, lo único que nos queda por hacer es lo mismo que en el robo de datos en un ataque presencial: se intentará hacer un inventario de la información robada, el alcance de dicha brecha de datos, y se dará parte a la policía. Es importante también tener en cuenta que hay que dar parte a las personas cuya información se ha visto comprometida, como dictamina la Ley Orgánica de Protección de Datos.

### Caída del suministro eléctrico

Una vez el apagón ya haya ocurrido, y hayamos respondido a la contingencia como se verá en el posterior apartado, se encenderán todos los equipos para analizarlos, priorizando los servidores y aquellos equipos que fueran apagados “de forma no segura”.

Se le preguntara a cada uno de los operarios de cada equipo cuales eran las últimas operaciones que estaban haciendo con ellos, para que el equipo informático revise que estas últimas operaciones han sido guardadas con éxito, y no se haya hecho un trabajo perdido.

Además, el equipo informático hará una revisión de la base de datos, para comprobar que está consistente.

### Caída de red

Debido al poco nivel de amenaza que supone, no se hará mayor plan de continuidad.

Cabe destacar que el equipo informático se encargará de llamar a la proveedora para comprobar cuando se restaurará el servicio, y si no es dentro de un tiempo relativamente corto (en las próximas 2-4 horas), montarán una pequeña red utilizando conexión móvil (4G o 5G) para llevar a cabo la atención al cliente online.

### Malfuncionamiento de equipos

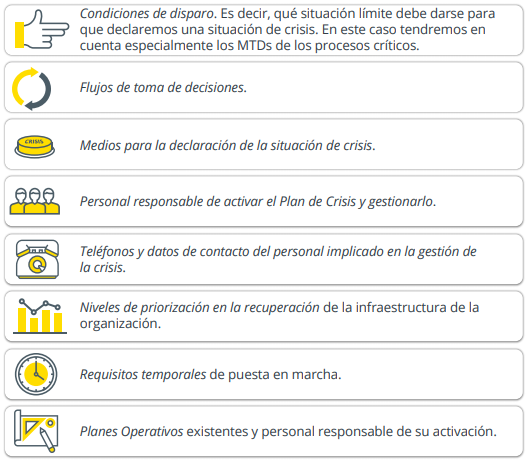
El único plan de continuidad presente es que el equipo informático haga una revisión para determinar el problema, y solucionarlo. Si no se consigue, se le dará al operario un PC de sustitución mientras se inspecciona el equipo mal funcionante más exhaustivamente.

## 4.4. Fase 3: Respuesta a la contingencia

Una vez ya tenemos detalladas las distintas amenazas, y que hacer una vez han ocurrido para recuperarnos lo antes posible, vamos a ver cómo responder en el momento de la contingencia para que, de nuevo, actuemos de acuerdo a un plan, y no de manera improvisada.

### Plan de Crisis y planes operativos de Recuperación de Entornos

En este apartado veremos, para cada amenaza descrita anteriormente, que hacer **en el momento que esta amenaza ocurre**. Como hemos visto anteriormente, un plan de crisis contiene los siguientes apartados:



En cuanto a los planes operativos, una vez tratemos la crisis, elegiremos los planes de respuesta adecuados a la crisis. A continuación, veremos las distintas crisis posibles, y su plan:

**Inundación**

La **condición de disparo** será que, debido a una gran tormenta o crecida, el agua empiece a entrar en el edificio.

Distinguiremos **dos tipos de inundaciones**: leves y graves.

**En una inundación leve**, serán los empleados que estén en ese momento de cara al público (seguridad y recepción) quienes informarán a todos los clientes de que evacuen el edificio, si es posible por las puertas principales, y si no, por las de emergencia. Será el personal de seguridad quien se encargará de guiar a los clientes hacia su salida. Mientras tanto, el resto de los trabajadores guardarán el trabajo que estén haciendo en sus equipos, procurarán moverlos, dentro de lo posible, a un lugar elevado (para evitar su deterioro si el agua sube), y desalojarán el edificio. Será el director, o la persona de máximo rango que se encuentre en ese momento en el edificio, quien se encargará de avisar a los bomberos vía telefónica. En este caso, la temporalidad adecuada es que los clientes se encuentren fuera del edificio en los primeros 15 minutos desde que se detecta la crisis, y los empleados no tarden más de 20 en hacerlo.

**En una inundación grave**, será el empleado de seguridad más cercano a la alarma del edificio quien de la alarma de emergencia. A raíz de esto, su prioridad será evacuar a los clientes lo más rápido posible, mientras que los trabajadores detendrán lo que están haciendo en el momento, procurarán no detenerse a recuperar sus pertenencias, y desalojarán el edificio con la mayor presteza posible. Será el empleado de seguridad que accionó la alarma quien se ponga en contacto con el servicio de emergencias, y no otro, para no colapsar dicho servicio. Todas estas operaciones se deberán realizar en un máximo de 10 minutos.

**Incendio**

La **condición de disparo** en este caso puede ser dos, que suene la alarma de incendios, o que un empleado o cliente vislumbre humo o fuego dentro del edificio.

Al igual que en el caso de la inundación, podemos distinguir dos tipos de incendios: leves o graves.

Consideramos **incendio leve** a aquel que tenemos la certeza de que es leve, y solo afecta a una máquina, equipo o mobiliario; es decir, es un incendio muy localizado, y siempre que haya sido encontrado por alguien antes de que salte la alarma de incendios. Será la persona que lo encuentre quien se encargue de ir al extintor más cercano, con la mayor velocidad posible, y procederá a extinguir el fuego. Posteriormente, informará al director, o al mayor cargo que se encuentre en el edificio, para dar el correspondiente parte.

Consideramos **incendio grave** en el momento en el que se nos ha avisado de que han avistado humo, pero no sabemos dónde, vemos un incendio que abarca más de un solo “objeto” (equipo, mobiliario, etc), o suena la alarma de incendios (da igual que el incendio por el que haya sido activada sea muy pequeño). En el momento que se conozca la amenaza, si no está sonando la alarma, se activará inmediatamente. A partir de aquí, se procederá como en el caso de una inundación grave: Será el personal de seguridad quien se encarga de guiar a los clientes al exterior por la salida, o por las puertas de emergencia, y los empleados dejarán todo lo que estén haciendo para evacuar, siguiendo el plan de evacuación según donde se encuentren. Esta operación no debe durar más de 5-10 minutos.

**Robo (presencial)**

La **condición de disparo** será el momento en el que se visualice al asaltante entrar en el edificio.

En este caso también distinguimos dos clases de robo, y la manera de actuar será ligeramente diferente:

Consideramos un **robo sin violencia** aquel robo en el que el asaltante (o asaltantes) no lleva armas (ya sean blancas o de fuego), y su única ofensiva es la amenaza. En este caso, como en el siguiente, se priorizarán las vidas humanas. El encargado de llevar a cabo este plan de crisis será el miembro de seguridad más cercano. Lo primero que hará será dar aviso inmediatamente por radio al resto de personal de seguridad, quienes se encargarán de acudir en su ayuda, e informar a la policía. y se aproximará al asaltante para reducirle. Para ello, tendrá que actuar con prudencia, ya que podría ser que se convirtiera en un robo con violencia. A continuación veremos lo que ocurre si es así.

Consideramos **robo con violencia** aquel en el cual el asaltante (o asaltantes), está armado. Nuestras prioridades son dos: proteger tantas vidas como sea posible, y avisar a las autoridades lo antes posible. Así, si los atacantes tienen rehenes, se hará lo que pidan para que liberen a estos. En este caso, será alguno de los empleados que no se encuentra en el mismo lugar de los atacantes quien intente avisar a las autoridades, mientras los trabajadores de seguridad les intentan retener lo máximo posible. Dejaremos su detención a las autoridades, ya que tienen más medios y experiencia que los integrantes de la empresa.

**Ciberataque**

Un ciberataque es muy difícil de detectar mientras ocurre, por esto los encargados de informática instalarán algún honey pot en la red. Así, la **condición de disparo** será muy simple, que un empleado de informática detecte algún intento de intrusión en la red, por un usuario externo a la misma. En este caso, dicho informático activará el proceso de seguridad, cortando toda conexión con la red exterior. Una vez cortado, se analizará meticulosamente la red interna con ayuda de todo el equipo para ver si el atacante sigue dentro, y si es así, detectarle y expulsarle.

**Caída de suministro eléctrico**

La **condición de disparo** será el apagón, y en el momento de este, el personal de informática más cercano irá a comprobar que el SAI funciona correctamente. Si es así, los empleados deberán guardar todas las operaciones que estén haciendo en sus equipos, y apagarlos. Mientras tanto, el equipo informático se ocupará de apagar de forma segura el servidor, y el director, o el máximo cargo que se encuentre en el momento en el edificio, se encargará de llamar a la proveedora de electricidad para que se instale un grupo electrógeno lo antes posible, y poder continuar con las labores rutinarias.

**Caída de red**

En este caso, no hay mucho que hacer. La **condición de disparo** será que la conexión de red con el exterior no funciona, por lo que algún miembro del equipo informático se encargará de llamar inmediatamente a la proveedora de servicios. Si dicha proveedora les informa de que a ellos no les consta que haya ningún corte de internet, el equipo informático se pondrá a trabajar en el problema lo antes posible, ya que se podría tratar de un ataque informático.

**Malfuncionamiento de Equipos**

La **condición de disparo** será que un empleado detecte que su equipo no está funcionando correctamente, por lo que lo que hará será acudir al departamento de informática, para solicitar su ayuda. Un informático hará un análisis del equipo para ver la posible causa del malfuncionamiento y poder repararlo. Otra vez, hay que actuar con cautela, pues puede tratarse de nuevo de indicios de un posible ataque informático.

### Procedimientos tecnicos de trabajos

En este apartado, se dispondrán diferentes documentos con información de utilidad referentes a cada una de las diversas amenazas:

**Elementos de emergencias**

El edificio dispone de 13 **extintores** para incendios normales, además de 4 **extintores especiales** **para fuegos electrónicos**.

Los trece extintores se encuentran dispuestos de la siguiente manera: dos en el hall principal, y uno en cada pasillo de las plantas superiores.

Los extintores para incendios electrónicos se encuentran dos en la sala de servidores, y uno en cada planta, al lado de la impresora.

También dispone de **alarma de incendios**, la cual tiene sensores de humos en todas las salas de edificios. Además de esto, dispone de un pulsador en la puerta de las escaleras de cada planta, por si se quiere accionar manualmente para cualquier emergencia.

Por último, disponemos de **martillos de emergencia** por si tuviéramos que romper alguna ventana, se encuentran también al lado de los pulsadores de la alarma.

**Ayuda con malfuncionamiento de equipos**

Si un equipo no funciona correctamente, hay una aplicación instalada llamada **TeamViewer**, con la que podremos ceder el control a un trabajador del área de informática, que intentará resolver el problema. Tan solo le tenemos que comunicar nuestro id y nuestra contraseña, como los que vienen a continuación



A la hora de iniciar el equipo después de un “apagado brusco”, lo primero que tenemos que hacer es comprobar que todos los documentos en los que estábamos trabajando siguen en su última versión. De no ser así, se informará también al equipo informático.

**Lista de inventariado: Equipos**

Se dispone de una lista de inventariado de equipos, para poder hacer inventario en el caso en el que se sufra un robo, o haya que comprobar su funcionamiento.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ORDENADORES PERSONALES** | | | | | | |
| **Nombre** | **Dirección IP** | **Dirección MAC** | **S.O.** | **Versión** | **Localización** | **Importancia** |
| PC1 | 192.168.0.4 | **2C-AE-3E-57-9F-DE** | Windows | 7 | Recepción | 5 |
| PC2 | 192.168.0.5 | **50-C7-0D-70-86-C6** | Windows | 7 | Despacho 101 | 4 |
| PC3 | 192.168.0.6 | **A2-DA-17-22-E8-44** | Windows | 7 | Despacho 102 | 4 |
| PC4 | 192.168.0.7 | **17-2E-9F-A9-45-A5** | Windows | 7 | Despacho 103 | 4 |
| PC5 | 192.168.0.8 | **6E-52-FA-7E-5E-2B** | Windows | 7 | Despacho 104 | 4 |
| PC6 | 192.168.0.9 | **76-A4-61-E0-E0-33** | Windows | 7 | Despacho 105 | 4 |
| PC7 | 192.168.0.10 | **22-61-12-79-3A-B3** | Windows | 7 | Despacho 106 | 4 |
| PC8 | 192.168.0.11 | **98-2A-6E-B1-BB-2A** | Windows | 7 | Despacho 107 | 4 |
| PC9 | 192.168.0.12 | **A6-05-B0-7D-6F-55** | Windows | 7 | Despacho 108 | 4 |
| PC10 | 192.168.0.13 | **DE-64-61-5D-32-B4** | Windows | 7 | Despacho 109 | 4 |
| PC11 | 192.168.0.14 | **3F-2B-28-64-6B-B6** | Windows | 7 | Despacho 110 | 4 |
| PC12 | 192.168.0.15 | **62-99-E2-BA-0A-3E** | Windows | 7 | Recepción | 5 |
| PC13 | 192.168.0.16 | **A2-CB-C0-3F-B4-4A** | Windows | 7 | Despacho 201 | 4 |
| PC14 | 192.168.0.17 | **4D-73-B4-A2-D0-07** | Windows | 7 | Despacho 202 | 4 |
| PC15 | 192.168.0.18 | **06-3B-0C-A2-71-E0** | Windows | 7 | Despacho 203 | 4 |
| PC16 | 192.168.0.19 | **30-3E-C7-A5-D9-71** | Windows | 7 | Despacho 204 | 4 |
| PC17 | 192.168.0.20 | **1D-AA-2E-B6-5F-9D** | Windows | 7 | Despacho 205 | 4 |
| PC18 | 192.168.0.21 | **1B-26-07-1E-BE-EB** | Windows | 7 | Despacho 206 | 4 |
| PC19 | 192.168.0.22 | **3B-37-DF-75-A2-84** | Windows | 7 | Despacho 207 | 4 |
| PC20 | 192.168.0.23 | **D7-19-6C-FE-45-37** | Windows | 7 | Despacho 208 | 4 |
| PC21 | 192.168.0.24 | **7C-01-F7-CB-37-66** | Windows | 7 | Despacho 209 | 4 |
| **Ordenadores Informática** | | | | | | |
| Inf1 | 192.255.0.1 | **2C-AE-3E-57-9F-DE** | Windows | 7 | Despacho 210 | 5 |
| inf2 | 192.255.0.2 | **50-C7-0D-70-86-C6** | Ubuntu | 20.04 | Despacho 301 | 7 |
| Inf3 | 192.255.0.3 | **A2-DA-17-22-E8-44** | Ubuntu | 20.04 | Despacho 302 | 7 |
| Inf4 | 192.255.0.4 | **17-2E-9F-A9-45-A5** | Ubuntu | 20.04 | Despacho 303 | 7 |
| Inf5 | 192.255.0.5 | **6E-52-FA-7E-5E-2B** | Ubuntu | 20.04 | Despacho 304 | 7 |
| Inf6 | 192.255.0.6 | **76-A4-61-E0-E0-33** | Ubuntu | 20.04 | Despacho 305 | 7 |
| Inf7 | 192.255.0.7 | **22-61-12-79-3A-B3** | Ubuntu | 20.04 | Despacho 306 | 7 |
| **Servidores** | | | | | | |
| Srvr1 | 192.255.0.10 | **50-C7-0D-70-86-C6** | Ubuntu Server | 21.04 | Planta -1 | 10 |
| Srvr2 | 192.255.0.11 | **50-C7-0D-70-86-C7** | Ubuntu Server | 21.04 | Planta -1 | 10 |
| Srvr3 | 192.255.0.12 | **50-C7-0D-70-86-C8** | Ubuntu Server | 21.04 | Planta -1 | 10 |
| **Miscelánea** | | | | | | |
| Impresora1 | 192.168.0.100 | **50-C7-0D-70-86-C6** | - | - | Planta 1 | 2 |
| Impresora2 | 192.268.0.101 | **50-C7-0D-70-86-C7** | - | - | Planta 2 | 2 |
| Impresora3 | 192.168.0.102 | **50-C7-0D-70-86-C8** | - | - | Planta 3 | 2 |
| Router1 | 192.255.0.0  192.168.0.0 | **50-C7-0D-70-86-C9** | Cisco | - | Planta 3 | 9 |
| Router1 | 192.168.0.1  192.168.0.2 | **50-C7-0D-70-86-C9** | Cisco | - | Planta 2 | 9 |
| Router1 | 192.168.0.3 | **50-C7-0D-70-86-C9** | Cisco | - | Planta 1 | 9 |

**Lista de inventariado: Archivos**

En cuanto a los archivos en formato físico se refiere, el inventario se encuentra en la sala del archivo, nada más entrar, en el primer casillero, el primer documento. Sin embargo, la sede central de Hacienda tiene una copia de dicho inventario, por lo que no debemos temer si se destruye como consecuencia de alguna amenaza.

Debido a la existencia ya de dichos documentos, no se detallarán en este informe.

**Backups Automáticos**

En cuanto a la realización de Backups se refiere, el equipo informático tiene automatizada esta tarea. Mediante un software específico, se realiza una copia de seguridad de todos los equipos hacia el servidor una vez cada tres días.

A su vez, el servidor realizará su copia de seguridad una vez cada mes a un servidor externo. Se ha decidido este periodo de tiempo tan largo entre copias de seguridad porque, por una parte, es una tarea costosa que tiene al servidor mucho tiempo trabajando, y por otra, el servidor de almacenamiento está conectado por RAID con otro servidor en otra localización, por lo que, si se perdieran los archivos, habría una alta probabilidad de recuperarlos.

Dichas copias de seguridad se efectuarán a media noche.

## 4.5. Fase 4: Prueba, Mantenimiento y Revisión

En esta fase del plan de contingencia, nos ocuparemos de todo lo que se refiere a mantener actualizado el mismo. Primero comenzaremos con el plan de pruebas.

### Plan de pruebas

A continuación, redactaremos una serie de pruebas, para ver que comprobarán, como se deberán realizar, y el resultado que esperamos obtener:

**Prueba interrupción servicio eléctrico**

En esta prueba se comprobará que, ante una interrupción súbita del servicio eléctrico, el sistema SAI funciona adecuadamente.

Para no ocasionar daños en el funcionamiento de Hacienda, esta prueba se realizará dos veces al año, pero durante la noche, cuando no esté abierta al público y los trabajadores no se encuentren en el lugar.

En primer lugar se encenderán todos los equipos, para simular un entorno de trabajo real, y a continuación se interrumpirá el suministro eléctrico del edificio. Después de esto, se comprobará que el Servicio de Alimentación Ininterrumpida realiza su trabajo, y se mantiene encendido y alimentando a los equipos el tiempo mínimo para guardar su progreso y apagarlos de forma segura.

El encargado de realizar esta prueba será el director de informática, junto con dos empleados de su elección.

**Simulacro de evacuación**

Dicho simulacro se realizará una vez al año, en horario laboral, elegido por consenso entre los jefes de departamento.

Dicha fecha y hora no se informarán a los trabajadores, que deberán responder como si de una emergencia se tratase. El objetivo es conseguir evacuar el edificio lo más rápido posible, dentro de los plazos anteriormente descritos, en las amenazas de incendio e inundación.

**Auditoría informática: Ejercicio de Red Team**

Esta prueba se realizará una vez cada dos años, y será contratada por el director de la delegación de Hacienda.

La prueba se contratará a una empresa externa de auditorías informáticas, a elección del director, y consistirá en un ejercicio de Red Team. Este ejercicio se basa en que un equipo de hackers intentará acceder a nuestro sistema, para ver hasta qué punto son capaces de llegar, y a cuanta información son capaces de acceder. Sobra destacar que aunque puedan acceder a información confidencial, no accederán a ella, sino que reflejarán en su informe hasta qué punto han conseguido vulnerar la seguridad.

El objetivo de esta prueba es ver hasta qué punto está el departamento de informática (y el resto de los empleados), preparados ante un ataque informático.

Posteriormente a cada una de estas pruebas, se realizará un informe con los resultados de esta. Dicho informe será realizado por el responsable de cada prueba (o por la empresa auditora en el caso del ejercicio de Red Team), y se entregarán al director. El director pondrá en conocimiento de la delegación central el resultado de las pruebas, y decidirá con ellos, mediante una reunión, si hay que tomar alguna medida excepcional. Algunas de estas medidas pueden ser:

* Cambiar algún tipo de prueba
* Cambiar algún objetivo de alguna prueba
* Concienciar/entrenar al equipo para próximas pruebas
* Añadir/eliminar pruebas

### Plan de Mantenimiento

En cuanto al mantenimiento del plan de contingencia se refiere, lo único destacable es la **actualización de los inventarios** cuando se añadan/se retiren nuevos equipos.

Además, cabe destacar la importancia de actualizar también los responsables de las pruebas y los planes de crisis, ya que en este plan se ha especificado quien era el responsable según su puesto de trabajo, pero sin dar nombres ni apellidos. Es importante que, si hay cambios en estos puestos, ya sea por contrataciones, despidos, o ascensiones, se le **informe al nuevo encargado de sus responsabilidades dentro del plan de contingencia**.

Por último, también habrá que cambiar el plan si se **redistribuyen los extintores o alarmas**, se compran más, o se elimina algún punto explicado anteriormente.

## 4.6. Fase 5: Concienciación

Esta es la última fase, y consiste en dar a conocer el plan de contingencia a todo el personal involucrado en Hacienda. Para ello, se ha optado por la estrategia de informarles presencialmente, por lo que llevaremos a cabo diferentes reuniones con ellos:

**Reunión principal**

Será una breve reunión en la que se informará al personal de la existencia de este plan de continuidad.

En ella, principalmente se explicará lo que es un plan de continuidad, sus importancias, y la manera en la que puede ayudar para que todo funcione correctamente.

**Segunda reunión: estrategias de continuidad**

En esta segunda reunión daremos a conocer todas las estrategias de continuidad que se han visto en la [Fase 2](#_4.3._Fase_2:).

Aquí, explicaremos detalladamente a todo el personal cuales son los planes de continuidad aplicables en cada caso, les haremos conocer sus responsabilidades, y resolveremos todas las posibles dudas que tengan. A parte, informaremos de quienes serán los responsable de activar los [Planes de crisis](#_Plan_de_Crisis), y con los que tendremos una reunión más adelante.

Por último, se le dará a cada empleado una copia del plan de contingencia, para que la conserven, revisen, y nos pregunten si les surge aluna duda fuera de la reunión.

**Tercera reunión: responsables de los Planes de crisis**

En esta última reunión, se informará a los responsables asignados de activar cada plan de crisis su tarea, que tienen que hacer exactamente, y como deberán gestionar adecuadamente dicha crisis.

A parte de las reuniones, se harán jornadas de concienciación informática de vez en cuando, como cursos de nociones básicas de seguridad informática para todos los empleados, o de cómo realizar copias de seguridad manualmente y la importancia de hacerlas.

# 7. Conclusión

Como conclusión a este trabajo, cabe destacar que he aprendido lo que es un plan de contingencia, algo que anteriormente desconocía su existencia. Además, he aprendido los pasos y fases que tiene, lo cual puede ser muy útil ya no solo si en un futuro se me encarga realizar algún plan de este tipo para alguna empresa, sino que también puede ser útil a la hora de leer e interpretar algún plan de contingencia ya hecho.

Algo muy curioso, es que he aprendido de la existencia del Esquema Nacional de Seguridad, ya que no sabía que todo el tema de la seguridad informática en las entidades públicas estaba “centralizado”.

Por último, cabe destacar que también he aprendido la existencia de las herramientas LUCIA y PILAR, y un poco el uso general de esta última.

Por todo esto, creo que ha sido un trabajo bastante didáctico y enriquecedor, el cual estoy seguro de que me servirá en un futuro.

# 8. Bibliografía

Administración Electronica. (s.f.). Obtenido de https://www.administracionelectronica.gob.es/pae\_Home/pae\_Estrategias/pae\_Seguridad\_Inicio/pae\_Esquema\_Nacional\_de\_Seguridad.html#.YMJ90vkzZhE

Agencia Tributaria. (s.f.). *agenciatributaria.gob.es*. Obtenido de https://www.agenciatributaria.gob.es/AEAT.sede/Inicio/\_otros\_/\_Direcciones\_y\_telefonos\_/Delegaciones\_y\_Administraciones/Castilla\_y\_Leon/Burgos/Delegacion/Delegacion.shtml

BOE. (s.f.). Obtenido de https://www.boe.es/eli/es/l/2015/10/01/40/con

BOE. (s.f.). Obtenido de https://www.boe.es/diario\_boe/txt.php?id=BOE-A-2018-5370

CCN. (s.f.). *pilar.ccn-cert.cni.es*. Obtenido de https://pilar.ccn-cert.cni.es/index.php/pilar/beneficios-de-pilar

CCN. (s.f.). *pilar.ccn-cert.cni.es*. Obtenido de https://pilar.ccn-cert.cni.es/index.php/pilar/que-es-pilar

CCN-Guia PILAR. (s.f.). Obtenido de https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2844-ccn-stic-470i2-pilar-continuidad-manual-de-usuario-v7-1/file.html

Default Reasoning. (s.f.). *defaultreasoning.com*. Obtenido de https://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

EAE Business School. (s.f.). Obtenido de https://retos-directivos.eae.es/plan-de-contingencia-ejemplo-definicion/

INCIBE. (s.f.). *incibe.es*. Obtenido de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad\_plan\_de\_contingencia\_y\_continuidad\_de\_negocio.pdf

University Of California. (s.f.). *itsm.ucsf.edu*. Obtenido de https://itsm.ucsf.edu/business-impact-analysis-bia-0