UNIVERSIDAD DE SANTIAGO DE COMPOSTELA

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

Implementación de un Sistema de Gestión de Continuidad de Negocio alineado con la ISO 22301 y la ISO 27031

Autor:
Lidia Sánchez Guerra
Directores:
Uxía Fernández García
José M. Cotos Yáñez

Grado en Ingeniería Informática

Febrero 2017

Trabajo de Fin de Grado presentado en la Escuela Técnica Superior de Ingeniería de la Universidad de Santiago de Compostela para la obtención del Grado en Ingeniería Informática

Dña. Uxía Fernández García, Directora Adjunta la empresa Ozona, y **D. José M. Cotos Yáñez**, Profesor del Departamento de Electrónica y Computación de la Universidad de Santiago de Compostela,

INFORMAN:

Que la presente memoria, titulada *Implementación de un Sistema de Gestión de Continuidad de Negocio alineado con la ISO 22301 y la ISO 27031*, presentada por **Dña. Lidia Sánchez Guerra** para superar los créditos correspondientes al Trabajo de Fin de Grado de la titulación de Grado en Ingeniería Informática, se ha realizado bajo nuestra dirección tanto desde la empresa Ozona como desde el Departamento de Electrónica y Computación de la Universidad de Santiago de Compostela.

Y para que así conste a los efectos oportunos, expiden el presente informe en Santiago de Compostela, a 8 de Enero de 2017:

La directora, El codirector, La alumna,

Uxía Fernández García José M. Cotos Yáñez Lidia Sánchez Guerra

Agradecimientos

A los directores de este proyecto, por el esfuerzo dedicado y la disponibilidad ofrecida durante estos meses, y a todas las personas que de algún modo han contribuido a la finalización exitosa de este proyecto.

Índice general

Índice de Figuras

Índice de Tablas

1. Introducción

1.1. Contextualización

El proyecto que se presenta en este documento tiene como objeto el desarrollo e implementación de un Sistema de Gestión de Continuidad de Negocio (en adelante, SGCN), alineado con los estándares internacionales ISO 22301 e ISO 27031, para la empresa Ozona (https://www.ozonaconsulting.com/).

El proyecto se realiza en el marco de trabajo regido por el convenio de colaboración entre Ozona y USC para la realización de prácticas en empresa y trabajos de fin de grado.

Mediante un SGCN, una organización puede asegurar la disponibilidad de sus procesos de negocio críticos ante situaciones de interrupción, así como implementar medidas preventivas para evitar los efectos negativos que puedan causar dichas situaciones. Por ejemplo: el servicio de virtualización es básico para que la empresa pueda entregar sus servicios a los clientes. Si el servicio de virtualización no está disponible, no habrá entrega de servicios y, por tanto, no se cumplirán los requisitos contractuales con dichos clientes provocando, entre otras, pérdidas económicas, pérdida de la reputación… Será necesario entonces realizar una evaluación de toda la empresa para identificar los servicios con mayor impacto sobre ésta, las amenazas que pueden materializarse y causar interrupciones, y la probabilidad de ocurrencia de éstas; es decir, realizar un proceso de análisis de riesgos, a partir del cual se tomarán las medidas pertinentes para evitar interrupciones y así asegurar la supervivencia empresarial ante situaciones adversas.

La norma ISO 22301 especifica los requisitos necesarios para el establecimiento, desarrollo, implementación, operación, monitorización y mejora de un SGCN. El estándar ISO 27031, alineado con la ISO 22301, incluye la especificación de las buenas prácticas para alinear las Tecnologías de la Información y las Comunicaciones (en adelante, TIC) con la continuidad de negocio.

Debido a la relevancia que tienen los servicios de Tecnologías de la Información (en adelante, TI) en Ozona, y la existencia de un Sistema de Gestión de Seguridad de la Información ya implementado, se tendrán en cuenta, para este proyecto, ambos estándares.

Adicionalmente a estos estándares, también serán utilizadas otras normas ISO alineadas con la continuidad de negocio. En el Capítulo 3 de esta memoria, se presentan en detalle todos los estándares utilizados para el desarrollo de este proyecto.

1.2. Motivación y Objetivos

Ozona ofrece a sus clientes servicios de assessment, auditoría, formalización de procesos, implementación, optimización y formación en las áreas de gestión de servicios de TI, seguridad de la información y continuidad de negocio. Actualmente, Ozona mantiene su propio sistema interno integrado de gestión de servicios de TI (certificación ISO 20000) y seguridad de la información (certificación ISO 27001). La incorporación de la gestión de continuidad de negocio al sistema integrado de Ozona permitiría, no sólo conseguir los beneficios asociados a la gestión de dicha área, sino también aportar valor al negocio, de manera que Ozona sea más competitiva en esta área.

El proyecto de implementación del SGCN tiene, principalmente, los siguientes objetivos:

- Identificar los servicios críticos para la empresa.
- Identificar y cuantificar los riesgos a los que están expuestos dichos servicios.
- Establecer medidas de actuación contra los riesgos de mayor impacto, con el fin de mitigarlos.
- Establecer Planes y Políticas orientadas a la continuidad y alineadas con los objetivos de negocio.
- Identificar a todas las partes interesadas, tanto internas como externas, obteniendo información sobre sus necesidades y expectativas, asegurando que éstas se cumplen.
- Establecer los procedimientos y niveles de comunicación apropiados para las partes interesadas.
- Establecer los roles y responsabilidades pertinentes, seleccionando al personal más adecuado en cada caso.
- Establecer procedimientos de monitorización, revisión y mejora del sistema.
- Conseguir un sistema gestionado que tenga en cuenta los cambios que se produzcan en la empresa y esté en constante actualización, controlando los riesgos emergentes y actuando contra ellos.
- Incluir el Sistema de Gestión de Continuidad de Negocio en el Sistema de Gestión Integrado de la empresa.

1.3. Estructura de la memoria

La memoria está organizada en varios capítulos cuyo contenido se presenta a continuación:

- Introducción: presentación general del proyecto, motivación y objetivos.

- Gestión del proyecto: incluye todos los apartados asociados a la gestión del TFG. La gestión del alcance define los límites del sistema a implementar, la

gestión de riesgos identifica las amenazas a las que está expuesto el proyecto y el nivel de riesgo asociado a cada una de ellas, la gestión de costes proporciona la estimación económica contemplada para el proyecto, la gestión temporal introduce el ciclo de vida sobre el que se desarrollará el proyecto y sus fechas temporales estimadas y, por último, la gestión de la configuración presenta el sistema de gestión documental que se empleará para garantizar la integridad y validez de los documentos del SGCN.

- Análisis: introduce los conceptos básicos para la comprensión de las normas ISO en que se basa el desarrollo del TFG. Se especifican los requisitos que tendrá el sistema y se detalla el caso de uso principal asociado a éste.

- Diseño e Implementación: incluye los detalles asociados al desarrollo del SGCN, desde su planificación inicial hasta la realización de la auditoría interna de evaluación de conformidad.

- Validaciones y pruebas: presenta el proceso de validación del sistema implementado.

- Conclusiones y ampliaciones: incluye una descripción de próximos pasos a seguir para la mejora del SGCN.

- Glosario: términos, definiciones y acrónimos requeridos para la adecuada comprensión de la temática del proyecto.

- Manual de usuario: presenta el documento principal generado para el uso directo por parte de los usuarios finales del SGCN.

- Bibliografía: referencias empleadas para el desarrollo del presente documento.

- Apéndice A: glosario con definiciones y términos.

- Apéndice B: Plan de Continuidad del SGCN. Los objetivos y metodología del Plan se encuentran especificados en el apartado 4.5.5. de este documento.

- Apéndice C: referencias bibliográficas empleadas en la redacción de esta memoria.

2. Gestión del Proyecto

2.1. Gestión del Alcance

La Gestión del Alcance define los límites que tendrá el proyecto a desarrollar, es decir, lo que se incluye y lo que no.

2.1.1. Descripción del alcance

Se implantará un SGCN alineado con las normas ISO 22301 y complementado con los requisitos relevantes de la norma ISO 27031.

De acuerdo con la metodología de implantación de sistemas de gestión de Ozona, la implantación de un SGCN sigue varios ciclos de mejora continua que se muestran en la Figura 2.1:

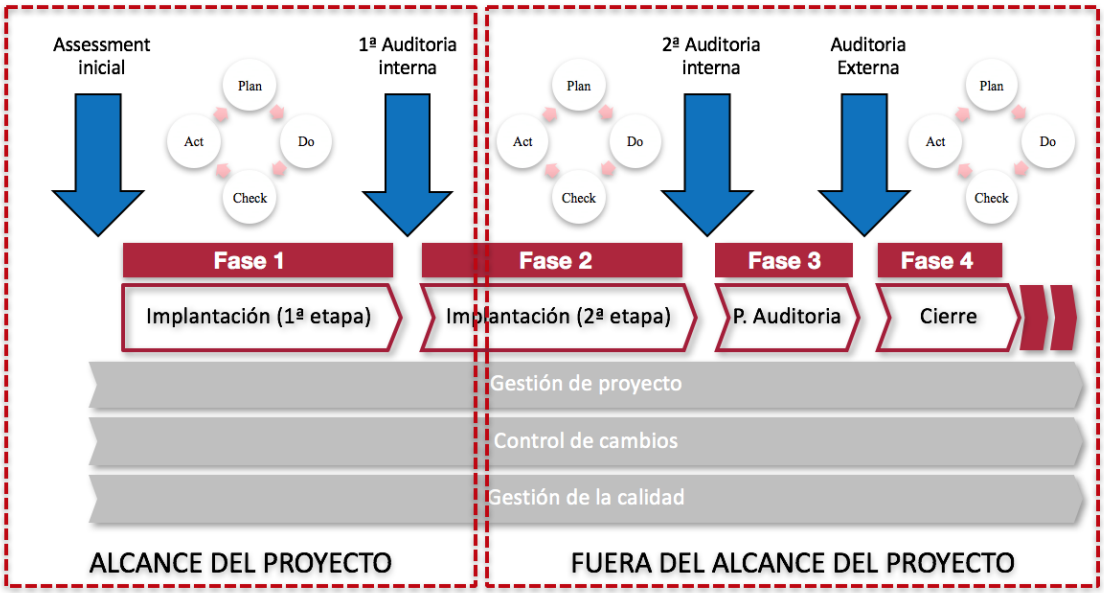

Figura 2.1: Metodología de implantación de sistemas de gestión en Ozona

Un proyecto completo de certificación para una empresa del tamaño de Ozona, tendría una duración estimada comprendida entre 8 y 10 meses, por lo que quedarán fases fuera del alcance de este proyecto. En cualquier caso, como veremos más adelante, el proyecto cubre la implantación de un SCGN completo, si bien, al final del proyecto éste no tendrá aun la madurez suficiente para pasar una auditoría externa.

En la Figura 2.2 se detallan las cláusulas en las que se agrupan los requisitos de la norma ISO 22301 y que serán contemplados en este proyecto:

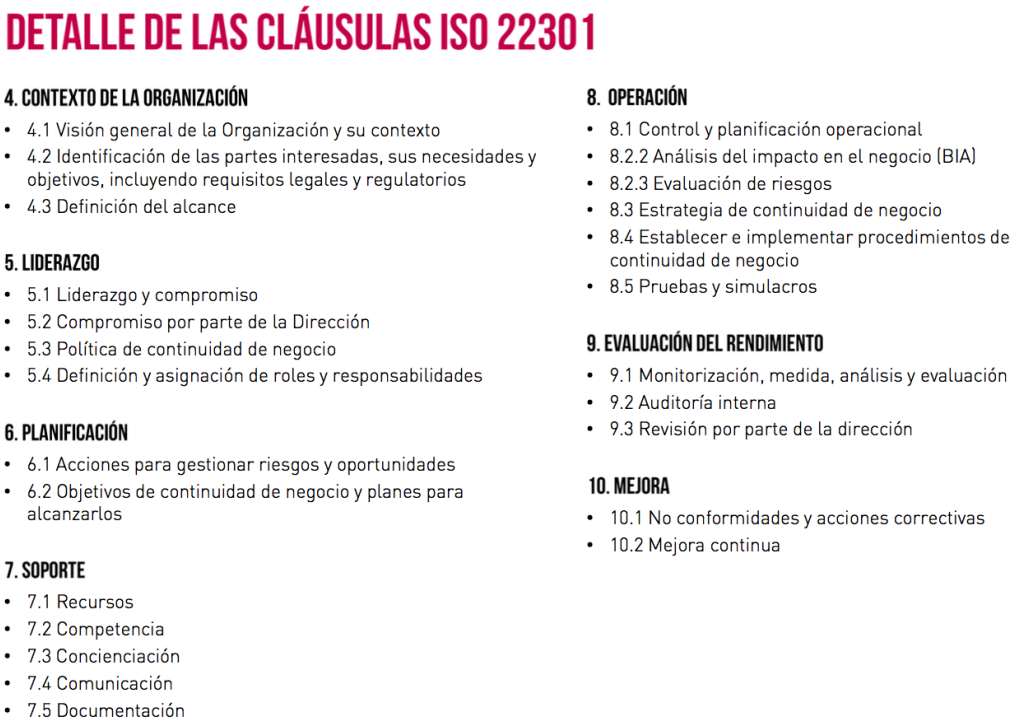

Figura 2.2: Cláusulas de la norma ISO 22301

En esta primera fase de implantación, perteneciente al alcance de este proyecto, el objetivo es cubrir todo el ciclo de vida del sistema de gestión y, con ello, los requisitos relacionados con los elementos que se van implementando, tal y como se muestra en la Figura 2.3 (el número por el que comienza la actividad, se refiere a la cláusula de la norma):

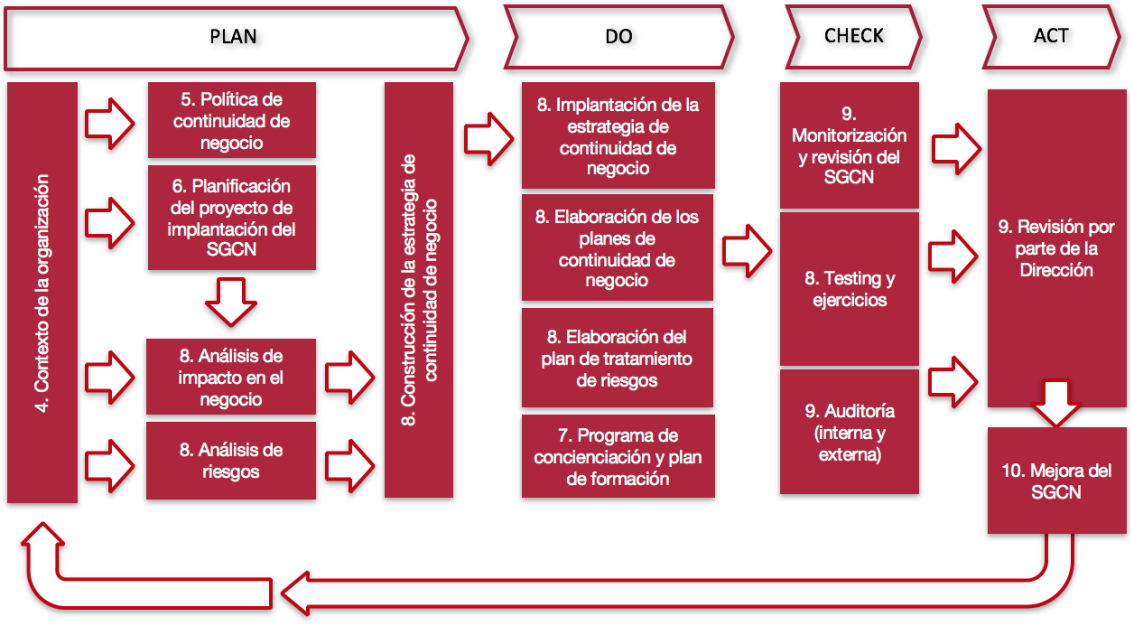

Figura 2.3: Ciclo de vida desglosado para la implementación del SGCN

Una vez finalizado un primer ciclo, se realiza una auditoría interna y se elabora un plan de acción para resolver todos los hallazgos identificados en la misma.

Se pasa entonces a la 2ª etapa de la implantación, que como ya se ha mencionado, por restricciones temporales, excede al alcance de este proyecto. Esta fase consiste en la implantación del plan de acción propuesto.

Si el proyecto de implantación del SGCN tiene además un objetivo final de certificación, como en este caso, se deberá realizar otra auditoría interna con un mínimo de un mes de antelación a la auditoría de certificación.

2.1.2. Criterios de aceptación

El SGCN incluirá los servicios, personas, responsabilidades, sistemas, comunicaciones y activos que soportan las actividades críticas de Ozona.

La certificación en la norma ISO 22301 es un objetivo adicional del proyecto de implantación del SGCN. Por tanto, como criterio de aceptación básico, el proyecto debe cumplir los requisitos de la ISO 22301.

La forma de verificar el cumplimiento de dichos requisitos será mediante las auditorías internas planificadas. En el ámbito de este proyecto se ha realizado 1 auditoría interna.

Por otro lado, el proyecto debe completarse antes de la fecha fin de entrega de este TFG, es decir, 10 de febrero de 2017.

2.1.3. Entregables del proyecto

La implantación del SGCN dará lugar a los siguientes entregables, que se condensarán en una única memoria:

- **Manual del SGCN**: es un documento básico para todo sistema de gestión ya que explica todos los elementos relevantes del sistema y referencia los documentos y metodologías clave para su desarrollo. Este documento permite tener una visión completa del sistema de gestión de continuidad de negocio. Además, sirve de apoyo durante las auditorías ya que contiene referencias a las evidencias de auditoría necesarias y se mantienen actualizadas.

- **Análisis de Impacto en el Negocio** (en adelante, **BIA**): se incluye el análisis de los procesos de negocio y servicios de TI de la organización. Describe de

manera detallada todos los elementos involucrados en el proceso o servicio, identificando los recursos clave y los riesgos asociados. Por último, evalúa el impacto a lo largo del tiempo asociado a la indisponibilidad del proceso o servicio analizado. De esta forma, se puede determinar las prioridades en cuanto a tiempos de recuperación cuando un incidente disruptivo afecta a más de un proceso o servicio. También proporciona un marco para garantizar que los recursos disponibles (de todo tipo: recursos humanos, técnicos o, incluso, financieros) se distribuyen de forma que proporcionen un mayor valor a la organización.

- **Documento de Estrategia**: define la estrategia de continuidad implantada para cada uno de los procesos y servicios de la organización, priorizando los más críticos.

- **Planes de Continuidad de Negocio**: describe los procedimientos de respuesta a incidentes disruptivos, y de continuación o restablecimiento de actividades críticas en un período de tiempo determinado. Se incluye en este apartado el Plan de *Disaster Recovery* (en adelante, DRP).

- **Plan de Comunicación**: establece todos los procedimientos de comunicación que se llevarán a cabo en caso de desastre, tanto a nivel interno (entre las personas y áreas de la empresa), como a nivel externo (clientes, proveedores, servicios de emergencia o, incluso, familiares del personal).

- **Informe de Pruebas del DRP**: informe de las pruebas realizadas al DRP.

- **Documento de definición de indicadores**: incluye la identificación de una serie de KPIs que permitirán monitorizar el sistema en unos términos objetivos.

- **Informe de auditoría interna**: registra los resultados de la auditoría interna que se realiza al SGCN para comprobar que cumple los requisitos y que se implementa y mantiene de una forma eficaz.

2.1.4. Restricciones del proyecto

El SGCN diseñado debe cumplir los requisitos impuestos por las normas ISO 22301 e ISO 27031, adaptando su implementación a las necesidades de Ozona.

Como ya se ha comentado en el apartado 2.1.1., por motivos temporales, el SGCN implantado durante este proyecto no tendrá madurez suficiente para la realización de una auditoría externa.

2.2. Gestión de Riesgos

En este apartado se incluye la gestión de los riesgos asociados al desarrollo del TFG.

2.2.1. Metodología

La metodología que se seguirá para la Gestión de Riesgos del proyecto será la propuesta por Sommerville y que está asociada al ciclo de vida en espiral, un proceso iterativo que se repetirá durante todo el ciclo de vida del proyecto.

El análisis de riesgos se reflejará, de manera detallada, en un documento Excel (*TFG_Identificación Riesgos.xlsx*) que además del propio análisis incluirá una hoja que reflejará los cambios que se realicen sobre dicho análisis en cada iteración. Este documento se incluye en la documentación entregada junto al presente documento.

Por tanto, el ciclo de vida en espiral mediante el que se realizará la gestión de riesgos comprende las siguientes fases:

- Identificación de riesgos: realizar un análisis que permita identificar los riesgos que afecten al proyecto, producto o negocio. La identificación se realizará mediante brainstorming y revisión de listas de control.

  Los riesgos identificados se clasificarán según la dimensión del impacto que tengan, siendo las distintas dimensiones posibles no excluyentes entre sí y entendiendo por dimensión aquellos elementos que se verán afectados en caso de materialización del riesgo. Los tipos de impacto definidos son los siguientes:

  - Proyecto: riesgos que afectan a la gestión del propio proyecto o que pueden comprometer su desarrollo.
  - Producto: riesgos que afectan a la calidad o corrección del sistema que se está desarrollando en el proyecto.
  - Negocio: aquellos riesgos que afectan a la organización que está desarrollando el proyecto.

  También habrá una segunda clasificación por categoría del riesgo, es decir, por la naturaleza del origen del riesgo:

  - Tecnología: riesgos asociados a algún software o hardware específicos que se empleen en el desarrollo del proyecto.
  - Personal: riesgos asociados a las personas que participan en la realización del proyecto, bien sea de forma directa: como desarrolladores de éste; o indirecta: se requieren como fuente de información para que los desarrolladores realicen ciertas tareas.
  - Organizacional: riesgos asociados al entorno organizacional en el que se desarrolla el proyecto.

  - Herramientas: riesgos asociados a herramientas CASE o cualquier software de soporte que se emplee en el desarrollo del proyecto.
  - Requisitos: riesgos asociados a cambios en los requisitos y el proceso de gestión que éstos requieren.
  - Estimación: riesgos asociados a planificaciones temporales o de recursos requeridos para el desarrollo del proyecto.

- Análisis de riesgos: mediante una valoración por intervalos, se analizarán los riesgos según su probabilidad e impacto. Además, será necesario definir un *apetito de riesgo*, entendiendo este concepto como el nivel y tipo de riesgo que una organización está preparada o dispuesta a aceptar. Aquellos riesgos que superen el apetito de riesgo deberán ser tratados con una estrategia determinada, con el fin de evitar la materialización de efectos adversos al proyecto. Los demás seguirán siendo revisados en las iteraciones posteriores, ya que su probabilidad o impacto pueden sufrir modificaciones.

  La clasificación establecida para los distintos niveles de probabilidad se muestra en la Tabla 2.1:

Probabilidad	Puntuación	Umbral	Descripción
Baja	1	<10%	Muy poco probable
Moderada	2	10-40%	Poco probable
Alta	3	40-80%	Muy probable
Muy alta	4	>80%	Casi segura

Tabla 2.1: Clasificación de niveles de probabilidad de riesgos

  La clasificación para los distintos niveles de impacto se realiza en base a umbrales que representan la repercusión que tendrá el riesgo sobre el coste total del proyecto. La especificación de los cuatro niveles se muestra en la Tabla 2.2:

Impacto	Puntuación	Umbral	Consecuencias en Plazo / Esfuerzo / Coste
Insignificante	1	<10%	La ocurrencia del riesgo no tendrá ningún impacto en el proyecto.
Tolerable	2	10-30%	La ocurrencia del riesgo tiene un impacto bajo en el proyecto, con consecuencias asumibles.
Serio	3	31-50%	La ocurrencia del riesgo tiene un impacto considerable, que puede comprometer el desarrollo del proyecto.
Catastrófico	4	>50%	La ocurrencia del riesgo causa daños irreparables o impide la continuación del proyecto.

Tabla 2.2: Clasificación de niveles de impacto de riesgos

Con ambos valores se crea la matriz que determinará el nivel de riesgo de cada uno de los riesgos identificados. Este nivel se obtiene como producto de los valores de impacto y probabilidad asignados.

El nivel de riesgo aceptable para Ozona está limitado a impactos menores que 'Serio' y a probabilidades inferiores a 'Moderada'. Englobaría los riesgos cuya puntuación pertenezca al área no destacada en la matriz. Los riesgos cuya puntuación pertenezca al área destacada de la Tabla 2.3 tendrán que tener una estrategia de tratamiento específica:

	PROBABILIDAD			
IMPACTO	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

Tabla 2.3: Matriz de niveles de riesgo

- Planificación de respuestas: teniendo la lista de riesgos que deben ser tratados será necesario realizar un análisis de cuáles son las estrategias más adecuadas que se deben poner en práctica para gestionarlos. Se distinguen cuatro estrategias de actuación posibles:

    - Prevención: aquellas estrategias con las que se reduce la probabilidad de ocurrencia del riesgo.
    - Minimización: engloba las estrategias cuyo objetivo es la reducción del impacto causado por un riesgo.
    - Contingencia: son aquellas estrategias que contemplan los escenarios de ocurrencia del riesgo, estableciendo planes de actuación para cada uno de ellos. Para este tipo de planes debe existir un indicador, es decir, una medida que indique cuándo debe ponerse en práctica el plan propuesto.
    - Transferencia: esta estrategia se basa en traspasar la gestión del riesgo a una entidad que asumirá su control con un determinado coste asociado.
    - Para los riesgos que no superan el apetito de riesgo la estrategia general que se aplica, de manera implícita, es asumir el riesgo; es decir, no establecer ninguna medida de tratamiento y, si se materializa, asumir las consecuencias que tenga asociadas.

- Seguimiento y control: deben reanalizarse la probabilidad y el impacto de cada uno de los riesgos de forma periódica. En este caso, se revisará la lista

con una frecuencia semanal, comprobando si se producen cambios en la probabilidad o el impacto de alguno de los riesgos, o si se ha alcanzado (o está a punto de alcanzarse) algún indicador de los planes de contingencia.

2.2.2. Identificación de riesgos

Tras el proceso de identificación de riesgos mediante brainstorming y revisión de listas de control, se obtiene la lista de riesgos. Este conjunto de riesgos se incluye en la hoja 'Lista Riesgos' del documento Excel de análisis de riesgos, tipificados y categorizados como se indica en la Tabla 2.4:

Identificador	Riesgo	Tipo de impacto	Categoría
R001	Cancelación del proyecto	Proyecto / Producto / Negocio	Organizacional
R002	No finalizar el proyecto antes de la fecha de entrega	Proyecto	Estimación
R003	Retrasos en el cumplimiento de los hitos planificados	Proyecto	Estimación
R004	Planificación temporal no realista del proyecto	Proyecto	Estimación
R005	Ausencia de control de versiones	Proyecto / Producto	Organizacional
R006	Pérdida de información	Proyecto	Organizacional
R007	Virus informático	Proyecto	Tecnología
R008	Análisis incorrecto de requisitos	Producto	Requisitos
R009	Pérdida del suministro eléctrico	Proyecto / Negocio	Organizacional
R010	Incendio	Proyecto / Negocio	Organizacional
R011	Calidad del trabajo insuficiente	Producto	Personal
R012	Hurto	Proyecto / Negocio	Organizacional
R013	Imposibilidad de concretar reuniones con involucrados	Proyecto	Organizacional
R014	Enfermedad	Proyecto	Personal
R015	Sistema no alineado con la norma a certificar	Producto	Requisitos
R016	Baja motivación del personal	Proyecto	Personal
R017	Retrasos en tareas dependientes por efecto cascada	Proyecto	Estimación

Tabla 2.4: Identificación de los riesgos del TFG

2.2.3. Análisis de riesgos

En la hoja *Análisis de Riesgos* se describen los riesgos identificados, asignando la probabilidad e impacto correspondientes y obteniendo el nivel de riesgo al que está expuesto el proyecto. En la columna de *Análisis* se justifican los valores asignados. Los detalles de este análisis se muestran en la Tabla 2.5:

Identificador	Descripción	Probabilidad	Impacto	Nivel de riesgo	Análisis
R001	El proyecto se cancela, es decir, no se desarrollará el TFG.	1	4	4	Dado que el TFG se inicia pocos días antes de que el anteproyecto sea aprobado y que la propuesta está supervisada por tutores académicos con experiencia sobre los requisitos mínimos de este tipo de proyectos, es poco probable que la propuesta no sea aprobada. Por otra parte, también es poco probable que alguna de las partes interesadas (estudiante que desarrolla el TFG y la empresa colaboradora, en este caso) cancele el desarrollo del proyecto. Si se produce la cancelación el impacto sería catastrófico porque implica la no realización del TFG.
R002	El proyecto no se finaliza antes de la fecha de entrega, por tanto, el TFG no se presenta en la convocatoria prevista.	3	4	12	Aunque se realiza una planificación inicial de los objetivos temporales que deben cumplirse, existen múltiples factores que pueden condicionar el logro de dichos objetivos, por tanto, la probabilidad de ocurrencia es considerable. El impacto sería catastrófico porque no se cumple el objetivo final de entrega del proyecto.
R003	No se logran los hitos planificados en el Gantt en las fechas estimadas, provocando retrasos en el desarrollo del proyecto que pueden llegar a causar que no se finalice a tiempo	3	3	9	La planificación estimada del proyecto se realiza al inicio de éste y existen numerosos factores que pueden condicionarla. La probabilidad de ocurrencia es mayor que el riesgo 'R002', ya que está referido a objetivos muy a corto plazo, en los que es más complicado compensar retrasos. Sin embargo, el impacto es menor: no lograr un hito planificado implicará un sobreesfuerzo posterior, pero no necesariamente desencadena la no finalización del proyecto en la fecha esperada.

R004	La planificación elaborada para el proyecto no se ajusta a la realidad, derivando en una infraestimación o sobreestimación, que impedirá lograr los objetivos del proyecto o que causará sobrecostes.	1	3	3	Dado que la empresa colaboradora en la realización del TFG tiene una amplia experiencia en el desarrollo de este tipo de proyectos, la probabilidad de realizar una estimación no realista es mínima. El impacto si sería alto; en el peor de los casos podría causar la no finalización del proyecto a tiempo.
R005	Para el desarrollo del TFG es necesario generar múltiples versiones de los distintos documentos intermedios o entregables, si éstas no se generan correctamente puede llegar a perderse información o avanzar en el proyecto usando como entrada información no válida.	3	3	9	Este tipo de proyecto implica la generación de múltiples documentos que sufren una actualización constante, por tanto, la probabilidad de que se produzcan conflictos de versiones es alta. El impacto, a su vez, también será considerable por la provocación de errores en el desarrollo.
R006	Se pierde información interna del proyecto o cualquier otro tipo de información que se utilice para el desarrollo de éste.	3	3	9	La probabilidad de perder información es alta debido al número de documentos generados y a que éstos son compartidos por las distintas partes involucradas. El impacto es alto: pueden perderse fuentes de información necesarias o ser necesario reelaborar trabajos ya finalizados.
R007	El ordenador en que se desarrolla el TFG sufre los efectos de un virus, causando la pérdida, corrupción, destrucción o sustracción de datos relativos al proyecto.	1	3	3	Dado que se utiliza Dropbox para la gestión documental, la pérdida de información por virus no tiene una probabilidad considerable. El impacto asociado a la pérdida de información es alto: pueden perderse documentos necesarios para el proyecto o ser necesario reelaborar trabajos ya finalizados.

R008	El análisis incorrecto de requisitos generará errores en el proyecto, provocando que el producto resultante no se ajuste a las especificaciones iniciales.	1	4	4	Dado que los requisitos vienen definidos y especificados por las normas ISO, se considera que un análisis incorrecto es poco probable. Por otro lado, la empresa colaboradora en la realización del proyecto tiene una amplia experiencia en este tipo de proyectos, lo que reduce todavía más la probabilidad de ocurrencia del riesgo ya que el análisis de requisitos es supervisado por ellos. El impacto sería 'Catastrófico' ya que no se desarrolla el proyecto planificado.
R009	Sin electricidad no hay acceso a la información del TFG ni se dispone de un equipo en el que avanzar en su desarrollo, las tareas que podrían realizarse son muy limitadas.	1	4	4	Los cortes eléctricos, aunque tienen un impacto catastrófico son poco habituales y cortos en el tiempo, por tanto, un corte de unas horas no afecta al proyecto.
R010	Un incendio provocaría la pérdida del ordenador en el que se desarrolla el TFG.	1	3	3	La probabilidad de que ocurra un incendio es muy baja, considerando además que se trabaja con un portátil (no existe una ubicación fija y constante). El impacto no sería relevante a nivel de pérdida de información, ya que se almacena todo en Dropbox, pero si a nivel de costes, ya que sería necesaria la adquisición de un nuevo equipo.
R011	Las tareas realizadas no cumplen las expectativas o requisitos mínimos establecidos para su validez.	1	4	4	La ocurrencia del riesgo es muy poco probable ya que el TFG es supervisado de manera continua por los tutores y se realizan las correcciones pertinentes. De materializarse, el riesgo tiene un impacto crítico ya que compromete el éxito del proyecto.
R012	Robo de información física del TFG.	1	1	1	La probabilidad de ocurrencia es muy baja: el acceso a la oficina (ubicación principal donde se desarrolla el proyecto) es limitado y controlado. Por otro lado, no tendría impacto porque toda la información está en formato digital.

R013	Indisponibilidad continua del personal involucrado en reuniones necesarias para el desarrollo de ciertas actividades del TFG.	2	4	8	Para el desarrollo del sistema planteado como objetivo del TFG es necesario mantener una serie de reuniones con personal de la empresa, la probabilidad de indisponibilidad sería considerable en períodos muy concretos, pero no con carácter continuo. El impacto de una indisponibilidad continua sí sería catastrófico ya que no se obtendría la información de entrada necesaria para el desarrollo del proyecto.
R014	Las personas involucradas en el desarrollo del TFG no pueden avanzar en éste por motivos de salud.	2	2	4	Se considera que las enfermedades más probables (gripe, por ejemplo) tienen una duración bastante corta y normalmente generan efectos negativos en la productividad pero no una indisponibilidad total del afectado, por tanto, el impacto en los avances del proyecto es asumible. Teniendo en cuenta las condiciones iniciales de los recursos, no se consideran enfermedades prolongadas o muy graves, debido a su mínima probabilidad.
R015	El sistema que se desarrolla no cumple el propósito básico del TFG de "implementación de un sistema alineado con ISO 22301".	1	4	4	Este riesgo es muy poco probable porque el TFG está supervisado en todas sus fases, garantizando su cumplimiento con la norma. El impacto sería crítico porque el TFG desarrollado no tendría validez.
R016	Baja motivación de los recursos humanos participantes en el desarrollo del TFG, provocando un descenso de la productividad, errores en las tareas realizadas,..	2	3	6	Este riesgo tiene una probabilidad media, ya que el proyecto se extiende durante varios meses y el número de personas involucradas es muy reducido, factores que pueden fomentar el estrés o la baja motivación. El impacto es alto, el éxito del proyecto tiene una dependencia total de que las tareas se realicen correctamente y, con este tipo de condicionantes, la calidad de las tareas realizadas resulta muy perjudicada.

R017	Una tarea que se retrase provocará a su vez un retraso sobre la lista de tareas que dependen de ella.	2	3	6	Existen determinadas tareas iniciales del TFG que condicionan su avance, ya que son necesarias para poder llevar a cabo las subsiguientes, por tanto, el impacto es alto porque están condicionando el desarrollo del proyecto. Dado que son actividades que se deben realizar al inicio del proyecto, la probabilidad de que se retrasen es considerable (personas involucradas que no están disponibles, avance en la tarea muy lento por falta de conocimiento,...).

Tabla 2.5: Tabla de análisis de los riesgos del TFG

2.2.4. Planificación de respuestas

Aquellos riesgos con un nivel de riesgo inferior a 6 se asumirán, por tanto, sus valores de probabilidad e impacto se mantendrán constantes; los demás tendrán una estrategia específica enfocada a la reducción del nivel del riesgo. Todas las estrategias deben ser justificadas de manera apropiada. Los resultados se muestran en la Tabla 2.6:

Identificador	Estrategia	Indicador (si aplica)	Descripción estrategia	Probabilidad residual	Impacto residual	Nivel de riesgo residual
R001	Asumir		Tal y como se ha definido en la metodología de análisis de riesgos de este proyecto, como el nivel de riesgo es menor al apetito de riesgo establecido, no se llevarán a cabo medidas de reducción de probabilidad o impacto.	1	4	4
R002	Prevención		Existe un procedimiento de seguimiento interno del proyecto, que permite tener una visión objetiva del avance realizado respecto al tiempo, identificando escenarios de retraso y tomando acciones correctivas que reduzcan la probabilidad de materialización de este riesgo.	1	4	4

R003	Plan de Contingencia	No se cumplen los plazos estimados con una desviación máxima de 1 semana.	Si no se cumplen hitos del proyecto será necesario realizar un reajuste en la planificación que permita compensar el desajuste producido lo antes posible, de manera que éste impacte mínimamente en el resto del proyecto.	3	2	6
R004	Asumir		Tal y como se ha definido en la metodología de análisis de riesgos de este proyecto, como el nivel de riesgo es menor al apetito de riesgo establecido, no se llevarán a cabo medidas de reducción de probabilidad o impacto.	1	3	3
R005	Prevención		Se utiliza un sistema de gestión documental compartido montado en Dropbox, que ofrece una serie de funcionalidades que permiten realizar una correcta administración de las distintas versiones y evitar pérdidas de información.	1	3	3
R006	Prevención		Al utilizarse Dropbox, se crea un lugar de almacenamiento compartido para todas las partes y que además es independiente de cualquier equipo. Además, Dropbox incorpora funcionalidades para recuperar documentos que hayan sido borrados, por tanto, la probabilidad de pérdida se reduce considerablemente.	1	3	3
R007	Asumir		La probabilidad inicial ya se ve reducida por el uso de Dropbox como medida preventiva para el tratamiento del riesgo 'R006'. Tal y como se ha definido en la metodología de análisis de riesgos de este proyecto, como el nivel de riesgo es menor al apetito de riesgo establecido, no se llevarán a cabo medidas de reducción de probabilidad o impacto.	1	3	3

R008	Asumir		Tal y como se ha definido en la metodología de análisis de riesgos de este proyecto, como el nivel de riesgo es menor al apetito de riesgo establecido, no se llevarán a cabo medidas de reducción de probabilidad o impacto.	1	4	0
R009	Asumir		Tal y como se ha definido en la metodología de análisis de riesgos de este proyecto, como el nivel de riesgo es menor al apetito de riesgo establecido, no se llevarán a cabo medidas de reducción de probabilidad o impacto.	1	4	4
R010	Asumir		Tal y como se ha definido en la metodología de análisis de riesgos de este proyecto, como el nivel de riesgo es menor al apetito de riesgo establecido, no se llevarán a cabo medidas de reducción de probabilidad o impacto.	1	3	3
R011	Asumir		Tal y como se ha definido en la metodología de análisis de riesgos de este proyecto, como el nivel de riesgo es menor al apetito de riesgo establecido, no se llevarán a cabo medidas de reducción de probabilidad o impacto.	1	4	4
R012	Asumir		Tal y como se ha definido en la metodología de análisis de riesgos de este proyecto, como el nivel de riesgo es menor al apetito de riesgo establecido, no se llevarán a cabo medidas de reducción de probabilidad o impacto.	1	1	1

R013	Prevención		Se notificará a los involucrados las distintas reuniones con suficiente antelación y con un horario flexible.	1	4	4
R014	Asumir		Tal y como se ha definido en la metodología de análisis de riesgos de este proyecto, como el nivel de riesgo es menor al apetito de riesgo establecido, no se llevarán a cabo medidas de reducción de probabilidad o impacto.	2	2	4
R015	Asumir		Tal y como se ha definido en la metodología de análisis de riesgos de este proyecto, como el nivel de riesgo es menor al apetito de riesgo establecido, no se llevarán a cabo medidas de reducción de probabilidad o impacto.	1	4	4
R016	Prevención		Para reducir la probabilidad de ocurrencia del riesgo se hará una revisión quincenal, que tendrá como objetivo mostrar los avances realizados en el TFG, evitando que las personas involucradas tengan una sensación de estancamiento.	1	3	3
R017	Minimización		La estrategia aplicada será la identificación inmediata de tareas clave al inicio del proyecto, de forma que éstas se prioricen. Además se dedicará especial esfuerzo a estudiar estas tareas básicas para asegurar que se evitan consecuencias negativas que se puedan propagar en cascada sobre el resto del proyecto. De esta forma se minimiza el impacto que puedan causar posibles retrasos sobre actividades clave.	2	2	4

Tabla 2.6: Planificación de respuestas a los riesgos del TFG

2.2.5. Seguimiento y control de riesgos

Todos los cambios realizados sobre el documento de análisis de riesgos deben registrarse en la hoja *Cambios en AR*. El proceso de gestión de cambios se detalla en el apartado 2.5.3.

2.3. Gestión Temporal

La gestión temporal tiene como objetivo establecer la planificación asociada a un proyecto, estimando recursos (personales, temporales y económicos) y estableciendo hitos. Permite tener una cierta visibilidad de cómo será el desarrollo del proyecto en relación con el tiempo y realizar un seguimiento objetivo sobre los avances que se llevan a cabo.

2.3.1. Ciclo de vida del proyecto

El ciclo de vida planteado para el desarrollo del proyecto se estructura en un assessment inicial, un ciclo de mejora continua y una auditoría interna. Tanto el assessment como la auditoría tienen como objetivo controlar la evolución de la implementación del sistema. En la Figura 2.4 se encuentra representado el ciclo de vida propuesto:

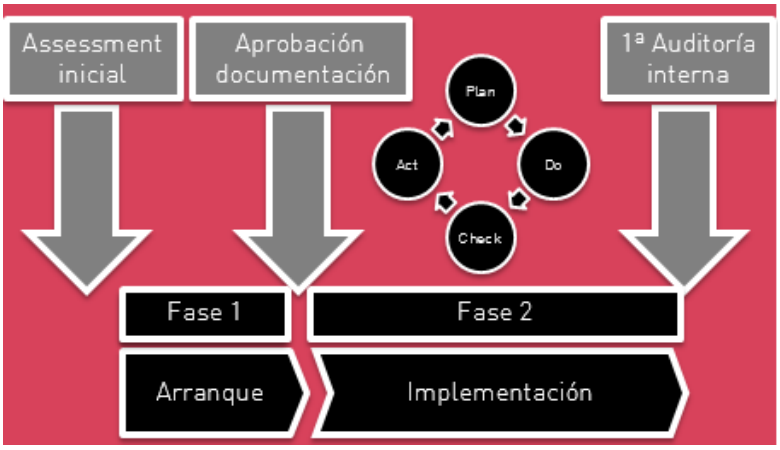

Figura 2.4: Ciclo de vida del proyecto

Tal y como se muestra en el diagrama anterior los proyectos de este tipo comienzan siempre con un assessment inicial, que permite:

- Establecer el punto de partida.

- Dotar a los consultores del proyecto de un conocimiento completo de la organización en los aspectos relacionados con el SGCN.
- Definir un punto de comparación para controles futuros.

Una vez realizado el assessment, comienza la implantación del SGCN siguiendo el ciclo de Deming (también conocido como ciclo PDCA), que constituye la base de la norma ISO 22301. Este modelo permite *planificar, establecer, implantar, operar, supervisar, revisar, mantener y mejorar de manera continua la eficacia del SGCN* [1]. El uso de este paradigma supone, además, que el SGCN se integre fácilmente con otros sistemas de gestión ISO, como: ISO 9000, para Sistemas de Gestión de Calidad; ISO 27001, para Sistemas de Seguridad de la Información o ISO 20000, para la gestión de servicios. En el Capítulo 3 se especifica la estructura de la norma en relación al ciclo de vida definido.

La auditoría interna se realiza una vez que el sistema esté implementado y operando. Tiene como objetivo evaluar el sistema de gestión, identificando las no conformidades, observaciones u oportunidades de mejor pertinentes. Los resultados de la auditoría sirven como entrada a un nuevo ciclo PDCA de mejora continua, que se basará en la elaboración e implementación de acciones correctivas y la explotación de oportunidades de mejora, garantizando el mantenimiento y mejora del SGCN. No obstante, esta fase se excede al alcance de este proyecto, por tanto, no será detallada.

2.3.2. Diagrama de Gantt

Para la planificación del proyecto se considera un esfuerzo diario de 5 horas. Se añaden como recursos la jefa de proyecto (Uxía Fernández; en adelante, UFG) y la desarrolladora (Lidia Sánchez; en adelante, LSG). El desglose de tareas del diagrama de Gantt elaborado se muestra en la Figura 2.5:

Nombre	Duracion
Inicio del Proyecto	**80 days**
Gestión del Proyecto	**80 days**
Elaborar Planificación	0,4 days
Crear Repositorio Documental	0,4 days
Realizar Análisis de Riesgos	3 days
Determinar Alcance	0,4 days
Estimar Costes	0,8 days
Elaborar Memoria	8 days
Fin Gestión del Proyecto	0 days
Planificación	**10 days**
Creación de plantillas	0,6 days
Contextualización de la Organización	2 days
Análisis del sistema y alcance	3,5 days
Elaborar Manual de SGCN	4,6 days
Elaborar Planes de Formación y Concienciación	2 days
Fin Planificación	0 days
Implementación	**62 days**
Elaboración de BIA	15 days
Revisión BIA	1 day
Realización de Análisis de Riesgos	8 days
Definición de Estrategia de Continuidad de Negocio	5 days
Identificación de Medidas de Protección y Mitigación	5 days
Elaboración de Plan y Procedimientos de Continuidad	18 days
Elaboración de Plan de Comunicación	5 days
Realización de Plan de Ejercicios y pruebas	5 days
Fin Implementación	0 days
Monitorización y Revisión	**4,3 days**
Monitorización, Medida y Análisis	3 days
Auditoría interna	2,5 days
Fin Monitorización y Revisión	0 days
Mejoras	**7,5 days**
Determinación de Acciones Correctivas	7,5 days
Fin Mejoras	0 days
Fin Proyecto	0 days

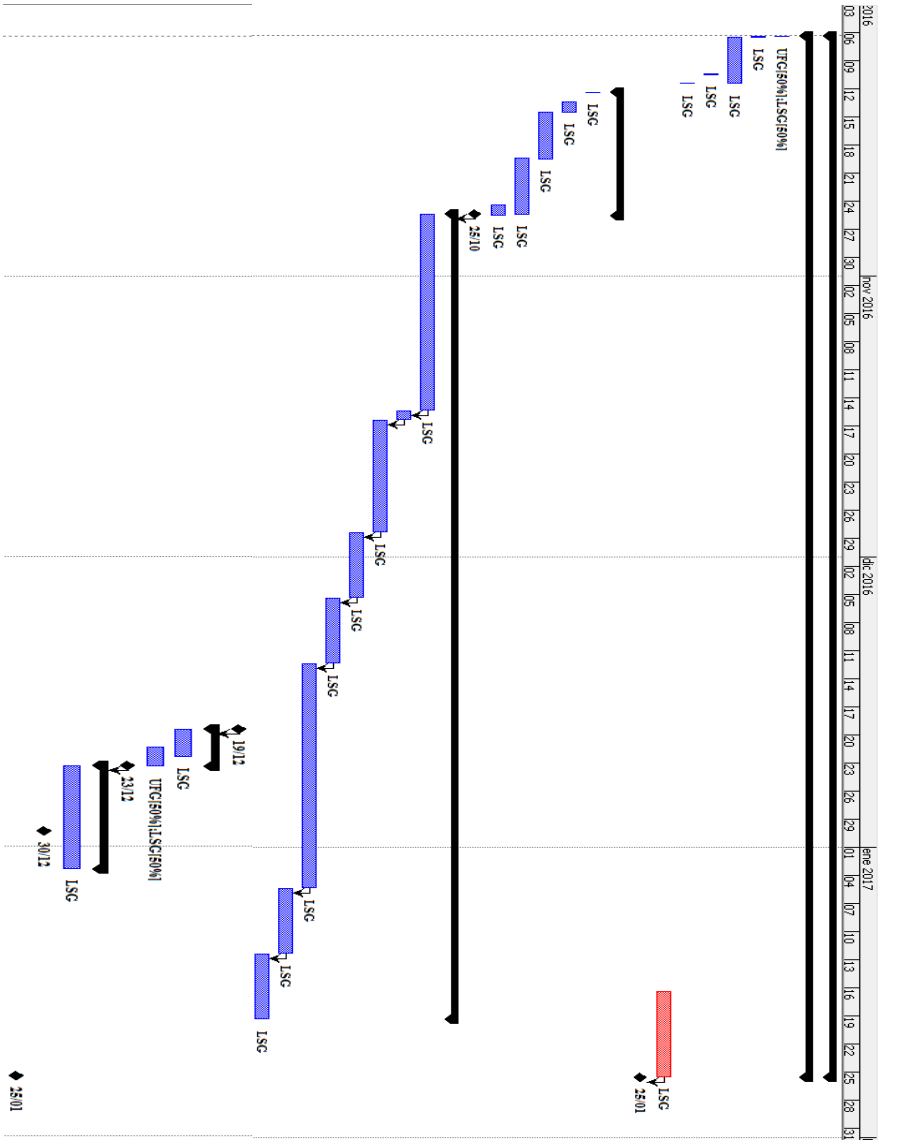

Figura 2.5: Diagrama de Gantt del proyecto

Como se observa en el diagrama, el BIA es una tarea condicionante para avanzar en el proyecto, ya que será la que proporcione información sobre qué servicios deberán incluirse en el SGCN y los riesgos a los que éstos están expuestos. Dichos riesgos serán analizados posteriormente, tarea que también será necesaria para continuar la fase de implementación.

Implícitamente, la fase de implementación será necesaria para poder comenzar la fase de monitorización y revisión.

2.4. Gestión de Costes

La gestión de costes incluye las estimaciones sobre el coste económico asociado al proyecto. El presupuesto elaborado debe contemplar todos los recursos necesarios para la realización de las actividades calendarizadas.

El proyecto presentado en este caso, por pertenecer al ámbito de la gestión, no tiene costes asociados a software o hardware específicos que requieran de su adquisición.

Los costes asociados se dividirán, por tanto, en los siguientes grupos:

- Personales: aquellos costes asociados a los recursos humanos, cuantificados en horas/hombre y tarifados según el perfil profesional del recurso involucrado.
- Materiales: aquellos costes que incluyen recursos físicos necesarios para el desarrollo del proyecto.
- Licencias: costes asociados a la adquisición de licencias de software y normas utilizadas en el proyecto.

2.4.1. Costes personales

Para el desarrollo de este proyecto las personas involucradas de forma directa son las especificadas en la Tabla 2.7. El coste/hora se corresponde con el coste utilizado en la empresa para el desarrollo de proyectos e incluye los costes de Seguridad Social y costes indirectos:

Recurso	Rol	Coste/hora	Horas dedicadas	Coste total
UFG	Jefa de proyecto	60 €	82	4920 €
LSG	Desarrolladora	15 €	415	6225 €
TOTAL				11145 €

Tabla 2.7: Costes personales incurridos al proyecto

Adicionalmente, también se tendrán en cuenta los costes asociados a personas de la empresa involucradas en reuniones necesarias para llevar a cabo determinadas tareas del proyecto y que se detallan en la Tabla 2.8:

Rol	Coste/hora	Horas dedicadas	Coste total
Responsable de Control de Proyectos	40	12	480 €
Directora Financiera	60	8	480 €
Responsable de SSII	45	18	810 €
Responsable de gestión de servicios	60	8	480 €
TOTAL			2250 €

Tabla 2.8: Costes de personal involucrado incurridos al proyecto

El coste de los recursos humanos en el proyecto se corresponde con un total de 13395 €.

2.4.2. Costes materiales

Por las características del proyecto, los costes materiales son reducidos y, como ya se ha mencionado anteriormente, no involucran hardware o software específico, siendo necesario únicamente un ordenador. Para calcular el coste asociado a este recurso se emplea la siguiente fórmula:

$$Coste = \frac{(Valor\ real - Valor\ residual)}{Vida\ útil} * \frac{Horas\ dedicadas}{Horas\ totales}$$

Donde:

- Valor real: coste original del ordenador.
- Valor residual: coste del ordenador en el mercado actual.
- Vida útil: número de años que se estima que el ordenador podrá cumplir correctamente con su función.
- Horas dedicadas: número de horas durante las que se ha utilizado el ordenador para el desarrollo del proyecto.
- Horas totales: número de horas que el ordenador está funcionando durante todo el año. (Considerando una media de 5 horas diarias de uso)

$$Coste = \frac{(800 - 250)}{4} * \frac{415}{(5 * 365)} = 31.63\ €$$

2.4.3. Costes de licencias

Los costes principales imputados en esta categoría se corresponden con la adquisición de las normas ISO utilizadas como base para el desarrollo de este proyecto y se especifican en la Tabla 2.9:

Norma	Coste
ISO 22301:2012	109.92€
ISO 27031:2011	147.19€
TOTAL	257.11€

Tabla 2.9: Costes de licencias incurridos al proyecto

2.4.4. Coste total del proyecto

Teniendo en cuenta los costes de todos los recursos involucrados en el proyecto, el presupuesto total que se estima se muestra en la Tabla 2.10:

Recursos	Coste
Personales	13395 €
Materiales	31.63 €
Licencias	257.11€
TOTAL	13683.74 €

Tabla 2.10: Coste total del proyecto

2.5. Gestión de la Configuración

El proceso de gestión de la configuración tiene como objetivos la gestión de cambios y versiones realizados durante todo el ciclo de vida del proyecto, garantizando que se trabaja sobre una versión estable y coherente.

2.5.1. Identificación de elementos de configuración

Se considera como elemento de configuración (en adelante, CI), cualquier documento generado para el desarrollo del proyecto, así como la propia documentación que se emplea para éste, ya sean estándares y documentos oficiales, o documentos internos de la empresa.

Los documentos generados para el desarrollo del proyecto podrán ser de tres tipos:

- Plantillas: modelos que sirven de base para la generación de documentos de desarrollo del sistema. Al ser recursos de uso genérico podrán generarse en varios idiomas, con el objetivo de poder ser utilizados en proyectos de la empresa para clientes de distintas localizaciones.
- Documentos internos: ficheros generados con contenidos necesarios para llevar a cabo el desarrollo del sistema.
- Actas de reunión: documentos generados con el objetivo de reflejar las conclusiones o decisiones llevadas a cabo durante encuentros entre personas involucradas en el proyecto y que tienen alguna repercusión en éste.

Los CIs siguen una nomenclatura general, que se define en la Tabla 2.11:

Tipo de CI	Nomenclatura
Plantilla	Tipo de Documento_SGCN_LG.extensión Donde: • **LG** es el idioma de la plantilla: ES (español), PT (portugués), EN (inglés).
Documento interno	Ozona_Tipo de Documento_SGCN_vX.Y.extensión Donde: • **Tipo de Documento** es el nombre identificativo del contenido que se encuentra en el archivo, por ejemplo: Manual, Plan de Comunicación,… • **vX.Y** es la versión del documento, por ejemplo, la primera versión será: v1.0
Acta de reunión	Ozona_Fecha_Acta Reunión_SGCN.extensión Donde: • **Fecha** indica la fecha en que se lleva a cabo la reunión, con el formato: ddMMyy (dd: día, mm: mes, yy: año). Por ejemplo, una reunión realizada el 5 de noviembre de 2016 se indicará como: 051116.
Documentación	No se asigna una nomenclatura a este tipo de documentos, sino que se mantiene su nombre original. Son ficheros estables que proceden de otras fuentes (externas o internas de la propia empresa).

Tabla 2.11: Nomenclatura de documentos en el sistema de gestión documental

2.5.2. Gestión documental

Toda la información del proyecto se gestiona mediante un sistema documental organizado en carpetas y albergado en el servicio de almacenamiento proporcionado por Dropbox.

La estructura de carpetas creada es de acceso compartido para los recursos involucrados de forma directa en el proyecto (especificados en la Gestión de Costes), y pretende ser intuitiva y está mapeada con las distintas cláusulas de la norma ISO 22301. A continuación se muestran: un diagrama de la estructura completa del sistema documental (Figura 2.6), una imagen de la estructura básica (primer nivel) del sistema (Figura 2.7) y una tabla detallada sobre el contenido de cada carpeta (Tabla 2.12):

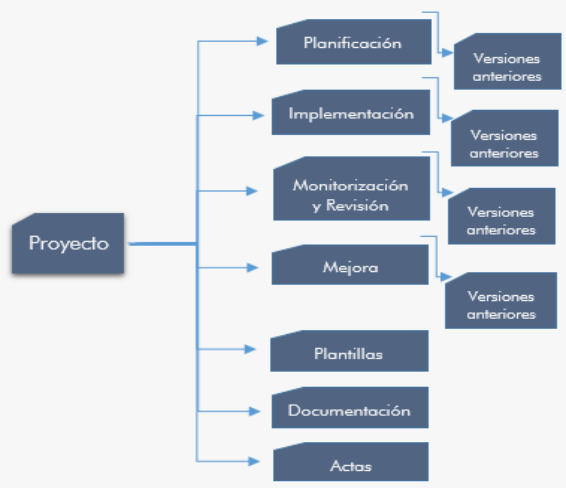

Figura 2.6: Estructura del sistema documental del proyecto

Como se ve en el diagrama, el sistema tiene una profundidad máxima de dos niveles e incluye, para las carpetas de documentos internos, una distribución específica para la gestión de las versiones.
Las carpetas de documentos internos son: Planificación, Implementación, Monitorización y Revisión y Mejora. Contienen, por tanto, los documentos generados durante el desarrollo del proyecto y que se requieren para la implantación del sistema de gestión de continuidad. Tendrán, por tanto, un mapeo directo con las cláusulas de la ISO 22301.

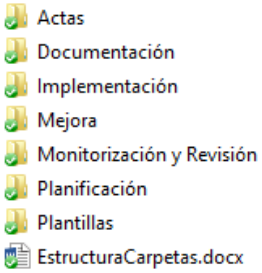

Figura 2.7: Primer nivel del sistema documental del proyecto

La imagen previa muestra, por tanto, el primer nivel del sistema documental. Incluye un documento *EstructuraCarpetas.docx*, cuyo objetivo es explicar de manera detallada la nomenclatura de documentos, la distribución de éstos en las distintas

carpetas y el mapeo de cada carpeta con las cláusulas de la ISO 22301[1], de manera que cualquier posible usuario que posteriormente a la finalización del proyecto necesite actualizar o consultar los documentos asociados al sistema de gestión de continuidad, tenga el conocimiento necesario para acceder fácilmente a la información necesaria.

Carpeta	Contenido	Cláusula asociada
Planificación	Incluye todos los documentos asociados con el contexto de la organización, las políticas y responsabilidades definidas para el sistema a implantar, la planificación de la implantación del sistema y el soporte, que incluye: recursos, planes de concienciación y comunicación y procedimientos de gestión documental.	Cláusula 4: Contexto de la Organización Cláusula 5: Liderazgo Cláusula 6: Planificación Cláusula 7: Soporte
Implementación	Incluye todos los documentos asociados a la operación del sistema: análisis de impacto en el negocio, análisis de riesgos, elaboración de estrategias, procedimientos y planes de continuidad.	Cláusula 8: Operación
Monitorización y Revisión	Incluye todos los documentos asociados a la evaluación del rendimiento: supervisión, medición, análisis y auditorías internas.	Cláusula 9: Evaluación de la ejecución
Mejora	Incluye los documentos asociados a la identificación de no conformidades y elaboración de acciones correctivas.	Cláusula 10: Mejora
Versiones anteriores	Contiene todas las versiones previas no finales de un documento, que no tienen validez actual, pero que pueden ser necesarias para el restablecimiento de versiones estables tras cambios no exitosos o como fuentes de información.	N/A
Actas	Incluye todos los documentos generados en las reuniones cuyos objetivos a tratar tengan relación con el sistema que se está desarrollando.	N/A
Documentación	Ficheros adicionales que puedan o hayan sido usados en algún momento para el desarrollo del proyecto pero que no pertenecen al mismo, es decir, no se generan durante el ciclo de vida del proyecto.	N/A
Plantillas	Incluye todas las plantillas que se usan para el desarrollo del proyecto.	N/A

Tabla 2.12: Especificación del contenido de carpetas del sistema de gestión documental del proyecto

2.5.3. Gestión de cambios y versiones

La gestión de cambios establece los procedimientos formales para la planificación, realización y supervisión de los cambios que deben realizarse. La gestión de

[1] La norma ISO 22301 está descrita en el apartado 3.1.3. de este documento.

versiones, por su parte, supervisa los cambios realizados, asegurando la integridad y validez de los CIs de la línea base.

Para este proyecto, el proceso de gestión de cambios es simple y se incluye como histórico en el propio CI, mediante una tabla de control de cambios como la que se muestra en la Figura 2.8:

Control de Cambios

Versión	Fecha	Autor	Descripción
1.0	*13/10/2016*	*Lidia Sánchez*	*Versión inicial del Manual del SGCN*

Figura 2.8: Tabla de control de cambios

No existe un procedimiento basado en solicitud y análisis de cambios ya que el proyecto está en desarrollo, es decir, no existe una línea base estable y liberada. Además, teniendo en cuenta las características del propio proyecto, todos los CIs están en constante actualización y los recursos implicados en su manipulación (desarrolladora o jefa de proyecto) tienen conocimiento completo sobre el estado del proyecto.
Sin embargo, por esta constante actualización, que provoca una generación de múltiples versiones de documentos, sí es necesario disponer de un control de versiones que garantice, como ya se ha mencionado previamente, la integridad y validez de los CIs.

Este control de versiones viene dado, tanto por la propia nomenclatura establecida para los documentos del sistema (especificada en el apartado Identificación de elementos de configuración), como por las funcionalidades ofrecidas por el servicio de almacenamiento de Dropbox. Estas funcionalidades comprenden, entre otras:

- Historial de versiones: permite recuperar las distintas versiones de un documento sometido a modificaciones. De esta forma, es posible restaurar una versión anterior estable de un documento tras cambios erróneos o inadecuados, cuando no se haya generado manualmente una copia del original como nueva versión.

- Recuperación de documentos eliminados: de esta forma pueden recuperarse documentos borrados por error, evitando pérdidas de información.

- Identificación de copias en conflicto: dado que a la carpeta tienen acceso y permisos de edición dos personas, ésta funcionalidad permite detectar situaciones que involucren modificaciones sobre el mismo documento al mismo tiempo, guardando automáticamente en copias diferentes los cambios realizados por cada persona. Además, el usuario puede obtener en

tiempo real la versión actualizada por el resto de usuarios con los que comparte la información.

3. Análisis

3.1. Normas ISO

3.1.1. Organización ISO

La Organización Internacional de Normalización (en adelante ISO), es una organización independiente y no-gubernamental dedicada a la creación de estándares de ámbito internacional y de carácter técnico. Dichos estándares tienen como objetivos mejorar la eficacia, seguridad y complejidad asociada al desarrollo y entrega de productos y servicios. Por otro lado, también proporcionan medidas para la protección de los clientes y usuarios, teniendo como fin la simplificación de su interacción con los productos y servicios.

La Organización ISO fundamenta su metodología en ocho principios:

- Enfoque en el cliente: las organizaciones dependen de sus consumidores, por tanto, debe existir una clara comprensión de sus necesidades actuales y futuras, así como dedicar esfuerzos a sobrepasar las propias expectativas de éstos.
- Liderazgo: personas que ejerzan el papel de líderes, estableciendo objetivos y orientando la estrategia de las organizaciones, con el objetivo de crear un ambiente interno en el que se involucre todo el personal.
- Participación del personal: el personal, como esencia de una organización, es clave para obtener los beneficios deseados. Por tanto, dicho personal debe estar plenamente involucrado en la organización, entendiendo la importancia de su contribución y su papel dentro de ella.
- Enfoque por procesos: gestionar las actividades y sus recursos relacionados como un proceso para mejorar la eficiencia en la obtención de los resultados.
- Orientar la gestión como un sistema: identificar y gestionar procesos interrelacionados como un sistema para mejorar la eficacia y eficiencia de las organizaciones en la consecución de sus objetivos.
- Mejora continua: mantener la mejora continua como un objetivo constante en las organizaciones, como mecanismo para garantizar el enriquecimiento de éstas.
- Toma de decisiones basada en hechos: utilizar los datos e información como una base de conocimiento que permita tomar decisiones eficaces fundadas en hechos.
- Relaciones de beneficio mutuo con proveedores: fomentar una relación positiva entre una organización y sus proveedores como medio para la creación común de valor.

3.1.2. Estructura de normas ISO

Todas las normas que elabora la ISO siguen una misma filosofía basada en el modelo PDCA:

- Di lo que haces
- Haz lo que dices
- Hazlo como lo dices
- Mejora

Además, estos estándares presentan una serie de características que los posicionan como los marcos estructurales más adecuados y versátiles:

- Definen la estructura: identifican los requisitos necesarios para cada sistema de gestión pero no determinan cómo deben implementarse dichos requisitos, por tanto, cada organización buscará el método de implementación que se ajuste mejor a sus necesidades.

- Necesidades mínimas: el estándar sólo recoge los requisitos mínimos para implantar un sistema de gestión, es decir, establece la base y punto de partida a partir del cual la organización elaborará su sistema concreto.

- Compatibilidad con buenas prácticas: la aplicación de un estándar no es restrictiva y permite la combinación con estándares de facto.

- Mejora continua: en el propio ciclo de vida del sistema se contempla la fase de mejora, lo que permite explotar oportunidades de mejora o adaptar al sistema a nuevas necesidades.

- Estructura común de alto nivel: entre los propios estándares ISO se define una estructura común. Dicha estructura viene especificada en el documento Anexo SL, publicado por la organización, y tiene como objetivo que todas las normas de Sistemas de Gestión ISO estén alineadas y con una mejor compatibilidad, favoreciendo a aquellas organizaciones que opten por mantener un Sistema de Gestión Integrado. Los apartados, o cláusulas, en que se organizan las normas son los siguientes:
    1. Alcance
    2. Referencias Normativas
    3. Términos y Definiciones
    4. Contexto de la Organización
    5. Liderazgo
    6. Planificación
    7. Soporte
    8. Operación
    9. Evaluación del desempeño
    10. Mejora

- Voluntarias: la adopción de estándares ISO es voluntaria. La organización ISO no regula ni legisla. No obstante, muchos de los estándares que elaboran sí han llegado a convertirse en un requisito legal impuesto por organizaciones reguladoras o gobiernos.

3.1.3. Normas ISO de Sistemas de Gestión dentro del alcance

Para el desarrollo de este proyecto se tendrán en cuenta las siguientes normas:

- ISO 22301: el estándar de gestión de continuidad de negocio. Es la norma principal que se seguirá para la implantación del SGCN. Establece los requisitos necesarios para montar un sistema que garantice la recuperación de los servicios críticos de una organización en el menor tiempo posible tras un incidente disruptivo. El contenido de las cláusulas específicas para esta norma son:
    - Cláusula 4: Contexto de la organización; incluye necesidades, requisitos y alcance del SGCN.
    - Cláusula 5: Liderazgo; incluye los requisitos específicos de la Alta Dirección en el SGCN, y cómo se organizan sus expectativas respecto a la organización por medio de la declaración de una Política.
    - Cláusula 6: Planificación; describe los requisitos en relación a los objetivos estratégicos y a los principios bajo los que se establecerá el SGCN.
    - Cláusula 7: Soporte; proporciona soporte a las operaciones del SGCN en los procesos de comunicación y competencia con las partes interesadas, y asegura el registro, control, mantenimiento y retención de la documentación requerida.
    - Cláusula 8: Operación; define los requisitos de continuidad, cómo alcanzarlos y desarrolla los procedimientos necesarios para gestionar un incidente disruptivo.
    - Cláusula 9: Evaluación del desempeño; requisitos mínimos para medir el rendimiento de la gestión de continuidad, su cumplimiento con la propia norma y con las expectativas establecidas.
    - Cláusula 10: Mejora; identificación de acciones correctivas para las no conformidades que se detecten en la fase de Evaluación del desempeño.

  En la Figura 3.1. se muestra una imagen de la relación de las cláusulas en el sistema:

Figura 3.1: Relación de las cláusulas del SGCN

Las cláusulas 4, 5 y 7 definen el entorno en que se establece el SGCN, mientras que las cláusulas 6, 8, 9 y 10 suponen el núcleo del sistema, manteniendo el ciclo PDCA en movimiento.

- ISO 22313: guía de aplicación de la ISO 22301. Proporciona recomendaciones o permisos sobre los requisitos fundamentales de la ISO 22301.

- ISO 27031: establece las directrices para la preparación de las TIC para la continuidad del negocio. Introduce el término IRBC con el objetivo de hacer énfasis en el entorno técnico completo, no sólo TI, reconociendo la importancia central de las comunicaciones, tanto de voz como de datos. Así, establece como requisito que deben ser gestionados los siguientes elementos:
    - Personas: identificando las estrategias apropiadas para mantener las habilidades y conocimiento de las TIC esenciales. Aparte de los colaboradores y empleados, también deben considerarse otros stakeholders que posean una amplia experiencia y conocimiento en TIC.

    - Instalaciones: definiendo estrategias para reducir el impacto de la falta de disponibilidad de las instalaciones normales TIC. Por tanto, se incluyen: instalaciones alternativas, lugares para trabajo remoto,…

    - Tecnología: asegurando que los servicios TIC sobre los cuales dependen las actividades críticas de negocio están disponibles antes de la reanudación de sus actividades de negocio críticas dependientes. La tecnología incluye: hardware, red y comunicaciones, y software.

- Datos e Información: diseñando soluciones de continuidad que cumplan el RPO de cada actividad de negocio crítica de la organización.
- Procesos: considerando los procesos necesarios para asegurar la viabilidad de la estrategia, que incluye los procesos necesarios para la prevención, detección, respuesta a incidentes y recuperación de desastres.

- Proveedores: identificando y documentando las dependencias externas que soportan la prestación de servicios TIC y tomando las medidas adecuadas para garantizar que el equipamiento y los servicios críticos pueden ser prestados por sus proveedores dentro de plazos predeterminados y acordados.

- ISO 22331: establece las directrices para la definición de la estrategia de negocio, evaluando los escenarios de riesgo en que se puede encontrar la organización y analizando las posibles estrategias de respuesta, de comunicación y de recuperación a aplicar ante la ocurrencia de éstos. El planteamiento que establece para la determinación y selección de estrategias se resume en el diagrama de la Figura 3.2:

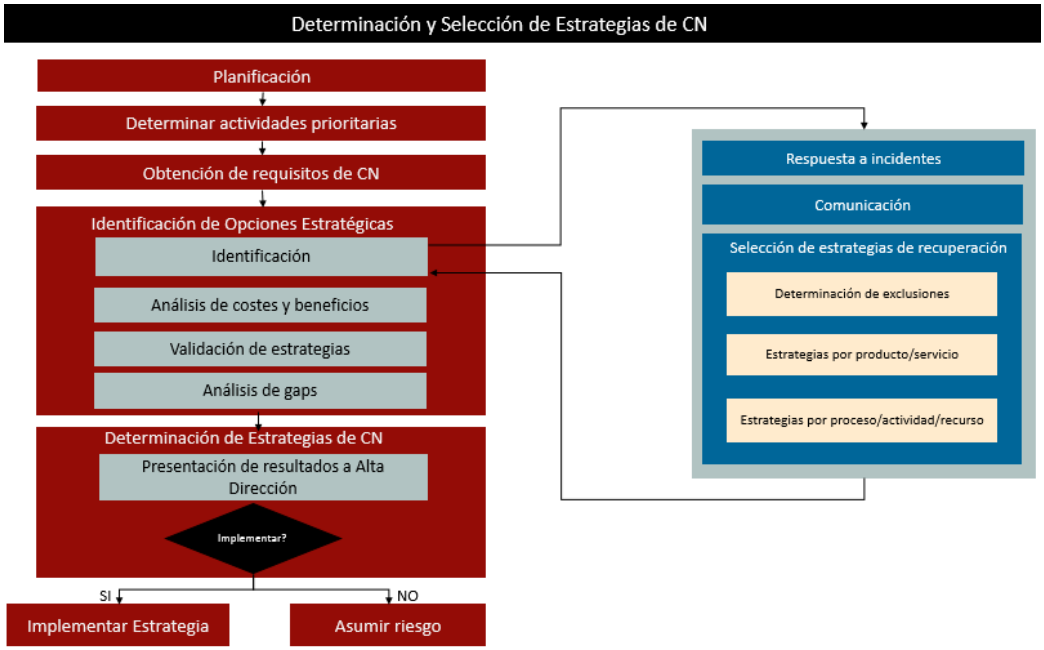

Figura 3.2: Esquema de determinación y selección de estrategias de continuidad

Otras normas relacionadas con las anteriores que serán utilizadas en momentos puntuales del desarrollo son:

- ISO 22317: establece las directrices para la realización del análisis de impacto en el negocio. Se ha utilizado como base para la metodología de realización de BIA.

- ISO 31000: estándar para el análisis de riesgos. Se ha utilizado como base en la metodología de análisis de riesgos.

3.2. Análisis de requisitos

En este apartado se presentan los requisitos que tendrá el SGCN, detallando el proceso de identificación de éstos, sus especificaciones y, por último, sus dependencias en la matriz de trazabilidad.

3.2.1. Identificación de requisitos

Como ya se ha mencionado en apartados anteriores, los requisitos del sistema, en su mayoría, vienen impuestos por los recogidos en la norma ISO 22301.

Los requisitos identificados para el sistema estarán clasificados según su categoría, funcionales o no funcionales, y su importancia. Esta distribución está condicionada por los siguientes criterios:

- Requisitos funcionales: engloba los requisitos que implican el suministro de un servicio por parte del sistema. Por ejemplo: el SGCN suministra el Plan de CN, que contiene la información necesaria para que una organización recupere la actividad normal de sus servicios críticos tras una interrupción. Su código identificativo comienza con 'RF'.

- Requisitos no funcionales: engloba los requisitos que son necesarios para el propio sistema, bien como fuentes de información o bien como productos generados para su propia gestión, pero no son un servicio directo para los usuarios del sistema. Por ejemplo: tener un procedimiento de control documental es un requisito obligado para el SGCN, impuesto por la ISO 22301, pero no es un procedimiento destinado al uso de los usuarios del sistema. Su código identificativo comienza con 'RNF'.

- Importancia alta: aquellos requisitos que suponen el núcleo de un SGCN y que establecen los procedimientos a seguir ante situaciones que puedan comprometer la continuidad de negocio.

- Importancia media: requisitos de soporte, necesarios para elaborar un SGCN adecuado a la organización, bien gestionado y monitorizado.

- Importancia baja: requisitos de cumplimiento recomendable para mejorar el rendimiento del SGCN en la organización.

En la Figura 3.3. se muestra la tabla con la lista de requisitos identificados, su código identificativo, su importancia, y las normas con las que está asociado:

Código	Requisito	Importancia	ISO 22301	ISO 27031	ISO 22317	ISO 22331	Otros
RNF1	Definir el contexto de la organización y su apetito de riesgo	Alta					
RNF2	Identificar las partes interesadas y sus requisitos y expectativas	Alta					
RNF3	Determinar el alcance del sistema	Alta					
RNF4	Realización de análisis de impacto en el negocio y análisis y tratamiento de riesgos	Alta					
RNF5	Establecimiento de los roles, responsabilidades y autoridades asociados al SGCN	Alta					
RF6	Elaboración de la Política de CN	Alta					
RNF7	Elaboración de la estrategia de CN	Alta					
RF8	Elaboración e implementación de planes para alcanzar objetivos de CN	Alta					
RF9	Elaboración de procedimientos de CN	Alta					
RF10	Establecimiento de planes de competencias, sensibilización y comunicación a recursos	Alta					
RNF11	Establecimiento de procesos de planificación y control de los requisitos del sistema	Alta					
RNF12	Establecimiento de procedimientos de creación, actualización y control de información documentada	Alta					
RF13	Elaboración de planes de ejercicios y pruebas	Alta					
RNF14	Creación de métricas de desempeño del sistema	Media					
RNF15	Implementación de procedimientos de CN	Alta					
RNF16	Monitorización del sistema	Media					
RNF17	Integración del SGCN en el Sistema Integrado de la organización	Baja					

Figura 3.3: Lista de requisitos del sistema

3.2.2. Especificación de requisitos funcionales

RF6	Elaboración de la política de CN
Descripción	
Debe elaborarse una política aprobada por la Dirección que sea apropiada a la finalidad de la organización, proporcione la estructura para el establecimiento de objetivos de CN y, por último, que incluya los compromisos formales de cumplimiento de requisitos y mejora continua del SGCN.	
Importancia	
Alta	
Criterio de validación	
Existe un documento con la política aprobado por la Dirección.	

RF8	Elaboración e implementación de planes para alcanzar objetivos de CN
Descripción	
Será necesario elaborar documentos con los pasos que se deben seguir para alcanzar los objetivos de continuidad de negocio.	
Importancia	
Alta	
Criterio de validación	
Existen planes orientados al cumplimiento de los objetivos de CN y además estos objetivos están alineados con la política previamente definida.	

RF9	Elaboración e implementación de procedimientos de CN
Descripción	
Deben documentarse procedimientos para asegurar la continuidad de las actividades y la gestión de los incidentes disruptivos. Deben incluirse las acciones inmediatas a llevar a cabo tras una interrupción.	
Importancia	
Alta	
Criterio de validación	
Existen procedimientos de actuación que contemplan los distintos escenarios de interrupción que afectan a los servicios críticos.	

RF10	Establecimiento de planes de competencias, sensibilización y comunicación a recursos
Descripción	
Será necesario establecer planes que aseguren que todos los recursos involucrados o que pueden estar afectados por el SGCN, disponen de los conocimientos necesarios, están al corriente de la situación exacta de la organización en caso de incidente disruptivo y/o comprenden la necesidad de la existencia del SGCN para la supervivencia de la organización y se involucran en su correcto funcionamiento.	
Importancia	
Alta	
Criterio de validación	
Existen planes de competencias, sensibilización y comunicación.	

RF13	Elaboración de planes de ejercicios y pruebas
Descripción	
Deberán elaborarse planes para la realización de pruebas que permitan comprobar la eficacia de las estrategias diseñadas.	
Importancia	
Alta	
Criterio de validación	
Existen planes de pruebas y alguna evidencia de informes de resultados.	

3.2.3. Especificación de requisitos no funcionales

RNF1	Definir el contexto de la organización y su apetito de riesgo
Descripción	
Debe definirse el contexto, interno y externo de la organización, que incluye los aspectos: económicos, sociales, legales,.. Así como el apetito de riesgo, es decir, establecer unos niveles de riesgo que la organización considere aceptables.	

Importancia
Alta
Criterio de validación
Existe un documento que especifica el contexto interno y externo de Ozona, así como el nivel de riesgo que se considera aceptable.

RNF2	Identificar las partes interesadas y sus requisitos y expectativas
Descripción	
Deben identificarse todos los stakeholders relacionados con los servicios contemplados en el alcance del sistema, identificando sus requisitos (qué quieren) y sus expectativas (qué esperan recibir). Los requisitos son aquellas condiciones que deben cumplirse. Por su parte, las expectativas son aspectos a tener en cuenta para una satisfacción alta del cliente.	
Importancia	
Alta	
Criterio de validación	
Existe un documento en el que se especifican las partes interesadas y sus requisitos y expectativas.	

RNF3	Determinar el alcance del sistema
Descripción	
Será necesario identificar claramente aquellos servicios que se incluirán en el alcance del SGCN y los que no, detallando en cada caso los criterios que se han seguido para concluir la decisión. Los servicios que sean categorizados como críticos tras la realización del BIA tendrán que incluirse obligatoriamente en el alcance.	
Importancia	
Alta	
Criterio de validación	
Existe un documento en el que se especifica el alcance que tendrá el sistema.	

RNF4	Realización de análisis de impacto en el negocio y análisis y tratamiento de riesgos
Descripción	
Debe realizarse un BIA que contemple todos los servicios de la organización y que permita obtener la lista de aquellos que son críticos, es decir, que tienen un impacto muy alto en la organización y que, en una situación de incidente disruptivo, su recuperación deberá realizarse lo antes posible a unos niveles mínimos aceptables para poder garantizar la viabilidad del negocio. Por otro lado deben identificarse, cuantificarse y establecerse estrategias de mitigación para todos aquellos riesgos que, en caso de materializarse, comprometerían alguno de los servicios anteriores.	
Importancia	
Alta	
Criterio de validación	
Existen documentos con el BIA y el análisis de riesgos.	

RNF5	Establecimiento de los roles, responsabilidades y autoridades asociados al SGCN
Descripción	
Será necesario identificar los roles necesarios, indicando para cada uno de ellos las responsabilidades y autoridades que tienen asociadas, asegurando que cada área del SGCN tiene un responsable nombrado formalmente y con unas competencias requeridas y apropiadas.	
Importancia	
Alta	
Criterio de validación	
Existe un documento con la descripción y asignación de los roles, responsabilidades y autoridades.	

RNF7	Elaboración de la estrategia de CN
Descripción	
Se elaborará una estrategia que garantice la máxima disponibilidad de las actividades críticas, la continuación, reanudación y recuperación de estas actividades, y la gestión de los impactos.	
Importancia	
Alta	
Criterio de validación	
Existe un documento que describe la estrategia de continuidad.	

RNF11	Establecimiento de procesos de planificación y control de los requisitos del sistema
Descripción	
Se establecerán procesos de revisión periódicos, que garanticen que el SGCN sigue cumpliendo los requisitos y detectando posibles necesidades de adaptación.	
Importancia	
Alta	
Criterio de validación	
Existe un documento en el que se describen estos procesos.	

RNF12	Establecimiento de procedimientos de creación, actualización y control de información documentada
Descripción	
Se elaborará un procedimiento formal que describa la ubicación de la información relativa al SGCN, quién tiene permiso de acceso, las medidas de seguridad para evitar la pérdida de información, cuál es el control de versiones,…	
Importancia	
Alta	
Criterio de validación	
Existe un documento con la descripción de la gestión documental para el SGCN.	

RNF14	Creación de métricas de desempeño de sistema
Descripción	
Se determinarán una serie de indicadores, cuyo objetivo será conocer el rendimiento del sistema, detectar posibles deficiencias,…	
Importancia	
Media	
Criterio de validación	
Existe un documento con la definición de los indicadores.	

RNF15	Monitorización del sistema
Descripción	
Deben establecerse procedimientos que determinen los métodos de medición, qué se va a medir, con qué frecuencia, cuándo serán analizados los resultados…	
Importancia	
Media	
Criterio de validación	
Existe un documento con la especificación de los procedimientos de monitorización.	

RNF16	Integración del SGCN en el Sistema Integrado de la organización
Descripción	
En la organización se encuentran implementados el Sistema de Gestión de Servicios ISO 20000 y el Sistema de Gestión de Seguridad de la Información ISO 27001. Por tanto, deberá implementarse el SGCN de manera que todos los sistemas tengan una operativa coherente que permita la consecución de los objetivos y misión del negocio.	
Importancia	
Baja	
Criterio de validación	
Se contempla la existencia del SGCN en el documento del Sistema Integrado.	

3.2.4. Matriz de trazabilidad

En la Figura 3.4 se muestra la matriz de trazabilidad de los requisitos del sistema. En cada una de las filas se indican cuáles son las dependencias de cada requisito:

	RNF1	RNF2	RNF3	RNF4	RNF5	RF6	RNF7	RF8	RF9	RF10	RNF11	RNF12	RF13	RNF14	RNF15	RNF16
RNF1																
RNF2	↑															
RNF3							↑									
RNF4	↑	↑	↑													
RNF5				↑												
RF6												↑				
RNF7				↑												
RF8												↑				
RF9	↑															
RF10				↑								↑				
RNF11			↑	↑												
RNF12																
RF13				↑				↑				↑				
RNF14												↑				
RNF15														↑		
RNF16																

Figura 3.4: Matriz de trazabilidad de los requisitos

3.3. Casos de uso

Para el proyecto que se presenta, y teniendo en cuenta los requisitos del sistema, la diagramación mediante casos de uso no resulta aplicable.

A pesar de esto, y por mantener una analogía con otro tipo de proyectos de desarrollo de software, se intentará modelar con la herramienta UML de casos de uso el asociado al Plan de Continuidad, considerando éste como el producto directo del sistema para sus usuarios. El diagrama se muestra en la Figura 3.5. Para este caso, habría tres actores: usuario general del sistema, responsable de continuidad y Alta Dirección. El responsable de continuidad debe elaborar el Plan de Continuidad, que incluirá a su vez el Plan de Recuperación (DRP) y el Plan de Contingencia de Pandemias. Estos planes serán revisados por la Alta Dirección. Por último, cualquier usuario del SGCN, en caso de emergencia, podrá ejecutar el Plan de Continuidad:

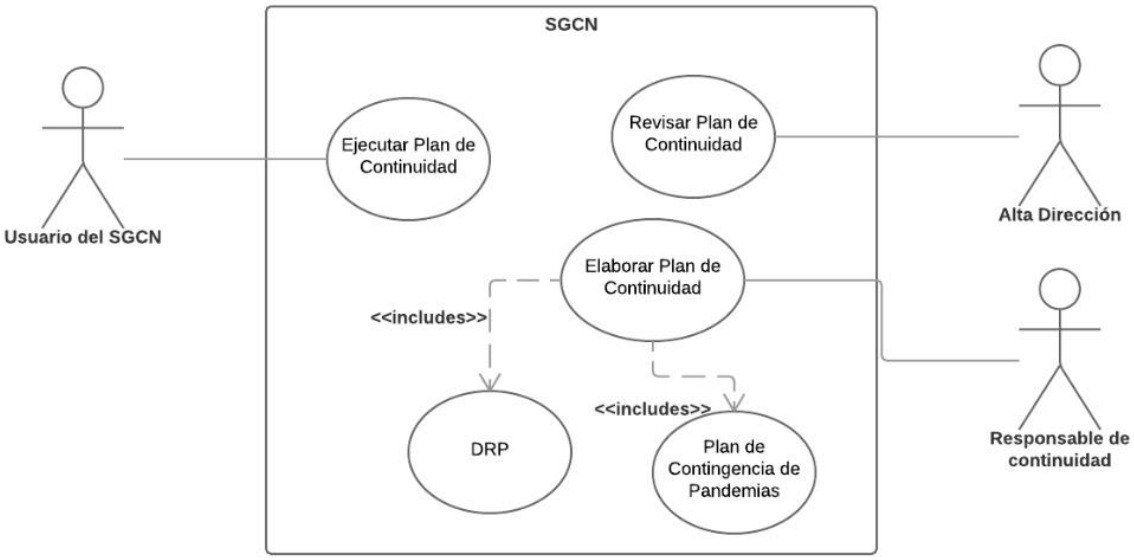

Figura 3.5: Caso de uso asociado al Plan de Continuidad del sistema

4. Diseño e Implementación

Este capítulo presenta el proceso de desarrollo del SGCN. Está organizado tomando como base las cláusulas de la norma ISO 22301.

4.1. Cláusula 4: Contexto de la Organización

La cláusula 4 de la norma comprende el análisis del contexto de la organización, incluyendo: necesidades, requisitos y alcance del SGCN.

Obtener un conocimiento general de Ozona y su contexto permite:

- Comprender los desafíos a los que debe hacer frente la organización para lograr el cumplimiento con la norma.
- Comprender los riesgos existentes en el mercado en que la organización desarrolla su actividad.
- Asegurar consistencia y alineación entre los objetivos estratégicos para la gestión de riesgos y la misión de la organización.

4.1.1. Presentación de la empresa

El grupo Ozona está centrado en la consultoría de procesos y en el suministro de servicios y soluciones informáticas. El conjunto de empresas que lo conforman se detalla en la Tabla 4.1:

Siglas	**SCPO**	**GPBA**	**OCSL**	**NUBIRA**
Nombre	Servicio de Consultoría de Procesos Ozona S.L.	GPBA Servicios Informáticos S.L.	Ozona Consulting S.L.	Nubira Serviços e Soluções Informáticas Lda.
NIF/CIF	B86171204	509948073	B15834872	513073213
Naturaleza jurídica	Empresa privada	Empresa privada	Empresa privada	Empresa privada
Domicilio social	Avda. de San Marcos, 31B 15890 Santiago de Compostela A Coruña	Rúa Basilio Teles nº 35, 9º Direito, 1070-020, Lisboa	Avda. de San Marcos, 31B 15890 Santiago de Compostela A Coruña	Rúa Basilio Teles nº 35, 9º Direito, 1070-020, Lisboa
Especialización	Ozona Consulting		Ozona Tecnología	

Ámbito	España	Portugal	España y Portugal	Portugal
Web	http://www.ozonaconsulting.com		http://www.ozonatecnologia.com http://www.ozonatech.com	

Tabla 13: Descripción de empresas del grupo Ozona

Ozona se divide en cuatro líneas de negocio indicadas a continuación:

- Gestión de servicios: orientada al diseño e implementación de sistemas basados en el estándar ISO 20000. Incluye además servicios de assessment y auditoría.
- Herramientas ITSM: orientada al diseño, implementación, operación y soporte de sistemas de monitorización enfocados a la gestión de servicios.
- Seguridad de la información: orientada al diseño e implementación de sistemas basados en el estándar ISO 27001. Incluye además servicios de assessment y auditoría.
- Continuidad de negocio / servicios TIC: orientada al diseño e implementación de sistemas basados en las ISO 22301 y 27031. Incluye además servicios de assessment y auditoría.

4.1.2. Contexto interno y externo

El contexto comprende las cuestiones, internas y externas, que son pertinentes para el propósito de Ozona, y que afectan a su capacidad para lograr los resultados previstos.

Los aspectos internos son aquellas cuestiones definidas por la propia organización, pertinentes para el propósito de ésta y que afectan a su capacidad para lograr los resultados previstos.

Los aspectos internos de Ozona se detallan en la Tabla 4.2:

Misión	La misión del grupo Ozona Consulting se basa en la especialización en áreas de negocio concretas, como medio para el posicionamiento en el mercado como empresas de referencia en su sector de actividad.
Valores	Los valores fundamentales que comparten los miembros de Ozona Consulting son: • Especialización. • Excelencia. • Creatividad.

Productos/Servicios	Consultoría técnica	• Estrategias de movilidad • Asesoramiento • Diseño, implementación y desarrollo de proyectos • Soporte y Mantenimiento
	Consultoría de procesos	• Gestión de Servicios de TI • Gestión de Seguridad de la Información • Gestión de Continuidad de Negocio
Clientes	Los clientes principalmente externos, tanto del sector público como privado.	

Tabla 14: Contexto interno de Ozona

Los aspectos externos engloban todo aquello que afecta a Ozona y que condiciona su capacidad para lograr los resultados previstos.

Entre los aspectos externos se distinguen:

- Entorno de negocio: enfocado en la especialización en áreas de negocio concretas.
- Entorno económico: marcado por la inestabilidad e imponiendo la necesidad de ser competitivos.
- Entorno social: la tecnología está integrada en la vida cotidiana.
- Entorno reglamentario.

4.1.3. Partes interesadas

Deben identificarse todas las partes interesadas relevantes para el SGCN, así como sus necesidades y expectativas. Las partes interesadas podrán ser tanto internas como externas.

En la Figura 4.1. se muestra el mapa de stakeholders de Ozona:

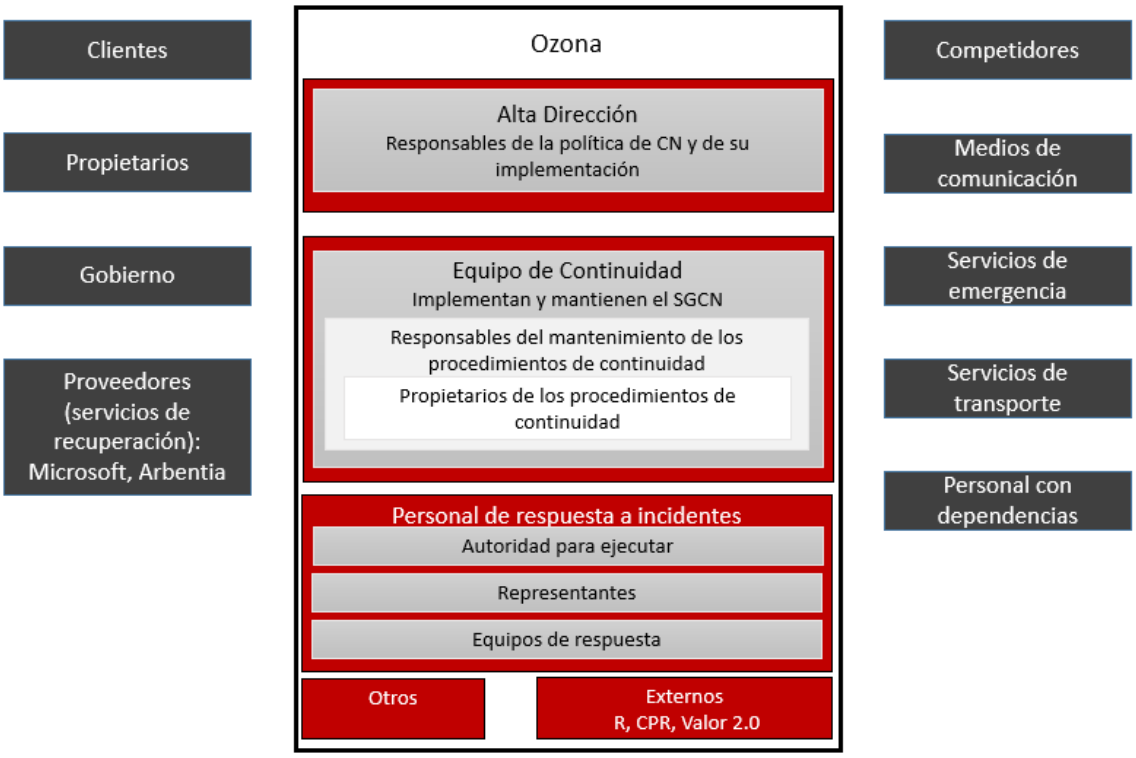

Figura 4.1: Diagrama de partes interesadas

4.1.4. Alcance del SGCN y exclusiones

El alcance de la continuidad de negocio de Ozona incluye todos los servicios, personas, responsabilidades, sistemas, comunicaciones, informaciones y activos que soportan las actividades prioritarias relacionadas con la actividad de la organización. Las actividades prioritarias han sido identificadas a través de la realización del BIA y serán detalladas en el apartado 4.5.

No se han identificado exclusiones.

4.1.5. Valor para el negocio

La implantación de un Sistema de Gestión de la Continuidad de Negocio está orientada a garantizar la disponibilidad de los procesos o servicios críticos de una organización. Supone un valor elevado para la organización, ya que garantiza que las necesidades de sus clientes estarán cubiertas, al menos en un porcentaje aceptable, incluso ante escenarios de interrupción graves.

Además, como el sistema se mantiene en un ciclo de mejora continua, estará en una adaptación constante al entorno, controlando y teniendo en cuenta los riesgos que puedan emerger o los cambios que se produzcan internamente.

Por último, dado que la Organización mantiene una línea de negocio enfocada en la continuidad de negocio, mantener un SGCN adecuado y efectivo supondrá una motivación positiva adicional para posibles clientes.

4.2. Cláusula 5: Liderazgo

La cláusula de Liderazgo está orientada al suministro de evidencias, por parte de la Alta Dirección, de su *compromiso en el establecimiento, operación, monitorización, revisión, mantenimiento y mejora del SGCN* [1].

La Política de Continuidad de Negocio es la evidencia del compromiso de la Alta Dirección en relación a la forma en que la Organización cumplirá los requisitos de continuidad de negocio y aquellos asociados a los clientes, a través de la implementación y operación de un Sistema de Gestión de Continuidad de Negocio (SGCN). La gestión de continuidad de negocio se ha establecido con el objetivo de asegurar que la Organización puede continuar cumpliendo las necesidades y expectativas de los clientes ante un escenario de interrupción de las operaciones habituales del negocio.

La Política se aplica a todos los departamentos y localizaciones. Todo el personal debe estar familiarizado con ella. Parte del personal tendrá, además, obligaciones específicas respecto a la continuidad de negocio, de las que deberán ser conscientes y cumplir tal y como se requiere. La asignación y comunicación de estas responsabilidades y autoridades debe ser llevada a cabo por la Alta Dirección.

La Política de Continuidad de Negocio de la Organización proporciona la declaración a través de la cual:

- Un Sistema de Gestión de Continuidad de Negocio (SGCN) es establecido y mantenido.

- Se identifican productos y servicios clave con sus actividades críticas y recursos de soporte.

- Se realiza una evaluación de riesgos y elaboran estrategias de mitigación para reducir la probabilidad de impacto de un incidente.

- Se desarrollan estrategias, procesos y planes para asegurar una respuesta efectiva a cualquier incidente, de manera que se cumplan los objetivos de continuidad de negocio.

- Se gestionan ejercicios y pruebas de los planes establecidos.

- El personal está sensibilizado y formado, de manera apropiada, para cualquier incidente.
- La junta ejecutiva asegura que el SGCN está actualizado y es efectivo, de manera que los planes definidos funcionarán cómo y cuándo se requiera.

4.2.1. Declaración de la Política

Es la Política de la Organización para mantener las competencias de continuidad de negocio que aseguren una recuperación rápida y eficiente de las operaciones esenciales ante cualquier incidente o desastre físico que ocurra en cualquiera de sus edificios. Para garantizar que estos planes cumplen completamente las necesidades de la Ozona, serán ejecutados regularmente y revisados anualmente.

Los objetivos de continuidad de negocio establecidos para Ozona son:

- Asegurar la seguridad del personal y otros ocupantes de los edificios.
- Minimizar la interrupción a los consumidores y proveedores y proteger así la reputación de la compañía y posición en el sector.
- Posibilitar la recuperación de las operaciones normales en el menor tiempo posible con la mínima interrupción.

Los planes de continuidad de negocio serán diseñados de manera que persigan la consecución de los objetivos presentados previamente.

La continuidad de negocio es completamente soportada por la Alta Dirección y el Equipo de Gestión, que espera que todo el personal sea consciente de su rol y que los planes estén preparados para ser implementados en cualquier momento. En particular:

- Se identifica un número concreto de propietarios de los planes que deben asegurarse de que éstos se mantienen y que cumplen los niveles de servicio requeridos.
- Los departamentos de soporte deben identificar áreas donde la resiliencia pueda ser mejorada y recomendar acciones con dicho propósito.
- Los propietarios de los planes deben asegurarse de que se realiza una revisión completa de sus planes anualmente y se comunican los resultados al Gestor de Continuidad de Negocio.
- Los propietarios de los planes deben asegurarse de que sus planes se someten a ejercicios anuales y garantizar que cualquier acción que ocurra se registra y que se actúa en consecuencia.
- Si ocurren cambios significativos en el negocio, los planes de continuidad de negocio deben ser revisados de forma apropiada.
- Deben identificarse los proveedores críticos y sus planes de continuidad de negocio deben ser aprobados por la Ozona previamente a la realización de acuerdos contractuales.

- Todo el personal debe ser consciente de los planes establecidos para su área y de su rol ante un incidente.

La Política proporciona un compromiso visible de la Alta Dirección con la continuidad de negocio que capacitará a Ozona para:

- Proporcionar continuidad a los servicios de los clientes incluso cuando las actividades de negocio se encuentren interrumpidas.
- Reducir la probabilidad e impacto de cualquier interrupción en el negocio.
- Reducir el impacto reputacional, operacional y financiero de cualquier incidente.

4.3. Cláusula 6: Planificación

La cláusula 6 describe los requisitos en relación a los objetivos estratégicos y a los principios bajo los que se establecerá el SGCN.

El objetivo principal de esta cláusula es, por tanto, la estimación temporal para la implementación del SGCN y el establecimiento del contexto en el que se implementará el sistema.

4.3.1. Gestión temporal de la implementación del SGCN

La gestión temporal que se realiza para la implementación del SGCN ya ha sido previamente presentada en el Capítulo 2 de este documento.

4.3.2. Creación del Manual

El Manual del SGCN es un documento principal que recoge la estrategia de la compañía, la estructura, responsabilidades, actividades, recursos, los procesos, etc. que Ozona ha establecido para llevar a cabo la gestión de continuidad de negocio. Se definen los documentos y procedimientos que deberán ser mantenidos como evidencias de una implementación efectiva de un programa de continuidad de negocio en Ozona.

Se presenta la información referente al SGCN, y las respectivas referencias a la documentación más relevante, siendo este un documento de guía para la comprensión del sistema y sus partes.

El contenido del Manual ya ha sido presentado en los apartados anteriores que referencian al contexto y a la Política.

4.3.3. Establecimiento de roles y responsabilidades

La identificación y asignación de los roles y responsabilidades asociados al SGCN es clave para alcanzar los objetivos del proyecto. Para el SGCN, los roles identificados se detallan en la Tabla 4.3:

Rol	Funciones y Responsabilidades
Dirección	- Aprobar la Política de Continuidad. - Aprobar los objetivos de continuidad. - Aprobar el Plan de Continuidad. - Aprobar las Estrategias de Continuidad. - Aprobar el presupuesto y los recursos necesarios. - Aprobar la estructura organizativa del SGCN. - Efectuar una revisión periódica del SGCN. - Aprobar las revisiones realizadas.
Patrocinador del SGCN	- Definir las expectativas del proyecto. - Financiar el proyecto. - Asignar el presupuesto. - Recibir los resultados del proyecto. - Tomar decisiones en relación a la financiación, cronograma y resultados. - Alinear el proyecto con los objetivos de la Organización - Intervenir en la resolución de conflictos. - Revisar periódicamente el estado del proyecto.
Coordinador del SGCN	- Establecer los objetivos, políticas y factores críticos de éxito. - Identificar las responsabilidades necesarias. - Definir y recomendar la estructura y gestión del proyecto. - Liderar el equipo para desarrollar el plan del proyecto. - Desarrollar el plan y determinar el presupuesto necesario. - Organizar, coordinar y administrar cada fase del proyecto. - Presentar el proyecto a la Dirección y partes implicadas. - Controlar el proceso a través de métodos de control efectivos y gestión de cambio. - Reportar de forma periódica el estado del proyecto.
Responsable de Continuidad	- Proponer los objetivos de recuperación. - Dirigir y liderar todas las actividades del PCN. - Declarar la contingencia ante el escenario de interrupción del lugar de trabajo, con base en las decisiones tomadas por el Comité de Crisis. - Liderar las reuniones del Comité de Crisis. - Advertir sobre nuevos riesgos que afectan la continuidad de la operación normal de la entidad y que ponen al descubierto debilidades del plan de continuidad. - Coordinar la ejecución de las pruebas del PCN.
Gestor de Continuidad	- Asegurar la gestión y operación del SGCN de la Organización. - Asegurar la divulgación de la Política de Continuidad. - Generar el Plan de Continuidad y actualizarlo cuando se produzcan cambios. - Planificar y dirigir las pruebas definidas en el Plan de Pruebas. - Asegurar la supervivencia de los procesos críticos tras una catástrofe o fallo muy grave. - Velar porque se siga y respete la metodología del proyecto. - Monitorizar, analizar y evaluar la efectividad del proceso de la gestión de la continuidad del servicio. - Apoyar las auditorías del SGCN.

	- Crear, implementar y mantener Planes de Formación y Concienciación en Continuidad de Negocio. - Ayudar a las distintas unidades de negocio en la adaptación del Plan de Continuidad. - Desarrollar, mantener, coordinar, operar y evaluar Planes de Divulgación y Coordinación de crisis.
Comité del SGCN	- Prestar un apoyo visible por parte de la Dirección al Plan de Continuidad de Negocio. - Controlar desde la perspectiva gerencial, el buen desarrollo del proyecto y que cumpla con los parámetros establecidos en el plan de proyecto y los compromisos entre las partes. - Tomar decisiones que tengan que ver con cambios importantes en el alcance del proyecto y en el esquema de contratación. - Facilitar los recursos necesarios para el desarrollo y mantenimiento del Plan de Continuidad de Negocio. - Aprobar los cambios del Plan de Continuidad de Negocio.
Comité de Gestión de Crisis	- Activar el PCN en cualquiera de los escenarios de contingencia o de desastre previamente establecidos. - Coordinar la respuesta ante los incidencias graves o catastróficas determinando, en caso de considerarlo necesario, el traslado de las operaciones a las ubicaciones de contingencia, y garantizando la reanudación de las mismas en el marco temporal establecido para ello. - Asegurar que se cuenta con los recursos económicos necesarios para afrontar las partidas de gastos extraordinarios en los que sea necesario incurrir durante el estado de contingencia o desastre y autorizar la ejecución de los mismos. - Aprobar los mensajes que serán enviados a la opinión pública, accionistas y proveedores acerca de la situación de la organización tras la contingencia o el desastre.

Tabla 15: Roles y responsabilidades del SGCN

Será necesario, además, realizar un análisis de los requisitos mínimos exigidos para cada uno de los roles, así como posibles incompatibilidades entre ellos. Todo este análisis se incluye en el documento *Ozona_Roles_SGCN_v1.0.docx*, incluido en la documentación entregada junto a esta memoria.

4.4. Cláusula 7: Soporte

La cláusula 7 proporciona soporte a las operaciones del SGCN en los procesos de comunicación y competencia con las partes interesadas, y asegura el registro, control, mantenimiento y retención de la documentación requerida.

4.4.1. Creación de plantillas

La creación de plantillas tiene como objetivo estandarizar los documentos, de manera que exista un único formato. Estas plantillas incluirán una explicación del contenido a incorporar para simplificar su uso lo máximo posible e independizarlo

de restricciones asociadas a las personas que las hayan creado. De esta forma se garantizan la uniformidad e integridad en la documentación del SGCN.

4.4.2. Plan de Comunicación

El Plan de Comunicación tiene como objetivo responder a la pregunta: ¿Qué mensaje se va a enviar? Es decir, establecer procedimientos efectivos de comunicación y consulta para regular el intercambio de información entre las partes interesadas.

Más concretamente, los objetivos específicos principales del Plan serán:

- Ayudar a las partes interesadas en la comprensión de los aspectos relacionados con la continuidad de negocio de la organización, mediante un diálogo continuo, basado en procedimientos de comunicación y consulta efectivos, y proporcionándoles la información necesaria para comprender todos los elementos tenidos en cuenta en los procedimientos de comunicación.
- Aumentar la importancia y el nivel de sensibilización en continuidad de negocio para dar soporte a las distintas responsabilidades de la organización.
- Mejorar la credibilidad y reputación de la Organización.
- Determinar la información que se comunicará, sus destinatarios y los umbrales temporales contemplados.
- Mantener informadas a las partes afectadas en caso de incidente.

Metodología

Para la elaboración del Plan de Comunicación, las actividades a realizar son:

- Identificación de las partes interesadas externas e internas.
- Definición de la estrategia de comunicación de Ozona.
- Asignación de los roles y responsabilidades de las partes en el proceso de comunicación.

Resultados

En la Tabla 4.4 se incluye la identificación de las partes interesadas:

Partes interesadas en la comunicación interna	
Dirección	Comunicar los impactos del incidente.
Empleados	Comunicar la Política de Continuidad.
Socios	Comunicar la situación del incidente.

Tabla 16: Partes interesadas en la comunicación interna del SGCN

Partes interesadas en la comunicación externa	
Familiares de los empleados	Comunicar accidentes que hayan afectado a la salud del empleado
Medios de comunicación	Comunicar accidentes que afecten a ciudadanos o áreas públicas. Ámbito local.
Clientes	Comunicar accidentes que afecten a los servicios que tienen contratados.
Proveedores	Comunicar accidentes que puedan requerir un suministro alternativo de recursos o afecten de alguna forma a los proveedores.
Ciudadanos	Comunicar accidentes que, por su alcance, puedan afectar a personas concretas o a áreas públicas.
Administración	Comunicar accidentes que puedan afectar al interés general o que impliquen el incumplimiento de algún aspecto legal o reglamentario.
Aseguradoras	Comunicar accidentes en activos asegurados
Vecinos	Comunicar accidentes en infraestructuras físicas colindantes cuando puedan representar un riesgo
Servicios de emergencia	Comunicar accidentes en los que pueda haber víctimas o que puedan representar un riesgo, en especial si se trata de un riesgo para las personas, animales o medio ambiente

Tabla 17: Partes interesadas identificadas en la comunicación externa

Estrategia de comunicación de Ozona

El propósito de la estrategia es la definición de una comunicación adecuada y eficaz para asegurar la protección del personal, líneas de negocio y reputación de la organización durante el proceso de recuperación de un incidente. Para lograrlo, la estrategia de comunicación debe perseguir los siguientes objetivos:

- Comunicación efectiva con todas las partes interesadas, tanto internas como externas.
- Asignar los roles y responsabilidades apropiados a los empleados.
- Suministrar la información adecuada al personal de manera regular, con el fin de que sean conscientes del procedimiento de comunicación y sus cambios.
- Establecer métodos de comunicación que aseguren que dicha comunicación se produce en caso de incidente.

Aide-mémoire

El objetivo del aide-mémoire es proporcionar información rápida y clara sobre el plan de comunicación en caso de emergencia, comprensible por cualquier miembro de la organización y con las indicaciones necesarias para proceder de la manera adecuada. Deberá depositarse un aide-mémoire en cada oficina, con el objetivo de que todo el personal disponga de toda la información necesaria para una correcta actuación.

Alerta

Una vez que se produce una emergencia, es necesario conocer lo más rápidamente posible cuál es la situación en la que se encuentra la organización. Para ello se elaborarán checklists con preguntas orientadas a conocer el alcance de la emergencia. Como resultado se producirá el informe de estado.

Comunicación

Teniendo los detalles sobre el impacto del incidente, debe activarse el Plan e iniciarse las comunicaciones pertinentes teniendo en cuenta las partes afectadas.

Definición de los flujos de comunicación

La definición de los flujos de comunicación proporciona la información necesaria sobre los emisores, destinatarios, contenidos y medios de cada proceso comunicativo que deba realizarse.

Flujos de comunicación internos

La Tabla 4.6 especifica los flujos de comunicación internos establecidos en el Plan:

Quién comunica	Qué comunica	A quién	Cómo
Dirección	Difusión de la Política de Continuidad	Todas las partes interesadas en el ámbito de la continuidad, incluyendo entidades externas	Publicación en la página web y envío por mail en su primera versión
Responsable de la persona que detecta el incidente	Incidentes que afectan o pueden afectar a la continuidad de negocio	La Dirección Responsable de Continuidad	Personal o telefónicamente
Responsable de Continuidad o sustituto	Activación del Comité de Crisis	Componentes del Comité de Crisis	Árbol de llamadas telefónico
Responsable de gestión de crisis o sustituto	Activación de los equipos de respuesta y/o recuperación	Equipos de respuesta y/o recuperación afectados	Árbol de llamadas telefónico
Recursos humanos	Incidente que afecta a la integridad de los trabajadores	Familiares de los trabajadores	Telefónicamente
Responsable del proveedor	Incidente que afecta a los proveedores críticos	Responsable de continuidad	Por correo electrónico o telefónicamente según urgencia
Responsable del área afectada	Incidente que requiere de la asistencia o soporte de proveedores	Responsable del proveedor requerido	Por correo electrónico o telefónicamente según urgencia
Responsable de Continuidad	Reportes del estado de la continuidad de negocio	Dirección	Informes de seguimiento de indicadores
Responsable de Continuidad	Informes de auditoría ISO 22301 (interna y externa)	Personal auditado Dirección	Envío del informe de auditoría

Responsable del plan de continuidad	Informes de pruebas del plan de continuidad	Personal involucrado en las pruebas	Envío del informe de pruebas por correo electrónico
Responsable del plan de continuidad	Modificaciones en el plan de continuidad	Lista de distribución que aparece en el plan correspondiente	Envío de la versión actualizada por mail y actualización del gestor documental
Responsable de Continuidad	Informe de BIA, informe de análisis de riesgos	Dirección	Presencialmente en una reunión

Tabla 18: Flujos de comunicación internos del SGCN

Flujos de comunicación externos

El medio principal a utilizar para estas comunicaciones será el teléfono, a excepción de aquellas comunicaciones que deban realizarse de manera presencial por requisito expreso de la parte interesada externa.

4.4.3. Plan de Formación y Awareness

Se entiende como Formación la adquisición de habilidades a nivel intelectual; y se entiende por concienciación (en su término anglosajón, awareness) al cambio en los hábitos a nivel de comportamiento.

Es necesario que todas las personas entiendan su rol en lo que se refiere a continuidad de negocio, ya que deben saber qué hacer y qué no en caso de que ocurra un incidente grave. Además, es necesario que sean capaces de aportar información adecuada.

El Plan de Formación y Concienciación tiene como objetivos responder a las preguntas: ¿Qué habilidades necesita adquirir el personal? Y ¿Qué comportamientos se quieren fomentar o cambiar entre el personal?

Metodología

Para la elaboración del Plan de Formación y Concienciación se seguirá un planteamiento enfocado en 4 dimensiones, especificadas en la Tabla 4.7:

Específico	Formación específica: roles concretos que requieren de una determinada formación, ya sea técnica o de habilidades
Obligatorio	Concienciación: todo el personal Introducción: personal nuevo

Habilidades	Formación en habilidades como el liderazgo a las personas que deben representar un rol clave en caso de activación del plan de continuidad
Cualificaciones	Certificaciones BCI (Business Continuity Institute) para los responsables del sistema de gestión.

Tabla 19: Dimensiones contempladas en el Plan de Formación y Awareness

Este Plan debe ser revisado anualmente, con la finalidad de identificar carencias formativas entre el personal o comportamientos inadecuados que puedan repercutir negativamente sobre la eficacia del SGCN implementado y sobre los que sea necesario aplicar acciones correctivas.

Resultados

Considerando la especialización y experiencia en el área del personal de Ozona, actualmente no se considera necesaria la formación para los roles principales del SGCN. Sin embargo, si se considera adecuado como objetivo a medio plazo, dar una formación de ISO 22301 Foundation a todo el personal que no posee ninguna certificación relacionada con continuidad de negocio. Este curso proporciona un conocimiento suficiente sobre los conceptos esenciales de continuidad y sirve, a su vez, como una primera tarea de concienciación del personal.
Las actividades principales del Plan de Concienciación que se llevarán a cabo de manera inmediata serán:

- Realización de una sesión de awareness.
- Presentación del SGCN implementado a través del correo electrónico corporativo, que incluya: la política elaborada sobre continuidad de negocio, la información de contacto de los responsables del sistema y las ubicaciones en las que puede encontrarse el Plan de Continuidad (presentado en el 4.5.5.), que será la salida principal del SGCN para todo el personal en su rol de usuarios de éste.
- Realización de una reunión, en presencial o en remoto, en la que el responsable de continuidad se encargue de presentar en detalle el SGCN, de manera que se garantice que todo el personal conoce su rol en el sistema y el propio funcionamiento de éste.
- Colocación de posters en todas las oficinas con la información de contacto de los responsables del sistema y la esquematización de pasos a seguir en caso de emergencia.

4.5. Cláusula 8: Operación

La cláusula 8 define los requisitos de continuidad, cómo alcanzarlos y desarrolla los procedimientos necesarios para gestionar un incidente disruptivo.

4.5.1. BIA

El análisis del impacto en el negocio permite:

- Identificar las actividades necesarias para entregar los servicios clave, es decir, aquellos incluidos en el alcance del SGCN.
- Identificar los recursos necesarios para realizar esas actividades.
- Recomendar objetivos de recuperación de actividades y recursos (en línea con la tolerancia de inactividad aprobada para cada uno de los servicios, teniendo en cuenta los costes potenciales asociados a alcanzar esos objetivos).
- Justificar los objetivos de recuperación de la actividad y de los recursos, basado en el impacto potencial de quiebre del servicio.

Metodología

La metodología que se seguirá para la realización del BIA se estructura en una serie de actividades especificadas a continuación:

Actividad 1: Identificación de requisitos previos

En la primera fase del BIA es necesario identificar un conjunto de requisitos previos. La identificación de estos requisitos implica la realización de un conjunto de actividades iniciales, detalladas a continuación:

- Identificación del contexto: es necesario determinar el contexto externo en el que opera la Organización (BIA) y determinar la legislación aplicable.

  Además, debe determinarse el contexto interno, incluyendo los productos/servicios, procesos, actividades y recursos. Es importante identificar y tener en cuenta los sistemas de gestión existentes en la Organización, así como identificar en qué ámbitos la Organización es más o menos resiliente (capacidad de recuperación).
- Identificación del alcance: es necesario formalizar y documentar el alcance, incluyendo aspectos relativos a:
  - Composición de la organización.
  - Procesos/actividades que realiza.
  - Productos/servicios que comercializa.
  - Instalaciones.
  - Personas.
  - Tecnología.
  - Proveedores.
- Identificar las funciones y responsabilidades: es necesario identificar todas las funciones y responsabilidades en el ámbito de aplicabilidad del BIA. En esta etapa, puede elaborarse una matriz que realice el mapeado entre los procesos y/o actividades con las respectivas funciones asociadas.

    - Establecimiento: determinar cuáles son las principales funciones que intervienen en la continuidad y cuáles son sus responsabilidades.
    - Asignación: la Dirección debe realizar un nombramiento formal.
    - Difusión: las funciones deben ser comunicadas a todas las partes afectadas.

  Como mínimo deberán definirse las siguientes funciones:
    - Sponsor del proyecto de BIA
    - Responsable de validar los resultados
    - Responsables de los procesos
    - Gestores de las actividades
- Conseguir el compromiso interno: esta actividad es una de las más importantes en esta fase. Las entrevistas del BIA requieren involucrar y disponer de las personas pertenecientes a las distintas áreas de negocio. El apoyo de la Dirección es crucial, ya que motiva un mayor apoyo y participación de las personas. Dicho apoyo está relacionado con la efectividad, alineación, cumplimiento, relaciones y visión general de la Organización.
- Identificación de recursos necesarios: los recursos necesarios deben ser identificados e involucrados. La Organización debe proporcionar los recursos necesarios para:
    - Cumplir la Política y alcanzar los objetivos de continuidad.
    - Tomar las decisiones adecuadas para personas y recursos relacionados, incluyendo el tiempo para cumplir roles y responsabilidades del proceso BIA, y formación y sensibilización.
    - Satisfacer los requisitos de cambio de Ozona.
    - Proporcionar funcionamiento y mejora continua del programa de continuidad de negocio.

Actividad 2: Planificar el BIA

Esta actividad incluye la planificación y gestión del proyecto. Las tareas necesarias se detallan a continuación:

- Elaborar el plan del proyecto: establecer el plan del proyecto (equipo del BIA, interlocutores, calendario), y atribuir los recursos para el proyecto.
- Obtener la aceptación del enfoque y del plan del proyecto por parte del sponsor del proyecto de BIA.
- Identificar la información relevante: determinar el tipo de información que será necesario pedir.

En este punto es necesario evaluar un conjunto de detalles, por ejemplo, sobre:

- Tipo de información: algunas de las entrevistas serán por servicio, proceso, actividad o área de negocio.
- Tipo de recursos: pueden establecerse desde los recursos necesarios para desarrollar la actividad, tales como recursos de personas y

subcontratados, conocimientos, skills, cualificaciones requeridas, equipos informáticos, aplicaciones y comunicaciones IT, elementos físicos (electrónicos o papel), entre otros. También existen los recursos necesarios en caso de emergencia, como por ejemplo: inmediatos, en menos de 1h, en 8 horas, en 24 horas, en 1semana, en más de 2 semanas.

- Tipo de dependencias: dependencias clave internas (entre funciones de negocio, entre departamentos y entre sistemas) y dependencias clave externas (con otras empresas del grupo y con proveedores externos).
- Frecuencia y tiempos clave: momentos del día, del mes, del año, que sean más críticos en determinadas actividades, por ejemplo, cierres mensuales, presentación de ofertas, picos previsibles de demanda, actividades que se deben realizar, necesariamente, en un determinado momento, etc.
- Procesos alternativos en caso de emergencia: alternativas viables, en caso de emergencia, para las actividades más relevantes. Por ejemplo, transferir determinadas actividades a un proveedor.
- Tipo de impacto: dada la interrupción de una actividad, será necesario determinar:
    - La descripción del impacto.
    - El valor del impacto en el tiempo (según la escala de valoración definida).
    - El RTO (tiempo en que debería ser recuperado).
    - El MTPoD (tiempo máximo a partir del cual provocaría daños irreparables).
    - El MBCO (nivel mínimo aceptable y durante cuánto tiempo).
- Establecer un método de recogida de información: es necesario seleccionar un método de recogida de información. Puede utilizarse cualquier método, siempre y cuando se garantice la consistencia de la información.
- Establecer un método de evaluación de la información recogida en las diferentes áreas de negocio que tenga en cuenta la matriz de impacto definida y los tipos de impacto, tales como la pérdida financiera, impacto para el cliente, impacto operacional, impacto en la reputación, impacto legal/regulatorio.

El método de BIA para Ozona consiste en:

- Planificar reuniones informales, pero estructuradas, orientándolas de manera que haga posible una comprensión clara de las áreas de la Organización.
- Llevar a cabo estas reuniones con el personal clave de cada área.
- Añadir a una plantilla la información obtenida en las entrevistas, y enviársela a los distintos participantes, para que éstos la validen.
- Se valorará la necesidad de contactar con algún entrevistado para aclarar o completar información o, incluso, realizar una segunda entrevista.
- Una vez validada la información, se generará un informe de conclusiones.

La información que se pretende conseguir se detalla a continuación:

- Visión general de las actividades que realiza.
- Información general del área, número de personas, ubicaciones desde las que trabajan de forma habitual, número de personas dedicadas a cada actividad, etc.
- Visión general del impacto que supondría no llevar a cabo las actividades identificadas.
- Tiempo máximo que podría interrumpirse cada una de las actividades
- Recursos necesarios (por ejemplo, personas, aplicaciones/servicios de TI, datos, proveedores o instalaciones) para poder reanudar cada una de las actividades, en un nivel aceptable.
- Cómo evoluciona la necesidad de recursos a lo largo del tiempo, es decir, que necesito tener el primer día, la primera semana, el primer mes o a partir del segundo mes.

Actividad 3: Ejecución del BIA

La ejecución del BIA consiste en un conjunto de entrevistas planificadas y estructuradas que tienen como principal objetivo conocer la actividad de cada área de negocio y evaluar qué tipo de impacto causaría alguna interrupción inesperada en sus actividades.

Estas entrevistas no siguen un cuestionario establecido, son entrevistas informales, pero sí responden a una estructura de recogida de información ya establecida, y abordan, de una forma general, los siguientes puntos:

- Enfoque general del área de negocio
- Identificación de las actividades clave
- Localización física del equipo
- Dimensión y perfil de los equipos
- Soporte en el que se encuentra la información crítica
- Redundancia de equipos
- Dependencia de los sistemas de información
- Diferentes tipos de impacto causado por alguna interrupción inesperada

Las salidas de esta actividad, directamente relacionadas con el análisis del impacto en el negocio, son:

- Evaluación de impactos a lo largo del tiempo en lo que se refiere a un fallo en la entrega de productos o servicios, que sirve de justificación para las necesidades de continuidad de negocio.
- Documentación de una lista de productos y servicios priorizados.
- Relacionar los productos/servicios con los procesos.

- Priorizar los procesos, comenzando por la priorización de productos/servicios. Un proceso será crítico, en la medida en que soporte productos y servicios críticos.
- Identificar los requisitos mínimos para operar cada proceso (personas, instalaciones, equipos, proveedores) y en qué plazo (la escala definida en Ozona se basará en los siguientes plazos: 1 día, 3 días, 1 semana, 2 semanas, 1 mes, más de 2 meses).
- Bajar el nivel de las actividades que permiten que el proceso sea entregado cuando el detalle de la actividad sea relevante.

Además de esto, habrá salidas para otras actividades de continuidad de negocio:

- Cambios en el alcance del programa de continuidad de negocio de Ozona.
- Identificación de requisitos legales, reglamentarios y contractuales (obligaciones).
- Riesgos identificados que afectan a los servicios, procesos o actividades críticas.

Actividad 4: Validar el BIA

La aprobación de resultados debe ser realizada por la Dirección. Las actividades de validación del BIA incluyen, esencialmente:

- Aprobación de los resultados del BIA: la priorización de productos y servicios, la priorización de procesos y la priorización de actividades (incluyendo recursos e interdependencias).
- Compilación del feedback y actualización de la información.
- Elaboración de un informe final de conclusiones que incluya:
    - Una descripción general del proceso de BIA, incluyendo objetivos y alcance.
    - Los impactos que influyen en la consecución de los requisitos de continuidad de negocio.
    - Prioridades recomendadas para los productos y servicios, procesos, actividades y recursos.
    - Conclusiones y próximos pasos (por ejemplo: selección del a estrategia de continuidad).

Es normal que se realice una revisión del BIA en aquellos casos en que la estrategia implique inversiones muy sustanciales que estén fuera del presupuesto o sean inaccesibles.
En este punto, es necesario tener un conocimiento de lo que la organización podrá tolerar en caso de interrupción, y lo que está preparada para invertir a corto y largo plazo.

Actividad 5: Monitorizar y Revisar BIA

El BIA debe ser revisado y actualizado de forma anual, y realizado completamente cada tres años, o siempre que se considere necesario, sea por cambios en la organización o en sus objetivos estratégicos, por cambios legales o por cambios en el alcance.
La revisión de un BIA puede tener varios motivos, entre ellos:

- La revisión anual.
- Cambio de dirección estratégica.
- Cambio de producto o servicio.
- Modificación de la norma.
- Cliente y/o cambio contractual.
- Cambios operativos, incluyendo novedades/cambios en aplicaciones/TIC, cadena de suministros (internalización /externalización), y recursos web/instalación.
- Cambio estructural.
- Después de un ejercicio de continuidad de negocio.
- Después de una interrupción.

Resultados

Los servicios presentes en Ozona pueden dividirse en dos áreas de negocio:

- Dinámica de proyectos: incluye servicios relacionados con el seguimiento del estado de los proyectos que desarrollan los consultores.
- Dirección financiera: incluye todos los servicios relacionados con los aspectos financieros de la empresa: tesorería, control de ingresos, impuestos,…

Cada uno de los servicios identificados será especificado con el detalle indicado en la metodología y se le asignará un impacto sobre la organización en función del tiempo. Los niveles de impacto se definen en la 'Matriz de impactos'.
La 'Matriz de impactos' clasifica el tipo de impacto según su categoría y su repercusión negativa en cada ámbito. Las categorías identificadas son:

- Impacto financiero
- Impacto en el cliente o en los servicios
- Impacto operativo
- Impacto reputacional
- Impacto en requisitos legales y/o contractuales
- Impacto en empleados y/o salud pública
- Impacto en confidencialidad, integridad y/o disponibilidad de la información.

Las dimensiones del impacto se clasifican en una escala numérica de 1 (menor impacto) a 4 (mayor impacto).

Después de realizar el análisis de ambas áreas, se obtiene el informe de conclusiones del BIA que proporciona la lista de servicios ordenados por su criticidad en función del tiempo y la lista de recursos críticos con los tiempos de recuperación objetivo.

Las Tablas 4.8 y 4.9, incluidas a continuación, muestran la lista obtenida, ordenada de mayor a menor criticidad de los servicios:

Impacto de una interrupción a lo largo del tiempo								
Proceso o servicio e negocio	MTPoD	RTO	Impacto hasta 1 día	Impacto hasta 3 días	Impacto hasta 1 semana	Impacto hasta 2 semanas	Impacto hasta 1 mes	Impacto hasta 2 meses
Impuestos	1 día	1 hora	3	4	4	4	4	4
Laboral	3 días	1 día	1	2	3	3	4	4
Facturación	1 semana	1 día	1	1	2	3	4	4
Seguimiento de proyectos	1 mes	2 semanas	1	1	1	2	3	3
Control de backlog de facturación	2 semanas	1 semana	1	1	1	2	2	3
Gestión de Pagos	1 mes	1 día	1	1	1	1	2	3
Control de ingresos	1 mes	2 semanas	1	1	1	1	2	2
Contabilidad	1 mes	1 día	1	1	1	1	2	2
Financiación	1 semana	1 día	1	1	1	1	2	2
Control de imputaciones	2 meses	2 semanas	1	1	1	1	1	2
Tesorería y Gestión de Cobros	1 mes	1 día	1	1	1	1	1	2

Tabla 20: Impactos de interrupción de cada servicio a lo largo del tiempo

Adicionalmente, para cada servicio, se incluyen las columnas de MTPoD (tiempo máximo tolerable de interrupción) y RTO (tiempo objetivo de recuperación). Para una mejor comprensión de la tabla resultante, teniendo en cuenta los servicios más críticos, las conclusiones obtenidas son:

- El servicio de Impuestos no puede estar interrumpido más de 1 día. Además, debería poder recuperarse en 1 hora. Si se supera el tiempo máximo de interrupción contemplado, el impacto se elevaría a magnitud 3. Consultando la matriz de impactos, esto se traduce en un impacto financiero de cifras muy elevadas que puede comprometer la viabilidad del negocio. También tendría un impacto reputacional.

- El servicio de Laboral no puede estar interrumpido más de 3 días y debería recuperarse en un máximo de 1 día. Si se supera este límite, el impacto asociado se corresponde al nivel 2, que se traduce en pérdidas asumibles de poca gravedad. Sin embargo, si la interrupción se extiende a 1 semana, el impacto se eleva a nivel 3, de forma que sus consecuencias pueden tornarse comprometedoras para la empresa.

- El servicio de Facturación podría estar hasta 1 semana interrumpido, aunque debería recuperarse en 1 día. En este caso, no habría un impacto grave hasta las 2 semanas de interrupción.

- El servicio de Seguimiento de Proyectos podría estar hasta 1 mes interrumpido sin provocar consecuencias graves en la empresa, aunque deberían comenzar las tareas de recuperación en un máximo de 2 semanas.

La lista de recursos críticos obtenida se muestra a continuación. Para cada uno de ellos se analiza la necesidad de elaborar un Plan de recuperación. Las opciones a valorar en este análisis serán:

- Se requiere un Plan específico debido a la criticidad y complejidad asociada al recurso o a la falta de alternativas que sustituyan al recurso.
- El recurso no requiere un Plan específico porque ya es gestionado, o puede gestionarse, mediante medidas de mitigación de riesgos.
- El recurso no requiere de un Plan específico porque existen recursos alternativos a su uso. Esta categoría no excluye de la aplicación de medidas de mitigación de riesgos asociados al recurso cuando sea necesario.

Recurso crítico	RTO más exigente	Procesos/Actividades dependientes	Plan de Recuperación
Navision	1 día	Control de imputaciones Seguimiento de proyectos Contabilidad Facturación Tesorería y Gestión de Cobros Financiación	Navision es clave para los servicios críticos de la empresa, por ello será necesario elaborar un Plan específico de recuperación.
Herramienta de dedicaciones	2 semanas	Control de imputaciones Seguimiento de proyectos	Aunque la herramienta de dedicaciones no tiene una criticidad temporal elevada, sí es necesario elaborar un Plan de Recuperación, ya que no se dispone de una herramienta alternativa para asumir esta funcionalidad.
Dropbox	1 semana	Seguimiento de proyectos	No es necesaria un Plan concreto ya que la información almacenada puede obtenerse de otras fuentes.

Documentos asientos contables	2 semanas	Contabilidad	No se requiere un Plan, la información puede obtenerse de otras fuentes.
Impresora	Horas	Facturación	Aunque temporalmente es muy crítico, no es necesario un Plan ya que está gestionado mediante medidas de mitigación de riesgos.
Excel	1 día	Tesorería y Gestión de Cobros	No es necesario un Plan, el software puede encontrarse en cualquier ordenador.
Factura proveedor	1 día	Gestión de Pagos	No es necesario un Plan, los datos están registrados en Navision. Sólo sería necesario solicitar duplicados, pero los pagos se efectuarían.
Datos Navision	1 hora	Gestión de Pagos Impuestos	Los datos de Navision se gestionan con el mismo Plan elaborado para Navision.
Datos Excel	1 día	Gestión de Pagos	No es necesario un Plan, la información podría generarse de nuevo desde la herramienta Navision.
Internet	1 hora	Impuestos	No se requieren necesidades específicas para la conexión, por tanto, se gestionará a través de mitigación de riesgos.
Documentos justificativos	1 semana	Impuestos	La ausencia de los documentos en formato físico no impide la realización de la tarea, por tanto, no es necesario un Plan específico. Se solicitarán duplicados.
A3Nom	1 día	Laboral	No se ha elaborado un Plan específico ya que el servicio será externalizado en el mes de abril. Se eliminará este recurso y el riesgo asociado al servicio será responsabilidad de terceros.
Documentos físicos	1 mes	Financiación	No es necesario un Plan específico, se gestiona mediante mitigación de riesgos. Se requiere solicitud de duplicados.
Aplicación Red Seguridad Social	1 día	Laboral	Se gestiona mediante mitigación de riesgos. No se requiere un plan específico.
File Server (R)	4 horas	Administración y Perfiles Citrix	El servicio de acceso remoto Citrix está incluido y gestionado en el Plan de recuperación de Navision.
Share Point (R)	24 horas	Informes y Contabilidad (backlog)	La información incluida en este recurso se encuentra también en File Server, que está contemplado en el Plan de recuperación de Navision.
Share Point (Office 365)	N/A	Tecnología	Esta tecnología no sería crítica para el acceso a la información de Share Point, porque ésta se

			encuentra en File Server que sí tiene un Plan de recuperación asociado.
Share Point (Citrix)	N/A	Tecnología	Citrix está incluido en el Plan de recuperación de Navision, por tanto, la recuperación de Share File está contemplada ya en este Plan.

Tabla 21: Recursos críticos identificados para los servicios

Por último, la lista de riesgos resultante derivada de los recursos críticos utilizados por cada servicio servirá de entrada para la siguiente tarea (Análisis de Riesgos).

4.5.2. Análisis de Riesgos

El objetivo del proceso de análisis de riesgos es identificar todas las amenazas a las que se encuentra expuesto el SGCN, evaluando cuantitativamente este nivel de exposición y estableciendo estrategias de tratamiento, cuando sea necesario, con el fin de disminuir, lo máximo posible, las consecuencias que pueden tener la materialización de uno de estos riesgos.

Metodología

A continuación describe brevemente el enfoque utilizado para la elaboración de la metodología de análisis de riesgos, incluyendo el proceso de desarrollo de análisis de riesgos, la identificación de las amenazas y vulnerabilidades existentes en la empresa, y la presentación de las matrices de nivel de impacto y probabilidad utilizadas en la evaluación de riesgos. Esta metodología de análisis de riesgos tiene como base los requisitos que establece la norma internacional ISO 31000:2009.

Esta norma internacional permite que cualquier empresa pueda realizar una gestión eficaz del riesgo al que se encuentra expuesta, mediante la identificación, análisis y evaluación de los riesgos, favoreciendo con estas prácticas la consecución de sus objetivos.

El proceso de gestión de riesgos utilizado en esta metodología está presentado en la Figura 4.2:

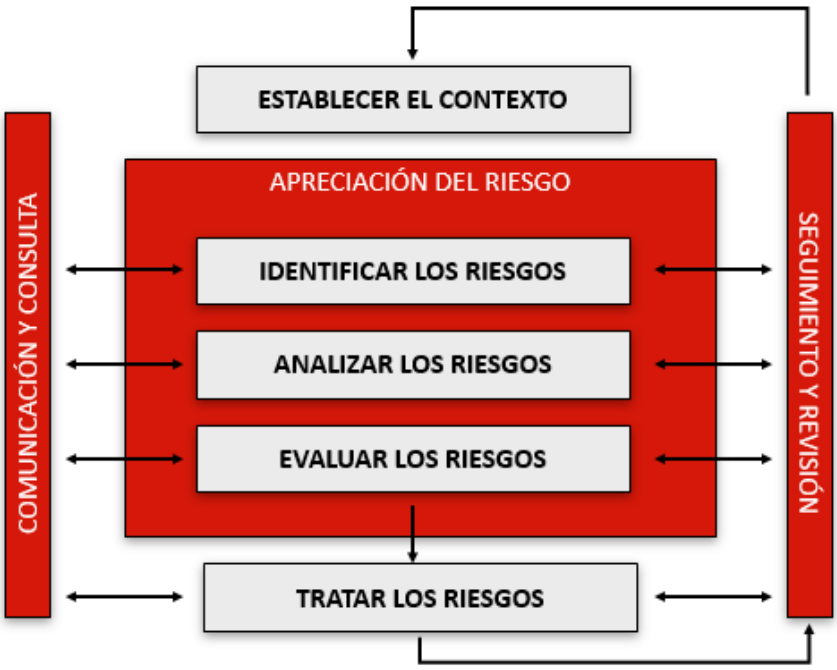

Figura 4.2: Proceso de gestión de riesgos

Fases del proceso de gestión de riesgos

- Comunicación y consulta: La comunicación y consulta a las partes interesadas, internas y externas, deberá ocurrir durante todas las fases del proceso de gestión de riesgos.
  La comunicación y la consulta con las partes interesadas son importantes, ya que estas producen juicios sobre riesgos basados en las percepciones de estas partes sobre dichos riesgos. Estas percepciones sobre los riesgos pueden variar debido a diferencias en los valores, necesidades, presupuestos, conceptos y preocupaciones de las partes interesadas. Dado que sus puntos de vista pueden tener un impacto significativo en las decisiones tomadas, las percepciones de las partes interesadas deberían ser identificadas, registradas y consideradas en el proceso de toma de decisiones.
  La comunicación y consulta deberán facilitar el intercambio de información verdadera, pertinente, precisa y comprensible, respetando los aspectos de confidencialidad e integridad personal.

- Establecer el contexto: a través del establecimiento del contexto, la empresa enuncia sus objetivos y define los parámetros internos y externos a tener en cuenta cuando se gestiona el riesgo, así como el ámbito y los criterios de riesgo para las partes restantes del proceso. Las actividades que forman parte de esta fase son:

    - Establecimiento del contexto externo: el contexto externo es el ambiente externo en el cual la empresa intenta alcanzar sus objetivos.

Puede incluir, por ejemplo: los entornos social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo; los factores clave y tendencias con impacto en los objetivos de la empresa; las relaciones con las partes interesadas externas, sus percepciones y valores, etc.

- Establecimiento del contexto interno: el contexto interno es el ambiente interno en el cual la empresa intenta alcanzar sus objetivos. Puede incluir, por ejemplo: el gobierno, estructura organizacional, funciones y responsabilidades; las políticas, objetivos y las estrategias implementadas para alcanzarlos; las capacidades, comprendidas en términos de recursos y conocimiento; las relaciones con las partes interesadas internas, sus percepciones y valores; la cultura de la empresa; los sistemas / flujos de información y procesos de toma de decisiones, etc.

- Establecimiento del contexto del proceso de gestión de riesgos: deberán ser establecidos los objetivos, las estrategias, el ámbito y los parámetros de las actividades de la empresa, donde el proceso de gestión de riesgos se está aplicando. La gestión de riesgos deberá ser desarrollada justificando los recursos utilizados en su implementación. Deberán ser también especificados los recursos requeridos, las responsabilidades y autoridades y los registros a mantener.

  El establecimiento, tanto del contexto interno como del contexto externo, así como del propio proceso de gestión de riesgos, donde se identifican las áreas/procesos críticos de negocio se realiza durante el proceso de BIA. Para este análisis de riesgos sólo se considerarán las áreas/procesos con un valor de impacto igual o superior a 3.

- Definición de los criterios de riesgo: los criterios deberán reflejar los valores, objetivos y recursos de la empresa. Algunos criterios pueden ser impuestos por, o derivar de, exigencias legales y requisitos reglamentarios y otros requisitos suscritos por la empresa.

En el Sistema de Gestión de Continuidad de Negocio se realizará un planteamiento basado en la pérdida de recursos, facilitando el análisis de causas de interrupción y elaboración de planes de continuidad. Se consideran, por tanto, cuatro categorías de recursos:

- Personas: pérdida de equipos, siendo especialmente crítico en equipos que por naturaleza de la actividad que desempeñan, tienen dimensión reducida, pudiendo existir elementos sin redundancia (e.g. especialista único en determinado sistema), o que todos ellos se encuentren en una misma localización. Se consideran recursos humanos de terceros integrados en

equipos de la organización (equipo extendido), dado que en caso de interrupción del proveedor, ésta podría considerar la necesidad de contratación directa.

- Instalaciones y equipamientos: pérdida de instalaciones y equipamientos de usuario final, tanto por pérdida directa como por condicionamiento de la accesibilidad y/o funcionalidad. Se consideran en la misma categoría instalaciones y equipamientos, dado que normalmente la pérdida de una instalación tiene como consecuencia la pérdida de los equipamientos residentes (equipamiento de puesto de trabajo, coches,…).

- Tecnología: pérdida de infraestructuras tecnológicas que soportan los equipamientos de usuario final. En esta categoría se consideran servidores, redes (voz y datos), aplicaciones y datos. Podrán ser críticos puntos únicos de fallo, o incluso si existe redundancia el hecho de que ocurra un mismo incidente puede alcanzar los sistemas principales y los alternativos.

- Proveedores: pérdida de suministro y de prestación de servicios. Se consideran proveedores de recursos humanos, equipamientos y materias primas, así como prestadores de servicios (mantenimiento, limpieza, seguridad,…). Normalmente la externalización permite transferir la responsabilidad de asegurar la continuidad por pérdida de recursos, siendo necesario sin embargo, asegurar que efectivamente se toma esa responsabilidad.

Las fases siguientes de este proceso corresponden a la etapa de apreciación del riesgo. La apreciación del riesgo es una etapa global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Identificación del riesgo

Ozona deberá identificar las fuentes de riesgo, áreas de impacto, eventos (incluyendo alteraciones de las circunstancias), respectivas causas y consecuencias potenciales. El objetivo de esta etapa es generar una lista con los riesgos, basada en los eventos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos de la empresa. La identificación realizada es crítica, pues un riesgo no identificado en esta fase no será incluido en el análisis posterior.

La identificación deberá incluir los riesgos cuya fuente esté o no sobre el control de la empresa, aunque la fuente o causa del riesgo puedan no ser evidentes.

Así como se identifica lo que pueda ocurrir, es también necesario considerar posibles causas y escenarios que muestren cuales son las consecuencias que pueden ocurrir. Todas las causas y consecuencias significativas deberán ser consideradas.

Para alcanzar un planteamiento basado en la pérdida de recursos, el BIA se ha realizado con base en las cuatro categorías de recurso referidas. Esto significa que por área/proceso debe ser identificadas tanto las amenazas como las vulnerabilidades existentes en cada categoría.

Análisis de los riesgos identificados

El análisis de riesgos implica realizar una comprensión de éstos. El análisis de riesgos proporciona una entrada para la evaluación del riesgo y para las decisiones sobre qué riesgos deben ser tratados, y sobre las estrategias y métodos más apropiados para dicho tratamiento. El análisis de riesgos también puede ser una entrada para la toma de decisiones, donde tengan que realizarse elecciones y las distintas opciones involucren tipos y niveles de riesgo diferentes.

El análisis de riesgos implica considerar las causas y fuentes de riesgo, sus consecuencias positivas y negativas y la probabilidad de que dichas consecuencias ocurran. Deberán ser identificados los factores que afectan al impacto y a la probabilidad. El riesgo es analizado, determinando su impacto y probabilidad y otros atributos del riesgo. Un evento puede tener múltiples consecuencias y puede afectar a múltiples objetivos. Los controles existentes, y su eficacia y eficiencia, también deberán ser considerados.

La forma en la que el impacto y la probabilidad son expresados, y el modo en que son combinados para determinar un nivel de riesgo, deberán reflejar el tipo de riesgo, la información disponible y el propósito para el cual la salida sobre la apreciación del riesgo va a ser utilizada. Todo esto deberá ser consistente con los criterios de riesgo. También es importante considerar la interdependencia de los diferentes riesgos y sus fuentes.

En la fase de evaluación de los riesgos es necesario, para el cálculo del riesgo, asociar al impacto de la interrupción de las categorías de recursos, contempladas en el BIA, una probabilidad de ocurrencia.

La probabilidad de ocurrencia resulta de la conjugación de la amenaza y de la vulnerabilidad identificadas en la fase anterior. La amenaza supone el factor contextual y la vulnerabilidad es la debilidad existente en la empresa, que puede llegar a ser explotada por la amenaza asociada.

Las medidas implementadas de reducción de impacto y/o probabilidad pueden ser variadas, pero siempre que se identifique una medida será necesario tener presente si ésta reducirá el impacto o la probabilidad.

Tras la implementación de las medidas identificadas deberá ser calculado el riesgo actual. Este riesgo es calculado a través de una multiplicación directa entre el

impacto actual y la probabilidad actual. De nuevo, se utilizará la matriz de tipos de impacto y la tabla de probabilidad, mencionadas anteriormente.

Evaluación de riesgos

La finalidad de la evaluación del riesgo es apoyar la toma de decisiones, teniendo como base los resultados del análisis de riesgos, sobre qué riesgos necesitan tratamiento y la prioridad en la implementación de éste.

La evaluación de riesgos engloba la comparación del nivel de riesgo identificado en el desarrollo del proceso de análisis con los criterios de riesgo, considerando el contexto. Teniendo como base esta comparación, puede ser considerada la necesidad de tratamiento.

Las decisiones deberán tener en cuenta el contexto extendido del riesgo e incluir consideraciones sobre la tolerancia de los riesgos soportados por las partes, no los beneficios del riesgo para la empresa. Las decisiones deberán ser tomadas de acuerdo con las exigencias legales, reglamentarias y otros requisitos.

En determinadas circunstancias la evaluación del riesgo puede llevar a una decisión de efectuar análisis adicionales. La evaluación del riesgo puede llevar también a la decisión de no efectuar el tratamiento del riesgo, además de mantener los controles existentes. Esta decisión estará influenciada por la actitud de la empresa de cara al riesgo y por los criterios de riesgo que hayan sido establecidos.

En esta etapa es necesario verificar si el valor del riesgo actual está dentro de los valores del apetito de riesgo definido por la empresa. Este apetito de riesgo se muestra en la Figura 4.3, y engloba todos aquellos riesgos cuyo producto de impacto y probabilidad se encuentra en la zona enmarcada:

		IMPACTO				
		0 NO APLICA	1 LEVE	2 MODERADO	3 GRAVE	4 MUY GRAVE
PROBABILIDAD	4 FRECUENTE	0	4	8	12	16
	3 PROBABLE	0	3	6	9	12
	2 RARO	0	2	4	6	8
	1 IMPROBABLE	0	1	2	3	4

Figura 4.3: Matriz de niveles de riesgo

CATEGORÍA DE RIESGO	VALORACIÓN	ACCIÓN
MUY ELEVADO	[12-16]	Las medidas para reducción del riesgo tienen que ser implementadas, siendo necesaria la aplicación de medidas de control específicas hasta que la situación esté resuelta.
ELEVADO	[6-9]	Las medidas para la reducción del riesgo deben ser implementadas con urgencia, dentro de un período de tiempo definido y puede ser necesario aplicar medidas de control específicas hasta que la situación esté resuelta.
MODERADO	[3-4]	Debe ser realizada una monitorización del riesgo para definir medidas complementarias de control. Las medidas de control delriesgo deben ser implementadas dentro de un período de tiempo definido y su eficacia debe ser controlada.
ACEPTABLE	[1-2]	No son necesarias medidas de control complementarias. Es necesario garantizar que las condiciones de control existentes son aplicadas y mantenidas.

Figura 4.4: Descripción de niveles de riesgo

Tratamiento de riesgos

El tratamiento del riesgo implica la selección de una o más opciones para modificar los riesgos y la implementación de esas opciones. Una vez implementados, los tratamientos proporcionan o modifican controles.

Sólo los riesgos con valor de riesgo actual superior al apetito de riesgo deben ser incluidos en esta fase.

El tratamiento del riesgo implica un proceso cíclico que incluye:

- Evaluar un tratamiento del riesgo
- Decidir si los niveles de riesgo residual son tolerables
- Si no son tolerables, generar un nuevo tratamiento del riesgo
- Evaluar la eficacia de ese tratamiento

Por tanto, las actividades que forman parte de esta fase son:

- Identificación de la estrategia del riesgo: las opciones de tratamiento del riesgo pueden incluir, por ejemplo: evitar el riesgo, asumir o aumentar el riesgo, eliminar la fuente de riesgo, alterar la verosimilitud/consecuencias, retener el riesgo, etc.

- Selección de opciones de tratamiento del riesgo: podrán ser consideradas y aplicadas individualmente, o de forma combinada, diversas opciones de tratamiento del riesgo. El plan de tratamiento deberá identificar claramente el orden de prioridad de implementación de los tratamientos individuales del riesgo.

- Preparación e implementación de planes de tratamiento del riesgo: el objetivo de los planes de tratamiento del riesgo es documentar la forma en la que serán implementadas las opciones de tratamiento escogidas. Los responsables de la decisión y otras partes interesadas deberán ser

conscientes de la naturaleza y dimensión del riesgo residual después del tratamiento del riesgo. El riesgo residual deberá ser documentado y sujeto a monitorización, revisión y, cuando sea apropiado, posterior tratamiento.

Seguimiento y Revisión de Riesgos

Los procesos de seguimiento y revisión de la empresa deberán englobar todos los aspectos del proceso de gestión de riesgos con el objetivo de:

- Asegurar que los controles son eficaces y eficientes, tanto en el diseño como en la operación.
- Obtener información adicional para mejorar la apreciación del riesgo.
- Analizar y aprender con los eventos (incluidos los casi accidentes), mudanzas, tendencias, sucesos y fallos.
- Detectar alteraciones en el contexto, externo e interno, incluyendo alteraciones sobre los criterios de riesgo y sobre el propio riesgo, que pueden requerir la revisión de los tratamientos del riesgo y de las prioridades.
- Identificar los riesgos emergentes.

Las responsabilidades respecto a la monitorización y revisión deben estar claramente definidas.

El progreso en la implementación de los planes de tratamiento del riesgo proporciona una medida del rendimiento. Los resultados pueden ser incorporados en la gestión global del rendimiento de la empresa, en su medición y en las actividades de reporte interno y externo.

Los resultados de la monitorización y revisión deberán ser registrados y reportados, externa e internamente, según sea apropiado, y deberán ser usados también como una entrada para la revisión de la estructura de gestión del riesgo.

Resultados

El análisis de riesgos es muy extenso y contiene información de Ozona de carácter privado, por tanto, en este documento no se incluirá la información completa generada para el análisis, sólo la identificación de los riesgos a tratar.

En la Figura 4.5 se muestra el mapa de calor obtenido tras el análisis. El mapa de calor es una matriz probabilidad/impacto que clasifica los riesgos en función del nivel de riesgo asociado y destaca aquellos riesgos que deben ser tratados porque pertenecen al área de riesgo no aceptable:

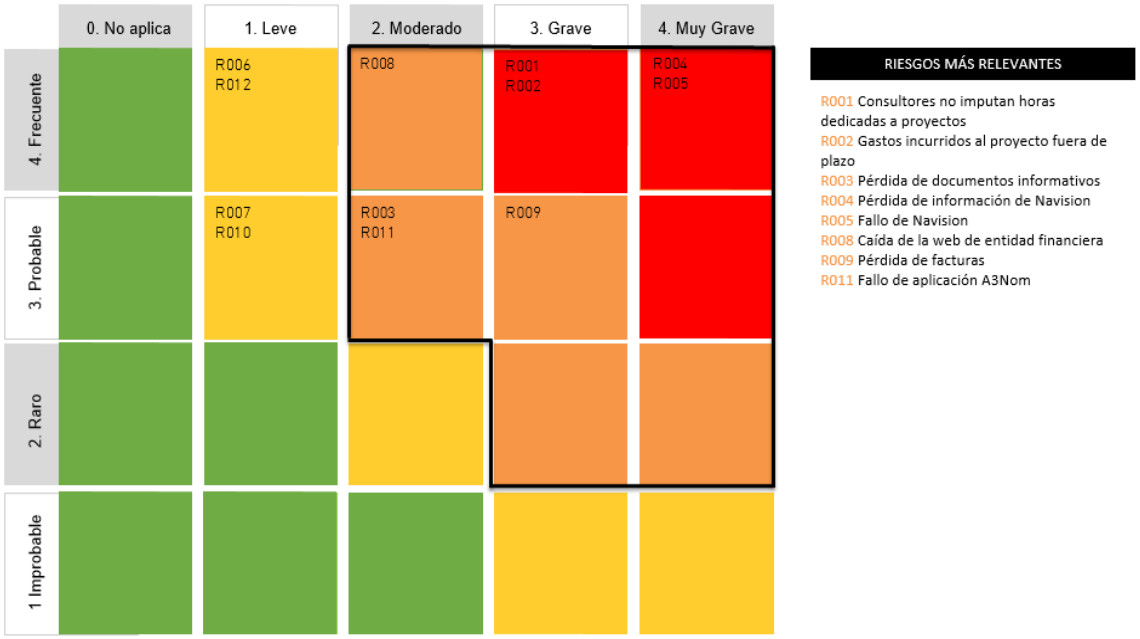

Figura 4.5: Mapa de calor de los riesgos identificados en el análisis

Para la lista de riesgos más relevantes será necesario, por tanto, elaborar un plan de tratamiento.

4.5.3. Estrategia de Continuidad

El objetivo del proceso de selección de la Estrategia es proporcionar orientación en la definición de las acciones necesarias para proteger a la organización, y seleccionar las soluciones de recuperación más apropiadas para las funciones críticas del negocio y el soporte a recursos.

La Estrategia de Continuidad de Negocio es la base de los Planes de Continuidad de Negocio, genera una visión y dirección para la empresa, estableciendo las declaraciones sobre su misión e identificando mercados y objetivos a través de los cuales la empresa alcanzará dicha misión. En términos de continuidad, genera las estrategias operativas alternativas necesarias para mantener las actividades críticas de la empresa.

Metodología

La metodología que se sigue para la selección y determinación de la Estrategia de Continuidad se organiza en una serie de actividades detalladas a continuación:

Actividad 1: Identificación de escenarios de riesgo

Para cada área de negocio será necesario evaluar los distintos escenarios que pueden causar la interrupción de los servicios críticos identificados en el BIA.
Dada la diversidad de escenarios en los que puede encontrarse la organización y que pueden causar una interrupción en el negocio, el planteamiento basado en causas de interrupción no sólo implica un gran esfuerzo dado el elevado número de planes necesarios, sino también un posible esfuerzo en vano por el hecho de no ser posible prevenir todos los escenarios que pueden ocurrir.

Por las razones indicadas, la práctica a implementar en el SGCN, será un planteamiento basado en la pérdida de recursos, considerando cuatro categorías de recurso:

- Personas: pérdidas de equipos directos, siendo especialmente crítico en equipos que por la naturaleza de la actividad tienen dimensión reducida, pudiendo existir elementos sin redundancia (p.e. Especialista único en un determinado sistema), o que se encuentran todos en una misma localización. Se consideran recursos humanos de terceros integrados en los equipos de Ozona, dado que en caso de interrupción del proveedor, Ozona podrá considerar la posibilidad de contratación directa.

- Instalaciones y Equipamientos: pérdida de las instalaciones y equipamientos de usuario final, tanto por pérdida directa como por condicionamiento de accesibilidad y/o funcionalidad. Se consideran las instalaciones y equipamientos en la misma categoría, ya que normalmente la pérdida de una instalación implica la pérdida de los equipamientos resientes (equipamiento de puesto de trabajo, coches,...).

- Tecnología: pérdida de infraestructuras tecnológicas asociadas a los equipamientos de usuario final. En esta categoría se consideran servidores, redes (voz y datos), aplicaciones y datos. Podrán ser críticos puntos únicos de fallo, o incluso cuando existe redundancia, la ocurrencia de un mismo incidente puede afectar a los sistemas principales y a los alternativos.

- Proveedores: pérdida de suministro y de prestación de servicios. Se consideran proveedores de recursos humanos y equipamientos, así como prestadores de servicios (mantenimiento, limpieza, seguridad,…). Normalmente, la externalización permite transferir la responsabilidad de asegurar la continuidad por pérdida de recursos siendo necesario, sin embargo, asegurar que esa responsabilidad es asumida.

Por tanto, para cada tipo de recurso se identificará el escenario de riesgo que puede causar su pérdida y los recursos mínimos necesarios para la activación del Plan de Continuidad que restaurará el servicio crítico afectado a unos niveles aceptables.

Actividad 2: Identificación de estrategias de continuidad

Para cada uno de los escenarios de riesgo identificados se elaborará una estrategia de actuación en caso de ocurrencia de ese escenario. Esta estrategia se especifica indicando:

- Situación normal: representa la operativa del servicio de manera habitual.
- Respuesta inmediata: representa las acciones inmediatas a realizar ante la ocurrencia del escenario.
- Respuesta a medio plazo: representa las acciones que se llevarán a cabo si el escenario se extiende en el tiempo.
- Vuelta a la normalidad: representa la situación que tendrá lugar una vez que se dé por finalizada la situación de escenario de riesgo.

Resultados

La identificación de los escenarios de riesgo se incluye en las Tablas 4.10 y 4.11:

Área de negocio: Dinámica de Proyectos			
Tipo de recurso	Recursos críticos	Escenarios	Recursos futuros para activación del Plan
Personas	Consultores (internos y externos) Administración Valor 2,0	Huelga Pandemia Pérdida de competencias	Todo el equipo de consultores 1 miembro de Administración RGG o SNC
Instalaciones y Equipamientos	Oficina San Marcos, Roxos, Madrid, Lisboa	Indisponibilidad de oficinas	Trabajo en remoto Oficina alternativa con adquisición de equipos de sobremesa por empleado
Tecnología	Herramienta de dedicaciones Navision Dropbox GSuite	Indisponibilidad herramienta dedicaciones Indisponibilidad de Navision Indisponibilidad de Dropbox	Navision Dropbox Herramienta dedicaciones
Proveedores	Arbentia (Proveedor de Navision) Data Center R	Indisponibilidad de Arbentia Indisponibilidad de R	Proveedor de Navision Microsoft

Tabla 22: Especificación de escenarios de riesgo para el área de Dirección de Proyectos

Área de negocio: Dirección Financiera			
Tipo de recurso	Recursos críticos	Escenarios	Recursos futuros para activación del Plan
Personas	Alba, Chus, Cristina Sande, Karina, Carla Cordeiro, Carla Amorim, Gestoría (Portugal)	Huelga Pandemia Pérdida de competencias	Todos los asociados a la localización del incidente (España o Portugal)
Instalaciones y Equipamientos	Oficina San Marcos, Roxos, Madrid, Lisboa	Indisponibilidad de oficinas	Trabajo en remoto Oficina alternativa con adquisición de equipos de sobremesa por empleado
Tecnología	Navision	Indisponibilidad de Navision	Navision
Proveedores	Arbentia Data Center R Gestoría	Indisponibilidad de Arbentia Indisponibilidad de R Indisponibilidad de Gestoría	Proveedor de Navision Microsoft

Tabla 23: Especificación de escenarios de riesgo para el área de Dirección Financiera

En ambos casos, los escenarios en los que se puede encontrar Ozona son los mismos. A continuación se detallará la estrategia a aplicar para cada uno de ellos:

Escenario 1: Huelga

En el caso de Ozona, los procesos no tienen una criticidad temporal tan elevada como para no poder asumir la ausencia de los trabajadores durante unos días. Por tanto, para el escenario de huelga no se contemplará una estrategia específica de actuación.

Escenario 2: Pandemia

Ante la ocurrencia de este escenario, será necesaria la activación de un Plan de Contingencia de Pandemias específico que, dependiendo del número de afectados se activará a un nivel de gravedad concreto. El diagrama asociado representa la estrategia definida para el escenario en la Figura 4.5:

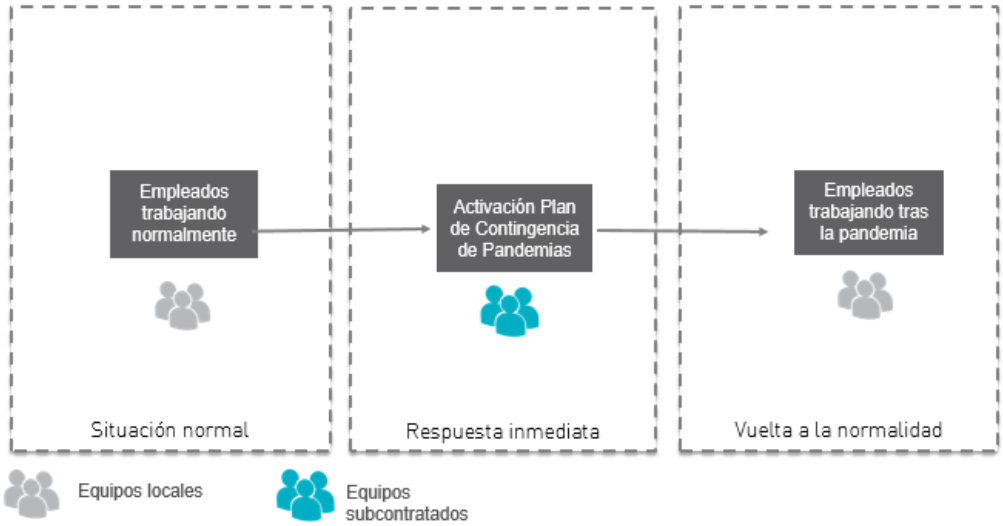

Figura 4.6: Estrategia asociada a escenarios de pandemia

Escenario 3: Pérdida de competencias

La pérdida de competencias está asociada con la salida, temporal o permanente, de recursos humanos con conocimientos específicos. Como Ozona es una empresa pequeña con un número de recursos reducido, es muy probable que la carga de trabajo asociada a estos recursos no pueda repartirse entre el resto del personal (tanto por falta de tiempo como de conocimientos), por tanto, la respuesta inmediata será la subcontratación. La subcontratación permitirá avanzar las tareas que están en desarrollo, evitando la imputación de retrasos en los proyectos.
En el caso de salidas permanentes o bajas temporales prolongadas (más de 6 meses), Ozona deberá iniciar un período de selección de personal y activar un Plan de Formación, de manera que el nuevo personal adquiera las competencias específicas que se requieren. Una vez que se termine el período de formación, Ozona comenzará a operar de nuevo en un escenario de normalidad. El diagrama que representa la estrategia definida para este escenario se muestra en la Figura 4.6:

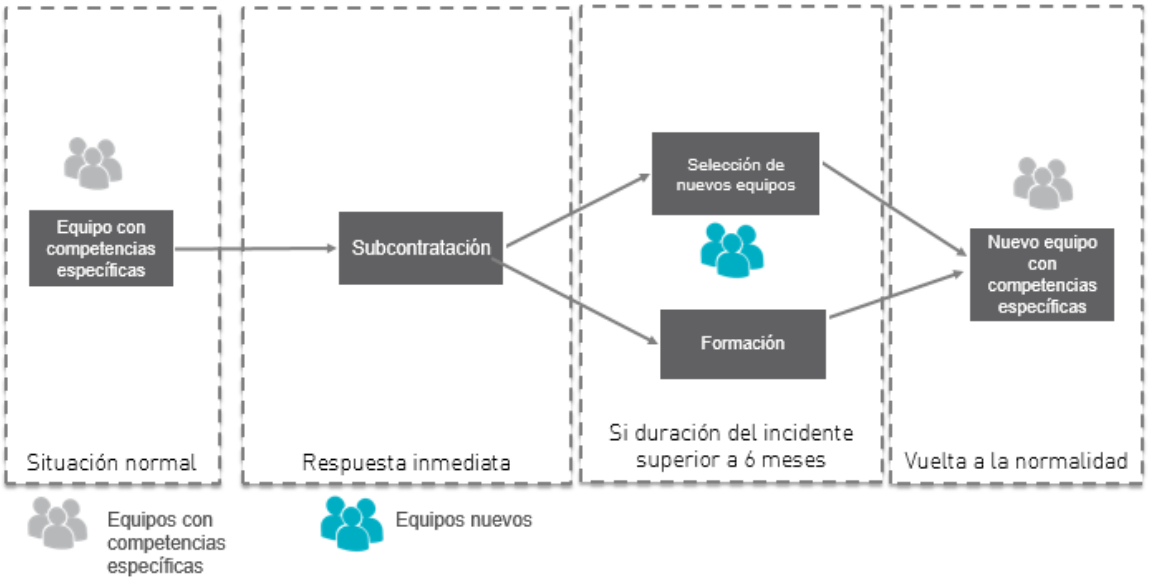

Figura 4.7: Estrategia asociada a escenarios de pérdida de competencias

Escenario 4: Indisponibilidad de la Oficina de San Marcos (Santiago de Compostela)

En la oficina de San Marcos todo el personal depende de un equipo de sobremesa. Por tanto, en caso de indisponibilidad del edificio, por cercanía, la respuesta inmediata será el traslado a la oficina de Roxos.
Si la indisponibilidad se prolonga a más de 3 meses, será necesario alquilar una nueva oficina, realizando la adquisición de los equipos de sobremesa que se requieran. La vuelta a la normalidad se producirá cuando exista de nuevo una ubicación estable para la oficina. El diagrama que representa la estrategia definida para este escenario se muestra en la Figura 4.7:

Figura 4.8: Estrategia asociada al escenario de indisponibilidad de la Oficina en San Marcos

Escenario 5: Indisponibilidad de la Oficina de Roxos, Madrid o Lisboa

En el caso de las oficinas de Roxos, Madrid o Lisboa, dado que todo el personal utiliza portátiles y tienen capacidad para trabajar de forma remota, la respuesta inmediata ante la indisponibilidad de alguno de los edificios será el trabajo en remoto.
Igual que en el escenario anterior, si la indisponibilidad se prolonga durante más de 3 meses, será necesario alquilar una nueva oficina. Se volverá a una situación de normalidad cuando exista una ubicación estable de la oficina. El diagrama que representa la estrategia definida para este escenario se muestra en la Figura 4.8:

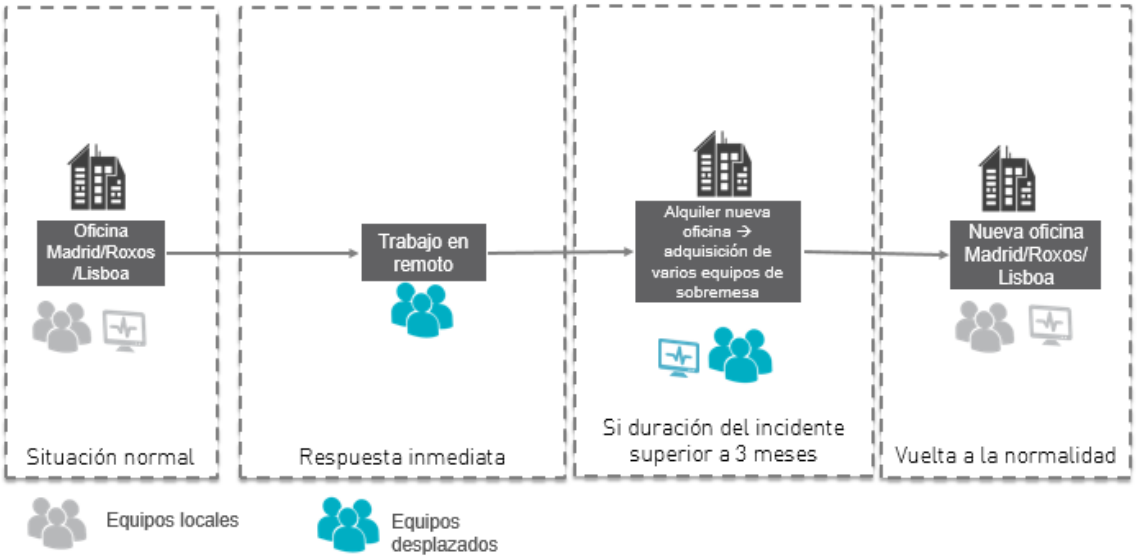

Figura 4.9: Estrategia asociada a la indisponibilidad de las oficinas de Roxos, Madrid o Lisboa

Escenario 6: Indisponibilidad de la herramienta de dedicaciones

Los consultores de Ozona utilizan una herramienta interna para el registro de las horas imputables a cada proyecto. En caso de indisponibilidad de esta herramienta, la respuesta inmediata será el uso de hojas Excel en las que los consultores lleven un registro manual de su dedicación horaria a los distintos proyectos. Esta estrategia se aplicará el tiempo que sea necesario hasta que la herramienta esté operativa de nuevo. El diagrama que representa la estrategia definida para este escenario se representa en la Figura 4.9:

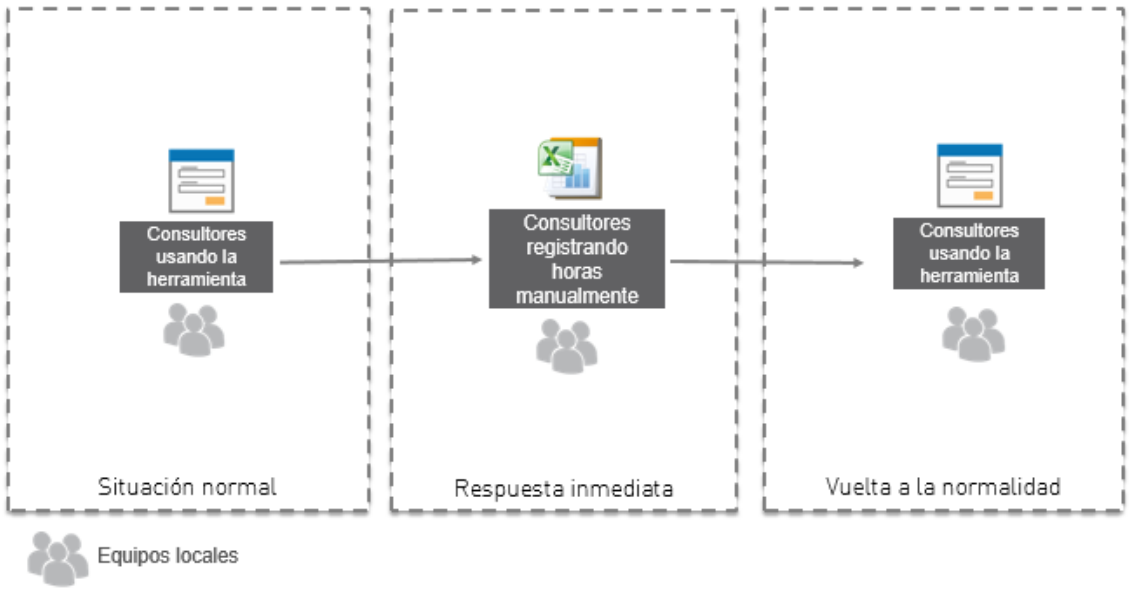

Figura 4.10: Estrategia asociada a la indisponibilidad de la herramienta de dedicaciones

Escenario 7: Indisponibilidad de Navision

Navision es un recurso crítico para el proceso de Dinámica de Proyectos, y su recuperación es, por tanto, prioritaria. Pero para llevarla a cabo es necesario tener en cuenta si la indisponibilidad se produce de forma directa (falla la herramienta) o indirecta (por alguna dependencia inherente a su funcionamiento). También será importante tener en cuenta las fechas en que se produzca la indisponibilidad, ya que en función de éstas, la recuperación podrá ser o no ser necesaria de manera inmediata.

Teniendo en cuenta las condiciones de la indisponibilidad, se activará el DRP adaptado según la situación concreta que se ha identificado. Este DRP es, por tanto, un Plan de recuperación integrado que engloba la recuperación de varios recursos críticos interrelacionados: Navision, Citrix, Data Center y File Server.
La estrategia de actuación en caso de indisponibilidad de Navision se describe en la Figura 4.10:

Figura 4.11: Estrategia asociada a la indisponibilidad de Navision

Los períodos de criticidad se establecieron durante el proceso de realización del BIA.

Otros escenarios

Los demás escenarios identificados no tienen una criticidad suficiente tal que requiera una estrategia específica de tratamiento, más concretamente:

- Indisponibilidad de Arbentia: este escenario sería crítico si la indisponibilidad fuese simultánea con una indisponibilidad de R. Se considera que es muy poco probable la ocurrencia de ambos incidentes al mismo tiempo.

- Indisponibilidad de Gestoría (Portugal): no es un escenario crítico para el área de negocio. Muchas de las funciones realizadas por este proveedor son

conocidas por personal interno de Ozona, permitiendo que se sigan realizando casi todas las tareas subcontratadas en caso de ser necesario.

4.5.4. Estrategias para la recuperación de elementos TIC de actividades prioritarias

Para poder elaborar los Planes de Recuperación de los recursos TI de las actividades críticas de Ozona, es necesario conocer el detalle de la arquitectura actual de dichos recursos.

El sistema en el que está montado Navision está ubicado en uno de los Data Center del proveedor R. Este sistema se compone de:

- 1 servidor virtual de base de datos SQL.
- 1 servidor virtual donde se encuentra instalado Navision.
- 1 cabina de almacenamiento en alta disponibilidad. El almacenamiento de alta disponibilidad se consigue con otra cabina ubicada en otro Data Center y que se menciona en los párrafos siguientes.

El sistema tiene dependencias con otros servicios, que será necesario considerar en el DRP, ya que pueden ser el origen de una indisponibilidad de éste:

- Servicio de acceso remoto Citrix: se utiliza para proporcionar a los usuarios acceso al servicio desde dentro o fuera de la red de Ozona.
- Servicio de virtualización: es un servicio en alta disponibilidad, utiliza 2 servidores físicos diferentes, en caso de caída de uno de ellos, el otro asume la capacidad completa.
- Servicio de autenticación

Aunque no es una dependencia, cabe destacar la necesidad del servicio de backup y recuperación.

Como ya se mencionó en la descripción del sistema, en un segundo Data Center, dentro de la misma red del proveedor, Ozona dispone de otra cabina de almacenamiento de alta disponibilidad en la que se almacenan los backups y snapshots de las máquinas virtuales del sistema principal.

Por último, existe un entorno inactivo montado en Microsoft Azure que dispone de todos los elementos necesarios para poder asumir la producción en caso de indisponibilidad del Data Center de R. Además, también contiene los backup del almacenamiento.

En la Figura 4.12 se muestra un diagrama que resume la situación presentada previamente:

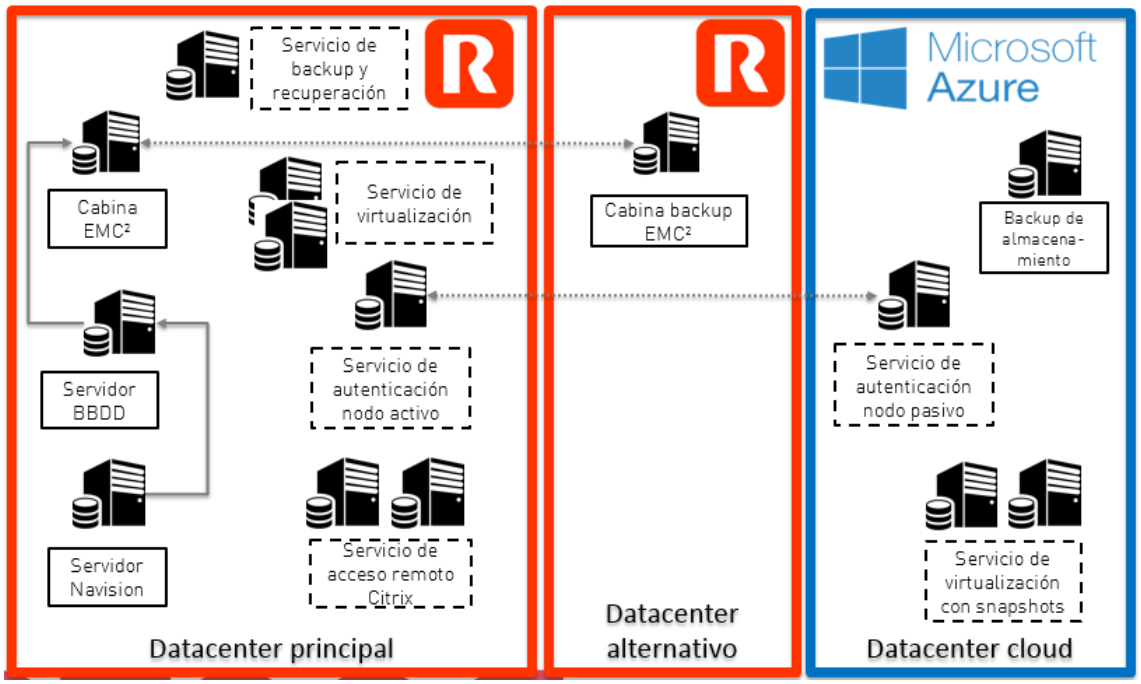

Figura 4.12: Diagrama de infraestructura TI

Por tanto, la estrategia de recuperación en caso de indisponibilidad del Data Center se compone de los siguientes pasos:

1. Levantar las máquinas ya disponibles en Azure (Todas las necesarias para el correcto funcionamiento de Navision, como hemos visto antes: BBDD de Navision y servidor Navision, BBDD Citrix y servidor Citrix y el servidor Veeam backup. El servidor de Active Directory ya se encuentra activo en Azure.

2. Recuperar la información desde el backup existente y volcarla en el servidor de BBDD.

3. Verificar el correcto funcionamiento del sistema.

Este tipo de estrategia se conoce como *Warm site*, caracterizada porque se dispone de los elementos hardware y sólo es necesario instalar los elementos software para poner el sistema en funcionamiento.

Considerando los tiempos de recuperación y la infraestructura ya existente en Ozona, se han descartado otros tipos de opciones estratégicas:

- *Cold site*: se caracteriza por la existencia de una ubicación que dispone de servicios básicos, pero que no incorpora hardware, software o, incluso, comunicaciones. La preparación de esta localización podría requerir tiempos del orden semanal. Esta estrategia no es válida, ya que no permitiría la recuperación del sistema en los RTOs más exigentes.

- *Hot Site*: una estrategia más agresiva que *Warm Site*. En ella se dispone tanto de hardware como de software y los servidores contienen la información actualizada. Este tipo de estrategia se descarta, ya que el análisis coste/beneficio solamente se justifica para sistemas muy críticos con objetivos de recuperación que no sea viable conseguir de otro modo.

Con respecto a la estrategia de backup de las bases de datos, de entre las opciones de que se han analizado:

- Backup de la base de datos en *Frío***:** Los backup en frio implican parar la base de datos en modo normal y copiar todos los archivos sobre los que se asienta. Antes de parar la base de datos hay que parar también todas las aplicaciones que están trabajando con la base de datos. Una vez realizada la copia de los archivos, la base de datos se puede volver a arrancar.

- Backup de la base de datos en *Caliente***:** El backup en caliente se realiza mientras la base de datos está abierta y funcionando en modo ARCHIVELOG. Habrá que tener cuidado de realizarlo cuando la carga de la base de datos sea pequeña. Este tipo de backup consiste en copiar todos los archivos correspondientes a un tablespace determinado, los archivos redo log archivados y los archivos de control. Esto para cada tablespace de la base de datos.

- Backup *Lógicos con Export / Import***:** Estas utilidades permiten al DBA hacer copias de determinados objetos de la base de datos, así como restaurarlos o moverlos de una base de datos a otra. Estas herramientas utilizan comandos del SQL para obtener el contenido de los objetos y escribirlos en/leerlos de archivos.

Por las características de las bases de datos y el uso que se hace de los datos almacenados, nos hemos decantado por el backup en *Frío* semanal completo y diario incremental.

Modelado de la arquitectura de los servicios

Una vez conocidas las características generales del sistema, es necesario modelar cada servicio concreto, identificando los servidores que lo componen y las dependencias, tanto entrantes como salientes, con otros servicios.

- Modelado de servicio de gestión financiera (Navision)

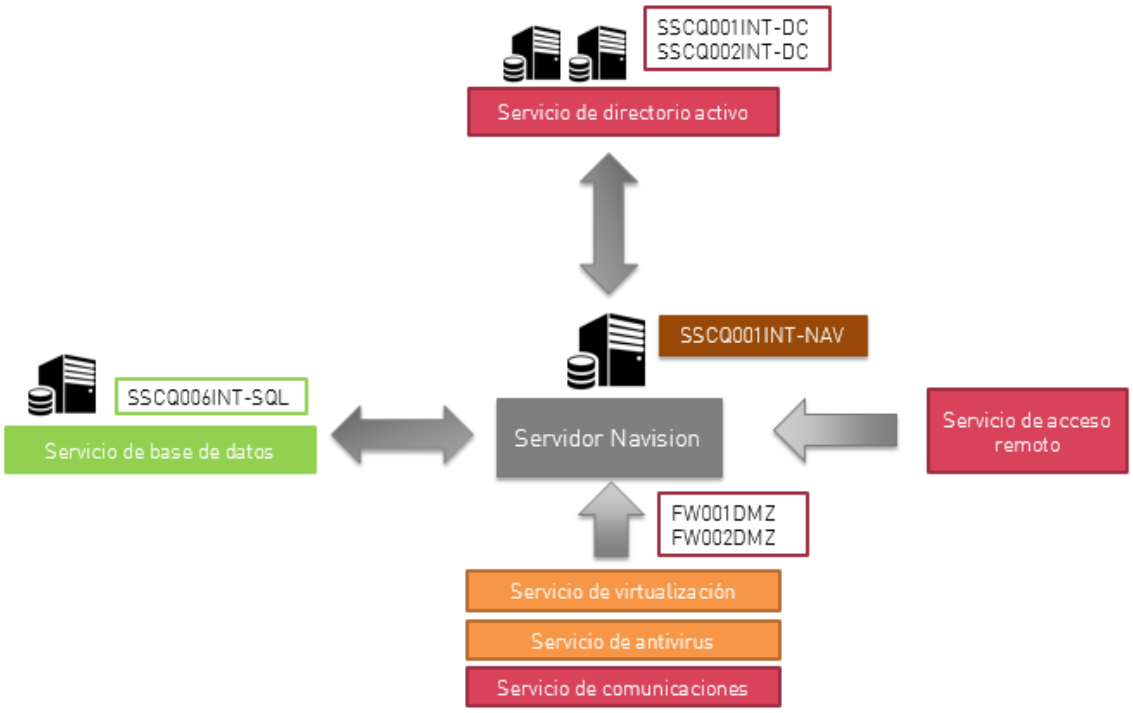

Figura 4.13: Modelado del servicio de gestión financiera

Navision se encuentra instalado en el servidor SSCQ001INT-NAV. Impactan de manera crítica sobre él el servicio de acceso remoto Citrix, el servicio de comunicaciones y el de directorio activo. La caída de uno de estos servicios provoca, por tanto, la caída de Navision.

Las dependencias con el servicio de virtualización y el de antivirus no son críticas.

- Modelado de servicio de base de datos (Datos de Navision y de Citrix)

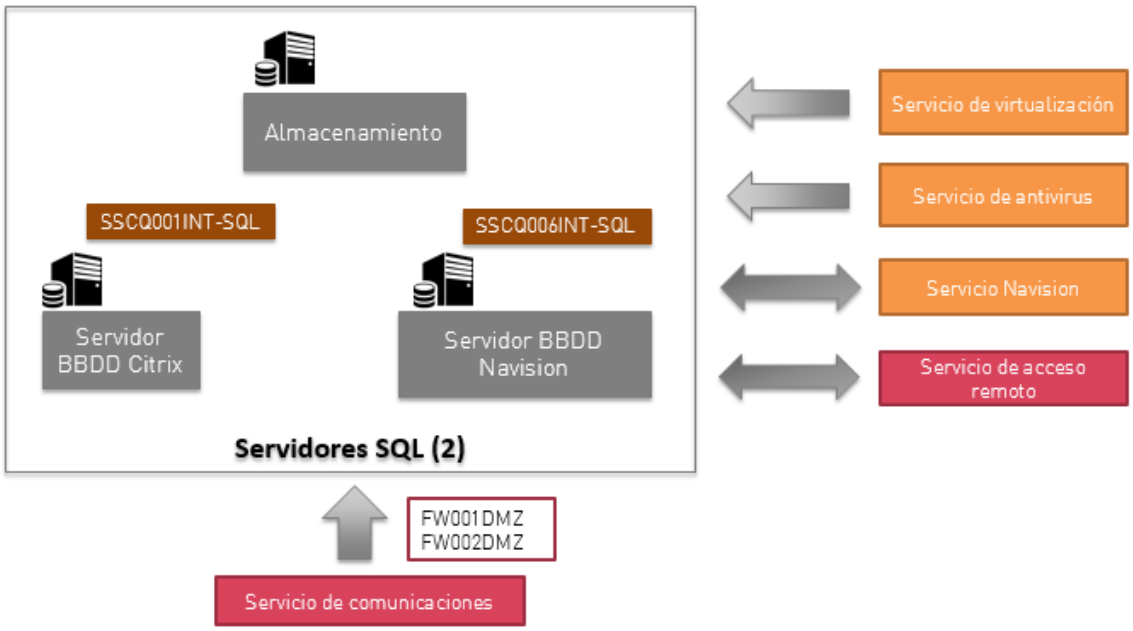

Figura 4.14: Modelado del servicio de base de datos

La base de datos de Citrix se encuentra en el servidor SSCQ001INT-SQL y la base de datos de Navision en el servidor SSCQ006INT-SQL.
Si fallan el servicio de acceso remoto o el de comunicaciones, no se podrá acceder a los datos almacenados en las bases de datos.

- Modelado del servicio de acceso remoto (Citrix)

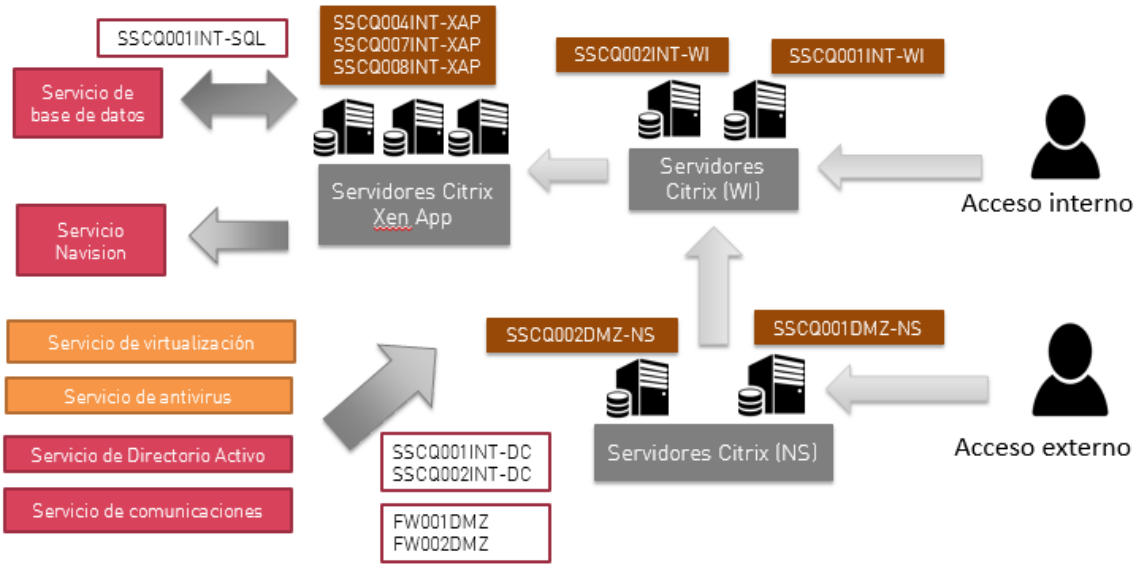

Figura 4.15: Modelado del servicio de acceso remoto

El servicio de acceso remoto se compone de 3 servidores Xen App (SSCQ004INT-XAP, SSCQ007INT-XAP y SSCQ008INT-XAP), 2 servidores Web Interface para el acceso interno desde la red de Ozona (SSCQ002INT-WI y SSCQ001INT-WI) y 2 servidores NetScaler para el acceso externo de usuarios.

La indisponibilidad de los servicios de comunicaciones, directorio activo y base de datos implican la indisponibilidad del servicio de acceso remoto.

4.5.5. Plan de Continuidad y Procedimientos de Recuperación

El Plan de Continuidad de Negocio permite a Ozona responder a un incidente y garantizar tanto la seguridad del personal, como la continuidad de las operaciones de negocio, en caso de que dichos incidentes impidan el acceso a las instalaciones o impacten de alguna forma en la entrega de servicios.
Los objetivos del Plan de Continuidad de Negocio son, por tanto:

- Asegurar que el personal está lo más a salvo y seguro posible.
- Determinar qué ha ocurrido.
- Determinar el impacto del incidente.
- Decidir el nivel de escalado requerido.
- Identificar los roles y responsabilidades de los usuarios del Plan, y aquellos con autoridad para invocarlo.
- Gestionar la respuesta que permita al negocio la reanudación de los servicios lo antes posible y el regreso gradual a la normalidad de las operaciones, dentro de las ventanas de tiempo acordadas.
- Proporcionar procesos y procedimientos basados en las estrategias de Continuidad de Negocio definidas en el documento.

Los Procedimientos tienen como objetivo especificar las acciones necesarias para llevar a cabo una tarea concreta.

Metodología

La metodología que se seguirá para la elaboración del Plan de Continuidad consiste en elaborar el conjunto de acciones a realizar una vez que se detecta que la empresa se encuentra en un escenario de riesgo que compromete la disponibilidad de sus actividades críticas. Estas acciones tendrán un responsable determinado que debe encargarse de su realización.

Durante el tiempo que se prolongue el incidente que ha causado la activación del Plan, debe realizarse un seguimiento y documentar detalladamente la sucesión de hechos que ocurran.

El Plan invocará, a su vez, los Planes o Procedimientos que correspondan.

El Plan de Continuidad es la salida directa de la que dispone el usuario final del SGCN. Para cada uno de los escenarios de riesgo planteados, se establecen una serie de acciones a realizar.

Debido a la extensión del Plan de Continuidad, en este documento sólo se mostrarán las acciones asociadas a un escenario a modo de ejemplo. El Plan completo se presenta como anexo en esta memoria.

En la Tabla 4.12 se muestran las acciones para el escenario de *indisponibilidad de Navision*:

Ref.	Acción	Responsable
Confirmación del evento		
601	**INFORMAR.** Una vez que se detecta la indisponibilidad de Navision, será necesario que se envíe un comunicado a todo el personal para notificar que existe un problema en el sistema y que se está revisando.	Responsable del sistema
602	**EVALUAR.** Debe realizarse una evaluación de lo que ocurre: cuándo falla, cuál es el origen,…	Responsable del sistema
603	**ACTIVAR.** Una vez que se conocen los detalles del incidente que afecta a Navision, debe activarse el DRP en las condiciones apropiadas	Responsable del sistema
604	**INFORMAR.** Cuando el sistema se restaure será necesario informar a todo el personal.	Responsable del sistema
605	**DOCUMENTAR.** Una vez resuelto el incidente, deberá generarse un documento detallado que describa la situación inicial y solución aplicada	Responsable del sistema
606	**MEJORAR.** Con los resultados obtenidos tras la solución del incidente, deberá revisarse la efectividad del DRP, identificando posibles acciones de mejora.	Dirección

Tabla 24: Plan de Continuidad elaborado para el escenario de indisponibilidad de Navision

Como se observa en las acciones definidas en el Plan de Continuidad, para el escenario de *indisponibilidad de Navision* es necesaria la activación del DRP, que se formaliza mediante un procedimiento técnico que describe los pasos que es necesario realizar para recuperar la infraestructura IT de los servicios críticos de Ozona.

Este procedimiento se organiza en bloques de tareas (Tablas 4.13, 4.14, 4.15 y 4.16) que se realizarán de forma secuencial, especificadas con el detalle técnico relativo a la infraestructura, con el tiempo estimado de realización, los recursos necesarios y con la identificación del rol específico requerido para llevar las tareas a cabo:

B1: BLOQUE 1		
Perfiles requeridos: 1 Perfil Técnico de Virtualización	Requisitos para ejecutarlo: • Snapshots de servidores	Tiempo estimado de ejecución: 45 minutos
VERIFICACIÓN DIRECTORIO ACTIVO Y RECUPERACIÓN DE MÁQUINAS VIRTUALES Detalle del procedimiento técnico: 1. Verificar que la máquina de Directorio Activo de Azure se ha establecido como controlador principal y que funciona correctamente (SSCQ002INT-DC). 2. Recuperar servidores de BBDD (Levantar snapshot de los servidores SSCQ001INT-SQL, SSCQ006INT-SQL) 3. Recuperar servidores de Antivirus (Levantar snapshot del servidor SSCQ001INT-CVM). 4. Recuperar servidores de Acceso Remoto (pueden arrancarse en paralelo): 2.1. Servidor de XenApp y Bróker de conexiones. Se copiará y arrancará al menos uno de los servidores (Levantar snapshot de los servidores SSCQ004INT-XAP, SSCQ007INT-XAP, SSCQ008INT-XAP). 2.2. Servidor de acceso interno: se copiará al menos una de las máquinas y se arrancará (Levantar snapshot de los servidores SSCQ001INT-WI, SSCQ002INT-WI). 2.3. Servidor de acceso externo: se copiará al menos una de las máquinas y se arrancará (Levantar snapshot de los servidores SSCQ001DMZ-NS, SSCQ002DMZ-NS). 5. Recuperar servidor de Veeam Backup (Levantar snapshot del servidor SSCQ001VBM). 6. Recuperar servidor de Navision (Levantar snapshot del servidor SSCQ001INT-NAV).		

Tabla 25: Bloque 1 de acciones del DRP

B2: BLOQUE 2		
Perfiles requeridos: 1 Perfil Técnico de bases de datos (SQL Server) y backup (Veeam Backup)	Requisitos para ejecutarlo: • Ficheros de backup	Tiempo estimado de ejecución: 3 horas

Detalle del procedimiento técnico: 1. Recuperar el último backup de cada instancia de BBDD requerida por los servicios (pueden realizarse en paralelo): 3.1. Instancia XenApp sobre el servidor SSCQ001INT-SQL. 3.2. Instancia DB_WEBNAV sobre SSCQ006INT-SQL.

Tabla 26: Bloque 2 de acciones del DRP

B3: BLOQUE 3		
Perfiles requeridos: 1 perfil técnico de acceso remoto	Requisitos para ejecutarlo: • Checklist de pruebas	Tiempo estimado de ejecución: 30 minutos
Prueba funcional acceso remoto: 1.- Verificar que los usuarios consiguen conectarse a la granja Citrix desde dentro de la red de Ozona 2.- Verificar que los usuarios consiguen conectarse a la granja Citrix desde fuera de la red de Ozona 3.- Verificar que, una vez conectado, consigue lanzarse la conexión a Navision 4.- Verificar que se cargan correctamente los perfiles de usuario 5.- Verificar que se mapean las unidades de disco de usuario que correspondan 6.- Verificar que se mapean las impresoras de usuario y que se puede imprimir desde ellas 7.- Verificar que cargan correctamente las políticas de seguridad		

Tabla 27: Bloque 3 de acciones del DRP

B4: BLOQUE 4		
Perfiles requeridos: Especialista funcional Navision	Requisitos para ejecutarlo: • Checklist de pruebas	Tiempo estimado de ejecución: 45 minutos
Prueba funcional acceso a Navision: 1.- Revisión de movimientos de Proyectos en todas las empresas 2.- Revisión de movimientos contables en todas las empresas 3.- Revisión proyectos todas las empresas 4.- Revisión Pedidos, última factura de compras y última factura de ventas de todas las empresas 5.- Revisión de últimas hojas de horas 6.- Prueba de verificación de impresión desde impresoras de administración		

Tabla 28: Bloque 4 de acciones del DRP

4.5.6. Pruebas

El Plan de Pruebas (referido en la norma con el término Plan de Ejercicios y Testing), tiene como objetivos principales:

- Evaluar los Planes de Continuidad y de Recuperación.
- Establecer una duración precisa y realista de las actividades descritas en el Plan de Continuidad.
- Infundir confianza en los equipos, que comprueban la eficacia de los planes que elaboran.
- Identificar áreas de mejora en el plan, estrategia, procesos, contenidos y recursos.
-

Metodología

Para la elaboración del Plan de Pruebas se realizarán las siguientes tareas:

1. Definición del alcance de las pruebas: qué escenarios del Plan de Continuidad se van a evaluar.
2. Determinación de las fechas de realización de las pruebas.
3. Identificación de los requisitos previos que deben cumplirse antes de comenzar las pruebas.
4. Definición de los roles y responsables en el proceso de realización de las pruebas.
5. Descripción detallada de las pruebas a realizar.

Por último, una vez realizadas las pruebas deberán documentarse los resultados, registrando cualquier incidente o suceso anómalo ocurrido.

Resultados

En las Figuras 4.15 y 4.16 se muestra la planificación realizada para las pruebas a realizar sobre los Planes de Continuidad y Recuperación del SGCN. Se han planificado todas las pruebas a realizar, aunque el alcance de este proyecto sólo incluirá la realización de la primera prueba:

	PLAN DE DISASTER RECOVERY				
	Planes que se incluyen en la prueba y tipo de prueba a realizar		Roles que intervienen y tipo de participación		
	DRP	Plan de comunicación	Dirección	Áreas de negocio	Proveedores
Febrero 2017	B				
Agosto 2017	B	A			
Febrero 2018	C	B	1	1	
Agosto 2018	C	B	2	2	1
Agosto 2019	C	C	3	3	2
Agosto 2020	C	C	3	3	3

Figura 4.16: Planificación para pruebas del DRP

	PLAN DE CONTINUIDAD DE NEGOCIO					
	Planes que se incluyen en la prueba y tipo de prueba a realizar			Roles que intervienen y tipo de participación		
	Evacuación	Plan de comunicación	Plan de continuidad de negocio	Dirección	Áreas de negocio	Proveedores
Febrero 2017						
Agosto 2017			A			
Febrero 2018	B	B	B	1	1	
Agosto 2018	C	B	B	2	2	1
Agosto 2019	C	B	C	3	3	2
Agosto 2020	C	C	C	3	3	3

Figura 4.17: Planificación para pruebas del Plan de Continuidad

Los tipos de pruebas contemplados en el Plan se especifican a continuación:

- Tipo A - Prueba básica (ejercicio en sala, se reúne un grupo y se simula un escenario).
- Tipo B - Prueba intermedia (se simula, una activación sin hacer uso completo de todos los recursos de respaldo e involucrando a los roles que tienen papeles relevantes dentro del plan).
- Tipo C - Prueba completa (se simula, una activación real, involucrando a todo tipo de participantes).

Respecto a los grados de responsabilidad de cada rol implicado, se distinguen los siguientes tipos:

- Tipo 1: el rol es informado y recibe notificaciones.
- Tipo 2: el rol tiene asignadas actividades de despacho, llamadas, respuesta a mails, etc.
- Tipo 3: el rol tiene asignadas actividades de todo tipo y participa durante todo el tiempo de ejecución de la prueba.

La prueba a realizar que se incluye en el alcance de este proyecto engloba únicamente el DRP. Como se indica en la Tabla 4.16 la prueba del Plan de Continuidad completo no se realizará hasta el mes de Agosto, momento en que el SGCN tendrá un nivel de madurez suficiente para realizar una evaluación de su eficacia completa.

El proceso de prueba del DRP se especifica en la Tabla 4.17:

Prueba Nº	Descripción de la Prueba	Duración estimada
1	Contacto con el responsable de activación del plan	20 minutos
2	Decisión de activación del plan	10 minutos
3	Contacto con personal técnico	30 minutos
5	Verificación directorio activo: Verificar que la máquina de Directorio Activo de Azure se ha establecido como controlador principal y que funciona correctamente (SSCQ002INT-DC).	15 minutos
6	Recuperación de máquinas virtuales	15 minutos

7	Actualizar el DNS	20 minutos
	Copiar imagen de los servidores e ir arrancándolos en el siguiente orden:	-
8	**Directorio Activo**. Se copiará al menos una de las máquinas y se arrancará (SSCQ001INT-DC, SSCQ002INT-DC)	30 minutos
9	**Servidores de DDBB**. • Recuperación de los servidores de DDBB (SSCCQ001INT-SQL, SSCQ009INT-SQL, SSCQ006INT-SQL) • Recuperación del último backup de cada instancia de DDBB requerida por los servicios (pueden realizarse en paralelo): o Instancia XenApp sobre el servidor SSCCQ001INT-SQL o Instancia DB_WEBNAV sobre SSCQ006INT-SQL	3 horas
10	**Servidores Antivirus** (SSCQ001INT-CVM)	30 minutos
11	**Servidores de acceso remoto** (se pueden arrancar en paralelo) • Servidor de Xen App y Bróker de conexiones. Se copiará y arrancará al menos uno de los servidores (SSCQ004INT-XAP, SSCQ007NT-XAP, SSCQ008INT-XAP) • Servidor de acceso interno. Se copiará al menos una de las máquinas y se arrancará (SSCQ001INT-WI, SSCQ002INT-WI) • Servidor de acceso externo. Se copiará al menos una de las máquinas y se arrancará (SSCQ001DMZ-NS, SSCQ002DMZ-NS)	30 minutos
12	**Servidor de Navision** (SSCQ001INT-NAV)	30 minutos
13	**Validaciones** mediante checklists para acceso remoto	30 minutos
14	**Validaciones** mediante checklists para Navision	45 minutos

Tabla 29: Especificación de las actividades a realizar para la prueba del DRP

Cabe destacar que las pruebas 1-3 pertenecen al flujo de acciones definidas en el DRP y que son previas a la activación de éste último, tal y como refleja la Tabla 4.12 de descripción del Plan de Continuidad para el escenario de *indisponibilidad de Navision*.

Resultados de la prueba

Los resultados de la prueba del DRP tuvieron resultados positivos, garantizando la eficacia de éste. En la Tabla 4.18 se muestra el informe generado:

Prueba Nº	Duración estimada	Hora inicio	Hora fin	Duración real	Resultado
1	20 minutos	10:05	10:10	12 minutos	Correcto ☒ Error ☐
2	10 minutos	10:10	10:12	2 minutos	Correcto ☒ Error ☐
3	30 minutos	10:15	11:33	2 minutos	Correcto ☒ Error ☐
4	60 minutos	11:10	11:59	15 minutos	Correcto ☒ Error ☐
5	25 minutos	12:09	12:32	20 minutos	Correcto ☒ Error ☐
6	15 minutos	12:32	13:41	12 minutos	Correcto ☒ Error ☐
7	20 minutos	13:41	14:00	15 minutos	Correcto ☒ Error ☐
8	30 minutos	14:00	14:13	20 minutos	Correcto ☒ Error ☐
9	3 horas	14:13	17:00	2 horas 50 minutos	Correcto ☒ Error ☐
10	30 minutos	17:03	17:35	32 minutos	Correcto ☒ Error ☐
11	30 minutos	17:36	18:06	30 minutos	Correcto ☒ Error ☐
12	30 minutos	18:10	18:40	30 minutos	Correcto ☒ Error ☐
13	30 minutos	18:45	19:15	30 minutos	Correcto ☒ Error ☐
14	45 minutos	19:15	19:45	30 minutos	Correcto ☒ Error ☐
GLOBAL	7 horas 40 minutos	10:05	17:10	5 horas 9 minutos	Correcto ☒ Error ☐

Tabla 30: Resultados de las pruebas del DRP

Como comentarios relevantes sobre las pruebas:

- Pruebas 1, 2 → No se consigue contactar en la primera llamada con Raquel Porciúncula (responsable de activación del Plan), por lo que se contacta a Uxía Fernández (responsable delegada de activación del Plan).

4.6. Cláusula 9: Monitorización y Revisión

La cláusula 9 establece los requisitos mínimos para medir el rendimiento de la gestión de continuidad, su cumplimiento con la propia norma y con las expectativas establecidas.

Las medidas de rendimiento seleccionadas serán el medio para la determinación del éxito o fallo del SGCN. Los objetivos de la monitorización en el contexto de un sistema de gestión incluyen:

- Evaluación de la eficacia de los procedimientos.

- Verificación de cumplimiento de los requisitos impuestos por el estándar.
- Suministro de una fuente de información para las distintas revisiones del sistema con el fin de favorecer la toma de decisiones y justificar la necesidad de mejoras.

4.6.1. Identificación de indicadores

La norma ISO 22301 no identifica lo que debe ser medido o monitorizado, esta es una tarea que debe realizar la organización en función de sus necesidades.

Metodología

Para definir las métricas de rendimiento e indicadores la organización debe determinar:

- Qué va a ser medido.
- Método de medición.
- Frecuencia de medición.
- Planificación del análisis de los resultados.

Las métricas definidas seguirán la regla conocida como SMART, por sus siglas en inglés, lo que implica que serán:

- Específicas: definidas de forma clara y concreta, evitando posibles ambigüedades.
- Medibles: se cuantifican y pueden compararse con otros datos. Es posible realizar un análisis estadístico.
- Alcanzables: razonables y aceptables tanto en términos temporales, como en el propio contexto en que se encuentra implementado el SGCN.
- Realistas: está alineado con los objetivos de la organización y con un coste aceptable en relación a los recursos requeridos.

Resultados

Para la monitorización del SGCN de Ozona se han definido una serie de objetivos globales que se listan a continuación:

- Objetivo 1: Política de Continuidad de Negocio comunicada.
- Objetivo 2: Asegurar la adecuación de los Planes de Continuidad.
- Objetivo 3: Asegurar la mejora continua del Sistema de Gestión.
- Objetivo 4: Ser la primera PYME de España y Portugal en lograr la certificación ISO 22301.

Para cada uno de estos propósitos generales se identificarán una serie de objetivos específicos. Cada uno de ellos tendrá un indicador asociado, con unos valores a alcanzar y una frecuencia de seguimiento determinada:

Objetivo Específico 1.1 Política de CN comunicada a todos los empleados	
Descripción	La política de continuidad de negocio debe ser comunicada a todo el personal de Ozona y a todas las demás partes interesadas. Se realizará una encuesta personal, dado el bajo número de empleados de la empresa, para garantizar que todos ellos la conocen.
Indicador	% del personal conocedor de la política.
Valor objetivo	100% del personal interno que participa del sistema de gestión informado al fin de la implantación (estimada Septiembre 2017).
Seguimiento	Trimestral

Tabla 31: Especificación del Objetivo Específico 1.1

Objetivo Específico 1.2 Política de CN comunicada a todos los colaboradores habituales	
Descripción	La política de continuidad de negocio debe ser comunicada a todo el personal de Ozona y a todas las demás partes interesadas. Se realizará una encuesta personal, dado el bajo número de personas involucradas, para garantizar que todos ellos la conocen.
Indicador	% del personal conocedor de la política.
Valor objetivo	100% de colaboradores habituales y proveedores que participan del sistema de gestión informado al fin de la implantación (estimada Septiembre 2017).
Seguimiento	Trimestral

Tabla 32: Especificación del Objetivo Específico 1.2

Objetivo Específico 2.1 Asegurar que el Programa de Ejercicios es suficiente y se cumple	
Descripción	El programa incluye ejercicios que prueban todos los elementos relevantes y sus interrelaciones a lo largo del año.
Indicador	Pruebas planificadas y realizadas de los planes de continuidad y del DRP.
Valor objetivo	Deberá haber una prueba, al menos de tipo B, de los planes de continuidad y del DRP antes de finalizar el ciclo de implantación.
Seguimiento	Trimestral

Tabla 33: Especificación del Objetivo Específico 2.1

Objetivo Específico 3.1 Asegurar la mejora continua de los Planes de Continuidad	
Descripción	Para asegurar la mejora continua de los planes y del sistema de gestión, se debe garantizar que los ejercicios y pruebas realizados se analizan y documentan, que los planes se revisan para incorporar el posible feedback obtenido y que las acciones identificadas se analizan y planifican cuando procede.

Indicador	Informes de pruebas y revisiones de los planes después de haberlas realizado.
Valor objetivo	100% de ejercicios realizados tienen informes documentados 15 días después de su realización. 100% de los planes revisados 1 mes después de emitido el informe. 100% de mejoras identificadas analizadas y planificadas, si procede, en los 3 meses siguientes a la emisión del informe.
Seguimiento	Trimestral

Tabla 34: Especificación del Objetivo Específico 3.1

Objetivo Específico 3.2 Asegurar la mejora continua del Sistema de Gestión	
Descripción	Para asegurar la mejora continua del sistema de gestión, se debe garantizar que las auditorías internas planificadas son realizadas y que las acciones, correctivas y de mejora, identificadas se analizan y planifican cuando procede.
Indicador	Auditorías internas y externas realizadas.
Valor objetivo	Durante 2017 se prevé la realización de 2 auditorías internas y 1 externa. 100% de mejoras identificadas analizadas y planificadas, si procede, en los 3 meses siguientes a la emisión del informe.
Seguimiento	Trimestral

Tabla 35: Especificación del Objetivo Específico 3.2

Objetivo Específico 4.1 Sistema de Gestión Integrado ISO 22301 + ISO 20000 + ISO 27001	
Descripción	El objetivo en 2017 será la certificación ISO 22301.
Indicador	Certificado.
Valor objetivo	Obtención de la certificación.
Seguimiento	Puntual, tras la auditoría de certificación.

Tabla 36: Especificación del Objetivo Específico 4.1

Una vez especificados los objetivos, se realiza el seguimiento con los siguientes resultados:

Objetivo 1.1: Empleados del Grupo Ozona con conocimientos de la política de CN						
Resultados	Q1	Q2	Q3	Q4	TOTAL	OBJETIVO
Personal consultoría ES	7	0	0	0	7	7
Personal consultoría PT	2	0	0	0	2	4
Personal tecnología ES	3	0	0	0	3	10
Personal tecnología PT	0	0	0	0	0	2
Comentarios	El personal de consultoría fue informado durante el kick off 2017 realizado en Enero.					

	Del área de tecnología, por el momento, solo las personas involucradas en el proyecto (RAY, CSS y FVV) han sido informadas de la política. Se espera realizar una acción de comunicación en el próximo evento conjunto los días 9 y 10 de Junio de 2017.
Análisis del cumplimiento	Si se realiza lo planificado, se llegará a la fecha objetivo con el objetivo cumplido.

Tabla 37: Informe de seguimiento del Objetivo Específico 1.1

Objetivo 1.2: Política de CN comunicada a todos los colaboradores habituales						
Resultados	Q1	Q2	Q3	Q4	TOTAL	OBJETIVO
Colaboradores externos	4	0	0	0	4	4
Proveedor R	0	0	0	0	0	1
Proveedor Arbentia	0	0	0	0	0	1
Comentarios	Filipe Martins y Susana Naveira fueron informados durante el kick off 2017 realizado en Enero. Cristina Pardo y Rafa García fueron informados durante la elaboración del BIA R y Arbentia serán informados una vez que todos los empleados estén informados; previsto Julio 2017.					
Análisis del cumplimiento	Si se realiza lo planificado, se llegará a la fecha objetivo con el objetivo cumplido.					

Tabla 38: Informe de seguimiento del Objetivo Específico 1.2

Objetivo 2.1: Asegurar que el Programa de Ejercicios es suficiente y se cumple						
Resultados	Q1	Q2	Q3	Q4	TOTAL	OBJETIVO
Ejercicios de tipo B de los planes de continuidad planificados	0	0	1	0	1	1
Ejercicios de tipo B del DRP planificados	1	0	0	0	1	1
Ejercicios de tipo B del DRP realizados	1	0	0	0	1	1
Ejercicios de tipo B de los planes de continuidad realizados	0	0	0	0	0	1
Comentarios	-					
Análisis del cumplimiento	Se deberá garantizar que se realiza el ejercicio planificado para Agosto de 2017.					

Tabla 39: Informe de seguimiento del Objetivo Específico 2.1

Como ya se detalló en el apartado 4.5.6., sólo se ha realizado la prueba del DRP. No obstante, la prueba del Plan de Continuidad completo sí está planificada.

Objetivo 3.1: Asegurar la mejora continua de los Planes de Continuidad						
Resultados	Q1	Q2	Q3	Q4	TOTAL	OBJETIVO
Ejercicios realizados con informe documentado a tiempo	1	0	0	0	1	2
Planes revisados a tiempo después de un ejercicio	1	0	0	0	1	2
Mejoras analizadas y planificadas cuando procede	0	0	0	0	0	0
Comentarios	El objetivo de acciones de mejora podrá cambiar a medida que se realicen informes que las identifiquen.					
Análisis del cumplimiento	Por el momento va todo según lo previsto, habrá que garantizar que todo funciona correctamente una vez realizado el ejercicio de Agosto.					

Tabla 40: Informe seguimiento del Objetivo Específico 3.1

El objetivo de documentar el informe de los ejercicios y revisar los planes no se cumple totalmente porque el Ejercicio correspondiente al Plan de Continuidad todavía no se ha llevado a cabo.

Objetivo 3.2: Asegurar la mejora continua del Sistema de Gestión						
Resultados	Q1	Q2	Q3	Q4	TOTAL	OBJETIVO
Auditorías internas realizadas	1	0	0	0	1	2
Auditorías externas realizadas	0	0	0	0	0	1
Acciones correctivas implementadas	0	0	0	0	0	0
Acciones de mejora analizadas y planificadas cuando procede	0	0	0	0	0	0
Comentarios	El objetivo de acciones correctivas y de mejora podrá cambiar a medida que se realicen informes que las identifiquen.					
Análisis del cumplimiento	Por el momento va todo según lo previsto, habrá que garantizar que se realizan las restante auditorías planificadas y las acciones correctivas que se identifiquen.					

Tabla 41: Informe de seguimiento del Objetivo Específico 3.2

Objetivo 4.1: Sistema de Gestión Integrado ISO 22301 + ISO 20000 + ISO 27001	
Análisis de cumplimiento global	RESULTADO
Se ha planificado la auditoría de certificación en Octubre de 2017, junto con los sistemas de gestión ISO 20000 e ISO 27001 ya certificados.	NO

Tabla 42: Informe de seguimiento del Objetivo Específico 4.2

4.6.2. Auditoría interna

El objetivo de la auditoría interna es proporcionar a la organización información sobre el nivel de cumplimiento conforme a la norma en que se encuentra y recomendaciones para mejorar el sistema. La auditoría interna es realizada por la organización en sí misma.

Metodología

Para la realización de la auditoría se utilizará una herramienta interna de Ozona. En esta herramienta se encuentran los requisitos incluidos en la norma. El auditor deberá indicar el grado de conformidad de cada requisito en función de las evidencias existentes en el sistema implementado. Como resultado, se generarán unas gráficas que muestran el nivel de conformidad y permiten conocer el estado actual del sistema.

En este tipo de procesos, los cuatro conceptos clave a tener en cuenta son:

- No-conformidad: aspecto de la implantación de un proceso que supone un incumplimiento total o relevante en la adecuación a los marcos de referencia y frameworks aplicados en el auditoría.
- Observación: aspecto de la implantación de un proceso que supone un incumplimiento menor o poco relevante en la adecuación a los marcos de referencia y frameworks aplicados en el auditoría.
- Punto Fuerte: aspecto de la implantación de un proceso que merece una mención específica por su alto nivel de madurez o de adecuación a los marcos de referencia y frameworks aplicados en el auditoría.
- Oportunidad de Mejora: aspecto de la implantación de un proceso que se propone mejorar pero que no tiene una correspondencia directa con un requisito de norma aunque sí habitualmente a requisitos de auditoría.

Resultados

A partir de las evidencias existentes sobre el sistema, se elabora un gráfico que resume la situación actual de conformidad con la norma ISO 22301 donde cada requisito se pondera en una escala de 0-3, donde 0 indica que no hay ninguna

evidencia en absoluto, 1 que hay alguna evidencia, 2 que hay evidencia pero no lo suficientemente conforme con todos los requisitos y 3 que cumple plenamente los requisitos. En la Figura 4.18 se muestra el resumen de cumplimiento por cláusula:

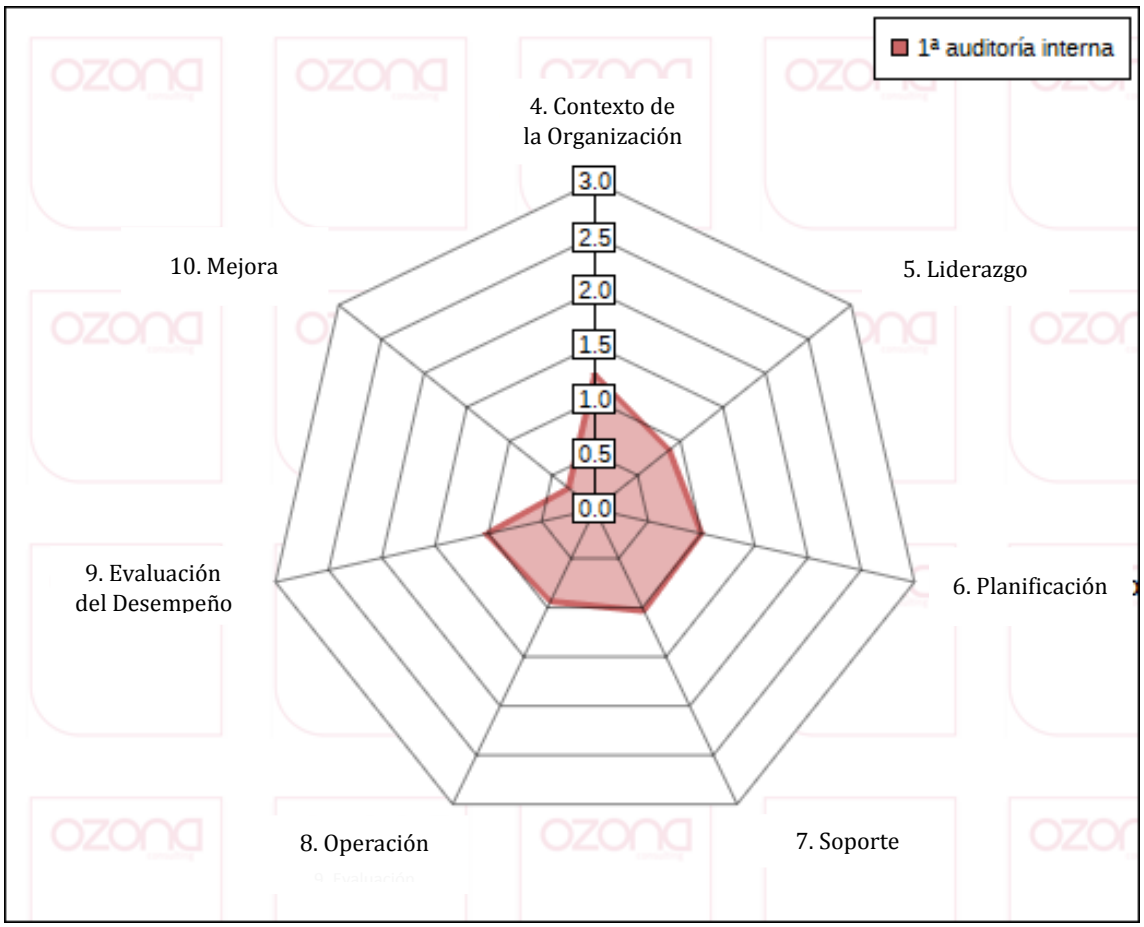

Figura 4.18: Nivel de cumplimiento por cláusula del SGCN

Como el sistema todavía está en una fase inicial de implementación, hay evidencias de todas las cláusulas pero todavía es necesaria la generación de evidencias adicionales con el objetivo de cumplir plenamente todos los requisitos.
Lógicamente, la cláusula de Mejora no tiene evidencias porque el sistema acaba de implantarse, por tanto, esto no sería una no conformidad en sí misma sino que es consecuencia de que el sistema se encuentre en una primera iteración del ciclo de vida PDCA.

El gráfico que se muestra en la Figura 4.19 presenta una visión más detallada del grado de cumplimiento en los subapartados de cada cláusula:

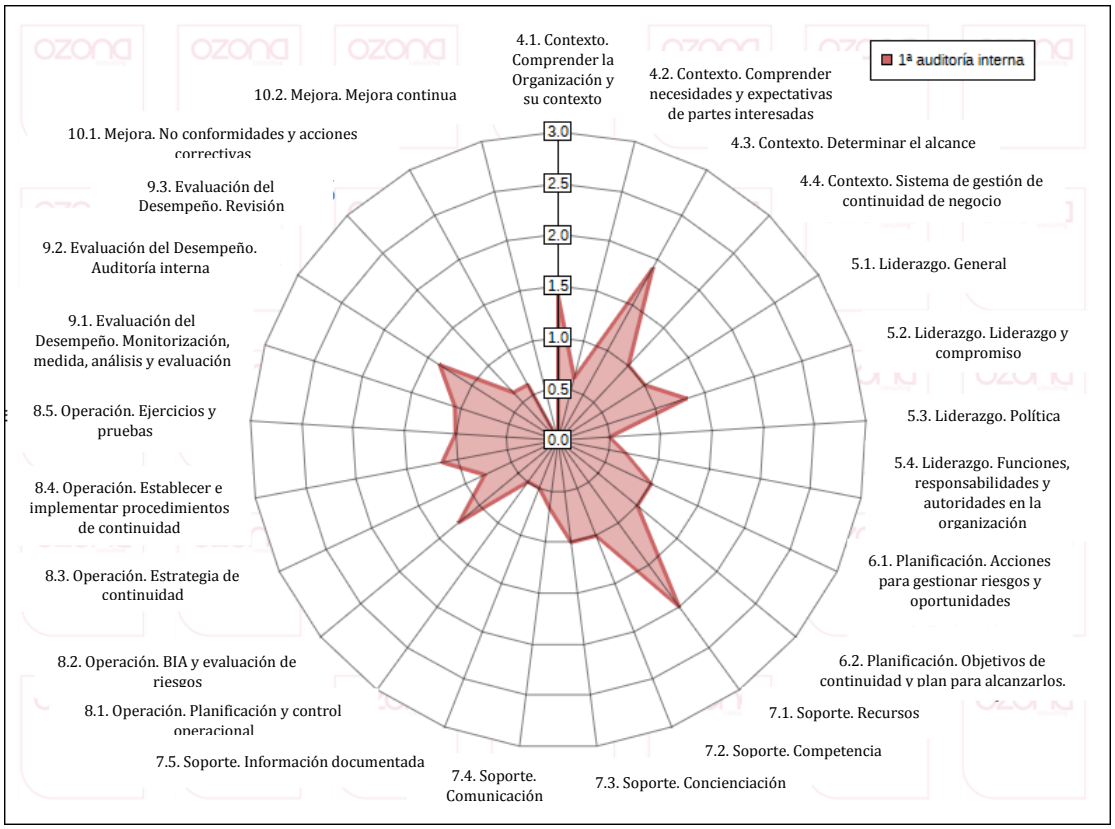

Figura 4.19: Grado de cumplimiento por subapartados de las cláusulas

Este gráfico nos proporciona información sobre la magnitud de evidencias para los requisitos de manera individual, pero para conocer el estado del SGCN de Ozona a nivel global es necesario evaluar el grado de gestión de los procesos en una escala definida. La Tabla 4.30 describe la escala de los niveles de madurez, en términos de gestión, en que pueden encontrarse los procesos, niveles definidos en la norma ISO 15504:

Nivel	Descripción
0 – Incompleto	El proceso no está implementado o falla en alcanzar su propósito.
1 – Realizado	Se implementa el proceso y alcanza sus objetivos.
2 – Gestionado	El proceso es gestionado y los productos resultantes se establecen, controlan y mantienen.
3 – Establecido	El proceso es definido y asimilado, se aplica.
4 – Predecible	El proceso es medido consistentemente en sus límites definidos.
5 – Optimizado	El proceso se mejora continuamente para cumplir los objetivos de negocio relevantes actuales y proyectados.

Tabla 43: Descripción de niveles de madurez para sistemas de gestión

Teniendo en cuenta la media de niveles obtenida a partir del estado de cada proceso, Ozona puede encontrarse en uno de los niveles de madurez detallados en la Tabla 4.31:

Nivel	Descripción
Inmadura	Ineficiencia total en la consecución de objetivos
Básica	Existe comunicación informal y escasa entre departamentos. Procesos operativos estáticos.
Gestionada	Pequeña coordinación de procesos cruzados. Surgen líderes de procesos que dinamizan procesos de forma individualizada.
Establecida	Comienza la gestión de procesos. Empieza a existir alineación con la estrategia de la organización y coordinación interdepartamental.
Predecible	Total integración de procesos. Acuerdo de mejora continua de los procesos. Alineamiento con la estrategia corporativa.
Innovadora	Procesos repetidos, medidos y evaluados continuamente. Colaboración proactiva entre divisiones para la mejora de procesos.

Tabla 44: Descripción para niveles de madurez de una organización con sistemas de gestión implantados

El gráfico de niveles de madurez por proceso obtenido en la auditoría en la Figura 4.20:

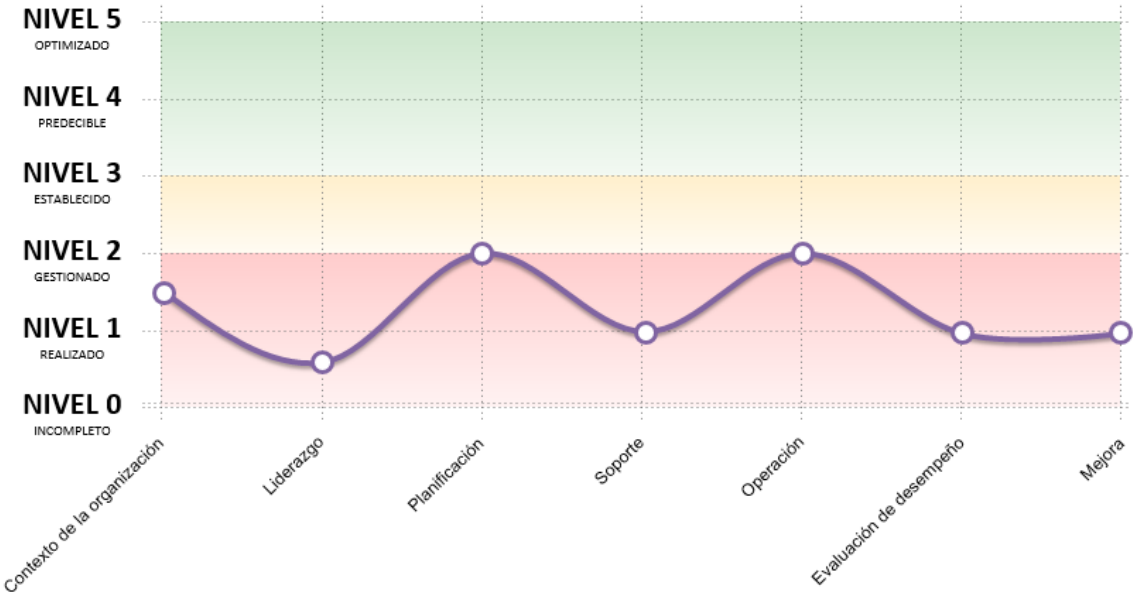

Figura 4.20: Niveles de madurez del SGCN por cláusula

Por tanto, el nivel de madurez global actual de Ozona se sitúa en *Realizado*, con una progresión creciente muy cercana al nivel siguiente de *Gestionado*. Aquí se observa de manera clara que el SGCN todavía tiene carencias en su nivel de madurez.

4.6.3. Revisiones de Alta Dirección

La Alta Dirección debe asegurarse que el sistema de gestión es revisado a intervalos planificados. En estas revisiones deben decidirse los siguientes aspectos: cambios en el alcance y mejoras a la eficacia del SGCN, modificación de la estrategia y los procedimientos de recuperación de los recursos críticos para responder a eventos que puedan tener un impacto sobre los servicios críticos, incluyendo situaciones en que se produzcan cambios en los requisitos de negocio, de resiliencia o en el nivel de riesgo, la necesidad de recursos adicionales o el ajuste de financiación o asignación presupuestaria para el sistema.

Aunque la realización de las revisiones de Alta Dirección se excede a las competencias y alcance de este TFG, debido a su criticidad como tarea de mejora del SGCN debe ser comentada.

4.7. Cláusula 10: Mejora

Cláusula 10 engloba la identificación de acciones correctivas para las no conformidades que se detecten en la fase de Evaluación del desempeño (Cláusula 9).

Los objetivos principales de la cláusula de mejora son, por tanto:

- Eliminar las causas de las no-conformidades.
- Eliminar las causas de no-conformidades potenciales.
- Mejorar la eficacia del SGCN de manera continua.

4.7.1. Identificación de Acciones Correctivas

Con los resultados de la auditoría interna, se evaluarán las no-conformidades detectadas elaborando Planes de Acción para corregirlas. Estos Planes se compondrán de una serie de Acciones Correctivas que se irán implantando en el SGCN de manera controlada, realizando un seguimiento documentado de su estado de implementación.

La elaboración de Planes de Acción se excede al alcance de este proyecto. Sin embargo, a modo de ejemplo, se han identificado algunas acciones correctivas para no-conformidades detectadas en la auditoría:

No-conformidad	Acción correctiva
No se ha podido evidenciar que existan medidas de protección de la información documentada de forma que la protejan de modificaciones o borrado no autorizado.	Documentar las medidas de protección existentes. Analizar medidas de mayor protección que puedan ser incorporadas sin un coste elevado.
No se ha evidenciado que se haya realizado una revisión por parte de la Dirección.	Levantar acta de cada revisión que se realice detallando los temas tratados en la reunión. Planificar revisiones periódicas.
No se ha mostrado evidencia de la mejora continua.	Dado que el SGCN se encuentra en la primera fase de implementación, no existen evidencias de mejora todavía. Sin embargo, como acción de mejora se propone la elaboración de un procedimiento formal de seguimiento de acciones correctivas, asegurando que se generan evidencias de las medidas implementadas.

Tabla 45: Identificación de acciones correctivas a realizar

5. Validaciones y Pruebas

En el apartado 4.5.6. se ha presentado el Plan de Pruebas y los resultados de la prueba del DRP realizada.

Adicionalmente, como validación del sistema implementado, en este capítulo se presenta una comparativa de los resultados obtenidos en el assessment inicial y en la auditoría interna.

En la Figura 5.1 se comparan los niveles de conformidad obtenidos tras la realización de ambas actividades. Como se puede observar, tras la implementación del sistema se han generado evidencias de todas las cláusulas. Únicamente existe una carencia de pruebas en la cláusula de mejora, debido a que es la primera auditoría que se realiza y, por tanto, no se ha realizado un proceso de mejora previo. Por tanto, esto quiere decir que los procesos del sistema han comenzado a documentarse formalmente y gestionarse.

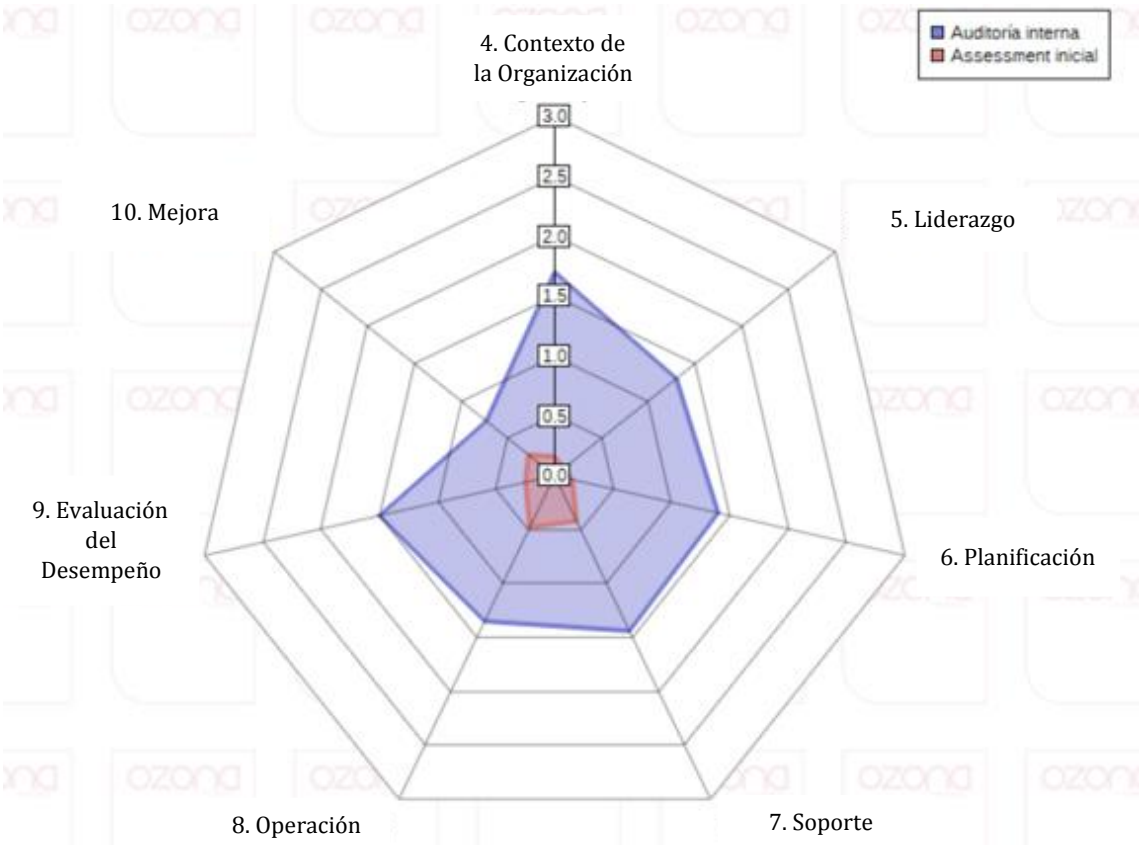

Figura 5.1: Comparativa assessment/auditoría de la conformidad con las cláusulas ISO 22301

La Figura 5.2 muestra la comparativa del grado de cumplimiento desglosada por subapartados. Se puede comprobar, de manera más clara, que el sistema implementado incorpora los requisitos contemplados en la norma y en el alcance de este proyecto, aunque su madurez o completitud no haya alcanzado los niveles aceptables para una certificación oficial.

Las cláusulas 4, 5 y 6 muestran un nivel de cumplimiento mayor respecto al resto. Esto se justifica porque el contenido de estas cláusulas tiene una mayor estabilidad que las demás, aún en el primer ciclo PDCA del SGCN. Las cláusulas 7 y 8 están en actualización constante durante las fases de implementación y, en su primera versión, es previsible que su cumplimiento sea reducido, ya que se encuentran en una fase inicial de desarrollo. La cláusula 9 sí incluye evidencias considerables por el establecimiento y seguimiento de indicadores, y la realización de la auditoría. Por último, la cláusula 10 tiene un desarrollo muy limitado dado que el sistema todavía está en su primera fase de implementación.

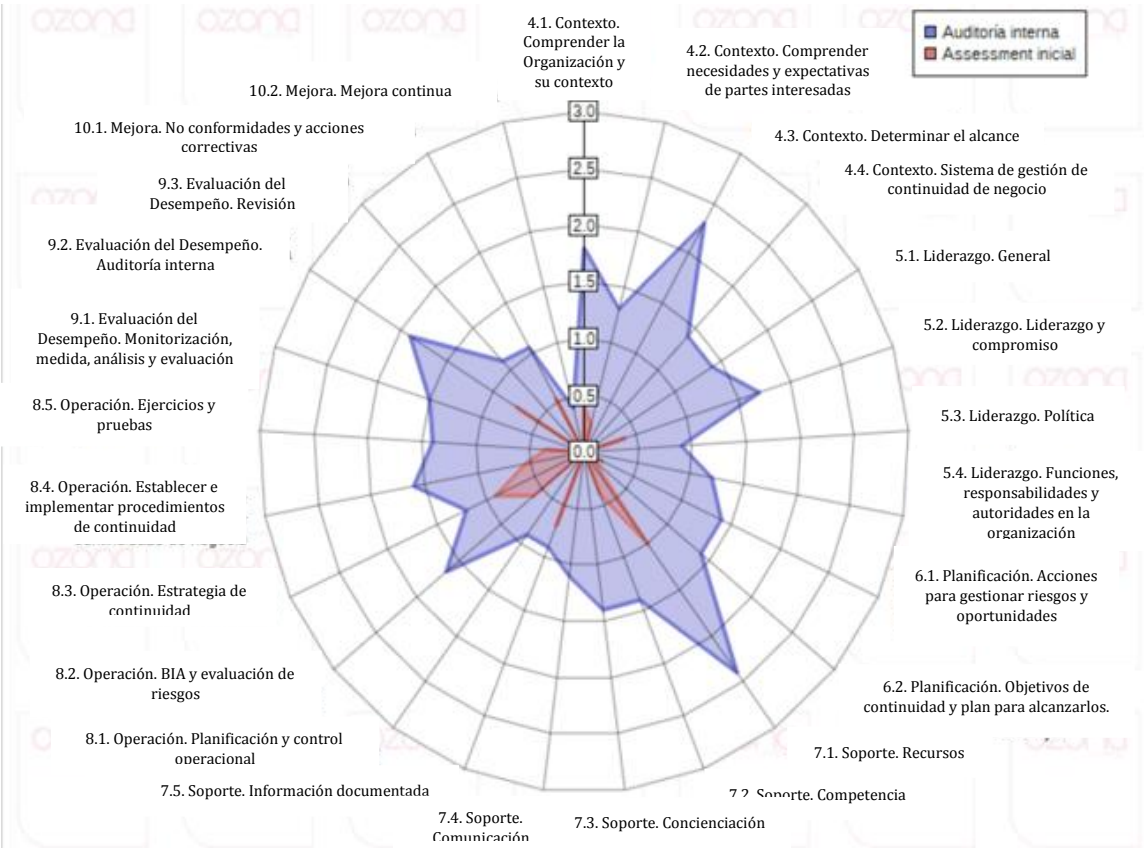

Figura 5.2: Grado de cumplimiento assessment/auditoría por subapartados de las cláusulas

Por último, la comparación de los niveles de madurez se muestra en la Figura 5.3. Todas las cláusulas alcanzan el nivel 1, es decir, se realizan. Por tanto, se puede validar que el SGCN cumple los requisitos especificados en el capítulo 3, aunque sea a un nivel básico. En varias cláusulas ya se ha alcanzado el nivel 2, es decir, los procesos comienzan a establecerse formalmente y siguiendo para su gestión los procedimientos documentados.

Es importante destacar que para aumentar el grado de madurez es necesario que pase tiempo, no es suficiente con tener evidencias de que algo se ha hecho de forma correcta una sola vez. Por ejemplo, para alcanzar un nivel 3 es necesario que una

misma actividad se haya realizado en más de una ocasión y por los plazos que se manejan en este tipo de proyectos, para algunas de las cláusulas, se requiere de varios meses.

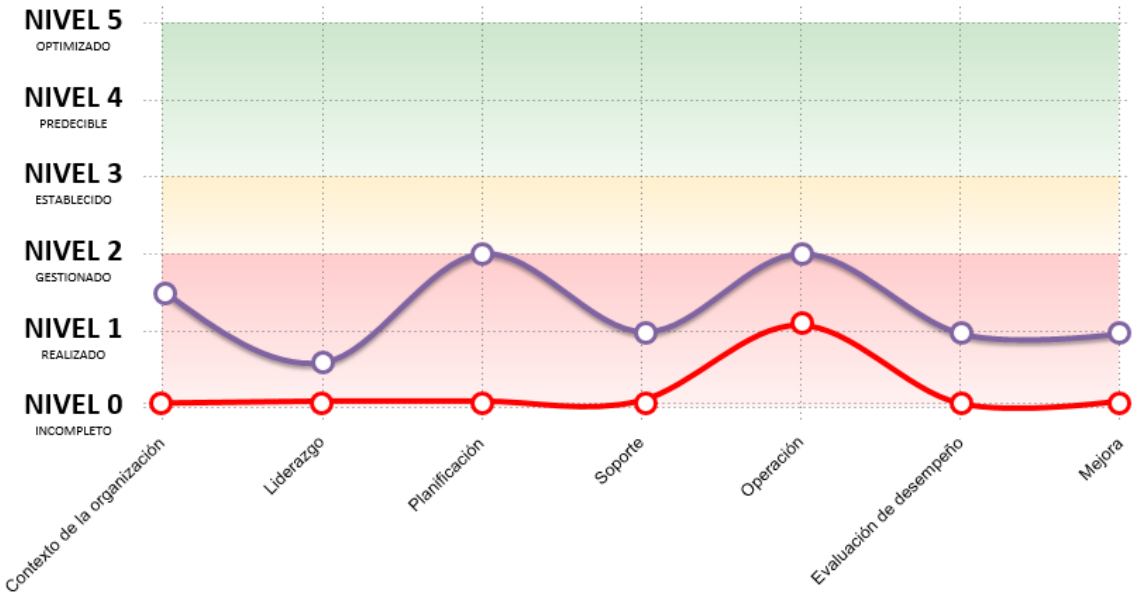

Figura 5.3: Comparativa de niveles de madurez assessment/auditoría del SGCN por cláusula

6. Conclusiones y ampliaciones

Se puede concluir, por tanto, que se han alcanzado los objetivos contemplados para este TFG, implementando un SGCN alineado con las normas ISO 22301 e ISO 27031.

Como ampliaciones inmediatas al SGCN, se implementarán las acciones correctivas identificadas tras la realización de la auditoría interna, comenzando así la segunda fase de implementación, detallada en el apartado 2.1. Se estima además que se podrá conseguir la certificación oficial de la norma en el último trimestre del año 2017.

Como perspectiva a largo plazo, el SGCN será mejorado y mantenido anualmente para conseguir un sistema más eficiente y para conservar la certificación.

Por último, y con el objetivo de enfatizar en la importancia de la continuidad de negocio, a continuación se presentan una serie de estudios que muestran datos reales sobre la relevancia de esta área y su relación con los servicios TI.

En la Figura 6.1 se muestran los resultados de una encuesta realizada por BSI a 200 empresas inglesas sobre el origen de incidentes disruptivos que afectaron a la continuidad de sus negocios. BSI es la Institución de Estándares Británicos, miembro de la ISO y participante en la elaboración de las normas internacionales asociadas a esta organización.

Eventos	2008	2009	2010	2011	2012	2015
Lluvia extrema (inundación /viento fuerte)	29	25	58	64	49	54
Ausencia de personas (debido a una enfermedad)	35	24	28	34	34	42
Pérdida de IT	43	40	35	34	39	40
Corte de telecomunicaciones	30	23	20	20	24	27
Interrupción del transporte	-	-	22	30	20	27
Imposibilidad de acceso a la instalación	16	13	22	26	20	24
Colegio/cierre de guardería	–	–	18	17	22	20
Corte de suministro eléctrico	–	–	–	–	–	20
Pérdida de las competencias clave	21	14	15	18	19	18
Interrupción de la cadena de suministro	12	9	13	19	15	14
Salud laboral & incidentes de seguridad	17	16	14	15	16	12
Salud de los clientes/incidente de seguridad del producto	7	4	6	7	7	12
Ausencia de agua/alcantarillado	–	–	6	9	8	10
Publicidad negativa/cobertura	18	14	9	11	13	10
Acción industrial	7	7	4	6	22	8
Daños en la imagen de la organización/reputación/marca	10	11	22	10	10	8
Incidente ambiental	7	7	5	7	6	6
Protesta de grupos de presión	6	7	6	6	8	6
Ciberataque	–	–	–	4	6	5
Escape de gas	–	–	–	–	–	4
Incendio	5	5	4	4	6	4
Acto terrorista	3	2	1	2	2	2

Figura 4: Encuesta de BSI sobre eventos de continuidad desde 2008 a 2015

Por una parte, el número de incidentes disruptivos es considerable, ya que se trata de incidentes que pueden comprometer la estabilidad de una empresa. Por otra, entre los primeros 5 puestos se encuentran la pérdida de sistemas TI y el corte de las telecomunicaciones. Esto quiere decir que habitualmente se producen eventos que causan interrupciones críticas en la organización a causa de fallos relacionados con las TIC.

También obtenida de un estudio de BSI, a continuación se listan amenazas relacionadas con las TIC y que están incluidas en el Top 10 de amenazas consideradas por las empresas:

1. Ciberataque
2. Violación de datos
3. Interrupciones TIC no planificadas
5. Incidente de seguridad

De las 10 amenazas principales que afectan a las empresas, 4 de ellas involucran a las TIC y se encuentran entre las 5 primeras posiciones.

La continuidad de negocio es, por tanto, clave para asegurar la supervivencia de las organizaciones, ya que presenta un medio para responder a interrupciones que afectan a sus servicios críticos. Pero también es indispensable que las organizaciones presten especial atención a sus servicios TIC al desarrollar el área de continuidad, ya que actualmente existe una dependencia muy alta de éstos y extendida a todos los sectores que supone una criticidad sobradamente justificada de manera empírica.

Por último, la Figura 6.2 pretende mostrar una última reflexión de las consecuencias que puede suponer la presencia o ausencia de la gestión de la continuidad de negocio en una organización:

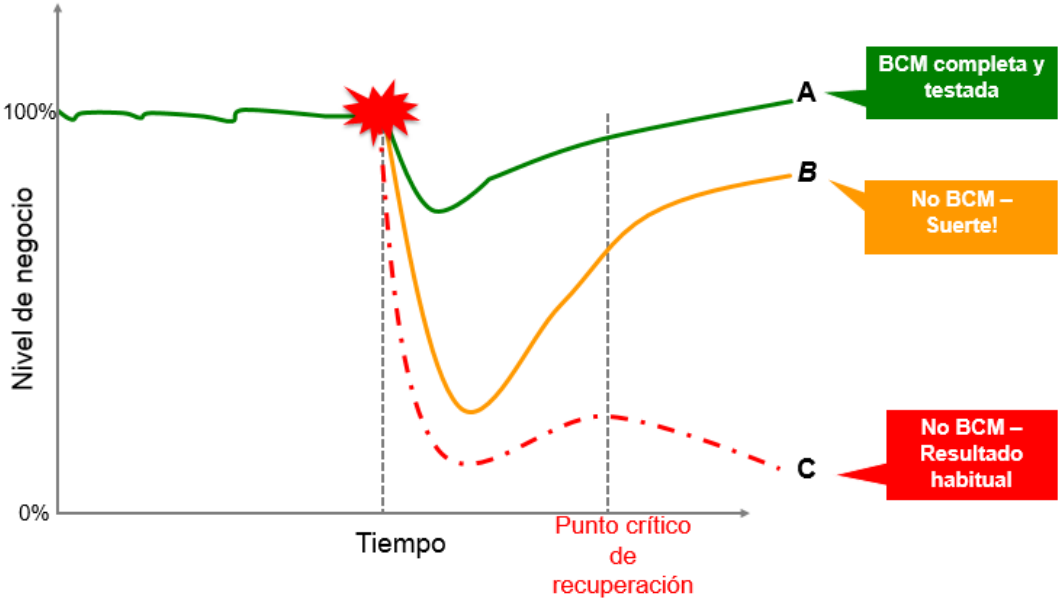

Figura 5: Consecuencias de la existencia/ausencia de gestión de continuidad del negocio para la organización

En las condiciones habituales, el nivel de negocio se mantiene con pequeñas variaciones en todas las organizaciones. Sin embargo, en caso de interrupción crítica, es muy frecuente que aquellas organizaciones sin gestión de continuidad no puedan afrontar los puntos críticos de recuperación y terminen cerrando porque son incapaces de reincorporarse en sus niveles operativos regulares. Algunas organizaciones sin gestión de continuidad sí son capaces de reanudar su actividad pero deben enfrentarse a una pendiente de recuperación muy pronunciada y extensa en el tiempo, con las pérdidas que esto supone. Por otro lado, las organizaciones que sí realizan una gestión de la continuidad consiguen recuperarse antes de los tiempos máximos de reanudación y son capaces de recuperar su nivel de negocio habitual en poco tiempo.

Apéndice A: Glosario

activación: acto de declarar que las disposiciones sobre continuidad del negocio de la organización se debe poner en marcha con objeto de continuar suministrando los productos y servicios principales. [1]

actividad crítica: actividad clave para la organización, cuya indisponibilidad tendría un impacto suficiente para comprometer la supervivencia de ésta.

Alta Dirección: persona o grupo de personas que dirige y controla una organización al más alto nivel. [1]

BIA (Análisis de Impacto en el Negocio): proceso de analizar las actividades y el efecto que una interrupción del negocio puede tener sobre éstas. [4]

apetito de riesgo: nivel y tipo de riesgo que una organización está preparada para aceptar. [1]

assessment: proceso de evaluación del estado concreto de una entidad respecto a una serie de requisitos.

auditoría: proceso sistemático, independiente y documentado para obtener pruebas de auditoría y evaluarlas objetivamente para determinar la amplitud con que se cumplen los criterios de dicha auditoría. [1]

auditoría interna: auditoría realizada por la propia organización o en su nombre, para su revisión por la dirección y para otros fines internos, y que podría constituir la base para una autodeclaración de conformidad de la organización. [1]

conformidad: cumplimiento de un requisito. [4]

continuidad de negocio: capacidad de la organización para continuar realizando la entrega de productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo. [4]

DRP (Plan de Recuperación de Desastres): plan definido y documentado formalmente para la recuperación de las capacidades TIC cuando ocurre una interrupción. [3]

ejercicio: pruebas planificadas formalmente y realizadas con el objetivo de comprobar la efectividad de los planes implementados.

incidente: situación que podría provocar o conducir a una interrupción, una pérdida, una emergencia o una crisis. [4]

IRBC (Preparación de las TIC para la Continuidad de Negocio): capacidad de una organización para soportar sus operaciones de negocio mediante la prevención, detección y respuesta a interrupciones y recuperación de sus servicios TIC. [3]

KPI (Indicador Clave de Desempeño): un indicador es una métrica para la cuantificación del nivel de rendimiento de un proceso a lo largo del tiempo.

MBCO (Objetivo Mínimo de Continuidad de Negocio): nivel mínimo de servicios y/o productos que es aceptable por la organización para conseguir sus objetivos de negocio durante una interrupción. [1]

no-conformidad: no cumplimiento de un requisito. [4]

parte interesada: persona u organización que puede afectar, ser afectada por, o percibir que ella misma puede verse afectada por una decisión o actividad. Puede tratarse de un individuo o de un grupo que tiene un interés en alguna decisión o actividad de una organización. [1]

Plan de Continuidad: procedimientos documentados que conducen a las organizaciones a responder, recuperar, reanudar y restaurar el nivel de operación predefinido después de una interrupción. [1]

procedimiento: manera específica de realizar una actividad o un proceso. [1]

proceso de negocio: conjunto de actividades interrelacionadas o interactivas que transforman las entradas en resultados. [1]

RPO (Punto Objetivo de Recuperación): período de tiempo después de un incidente, dentro del cual: se debe reanudar un producto o servicio, una actividad o dentro del que se deben recuperar los recursos. [1]

RTO (Punto de Recuperación Temporal): punto a partir del cual debe ser posible recuperar la información utilizada por una actividad, para que ésta pueda funcionar tras una interrupción. [1]

servicio TI: resultado beneficioso, soportado a partir de bienes informáticos, proporcionado por una organización a sus clientes, destinatarios o partes interesadas.

Sistema de Gestión: conjunto de elementos interrelacionados o interactivos de una organización que sirve para establecer políticas y objetivos, así como los procesos para conseguir estos objetivos. [1]

SGCN (Sistema de Gestión de Continuidad de Negocio): parte del sistema de gestión global que establece, implanta, opera, supervisa, revisa, mantiene y mejora la continuidad de negocio. Incluye la estructura de la organización, las políticas, la

planificación de actividades, las responsabilidades, los procedimientos, los procesos y los recursos. [1]

Apéndice B: Plan de Continuidad

Este Apéndice incluye el Plan de Continuidad del SGCN de Ozona, considerándolo como Manual de Usuario, ya que supone la salida directa del SGCN que será ejecutado por cualquier miembro de la organización en caso de emergencia.

Apéndice C: Bibliografía

[1] ISO 22301:2012, *Societal Security – Business Continuity Management Systems – Requirements*.

[2] St. Germain, R., Lachapelle, E. (2012). *Certified ISO 22301 Lead Implementer*. PECB.

[3] ISO/IEC 27031:2011, *Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity*.

[4] ISO 22300:2012, *Societal Security. Terminology (ISO 22300:2012)*.