Contenido

9. Plan de implantación

9.1. Migración y/o carga inicial de datos

<Lista de tablas de la base de datos y otros ficheros que hay que rellenar con datos, indicando el origen de los datos y si necesitan alguna transformación previa a la carga (lo que implicaría desarrollo de software específico para esta transformación). Los datos pueden proceder del sistema actual del cliente o ser datos fijos, como códigos postales o plantillas para mensajes preestablecidos de correo electrónico. La lista debe estar ordenada, por orden temporal de carga utilizando la integridad referencial de la base de datos.>

9.2. Manual de explotación

<El objetivo de este documento es recoger el conjunto de tareas que se deberán realizar para la correcta explotación del sistema. Se deberán indicar, entre otros aspectos, las tareas programadas (gestión de backups, mantenimiento de logs, etc.), procedimiento de paradas programadas, monitorización y gestión de la capacidad. La tabla muestra la información que puede ir en un manual de explotación ***Se debe rellenar la columna Descripción en los Elementos que no están sombreados.****>*

ELEMENTO	DESCRIPCIÓN
1. CALENDARIO DE OPERACIONES A REALIZAR.	*<Calendario resumen en el que se especifica en qué momento debe realizar cada una de las actividades que se describen a continuación.>* Tras revisar y aceptar las operaciones de explotación se formará a todos los empleados del departamento de recursos humanos que realzará el mantenimiento. A lo largo del funcionamiento del sistema el departamento de recursos humanos atenderá a las peticiones de los usuarios, monitorizará las copias de seguridad y gestionará la configuración y actualización de los componentes del sistema. También realizará revisiones rutinarias, a diario a ser posible, sobre el sistema y sus componentes.
2. DISPOSITIVOS DE ALMACENAMIENTO SECUNDARIO A UTILIZAR.	*<En este punto se le da información sobre los dispositivos de almacenamiento secundario que se deberán utilizar para hacer copias de seguridad o salvados de la base de datos u otra información del Sistema.>*

	Disponemos de dos dispositivos de almacenamiento secundario, dedicados a copias de seguridad de la base de datos, el estado de la aplicación y sus recursos. Uno de ellos local, y otro externo. Así dispondríamos 3 instancias paralelas de la base de datos, distribuidas en 2 soportes diferentes, siendo 1 de ellos externo, siguiendo así la regla 3-2-1 y asegurando la integridad de los datos ante cualquier evento inesperado. Los dispositivos son 2 servidores, uno es el servidor de aplicación situado en las instalaciones de la empresa, que maneja la instancia funcional de la base de datos y contiene el estado actual y recursos de la aplicación. Este servidor tendrá acceso a un disco duro en el que realizar las copias de seguridad pertinentes, estas serán de la base de datos primariamente pero también albergará consigo archivos de estado, configuración, multimedia, archivos XML, demás. Por otro lado, tenemos aquel que maneja la copia de seguridad externa. Puede ser otro servidor de la empresa en una instalación distinta, pero lo más recomendable en términos de coste es almacenarse y gestionarse en la nube con servicios de terceros.
3. REALIZACIÓN DE COPIAS DE SEGURIDAD.	*<En este punto se le informa de cómo realizar, paso a paso, las Copias de Seguridad. También se le indican los momentos más adecuados para realizarlas y los requisitos que se deben cumplir para que éstas puedan llevarse a cabo y resulten útiles.>* En primer lugar, la copia de seguridad local se gestiona mediante una segunda base de datos, almacenados en el disco duro mencionado, con el gestor operando en el mismo servidor que la principal. Esta base de datos secundaria recibirá los cambios que hayan ocurrido en los datos de la primaria a lo largo del día y los aplicará en los suyos. Tras ello, se encargará de almacenar en el correspondiente zip la instancia actual, así como subirla la nube. Dichos archivos comprimidos se guardarán durante una semana, tanto en local como en global, teniendo así un histórico semanal a nuestra disposición. Con este sistema, la base de datos principal puede permanecer operativa durante estos procesos. Para el resto de los archivos la copia de seguridad guardará los mismos en el disco duro pero en los archivos comprimidos solo guardará aquellos que se vean modificados o eliminados en comparación con la última copia de seguridad. Es decir, si se borra un archivo este quedará en el archivo comprimido, si no se borra seguirá permaneciendo en la última copia local pero no en los históricos.

4. CLASIFICACIÓN Y ACCESO DE COPIAS DE SEGURIDAD.	*<Información para administrar las Copias de Seguridad de forma que si es necesario acudir a ellas sigan un orden cronológico y estén debidamente etiquetadas e identificadas.>* Las copias de seguridad comprimidas se realizan diariamente, por lo que pueden simplemente clasificarse por día, reflejando la fecha de realización en el nombre. La base de datos paralela se encuentra totalmente automatizada, y el acceso tanto a ella como a las copias de seguridad derivadas de esta se encuentra reservado al personal de recursos humanos, por labores de mantenimiento y recuperación de datos. Esto refiere tanto a las locales como a aquella situada en la nube. Los archivos ajenos a la base de datos se guardan junto a la misma dentro del directorio o comprimido clasificado por día. Se clasificarán por tipo de archivo, por ejemplo, los archivos XML en una carpeta XML o los archivos JSON en una carpeta JSON.
5. MONITORIZACIÓN Y GESTIÓN DE LA CAPACIDAD.	*<Descripción detallada de aquellos recursos del Sistema que deben ser monitorizados. Se indicarán las necesidades de monitorización existentes para cada recurso, los umbrales esperados y las previsiones estimadas de crecimiento del Sistema en términos de almacenamiento, capacidad de procesamiento, tráfico de red y cualquier otro recurso.>* En primer lugar, vamos a decidir qué medidas tomar y qué hacer con los datos de los proyectos finalizados, ya que en principio no trabajamos más con ellos. Lo ideal sería liberarlos de la base de datos y mantenerlos fuera del sistema de copias de seguridad periódico, ya que el coste de almacenamiento del histórico semanal sería enorme. Decidimos, a la hora de finalizar un proyecto, exportaremos los datos correspondientes y los comprimiremos, para luego trasladarlos tanto al almacenamiento local como global. En cuanto a tamaño de datos, se estima que cada instancia de la base de datos debería ocupar alrededor de 30 GB teniendo en cuenta la base de datos y los recursos externos, reduciéndose ligeramente en las copias comprimidas. Por lo tanto, hablaríamos de alrededor de 200 GB para el histórico semanal, reflejado en sistemas local y global, y unos 85 GB para los proyectos finalizados. Para un manejo correcto y escalable de estos datos, dispondremos de un disco duro de 512GB como mínimo, y en el almacenamiento global, contratar un servicio que permita un mínimo de 300 GB, ampliable según se necesite.

	Dispondremos de un trabajador responsable de gestionar la suscripción al servicio de almacenamiento en la nube, y sea capaz de ampliar, una vez se requiera, tanto el almacenamiento local (mediante un segundo disco duro, dividiendo los datos en base de datos con copias y proyectos finalizados), como el global.
6. EMISIÓN DE INFORMES A PETICIÓN.	*<Listado de posibles informes a petición y usuarios autorizados.>* Los informes a petición pueden ser auditorías o revisiones de calidad, informes de no conformidad o informes de vista técnica para estudiar o comprender el sistema. Además, existen informes de estadísticas y datos que, por lo general, los solicitarán jefes de departamento, así como la dirección. El resto las puede solicitar cualquier empleado responsable, además de los jefes de departamento y la alta dirección. Todo informe se lleva a cabo por el departamento de RRHH.
7. ESTABLECIMIENTO DE PUNTOS DE RESTAURACIÓN DEL SISTEMA.	*<Información para que el operario conozca los pasos a seguir para establecer puntos de restauración del sistema que permitan deshacer los cambios realizados en el Sistema desde la última vez que el equipo funcionaba correctamente.>* Los puntos de restauración se establecen automáticamente tras cada transacción y se eliminan en la realización de la copia de seguridad, donde el último punto de restauración es la propia copia. Para reestablecer un punto de restauración el operario podrá deshacer desde la propia aplicación web todo cambio que haya realizado.
8. SALVADO DE LA BASE DE DATOS.	*<Enumeración de las tareas a realizar y las normas que se deben cumplir para realizar el salvado de la base de datos.>* El salvado de la base de datos se realiza automáticamente por el sistema a medianoche tras haber realizado las listas de petición. El sistema sigue los siguientes pasos para realizar el salvado: 1. Borra el comprimido diario más antiguo (solo si tiene una semana de antigüedad). 2. Crea una copia comprimida de la base de datos secundaria. 3. Elimina los logs con una semana de antigüedad o más. 4. Actualiza la base de datos secundaria acorde a los cambios realizados en la principal. 5. Elimina el comprimido más antiguo de la copia de seguridad global (solo si tiene una semana de antigüedad). 6. Sube el comprimido que ha creado en el segundo paso.
9. TAREAS DE MANTENIMIENTO DE LOS EQUIPOS.	*<Enumeración de las tareas de mantenimiento y revisiones periódicas que los equipos precisan.>*

	El mantenimiento es realizado por el departamento de RRHH, tiene cuatro roles que realizan las siguientes tareas: • El **supervisor del sistema**, que en principio será el jefe del departamento, es aquel que conoce el sistema e informa a sus subordinados de las solicitudes que se generen. • El **gestor de mantenimiento** recibe la solicitud del supervisor y asume la responsabilidad de llevar a cabo la tarea de mantenimiento solicitada, además de realizar un seguimiento de esta. • El **desarrollador de mantenimiento** realiza los cambios solicitados y es supervisado por el gestor de mantenimiento. • El **gestor de configuración** se encarga de mantener actualizado el software de la aplicación como los archivos de configuración del sistema y sus aplicaciones. Nótese que pueden haber más de un perfil con estos roles.
10. RESPONSABLES DIRECTOS DE CADA FUNCIONALIDAD DEL SISTEMA.	*<Listado de los responsables (y modos de contactar con ellos) de cada proceso que se debe lanzar y que le ha podido dar problemas. Aparece un responsable funcional (usuario de la propia empresa) y un responsable técnico (responsable de mantenimiento de la propia empresa o de la empresa con la que lo tenemos contratado)>* Los responsables del mantenimiento son el departamento de RRHH de COANDES. El responsable de la explotación del sistema es la propia empresa COANDES. En particular, el supervisor del sistema mencionado en el apartado nueve. En caso de cualquier defecto en la aplicación serán sus proveedores, es decir, nosotros, los responsables. Para solicitar desarrollar cualquier escalabilidad o adaptación tecnológica del software el responsable pueden ser sus proveedores o cualquier otra empresa que realice mantenimiento adaptativo, evolutivo o perfectivo.
11. ACTUACIONES ANTE SITUACIONES DE RIESGO.	*<Incluye aquellas actuaciones destinadas a restaurar el servicio ante situaciones anormales como caídas del Sistema, corte de suministro eléctrico, pérdida de datos, fallos de seguridad, etc. (planes de contingencia).* *Todas aquellas personas relacionadas con el Sistema que se puedan ver afectadas por un arranque, rearranque o parada del Sistema, deben ser avisadas a través de una lista de correo.>* En caso de caída del sistema se deberá de restaurar el funcionamiento del sistema y cargar la copia de seguridad más reciente (o aquel punto

	de restauración que se quiera). Para llevar esto a cabo hay que cargar la base de datos. En caso de pérdida de datos, se pueden cargar datos o elementos aislados de la última copia de seguridad. Alternativamente se pueden descomprimir copias más antiguas y cargar sus datos manualmente, esta tarea la realiza el personal de mantenimiento. En caso de corte de suministro eléctrico o de daño físico al servidor la restauración de los datos depende del servidor en la nube. Si se pierde la copia de seguridad local también depende de la misma. Cualquier usuario de la aplicación se verá afectado por la inactividad de la aplicación si el servidor no se encuentra funcional. En el rearranque, hasta que no se carguen los datos también se verán afectados todos los usuarios. Si se pierde el proceso desde la última copia de seguridad se verá afectado el personal técnico, no el cliente.
12. ROTACIÓN DE LOGS. PERIODICIDAD.	*<Entre las tareas programadas del Sistema encontramos la rotación de Logs. En este apartado se describirá la política de rotación de logs y la periodicidad de esta rotación. Quedarán definidas las condiciones de rotación (tamaño de logs, intervalo de tiempo, etc.), el procedimiento de rotación y la política de almacenamiento de logs antiguos, así como cualquier otra información que pueda resultar de interés.>* Los logs se guardan nada más realizar cualquier acción en la base de datos. Los archivos de logs se copian de la misma manera que el resto de los datos a la hora de realizar las copias de seguridad. En el servidor principal solo se mantienen los logs de la última semana, de forma que al realizar una copia de seguridad de la base de datos principal solo se copian los logs de la última semana y por efecto cascada cada copia de seguridad tiene los logs relativos a una semana.

9.3. Manual de usuario

<Se incluirá el índice detallado completo y el desarrollo de los apartados necesarios para incluir las funciones indicadas en el documento Documento_del_Proyecto (El manual no será completo). El manual no debe solo mostrar las pantallas, debe indicar como usar la aplicación para realizar procedimientos completos, explicar los mensajes de error, resolver dudas sobre posibles valores o formato de campos de entrada, etc. En la documentación está disponible un ejemplo real de manual de usuario. Algunos errores comunes que hay que evitar:

-Incoherencia con el resto de artefactos, por ejemplo, decir en el manual que al iniciar sesión hay una opción de recuperar contraseña y que no exista un caso de uso 'Recuperar contraseña' que sea llamado con extend desde el caso de uso Iniciar sesión.

-No explicar las consecuencias de acciones importantes, como el borrado. Por ejemplo, en una gestión de empleados que tienen tareas asignadas, si se tiene que dar de baja un empleado: que pasa con las tareas

asignadas o con aquellas tareas que ya ha terminado pero que siguen en la base de datos asociadas a ese empleado.

-Explicar las pantallas, sin explicar el proceso completo. Por ejemplo, en una pantalla en la que el empleado cierra una tarea: si un empleado debe cerrar una tarea como máximo 24 horas después de terminarla, que pasa si no lo hace. Otro ejemplo en esa misma pantalla: el texto "Si se usa el botón de 'Cerrar tarea', y el procedimiento falla, aparece este mensaje de error: 'La tarea no puede ser cerrada'" no es correcto ya que, el mensaje debería decir al usuario por qué no puede ser cerrada y el manual explicar en todos los posibles casos que debe hacer para resolver el problema que le impide cerrar la tarea.>