Universidad de Alcalá

Escuela Politécnica Superior

Universidad de Alcalá

PECL 3 – ARTEFACTO 11

ANEXO – MANUAL DE EXPLOTACIÓN

Ing. Software

Laboratorio Martes 12:00 – 14:00

Grado en Ingeniería Informática – Curso 2018/2019

Eduardo Graván Serrano – 03212337L

Marcos Barranquero Fernández – 51129104N

Sonia Rodríguez-Peral Bustos - 54302528B

Adrián Montesinos González – 51139629A

Alejandro Caballero Platas – 50891258D

El siguiente manual recoge todas aquellas tareas que deberán ser utilizadas para la correcta explotación del sistema. Así pues, contiene aquellas tareas programadas a realizar, junto con su procedimiento de paradas, su monitorización y gestión de capacidad entre otras cosas.

CALENDARIO DE OPERACIONES A REALIZAR

Para la realización de las tareas es necesario realizar un calendario de programación previo, de forma que cada tarea estará asignada a un día e incluso momento específico. Para su explicación se muestra la siguiente tabla, la cual representaría a un mes estándar de 30 días.

Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7
Análisis disco duro Eliminar cahes Vaciar papelera		Rotación de logs			Rotación de logs	Depuración de los equipos informáticos
Día 8	**Día 9**	**Día 10**	**Día 11**	**Día 12**	**Día 13**	**Día 14**
	Rotación de logs			Rotación de logs		Depuración de los equipos informáticos
Día 15	**Día 16**	**Día 17**	**Día 18**	**Día 19**	**Día 20**	**Día 21**
Rotación de logs			Rotación de logs			Depuración equipos infor. Rotación de logs
Día 22	**Día 23**	**Día 24**	**Día 25**	**Día 26**	**Día 27**	**Día 28**
		Rotación de logs			Rotación de logs	Depuración de los equipos informáticos
Día 29	**Día 30**					
	Rotación de logs					

Calendario de 30 días.

Las fechas no tienen por qué ser exactas, pero si es recomendable que se sigan.

Se tendrá acceso a los informes en cualquier momento siempre y cuando se tengan los permisos requeridos.

Los **informes diarios** se realizarán cada día tras terminar la jornada laboral (23:00) y los **informes semanales** los fines de semana. Sin embargo, podrán emitirse manualmente debido a peticiones del Coordinador o el Superusuario.

Las **copias de seguridad** se realizarán de manera diaria tras terminar la jornada laboral (23:00). Sin embargo puede hacerlas el Coordinador y el Superusuario manualmente según qué situaciones.

Se podrá **acceder a las copias de seguridad** en cualquier momento, pero solo por el Coordinador o el Superusuario

Los puntos de restauración se realizan diariamente por GoBack. Pero pueden realizarse manualmente por el usuario si lo cree conveniente.

La monitorización de las acciones del sistema se hará cada dos meses el primer año y luego mensualmente.

El salvado de la base de datos se realizará de manera diaria tras terminar la jornada laboral (23:00).

DISPOSITIVOS DE ALMACENAMIENTO SECUNDARIO A UTILIZAR

El almacenamiento secundario se trata de un medio de almacenamiento definitivo, no volátil como sería la memoria RAM. En nuestro caso se utilizarán medios de almacenamiento magnético, los Discos Duros y una nube.

Los discos duros nos proporcionan un rápido acceso y son capaces de almacenar incluso 1TB = 1024GB de información. Sin embargo será conveniente tenerlos almacenados en un lugar libre de polvo para evitar daños en el propio disco que nos hagan perder la información. Estos contendrán información que sea requerida de manera común por algún motivo.

Sin embargo, el dispositivo principal de almacenamiento secundario será la nube, de manera que nos aseguraremos de que la información no se perderá.

Por último, dependiendo del tipo de información, esta se mantendrá guardada durante un cierto periodo de tiempo, por lo que será conveniente tener cada cosa guardada por separado.

REALIZACIÓN DE COPIAS DE SEGURIDAD

En cuanto a la realización de copias de seguridad, se realizarán de manera periódica una vez al día tal y como pone en el calendario. Los backups serán realizados de manera automática para la nube, y por el Coordinador correspondiente a cada oficina para los discos duros cuando sea necesario. Solo el Coordinador de la propia oficina y el Superusuario tendrán acceso a dichos datos.

Para que las copias de seguridad se lleven a cabo, será necesario que se cumplan una serie de requisitos:

1. **Seguridad y fiabilidad**: Para garantizar la seguridad de la información, el sistema deberá ser fiable, deberá tener un buen antivirus y que todos los programas estén actualizados. También deberá haber sistemas de encriptación y la información deberá estar correctamente guardada.

2. **Automatización:** La copias de. seguridad deberán hacerse de manera automática, pues si fuera manual conllevaría errores de guardado, pérdidas, etc. Solo el Coordinador de la oficina o el Superusuario realizará copias manuales cuando sea preciso.

3. **Espacio de almacenamiento**: La nube o el disco duro utilizados deberá tener el almacenamiento suficiente para soportar la información que debe de guardar.

4. **Sencillez y buena interfaz:** lo deseable es que la interfaz del programa en la nube que estemos empleando sea lo más intuitiva posible, de modo que cualquier persona autorizada pueda recuperar datos de manera sencilla y en el menor tiempo posible.

CLASIFICACIÓN Y ACCESO DE COPIAS DE SEGURIDAD

Los datos a respaldar y el periodo de su almacenamiento, dependerán del tipo de información que contenga. Así pues, tendremos la información separada en discos duros según la duración la información (**https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-16673**):

Los contratos, ya sean con empleados, proveedores, clientes... tendrán una duración de diez años.

Las facturas por compras a proveedores o por ventas a clientes tendrán una duración de cinco años.

El resto de información será guardada durante 2 años.

Además de seguir este método de guardado, la información estará guardada cronológicamente, para facilitar el acceso a esta.

A esta información sólo tendrán acceso el Superusuario y el Coordinador correspondiente a cada oficina. Sin embargo, podrá ser requerida por otros organismos externos, los cuales podrán ejercer en cualquier momento alguno de los ejercicios ARCO u otros:

- **A**cceso: a los datos que la empresa posee sobre el afectado
- **R**ectificación: derecho a cambiar dichos datos
- **C**ancelación: derecho a la eliminación o supresión de sus datos
- **O**posición: derecho a solicitar que la empresa no haga uso de sus datos
- Portabilidad: derecho a que la empresa ceda o transfiera sus datos a otra con un fin
- Limitación: los datos serán marcados para que no puedan ser tratados en el futuro

MONITORIZACIÓN Y GESTIÓN DE LA SEGURIDAD

Es necesario realizar un proceso riguroso para estimar la capacidad y las actividades necesarias para adecuar las infraestructuras que soportan los servicios a la demanda (en cada momento). De esta manera, obtendremos unos servicios con la mayor calidad posible y de la manera más eficiente.

Una mala gestión de la capacidad puede acarrear que las infraestructuras sean insuficientes para soportar la demanda de usuarios, produciendo así una reducción de calidad en el servicio o incluso su interrupción. O todo lo contrario, que no se haga uso de esos recursos, lo que conlleva ineficiencia en términos de costes.

Para obtener unas predicciones precisas se necesitan de una metodología y de unas buenas prácticas. Es necesario un equilibrio entre coste y capacidad y entre provisión y demanda. Este proceso comprende:

1. Realización de previsiones de futuros requisitos basados en la demanda **actual.**
2. Elaboración de una planificación de la capacidad que permitan proporcionar una calidad adecuada. Para ella nos apoyamos en una serie de subprocesos:
    - ***Gestión de la capacidad de negocio***: se deben tener en cuenta las futuras necesidades del negocio
    - ***Gestión de la capacidad de los servicios***: los servicios ofrecidos deben seguir unas exigencias mínimas en cuanto a calidad
    - ***Gestión de la capacidad de los recursos***: se deben gestionar los recursos de bajo nivel de las infraestructuras
3. Monitorización del rendimiento, de los servicios y de los componentes que lo soportan.
4. Realización de actividades de optimización.
5. Influenciar en la demanda positivamente.

Para obtener unos servicios buenos y eficientes, deberá monitorizarse todas aquellas acciones que puedan influir en el sistema en cuanto a capacidad, lo cual se hará cada 2 meses. Estas serían las siguientes:

- ***Capacidad de procesamiento***: Inicialmente disponemos de 150 empleados los cuales pueden estar conectados al sistema simultáneamente. Esperamos crecer que siga siendo capaz de procesar todas las peticiones que puedan realizar los empleados de

acuerdo al número de empleados.

- ***Stock de piezas***: Inicialmente se dispone de una cantidad preestablecida de cada pieza. Dependiendo de la demanda de cada pieza, se aumentará o disminuirá la cantidad a pedir de acuerdo a la siguiente fórmula:

Si *Cantidad_Viejo_Pedido - Cantidad_Piezas_Gastadas > 5*

$$Cantidad\_Nuevo\_Pedido = \frac{Cantidad\_Viejo\_Pedido - Cantidad\_Piezas\_Gastadas}{2} + Cantidad\_Piezas\_Gastadas$$

Si *Cantidad_Viejo_Pedido - Cantidad_Piezas_Gastadas < 5*

$$Cantidad\_Nuevo\_Pedido = \frac{Cantidad\_Piezas\_Gastadas - Cantidad\_Viejo\_Pedido}{2} + Cantidad\_Viejo\_Pedido$$

Sino

$$Cantidad\_Nuevo\_Pedido = Cantidad\_Viejo\_Pedido$$

- ***Nuevos clientes***: Inicialmente tenemos una media de 3000 clientes entre todas las oficinas. Esperamos crecer de manera exponencial mensualmente iniciando con 100 el primer mes.
- ***Nuevos proveedores***: Inicialmente disponemos de un total de 10 proveedores dispersos a lo largo del país. Esperamos seguir con estos a no ser que nos sean necesarios más. No más de 1 cada 4-5 meses.
- ***Nuevos empleados***: Inicialmente disponemos de 150 empleados. Si los cálculos previstos en cuanto a los clientes van bien, los contratos deberán crecer también de manera exponencial de 1,5 mensualmente.

EMISIÓN DE INFORMES A PETICIÓN

En el sistema se pueden pedir una serie de informes a los cuales tienen acceso el Coordinador correspondiente a cada oficina y el Superusuario. La lista de informes a petición por los usuarios es la siguiente:

- ***Informes de empleados***: Serán aquellos informes correspondientes a un empleado concreto debido a algún incidente o percance que haya podido ocurrir en su horario laboral. Tendrán acceso el Superusuario y el Coordinador (siempre que no sea acerca de él).
- ***Informes de peticiones de trabajo***: Serán aquellos informes que contengan información sobre las peticiones de trabajo (datos del cliente, datos del coordinador que la realizó, posibles incidencias [faltas de respeto por parte del cliente…], etc). Tendrá acceso el Superusuario.
- ***Informes de partes de trabajo***: Serán aquellos informes que contengan información sobre los partes de trabajo (técnico encargado, datos del cliente, datos del suceso, piezas usadas, etc). Tendrán acceso el Superusuario y el Coordinador de la oficina.
- ***Informes de facturación***: Serán aquellos informes que contengan información sobre toda posible facturación. Aquí encontraremos facturas respecto a clientes (ofreciendo nuestros servicios) y respecto a proveedores (pidiendo sus servicios). Tendrán acceso el Superusuario y el Coordinador de la oficina.
- ***Informes de gastos de material***: Serán aquellos informes que contengan información sobre el coste de los materiales comprados y cuántos han sido gastados. Esto será útil para la posterior gestión de la capacidad. Tendrán acceso el Superusuario y el Coordinador de la oficina y además, en este caso, el Responsable de almacén.

En los casos de los informes de facturación y gastos, estos no podrán ser modificados.

ESTABLECIMIENTO DE PUNTOS DE RESTAURACIÓN DEL SISTEMA

Un punto de restauración es una copia de seguridad de la información contenida en un computador y que se clasifica con una fecha y hora específica. Estos puntos son creados automáticamente por programas de restauración, en nuestro caso GoBack, con el fin de permitir deshacer los cambios realizados en el sistema desde que el equipo funcionaba correctamente.

GoBack realiza puntos de restauración cada vez que se realiza una modificación medianamente importante como la instalación (o desinstalación) de un programa o la adición (o eliminación) de archivos de la carpeta Mis documentos..

Por otro lado, si el usuario lo cree conveniente, en Windows 7, 8 y 10, es posible realizar puntos de restauración:

1. Menú ***Iniciar***: Escribimos ***crear*** en el cuadro de búsqueda (*Buscar programas y archivos*)
2. Clickamos en ***Crear un punto de restauración***
3. En la ventana que se nos abre, ***Propiedades del sistema***, hacemos click en ***Crear***
4. En la ventana de ***Protección del sistema***, escribimos una descripción y damos a ***Crear***
5. Tras crear el punto damos a ***Aceptar*** y cerramos y guardamos los cambios realizados

SALVADO DE LA BASE DE DATOS

Diariamente se realiza un backup con todas las acciones y registros realizados en el día, los cuales son guardados en una carpeta como un nuevo archivo .rar con la fecha del día. a estos archivos principalmente tendrán acceso el Superusuario, el Coordinador de cada oficina y el Responsable de almacén.

TAREAS DE MANTENIMIENTO DE LOS EQUIPOS

Para el mantenimiento de los equipos será necesario que estos se encuentren actualizados y que dispongan de un buen antivirus también actualizado. Además, se realizarán otra serie de tareas:

Cada 7 días (fin de semana)	Deberá eliminarse toda aquella información innecesaria que pueda encontrarse en los equipos
1 vez al mes a principios	Vaciar la papelera de reciclaje, eliminar temporales y caches, hacer un análisis exhaustivo del disco duro en busca de programas dañinos.

Cada siete días, deberá eliminarse toda aquella información innecesaria que pueda encontrarse en los equipos.

RESPONSABLES DIRECTOS DE CADA FUNCIONALIDAD DEL SISTEMA

En el siguiente sistema, encontraremos 3 tipos de responsables principales que serán: el Superusuario, los Coordinadores de los departamentos y los Responsables de almacén. Se podrá contactar con ellos mediante dos vías, dependiendo de la gravedad del problema:

1. ***Correo electrónico***: será en el caso de que el incidente no sea demasiado grave y pueda solucionarse más adelante.
2. ***PDA o Teléfono móvil***: en caso de que el problema necesite una solución inmediata.

A continuación se mostrará una lista con los procesos que pueden acarrear problemas junto a los responsables correspondientes. Estos serán:

- Responsable funcional: usuario de la empresa
- Responsable técnico: un único responsable de mantenimiento de la empresa. En nuestro caso un subcontratado de la Oficina de Tecnologías de la Información y Comunicaciones (Oficinas TIC)

Proceso	Responsable funcional	Responsable técnico
Gestión clientes	Coordinador Departamento	Oficina TIC
Gestión empleados	Coordinador Departamento	Oficina TIC
Gestión proveedores	Responsable de almacén	Oficina TIC
Gestión informes	Superusuario	Oficina TIC
Gestión peticiones de trabajo	Coordinador Departamento	Oficina TIC
Gestión piezas y pedidos	Responsable de almacén	Oficina TIC
Gestión partes de trabajo	Técnico de campo	Oficina TIC
Gestión presupuestos	Coordinador Departamento	Oficina TIC
Gestión facturas	Superusuario	Oficina TIC
Gestión coordinadores	Superusuario	Oficina TIC
Gestión oficinas	Superusuario	Oficina TIC

ACTUACIONES ANTE SITUACIONES DE RIESGO

En el caso de que ocurra algún percance imprevisto (apagón, tormenta, fallo de seguridad, etc), es necesario disponer de un plan de contingencia para tratarlo. En estos casos, todos los usuarios serán informados mediante un correo electrónico para que sean conscientes del suceso. Así pues, dividiremos los sucesos en varias categorías:

Vulneración de la seguridad: constará de aquellos sucesos en los que la información ha sido sustraída. En estos prevalece el dicho *"Mejor prevenir que curar"*. Por ello, es importante seguir una serie de normas:

- Política de mesas limpias (mesa ordenada y sin nada a la vista)
- Bloqueos de pantalla, identificaciones con usuario y contraseña
- Antivirus y programas actualizados
- No abrir spam o correos misterios (phishing)
- Disponer de cámaras y medidas de seguridad

En el caso de que la sustracción no haya podido evitarse, lo primordial será identificar el daño y evaluar su gravedad, para posteriormente gestionarlo. El proceso de respuesta a una brecha de seguridad consta de tres partes:

- ***Contener el incidente***: con el fin de desarrollar una estrategia de respuesta correcta (cerrar el sistema, aislar la red, deshabilitar ciertas funciones, etc).
- ***Erradicar la situación generada por el incidente***: para solventar algunos de los incidentes (eliminar malware, cambiar contraseñas, etc)
- ***Realizar las acciones de recuperación oportunas***: su fin es restablecer el servicio en su totalidad teniendo en cuenta el suceso y mejorando así las medidas de seguridad.

Daños ambientales y desastres naturales: incluye a sucesos tales como: tormenta eléctrica, terremoto, apagón, etc. Son aquellos que causarían una caída del sistema. Por ello es necesaria la realización de copias de seguridad diarias.

Incidencias del cumplimiento: relacionadas con el incluplimiento de la legislación vigente en materia de protección de datos. En este caso vuelve a ser primordial el prevenir. Encontraríamos casos como puede ser:

- ***Ausencia de procedimientos para el ejercicio de derechos***: la cual se corrige con procedimientos y canales para el ejercicio de derechos.
- ***Ausencia de legitimidad para el tratamiento de los datos personales***: mediante cláusulas informativas y base legitimadora para el tratamiento de datos.
- ***Tratamiento ilícito de datos personales:*** con la monitorización del uso de datos personales.

ROTACIÓN DE LOGS Y PERIODICIDAD

Los logs son los encargados de monitorizar las actividades de las aplicaciones y dispositivos. Estos pueden consumir rápidamente gran cantidad de almacenamiento de un servidor. Gracias a la rotación de los logs, se puede limitar el volumen de datos que se tienen disponibles para examinar, además de limitar el número de archivos expuestos a un posible ataque cibernético. Por ello es necesario realizar las rotaciones de logs cada 3 días.