

Secuencia de Recuperación ante Incidencias en Recovery

*Plan de Continuidad Tecnológico (PCT)*

|  |  |  |
| --- | --- | --- |
| Nombre del Documento: | Fecha: | Versión: |
| 11. HRE\_PCT\_Sec\_Recuperación ante Incidencias en Recovery\_v3.00.docx | 21/03/2019 | 3.00 |
| Responsable: | Sr. Antonio Saez | |
| Elaborado por: | PFS GROUP | |
| Revisado por: | Sr. Félix de Lelis / Sr. Miguel Delgado | |
| Aprobado por: | -- | |
| Ámbito de afectación: | HRE | |

CONTROL DE DOCUMENTACIÓN

LISTA DE DISTRIBUCIÓN

|  |  |
| --- | --- |
| Nombre del destinatario | Ámbito del destinatario |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

CONTROL DE CAMBIOS DEL DOCUMENTO

|  |  |  |  |
| --- | --- | --- | --- |
| Ver. | Fecha | Descripción cambios | Páginas afectadas |
| 1.00 | 7/09/2017 | Actualización contactos y procedimiento copias  Cambios menores y revisión 2017 | Anexo I, II y III |
| 2.00 | 29/06/2018 | Actualización contactos y procedimiento copias  Cambios menores y revisión 2018  (actualización de las antiguas secuencias 1.00 de Recovery Cajamar y Sareb de 2017) | Anexo I, II y III |
| 3.00 | 21/03/2019 | Validación 2019 |  |
|  |  |  |  |

ACCIONES PENDIENTES

|  |  |  |
| --- | --- | --- |
| Descripción | Responsable | Fecha objetivo |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

ÍNDICE

[ÍNDICE 3](#_Toc519056493)

[1 INTRODUCCIÓN 4](#_Toc519056494)

[1.1 ÁMBITO DE APLICACIÓN 4](#_Toc519056495)

[1.2 ALCANCE 4](#_Toc519056496)

[1.3 TIEMPO DE EJECUCIÓN 4](#_Toc519056497)

[1.4 DOCUMENTOS RELACIONADOS 5](#_Toc519056498)

[2 DIAGRAMA DE FLUJO 6](#_Toc519056499)

[2.1 INDISPONIBILIDAD SERVIDORES DE PRODUCCIÓN 6](#_Toc519056500)

[2.2 CORRUPCIÓN/RESTAURACIÓN BASE DE DATOS 7](#_Toc519056501)

[2.3 FALLO DEL FICHERO DE APROVISIONAMIENTO 7](#_Toc519056502)

[3 DESCRIPCIÓN DE LA SECUENCIA 8](#_Toc519056503)

[3.1 INDISPONIBILIDAD SERVIDORES DE PRODUCCIÓN 8](#_Toc519056504)

[3.2 CORRUPCIÓN/RESTAURACIÓN BASE DE DATOS 8](#_Toc519056505)

[3.3 FALLO DEL FICHERO DE APROVISIONAMIENTO 9](#_Toc519056506)

[4 ROLES Y RESPONSABILIDADES DE LA SECUENCIA 10](#_Toc519056507)

[4.1 INDISPONIBILIDAD DE LOS SERVIDORES DE PRODUCCIÓN 10](#_Toc519056508)

[4.2 CORRUPCIÓN/RESTAURACIÓN DE LA BASE DE DATOS 10](#_Toc519056509)

[4.3 FALLO DEL FICHERO DE APROVISIONAMIENTO 10](#_Toc519056510)

[5 ACTIVIDADES DE LA SECUENCIA DE RECUPERACIÓN 11](#_Toc519056511)

[5.1 GENERALIDADES 11](#_Toc519056512)

[5.2 INDISPONIBILIDAD DE LOS SERVIDORES DE PRODUCCIÓN 11](#_Toc519056513)

[5.3 CORRUPCIÓN/RESTAURACIÓN BASE DE DATOS 14](#_Toc519056514)

[5.4 FALLO DEL FICHERO DE APROVISIONAMIENTO 15](#_Toc519056515)

[6 ANEXOS 16](#_Toc519056516)

[6.1 ANEXO I: PERSONAS DE CONTACTO 16](#_Toc519056517)

[6.2 ANEXO II: POLÍTICA DE RESPALDO DE DATOS Y PLANIFICACIÓN DE LAS COPIAS DE SEGURIDAD 17](#_Toc519056518)

[6.3 ANEXO III: ESQUEMA DEL SISTEMA DE INFORMACIÓN RECOVERY SAREB 17](#_Toc519056519)

INTRODUCCIÓN

El propósito del presente documento es:

* describir los procedimientos de recuperación ante un incidente crítico o bien una indisponibilidad completa.
* describir los procedimientos de vuelta a la normalidad.

ÁMBITO DE APLICACIÓN

Este documento se aplica a los Sistemas de Producción Cliente (SPC), en concreto para el cliente HRE Haya Real Estate, para la aplicación Recovery.

ALCANCE

* Servidores de Producción: Application Server (Frontal), Batch Server, Database Server. HW, SW y configuración. Comunicaciones e infraestructura necesaria.
* Gestión del Aprovisionamiento (manos remotas PFS)

TIEMPO DE EJECUCIÓN

INDISPONIBILIDAD SERVIDORES DE PRODUCCIÓN

Application Server (Frontal)

| Inicio/Fin/Duración | Descripción |
| --- | --- |
| Inicio | Desde que se recibe la alerta de la no disponibilidad del nodo activo por parte del sistema de monitorización redundante. |
| Fin | Una vez se ha activado uno de los nodos alternativo. |
| Duración | 0h (Nota: se gestiona de manera automática por el balanceador de carga, el usuario no percibe la indisponibilidad) |

#### Database Server (Oracle)

| Inicio/Fin/Duración | Descripción |
| --- | --- |
| Escenario Caída Nodo Primario | |
| Inicio | Desde que se recibe la alerta de la caída del nodo Primario (Primary) por parte del sistema de monitorización redundante. |
| Fin | Una vez se ha gestionado el Failover activando el nodo Secundario (Standby) y se restablece el servicio. |
| Duración | 2 h |
| Escenario Caída Nodo Secundario | |
| Inicio | Desde que se recibe la alerta de la caída del nodo Secundario (Standby) por parte del sistema de monitorización redundante. |
| Fin | Una vez se restablece el nodo Secundario. |
| Duración | N/A (Nota: el servicio al usuario no se ve interrumpido ante una caída del nodo Secundario). |

#### Batch Server

| Inicio/Fin/Duración | Descripción |
| --- | --- |
| Escenario Caída Primary | |
| Inicio | Desde que se recibe la alerta de la caída del Batch por parte del sistema de monitorización redundante. |
| Fin | Una vez se restablece el Batch. |
| Duración | N/A  Nota: el servicio al usuario no se ve interrumpido ante una caída del Batch. |

CORRUPCIÓN/RESTAURACIÓN BASE DE DATOS

| Inicio/Fin/Duración | Descripción |
| --- | --- |
| Inicio | Una vez detectado el incidente y determinado su alcance. |
| Fin | Una vez se restablece la situación normal. |
| Duración | 24 h  Nota: Tiempo máximo para restablecer la BBDD completa. |

### FALLO DEL FICHERO DE APROVISIONAMIENTO

| Inicio/Fin/Duración | Descripción |
| --- | --- |
| Inicio | Desde que se recibe la alerta de fallo del fichero de aprovisionamiento por parte del sistema de carga. |
| Fin | Una vez se realiza la carga. |
| Duración | N/A  Nota: el servicio al usuario no se ve interrumpido ante un fallo en el fichero de aprovisionamiento. |

DOCUMENTOS RELACIONADOS

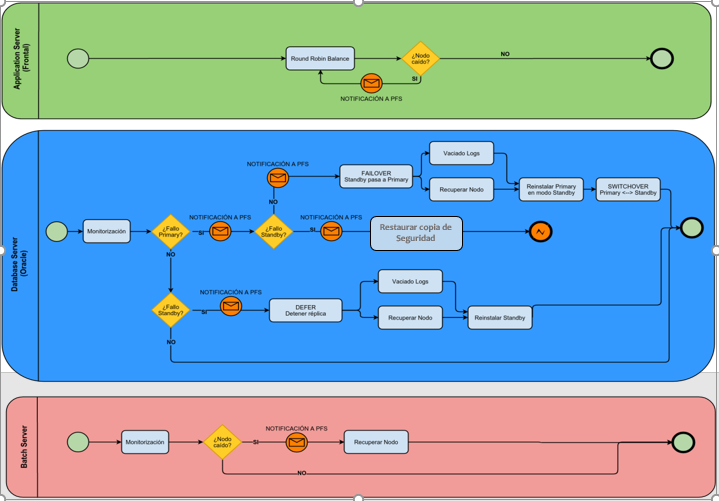
A la hora de realizar esta secuencia, se han tenido en cuenta, o bien se referencian los siguientes documentos:

| Documentación de Referencia |
| --- |
| Política de Respaldo de Datos y Planificación de las Copias de Seguridad (Cap. 6.2 Anexo II) |
| 10. HRE PCT PR Recuperación ante Indisponibilidad del CPD Principal de RSI |
|  |

DIAGRAMA DE FLUJO

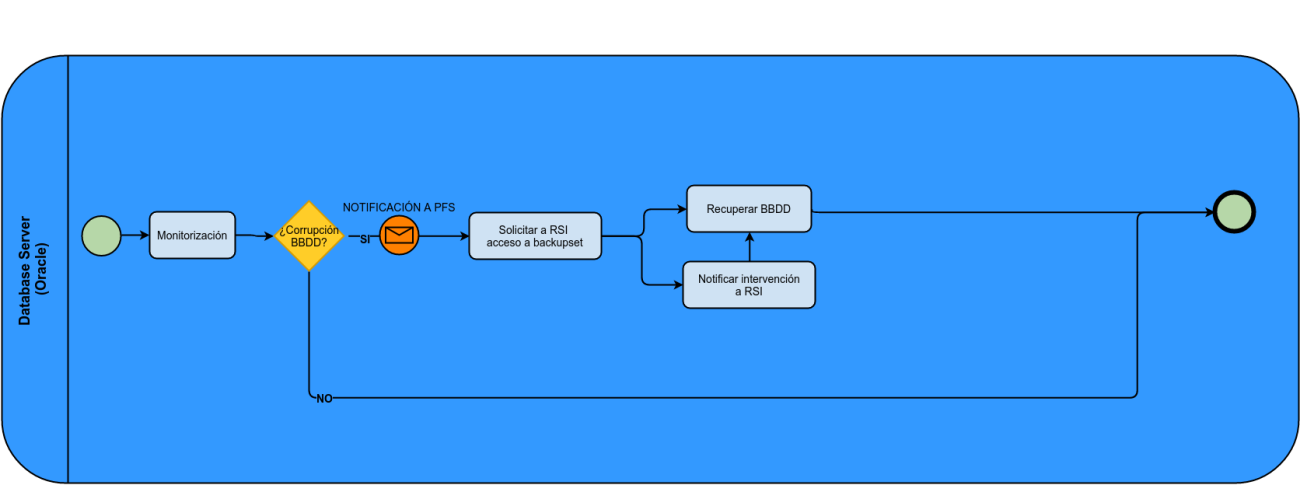
A continuación, se muestran los tipos de contingencias establecidos:

INDISPONIBILIDAD SERVIDORES DE PRODUCCIÓN

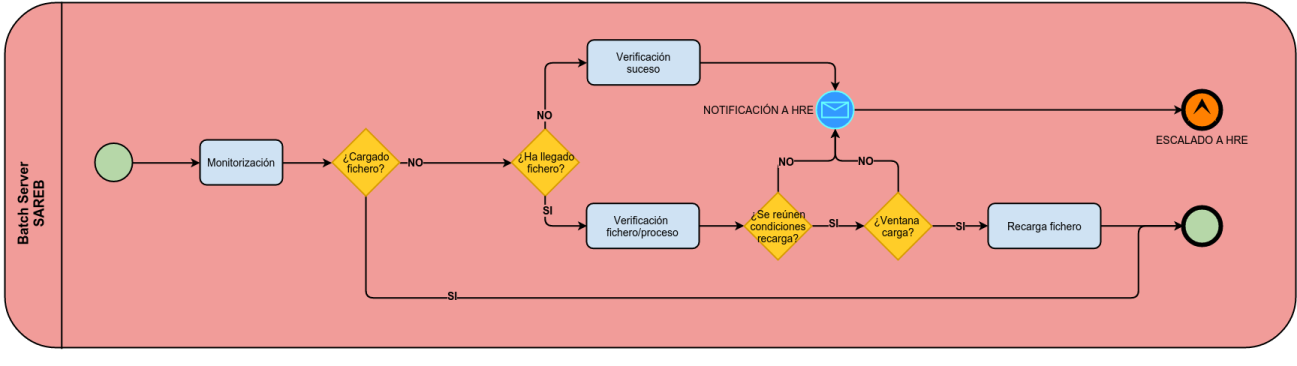


“Modificar gráfico: “Activar plan de contingencia” por “Restaurar copia de seguridad” (2.2)

CORRUPCIÓN/RESTAURACIÓN BASE DE DATOS



FALLO DEL FICHERO DE APROVISIONAMIENTO



**Nota**: Se representa únicamente el aprovisionamiento de Recovery del Camino Crítico (Bloque PCR)

DESCRIPCIÓN DE LA SECUENCIA

INDISPONIBILIDAD SERVIDORES DE PRODUCCIÓN

En este apartado se contemplan distintos escenarios de no disponibilidad de los servidores de producción, es decir, frontales de la aplicación, máquinas de base de datos y servidor batch.

Se enumeran distintos procedimientos para cada uno de los escenarios, describiendo las actividades a realizar por cada uno de los departamentos de PFS o los proveedores implicados.

La indisponibilidad de Servidores de Producción responde a una estrategia de tolerancia a fallos mediante redundancia de HW, para el caso de los servicios más críticos. Se resume de la siguiente manera:

* Servidores de Aplicación (Frontal): redundancia de hardware y automatización del balanceo de carga entre nodos, en distintos datacenters.
* Servidores de Base de Datos: redundancia de hardware y réplica mediante gestión de nodos Activo y Pasivo, en distintos datacenters.
* Servidor de Batch: recuperación en hardware alternativo, en distintos datacenters.

CORRUPCIÓN/RESTAURACIÓN BASE DE DATOS

Se entiende por corrupción de datos, a la introducción, modificación o alteración de los datos originales de manera no deseada, afectando la integridad y/o coherencia de los datos.

En el contexto de Base de Datos esta situación puede ocurrir por una carga de ficheros mal formateados, manipulación de datos indebida o errores en la programación del código.

La corrupción accidental de datos puede ser:

* parcial (afectar a algunas tablas)
* bien a toda la base de datos, y la recuperación manual puede ser muy compleja.

En estos casos puede interesar una restauración (parcial o total, según proceda), de los elementos de base de datos afectados, desde la última copia de seguridad válida.

La restauración de una copia de seguridad recuperará la integridad de los datos, si bien implicará una pérdida mínima de los mismos, dado que se pierden aquellos datos introducidos por el usuario desde la fecha de la copia de seguridad que se va a restaurar, a no ser que se haga una restauración completa y se dispongan de todos los “archivelogs”.

La estrategia para mitigar pérdidas de datos por corrupción o restauración de la BBDD se define en el anexo PCT-HRE: Política de Respaldo de Datos y Planificación de las Copias de Seguridad

FALLO DEL FICHERO DE APROVISIONAMIENTO

El aprovisionamiento de Recovery HRE está compuesto por ficheros con origen en dos carteras diferentes:

* aprovisionamiento proveniente de CAJAMAR
* aprovisionamiento proveniente de SAREB (IRIS HRE)
* aprovisionamiento proveniente de “nuevas Carteras” (IRIS HRE)

La gestión del envío de estos ficheros es responsabilidad de dichas entidades.

PFS monitoriza la recepción y carga de ficheros y notifica a HRE en caso de fallos, solicitando autorización a la entidad para la realización de las cargas fuera de la ventana horaria establecida.

ROLES Y RESPONSABILIDADES DE LA SECUENCIA

A continuación, especificamos los datos de contacto del Personal que se responsabilizaría de la resolución de la incidencia, en caso de materializarse la contingencia.

INDISPONIBILIDAD DE LOS SERVIDORES DE PRODUCCIÓN

**Responsable/s de la ejecución de la secuencia:**

Operador Backups RSI, Técnica de Sistemas RSI

Técnica de Sistemas PFS, Administrador de BBDD PFS y Operaciones PFS.

**Localización desde dónde se puede ejecutar la secuencia:**

Puede realizarse en remoto, desde cualquier ubicación, conectando a través de la VPN de PFS.

CORRUPCIÓN/RESTAURACIÓN DE LA BASE DE DATOS

**Responsable/s de la ejecución de la secuencia:**

Operador Backups RSI, Técnica de Sistemas RSI

Técnica de Sistemas PFS, Administrador de BBDD PFS y Operaciones PFS.

**Localización desde dónde se puede ejecutar la secuencia:**

Puede realizarse en remoto, desde cualquier ubicación, conectando a través de la VPN de PFS.

FALLO DEL FICHERO DE APROVISIONAMIENTO

**Responsable/s de la ejecución de la secuencia:**

Operaciones Bankia (Sareb), Operaciones Cajamar, Operaciones PFS.

**Localización desde dónde se puede ejecutar la secuencia:**

Puede realizarse en remoto, desde cualquier ubicación, conectando a través de la VPN de PFS.

ACTIVIDADES DE LA SECUENCIA DE RECUPERACIÓN

GENERALIDADES

|  |  |
| --- | --- |
| Detección de incidentes | Existe un sistema de monitorización redundante:   * Uno es realizado por el personal de RSI (Nimbus) * El otro se realiza en PFS (Nagios). |
| Notificación de incidentes | En caso de ser detectado un incidente por RSI, el método de notificación es por mail al buzón de Explotación:  guardias-devops@pfsgroup.es  Además RSI notifica telefónicamente:   * dentro del horario laboral, al teléfono fijo de Explotación * fuera de horario laboral, a los móviles de guardias DevOps. |

INDISPONIBILIDAD DE LOS SERVIDORES DE PRODUCCIÓN

Application Server (Frontal)

|  |  |
| --- | --- |
| Servidores | AP01, AP02, AP03 (Planificado 3T 2016) |
| Ubicación | RSI |
| Escenario Caída Parcial | La caída de alguno de los nodos es gestionada de manera automática por un Round Robin (ubicado en RSI) que deriva las solicitudes al nodo vivo. |
| Escenario Indisponibilidad Total | Activación Plan de Contingencia (Ver 13. HRE PCT PR Recuperación ante Indisponibilidad del CPD Principal de RSI) |

Database Server (Oracle)

|  |  |
| --- | --- |
| Servidores | BD01 (Standby), BD02 (Primary) |
| Ubicación | RSI |
| Escenario Caída Parcial | Existe una configuración nodo Activo/Pasivo usando la tecnología Oracle Dataguard. |
| Escenarios | Caída nodo Primario: |
|  | Ante este escenario Oracle provee la operación "Failover", que gestiona precisamente el cambio de rol ante un fallo de la Primary.  La Standby pasa a ser Primary dando servicio al cliente, y la antigua Primary permanece caída pendiente de una recuperación.  En tal caso se vaciarán cada 4 horas los archived logs de la base de datos que adquiere el rol Primary para evitar un llenado de disco que pudiera detener la base de datos.  Para más información, consultar el documento y sus referencias Operativa con DATA GUARD.  **Procedimiento**:  Una vez detectada la caída, el Administrador de Base de Datos (PFS) lanzará los comandos para realizar el Failover del Primary y poder dar servicio con la réplica.  Posteriormente solicitará a RSI que realice el vaciado de logs cada 4 horas, hasta nuevo aviso (para evitar el llenado del disco).  **Vuelta a la normalidad:**  Volver a la situación anterior en este escenario implica dos pasos:   * recuperar el error que haya provocado la caída del nodo Primario (la casuística aquí es muy extensa, puede ir desde un problema en la conectividad de red hasta una reinstalación del sistema operativo y software de BBDD, etc.) * rehacer el "espejo" creado entre los dos nodos.   El primer paso dependerá del problema presentado en el servidor, suponiendo que del backup de RSI de sistema de ficheros pueda restaurarse tanto el Sistema Operativo, el software de BBDD Oracle, la configuración de red, etc.  Si es fallo de algún componente físico tenemos el compromiso de RSI de reponer los componentes en un tiempo máximo de 4 horas, según su SLA.  Una vez quede resuelta la caída del nodo, se reinstalará la réplica de Data Guard con RMAN siguiendo los pasos de la instalación Instalación Data Guard en Haya, a partir del punto "Creación de la base de datos Standby" - punto 4, teniendo en cuenta que la base de datos Standby será la del nodo Primario que cayó.  Opcionalmente, se puede realizar un Switchover restaurando los roles de inicio siguiendo el documento Operativa con Data Guard. |
|  | Caída nodo Secundario: |
|  | En este escenario la Primary sigue dando servicio al cliente igual que antes, sólo que hay que detener la transferencia (DEFER) de archived redo logs hacia la Standby y vaciar los archived redo logs en la Primary cada 4 horas, puesto que se llenará el disco muy rápidamente, pudiendo llegar a pararse también la Primary si se llena al 100%.  Posteriormente se recuperará la réplica en la Standby, dependiendo del problema puede resolverse automáticamente, manualmente, o necesitar reconstruir la réplica por completo mediante RMAN. Consultar para ello los documentos Operativa con DATA GUARD e Instalación DATA GUARD en HAYA, así como Oracle Docs: Data Guard Concepts and Administration.  **Procedimiento**:  Una vez detectada la caída, el Administrador de Base de Datos (PFS) detendrá la transferencia del archived redo logs. Se sigue dando servicio puesto que la Primary está operativa. No es necesario realizar Failover.  Posteriormente solicitará a RSI que realice el vaciado de logs cada 4 horas hasta nuevo aviso (para evitar el llenado del disco).  **Vuelta a la normalidad:**  Al igual que en el caso de caída de nodo Primario, el primer paso para volver a la situación es recuperar la operatividad del nodo caído.  Posteriormente se reinstalará la réplica de Data Guard con RMAN siguiendo los pasos de la instalación Instalación Data Guard en Haya, a partir del punto "Creación de la base de datos Standby" - punto 4.  Terminada esta recuperación cada nodo tiene los roles iniciales, no siendo necesario ningún paso adicional. |
| Escenario Indisponibilidad Total | **Caída total/Pérdida total de la base de datos (Primary y Standby):**  Ante una pérdida total se recuperará una de las dos instancias, y otorgarle el rol de Primary (si no lo tenía) para poder dar servicio (Failover).  A continuación se recuperará o reconstruirá la réplica Standby a partir del último backup.  **Procedimiento**:  Consultar 13. HRE PCT PR Recuperación ante Indisponibilidad del CPD Principal de RSI |

Batch Server

|  |  |
| --- | --- |
| Servidores | BA01 |
| Ubicación | RSI |
| Escenario Caída Parcial | Se restaurará del backup disponible el filesystem, en otra máquina que se habilitará en ese momento. |
| Escenario Indisponibilidad Total | Activación Plan de Contingencia (Ver 13. HRE PCT PR Recuperación ante Indisponibilidad del CPD Principal de RSI) |

CORRUPCIÓN/RESTAURACIÓN BASE DE DATOS

|  |  |
| --- | --- |
| Ámbito | Servidores BBDD (BD02, BD01) ubicados en RSI |
| Escenario | Corrupción/Restauración BBDD |
| Procedimiento | Una vez detectado el incidente y determinado su alcance (parcial o total):   * Si se trata de la corrupción de un conjunto de tablas (daño parcial), se restaurará partiendo de la copia lógica (dump) que realizamos diariamente de la BBDD de producción como parte del Plan de Contingencia. * Si se trata de la corrupción de un esquema completo, se restaurará partiendo de la copia lógica (dump) diaria que realizamos diariamente de la BBDD, salvo ADJ\_ADJUNTOS. En caso de requerir otro PITR, se restaurará la BBDD de la copia de seguridad de RMAN en otro almacenamiento, para recuperar lógicamente el esquema hasta la fecha necesaria e importar en la base de datos de producción. * Si se trata de la pérdida de algún otro objeto de base de datos, como vistas, índices, procedimientos, etc., se restaurará desde la copia lógica (dump) que realizamos diariamente.   Además se notificará sobre la situación a RSI a fin de que no tengan en cuenta las alertas que puedan surgir, indicando el rango horario de la intervención, o bien hasta nuevo aviso, evitando de esta manera falsas alertas de monitorización. |

FALLO DEL FICHERO DE APROVISIONAMIENTO

|  |  |
| --- | --- |
| Ámbito | Batch server (BA01) ubicado en RSI |
| Escenario | Fallo del fichero de aprovisionamiento de SAREB |
| Procedimiento | **Descripción de la operativa habitual:**  Los ficheros son generados por Bankia y enviados mediante SFTP a PFS para su carga en la cartera de Haya-Sareb.  **Modo de Detección del fallo:**  El proceso de carga orquestado por PFS, enviará un mail ante cualquier fallo en la misma al equipo de operaciones.  **Procedimiento**:  Si el fallo se debe a "fallo del fichero de aprovisionamiento", se avisará a Pilar Carpio y Silvia Díaz (HRE).  En caso de recibir los ficheros fuera de horario, se solicitará autorización a Pilar Carpio y Silvia Díaz (HRE) para realizar la carga. |

ANEXOS

ANEXO I: PERSONAS DE CONTACTO

**RSI**

**Fuera de horario:** hay que llamar a SALA al teléfono 918 070 255, el correo es prexexso@cajarural.com.

**En horario laboral:** centralita, el número es 918 070 100.

Existe una persona de arquitectura asignada encargada de coger todas las peticiones recibidas de PFS, sus datos son:

* Correo: rsisar@cajarural.com
* Correo personal: silvia\_martinez\_rsi@cajarural.com
* Teléfono: 918 076 756
* Móvil: 649 344 534

En caso de no lograr contactar por ninguna de las vías anteriores, se pueden utilizar los siguientes contactos:

|  |  |  |  |
| --- | --- | --- | --- |
| Departamento | Nombre | Correo | Teléfono/s |
| Compras | Andres Hernández | andres\_hernandez\_rsi@cajarural.com | 918 078 338  669 890 367 |
| Producción | Javier Cia | javier\_cia\_rsi@cajarural.com | 629 36 95 21 |
| Backup | Jorge Castillón | jorge\_castillon\_rsi@cajarural.com | 639 76 24 75 |

**PFS**

Buzones:

* guardias-devops@pfsgroup.es
* Teléfono de guardia explotación: 960 643 409

|  |  |  |  |
| --- | --- | --- | --- |
| Departamento | Nombre | Correo | Teléfono/s |
| Dirección IT | Pedro Blasco | pedro.blasco@pfsgroup.es | 691 032 291 |
| Explotación / Técnica de Sistemas | Miguel Delgado | miguel.delgado@pfsgroup.es | 618 615 109 |
| Administración BBDD | Félix de Lelis | felix.delelis@pfsgroup.es | 625 101 215 |
| Operaciones | Vicente Orón | vicente.oron@pfsgroup.es | 652 579 764 |

**HRE**

|  |  |  |  |
| --- | --- | --- | --- |
| Departamento | Nombre | Correo | Teléfono/s |
| Dpto. de Sistemas | Antonio Obón | aobon@haya.es | 659 836 112 |

ANEXO II: POLÍTICA DE RESPALDO DE DATOS Y PLANIFICACIÓN DE LAS COPIAS DE SEGURIDAD



ANEXO III: ESQUEMA DEL SISTEMA DE INFORMACIÓN RECOVERY SAREB

