

# Plan de Contingencia

ESTACIÓN DE TRENES DE BURGOS

David Herrero de la Peña | Seguridad Informática | 26 de marzo de 2014

## Contenido

[Qué es un Plan de Contingencia. 3](#_bookmark0)

[Por qué implementar un plan de contingencia. 4](#_bookmark1)

[Introducción 5](#_bookmark2)

[Objetivos 5](#_bookmark3)

[General 5](#_bookmark4)

[Específicos 5](#_bookmark5)

[Fase 1: Análisis de la organización 6](#_bookmark6)

[Fase 2: Análisis de Riesgos 7](#_bookmark7)

[Fase 3: Planes de Contingencia 9](#_bookmark8)

[PC 1: Riesgo 1-3, Incendios-Sismos 10](#_bookmark9)

[*Plan de Respaldo 10*](#_bookmark10)

[*Plan de Emergencia 10*](#_bookmark11)

[*Plan de Recuperación 11*](#_bookmark12)

[PC 2: Riesgo 2: Inundaciones 12](#_bookmark13)

[*Plan de Respaldo 12*](#_bookmark14)

[*Plan de Emergencia 12*](#_bookmark15)

[*Plan de recuperación 12*](#_bookmark16)

[PC 3: Riesgo 4-5, Corte eléctrico-Fallo generador auxiliar 14](#_bookmark17)

[*Plan de Respaldo 14*](#_bookmark18)

[*Plan de emergencia 14*](#_bookmark19)

[*Plan de Recuperación 14*](#_bookmark20)

[Pc 4: Riesgos 7-12-13, Robo de información, robo de equipos, vandalismo 15](#_bookmark21)

[*Plan de Respaldo 15*](#_bookmark22)

[*Plan de Emergencia 15*](#_bookmark23)

[*Plan de Recuperación 16*](#_bookmark24)

[PC 5: Riesgo 8, Infección por Virus 17](#_bookmark25)

[*Plan de Respaldo 17*](#_bookmark26)

[*Plan de Emergencia 17*](#_bookmark27)

[*Plan de Recuperación 17*](#_bookmark28)

[PC 6: Riesgo 9-10, Fallo Servidor – Fallo estaciones de trabajo 18](#_bookmark29)

[*Plan de Respaldo 18*](#_bookmark30)

[*Plan de Emergencia 18*](#_bookmark31)

[*Plan de Recuperación 18*](#_bookmark32)

[PC 7: Riesgo 11: Ausencia de personal técnico en la estación 19](#_bookmark33)

[*Plan de Respaldo 19*](#_bookmark34)

[*Plan de Emergencia 19*](#_bookmark35)

[*Plan de Recuperación 19*](#_bookmark36)

[Bibliografía 20](#_bookmark37)

## Qué es un Plan de Contingencia.

En pocas palabras se podría decir que un plan de contingencia es una serie de procedimientos y actividades que debería realizar una empresa u organización en caso de un funcionamiento anormal de la misma, este funcionamiento anormal puede ser debido a un incidente interno o externo.

El que una organización reconozca que puede ser vulnerable en algunos casos implica un avance a la hora de superar cualquier imprevisto.

El plan de contingencia es el equivalente informático a los planes de continuidad de negocio que se dan en otros departamentos, pero debido a la importancia de la informática en las organizaciones de hoy en día, es el más relevante de todos.

El plan de contingencia se centra en la recuperación de los servicios y recursos de TI después de un desastre. Especifica los protocolos y procedimientos necesarios para la recuperación.

En el plan de contingencia deben aparecer las personas responsables de llevar a cabo cada una de las acciones, así como los recursos y servicios a lo que afectarán.

El plan de contingencia de una organización sigue típicamente el ciclo de vida PDCA (plan-do- check-act), es decir :

* “PLAN”- se analizan todos los riesgos y sus posibles consecuencias para la organización .
* “DO”- una vez identificadas las debilidades, se buscan posibles soluciones para evitarlos, o para paliar las consecuencias, siempre teniendo en cuenta que el coste de la prevención del riesgo no puede ser mayor que el coste de recuperación si no hubiera ningún plan especificado.
* “CHECK”- el plan de contingencia debe estar siempre actualizado, se debe actualizar más o menos cada seis meses, un plan de contingencia desactualizado no ayudaría en caso de una catástrofe y además crea una situación de false seguridad que hace que se preste menos importancia a nuevas amenazas.
* “ACT”- una vez que se produce la catástrofe o cualquier tipo de problema hay que consultar directamente al plan de contingencia y seguir cada uno de los procedimientos descritos en él.

Este ciclo de vida nunca se detiene, y una vez que se sale de la última parte se debe empezar de nuevo a planificar mejoras y a analizar nuevos riesgos posibles para la organización, con esto se consigue un proceso de mejora continua para el plan de contingencia y que nunca esté desactualizado.

Dentro del plan de contingencia se encuentran otros tres sub-planes:

* Plan de respaldo: ”antes”, aquí se definen las medidas preventivas a realizar antes de que se produzca la catástrofe o amenaza, la finalidad de estas medidas es evitar que se llegue a producir la amenaza, eliminando así cualquier problema que pudiera haber ocasionado. Por ejemplo, en los planes de emergencia puede estar estipulado que todas las salas que contengan equipos informáticos importantes deben estar a más de 3 metros sobre el nivel del suelo, o al menos, que las salas dispongan de un sistema de bombeado de agua, para evitar inundaciones en caso de tormentas fuertes.
* Plan de emergencia: ”durante” , en este caso se definen los procedimientos y los responsables de llevarlos a cabo en caso de que la amenaza ocurra, con el fin de minimizar los efectos producidos. Puede ser una parte crítica del proceso, ya que si se lleva bien a cabo

se pueden reducir al mínimo los efectos de una amenaza que en principio parecía muy peligrosa. Por ejemplo, y siguiendo la línea del ejemplo anterior, si se avecina una gran tormenta, en los planes de emergencia se puede estableces el cubrir todas las ventanas con protecciones y asegurar la estanqueidad de las salas con equipos informáticos para evitar inundaciones, o incluso apagar todos los equipos si se llegan a inundar las salas.

* Plan de recuperación: ”después” ,son las medidas necesarias después de que la amenaza

haya ocurrido y después de haberla controlado, gracias a los planes de emergencia, o porque la amenaza ha desaparecido sola. La finalidad de estos procedimientos es la de restaurar el estado de las cosas tal y como estaban antes de que ocurriera la amenaza.

En algunos casos , y para estar en consonancia con el modelo PDCA se puede tener un cuarto plan, llamado Plan de Pruebas, en el que estarán descritos los procedimientos y pruebas necesarios para testear el sistema.

En cada uno de estos planes estarán definidos, además de los procedimientos necesarios:

* Recursos necesarios y su ubicación.
* Personas implicadas en el plan, especialmente los responsables de cada uno de los procedimientos.
* Procedimientos detallados paso a paso.

## Por qué implementar un plan de contingencia.

El principal motivo al implementar un plan de contingencia es el de reducir costes, al crear el plan de contingencia hay que tener en cuenta que el coste de control de una amenaza nunca podrá ser mayor que el coste de recuperación de los problemas provocados por esa amenaza si no hubiera ningún plan.

Además al realizar el análisis de riesgos se consigue conocer la propia organización de una manera mucho más profunda, es importante saber lo que tenemos para poder empezar a realizar cualquier mejora.

Como resultado final, tener listo un plan de contingencia hará que en caso de accidente no perdamos clientes, reputación, imagen de empresa, datos, beneficios, etc. Y evitar así que por una amenaza la organización desaparezca.

# Plan de Contingencia: Estación

de Trenes Rosa de Lima

## Introducción

Desde los inicios de los sistemas de información se comprendió que las contingencias forman parte inherente de los mismos. Las amenazas a la información pueden provenir de muchas fuentes, tanto de origen natural (terremotos, tormentas, etc.), de origen humano (retaliaciones, celos profesionales, competencia, huelga, problemas laborales, entre otros), como de origen técnico (fallas del hardware, del software, con el suministro de energía, etc.). Y es casi siempre una situación no prevista la que regularmente provoca una crisis y las consecuencias de la misma, según su impacto y extensión, pueden ser catastróficas para los intereses de cualquier organización.

La nueva estación de trenes Rosa de Lima de Burgos, construida en el 2008, es un claro ejemplo de modernidad y de informatización de todos los componentes. Esto se plasma en el hecho de que para llegar a los andenes solo se pueda ir en escaleras mecánicas o en ascensores.

Esta estación se encuentra lejos del centro de la ciudad y además es la única estación de trenes que tiene esta ciudad, es por ello que el garantizar el funcionamiento de la estación es crucial para todos los viajeros que usan el tren diariamente en Burgos.

En este plan de contingencia, para cada una de las amenazas previstas se deberá tener un plan de contingencia con tres sub-planes, de **respaldo**, de **emergencia** y de **recuperación**. En el caso de las amenazas no-previstas se contará con un plan de emergencia y recuperación **común**.

Además cada uno de estos planes deberá tener un **responsable** encargado de la ejecución y organización del mismo.

## Objetivos

### GENERAL

El objetivo de este plan de contingencia es reanuda en el menor tiempo posible todas las actividades después de un fallo técnico y/o humano o después de una catástrofe natural.

Minimizando las molestias en los pasajeros para así no dañar la imagen de la empresa.

### ESPECÍFICOS

* Garantizar el funcionamiento de los sistemas de información y su recuperación en el menor tiempo posible de cualquier fallo que interrumpa el servicio.
* Mantener la estación conectada permanentemente a los servicios centrales de ADIF.
* Minimizar el uso de recursos en caso de emergencia.
* Evitar la incomunicación total de los pasajeros que usen el servicio de ferrocarril en burgos.

## Fase 1: Análisis de la organización

*“Esta parte del documento se ha realizado basándose en estimaciones, ya que por el momento ADIF no ha respondido a los email que he enviado para preguntar sobre la estructura informática implantada en la estación de trenes Rosa de Lima*

***26 marzo****: Buenas tardes, al tratarse de información de un activo que no es de nuestra Dirección, hemos remitido su solicitud al área de Estaciones de ese ámbito.*

*Muchas gracias. Atentamente,* [*redconvencional@adif.es*](mailto:redconvencional@adif.es)*”*

La primera parte para realizar el plan de contingencia es un análisis de los activos disponibles.

Se hará primero una división por tipo de activos, y luego otra división por localización de los mismos.

#### TIPO DE ACTIVO

* **Software**: Windows 7 SP 1, Antivirus Microsoft Security Essentials, Suite Microsoft Office, Base de Datos Oracle, Software gestión de billetes ADIF, Software gestión de llegadas/salidas de trenes ADIF, Software de comunicación con el centro de operaciones ADIF, SO Ubuntu Server, Trend Micro ProtectLink Gateway, Administración de servidor UCS y de sistemas Cisco.
* **Hardware**: Terminales de operaciones Intel core i5 x10 unidades,monitores lcd 23” x20 unidades, impresora canon i-SENSYS LBP6680x x2 unidades, Máquinas impresoras de billetes x6 unidades, Switch Cisco Small Business de la serie 500 x4 unidades, Router Cisco SRP521W-U 4 2 unidades, Servidores de rack Cisco UCS de la serie C x1 unidad.
* **Conectividad**: Cableado fast Ethernet cat 6, 40 tomas Ethernet, acceso a red interna de ADIF mediante VPN.
* **Hot Room**: Unidad móvil con conexión a la red via satélite, servidor CISCO preparado para suplir al servidor del CPD y una estación de trabajo. Generador propio de corriente.

#### LOCALIZACION ACTIVO

* **Venta de tickets**: sala de venta de tickets, 6 ordenadores intel i5, 6 pantallas, 1 impresora1, 13 tomas fast Ethernet, 1 Router cisco, 4 máquinas impresoras de billetes, 1 switch cisco. Todos los ordenadores con suit office, antivirus, y software de comunicación con el centro de operaciones ADIF, software de gestión de billetes.
* **CPD**: Servidor de rack CISCO serie C, Trend Micro ProtectLink Gateway, SW Administración de servidor CISCO, Base de datos Oracle, SO Ubuntu Server, Software comunicación ADIF, 1 Router CISCO,1 Switch CISCO,1 monitor,7 Conexiones Ethernet.
* **Oficinas**: 4 ordenadores Intel i5,4 pantallas, 1 impresora, Microsoft Office, antivirus, Software ADIF comunicación, 1 router CISCO, 1 Switch CISCO, 10 salidas Ethernet.
* **Resto de estación**: 10 monitores, 2 máquinas impresoras de billetes, 1 router CISCO, 1 Switch CISCO, 20 salidas Ethernet.
* **Hot Room**: Servidor CISCO x1, SO Ubuntu server con Oracle, estación de trabajo x1. Grupo electrógeno independiente.

La sala del CPD se encuentra en la planta 0, tiene un sistema de refrigeración propio y dispone de un SAI alimentado por un generador independiente de Gas-oil que se encuentra en una sala separada e ignífuga.

La venta de tickets también se encuentra en el piso 0, junto a las oficinas. No disponen de SAI, y la refrigeración es la común al resto de la estación.

Una vez identificados los activos que tiene la estación es momento de definir los responsables de llevar a cabo los planes de contingencia, esta división se ha hecho teniendo en cuenta la división física de la estación para asegurar así una rápida ejecución del plan de contingencia:

* **CPD**: el administrador de sistemas será el encargado de llevar a cabo todas las acciones necesarias que involucren a cualquier activo que se encuentre dentro del CPD o que dependa directamente del mismo.
* **Venta de tickets**: cada uno de los empleados será responsable de llevar las acciones necesarias en su puesto de trabajo, siempre coordinados por el jefe de la sección.
* **Oficinas**: El director de la oficina será el encargado de supervisar todo el procedimiento y de llevar a cabo las acciones necesarias sobre las partes comunes, pero cada empleado deberá llevar a cabo el plan sobre su propio puesto de trabajo.
* **Resto de estación**: el administrador de sistemas será el encargado de designar un responsable para que actúe en el resto de la estación mientras él se encarga del manejo del CPD.

## Fase 2: Análisis de Riesgos

Ahora se van a analizar todos los riesgos a los que está expuesta la estación de trenes, se dividirán por la frecuencia de ocurrencia (1-remoto, 2-ocasional,3-problable,4-recurrente) y por la cantidad de daños que ocasionarían (1-poco,2-moderado,3-alto,4-gran daño), siendo el significado de los daños:

* Poco: no afecta al normal funcionamiento de la estación pero puede ocasionar molestias a viajeros o al personal.
* Moderado: afecta al normal funcionamiento de la estación, pero todavía es posible el uso de la estación por los viajeros.
* Alto: la estación no puede seguir funcionando y por lo tanto habría que recurrir a medios alternativos para acomodar a los viajeros.
* Grand daño: la estación quedaría inutilizada por un periodo muy largo en el tiempo.

En la ocurrencia de los riesgos no puede haber ninguno que sea continuo, en ese caso no sería un riesgo si no un problema conocido y habría que solucionarlo por medio de otras actuaciones y no con un plan de contingencia.

La importancia de un riesgo vendrá condicionada por la suma de estas dos variables, siendo un riesgo de nivel 2 el menos importante y uno de nivel 8 el más importante.

Además habrá que tener en cuenta si el riesgo es controlable/predecible, o no controlable/predecible, para aplicar entonces un plan u otro.

También habrá que tener en cuenta a que afecta el riesgo, a la infraestructura, a los servicios prestados, al personal, o a la información.

Para resumir los riesgos se presentarán los mismos en una tabla.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Numero** | **Riesgo** | **Afecta a** | **Daño** | **Ocurrencia** | **Importancia** |
| **1** | Incendio | Infraestructura, Personal, Datos, Servicios | Alto-Gran Daño | Remoto | 4-5 |
| **2** | Inundación | Infraestructura, Datos, Servicios | Alto | Remoto | 4 |
| **3** | Sismo | Infraestructura, Personal, Datos, Servicios | Gran Daño | Remoto | 5 |
| **4** | Corte suministro eléctrico | Servicios, Datos | Moderado | Probable | 5 |
| **5** | Fallo generador aux | Servicios, Datos | Alto | Ocasional | 5 |
| **6** | Corte suministro internet | Servicios, Datos | Poco | Recurrente | 5 |
| **7** | Robo de Información | Datos | Poco | Ocasional | 3 |
| **8** | Infección por virus | Servicios, Datos | Poco | Ocasional | 3 |
| **9** | Fallo del Servidor | Servicios, Datos | Poco | Ocasional | 3 |
| **10** | Fallo estaciones de trabajo | Servicios, Datos | Poco | Recurrente | 5 |
| **11** | Ausencia personal técnico | Personal, Servicios | Poco | Probable | 4 |
| **12** | Robo de equipos importantes | Infraestructura, Datos | Moderado | Ocasional | 4 |
| **13** | Vandalismo | Infraestructura | Poco | Recurrente | 5 |

## Fase 3: Planes de Contingencia

En este apartado, para cada uno de los riesgos identificados se creará un plan de contingencia, en caso de que alguno de los riesgos afecten a los mismos elementos y se puedan evitar con las mismas medias se desarrollarán juntos.

En caso de que el riesgo sea predecible también habrá un plan de respaldo, además de los planes de emergencia y recuperación comunes a todos.

En la imagen siguiente se ve cual debe ser el flujo normal en caso de un incidente:

Ocurre el evento Informar al responsable

Iniciar el plan de Emergencia

Evaluar los daños

Iniciar el plan de Recuperación

Informe final

*Ilustración 1 Flujo en caso de evento*

### PC 1: RIESGO 1-3, INCENDIOS-SISMOS

En este plan se recogen las operaciones necesarias en caso de que se produzca un incendio total o al menos en alguna de las salas que contienen equipos informáticos.

El objetivo es minimizar los daños producidos por el fuego/terremoto y la pérdida total o parcial de los datos.

Este plan de contingencia deberá ser lanzado en cuanto se encuentren indicios de un fuego: humo, corte de la red, etc.

Contactos necesarios:

* Emergencias: 112
* Administrador de Sistemas : xxx xxx xxx Responsable:
* Administrador de Sistemas: xxx xxx xxx
* Jefe de oficina: xxx xxx xxx

### Plan de Respaldo

Para evitar que se produzcan incendios en las instalaciones se deberán tener presentes las siguientes normas:

* Instalar extintores en todas las salas que contengan equipos informáticos.
* Verificar periódicamente la fecha de caducidad de los extintores.
* Los extintores deben ser de CO2 para evitar dañar los equipos informáticos con agua.
* Limpiar con frecuencia el sistema de refrigeración del CPD para evitar la acumulación de suciedad.
* Comprobar periódicamente las tomas de corriente para detectar fallas.
* Evitar el uso de alargadores conectados en paralelo.
* Comprobar que el aislante ignifugo del CPD se encuentra en buenas condiciones y no tiene fisuras.
* Guardar las copias de seguridad diarias en una caja fuerte en otra sala sin ningún equipo informático ni tomas de corriente.
* Llevar las copias de seguridad semanales a una caja fuerte situada en otro edificio de Burgos.
* Charlas sobre prevención de fuegos y accidentes.
* Instalar detectores de humo en el CPD.

### Plan de Emergencia

Estas acciones se deberán llevar a cabo en cuanto se produzca el fuego, todo coordinado por el responsable.

1. Avisar a emergencias cuando se ha producido el fuego y en qué lugar.
2. Avisar a todo el personal que evacúe las zonas peligrosas.
3. Si el fuego es muy pequeño:
   1. Apagar el fuego con los extintores de CO2.
   2. Intentar extraer los medios de almacenamiento del servidor.
   3. Empezar a trabajar con la unidad móvil.
   4. Si se apaga pasar al plan de Recuperación.
4. Si el fuego es relativamente grande:
   1. Cortar el suministro eléctrico de inmediato.
   2. Evacuar a zona segura y seguir las indicaciones de los equipos de emergencia.
   3. Evaluar si hay algún herido y asegurarse de que sea atendido de inmediato.

### Plan de Recuperación

Estas acciones se llevarán a cabo una vez el incendio se haya extinguido por completo y los cuerpos de emergencia se hayan marchado.

* Evaluar los daños producidos por el incendio, tanto en infraestructura como personales.
* Inventario general de todos los elementos afectados.
* En caso de activos dañados dar la orden de recuperación o de sustitución oportuna.
* Si el incendio ha supuesto la pérdida de datos restaurar el sistema a un estado consistente con las copias de seguridad disponibles.
* Realizar un informe con las causas del incendio y la actuación efectuada para mejorar el plan de contingencia.

Una vez se hayan realizado todas las acciones el responsable podrá cerrar el plan de contingencia y pasar a un normal funcionamiento de la estación.

### PC 2: RIESGO 2: INUNDACIONES

Debido a la situación de la estación en la parte baja de una ladera y por la situación en la planta 0 del CPD es posible que ocurran inundaciones debido a fuertes tormentas o deshielos repentinos.

Este plan no se deberá lanzar solo en caso de grandes inundaciones, si no también en caso de pequeñas inundaciones producidas por fallos en el sistema de cañerías y sanitarios.

Contactos necesarios:

* Emergencias: 112
* Administrador de Sistemas : xxx xxx xxx
* Servicio técnico : xxx xxx xxx Responsable:
* Administrador de Sistemas: xxx xxx xxx
* Jefe de oficina: xxx xxx xxx

### Plan de Respaldo

* Instalar y verificar el funcionamiento de bombas de achique en el CPD.
* Limpiar las rejillas de evacuación situadas en la planta baja.
* Tener preparados pequeños sacos de arena para aislar el CPD en caso de inundación.
* Prohibir la entrada de líquidos en el CPD.

### Plan de Emergencia

1. Si la inundación es alta
   1. Llamar al número de emergencias y explicar la situación
   2. Avisar a todo el personal de que evacue los puestos de trabajo
   3. Desconectar toda la red eléctrica
   4. Seguir la indicaciones del personal de emergencias
2. Si la inundación es relativamente pequeña
   1. Avisar a todo el personal de que aplique el plan de contingencia
   2. Desconectar todos los aparatos eléctricos
   3. Sacar los medios de almacenamiento del servidor y llevarlos a otro lugar (oficina móvil)
   4. Usar los sacos de arena para contener el agua en un lugar
   5. Encender las bombas de achique si fuera necesario
   6. Secar todo los aparatos afectados
   7. No encender los equipos aunque parezcan secos, llamar al servicio técnico para que recuperen todo lo posible.
   8. Seguir trabajando y ofreciendo el servicio en la medida de lo posible desde la oficina móvil.

### Plan de recuperación

Una vez que la inundación haya pasado y todos los equipos estén totalmente secos:

* Volver a conectar el suministro eléctrico
* Volver a instalar los medios de almacenamiento en el CPD
* Si no funcionan usar una copia de seguridad inmediatamente anterior
* Si algún componente no funciona correctamente pedir su sustitución
* Realizar un informe con el inventario actual, fallos, y consecuencias de la inundación.

### PC 3: RIESGO 4-5, CORTE ELÉCTRICO-FALLO GENERADOR AUXILIAR

Este plan se deberá poner en marcha en cuanto se produzca un corte de luz, debido a un cortocircuito, una tormenta, o un fallo en el suministro generalizado.

Contactos necesarios:

* + Administrador de Sistemas : xxx xxx xxx
  + Servicio técnico : xxx xxx xxx
  + Empresa red eléctrica: xxx xxx xxx Responsable:
  + Administrador de Sistemas: xxx xxx xxx
  + Jefe de oficina: xxx xxx xxx

### Plan de Respaldo:

En caso de corte eléctrico o de fluctuaciones en la tensión de la red el CPD está conectado detrás de un SAI que debería evitar sobrecargar y apagones repentinos. Una vez que el SAI ha entrado en funcionamiento por un corte en la red eléctrica lo suficientemente continuado (5 minutos) el grupo electrógeno auxiliar entraría en funcionamiento automáticamente. Las oficinas y los puestos de venta de tickets podrían verse interrumpidos por falta de corriente eléctrica, en ese caso se debería conectar una estación de trabajo en uno de las tomas de corriente indicadas como “aux”, las cuales están conectadas también al grupo electrógeno y deberían permitir ofrecer los servicios mínimos a los viajeros.

Además:

* + Revisar regularmente las instalaciones eléctricas en busca de componentes en mal estado.
  + Arrancar cada semana el grupo electrógeno para limpiar el circuito de carburante.
  + Revisar el nivel de aceite y gas-oil del grupo electrógeno cada semana.
  + Evitar conectar en las tomas marcadas como “aux” aparatos no necesarios para el funcionamiento de la estación.

### Plan de emergencia:

En caso de corte del suministro eléctrico, el SAI y el grupo electrógeno deberían entrar en funcionamiento y el servicio no se vería afectado.

En caso de que el grupo electrógeno también fallase y se produjera un fallo eléctrico total:

1. Avisar a todo el personal que apague los equipos que sigan encendidos de forma segura.
2. Llamar al proveedor de energía para comprobar si es un fallo generalizado o local
3. Movilizar la oficina móvil para seguir prestando lo servicios mínimos.
4. Intentar descubrir el origen del fallo y llamar al servicio técnico para que hagan las reparaciones oportunas.

### Plan de Recuperación:

Una vez restablecida la corriente eléctrica trasladar los nuevos datos desde la afina móvil hasta el CPD, y volver a arrancar todos los equipos de forma paulatina. En caso de que el grupo electrógeno haya fallado llamar al servicio técnico para su reparación. Elaborar un informe.

### PC 4: RIESGOS 7-12-13, ROBO DE INFORMACIÓN, ROBO DE EQUIPOS, VANDALISMO

Todos estos riesgos tienen un factor común y es el hecho de que son realizados por personas (internas o externas) de forma voluntaria.

Estas mediadas también serán aplicables cuando se produzca una pérdida de información de forma involuntaria por culpa del personal interno.

Contactos necesarios:

* + Administrador de Sistemas : xxx xxx xxx
  + Servicio técnico : xxx xxx xxx
  + Policía : 091 Responsable:
  + Administrador de Sistemas: xxx xxx xxx
  + Jefe de oficina: xxx xxx xxx

### Plan de Respaldo:

Para evitar todos estos riesgos se deben seguir estos procedimientos:

* + Cada usuario de las aplicaciones del sistema deberá tener un password suficientemente largo y cambiarlo cada 3 meses, además se impartirán charlas para concienciar a todo el personal.
  + La red que se use para las aplicaciones de ADIF deberá estar separada físicamente de la red a la que puedan acceder los usuarios, y en ningún caso se hará por medio de alguna red Wireless.
  + Se instalarán cámaras de vigilancia en la estrada y en el mismo CPD.
  + El acceso al CPD estará restringido al administrador de sistemas y a los encargados que el crea conveniente, siempre mediante el uso de tarjetas personales y un sistema de identificación biométrico.
  + Todos los equipos personales tendrán un sistema antivirus y tendrán los puertos usb bloqueados.
  + En el servidor estará instalado y configurado un cortafuegos.
  + Habrá un guardia de seguridad patrullando toda la zona común para evitar actos vandálicos.

### Plan de Emergencia:

En cuanto se detecte el robo de información:

1. Desconectar el equipo del que se haya robado la información para evitar que el atacante lo use como puerta de enlace.
2. Monitorear todos los accesos las conexiones establecidas durante el robo.
3. Investigar los datos robados y su importancia.
4. Si además los datos han sido robados, restaurar a una versión anterior con las copias de seguridad.
5. Si el atacante es el propio personal de la estación, abrir diligencias contra sus actos e

investigar los motivos.

1. Elaborará un informe con las causas del robo y los medios utilizados. En caso de robo de equipos o vandalismo:
2. Avisas a la policía tan pronto como se descubran estos actos.
3. Evacuar a todo personal fuera del edificio o si no fuera posible a la sala del CPD.
4. Interrumpir las comunicaciones internas e intentar desconectar todos los equipos correctamente para evitar corrupción de datos.
5. Seguir las órdenes de los cuerpos de seguridad.

### Plan de Recuperación:

Este plan entrará en ejecución en cuanto se retiren los cuerpos de seguridad o se haya identificado al autor del robo de información.

* + Identificar los elementos afectados, repararlos o sustituirlos.
  + Tomar medidas de seguridad oportunas para que no vuelva a suceder el mismo accidente.

### PC 5: RIESGO 8, INFECCIÓN POR VIRUS

En este apartado se describen los procedimientos en caso de infección de una estación de trabajo por un virus informático, sea cual sea su naturaleza.

Contactos necesarios:

* + Administrador de Sistemas : xxx xxx xxx
  + Servicio técnico : xxx xxx xxx Responsable:
  + Administrador de Sistemas: xxx xxx xxx
  + Jefe de oficina: xxx xxx xxx

### Plan de Respaldo:

Para evitar la infección por virus:

* + Los equipos de trabajo conectados a la red dispondrán de un sistema antivirus instalado y actualizado.
  + La navegación estará restringida a las páginas necesarias para la prestación del servicio, como por ejemplo a la página principal de ADIF.
  + Se darán charlas al personal sobre los peligros de internet y como evitarlos.
  + Se instalarán cortafuegos en todos los routers del sistema.
  + No se permitirá el uso de pen drives en las estaciones de trabajo.
  + Aplicar filtros en el servidor de correo para evitar la entrada de spam en el sistema.

### Plan de Emergencia:

Una vez se haya detectado la presencia de un virus en el equipo, ya sea por un aviso del antivirus o por que el usuario note comportamientos extraños:

1. Seguir las instrucciones del equipo antivirus si las ofrece.
2. Llamar al servicio técnico y seguir las instrucciones.
3. Desconectar el equipo de la red para evitar infectar a más estaciones de trabajo.
4. En caso de no poder eliminar el virus, hacer un respaldo de los datos importantes alojado en el disco y volver a instalar todo el SW.

### Plan de Recuperación:

1. Mantener el equipo en cuarentena y bajo supervisión una semana después de que se infectara para comprobar que el virus ha sido eliminado completamente.
2. Analizar los logs del firewall para comprobar si ha sido un ataque externo o interno.
3. Analizar los daños ocasionados, y en caso necesario, usar una copia de seguridad anterior para volver a un estado consistente.
4. Realizar un informe con toda la información disponible, tanto del virus, como del procedimiento seguido para eliminarlo.

### PC 6: RIESGO 9-10, FALLO SERVIDOR – FALLO ESTACIONES DE TRABAJO

Este plan se deberá llevar a cabo cuando se detecte una falla en alguno de los equipos informáticos de los que se dispone en la estación de trenes.

Contactos necesarios:

* + Administrador de Sistemas : xxx xxx xxx
  + Servicio técnico central ADIF Madrid: xxx xxx xxx
  + Servicio técnico : xxx xxx xxx
  + CISCO: xxx xxx xxx Responsable:
  + Administrador de Sistemas: xxx xxx xxx
  + Jefe de oficina: xxx xxx xxx

### Plan de Respaldo:

Para evitar en la medida de lo posible fallos en los equipos informáticos:

* + Revisar periódicamente el estado de los conectores de todos los equipos informáticos.
  + Evitar enredos entre los cables de los aparatos eléctricos.
  + Sustituir lo antes posible las piezas que empiecen a mostrar un comportamiento anómalo.

### Plan de Emergencia:

En caso de que falle algún equipo o parte del mismo:

1. Avisar al servicio técnico y al administrador de sistemas si fuera necesario.
2. Evaluar la importancia del equipo, si se puede seguir ofreciendo el servicio de forma normal llamar al servicio técnico para que tengan constancia del fallo y lo arreglen lo antes posible.
3. Si no se puede seguir ofreciendo el servicio a causa del fallo (fallo del servidor), extraer los medios de almacenamiento y trasladarlos a la oficina móvil para no interrumpir el servicio.
4. Buscar el origen del fallo, en caso de encontrarlo, intentar solucionarlo consultando la documentación del frabricante.

### Plan de Recuperación:

* + Sustituir el equipo o la pieza que no funcione.
  + Comprobar que el resto de equipos con las mismas características no presenten ese fallo o signos de que vayan a fallar en el futuro inmediato.
  + Avisar a la empresa suministradora en caso de malfuncionamiento continuado.
  + Realizar un informe con las posibles causas del fallo.

### PC 7: RIESGO 11: AUSENCIA DE PERSONAL TÉCNICO EN LA ESTACIÓN

Este plan se deberá llevar a cabo cuando se produzca la ausencia de parte del personal técnico (administrador de sistemas, servicio técnico) en el momento de toma de decisiones claves que requieran de su conocimiento, normalmente durante la ejecución de cualquier otro plan de contingencia.

Contactos necesarios:

* + Administrador de Sistemas : xxx xxx xxx
  + Servicio técnico central ADIF Madrid: xxx xxx xxx
  + Servicio técnico : xxx xxx xxx Responsable:
  + Administrador de Sistemas: xxx xxx xxx
  + Jefe de oficina: xxx xxx xxx

### Plan de Respaldo:

* + El jefe de informática de la estación de trenes deberá asegurarse de que su compañero de trabajo reciba la formación necesaria para poder llevar a cabo su trabajo en caso de emergencia.
  + El personal técnico deberá comunicar con la máxima anticipación posible su ausencia durante una jornada de trabajo.
  + Establecer un sistema de control de asistencia para asegurar que todo el personal cumple con su horario estipulado.

### Plan de Emergencia:

Si se produce la ausencia de parte importante del personal técnico en un momento de necesidad, se deberán seguir los siguientes procedimientos.

1. Hablar con otro empleado del servicio técnico presente e intentar resolver el problema él.
2. Si no se ha podido resolver el problema, llamar al servicio técnico central para obtener asistencia telefónica o por cualquier otro medio disponible.

### Plan de Recuperación:

Será en personal de servicio técnico ausente el encargado de restituir el sistema a su normal funcionamiento en el momento de su vuelta, si el personal técnico ausente no volviera contactar con el departamento de recursos humanos para la sustitución del mismo. Dicho contacto no se deberá hacer antes de las primeras 8 horas desde la ausencia ni más tarde de 24 horas.

## Bibliografía

* + <http://www.slideshare.net/ydaleuporsiempre_16/plan-de-contingencia-8874729>
  + <http://www.imarpe.pe/imarpe/archivos/informes/imarpe_resol_de_158_2012_conting.pdf>
  + [http://victdelr.wordpress.com/category/guia-para-elaborar-un-plan-de-contingencia-](http://victdelr.wordpress.com/category/guia-para-elaborar-un-plan-de-contingencia-informatico/) [informatico/](http://victdelr.wordpress.com/category/guia-para-elaborar-un-plan-de-contingencia-informatico/)
  + [https://www.inteco.es/extfrontinteco/es/pdf/Formacion\_Plan\_Contingencias\_Informaticas.](https://www.inteco.es/extfrontinteco/es/pdf/Formacion_Plan_Contingencias_Informaticas.pdf) [pdf](https://www.inteco.es/extfrontinteco/es/pdf/Formacion_Plan_Contingencias_Informaticas.pdf)
  + [http://www.esevictoria.gov.co/sitio2/SGSI/DOCUMENTOS%20PLAN%20DE%20CONTING](http://www.esevictoria.gov.co/sitio2/SGSI/DOCUMENTOS%20PLAN%20DE%20CONTINGENCIA/Plan%20_Contingencia_Documento_HLV.pdf) [ENCIA/Plan%20\_Contingencia\_Documento\_HLV.pdf](http://www.esevictoria.gov.co/sitio2/SGSI/DOCUMENTOS%20PLAN%20DE%20CONTINGENCIA/Plan%20_Contingencia_Documento_HLV.pdf)
  + <http://www.adif.es/es_ES/index.shtml>
  + <http://www.cisco.com/es/>
  + Teoría explicada en clase