UNIVERSIDAD
DE BURGOS

PLAN DE CONTINGENCIA:

ESTACION DE CIUDAD REAL

EDUARDO MORA GONZALEZ

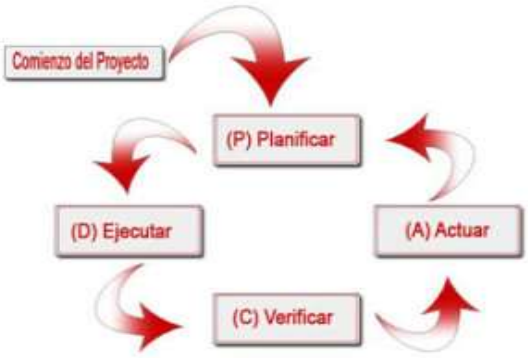
Contenido

1. INTRODUCCIÓN

Un plan de contingencia **[R1]** es un modelo sistemático de actuación que tiene por objeto anticiparse a situaciones en que esté próximo un daño o en que exista la posibilidad de que éste suceda o no.

Por ello, para realizar una correcta gestión de los riesgos empresariales, es necesario realizar este tipo de plan para conseguir reducir el impacto de los cambios.

Normalmente un plan de contingencia tiene un ciclo de vida **[R2]** PDCA (Planificar → hacer → comprobar → actuar), este plan nace de un análisis de riesgos donde se identifican las amenazas que pueden afectar a la continuidad de negocio.



El plan de contingencia se revisará periódicamente. Generalmente la revisión suele venir acompañada sobre un nuevo análisis de riesgos. Adicionalmente, el plan de contingencia debe expresar claramente:

- El personal implicado en el cumplimiento del plan y su rol dentro del mismo.
- Qué recursos materiales y técnicos son necesarios.
- Cómo son los protocolos de actuación que se deben seguir.

1.1. ISO 22301

La norma ISO 22301 especifica los requisitos para un sistema de gestión encargado de proteger a su empresa de incidentes que provoquen una interrupción en la actividad, reducir la probabilidad de que se produzcan y garantizar la recuperación de su empresa.

Una adecuada gestión de la continuidad del negocio permite a las organizaciones: [**R3]**

- Tener la capacidad de resistir los efectos de un incidente (resilencia) así como prevenir o evitar los posibles escenarios originados por una situación de crisis.
- Gestionar la interrupción de sus actividades minimizando las consecuencias económicas, de imagen o de responsabilidad civil derivadas de la misma.
- Adquirir una mayor flexibilidad ante la interrupción de sus actividades.
- Reducir los costes asociados a la interrupción.
- Evitar penalizaciones por incumplimiento de contratos como proveedor de productos o servicios.
- Disponer de una metodología estructurada para reanudar sus actividades después de una interrupción.
- Aumentar su prestigio ante clientes y partes interesadas.
- Posibilidad de ventajas económicas a la hora de contratar seguros empresariales.

2. PLAN DE CONTINGENCIA: ESTACIÓN DE CIUDAD REAL

El plan de contingencia desarrollado a continuación tiene como objetivo el de reanudar en el menor tiempo posible el funcionamiento de la estación después de un incidente tanto natural como humano. Para ello, se deben cumplir los siguientes objetivos parciales:

- Mantener la estación conectada permanentemente a los servicios centrales.
- Evitar la incomunicación total de los pasajeros.
- Minimizar el uso de recursos en caso de emergencia.

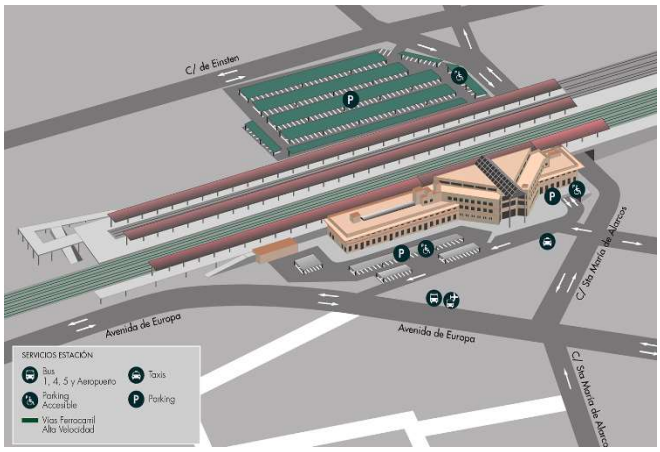
2.1. FASE I: ANÁLISIS A NIVEL DE LA ORGANIZACIÓN

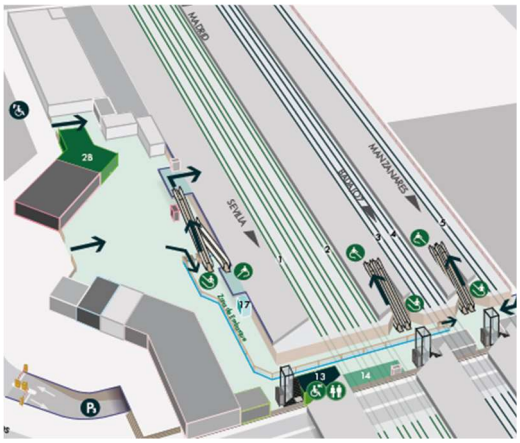
La organización es una entidad pública empresarial española dependiente del Ministerio de Transportes, Movilidad y Agenda Urbana, que tiene como objetivo la construcción de líneas de ferrocarril y la gestión de su explotación.

Centrándonos en la estación de Ciudad Real fue inaugurada en 1992 tras la puesta en marcha de la alta velocidad Madrid-Sevilla. La estación que se encuentra situada a 633,84 metros de altitud forma parte de los trazados de las siguientes líneas de ferrocarril:

- Línea férrea de ancho ibérico Manzanares-Ciudad Real, punto kilométrico 262.2
- Línea férrea de ancho ibérico Ciudad Real-Badajoz, punto kilométrico 175.2
- Línea férrea de ancho internacional y alta velocidad Madrid-Sevilla punto kilométrico 170,748.3

La distribución de la estación es la siguiente:





En esta primera imagen **[R4]** disponemos de una visión global de la localización de la estación y todo lo que dispone a su alrededor. En la segunda imagen **[R4]** se muestra el plano del interior de la estación.

2.1.1. ACTIVOS DE LA ESTACION

La estación cuenta con los siguientes activos:

- **Activos Software:**
    - El sistema operativo usado es Windows 10 con las herramientas de seguridad que este dispone.
    - La base de datos esta centralizada y esta implementada en ORACLE.
    - Para la gestión de los billetes se usa el software propio de la organización.
    - Para el control de llegadas y salida, se usa el software implementado por DEIMOS SPACE.
    - Para la comunicación usan los sistemas Cisco.

- **Activos Hardware:**
    - Terminales de operaciones Intel i7 con su monitor correspondiente.
    - Impresora HP jet pro m102w.
    - Máquinas de impresión de billetes.
    - Routers Cisco SRP521W-U 4.
    - Servidores de rack Cisco UCS de la serie C.
    - Cableado Ethernet.

- **Activos de la sala de seguridad:**
    - Unidad móvil con conexión a la red vía satélite.
    - Servidor CISCO preparado para suplir al servidor de la estación.
    - Estación de trabajo.
    - Generador propio de corriente.

2.1.2. RESPONSABLES DE LA ESTACION

En la estación existen 3 responsables que son los encargados de lleva 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:

- **Responsable del CPD:** encargado de llevar a cabo todas las acciones necesarias que involucren a cualquier activo.
- **Responsable de las ventas de billetes:** 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.
- **Resto de la estación:** 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.

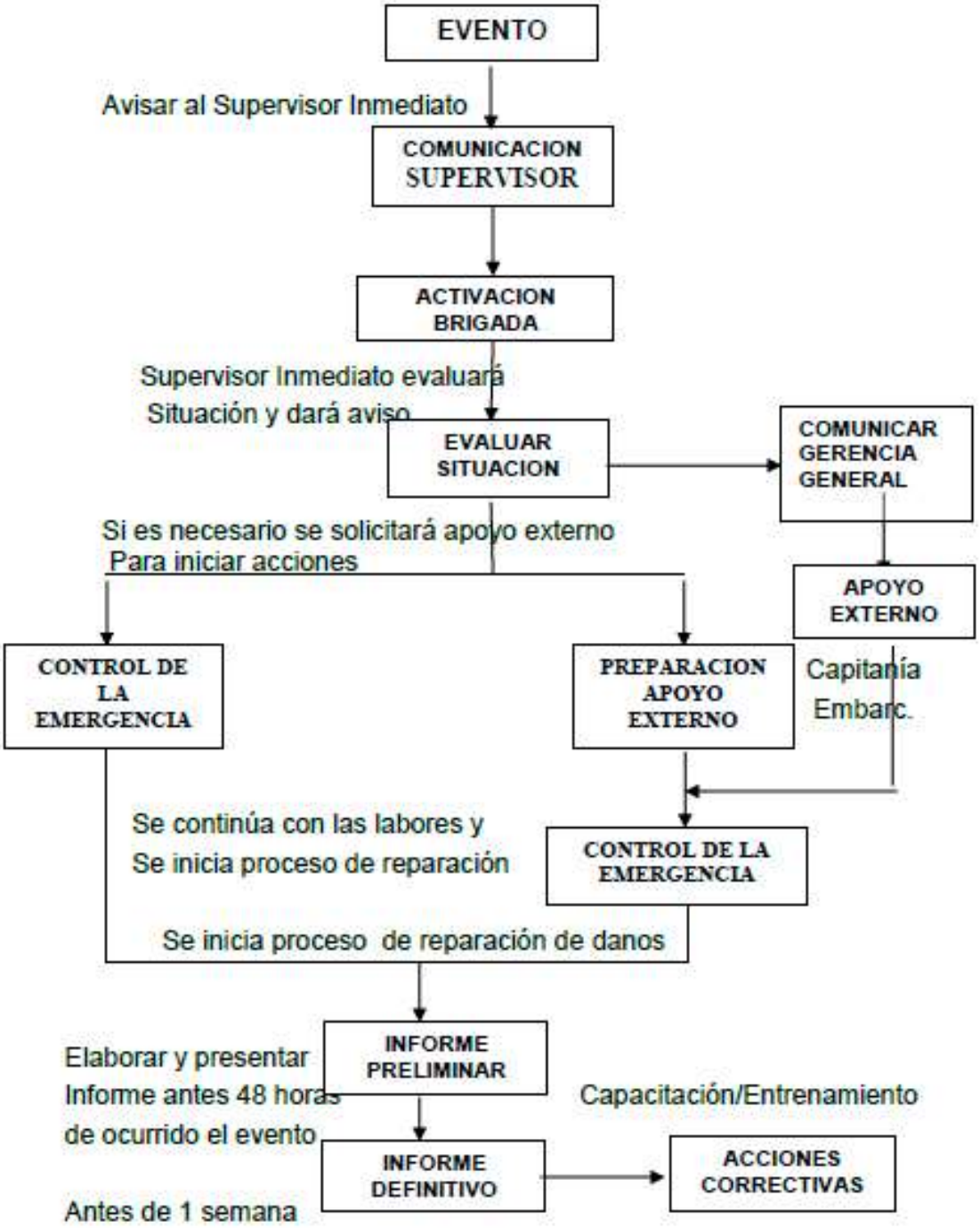
2.2. FASE II: ANÁLISIS DE RIESGOS

En la fase de análisis de riesgos, se hace un análisis estricto de todos los riesgos que pueden ocurrir investigando en la frecuencia que estos pueden ocurrir y la cantidad de daños que pueden causar. En la siguiente tabla se hace un resumen de estos riesgos:

RIESGO	AFECTA	DAÑO	FRECUENCIA
Riesgo Medioambiental (terremotos, inundación, epidemia, incendio, …)	Infraestructura, Personal, Datos, Servicios	Muy Alto	Remota
Corte suministros (internet, electricidad, …)	Servicios y Datos	Alto	Ocasional
Robo (vandalismo, informático, ...)	Infraestructura y Datos	Muy Alto /Alto	Probable
Fallos y Averías (Red, Equipos, …)	Infraestructura y Datos	Moderado	Ocasional

2.3. FASE III: PLANES DE CONTINGENCIA

En este apartado, para cada uno de los riesgos identificados en el punto anterior se analizará y se creará un plan de contingencia. El flujo para cualquier incidente es el siguiente [R5]:



2.3.1. RIESGO MEDIOAMBIENTAL

En este plan se recogen las operaciones necesarias en caso de que se produzca un riesgo medioambiental. El objetivo de este plan es minimizar los daños producidos tanto en la infraestructura, en las personas, los datos o en los servicios.

RELACIÓN DE CONTACTOS EN CASOS DE EMERGENCIAS

CONTACTO	NUMERO
EMERGENCIAS	112
POLICIA	092
DIRECTOR	926 XXX XXX
RESPONSABLE DEL CPD	926 XXX XXX

PLAN DE RESPALDO

Para evitar en la medida de lo posible el riesgo y en caso de que ocurra paliarlo de una manera rápida y eficaz se deben seguir las siguientes normas:

- Instalar extintores de CO2 en todas las salas que contengan equipos informáticos.
- Instalar extintores normales en todas las salas.
- Instalar y verificar el funcionamiento de bombas de achique en el CPD.
- Instalar detectores sísmicos en varios puntos.
- Tener preparados pequeños sacos de arena para aislar el CPD en caso de inundación.
- Verificar periódicamente la fecha de caducidad de los extintores.
- Limpiar con frecuencia el sistema de refrigeración.
- Comprobar periódicamente las tomas de corriente para detectar fallas.
- Guardar las copias de seguridad diarias en una caja fuerte en otra sala sin ningún equipo informático ni tomas de corriente.
- Charlas sobre prevención de fuegos y accidentes.
- Instalar detectores de humo en el CPD.
- Limpiar las rejillas de evacuación situadas en la planta baja.
- Prohibir la entrada de líquidos en el CPD.

PLAN DE EMERGENCIA

Estas acciones se deberán llevar a cabo en cuanto se produzca un incidente, todo debe coordinado por el responsable correspondiente:

1. Avisar a emergencias cuando se ha producido el incidente y en qué lugar.
2. Avisar a todo el personal que evacúe las zonas peligrosas.
3. Si el riesgo es muy pequeño:
   a. Intentar acabar con el riesgo usando los medios disponibles (sacos de arenas, extintores…)

   b. Intentar extraer los medios de almacenamiento del servidor.

   c. Si el riesgo se acaba pasar al plan de Recuperación.

4. Si el riesgo es relativamente grande:
   a. Cortar el suministro eléctrico de inmediato.
   b. Evacuar a zona segura y seguir las indicaciones de los equipos de emergencia.
   c. 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 riesgo 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.
- Volver a conectar el suministro eléctrico
- Volver a instalar los medios de almacenamiento en el CPD
- Inventario general de todos los elementos afectados.
- En caso de activos dañados dar la orden de recuperación o de sustitución oportuna.
- Realizar un informe con las causas del riesgo y la actuación efectuada para mejorar el plan de contingencia.

2.3.2. CORTE DE SUMINISTROS

En este plan se recogen las operaciones necesarias en caso de que se produzca un corte de suministros. El objetivo de este plan es minimizar los daños producidos tanto en los datos o en los servicios.

RELACIÓN DE CONTACTOS EN CASOS DE EMERGENCIAS

CONTACTO	NUMERO
COMPAÑÍA ELECTRICA	91X XXX XXX
COMPAÑÍA INTERNET	XXXX
COMPAÑÍA AGUA	91X XXX XXX
DIRECTOR	926 XXX XXX
RESPONSABLE DEL CPD	926 XXX XXX

PLAN DE RESPALDO

En caso de corte eléctrico o de fluctuaciones en la tensión de la red, la estación dispone de un generador que se activara a los 3 minutos del corte de la red además hasta que se ponga en funcionamiento del generador hay unas baterías en el sistema que tiene una duración de 10 minutos para que la electricidad sea continua.

En caso de corte de internet, la estación tiene contratada con otra compañía un sistema de cobertura a baja velocidad de internet en caso de problemas.

Además, para todos los suministros se debe:

- Revisar regularmente las instalaciones en busca de componentes en mal estado.
- Arrancar cada semana el grupo electrógeno para limpiar el circuito de carburante.
- Revisar el estado de la velocidad del internet.
- Revisar el nivel de aceite y gas-oil del grupo electrógeno cada semana.
- Revisar las tuberías y los cableados.

PLAN DE EMERGENCIA

En caso de corte del suministro los grupos auxiliares deben entrar en funcionamiento. Además de:

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 al CPD, y volver a arrancar todos los equipos de forma paulatina, revisar el estado de los sistemas auxiliares y elaborar un informe.

2.3.3. ROBO

En este plan se recogen las operaciones necesarias en caso de que se produzca un robo. El objetivo de este plan es minimizar los daños producidos tanto en la infraestructura y en los datos.

RELACIÓN DE CONTACTOS EN CASOS DE EMERGENCIAS

CONTACTO	NUMERO
POLICIA	092
DIRECTOR	926 XXX XXX

PLAN DE RESPALDO

Para evitar en la medida de lo posible el riesgo y en caso de que ocurra paliarlo de una manera rápida y eficaz se deben seguir las siguientes normas:

- Cada usuario deberá tener una contraseña suficientemente largo y cambiarlo cada 3 meses, además se impartirán charlas para concienciar a todo el personal.
- En el servidor estará instalado y configurado un cortafuegos.
- La red que se use para las aplicaciones de ADIF deberá estar separada físicamente de la red a la que puedan acceder los usuarios.
- Se instalarán cámaras de vigilancia.
- 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.
- Habrá un guardia de seguridad patrullando toda la zona común para evitar actos vandálicos.

PLAN DE EMERGENCIA

En caso de robo de equipos o vandalismo:

1. Avisas a la policía.
2. Evacuar a todo personal fuera del edificio o si no fuera posible a la sala del CPD.
3. Interrumpir las comunicaciones.
4. Apagar todos los equipos correctamente para evitar corrupción de datos.
5. Seguir las órdenes de los cuerpos de seguridad.

En cuanto se detecte el robo de información:

1. Desconectar el equipo del que se haya robado la información.
2. Monitorear todos los accesos las conexiones establecidas.
3. Investigar los datos robados y su importancia.
4. Si el atacante es el propio personal de la estación, abrir diligencias contra sus actos e investigar los motivos.
5. Elaborará un informe con las causas del robo y los medios utilizados.

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.

2.3.4. FALLOS Y AVERIAS

En este plan se recogen las operaciones necesarias en caso de que se produzca un fallo o una avería. El objetivo de este plan es minimizar los daños producidos tanto en la infraestructura, los datos o en los servicios.

RELACIÓN DE CONTACTOS EN CASOS DE EMERGENCIAS

CONTACTO	NUMERO
SERVICIO TECNICO	926 XXX XXX
DIRECTOR	926 XXX XXX
RESPONSABLE DEL CPD	926 XXX XXX

PLAN DE RESPALDO

Para evitar en la medida de lo posible el riesgo y en caso de que ocurra paliarlo de una manera rápida y eficaz se deben seguir las siguientes normas:

- 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

Estas acciones se deberán llevar a cabo en cuanto se produzca un incidente, todo debe coordinado por el responsable correspondiente:

1. Avisar al servicio técnico.
2. Evaluar la importancia del equipo.
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 fabricante.

PLAN DE RECUPERACIÓN

- Sustituir el equipo o la pieza que no funcione.
- Comprobar que el resto de los equipos con las mismas características no presenten ese fallo o signos de que vayan a fallar en el futuro inmediato.
- Realizar un informe con las posibles causas del fallo.

3. CONCLUSIÓN

Al concluir este trabajo me he dado cuenta de que el proceso de seguridad que se deben tener en cualquier organización debe ser bastante claros y deben ser revisados sus distintos planes de contingencia de manera periódica.

Investigar sobre los planes de contingencia y simular uno me ha ayudado mas a comprender la importancia de estos y como se deberían realizar en todos los riesgos.

REFERENCIAS

- **R1:** https://www.emprendepyme.net/plan-de-contingencia.html
- **R2:**https://ofiseg.wordpress.com/2012/04/19/necesidad-de-un-plan-de-contingencia/
- **R3:**https://www.aenor.com/certificacion/tecnologias-de-lainformacion/continuidad-negocio
- **R4:**https://estaciones.adif.es/EstacionBolsillo/estaciones/zonales/1764?menuNORelevante=true
- **R5:**https://www.monografias.com/trabajos95/plancontrolcontingencias/plan-control-contingencias2.shtml

WEBGRAFIA

- https://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/
- https://www.isotools.org/2019/06/04/elementos-del-plan-de-contingencia-segun-iso-22301/
- http://www.adif.es/es_ES/index.shtml
- http://www.adif.es/AdifWeb/estacionesMapa.jsp?i=es_ES
- https://www.inteco.es/extfrontinteco/es/pdf/Formacion_Plan_Contingencias_Informaticas.pdf
- Material de clase
- https://www.monografias.com/trabajos95/plan-control-contingencias/plan-control-contingencias2.shtml
- https://image.slidesharecdn.com/plandeemergencia-140617001325-phpapp02/95/plan-de-emergencia-33-638.jpg?cb=1402964066