Plan de continuidad de negocio

Sistema de Gestión de Seguridad de la Información

Fecha: 31/02/2022

Estado: Aprobado

Versión: 22

Confidencial – Véase la Lista de Acceso

Tabla de contenido

Plan de continuidad de negocio

Sistema de Seguridad de la Información

Versión Aprobada:				
	Nombre	**Función**	**Firma**	**Fecha**
Elaborado	Marcos Bouza Fernández	Responsable de seguridad		11/01/2010
Revisado	Marcos Bouza Fernández	Responsable de seguridad		06/03/2014
Aprobado	Marcos Bouza Fernández	Responsable de seguridad		06/03/2014

Lista de Acceso:
Acceso Interno
Personal propio de SIGA98
Acceso Externo

Historial de Revisiones:			
Versión	**Fecha**	**Descripción**	**Autor**
1	20/01/2010	Se añaden los acuerdos	Eva Lucía Garrido
2	19/02/2010	Reunión y seminarios (6.1)	Eva Lucía Garrido
3	23/02/2010	Simulacro Caída Internet (8.1)	Marcos Bouza Fernández
4	24/02/2010	Simulacro Pérdida Datos (8.2)	Marcos Bouza Fernández
5	23/07/2010	Simulacro Caída Luz (8.3)	Marcos Bouza Fernández
6	27/08/2010	Simulacro Recuperación Correo (8.4)	Marcos Bouza Fernández
7	20/09/2010	Actualización Manuales de Configuración	Marcos Bouza Fernández
8	22/10/2010	Simulacro Caída Telefónica (8.5)	Marcos Bouza Fernández
9	19/11/2010	Simulacro Recuperación Servidor (8.6)	Marcos Bouza Fernández
10	25/02/2011	Simulacro Fallo Centralita (8.7)	Marcos Bouza Fernández
11	20/05/2011	Actualización simulacros	Marcos Bouza Fernández
12	10/04/2012	Separación de los modelos y registros a cumplimentar periódicamente del propio documento de "Plan de Continuidad de Negocio" manteniéndolos como anexos del mismo.	Marcos Bouza Fernández
13	20/06/2012	Actualización esquema fallo eléctrico y caída línea telefónica	Marcos Bouza Fernández
14	13/01/2013	Actualización esquema de red	Marcos Bouza Fernández
15	06/03/2014	Actualización PC-02	Marcos Bouza Fernández
16	21/04/2015	Actualización PC-02	Marcos Bouza Fernández
17	19/02/2016	Actualización y mejora de plan de continuidad de negocio	Marcos Bouza Fernández
18	20/01/2017		Marcos Bouza Fernández
19	19/10/2020	Actualización Recursos	Marcos Bouza Fernández
20	14/04/2021	Actualización Imposibilidad de acceso	Marcos Bouza Fernández
21	31/03/2022	Actualización inclusión delegación Madrid	Marcos Bouza Fernández
22	20/05/2024	Actualización mapa de Red, cargos personas, y actualización PC	Marcos Bouza Fernández

Objeto

El propósito de este Plan es el de aumentar la probabilidad de continuidad de las funciones críticas de SIGA98 en caso de que un incidente interrumpa los principales procesos de negocio, proporcionando un enfoque organizado y consolidado para dirigir las actividades de respuesta y recuperación, evitando la confusión, la toma de decisiones en momentos de tensión y proporcionar una respuesta rápida y apropiada a cualquier incidente imprevisto.

Definiciones previas

Alcance del plan

El plan de continuidad de negocio desarrollado en este documento abarca las siguientes instalaciones (oficinas centrales y delegación en Madrid) y las siguientes áreas funcionales… (Financiero, comercial, RRHH, fabricación, etc.).

Debido a que las oficinas de Madrid no disponen ni de CPD ni de servidor propio y están interconectados a la red interna de SIGA98, no se desarrolló un plan específico de continuidad para las mismas.

Sí se podrá tener en cuenta en los Planes de Contingencia en los que puedan impactar tanto en positivo como en negativo.

En ningún caso, el hecho de cualquier tipo de incidente en las instalaciones de Madrid tendrá un impacto de forma sensible en el día a día de SIGA98

Se tendrán en cuenta aquellos incidentes que causen un impacto en el normal desempeño de los servicios de SIGA98, especialmente en los activos con mayor valoración:

- Aplicación THEMPUS
- Evidencias electrónicas
- Correo electrónico
- Datos clientes
- Código fuente (datos + soporte)
- Datos dpto. económico
- Centra
- Centralita telefónica
- Línea de voz
- Línea internet
- Suministro eléctrico
- Instalaciones
- Servidor SIGA
- Cualquier incidente que suponga la paralización de actividades de la organización por motivos ajenos a la tecnología, tales como problemas laborales propios o del sector o problemas laborales que afecten al área geográfica donde se encuentra ubicada la organización.

Premisas de partida

El plan se ha desarrollado sobre los siguientes supuestos:

- Sólo el área habitual de trabajo ha sido afectada por el incidente; todos los lugares alternativos pre-designados están intactos.
- Los almacenes externos de archivos de backup e información están intactos y accesibles.
- El personal cualificado en cantidad suficiente (identificado en los capítulos correspondientes de este plan) está disponible para realizar los trabajos de recuperación.
- Los trabajos de recuperación se están realizando de acuerdo con los procedimientos descritos en el plan.
- Las copias de seguridad y su correspondiente rotación (incluyendo papel, fichas, soportes electrónicos) se han realizado correctamente.
- El backup de las telecomunicaciones y las estrategias de recuperación identificadas en este plan están completamente realizadas y comprobadas.
- Las estrategias de recursos y soluciones de recuperación (por ejemplo, soluciones de reposición de ordenadores) están

disponibles, realizadas y comprobadas satisfactoriamente.

- Las organizaciones externas como clientes, suministradores y organismos públicos cooperarán razonablemente durante el periodo de los trabajos de recuperación.
- Se han realizado adecuadamente los programas de prueba y plan y las modificaciones pertinentes como consecuencia de su resultado.
- La revisión del plan, mantenimiento, y actualizaciones están realizadas con periodicidad para asegurar que responde a las necesidades de cada momento.
- Se han realizado adecuadamente los programas de sensibilización y entrenamiento.
- Las instalaciones en Madrid están disponibles

Procesos o funciones críticas de la organización

A continuación, se enumeran por orden de criticidad los procesos o funciones críticas de la organización.

Departamento	Activo	Ubicación	Tiempo objetivo de recuperación
Todos	Aplicación THEMPUS	Centro datos AXARNET	4 horas
Todos	Evidencias electrónicas	Centro datos AXARNET	24 horas
Todos	Correo electrónico	Centro datos Ultreia	2 horas
Todos	Datos clientes	Siga	12 horas
Desarrollo	Código fuente (datos + soporte)	Siga	12 horas
Económico	Datos dpto. económico	Siga	12 horas
Todos	Centralita telefónica	Movistar	2 horas
Todos	Línea de voz	Siga	2 horas
Todos	Línea internet	Siga	1 hora
Todos	Suministro eléctrico	Siga	1 hora
Todos	Instalaciones	Siga	12 horas
Todos	Servidor SIGA	Siga	12 horas

Tabla 1. Procesos o funciones críticas de la organización

Recursos críticos

Aplicaciones

Aplicación	Versión	Utilizada por:	Observaciones
Sg21	N.A.	Dep. Financiero	Accesible online
Putty	N.A.	Dep. Técnico	Accesible online
SmartFTP	N.A.	Dep. Técnico	Accesible online
Keepass	N.A.	Todos	Accesible online

Tabla 2. Aplicaciones críticas

Registros vitales y backups

Registro	Ubicación	Observaciones
Backup total	SIGA/MEGAVEDRA	Copia de respaldo de todos los registros críticos y vitales para SIGA
Claves de acceso	SIGA	Llave USB y online

Tabla 3. Registros vitales y backups

Necesidades de personal

Descripción	Persona propuesta	Suplente
Atención telefónica	Alberto Jiménez	Begoña Martínez, Natalia Reguera
Responsable técnico	Marcos Bouza	Katia Otero
Programador	Arturo Arias	Pilar Raña
Director General	Miguel Angel Romero	Eva Garrido

Tabla 4. Necesidades de personal

Necesidades de hardware

Nombre	Descripción	Unidades	Observaciones
PC´s	Fijos y portátiles	4	Acuerdo colaboración Megavedra

Tabla 5. Necesidades de hardware

Otros recursos

Nombre	Descripción / Unidades	Observaciones
Local	Instalaciones en el Colegio de Gestores de Pontevedra	Acuerdo colaboración con Colegio de Gestores
Línea teléfono	902 114 509	Acuerdo de colaboración con Telefónica
Internet	Conexión	Acuerdo de colaboración con el Colegio

Tabla 6. Aplicaciones críticas

Estrategia de continuidad

Introducción

La estrategia de continuidad de negocio de SIGA98 se basa en la identificación y disponibilidad de una serie de elementos clave para reestablecer dentro del tiempo objetivo de recuperación, los servicios que pudieran estar afectados por una determinada situación de emergencia.

- **Centro principal:** ubicación habitual de trabajo para la organización.
- **Delegación Madrid:** ubicación de trabajo en Madrid
- **Centro alternativo:** es el lugar elegido para ubicar o poner en marcha los procedimientos o actividades críticos de la organización. En función de la magnitud y localización del desastre, el centro alternativo también podrá tomar diferentes ubicaciones.
- **Acuerdos de ayuda/colaboración:** convenios o contratos establecidos con terceros para colaborar en alguno de los aspectos relevantes para el restablecimiento de los servicios afectados.
- **Comunicaciones alternativas:** estrategia de comunicaciones tanto con clientes y proveedores, así como entre los miembros de la propia organización.
- **Centro de almacenamiento externo:** lugar elegido para salvaguardar tanto los elementos de backup necesarios como cualquier otro recurso vital para reestablecer los servicios afectados.
- **Equipos de recuperación:** son los grupos de personas que se encargan de una serie de actividades para conseguir un proceso de recuperación efectivo. Un equipo puede constar de una sola persona, y una persona puede pertenecer a más de un equipo.

A continuación, se definen y describen cada uno de los elementos anteriores.

Centro principal

El centro principal de operación de la organización es su oficina, ubicada en c/ Pedro Sarmiento de Gamboa, 12, bj (Pontevedra). Los datos de contacto del centro principal son:

- Teléfono: +34 986 866 171
- Fax: +34 986 865 244
- Email de contacto: administracion@gestores.net

Centro secundario (delegación de Madrid)

La delegación de la organización tiene sus oficinas en C/Factor Nº16, (Madrid)

Centro alternativo

La sede del Colegio de Gestores Administrativos de Galicia (delegación de Pontevedra):

- C/ Blanco Porto, número 9-1º,
- 36001
- Pontevedra.

Acuerdos de ayuda/colaboración

- Acuerdo de colaboración Megavedra
- Acuerdo de colaboración con Colegio de Gestores Administrativos de Galicia, delegación de Pontevedra.
- Acuerdo de colaboración con Telefónica para restablecer la línea 902 114 509

Comunicaciones alternativas

Tipo de comunicación	Medio	Responsable
Clientes y usuarios	Correo electrónico a las listas de los de clientes, y a correos de personal, al igual que comunicación a través de móviles.	Responsable de seguridad y la dirección
Proveedores	Teléfonos móviles y del correo electrónico en web	Responsable de seguridad y la dirección
Entre trabajadores	Teléfonos móviles y del correo electrónico en web	N.A.
Dirección	Teléfonos móviles de la empresa	Dirección
Con suministradores	Teléfono y correo electrónico	Responsable de seguridad y la dirección

Centro de almacenamiento externo

Megavedra

Equipos de recuperación

A continuación, se definen los diferentes equipos de recuperación necesarios por SIGA98 para llevar a cabo su estrategia de continuidad de negocio.

Equipo de Gestión de incidentes				
Nombre	**Apellidos**	**Teléfono del trabajo**	**Teléfono móvil**	**Teléfono privado**
Miguel Ángel	Romero Davila	986866171	676563214	669399141
Marcos	Bouza Fernández	986866171	661872070	675900430
Eva Lucía	Garrido Durán	986866171	628238428	649079464
Equipo de Operaciones Informáticas				
Nombre	**Apellidos**	**Teléfono del trabajo**	**Teléfono móvil**	**Teléfono privado**
Marcos	Bouza Fernández	986866171	661872070	675900430
Katia	Otero del Río	986866171		6511676586
Pilar	Raña Vázquez	986866171		676671254
Arturo	Arias	986866171		634596979
Equipo de Administración				
Nombre	**Apellidos**	**Teléfono del trabajo**	**Teléfono móvil**	**Teléfono privado**
Eva Lucía	Garrido Durán	986866171	628238428	649079464
Patricia	Pérez Pérez	986866171		661154413
Equipo de Atención a Usuarios				
Nombre	**Apellidos**	**Teléfono del trabajo**	**Teléfono móvil**	**Teléfono privado**
Eva Lucía	Garrido Durán	986866171	628238428	649079464
Begoña	Martínez Arís	986866171		619851551
Alberto	Jiménez Rey	986866171		626354476
Natalia	Regueira	986866171		659928472

Tabla 7. Equipos de recuperación

Listado de contactos de emergencia

- Interno: Ver apartado 3.7
- Externo: Base de datos clientes online
- Axarnet: 911 868 181

Equipos de emergencia

- Emergencias: 112
- Urgencias sanitarias: 061
- Bomberos: 080
- Guardia civil: 062
- Policía nacional: 091
- Protección civil: 1006
- Hospital 1: 986800000

Plan de acción

Notificación de alerta

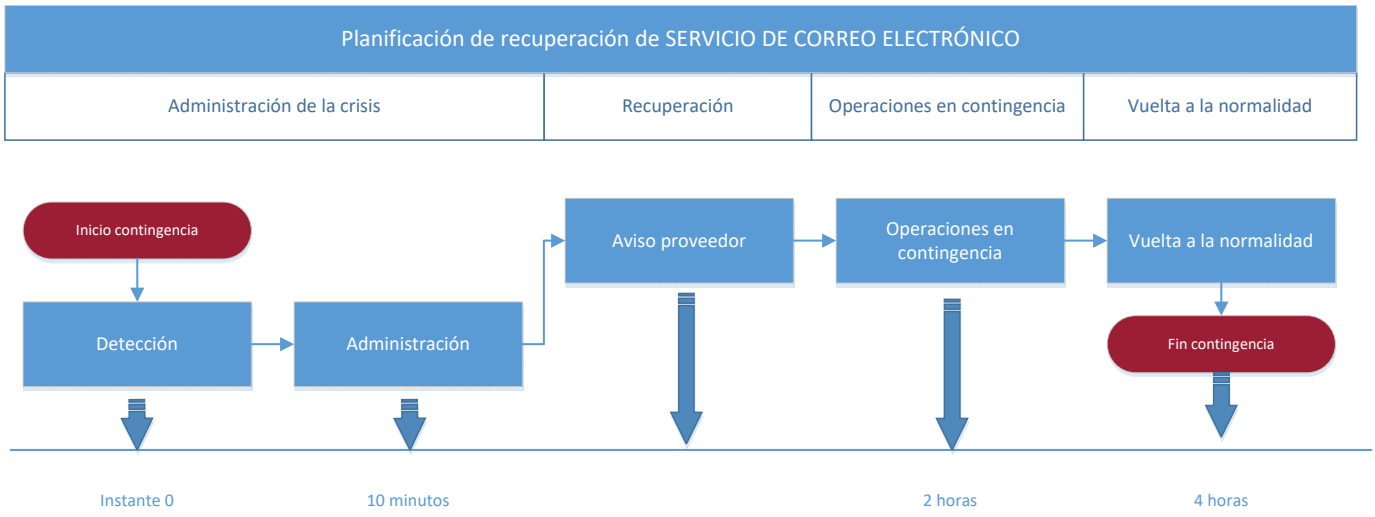
El plan de acción puede ser activado de dos formas, como resultado de un incidente que suponga la evacuación de las instalaciones o como resultado de un problema determinado. Cualquiera que sea el origen del incidente, éste deberá comunicarse al responsable de gestión de incidentes o a su suplente, que deberá analizar y evaluar el alcance de este y decidir la puesta en marcha o no del plan de continuidad de negocio en su totalidad o alguna de sus partes.

Distribución de tareas

En la siguiente tabla se muestran posibles situaciones de alerta y las acciones correspondientes para cada una de ellas.

Código	Situación de Contingencia/ Incidencias	Acciones a tomar
PC-01	CAÍDA E-MAIL	1. Revisar que existe conectividad a internet 2. Revisar si el servidor de correo está funcionado 3. Si el servidor no funciona iniciar PC-01
PC-02	CAÍDA SERVIDOR	1. Revisar que existe conectividad con el servidor 2. Revisar que no se ha apagado 3. Si el servidor no funciona iniciar PC-02
PC-03	CAÍDA LÍNEA INTERNET	1. Comprobar que no se puede navegar 2. Comprobar que el router de telefónica está encendido 3. Comprobar que el servidor funciona correctamente 4. Si no hay conexión iniciar PC-03
PC-04	CÁIDA SUMINISTRO ELÉCTRICO	1. Comprobar que los fusibles están encendidos 2. Si no hay luz iniciar PC-04
PC-05	PÉRDIDA LÍNEA DE VOZ	1. Comprobar operatividad centralita 2. Si no hay línea iniciar PC-05
PC-06	PÉRDIDA CENTRALITA TELEFÓNICA (servicio)	1. Comprobar conexión eléctrica 2. Iniciar PC-06
PC-07	DESASTRE GENERAL (pérdida de instalaciones)	Iniciar PC-07
PC-08	PÉRDIDA DE DATOS Datos clientes Código fuente Datos dpto. económico	Iniciar PC-08
PC-09	CAIDA THEMPUS	Iniciar PC-09
PC-10	Evidencias electrónicas	Iniciar PC-08
PC-11	Imposibilidad acceso instalaciones	Iniciar PC-11

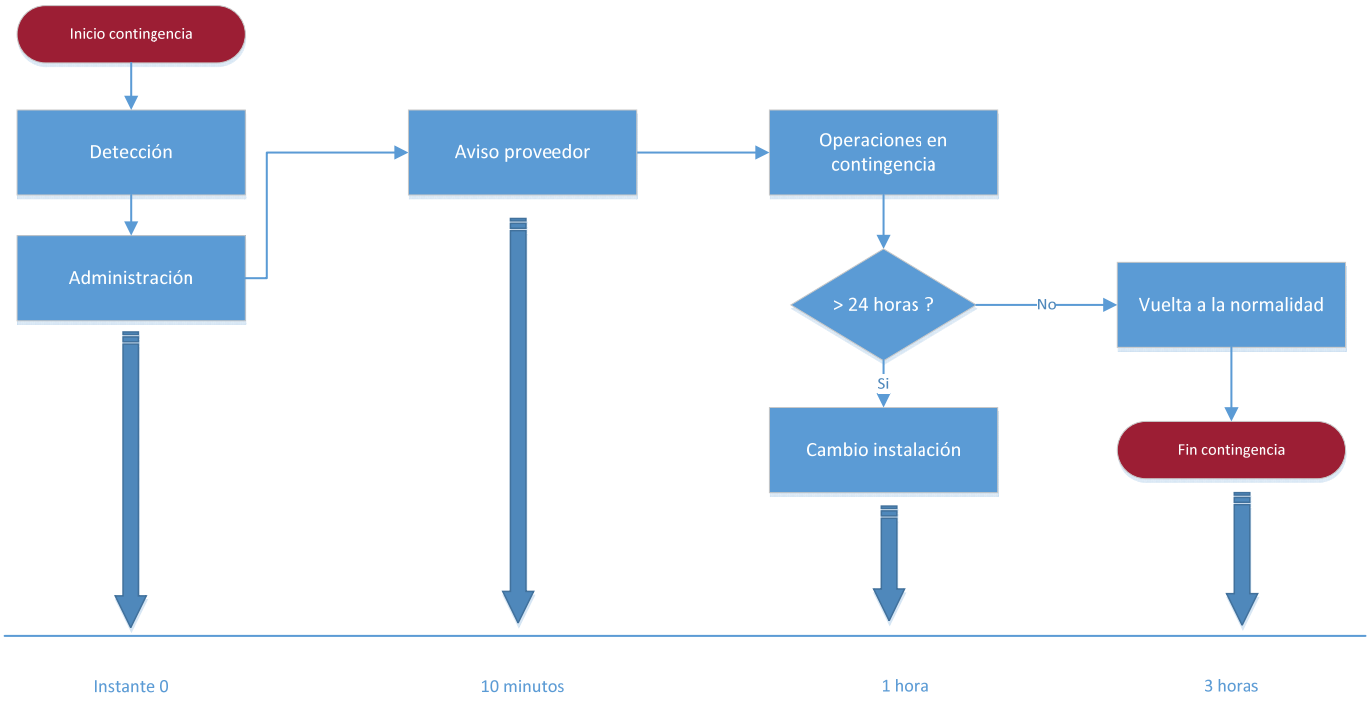
Tabla 8. Situaciones de contingencia.


Planificación de recuperación de SERVICIO DE CORREO ELECTRÓNICO
Administración de la crisis
Recuperación
Operaciones en contingencia
Vuelta a la normalidad
Inicio contingencia
Detección
Administración
Aviso proveedor
Operaciones en contingencia
Vuelta a la normalidad
Fin contingencia
Instante 0
10 minutos
2 horas
4 horas


Planificación de recuperación de SERVIDOR SIGA
Administración de la crisis
Recuperación
Operaciones en contingencia
Vuelta a la normalidad
Inicio contingencia
Detección
Administración
Restauración sistema
Restauración backup
Operaciones en contingencia
Vuelta a la normalidad
Fin contingencia
Instante 0
10 minutos
1 hora
3 horas

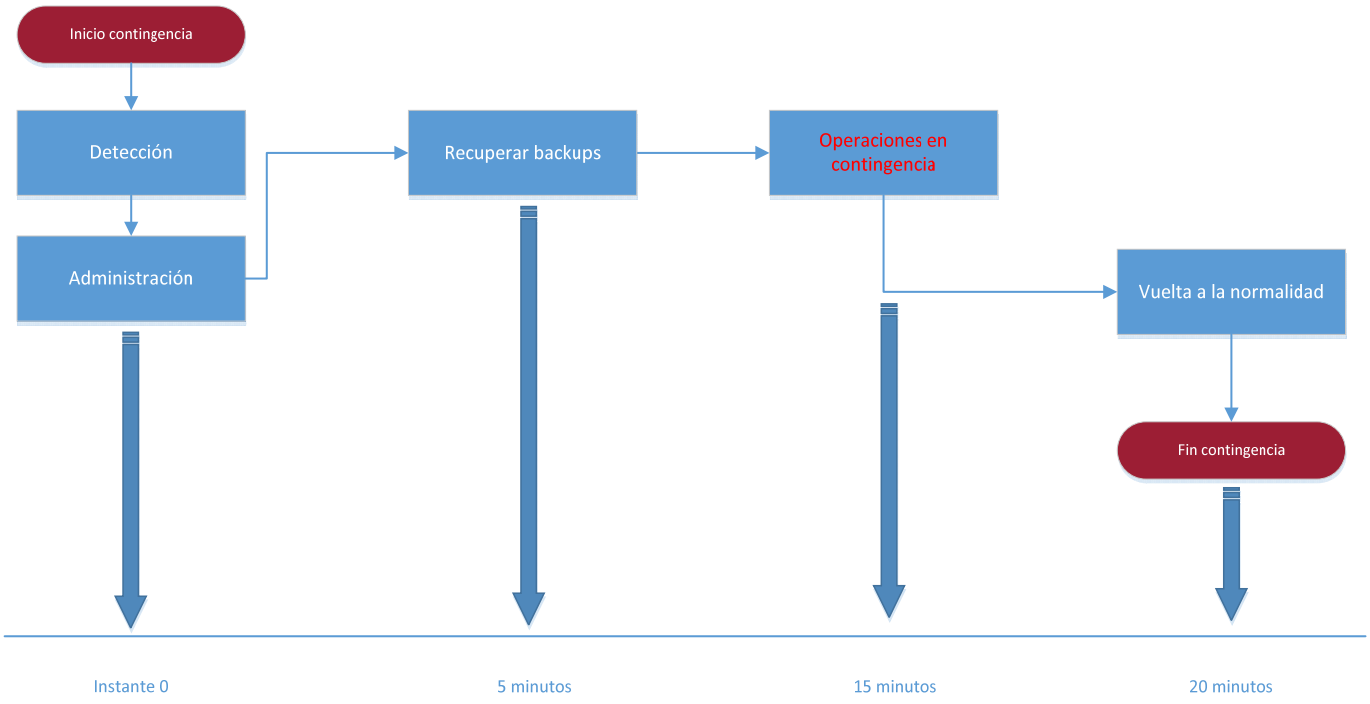
Planificación de recuperación de servicio de SUMINISTRO ELÉCTRICO

Administración de la crisis	Recuperación	Operaciones en contingencia	Vuelta a la normalidad

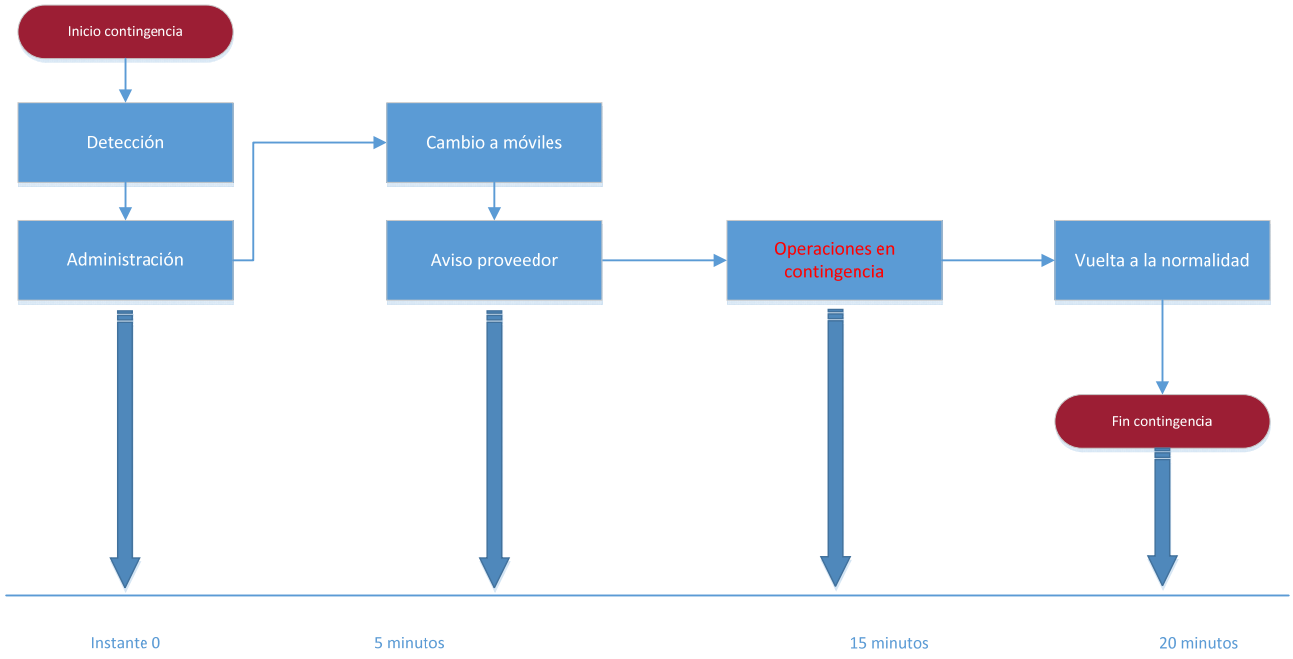


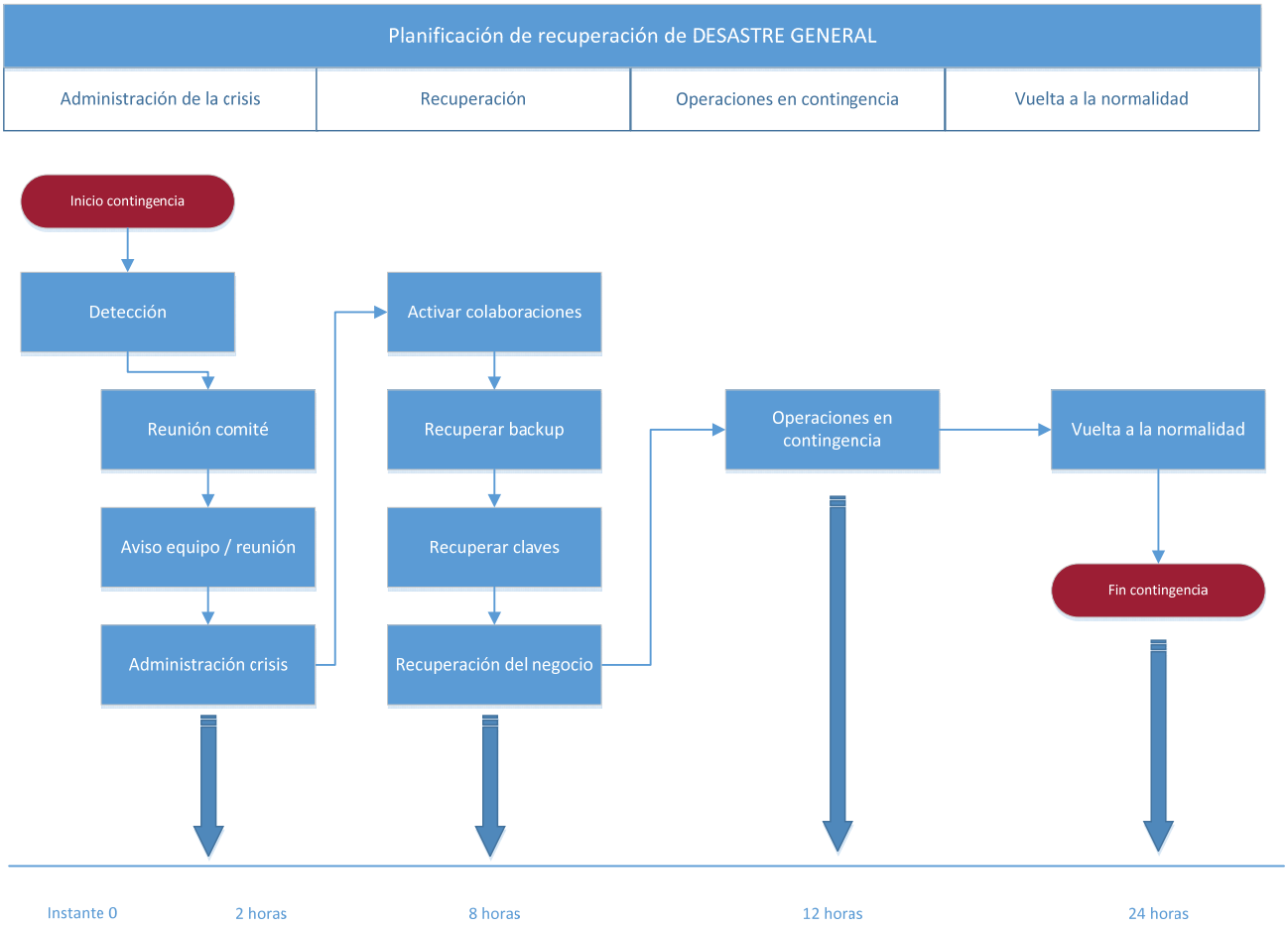
Planificación de recuperación de PÉRDIDA DE DATOS

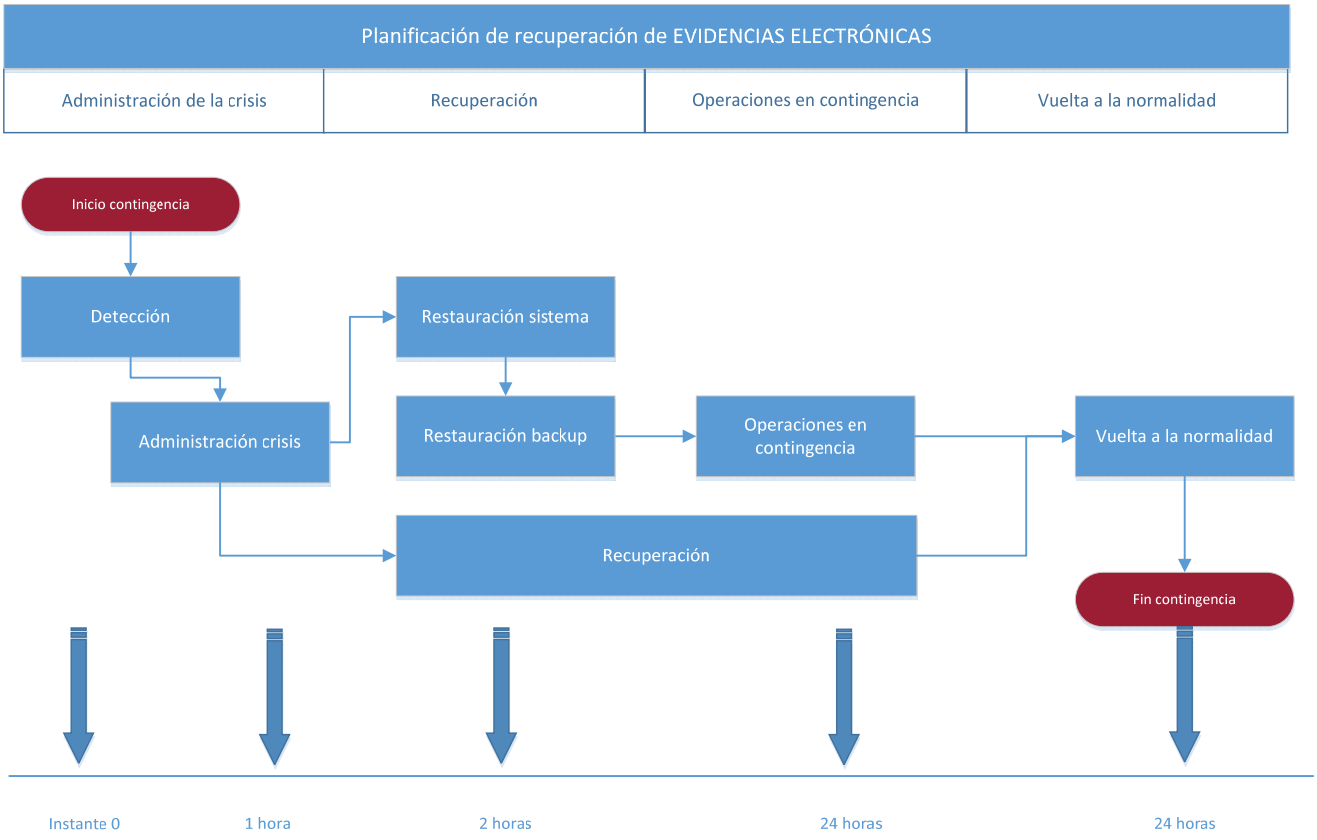
Administración de la crisis	Recuperación	Operaciones en contingencia	Vuelta a la normalidad

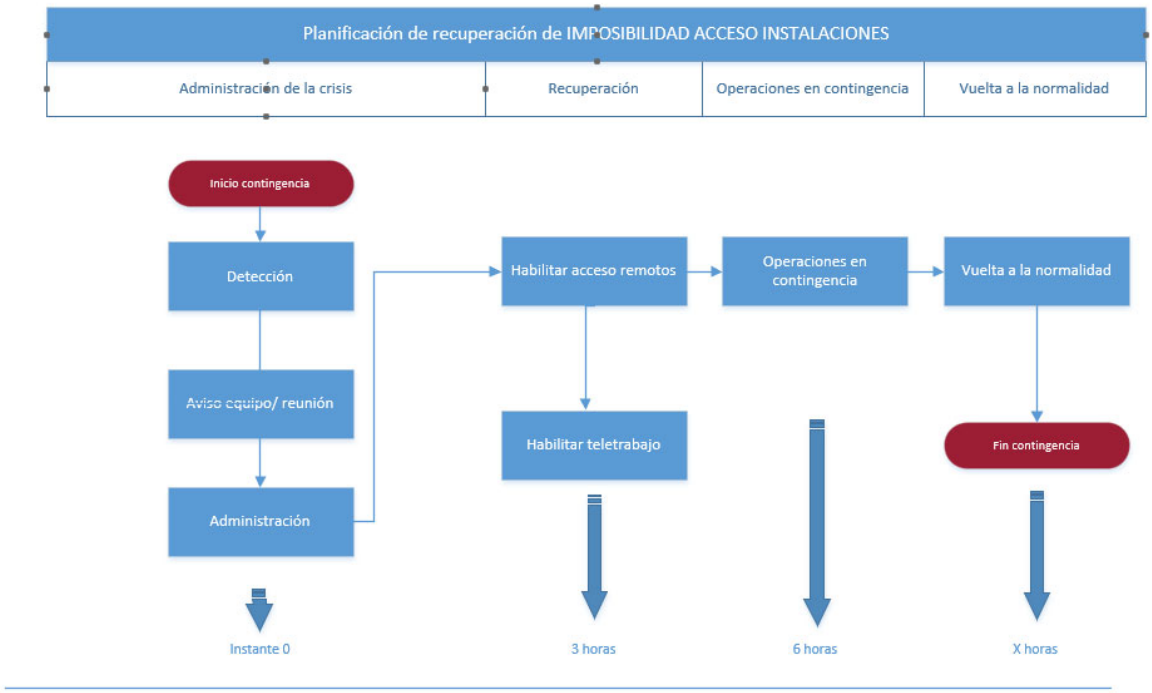


Planificación de recuperación de CENTRALITA TELEFÓNICA			
Administración de la crisis	Recuperación	Operaciones en contingencia	Vuelta a la normalidad




Planificación de recuperación de DESASTRE GENERAL
Administración de la crisis
Recuperación
Operaciones en contingencia
Vuelta a la normalidad
Inicio contingencia
Detección
Reunión comité
Aviso equipo / reunión
Administración crisis
Activar colaboraciones
Recuperar backup
Recuperar claves
Recuperación del negocio
Operaciones en contingencia
Vuelta a la normalidad
Fin contingencia
Instante 0
2 horas
8 horas
12 horas
24 horas


Planificación de recuperación de EVIDENCIAS ELECTRÓNICAS
Administración de la crisis
Recuperación
Operaciones en contingencia
Vuelta a la normalidad
Inicio contingencia
Detección
Administración crisis
Restauración sistema
Restauración backup
Recuperación
Operaciones en contingencia
Vuelta a la normalidad
Fin contingencia
Instante 0
1 hora
2 horas
24 horas
24 horas


Planificación de recuperación de IMPOSIBILIDAD ACCESO INSTALACIONES
Administración de la crisis
Recuperación
Operaciones en contingencia
Vuelta a la normalidad
Inicio contingencia
Detección
Aviso equipo/ reunión
Administración
Habilitar acceso remotos
Habilitar teletrabajo
Operaciones en contingencia
Vuelta a la normalidad
Fin contingencia
Instante 0
3 horas
6 horas
X horas

Procedimientos de respuesta

A continuación, se muestran los procedimientos de restauración.

Código:	Nombre:
PC-01	Recuperación del sistema Correo electrónico
Equipo de recuperación/ Responsable:	
Equipo de Operaciones Informáticas	
Recursos necesarios:	
Transferido a proveedor	
Tiempo objetivo de recuperación:	
2 horas	
Pre-requisitos:	
• Para poder restaurar el sistema de correo deben comprobarse que se dispone de las copias de respaldo y de los parámetros de configuración (por parte del proveedor). • Debe disponerse de conectividad a Internet.	
Secuencia de Acciones:	
Ponerse en contacto con proveedor para inicializar la recuperación. Realizar seguimiento, cada 30 minutos, del avance de la recuperación. Una vez reestablecido el servicio, se comunicará a los afectados el" fin de situación de contingencia".	

Código:	Nombre:
PC-02	Recuperación Servidor Siga
Equipo de recuperación/ Responsable:	
Equipo de Operaciones Informáticas	
Recursos necesarios:	
• Servidor • Copias de respaldo del servidor caído	
Tiempo objetivo de recuperación:	
12 horas	
Pre-requisitos:	
• Disponer del SW de instalación/restauración • Disponer de backups actualizados	
Secuencia de Acciones:	
1. Si la avería es de HW entonces: a. Adquirir nuevo servidor b. Levantar nueva máquina virtual con la copia de seguridad (HYPER-V2) 2. Si afecta a la máquina virtual restaurar copia de seguridad (HYPER-V2) 3. Revisar la configuración del servidor de acuerdo con el checklist "Comprobación del servidor" * Si la avería es HW y requiere mayor tiempo de restauración se copia la BD de clientes a cualquier PC que hará de "servidor" mientras no se restablece el servidor primario. Una vez reestablecido el servicio, se comunicará a los afectados el" fin de situación de contingencia".	

Código:	Nombre:
PC-03	Caída Internet

Equipo de recuperación/ Responsable:

Equipo de Operaciones Informáticas

Recursos necesarios:

- Conexión R
- Disponer número teléfono proveedor
- Conexión 4G/5G *

Tiempo objetivo de recuperación:

1 hora

Pre-requisitos:

Línea de conexión R operativa

Secuencia de Acciones:

En el caso de fallo del acceso principal a internet (MOVISTAR MacroLAN), el cambio al acceso de backup (VPN Movistar) se realiza de forma automática y transparente al usuario, debido a la existencia de un balanceador.

En caso de fallar la línea de backup (VPN Movistar) se cambiaría al proveedor R.

El cambio al proveedor de respaldo requiere de una intervención física. Será necesario conectar el router de R al switch y desconectar el router de Movistar.

Una vez que se ha producido el cambio al acceso de backup (), deben modificarse los aspectos de configuración afectados por el cambio de IP pública.

Una vez se haya finalizado la situación de contingencia, y se reestablezca el acceso principal a internet (MOVISTAR MacroLAN), en el caso de haber estado en bakcup de VPN Movistar no será necesario realizar ninguna acción y de haber pasado a R, habrá que desconectar del switch el router de R y volver a conectar el de Movistar

Una vez reestablecido el servicio, se comunicará a los afectados el" fin de situación de contingencia".

*Se podrá acceder con los portátiles vía 4G/5G a aplicaciones online críticas.

Código:	Nombre:
PC-04	Interrupción de suministro eléctrico

Equipo de recuperación/ Responsable:

Dpto. técnico

Recursos necesarios:

SAI

Tiempo objetivo de recuperación:

1 hora

Pre-requisitos:

- Disponer de SAI
- Disponer número teléfono proveedor

Secuencia de Acciones:

1. Activar en la web aviso de caída (www.gestores.net/aviso.htm)
2. Apagado seguro de los PC. Hay que ver el tema de los registros del SAI y su duración.
3. Shutdown del servidor
4. Llamar al proveedor (Naturgy)
5. Una vez reestablecido el servicio, se comunicará a los afectados el" fin de situación de contingencia".

Código:	Nombre:
PC-05	Caída línea de comunicaciones de voz
Equipo de recuperación/ Responsable:	
Dpto. técnico	
Recursos necesarios:	
Móviles	
Tiempo objetivo de recuperación:	
2 horas	
Pre-requisitos:	
Disponer número teléfono proveedor	
Secuencia de Acciones:	
1. Notificar vía correo electrónico a los clientes. 2. Llamar a proveedor (MOVISTAR) para notificar incidencia 3. Usos de móviles de empresa y particulares para atender incidencias graves 4. Una vez reestablecido el servicio, se comunicará a los afectados el" fin de situación de contingencia".	

Código:	Nombre:
PC-06	Fallo Centralita
Equipo de recuperación/ Responsable:	
Dpto. Técnico	
Recursos necesarios:	
Móviles	
Tiempo objetivo de recuperación:	
2 horas	
Pre-requisitos:	
Disponer número teléfono proveedor	
Secuencia de Acciones:	
• Notificar vía correo electrónico a los clientes. • Llamar al proveedor (MOVISTAR) • Usos de móviles de empresa y particulares para atender incidencias graves • Una vez reestablecido el servicio, se comunicará a los afectados el" fin de situación de contingencia".	

Código:	Nombre:
PC-07	Desastre General

Equipo de recuperación/ Responsable:

Todos los equipos de recuperación

Recursos necesarios:

Todos los recursos del plan de contingencia

Tiempo objetivo de recuperación:

12 horas

Pre-requisitos:

Todos los recursos disponibles

Secuencia de Acciones en horario laboral:

1. Evacuación de Personal según plan de prevención

1. El Equipo de Gestión de incidentes se hace con una copia del plan (online, llave USB)
2. Notificar al colegio la activación del plan de contingencia
3. Desde la delegación de Madrid se asume el mantenimiento y soporte de emergencia de las aplicaciones SIGA, teniendo máxima prioridad la plataforma Thempus
4. Reunión del comité de crisis en las instalaciones del colegio
5. Ponerse en contacto con empresas con acuerdos de colaboración para iniciar planes de contingencia
    1. Avisar al proveedor de sistemas (Megavedra)
    2. Avisar al proveedor de comunicaciones (MOVISTAR)
3. Activar aviso en web de situación de contingencia
4. Cumplimiento acuerdo colaboración con Colegio (instalaciones, internet, teléfono)
5. Cumplimiento acuerdo colaboración con Telefónica
6. Recuperar claves. Caja Fuerte, USB, online en www.gestores.net/ plancontingencia/claves.zip
7. Recuperar / Restaurar backups. Ver Procedimiento backups (Sala servidor y online www.gestores.net/plancontingencia/backups.pdf)
8. Recuperar datos clientes (www.gestores.net/plancontingencia/clientes.rar o en llave USB)

Secuencia de Acciones en horario no laboral:

1. Reunión de Equipo de Gestión de incidentes
2. El Equipo de Gestión de incidentes se hace con una copia del plan (online, instalaciones del colegio)
3. El equipo de Gestión de incidentes avisa a todos los demás equipos
4. Notificar al colegio la activación del plan de contingencia
5. Reunión del comité de crisis en las instalaciones del colegio
6. Ponerse en contacto con empresas con acuerdos de colaboración para iniciar planes de contingencia
7. Activar aviso en web de situación de contingencia
8. Cumplimiento acuerdo colaboración con Colegio (instalaciones, internet, teléfono)
9. Cumplimiento acuerdo colaboración con Telefónica
10. Recuperar claves online www.gestores.net/plancontingencia/seguridad.zip
11. Recuperar /Restaurar backups. Ver procedimiento backups (Oonline www.gestores.net/plancontingencia/backups.pdf)
12. Recuperar datos clientes (www.gestores.net/plancontingencia/clientes.rar o en llave USB)
13. Si la situación se alarga al horario laboral, la delegación de Madrid asume el mantenimiento y soporte de emergencia de las aplicaciones SIGA, teniendo máxima prioridad la plataforma Thempus.
14. Una vez reestablecido el servicio, se comunicará a los afectados el" fin de situación de contingencia".

Código:	Nombre:
PC-08	Pérdida Datos
Equipo de recuperación/ Responsable:	
Dpto. técnico	
Recursos necesarios:	
Copia de seguridad	
Tiempo objetivo de recuperación:	
12 horas	
Pre-requisitos:	
Disponer de copia de seguridad	
Secuencia de Acciones:	
• Recuperar copia de seguridad • Restaurar copia de seguridad siguiendo manual "Procedimiento Backups" (llave USB y online en http://www.gestores.net/plancontingencia/backups.pdf • Una vez reestablecido el servicio, se comunicará a los afectados el" fin de situación de contingencia".	

Código:	Nombre:
PC-09	Caída THEMPUS
Equipo de recuperación/ Responsable:	
Equipo de Operaciones Informáticas	
Recursos necesarios:	
• Todos los recursos del plan	
Tiempo objetivo de recuperación:	
4 horas	
Pre-requisitos:	
• Disponer de copia de seguridad Disponer de máquinas de respaldo	
Secuencia de Acciones:	
Ver Anexo D	

Código:	Nombre:
PC-10	Recuperación de Evidencias Electrónicas
Equipo de recuperación/ Responsable:	
Equipo de Operaciones Informáticas	
Recursos necesarios:	
Todos los recursos del plan	
Tiempo objetivo de recuperación:	
24 horas	
Pre-requisitos:	
• Disponer de copia de seguridad • Disponer de máquinas de respaldo	
Secuencia de Acciones:	
Ver Anexo D	

Código:	Nombre:
PC-11	Imposibilidad acceso instalaciones
Equipo de recuperación/ Responsable:	
Todos los equipos de recuperación	
Recursos necesarios:	
Todos los recursos del plan de contingencia	
Tiempo objetivo de recuperación:	
6 horas	
Pre-requisitos:	
Todos los recursos disponibles	
Secuencia de Acciones en horario laboral:	
1. Prohibir el acceso a las instalaciones de todo personal 2. Habilitación de VPN y/o puestos de TeamViewer 3. Habilitación de CentrexIP 4. El responsable de Seguridad deshabilitará todos los procesos de copia de seguridad que provocan el apagado de los equipos. 5. Distribución de portátiles a los empleados que carezcan de portátil u PC propio. 6. la delegación de Madrid asume el mantenimiento y soporte de emergencia de las aplicaciones SIGA, teniendo máxima prioridad la plataforma Thempus 7. Habilitación de teletrabajo atendiendo a las indicaciones de I-SI-02-14	

Revisiones y mantenimiento

Autorización de revisión

El responsable de Seguridad de SIGA98 es el encargado de autorizar la introducción de cambios en el Plan de Contingencia, previo estudio de la idoneidad de estos.

Frecuencia de actualización

El Plan de Continuidad de Negocio será revisado al menos una vez al año, coincidiendo con la Revisión por la Dirección del SGSI.
No obstante, cualquier miembro de SIGA98 puede sugerir una revisión del plan cuando detecte que este pueda verse afectado por:

- Introducción de nuevos equipos
- Actualizaciones de los sistemas
- Cambios en personal, direcciones o números de teléfonos, estrategia comercial, local, medios y recursos, legislación, contratistas, proveedores y clientes claves, procesos, riesgos, etc.

El histórico de todas las versiones y modificaciones introducidas en este Plan de Contingencia se encuentran detalladas en la tabla de control de versiones de la segunda página de este documento.

Lista de distribución del plan

El presente plan de continuidad ha sido comunicado y distribuido a las siguientes personas:

Ejemplar Nº	Asignado a	Cargo
001	Miguel Ángel Romero Dávila	Director General
002	Eva Lucía Garrido Durán	Directora Administración
003	Marcos Bouza Fernández	Director Técnico

Tabla 9. Lista de distribución del plan

Copias externas

Copia online en: http://www.gestores.net/plancontingencia/plan_contingencia.pdf

Copia en la caja fuerte

Manuales de configuración

Backups

Nombre del activo:	<Backups>
Nombre del documento:	<Procedimiento Bakcups>
Tipo de documento:	Manual propio de la empresa
Ubicación formato electrónico:	company/SIGA Doto_Tecnico/Manuales/backups.pdf
	Llave USB, www.gestores.net/plancontingencia/ backups.pdf

Servidor THEMPUS Apache

Nombre del activo:	*<ServidorThempusApache>*
Nombre del documento:	<Manual Configuración Servidor THEMPUS APACHE>
Tipo de documento:	Manual propio de la empresa
Ubicación formato electrónico:	company/SIGA Dpto_Tecnico/Manuales/ServidorThempusApache.pdf
	Llave USB, www.gestores.net/plancontingencia/ ServidorThempusApache.pdf

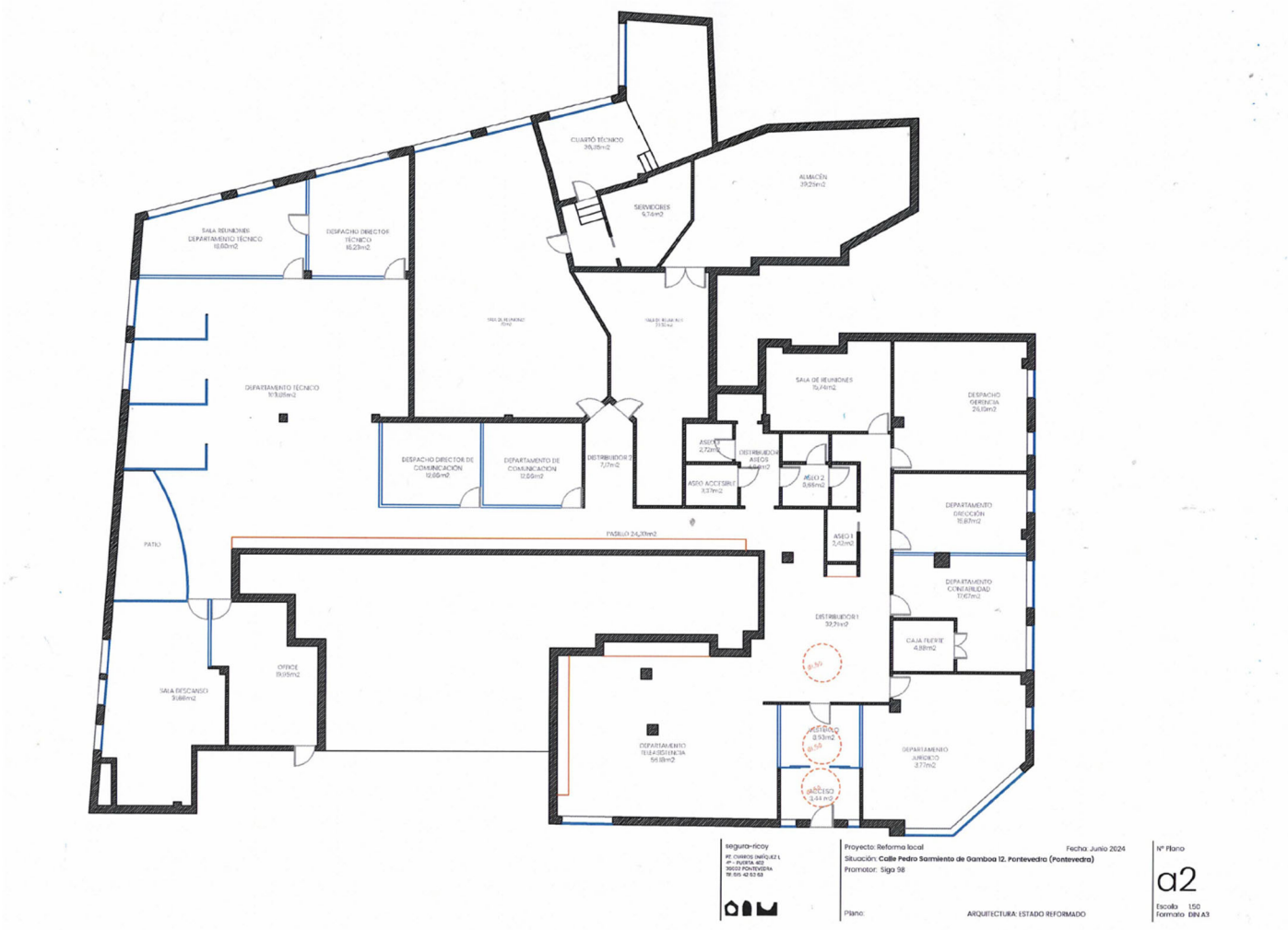
Servidor THEMPUS Cluster

Nombre del activo:	*<ServidorthempusCluster>*
Nombre del documento:	<ServidorThempusCluster>
Tipo de documento:	Manual propio de la empresa
Ubicación formato electrónico:	company/SIGA Dpto_Tecnico/Manuales/ServidorThempusCluster.pdf
	Llave USB, www.gestores.net/plancontingencia/ ServidorThempusCluster.pdf

Planos de situación

Centros principales

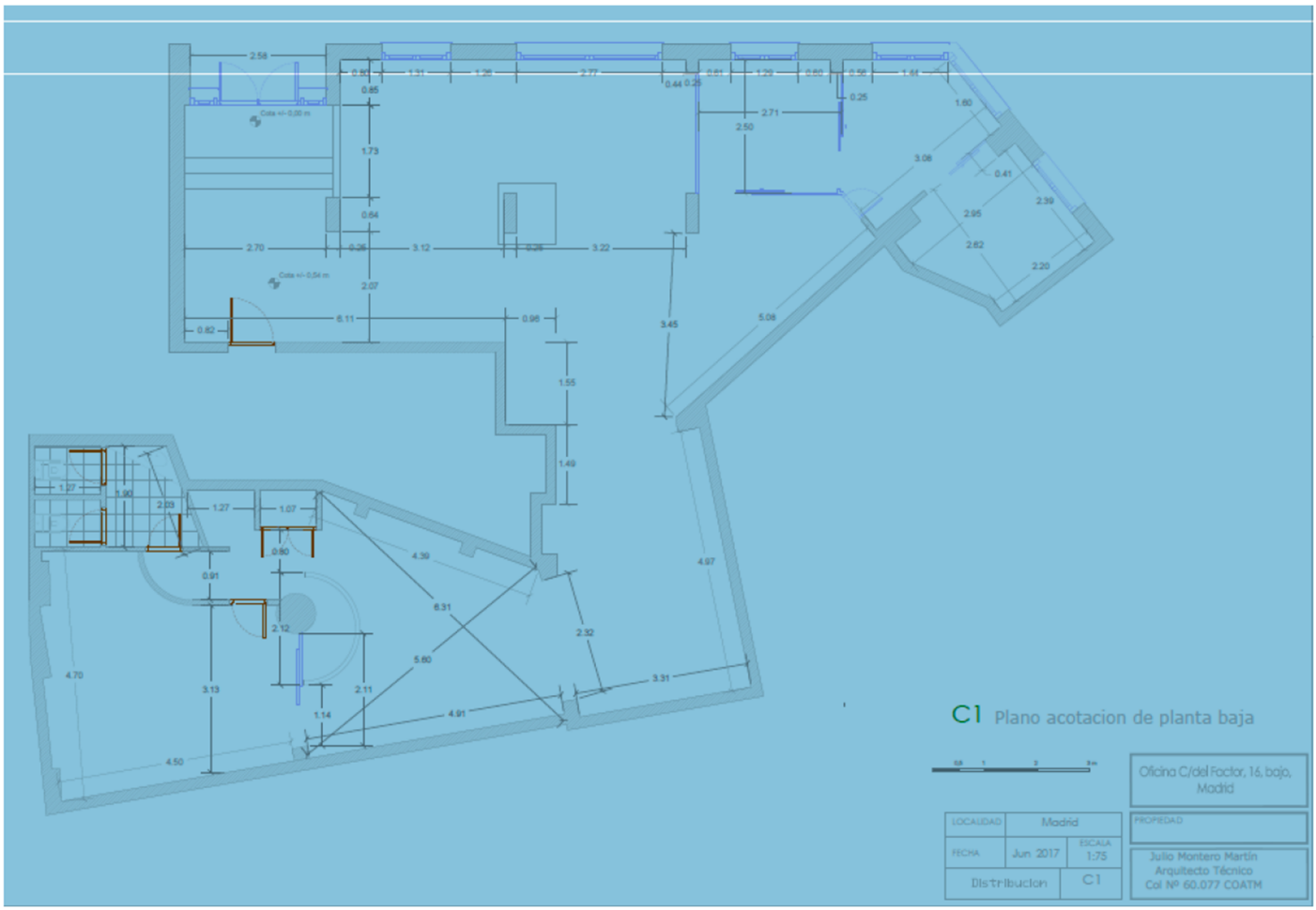
Plano de oficinas de SIGA98



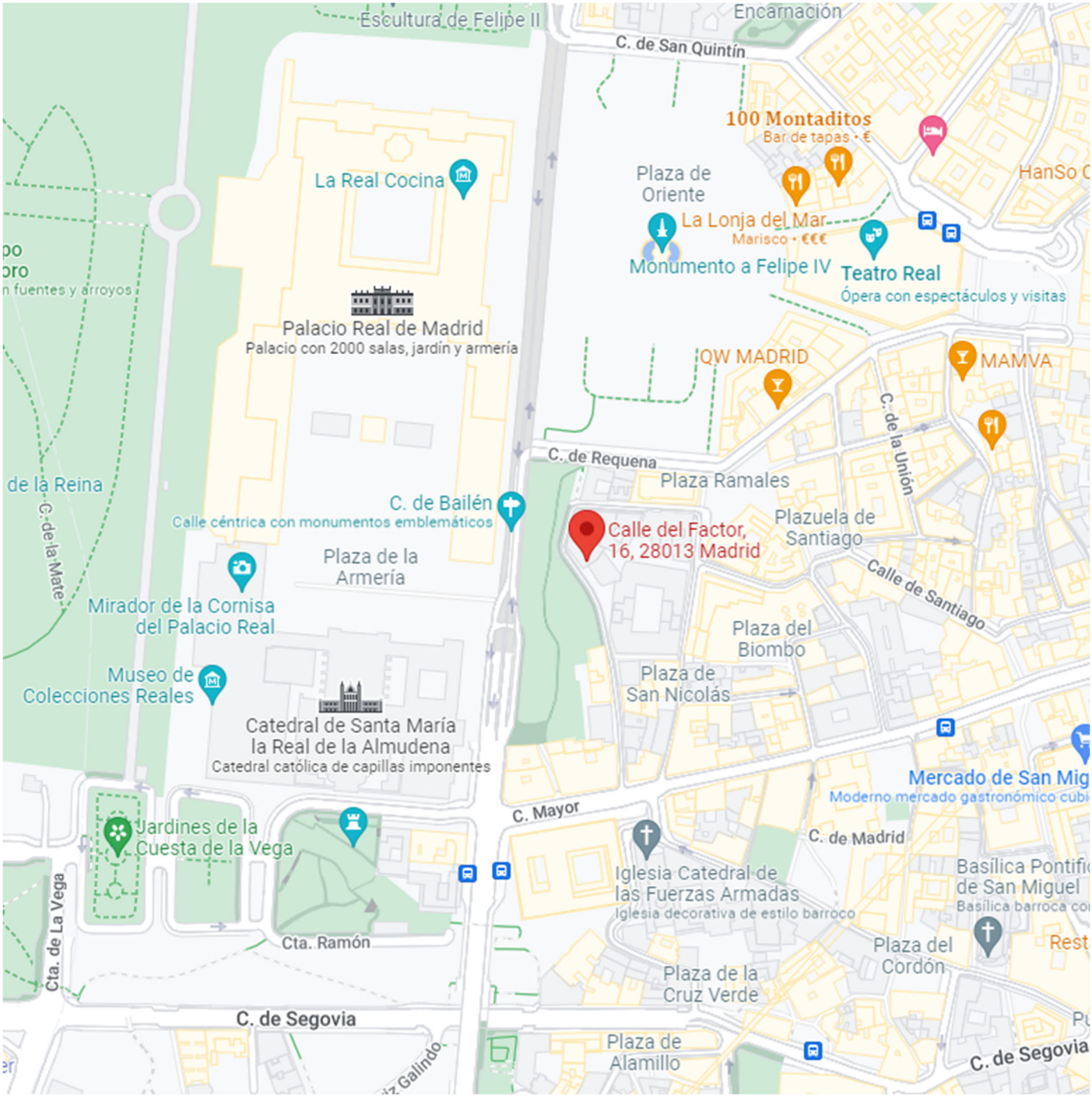
Plano de entorno (Google Maps)

Centros principales

Plano de delegación Madrid de SIGA98



Plano de entorno (Google Maps)



Instalaciones alternativas

Plano de situación

Esquemas de red

Ver Anexo F

Recuperación de copias y plantillas de notificación

Recuperación copias de respaldo

Las copias de seguridad se encuentra en el NAS.

Registros de control de eficiencia y mantenimiento del plan

Formación y sensibilización de los participantes en el plan.

La formación y sensibilización del personal es gestionada según lo establecido en el proceso P_AP_04 *Recursos humanos*.

Las actividades de planificación, seguimiento, control y evaluación de la eficacia de la formación, son registradas en la intranet corporativa de SIGA98, del mismo modo que el resto de actividades formativas.

Pruebas y simulacros (Ver Anexo A)

Para poder comprobar el correcto funcionamiento del plan y detectar/mejorar incidencias en el mismo, se planifican simulacros periódicos.

Los resultados de los simulacros y pruebas realizados se plasman por escrito reflejando el escenario, los resultados de los mismos y las lecciones aprendidas en cada uno de los casos.

Listas de chequeo (Ver Anexo B)

Al objeto de realizar controles periódicos sobre las medidas de emergencia y seguridad establecidas, se cumplimentan los checklist de seguridad y de servidor con periodicidad semestral.

Evacuación del personal en caso de emergencia

Lista de tablas y figuras