PSI-12 Continuidad de Negocio

Revisado por:	Aprobado por: Dirección	Elaborado por: Resp. de Sistema
Fecha:	**Fecha:**	**Fecha:**
Firma:	**Firma:**	**Firma:**

0. Objeto

El objetivo del presente documento es definir la sistemática establecida por **CLÍNICA BEIMAN** para salvaguardar la actividad normal de la empresa cuando se produzcan contingencias graves que afecten a la información e impidan parcial o totalmente su normal funcionamiento.

La continuidad de negocio es un componente de la estrategia de gestión del riesgo de la empresa. La dirección da la máxima prioridad a asegurar que los procesos críticos y la tecnología, puedan continuar dando el servicio a los clientes y usuarios, a pesar de inconvenientes y circunstancias adversas.

Los objetivos de este proceso son:

- Optimizar la efectividad de las operaciones tras una contingencia.
- Identificar las actividades, recursos y procedimientos para llevar a cabo las operaciones y los servicios imprescindibles en caso de una interrupción prolongada de la operativa normal.
- Asignar responsabilidades al personal y proporcionar indicaciones para la recuperación de los sistemas en caso de interrupciones prolongadas de la operativa normal.
- Asegurar la coordinación con otras organizaciones cuya colaboración pueda ser necesaria.

0.1. Entradas y salidas del proceso

Entradas:

- Incidentes alteradores que afecten a la continuidad del negocio

Salidas:

- Recuperación ante las situaciones de crisis o desastre.

1. Procesos y activo críticos de la organización

Los procesos que se han determinado como críticos han sido reflejados en el correspondiente Plan de Continuidad de Negocio (PCN) de **CLÍNICA BEIMAN.**

Los activos críticos son los identificados en la matriz de análisis de riesgos.

Responsable: Dirección/Responsable de Seguridad de la Información

2. Detección de situaciones de emergencia

Quien detecte cualquier posible situación de emergencia lo notificará al Responsable de Área asignado o en su defecto a Dirección, transmitiéndole toda la información posible, por los canales definidos a tal fin en el PCN. Al menos, debería comunicar los siguientes datos:

- Ubicación u origen de la contingencia

- Naturaleza de la contingencia: realizar la descripción de la contingencia
    - Emergencias: Incendio y/o explosión, inundación, etc.
    - Fallos/pérdidas de activos críticos, que dificulten o impidan el correcto desarrollo de la actividad (caída servidores, caída de suministro eléctrico, caída de red, etc.).
- Magnitud de la contingencia: valoración preliminar sobre la gravedad de la contingencia

Responsable: Todo el personal

3. Evaluación

Si es posible acude al lugar dónde se ha producido la contingencia, y en cualquier caso realiza una valoración preliminar. Esta persona valorará la necesidad de activar el plan de continuidad en función de la contingencia identificada.

Responsable: Responsable de Seguridad de la Información/Responsables de Área

4. Activación, comunicación y escalado

CLÍNICA BEIMAN ha determinado una lista de personas para que, en el caso de que cualquier miembro de la misma detecte una crisis o desastre, lo comunique directamente a las personas incluidas en ella y por orden, puesto que son los encargados de iniciar o activar el proceso de gestión de la continuidad, incluidos en el registro de personal para la activación de los planes de continuidad.

Responsable: Todo el personal

5. Estrategias de recuperación

Se han considerado varios escenarios como base para la gestión de la continuidad de la seguridad de la información y se han asumido varios supuestos, los cuales están recogidos en el plan de continuidad. Este plan presupone dos principios claves las instalaciones de la empresa no son accesibles, o los activos críticos se han visto afectados de modo tal que **CLÍNICA BEIMAN** no puede realizar las operaciones y servicios habituales.

Las principales áreas asumidas en la preparación de este plan son:

- Los sistemas no están operativos y no pueden ser recuperados dentro de las siguientes 24 horas.
- El personal clave relacionado con los activos y servicios incluidos en este plan han sido identificados y formados en sus funciones y responsabilidades en caso de emergencia y están disponibles para activar el plan.
- Las medidas de seguridad (sistemas de extinción de incendios, alarmas, extintores, etc.) están completamente operativos en el momento del desastre.

- Las copias de seguridad actualizadas están intactas y disponibles en un almacenamiento fuera de la ubicación original.
- La estrategia de recuperación elegida por la empresa consiste en tener un CPD de emergencia y existirá un backup cifrado en la nube.

1. SERVIDORES

Los servidores gracias a las copias de seguridad programadas y a la naturaleza de estos pueden subsistir a cualquier incidencia, sin una perdida notable de información.

El servidor que contenga información clasificada como crítica o que contenga el gestor de pacientes KYROS24h debe tener las siguientes características software:

- Sistema operativo: Debian 11.3.0
- Sistema operativo: Microsoft Windows Server 2022 Standard
- Servidor web: Server.Apache 2.4
- Servidor de base de datos: MySQL Server.
- Servidor web: IONOS
- SOFTWARE

Para la continuidad de las aplicaciones críticas, disponemos de la posibilidad de la descarga del software del proveedor a través de la correspondiente licencia.

2. PERSONAS

   Las personas sirven de respaldo unas con otras.

3. INFORMACIÓN

Sobre la información crítica se realiza copias de seguridad de forma continua y previamente establecida por el Responsable de Seguridad.

No obstante, en **CLÍNICA BEIMAN** se dispone de una copia de seguridad con toda la información crítica de la empresa, ubicada en una zona completamente protegida de cualquier tipo de contingencia (inundación, incendio, etc.)

4. COMUNICACIONES

Existe un contrato de soporte con las empresas suministradoras.

5. INSTALACIONES

CLÍNICA BEIMAN dispone de instalaciones alternativas en otros lugares para dar soporte a nuestros clientes, pero que en ningún caso funcionan de forma autónoma y dependen completamente de la sede principal.

En caso de no poder acceder al lugar de trabajo, el personal sería desplazado a sus domicilios particulares y toda la infraestructura necesaria.

Se dispone de otro CPD en las instalaciones de la delegación de **CLÍNICA BEIMAN** Las Cabezas, realizándose una copia del CPD principal mediante la herramienta Duplicati diariamente y en horario nocturno.

Responsable: Responsable de Seguridad de la Información

6. Contingencias identificadas y Plan de Continuidad

Todas las contingencias han sido identificadas en el PCN de **CLÍNICA BEIMAN.**

Responsable: Responsable de Seguridad de la Información

7. Revisión del Plan de Continuidad

El plan de continuidad de la empresa tiene que ser realizable en cualquier momento. Para ello, se llevarán a cabo revisiones periódicas en las que se asegurará:

- Las responsabilidades están correctamente definidas y los responsables adecuadamente formados y entrenados para la puesta en marcha de los correspondientes planes.
- Los activos pueden ser sustituidos en la forma y plazos previstos, especialmente aquellos identificados como de especial dificultad de recuperación

La necesidad de actualizar activos cuya reposición no pueda ser asegurada (por no existir en el mercado, por tratarse de sistemas antiguos u obsoletos, etc.).

Responsable: Responsable de Sistema

8. Pruebas de continuidad

El correcto funcionamiento del Plan de continuidad definido, así como la eficacia de las estrategias de recuperación tanto parciales (por activos) como globales (de actividad), definidas en el mismo, son fundamentales para asegurar la continuidad de la actividad de **CLÍNICA BEIMAN.**

Es absolutamente necesario realizar ensayos periódicos para el éxito en la respuesta y recuperación ante fallos.

Se deben diseñar anualmente los Programas o Planes de Pruebas del Plan de Continuidad, en el que se incluya el calendario de simulacros para los activos críticos.

Las pruebas o simulacros planificados deben asegurar que se contemplan los diferentes escenarios que pueden producirse:

- Pruebas técnicas de recuperación parcial, en las instalaciones de la empresa.
- Pruebas del cumplimiento de los compromisos de servicio de los proveedores (por ejemplo: Internet, proveedor de equipos, etc.).
- Pruebas de evacuación del personal (coordinación con SPA).

Responsable: Responsable de Seguridad de la Información

9. Formatos y anexos

Descripción	Tiempo de archivo de los registros que genera	Responsable
Plan de Continuidad	3 años	Resp. del Sistema
Simulacros	3 años	Resp. del Sistema

Registro de las modificaciones		
Revisión	**Fecha**	**Naturaleza de la revisión**
00	10/08/2022	Edición Inicial