Objetivo	Fortalecer la capacidad de respuesta de la <ENTIDAD DISTRITAL> ante situaciones de fallas o desastres, mediante la creación, ejercicios de pruebas y mejora continua del plan de continuidad de negocio, para permitir la continuidad de la operación de los servicios críticos de la < ENTIDAD DISTRITAL >.
Responsable del documento	<NOMBRE DEL LÍDER DEL PROCESO ASOCIADO>

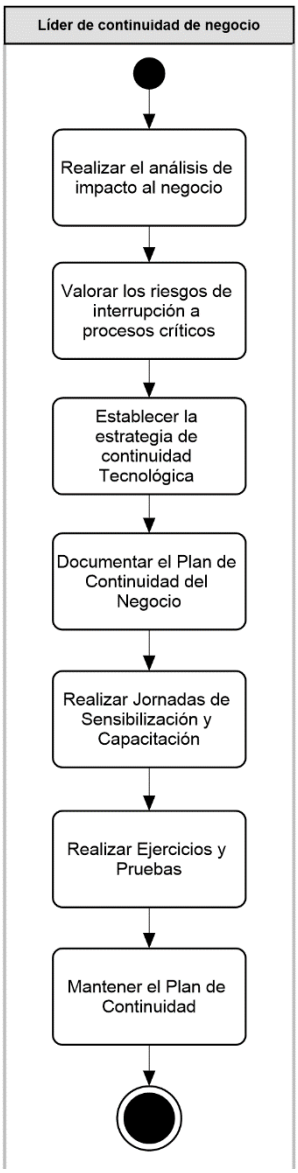
Definiciones

1. **Activación**: Acto de declarar que los acuerdos de la organización de Continuidad de Negocio deben llevarse a la práctica con el fin de continuar la entrega de productos o servicios clave.
2. **Análisis de Impacto al Negocio (BIA, por sus siglas en inglés, Business Impact Analisys):** Proceso del análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas.
3. **Continuidad de Negocio:** Capacidad de la organización para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial.
4. **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias.
5. **Incidente**: Situación que sería o podría llevar a una interrupción, pérdida, emergencia o crisis.
6. **Infraestructura:** Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización.
7. **Mejoramiento continuo:** Actividad periódica para mejorar el desempeño.
8. **BCP:** (por sus siglas en inglés, Business Continuity Plan - Plan de Continuidad de Negocio), Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel pre-definido de operación debido a la interrupción.
9. **Plan de emergencias:** Documento que contempla las acciones e instrucciones que se deben seguir para responder rápida, eficaz y con el menor traumatismo posible ante una Emergencia.
10. **DRP: (**Por sus siglas en inglés, Disaster Recovery Plan **-** Plan de Recuperación de Desastres), es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.
11. **Prueba**: Procedimiento para determinar la presencia, cualidad o veracidad de algo.
12. **RPO: (**Por sus siglas en inglés, Recovery Point Objetive - Punto Objetivo de Recuperación), punto en el cual la información usada por una actividad debe ser restaurada para permitir la reanudación de la operación.
13. **Recurso:** Todos los activos**,** recursos humanos, conocimientos, información, tecnología, locales y suministros e información que una organización tiene que tener disponibles para su uso, cuando sea necesario, con el fin de operar y cumplir con su objetivo.
14. **Riesgo**: Efecto de la incertidumbre sobre los objetivos.
15. **RTO:** (Por sus siglas en inglés, Recovery Time Objetive -Tiempo objetivo de recuperación), periodo de tiempo después de un incidente en el que: El producto o

servicio debe ser reanudado, o la actividad debe reanudarse, o los recursos deben ser recuperados.

ALCALDÍA MAYOR DE BOGOTÁ D.C. BOGOTÁ MEJOR PARA TODOS	PROCEDIMIENTO DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO	Código:
		Versión:
Proceso asociado	<NOMBRE DEL PROCESO ASOCIADO>	

Actividades del procedimiento:



Marco normativo

- Modelo de seguridad y privacidad de la información – Ministerio de las TIC
- ISO/IEC 27001:2013.
- ISO/IEC 22301:2011.

.

Lineamientos, políticas de operación y otros aspectos a tener en cuenta

[Los siguientes aspectos se puede adoptar como lineamientos y políticas de operación, y es a potestad de la entidad decidir cuáles adoptar.]

1. El líder de la Gestión de Seguridad de la Información para el Plan de Continuidad de Negocio de la <nombre de la entidad> tendrá de insumo los riesgos críticos hallados al aplicar el procedimiento de gestión de riesgos de seguridad de la información. Cualquier cambio en la definición de la criticidad de los riesgos debe ser informado al responsable de la gestión del Plan de Continuidad de Negocio de la <nombre de la entidad>.
2. El nivel de aceptación del riesgo de la matriz de riesgo de seguridad de la información deberá ser aprobado por la alta gerencia.
3. La identificación de los procesos críticos de la entidad debe ser un trabajo participativo de las diferentes dependencias de la Entidad Distrital.
4. Los cambios en la infraestructura y organización interna que afecte los procesos críticos definidos dentro del plan deben ser informados al responsable líder de la gestión de Seguridad de la Información del Plan de Continuidad de Negocio.
5. Los ejercicios y pruebas del plan de continuidad del negocio son parte vital para garantizar la operatividad del plan, los cuales se realizarán periódicamente previa definición del plan de trabajo y con la participación de los líderes de cada área de los procesos críticos y de la Oficina de Tecnologías de la Información, generando la documentación respectiva que soporte los resultados obtenidos e informarlos y notificarlos al Comité Institucional de Planeación y Gestión.
6. La activación y/o desactivación del BCP, está formalizada dentro del plan de emergencias.
7. La <nombre de la entidad> debe proveer los recursos necesarios establecidos mediante el Plan Anual de Gestión – PAG, y mediante los proyectos de inversión.
8. El líder de la gestión de Seguridad de la Información ejecuta la revisión del documento del BCP como mínimo una vez en el año, previa definición del plan de trabajo y debe considerar los resultados obtenidos en los ejercicios y pruebas realizados al BCP.
9. Los líderes de los procesos críticos son los responsables de liderar la operación del BCP, e informar cualquier cambio en el Plan de Continuidad de Negocio al líder de la gestión de Seguridad de la Información.