Procedimiento gestión de la continuidad del servicio TI

1. OBJETIVO

Impedir que una imprevista y grave interrupción de los servicios TI, debido a desastres naturales u otras fuerzas de causa mayor, tengan consecuencias graves para la Corporación, impida el normal funcionamiento de sus operaciones.

2. ALCANCE

Inicia con el Análisis de Impacto al Negocio (BIA), continua con la selección de estrategias y la definición del plan y finaliza con las pruebas y mantenimiento del BCP.

3. DEFINICIONES

Plan de continuidad del negocio (BCP): Es un plan logístico enfocado a los servicios TI para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de un desastre no deseado

Respaldo: Archivos, equipos, información y procedimientos disponibles para su uso en el caso de una falla o pérdida, si se destruyen los originales o si se está en el sitio alterno

Sitio alterno: Ubicación alterna de operaciones seleccionada para ser utilizada por la corporación cuando las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales después de que se ha producido una interrupción.

Gestión de continuidad de negocio (BCM): Proceso general de gestión holístico que identifica amenazas potenciales de la corporación y el impacto que se podría causar a la operación de negocio que en caso materializarse. Provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes interesadas claves, reputación, marca y actividades de creación de valor.

Plan de Continuidad de Negocio (BCP): Procedimientos documentados que guían orientan a la corporación para responder, recuperar, reanudar y restaurar la operación a un nivel de operación aceptable y tolerable tras presentarse una interrupción de servicios.

NOTA: Típicamente, esto incluye los recursos, servicios y actividades necesarios para garantizar la continuidad de las funciones críticas del negocio. [Fuente: ISO 22301]

Análisis del impacto al negocio (BIA): Análisis de actividades, servicios operacionales y el efecto que una interrupción del negocio podría tener sobre ellas. [Fuente: ISO 22300]

Nivel de Criticidad: Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o servicio que debe estar disponible y operativo constantemente o disponible y operativo al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.

Interrupción: Incidentes, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden detener de forma parcial o total, el normal curso de las operaciones de la corporación.

Plan de recuperación de desastres (DRP): Plan claramente definido y documentado el cual permite recuperar las capacidades de tecnología y Telecomunicaciones de los servicios de Tecnología de la información y telecomunicaciones cuando se presenta una interrupción.

Escenario de interrupción: Conjunto de situaciones que componen el estado de infraestructura tecnológica al momento de presentarse una interrupción.

Punto objetivo de recuperación (RPO): Punto en el tiempo previo a la interrupción en el cual los datos deben ser recuperados teniendo en cuenta la cantidad de datos que la corporación está dispuesta a perder.

Punto Tiempo objetivo de tiempo de recuperación (RTO): Periodo de tiempo en el cual los mínimos niveles de productos y/o servicios y los sistemas, aplicaciones, o funciones que los soportan deben ser recuperados después de que una interrupción ocurra.

Tiempo de trabajo en recuperación (WRT): Corresponde al tiempo posterior una vez se ha alcanzado el RTO hasta estabilizar con total normalidad la operación de la corporación.

Tiempo máximo de inactividad (MTD): Corresponde al tiempo que la corporación puede tolerar la ausencia o indisponibilidad de los servicios que permitan su normal operación. Normalmente se puede expresar como la suma de RTO y WRT.

Resiliencia: Capacidad de la corporación para resistir y recuperar su productividad cuando es afectada por una interrupción.

Disparador o detonante: Evento que hace que el sistema inicie una respuesta.

NOTA: También conocido como evento activador.

Proceso: Conjunto de actividades y recursos de trabajo relacionados entre sí, que basa su funcionamiento en entradas de información para obtener un resultado previsto conocido como salida que para el caso de la corporación se entiende como un servicio.

Área: Grupo al cual pertenecen los procesos de la organización de acuerdo con el mapa de procesos.

Servicio tecnológico: Conjunto de actividades, herramientas, aplicaciones, sistemas, elementos de conexión o dispositivos, que se encuentran disponibles para que los procesos de la corporación desarrollen sus actividades. También pueden llamarse productos tecnológicos.

Tipo de servicio: Clasificación para la agrupación de servicios de acuerdo con la función principal que presta para la corporación. (Ej. La función principal de los conmutadores es prestar un servicio de conectividad alámbrica).

Código malicioso: Es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos. Se trata de un tipo de amenaza que no siempre puede bloquearse con solo un software antivirus.

Activo de Información: Corresponde a aquella información que representa un valor para la corporación y por tanto se debe proteger. Se refiere a datos creados o usados en medio digital, hardware o software para procesamiento, transporte o almacenamiento de

información, herramientas o utilidades para el desarrollo o soporte de las tecnologías de la información.

4. CONDICIONES GENERALES

4.1 El área de TI es responsable de establecer y mantener las políticas de continuidad y las políticas de recuperación de información, identificando estándares, normas, directivas en la materia, documentarlas y publicarlas como lineamiento transversal para toda la Corporación.

4.2 El área de TI es la encargada de gestionar riesgos de Tecnologías de Información, y ejecutar el plan de continuidad de los servicios de TI.

4.3 Flujo de comunicación y autoridad

En caso de presentarse una interrupción de servicio, los conductos regulares de comunicación se encuentran establecidos por la organización en la Matriz de Flujo de Comunicación Interna que permite conocer la manera adecuada de informar sobre el estado de los servicios, bajo las condiciones previstas y así mismo indica los responsables. Los eventos de comunicación se presentan para informar los siguientes casos:

a. Evento de interrupción de servicios
b. Notificación oficial de interrupción e inicio de Plan de Continuidad.
c. Notificación de recuperación de servicios.
d. Notificación de estado de servicios

En cualquiera de los eventos anteriores, el documento relacionado indica que la comunicación se debe establecer de manera digital por medio del correo electrónico, motivo por el cual este servicio tendrá la prioridad de recuperación en caso de una eventual falla.

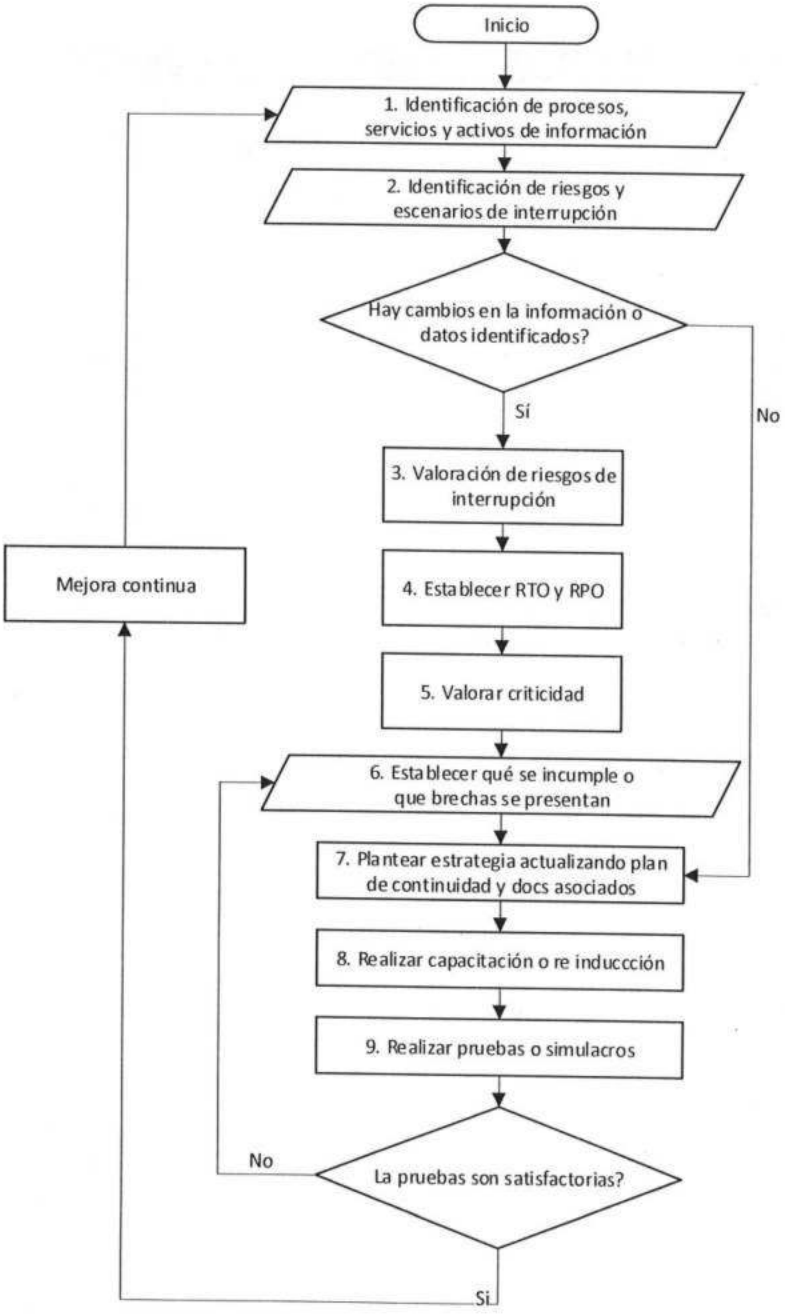
Procedimiento gestión de la continuidad del servicio TI

5. DESARROLLO

No.	Actividad	Responsable	Registro
1.	Identificar y clasificar los procesos, servicios y activos de información de la corporación.	Oficial TI	Instructivo plan de continuidad del negocio.
2.	Identificar los riesgos y posibles escenarios de interrupción que pueden afectar la operación de los servicios tecnológicos de la corporación.	Oficial TI	Matriz de escenarios de interrupción
3.	Valorar los riesgos de interrupción de servicios mediante la matriz de riesgos para los activos de la información de la Corporación.	Oficial TI	Matriz de riesgos H02-MA-SC-01
4.	Establecer los tiempos de recuperación y la tolerancia de pérdida de información de la corporación de acuerdo con los servicios y activos identificados.	Oficial TI	Planillas de Análisis de Impacto F03-PR-TI-06
5.	Valorar la criticidad de los servicios y activos de información tecnológica bajo responsabilidad de TI.	Oficial TI	Instructivo plan de continuidad del negocio.
6.	Establecer los incumplimientos a los requisitos (brechas) para plantear la metodología de continuidad que permita minimizar la probabilidad de materialización de riesgos o la ejecución de actividades de cumplimiento.	Oficial TI	Instructivo plan de continuidad del negocio.
7.	Actualizar el plan de continuidad de negocio y los documentos relacionados, donde se evidencie la estrategia de continuidad tecnológica analizando los riesgos y recursos de la corporación.	Oficial TI	Instructivo plan continuidad del negocio.
8.	Realizar jornadas de capacitación o reinducción	Oficial TI	Lista de Asistencia F10-TH-05
9.	Realizar pruebas, conforme a las frecuencias definidas en el plan de continuidad de negocio.	Oficial TI	Formato control de restauración de backups. F02-PR-T. I-03
10.	Mantener el plan de continuidad de negocio, registrando las mejoras identificadas durante los ejercicios de pruebas.	Oficial TI	Instructivo plan continuidad del negocio.

Procedimiento gestión de la continuidad del servicio TI

6. FLUJOGRAMA



7. DOCUMENTOS DE REFERENCIA

- ITIL V3
- NTC ISO-22301:2012 Continuidad de Negocio. Sistemas de gestión de Continuidad de Negocio. Requisitos.
- NTC ISO-IEC 27001:2013 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información Requisitos.
- Guía para la preparación de las TIC para la continuidad del negocio, MINTIC.

8. HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción
Septiembre 26 de 2017	1	Creación del procedimiento
Diciembre 11 de 2019	2	Se adiciona las definiciones de resiliencia, disparador o detonante, proceso, área, servicio tecnológico, tipo de servicio, código malicioso, nivel de criticidad, interrupción, Se adiciona el flujo de comunicación y autoridad en los casos de interrupción del servicio. Se incluye en el flujo, lo relacionado con los tiempos de recuperación y la tolerancia de pérdida de información de la corporación de acuerdo con los servicios y activos identificados. Incluye lo relacionado con los incumplimientos a los requisitos (brechas) para plantear la metodología de continuidad que permita minimizar la probabilidad de materialización de riesgos o la ejecución de actividades de cumplimiento.

Aprobación	Nombre	Cargo	Fecha Aprobación
Elaboró	Milena Hernández	Oficial T. I	Diciembre 11 de 2019
Revisó	María Ximena Obando Oscar Figueroa	Gerente Administrativa Financiera Asesor Calidad	
Aprobó	Juan Gabriel Pérez	Director Ejecutivo	

Juan Gabriel Pérez Chaustre
Director Ejecutivo