

Plan de Continuidad y Recuperación del Negocio

SOCIEDAD TEQUENDAMA

BOGOTA D.C.

Nuestras líneas de negocio son:



Contenido

Propósito

3

1. 3
2. **¡Error! Marcador no definido.**
3. **¡Error! Marcador no definido.**
4. 7
5. **¡Error! Marcador no definido.**
6. 10
7. 14
8. 15
9. 16
10. 17
11. **¡Error! Marcador no definido.**
12. 18
13. 19
14. 21
15. 23

Propósito

Este documento describe los lineamientos para cumplir con el plan de Continuidad y Recuperación tecnológica. Ante eventos que puedan impedir el normal desarrollo de las operaciones soportadas por la tecnología. La metodología a seguir tiene las siguientes etapas:

- a) Diagnóstico. Identificación del estado actual – As IS
- b) Planificación, Estudio y elaboración
- c) Ejecución e implementación.
- d) Prueba y Análisis de resultados
- e) Acciones de mejora

La implementación del Plan de Continuidad y Recuperación Tecnológica es un proceso que resguarda la operación y la información con el objetivo de continuar la operación mientras se recupera en su totalidad.

Este documento toma como marco de referencia la “Guía para la preparación de las TIC para la continuidad del negocio” y los Lineamientos Plan de Continuidad Tecnológico del Negocio Sector Defensa, contemplando parámetros aplicables y no su aplicabilidad exhaustiva al detalle.

1. Objetivo

Diseñar una estrategia de continuidad de los servicios de TI, que tenga como base la reducción del impacto de una interrupción en los servicios críticos de TI del negocio, este debe estar difundido, aprobado y respaldado por los directivos de la entidad.

- a) Realizar un análisis e identificación de recursos críticos de TI vitales servicios, aplicaciones y plataformas, para generar una estrategia que genere prioridades en caso de presentarse una o varias situaciones que causen interrupciones.
- b) Asegurar que el plan de continuidad de TI, se encuentre actualizado y permita afrontar las amenazas que traen consigo las nuevas tendencias tecnológicas sin perder el alcance de los requerimientos de la Entidad.
- c) Elaborar un plan de pruebas de continuidad de TI, que permita verificar y asegurar que los sistemas de TI, puedan ser recuperados de forma segura y efectiva, atendiendo y corrigiendo errores, que atenten contra la disponibilidad de las operaciones.
- d) Realizar capacitaciones del plan de continuidad de TI y análisis de impacto del negocio, a los entes o partes involucradas de la organización (Equipo de seguridad de sistemas de información de la entidad), para que conozcan cuáles son sus roles y responsabilidades en caso de incidentes o desastres.
- e) Aplicar una metodología para facilitar la recuperación de la operación y servicios tecnológicos críticos ante una eventual contingencia: procedimientos que respondan a las interrupciones
- f) Identificar el personal clave que participa en los procesos de recuperación y restauración de las plataformas y/o servicios.
- g) Establecer los tiempos mínimos de recuperación requeridos en los que no se vea afectado el negocio.

- h) Identificar los riesgos presentes para la continuidad.
- i) Establecer un plan de prueba, gestión y mantenimiento necesarias para garantizar los objetivos del Plan

Es necesario verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia generadas dentro de la entidad. Tanto el plan de continuidad de TI como el análisis de impacto del negocio deben estar disponibles apropiadamente dentro de la organización y en manos de los responsables de las áreas de TI quienes de forma segura deben garantizar su aplicabilidad en los momentos críticos, a su vez la entidad debe propender por un plan de sensibilización al interior de la misma con el propósito de indicar a todos sus miembros sobre la importancia de contar con un plan de continuidad y de análisis del negocio que van a garantizar el normal funcionamiento de las operaciones regulares en caso de presentarse problemas críticos en los sistemas de información y comunicaciones de la entidad

2. Definiciones

Sitio alternativo. Ubicación alterna de operaciones seleccionada para ser utilizada por una organización 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 a una organización y el impacto que se podría causar a la operación de negocio que en caso de materializarse y el cual 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. Procedimientos documentados que guían orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación debido una vez presentada / tras la interrupción. (recursos, servicios y actividades). ISO 22301]

Análisis del impacto al negocio (BIA por sus siglas en ingles). Proceso del análisis de actividades. Disponibilidad requerida de la plataforma tecnológica para soportar los procesos de la entidad, con el fin de garantizar la continuidad en la prestación del servicio a los usuarios internos y externos. [Fuente: ISO 22300]

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

Interrupción. Incidente, 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 afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

Recuperación de desastres de tecnología y telecomunicaciones (ITCTIC). Habilidad Capacidad de los elementos de tecnología y telecomunicaciones (ITC) de las TIC de la

organización para soportar sus funciones críticas a un nivel aceptable dentro de un periodo predeterminado de tiempo después de una interrupción.

Plan de recuperación de desastres de ICT LAS TIC (ICT DRP). Plan claramente definido y documentado el cual permite recuperar las capacidades de tecnología y Telecomunicaciones LAS TIC cuando se presenta una interrupción. Plan de continuidad de tecnología y telecomunicaciones las TIC.

Modo de falla. Describe la manera en que la falla ocurre y su impacto en la operación del sistema.

Preparación de las ICT TIC para la continuidad de negocio (IRBC). Capacidad de una organización para soportar sus operaciones de negocio mediante la prevención, detección y respuesta a una interrupción así como la recuperación de sus servicios de ICTTIC.

Objetivo mínimo de continuidad de negocio (MBCO). Mínimo nivel de productos y/o servicios que es aceptable para que la organización alcance sus objetivos de negocio durante una interrupción.

Punto objetivo de recuperación (RPO). Punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra.

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.

Resiliencia. Habilidad: Capacidad para que una organización para resistir cuando es afectada al ser afectada por una interrupción.

Evento activador. Evento que hace que el sistema inicie una respuesta.

Registro vital. Registro electrónico o en papel que es esencial para preservar, continuar o reconstruir las operaciones de una organización y proteger los derechos

Plataforma tecnológica crítica: Hace referencia a los sistemas de información, servidores, bases de datos, sistemas de almacenamiento y respaldo, equipos y enlaces de comunicación que son críticos para soportar los procesos y servicios de la entidad.

Norma NTC/ISO 22301: La Gestión de la Continuidad del Negocio (BCM) es un proceso de gestión que ayuda a identificar las amenazas potenciales y los riesgos de tipo operacional que amenazan la continuidad de las actividades de las Entidades y provee una estructura de referencia para la construcción de la resiliencia y la capacidad de una respuesta efectiva para construir confiabilidad y capacidades de respuesta efectiva que proteja los intereses de las entidades a partir de disrupciones. (MinTic, Guía para la preparación de las TIC para la continuidad del negocio, 2018)

MTD: Se considera como el Tiempo Máximo de Inactividad Tolerable según la traducción de sus siglas en Ingles (Maximum Tolerable Downtime). Tiempo máximo de inactividad que puede tolerar una organización antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso (servicio)

Nube Privada: La infraestructura de la Nube es operada únicamente para una organización. Puede ser administrada por la organización o por un tercero y puede existir tanto en las instalaciones de la organización como fuera de ellas. (MDN, 2022)

Software como Servicio (SaaS). La capacidad proporcionada al consumidor es utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura en la nube. Las aplicaciones son accesibles desde varios dispositivos cliente a través de una interfaz de cliente ligero como un navegador web. (MDN, 2022)

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilita la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. [Fuente: CONPES 3854, pág. 87]. (3854, 2016)

WRT (Work Recovery Time): Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

3. Técnicas de recolección de información

Utilizaremos las técnicas de recolección primaria y secundaria.

Se anexa formulario de preguntas. Este formulario será revisado y actualizado previo a cada actividad de recolección de información

Técnicas de recolección de información primaria. Entrevistas, encuestas y talleres

- Observación
- Indagación
- Conciliación
- Inspección
- Confirmación

Técnicas de recolección de información secundaria

- Investigación directa en internet

4. Fase de Análisis de Impacto del Negocio (BIA)

La fase de Análisis de Impacto del Negocio BIA (Business Impact Analysis) permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio.

Requerimientos:

Identificar las funciones y procesos importantes para la supervivencia de la entidad al momento de la interrupción, esto es tener en cuenta cuales de los procesos son claves para que entren en operación rápidamente asignándoles la mayor prioridad posible, frente a los de menor prioridad; sin embargo, para los procesos identificados como no prioritarios se deben preparar también planes de recuperación.

Revisar las consecuencias tanto operacionales como financieras, que una interrupción tendrá en los procesos considerados de alta prioridad.

Estimar los tiempos de recuperación, en razón a las posibles alteraciones de los procesos considerados de alta prioridad para el funcionamiento de las infraestructuras de TI, a saber MTD, RTO, RPO, WRT. El Informe contiene el detalle de las funciones y procesos críticos del negocio con información de los recursos requeridos y los tiempos de recuperación.

5. Aplicaciones y plataformas críticas para la operación del negocio.

En este paso se identifican las funciones del negocio útiles para apoyar la misión y los objetivos a alcanzar en el Sistema de Gestión de Seguridad de Información de la Sociedad cuyo resultado es la generación de los roles y procesos, que sirven de análisis para el cumplimiento de los siguientes pasos del BIA.

Nivel A: La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.

Nivel B: La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.

Nivel C: La operación no es una parte integral del negocio.

Categoría (Función del Negocio)	Proceso (Servicios)	Nivel	Tolerancia a Fallas (Horas)	Descripción	MTD (en días) (RTO + WRT)	Prioridad de recuperación	RPO	RTO	WRT
Aplicaciones	Sistemas de gestión documental	B							
Aplicaciones	ERP	A		Sistema financiero contable					
Aplicaciones	Nomina	A		Sistema de entrada de novedades administrativas. Interfaces con el Sistema Financiero					
Aplicaciones	PMS	A		Sistema de entrada de clientes hotel Interfaces con el Sistema Financiero: Terceros, produccion y caja: Suites, Catering, Marine beach?, Rosario?,Tayrona?					
Aplicaciones	POS	A		Sistema de entrada de clientes POS Interfaces con el Sistema Financiero: Terceros, produccion y caja: Suites, Catering, Marine beach?, Rosario?,Tayrona?					
Aplicaciones	ZUM	A		Sistema de entrada de eventos clientes					

Categoría (Función del Negocio)	Proceso (Servicios)	Nivel	Tolerancia a Fallas (Horas)	Descripción	MTD (en días) (RTO + WRT)	Prioridad de recuperación	RPO	RTO	WRT
				Generación de OS					
Aplicaciones	DIGIDOC	B		Sistema de radicación de facturas proveedor					
Aplicaciones	ERP BC365 Histórico V14	C		Aplicativo de consulta historico año 2020 a 2023					
Aplicaciones	PMS – Opera (histórico)	C		Aplicativo de consulta historico de clientes hotel					
Aplicaciones	Novasoft contabilidad (histórico)	C		Aplicativo de consulta historico de contabilidad año xxxxx a yyyy					
Aplicaciones	Nómina OPS (histórico)	C		Aplicativo de consulta historico de nomina año xxxxx a yyyy					
Aplicaciones	PMS - Quohotel (historico)	C		Aplicativo de consulta historico de clientes hotel año 2021 a 2023					
Aplicaciones	Sistema Parqueadero (Access Park)	A							
Web	Paginas web (Unidades de negocio y corporativa)	C							
Seguridad de la información	Firewall Forti	B		Firewall de la Sociedad					
Comunicacio nes	Acceso local a internet	A		Acceso de los usuarios a internet					
Comunicacio nes	Wifi	A		Acceso de los usuarios a internet					
Proveedores de Aplicaciones y/o comunicacio nes	Internos/Ext ernos	C		Desarrollo y/o soportes externo de aplicativos contratados o canales de comunicación					
Recurso Humano	Internos/Ext ernos	B		Profesionales encargados de la administración de TI de la Sociedad					

Nuestras líneas de negocio son:



Gastronomía
Tequendama



6. Procedimientos específicos que responden a interrupciones del servicio

– Árbol de llamadas

Cuando se presente un desastre, interrupción o evento contingente, se debe seguir la siguiente cadena de llamadas:

Responsabilidad	Area	Nombre	Numero celular	Correo electrónico
Líder Continuidad de Negocios	Planeación	Andrea Malagon		planeacion@sht.com.co
Líder de Recuperación ante desastres TIC	PMS – Opera (histórico)	Maikol Chavez		maikol.chavez@sht.com.co
Líderes de Continuidad de cada Proceso	Novasoft contabilidad (histórico)	Leidy Poveda		jefetalentohumano@sht.com.co
Líderes de Continuidad de cada Proceso	Sistema Parquadero (Access Park)	Diego Velasquez		coordinador.parquadero@sht.com.co
Líderes de Continuidad de cada Proceso	ERP Business Central 365	Holman Castillo		contador@sht.com.co
Líderes de Continuidad de cada Proceso	Nómina de novasoft	Leidy Poveda		jefetalentohumano@sht.com.co
Líderes de Continuidad de cada Proceso	Radoc / Integrateq	Ligia Sanabria		jefe.gestiondocumental@sht.com.co
Líder de Recuperación ante desastres TIC	Correo –e (G-Suite Google)	Maikol Chavez		maikol.chavez@sht.com.co
Líder de Recuperación ante desastres TIC	Enlace Cirion - Huéspedes	Jorge Rios		coordinador.ti@tequendamasuites.com
Líder de Recuperación ante desastres TIC	Enlace CWC Columbus – ST	Maikol Chavez		maikol.chavez@sht.com.co

Líder de Recuperación ante desastres TIC	Enlaces ETB - Teléfonos	Richard Gutierrez		analista.ti@tequendamasuites.com
Líder de Recuperación ante desastres TIC	Central Telefónica Hipath 4000	Maikol Chavez		maikol.chavez@sht.com.co
Líder de Recuperación ante desastres TIC	Líneas móviles Corp. Movistar	Maikol Chavez		maikol.chavez@sht.com.co
Líder de Recuperación ante desastres TIC	Celufijos Movistar	Maikol Chavez		maikol.chavez@sht.com.co
Líder de Recuperación ante desastres TIC	Firewall, Switches	Maikol Chavez		maikol.chavez@sht.com.co
Líder de Recuperación ante desastres TIC	Respaldos - Backups	Maikol Chavez		maikol.chavez@sht.com.co
Líder de Recuperación ante desastres TIC	UPS	Maikol Chavez		maikol.chavez@sht.com.co
Líder de Recuperación ante desastres TIC	Switches	Maikol Chavez		maikol.chavez@sht.com.co
Líder de Recuperación ante desastres TIC	AP	Maikol Chavez		maikol.chavez@sht.com.co
Líderes de Continuidad de cada Proceso	Cámaras	Diego Velasquez		coordinador.parqueadero@sht.com.co
Líderes de Continuidad de cada Proceso	HandPush EVO (turnos)	Leidy Poveda		jefetalentohumano@sht.com.co

- Actividades de notificación, evaluación y activación del DRP
 - Los usuarios deben reportar el incidente a la mesa de ayuda cuando:
 - NO se pueden utilizar los sistemas de información.
 - NO hay red de comunicaciones
 - NO hay servicio de correo electrónico

- NO hay acceso a los archivos electrónicos centralizados
- CUALQUIER otro evento de tecnología que afecte la prestación del servicio.
- El personal administrativo (Seguridad, Servicios Generales) deben reportar el incidente a la mesa de ayuda o Líder del centro de cómputo cuando:
 - SUENA la alarma del centro de cómputo
 - HAY inundación en cualquier piso
 - HAY un conato de incendio en el piso donde se encuentre ubicado el centro de cómputo
 - CUALQUIER otro evento que afecte o pueda afectar el centro de cómputo
- La mesa de ayuda debe atender el incidente, Dependiendo del caso como uno de los siguientes: Mantenimiento preventivo, correctivo y soporte técnico, y se continúa con la ejecución de esta guía si:
 - El incidente afecta la disponibilidad de los sistemas, a nivel general.
 - El incidente afecta la disponibilidad de la red de comunicaciones a nivel general.
 - Ningún usuario tiene acceso al correo electrónico.
 - Ningún usuario puede acceder a sus archivos electrónicos centralizados.
 - En cualquiera de los casos, debe escalarlo a los funcionarios responsables.
- El profesional especializado de la plataforma afectada debe realizar un diagnóstico sobre el incidente presentado, teniendo en cuenta:
 - Naturaleza e impacto del incidente.
 - Estrategias definidas en el DRP aplicables u otras soluciones potenciales
 - Tiempo estimado de solución del incidente.
 - Finalmente, comunicarse con el Director de TICs para informar los resultados del diagnóstico.
- El Director de TICs define si se activa o no el Centro de Cómputo Alterno, teniendo en cuenta los siguientes aspectos:
 - Si el evento afectó considerablemente el Centro de Cómputo Principal
 - Si la solución en sitio dura más de 24 horas.
- En caso de que se active, el líder de seguridad debe comunicar la activación al proveedor, teniendo en cuenta:
 - Fecha y hora a partir de la cual se da inicio a la activación.
- Funcionarios de la entidad que estarían en el proceso de activación, para que se tramiten los permisos de acceso correspondientes.
- El Líder de Infraestructura, coordina la ejecución de las actividades para recuperar la plataforma en el Centro de Cómputo Alterno, teniendo en cuenta:
 - Enrutamiento y activación de las comunicaciones hacia el Centro de Cómputo Alterno.

- Detención de la replicación de datos
- Verificación de la disponibilidad de información en el Centro de Cómputo Alterno
- Activación servicio de controladores de dominio y sistema operativo en servidores
- Activación servicio de bases de datos y aplicaciones.
- El Líder de infraestructura, verifica la disponibilidad de la plataforma desde el Centro de Cómputo Alterno, teniendo en cuenta:
 - Acceder a los sistemas de información
 - Realizar pruebas sobre los sistemas de información
- El Director de TICs, define si comunica o no el incidente a la Alta Dirección, caso en el cual se realizarían las actividades de manejo de crisis.
- El Líder responsable de la plataforma afectada, activa las estrategias de contingencia locales, teniendo en cuenta los siguientes aspectos:
 - Si es un evento que afectó las comunicaciones,
 - Configurar el Switchover de contingencia, en caso de falla en el switch Core.
 - Contactar al proveedor de comunicaciones, en caso de falla en router de conexión con intendencias, falla en router ubicado en cada intendencia, falla en enlaces con ISP, o falla en enlace con intendencias regionales.
 - Enrutar el tráfico por los demás switch que componen el stack, en caso de una falla de la fibra óptica de uno de ellos.
 - Utilizar el switch de piso como contingencia ante falla de un switch de piso en un centro de cableado.
 - Configurar el firewall de contingencia, en caso de falla del equipo principal.
 - Si es un evento que afectó la infraestructura de Bases de datos, almacenamiento y Respaldo
 - Recuperación de información y bases de datos desde los respaldos, en caso de corrupción de alguna base de datos y borrado o pérdida de datos.
- Qué hacer en caso de que la falla afecte a un equipo que no se encuentra en garantía, o contrato de mantenimiento?
 - El Líder responsable de la plataforma afectada solicita la contratación urgente de los servicios y equipos necesarios para solucionar el incidente.
 - El Director de Informática realiza la gestión para la contratación o compra de los servicios y/o equipos necesarios para solucionar el incidente.
 - El Líder responsable de la plataforma afectada coordina la solución con el proveedor contratado.
 - El Director de Informática comunica la solución del incidente a la entidad
 - El Director de Informática, en conjunto con los profesionales especializados, definen la estrategia de retorno a la normalidad, teniendo en cuenta:
 - Fecha del retorno a operación normal.

- Consideraciones especiales a aplicar en el proceso de retorno.
- Consideraciones especiales con respecto a la recuperación de la información y la integridad de los datos, cuando aplique.
- Sincronización entre los centros de cómputo, cuando se operó en el Centro Alterno de Cómputo, si aplica.
- El Líder Continuidad del Negocio, en conjunto con los funcionarios que participaron en la atención del incidente, documentan el incidente e identifican oportunidades de mejora para fortalecer el DRP.
- Se realiza el cierre del incidente, interrupción mayor o evento contingente, y se continúa con la ejecución del procedimiento de acciones preventivas y correctivas del SGSI.

7. Actividades de manejo de crisis

A Continuación, se listan las actividades y consideraciones necesarias para el manejo de una crisis que afecte o pueda afectar la reputación, imagen, u operación de la Sociedad Hotelera Tequendama

- El Director de Informática comunica a la Alta Dirección, teniendo en cuenta los siguientes aspectos:
 - Sistemas y servicios afectados
 - Resultados del diagnóstico
 - Acciones realizadas
 - Tiempo estimado para normalización
 - Riesgos a los que está expuesta la entidad por el desastre presentado, y las alternativas disponibles
 - Decisiones que debe tomar la alta dirección.
- La Alta Dirección (Equipo de Manejo de Crisis) evalúa la crisis y el impacto que puede tener para la reputación, imagen u operación de la entidad, al igual que define las acciones para afrontar la crisis.
- La Alta Dirección, a través de los voceros o funcionarios delegados, comunicará la crisis a nivel interno y externo, en caso de ser requerido, teniendo en cuenta los siguientes aspectos:
 - ¿Qué información concreta se tiene sobre la crisis (incidente presentado, diagnóstico, tiempo de solución)?
 - ¿Qué información está en proceso de verificación e investigación?
 - ¿Qué información válida se puede comunicar inmediatamente (mensaje)?
 - ¿Qué información se debe manejar al interior de la entidad?
 - ¿Quiénes fueron afectados por la crisis (audiencia)?
 - ¿Qué otras audiencias deberían saber sobre la crisis?
 - ¿Cómo se comunicará la información a los interesados o afectados (medio)?

- La comunicación de la crisis deberá considerar los siguientes principios:
 - Informar rápida y periódicamente: Ante una situación de crisis de alto impacto, la entidad debe establecerse como fuente primaria de información, asimismo, debe comunicar periódicamente la evolución de la atención de la crisis para evitar malos entendidos, especulaciones y rumores. Estos elementos le permitirán generar confianza y credibilidad con sus audiencias.
 - Decir la verdad: Ser honestos en los comunicados, sin embargo no significa transmitir TODA la información, sólo aquella que es suficiente para generar confianza y tranquilidad en la audiencia. Podrá existir información confidencial que deberá ser tratada como tal y no se necesite transmitir a los interesados.
 - Emitir reportes lo más exactos posibles: Publicar la información que se tiene disponible, siempre y cuando ésta haya sido validada. No especular, adivinar ni presentar situaciones hipotéticas.
- Las audiencias a considerar en la comunicación de la crisis son:
 - Sociedades inspeccionadas, vigiladas y/o controladas
 - Usuarios externos de los productos y/o servicios de la entidad.
 - Funcionarios
 - Opinión Pública
 - Gobierno y Autoridades
 - Líderes de Opinión
 - Contratistas y Proveedores
- La Alta Dirección, oc los funcionarios designados por esta, deberán realizar monitoreo permanente de la crisis y tomar las decisiones que correspondan para continuar con la mitigación del mismo. Se debe tener en cuenta:
 - ¿Qué información circula en los medios de comunicación?
 - ¿Qué información circula a nivel interno?
 - ¿Qué impacto sobre la crisis tiene la información que está circulando en los medios?
 - ¿Se requerirá realizar nuevos comunicados?

8. Actividades de mantenimiento

Es responsabilidad del Lider Continuidad del Negocio la actualización de las nuevas versiones al DRP, y la comunicación de las mismas a todos los funcionarios involucrados en el mismo.

La actualización y mantenimiento al DRP se debe realizar:

- Cuando ha transcurrido un año desde la última actualización.
- Cuando han ocurrido cambios en la plataforma tecnológica objeto del alcance de esta guía.
- Cuando los resultados de las pruebas requieren actualización del DRP o sus procedimientos.
- Cuando hay cambios en el personal que operaría el DRP.

- Cuando los resultados de auditorías así lo indican.

Algunas actividades a realizar para mantener vigente el DRP, son:

No	Actividad	Responsable	Frecuencia
1.	Actualización de los procedimientos de recuperación y contingencia de la plataforma tecnológica	Líderes de los procesos	Cada vez que se realice un cambio a la infraestructura de producción o se realice una prueba de contingencia
2.	Sincronización de la configuración de la infraestructura respaldada en el Centro de Cómputo Alterno (Incluyendo replicación de data)	Líder de Infraestructura Líder de redes y comunicaciones	Permanente
3.	Monitoreo de la infraestructura respaldada en el Centro de Cómputo Alterno, para verificar su disponibilidad en caso de que se presente un evento	Líder de Infraestructura	Permanente
4.	Ejecución de pruebas periódicas para verificar el correcto funcionamiento de los sistemas respaldados	Profesionales Especializados	Cada trimestre
5.	Ejecución del procedimiento de respaldo de datos de la infraestructura tecnológica	Líder de Infraestructura	Permanente
6.	Obtener imagen del sistema de servidores y equipos de red.	Líder de Infraestructura Líder de redes y comunicaciones	Semestral o cada vez que se realice un cambio a la infraestructura de producción o se realice una prueba de contingencia

9. Distribución de la guía: Plan de recuperación ante desastres:

Este documento guía deberá ser entregado bajo las siguientes consideraciones:

Se debe entregar una copia final COMPLETA del DRP al jefe de Planeación, Jefe de Tecnología, coordinador de tecnología

diferentes copias del documento guía deben ser controladas, y cada que se cambie de versión, se deberá recoger las versiones anteriores.

10. Recursos mínimos requeridos:

La infraestructura necesaria para soportar los procesos misionales de la entidad que serán recuperados en una contingencia son:

Cant.	Servidor Servicios y Software	Marca	Modelo	RAM	Almacenamiento
1	NOMINA NOVASOFT	NUBE			
1	ERP BC365	NUBE			
1	PMS / POS ZEUS	NUBE			
1	Integrateq	NUBE			

11. Condiciones generales

- El DRP está enfocado a la protección de la plataforma tecnológica que soporta los procesos misionales y de apoyo críticos de la Sociedad Tequendama: a) Suites, b) Operación logística, c) Parqueadero, d) Inmobiliaria, e) Catering, f) área administrativa y financiera, g) Talento humano
- Supuestos: La efectividad en la ejecución de este documento guía, ante la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente que afecte la plataforma tecnológica, se fundamenta en los siguientes supuestos:
 - Se dispone de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación para los sistemas críticos.
 - Los funcionarios que ejecutan esta guía, o sus suplentes, se encuentran disponibles y no han sido afectados por el desastre.
 - El desastre no afectó simultáneamente el Centro de cómputo principal y el Centro de Cómputo Alterno
 - El Centro de Cómputo Alterno estará habilitado para un promedio de 100 usuarios concurrentes.
 - Solo el funcionario responsable activará el DRP.
 - Se han realizado las pruebas de las estrategias y procedimientos al menos 1 vez al año, y han funcionado. Los funcionarios han participado en las pruebas y capacitaciones realizadas.
 - La realización de respaldos de las bases de datos e información se realiza de acuerdo a los procedimientos y frecuencias establecidas.

Nota: Los aspectos que se encontrarán en esta guía, en negrita y cursiva dependen de adquisición y funcionalidad de las estrategias de continuidad con la infraestructura contingente correspondiente.

12. Escenarios de desastre

Los escenarios de desastre, interrupción mayor o un evento contingente que contemplan esta guía son:

- **Centro de Cómputo / Data Center:**
 - No disponibilidad del Data Center por:
 - Atentado
 - Incendio
 - Inundación
 - Daño en el sistema de A/A
 - Daño en el suministro Eléctrico
- **Infraestructura de Comunicaciones**

No disponibilidad de los servicios de comunicaciones por fallas en:

 - switch core - tv
 - fibras opticas de conexión con centros de cableado
 - router core - tv
 - router de buenaventura
 - switch de piso - suites
 - enlaces de comunicación con isp
 - enlaces de comunicación con buenaventura
 - switch de una regional buenaventura
 - switch del firewall
 - firewall hw red administrativa
 - firewall sw red huéspedes
- **Infraestructura de Servidores:**

No disponibilidad de la infraestructura por fallas en:

 - servidor opera
 - servidor novasoft contabilidad
 - servidor central telefónica (virtualizado)
 - contact center, tarificador, grabador, adviser
 - servidor orfeo (nube)
 - servidor pfsense

- servidor cámaras (seguridad)
- g-suite (nube google)
- helpdesk (nube proveedor)
- servidor sistema parqueadero
- corrupción de la base de datos
- borrado o pérdida de datos
- falla total o parcial de la san
- falla total o parcial de la san en ag-log
- falla en switch conexión a la san
- falla total o parcial del servidor de respaldo

– **Aplicaciones**

- Clasifica las aplicaciones para la recuperación ante desastres,

– **Servicio de Internet**

El servicio puede verse afectado por:

- Incidente interno en las instalaciones de la empresa
- Incidente externo fuera de las instalaciones de la empresa

La solución puede ser directa por el proveedor ISP o requerir de un tercero como por ejemplo proveedor de servicio publico

– **Ciberataque**

- El ciberataque tiene diferentes impactos, la recuperación de datos puede darse en cualquier ubicación, en el entorno de producción original, un sitio de recuperación ante desastres aislado o ambos.
- Los planes de recuperación ante desastres generalmente se basan en la copia de datos más reciente. Con la recuperación de datos, debe buscar los datos «limpios» disponibles para el proceso de recuperación, ya que los más recientes pueden verse comprometidos.
- Construir el catálogo de activos de datos vitales, la arquitectura y procedimientos de recuperación implementados para protegerlos y realizar pruebas con frecuencia para poder actuar rápidamente después de un ciberataque para evaluar la situación y evitar pérdida de datos, es fundamental en la recuperación de datos realizar pruebas periódicas que permitan cumplir los objetivos de tiempo de recuperación (RTO) y los objetivos de punto de recuperación (RPO). En la recuperación de datos, se debe cuantificar RTO y RPO en función de la situación.

13. Roles y Responsabilidades

- Líder Continuidad de Negocios

Antes del evento	Durante el Evento	Después del evento
------------------	-------------------	--------------------

<ul style="list-style-type: none"> - Velar por la actualización del DRP y recursos requeridos. - Velar por la actualización, distribución y pruebas del DRP - Gestionar la consecución de los recursos para el DRP. - Comunicar a las personas que corresponda sobre la situación de contingencia. 	<ul style="list-style-type: none"> - Evaluar y activar el DRP y las estrategias de recuperación y contingencia. - Comunicar a Gerencia General sobre el estado de la operación de Contingencia. - Informar el momento en que opera en contingencia y que puede suceder con la prestación del Servicio - Liderar la operación bajo contingencia. - Comunicar a la dirección el desastre, interrupción o evento contingente. - Liderar el retorno a la normalidad. 	<ul style="list-style-type: none"> - Velar por la actualización del DRP acorde con los inconvenientes y oportunidades de mejora visualizados durante el evento de interrupción. - Informar a Gerencia General sobre el retorno a la normalidad y agradecer la comprensión y apoyo de todos en esta situación.
--	--	---

– Líder de Recuperación ante desastres TIC – Infraestructura, Comunicaciones y Mesa de ayuda

Antes del evento	Durante el Evento	Después del evento
<ul style="list-style-type: none"> - Comunicar necesidades de ajuste - Participar en la ejecución de las pruebas al DRP 	<ul style="list-style-type: none"> - Evaluar el desastre, interrupción o evento contingente. - En caso de no contar con un contrato de mantenimiento vigente se debe tener un listado de posibles proveedores de acciones correctivas de solución. - Comunicar el evento al Lider Continuidad del Negocio - Verificar disponibilidad y notificar al personal requerido para atender el evento. - Ejecutar las guías de contingencia y recuperación. - Comunicar a los proveedores la activación del DRP. - Solicitar la corrección del componente afectado y realizar seguimiento de la solución. - Estar atentos para dar una correcta información a las personas que lo requieran. - Mantener informado al Lider Continuidad del Negocio 	<ul style="list-style-type: none"> - Reportar los inconvenientes y oportunidades de mejora del DRP

– Líder de Recuperación ante **desastres** TIC - Seguridad

Antes del evento	Durante el Evento	Después del evento
<ul style="list-style-type: none"> - Coordinar actividades de entrenamiento, documentación y actualización del DRP. - Coordinar las actividades de pruebas del DRP. - Identificar los recursos requeridos para la operación del DRP. 	<ul style="list-style-type: none"> - Proveer soporte a los profesionales especializados. - Notificar al proveedor de Centro de Cómputo Alterno (si aplica). - Gestionar el alistamiento y disponibilidad del Centro de Cómputo Alterno. - Coordinar con los responsables el desplazamiento al Centro de Cómputo Alterno, de los funcionarios que activarán la infraestructura. (Si aplica) - Mantener informado al Lider Continuidad del Negocio 	<ul style="list-style-type: none"> - Actualizar el DRP, de acuerdo con los inconvenientes y oportunidades de mejora encontrados.

– Líderes de Continuidad de cada Proceso

Antes del evento	Durante el Evento	Después del evento
<ul style="list-style-type: none"> - Participar en la ejecución de las pruebas al DRP 	<ul style="list-style-type: none"> - Apoyar a los involucrados en el DRP, en actividades administrativas y logísticas ante una contingencia, entre otras. - Suministro de información de contrato - Logística de desplazamiento, si es requerido - Contacto de proveedores, si es requerido 	<ul style="list-style-type: none"> - Reportar los inconvenientes y oportunidades de mejora del DRP

14. Actividades de Recuperación y contingencia

El principal desafío en el plan de recuperación ante desastres son los cambios en el entorno de producción, flujos de trabajo, interdependencias de aplicaciones, para lo cual se tendrá actualizado los diferentes dominios de la arquitectura tecnológica. Existen otros factores que se complementaran en una siguientes versión relacionados con la preparación de diferentes escenarios no planificados, como la falta de disponibilidad de parte de personal o problemas con los aliados estratégicos o externos (por ejemplo, conseguir un equipo crítico, servicio público).

A continuación, se definen las guías o pasos a seguir para recuperar los componentes de la plataforma tecnológica:

– **En caso de falla de un servidor (Virtualizado en la nube del proveedor)**

- Conectarse a la nube del proveedor donde se encuentran los servidores virtualizados.
- Habilitar el(los) servidor(es) clones de los afectados.
- Cargar la última imagen del servidor afectado
- Restaurar la última copia full del servidor afectado

- Restaurar la última copia diferencial del servidor afectado
 - Restaurar la última copia incremental del servidor afectado
 - Habilitar las estaciones de trabajo
 - Comunicar a todos los integrantes de equipo de Continuidad que se deben usar los vínculos de contingencia para acceder al sistema afectado.
 - En caso de que las estaciones de trabajo también hayan sido afectadas se deben enviar las URLs por correo electrónico para que una vez los usuarios tengan estaciones de trabajo puedan acceder.
 - Solicitar que los usuarios hagan pruebas de registro, consulta, impresión; para confirmar que todo está operativo.
- **En caso de falla de un servidor local**
- Adquirir uno de similares características
 - Asegurarse que traiga el mismo sistema operativo que el servidor que falló.
 - Instalar actualizaciones
 - Montar última imagen realizada al servidor.
 - Restaurar la última copia full del servidor afectado
 - Restaurar la última copia diferencial del servidor afectado
 - Restaurar la última copia incremental del servidor afectado
 - Solicitar que los usuarios hagan pruebas de registro, consulta, impresión; para confirmar que todo está operativo
- **En caso de falla de los aplicativos**
- En términos generales, los aplicativos en la nube que no requieren la presencialidad del integrante en las instalaciones de la Sociedad podrán trabajar remotamente
 - Los proveedores de servicio de plataforma en la nube deberán aplicar sus políticas de backup y recuperar el sitio.
 - El proveedor de la plataforma debe proveer un enlace alternativo para la continuidad de la operación
 - ...
- **En caso de falla del servicio de Internet**
- En caso de falla del proveedor principal de la red administrativa entrara la contingencia del segundo proveedor
 - En caso de falla del primero y segundo proveedor de ISP se utilizaran las simcard en los puntos críticos del proceso
 - En términos generales, los aplicativos en la nube que no requieren la presencialidad del integrante en las instalaciones de la Sociedad podrán trabajar remotamente.
- **En caso de falla por Ciberataques**
- En construcción

15. Pruebas de recuperación ante desastres.

Para la verificación y mejora del plan de recuperación a continuación se describen las pruebas a ejecutar para su comprobación.

Comúnmente se presenta que el plan de recuperación puede fallar o no ejecutarse conforme al mismo dado los múltiples cambios en la empresa que no fueron identificados a tiempo o pasaron desapercibidos, como por ejemplo: no tener idea a quién llamar, la persona ya no trabaja para la empresa. Estos ejemplos son solo algunos de los problemas que pueden surgir ante un desastre no permitiendo cumplir oportunamente con la recuperación.

Para minimizar estos impactos es necesario probar el plan para saber con que tipo de problemas nos podemos encontrar ante un desastre real. El objetivo es descubrir problemas y realizar modificaciones oportunamente para evitar o minimizar los obstáculos en el momento de la recuperación.

El éxito de la recuperación, es saber qué tan cerca están las pruebas de un desastre real teniendo en cuenta que los eventos no tienen horario. Para que una prueba de recuperación sea exitosa se requiere probar los elementos programáticos para garantizar que el esfuerzo de recuperación es oportuno desde el mismo momento de la declaración del incidente.

Siempre existirá una brecha entre las condiciones reales del desastre y las pruebas mismas dado que las pruebas son controladas y predecibles, y el desastre es impredecible. La ejecución de las pruebas se puede realizar en escenarios aislados e involucrar a miembros seleccionados.

¿Qué tanto difieren las pruebas de las condiciones reales de un desastre? Entre mayor la diferencia de la prueba con las condiciones reales del desastre menor es la preparación para atender la misma.

Se debe tener en cuenta que las pruebas deben actualizarse cada vez que ingresan nuevas aplicaciones, se eliminan redundancias y migrar cargas de trabajo desde y hacia la nube; esto obviamente requiere que previamente se actualice el alcance del DRP teniendo en cuenta las interdependencias (cada aplicación que ingrese o se retire influye en otras aplicaciones).

De otra parte, es necesario identificar el tipo de desastre dado que si este es corresponde a un ciberataque la reacción es diferente.

Pruebas.

- Realizar pruebas simuladas para que los integrantes de la Sociedad dejen sus actividades rutinarias y recuerden el protocolo de comunicación, los roles, el personal de apoyo y actividades a ejecutar de acuerdo con el proceso crítico en riesgo.
- Definir un alcance completo de la prueba que cubra toda la organización, así se ejecute por partes.
- Registrar el resultado de las variables RTO y RPO para analizar los resultados de la prueba mostrando la tendencia y mejora de los mismos

Consideraciones a tener en cuenta para la realización de las pruebas


- Las pruebas se deben ejecutar en los tiempos programados, es decir, procurar que no se reprogramen a menos que sea por cambios o actualizaciones de TI cuando llegue el momento de realizar las pruebas. La continuidad permite mejorar la respuesta ante el desastre.
- Ajustar la configuración remota para estar preparado
- Analizar los casos donde se requiere interactuar con entidades bancarias o similares que requieren del envío de información para contar con documentos actualizados o la forma de construirlos. Sí, estamos en medio de una prueba y se requiere un archivo no previsto, no se puede volver a producción y sacarlo, dado que no podría hacer eso en un desastre real.
- Ejecutar en varios escenarios los datos que pueden verse comprometidos basado en los activos de datos vitales.

Frecuencia de ejecución de las pruebas

Esta frecuencia depende de la identificación de cuánto tiempo de inactividad puede permitirse que la Sociedad y si está realizando cambios importantes en su entorno, y los requisitos de recuperación influyen en la ejecución de las misma, es decir, que la frecuencia esta dada por el RTO, entre más corto más frecuentes serán las pruebas. Las pruebas se deben aplicar conforme la siguiente tabla:

- Recuperación de una semana = una prueba por año
- Recuperación de 48 horas = dos pruebas por año
- Recuperación de 24 horas = una prueba por trimestre

De otra parte, se debe considerar realizar pruebas adicionales después de realizar cambios importantes en el entorno o en los requisitos de recuperación internos o externos. Con el fin de agregar una prueba antes para asegurarse de que esos cambios se reflejen en el plan de recuperación ante desastres. De esa manera, si experimenta una interrupción asegura que los cambios que se realizaron no afectan el plan de recuperación.

ELABORO	APROBÓ
Maikol Chavez Coordinador Tecnología de la información y comunicaciones	Christian Henrique González Secretario General
Firma: 	Firma: 