DOCUMENTO BCP DE LA GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA

PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA

Versión: 1 del 29 de agosto de 2025

Contenido

1. Objetivo

Establecer los principios, la estructura y los requisitos para la planificación, implementación, mantenimiento y mejora de la continuidad del negocio y la recuperación ante desastres en la entidad y asegurar la disponibilidad de las actividades críticas y minimizar el impacto de cualquier interrupción en las operaciones, alineándose con los objetivos de recuperación (RTO y RPO) definidos en el proceso Gestión de Sistemas de Información y Tecnología.

Objetivos de Continuidad del Negocio

Tiempo Objetivo de Recuperación (RTO): Restaurar la funcionalidad mínima viable de los servicios críticos en un plazo máximo de 2 horas tras una interrupción4.

Punto de Recuperación Objetivo (RPO): Asegurar que la pérdida máxima de datos aceptable no exceda las 4 horas. Esto implica la realización de respaldos periódicos con una frecuencia que garantice este objetivo.

Resiliencia: Integrar la continuidad del negocio como un pilar en la planificación estratégica, de forma que sea un componente integral y no una acción reactiva.

2. Roles y Responsabilidades

Alta Dirección: Es responsable de aprobar la política y asignar los recursos necesarios para la implementación y el mantenimiento del plan de continuidad del negocio.

Comité de Continuidad del Negocio: Un equipo multidisciplinario responsable de la supervisión de la implementación, las pruebas y la actualización del plan de continuidad.

Líderes de Procesos Críticos: Son responsables de conocer y aplicar los procedimientos de continuidad y recuperación para sus respectivas áreas.

Personal en General: Todo el personal debe ser capacitado de forma regular en los procedimientos de emergencia y el uso de las herramientas de recuperación. La concienciación del usuario reduce significativamente la probabilidad de errores humanos que puedan causar interrupciones.

3. Definiciones

Activo de Información: Es el activo que contiene o está relacionado con la información y tiene valor para la entidad: personas, sistemas, edificios, etc..

Análisis de Impacto: Marco conceptual sobre el cual las entidades deben planear integralmente los alcances y objetivos, que permiten proteger la información, en todas sus áreas críticas.

Continuidad de Negocio: Propiedad Entrega de productos y servicios de manera óptima después de ocurrido un evento.

DRP: Cualquier información vinculada Información documentada que define los procedimientos, metodologías, funciones y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de perturbación. Sigla en Inglés, Disaster Recovery Plan (Plan de Recuperación ante Desastres).

Interrupción: Incidente anticipado o no, que afecte el normal curso de las operaciones de la entidad, ejemplo: ataques a la infraestructura o al sistema, fallas de potencia, huracanes, etc.

Plan de Continuidad de negocio: Procedimientos que orientan a la entidad para declarar, recuperar, restablecer y reintegrar la operación de forma óptima tras la interrupción.

Plan de Contingencia: Define los procedimientos y las rutas que se deben tomar para que la Entidad puedan continuar funcionando en caso de un evento de desastre.

Plataforma tecnológica crítica: Sistemas de Información vitales para apoyar los servicios y procesos: bases de datos, equipos, enlaces, servidores, etc....

RAS: Texto que plantea las diversas alternativas y soluciones viables para recuperar y reintegrar el sistema de tecnología ante un evento adverso. Sigla en inglés, Response Alternative and Solutions. (Soluciones y Alternativas de Respuesta)

RTO: Tiempo de recuperación para un proceso, servicio, sistema o plataforma tecnológica, después de ocurrido un evento de emergencia. Sigla en Inglés, Recovery time Objetive. (Objetivo de Tiempo de Recuperación)

RPO: Masa de Información que puede perder un proceso o servicio por un evento de crisis. Sigla en Inglés, Recovery Points Objetive. (Objetivo de Punto de Recuperación).

4. Normatividad de Operación

Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y, se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y, se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1955 de 2019. Por la cual se expide el Plan Nacional de Desarrollo, 2018-2022.

Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales, para la protección de datos personales.

Ley 1712 de 2014. Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario, del Sector de Tecnologías de la Información y las Comunicaciones.

Resolución Distrital 305 de 2008. Por la cual se expiden políticas públicas, para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones, respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

Resolución 004 de 2017. Por la cual se modifica la Resolución 305 de 2008 de la CDS.

Resolución 50 de 2021 MINTIC. Por la cual se establecen los lineamientos y estándares, para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitados de la política de gobierno digital.

RESOLUCIÓN 02277 DE 2025 Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

Documento CONPES 3701 de 2011 - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.

Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital.

Documento CONPES 3995 de 2020 - Política Nacional De Confianza y Seguridad Digital

NTC/ISO 27001:2013. Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

NTC/ISO 22301:2019 Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos

ISO 27031 – DE198-13 Tecnología de la Información, Técnica de Seguridad, Directrices para la continuidad del negocio.

5. Contenido

5.1. Principios Clave

Enfoque Proactivo: La continuidad del negocio se abordará desde una perspectiva proactiva, priorizando la alta disponibilidad, la redundancia de sistemas y la prevención de incidentes, en lugar de una respuesta únicamente reactiva.

Gestión de Riesgos: El Plan de tratamiento de riesgos de seguridad de la información será el documento base para el seguimiento continuo de los riesgos. Se utilizarán herramientas automatizadas de monitoreo que alerten sobre riesgos potenciales en tiempo real para una respuesta proactiva.

Integración con la Arquitectura: Los nuevos proyectos de TI críticos deben incluir desde su concepción un análisis de impacto y un plan de continuidad, garantizando que sus componentes sean recuperables y resilientes a interrupciones.

Pruebas y Mantenimiento: El plan de contingencia será un documento vivo que se revisará y actualizará constantemente. Se realizarán pruebas periódicas, como simulacros de interrupción y pruebas de conmutación por error, para validar su efectividad y asegurar que se cumplan los RTO y RPO.

Medidas y Requisitos de Implementación La entidad deberá:

Desarrollar y mantener un Plan de contingencia con un enfoque de alta disponibilidad que incluya procedimientos detallados para la recuperación de todos los sistemas y servicios críticos.

Implementar una arquitectura redundante con sistemas de hardware y software en espera (activos-activos o activos-pasivos) para garantizar una conmutación por error (failover) rápida.

Establecer un sistema de gestión de identidades y accesos (IAM) con alta disponibilidad para que los perfiles de usuario y sus permisos puedan ser restaurados rápidamente.

Actualizar el Manual de Políticas de Seguridad y Privacidad de la Información para incluir procedimientos claros sobre la gestión de incidentes, copias de seguridad y comunicación durante una crisis.

Cumplimiento y Revisión

El incumplimiento de esta política puede resultar en acciones disciplinarias. La política será revisada anualmente o ante cambios significativos en la entidad o su entorno.

6. Análisis de impacto del negocio

Proceso: Sistemas de Tecnología de la Información

	Impactos					Tiempos		
	Financiero	Reputacional	Legal y Regulatorio	Impacto en Usuarios / Ciudadanía		MTPD	RTO	RPO
Planeación de T.I. y Seguridad de la Información								
Evaluar tecnologías emergentes y decidir cuáles se adoptarán	Significativo	Moderado	Menor		Moderado	Entre 36 y 72 horas	Entre 16 y 32 horas	Entre 36 y 48 horas

	Impactos					Tiempos		
	Financiero	**Reputacional**	**Legal y Regulatorio**	**Impacto en Usuarios / Ciudadanía**		**MTPD**	**RTO**	**RPO**
Identificar las necesidades y requerimientos de los procesos de la entidad	Crítico	Significativo	Menor		Significativo	Entre 24 y 36 horas	Entre 8 y 16 horas	Entre 24 y 36 horas
Generar el plan estratégico de T.I. (PETI)	Crítico	Crítico	Significativo		Significativo	Entre 6 y 12 horas	Entre 2 y 4 horas	Entre 4 y 12 horas
Definir y consolidar planes, proyectos y programas de T.I.	Crítico	Crítico	Significativo		Moderado	Entre 6 y 12 horas	Entre 2 y 4 horas	Entre 4 y 12 horas
Definir y actualizar el Manual de Políticas de Seguridad y Privacidad de la Información	Significativo	Crítico	Significativo		Menor	Entre 6 y 12 horas	Entre 2 y 4 horas	Entre 4 y 12 horas
Realizar seguimiento a los riesgos de seguridad de la información/digital	Significativo	Crítico	Significativo		Significativo	Entre 1 y 6 horas	Entre 0 y 2 horas	Entre 0 y 4 horas
Gestión de la Información								
Definir la información que se va a generar a partir de las necesidades de los clientes internos y externos.	Moderado	Menor	Menor		Menor	Entre 12 y 24 horas	Entre 4 y 8 horas	Entre 12 y 24 horas
Gestionar las herramientas para la obtención y validación de la información.	Moderado	Significativo	Moderado		Significativo	Entre 6 y 12 horas	Entre 2 y 4 horas	Entre 4 y 12 horas
Establecer perfiles para el ingreso, modificación y consulta de la información.	Crítico	Crítico	Crítico		Crítico	Entre 1 y 6 horas	Entre 0 y 2 horas	Entre 0 y 4 horas
Auditar los mecanismos y controles de acceso a la información.	Significativo	Moderado	Menor		Menor	Entre 6 y 12 horas	Entre 2 y 4 horas	Entre 4 y 12 horas
Definir y actualizar los controles para la prevención o mitigación de riesgos asociados a los activos de información.	Significativo	Crítico	Significativo		Significativo	Entre 6 y 12 horas	Entre 2 y 4 horas	Entre 4 y 12 horas
Desarrollo y Mantenimiento de los Sistemas de Información								
Establecer acuerdos para el desarrollo de soluciones con los líderes de procesos.	Significativo	Menor	Menor		Insignificante	Entre 12 y 24 horas	Entre 4 y 8 horas	Entre 12 y 24 horas
Elaborar y ejecutar planes para el desarrollo de nuevos sistemas de información o mejoras a los existentes.	Significativo	Significativo	Significativo		Menor	Entre 12 y 24 horas	Entre 4 y 8 horas	Entre 12 y 24 horas

	Impactos					Tiempos		
	Financiero	Reputacional	Legal y Regulatorio		Impacto en Usuarios / Ciudadanía	MTPD	RTO	RPO
Garantizar la calidad del software a través de pruebas.	Significativo	Crítico	Significativo		Significativo	Entre 1 y 6 horas	Entre 0 y 2 horas	Entre 0 y 4 horas
Producir la documentación y manuales.	Menor	Significativo	Significativo		Insignificante	Entre 12 y 24 horas	Entre 4 y 8 horas	Entre 12 y 24 horas
Capacitar a los usuarios.	Significativo	Crítico	Significativo		Significativo	Entre 12 y 24 horas	Entre 4 y 8 horas	Entre 12 y 24 horas
Realizar soporte y acompañamiento a los usuarios finales.	Moderado	Significativo	Significativo		Moderado	Entre 12 y 24 horas	Entre 4 y 8 horas	Entre 12 y 24 horas
Gestionar los servicios de TI								
Desarrollar el Plan de contingencia con enfoque de alta disponibilidad.	Crítico	Crítico	Significativo		Significativo	Entre 1 y 6 horas	Entre 0 y 2 horas	Entre 0 y 4 horas
Administrar la capacidad del servicio	Moderado	Significativo	Moderado		Moderado	Entre 12 y 24 horas	Entre 4 y 8 horas	Entre 12 y 24 horas
Poner en producción los servicios	Significativo	Significativo	Significativo		Significativo	Entre 6 y 12 horas	Entre 2 y 4 horas	Entre 4 y 12 horas
Administrar la infraestructura de hardware, software base, redes y telecomunicaciones	Crítico	Crítico	Significativo		Crítico	Entre 1 y 6 horas	Entre 0 y 2 horas	Entre 0 y 4 horas
Realizar seguimiento a los logs de auditoría de los sistemas de información de la entidad.	Moderado	Moderado	Moderado		Moderado	Entre 12 y 24 horas	Entre 4 y 8 horas	Entre 12 y 24 horas

6.1. Objetivos de Recuperación para Actividades Críticas

Basado en el análisis de impacto del negocio, todas las actividades críticas deben adherirse a los siguientes objetivos para minimizar el daño:

RTO (Tiempo Objetivo de Recuperación): Entre 0 y 2 horas. Esto significa que, tras una interrupción, el servicio debe ser restaurado a su funcionalidad mínima viable en un máximo de dos horas.

RPO (Punto de Recuperación Objetivo): Entre 0 y 4 horas. Esto indica que la pérdida máxima de datos aceptable es de cuatro horas. Se deben realizar respaldos periódicos con una frecuencia mínima que garantice este objetivo.

6.2. Impacto

Impacto Financiero	El impacto financiero se refiere a las pérdidas económicas directas e indirectas que la entidad podría sufrir debido a una interrupción.
Impacto Reputacional	El impacto reputacional se relaciona con la pérdida de confianza pública, credibilidad y la imagen de la entidad.
Impacto Legal y Regulatorio	Este criterio mide el riesgo de incumplimiento de leyes, regulaciones, contratos y políticas.
Impacto en Usuarios (ciudadanía)	Este criterio evalúa cómo una interrupción afecta la capacidad de la entidad para prestar servicios a la ciudadanía.

Clasificación	**Categoría**	**Impacto**			
		Financiero	**Reputacional**	**Legal y Regulatorio**	**Impacto en Usuarios / Ciudadanía**
1	Insignificante	Costos de recuperación menores que no afectan el presupuesto operativo. No hay pérdidas de ingresos significativas	No hay afectación a la imagen de la entidad.	No hay incumplimientos de requisitos legales o contractuales	Retrasos mínimos en la prestación de servicios que son manejables y no generan quejas.
2	Menor	Costos que pueden ser absorbidos por el presupuesto sin requerir fondos adicionales. Pequeñas pérdidas de ingresos, fácilmente recuperables.	Insatisfacción de un grupo reducido de usuarios o ciudadanos. Algunos comentarios negativos en redes sociales o medios locales.	Incumplimiento de políticas internas o acuerdos de servicio no críticos. No hay sanciones legales o multas.	Algunos usuarios experimentan inconvenientes, pero se les puede dar solución en un corto período. Pequeño aumento en el número de quejas.
3	Moderado	Costos que afectan el presupuesto y pueden requerir una reasignación de fondos. Pérdida de ingresos que impacta la ejecución de proyectos a corto plazo.	Cobertura mediática negativa a nivel distrital. Afectación a la confianza de los grupos de interés y socios estratégicos.	Posible incumplimiento de regulaciones distritales o nacionales. Posibilidad de multas o sanciones menores.	Interrupción de un servicio no esencial para un grupo considerable de usuarios. Aumento significativo de quejas y reclamos, quejas que llegan a los medios.
4	Significativo	Costos que exceden el presupuesto disponible y requieren una solicitud de fondos de emergencia. Pérdidas de ingresos considerables que ponen en riesgo la continuidad de programas clave.	Gran cobertura mediática negativa a nivel nacional. La credibilidad del IDPC y sus directivos se ve seriamente comprometida, afectando la relación con el sector cultural y patrimonial.	Incumplimiento grave de leyes o regulaciones nacionales (p. ej., Ley de Archivo, Ley de Transparencia), generando multas, sanciones y procesos legales contra la entidad.	Interrupción total de un servicio esencial (p. ej., acceso a información patrimonial, servicios de asesoría). Se ven afectados un gran número de usuarios, generando un impacto negativo en la preservación y divulgación del patrimonio.

5	Crítico	Pérdidas financieras masivas que comprometen la sostenibilidad de la entidad a largo plazo. Requiere una intervención económica de alto nivel y puede llevar a la interrupción total de proyectos misionales.	Gran escándalo público que resulta en una crisis de confianza generalizada. Cuestionamiento de la capacidad de la entidad para cumplir con su misión, lo que puede llevar a sanciones o cambios en la dirección.	Incumplimiento que resulta en la pérdida de facultades legales para operar, o en demandas masivas y la intervención de organismos de control como la Procuraduría o la Contraloría.	Interrupción prolongada de servicios clave que afecta la misión de la entidad y la relación con la ciudadanía. Podría llevar a la pérdida irreversible de información o la incapacidad para proteger elementos patrimoniales.

MDPT	El Tiempo Máximo Tolerable de Interrupción (MTD o MAO) es la duración máxima que un proceso de negocio puede estar interrumpido sin causar un daño intolerable a la organización.
RTO	El Tiempo Objetivo de Recuperación (RTO) es el período máximo que un sistema, aplicación o proceso puede permanecer inactivo después de una interrupción antes de que cause un daño significativo al negocio.
RPO	El Punto de Recuperación Objetivo (RPO) se refiere a la cantidad máxima de datos que una empresa puede perder antes de que se causen daños significativos.

Nivel de Criticidad	**MDPT**	**RTO**	**RPO**	**Ejemplos de Procesos/Sistemas IDPC**
Crítico	Entre 1 y 6 horas	Entre 0 y 2 horas	Entre 0 y 4 horas	SISBIC (datos históricos y de gestión de patrimonio), Plataforma de Trámites Ciudadanos, Correo Electrónico Institucional (radicación de correspondencia oficial).
Prioridad Alta	Entre 6 y 12 horas	Entre 2 y 4 horas	Entre 4 y 12 horas	Sistemas de Gestión Documental (acceso a documentos recientes), Sistemas Financieros (contabilidad, pagos).
Prioridad Media	Entre 12 y 24 horas	Entre 4 y 8 horas	Entre 12 y 24 horas	Sistemas de Gestión de Recursos Humanos, Plataformas de Divulgación Cultural (sitio web principal, redes sociales).
Prioridad Baja	Entre 24 y 36 horas	Entre 8 y 16 horas	Entre 24 y 36 horas	Sistemas de Gestión de Proyectos internos no críticos, Aplicaciones de soporte administrativo.
Insignificante	Entre 36 y 72 horas	Entre 16 y 32 horas	Entre 36 y 48 horas	Sistemas de información para actividades de apoyo con bajo impacto en la misión, sistemas de archivo histórico de baja consulta.

7. Estrategias de Continuidad del Negocio por Actividad

A continuación, se detallan las estrategias de continuidad para cada una de las actividades críticas identificadas, enfocadas en cumplir con el RTO y RPO establecidos:

7.1. Identificar las necesidades y requerimientos de los procesos de la entidad

Estrategia: La recolección de requisitos es un proceso clave. Se debe contar con una plataforma centralizada y redundante para el almacenamiento de la información, accesible incluso en caso de fallas del sistema principal. Es de mucha criticidad mantener respaldos de la base de datos de requisitos en un sitio de recuperación para evitar la pérdida de información crítica y poder restaurarla en un tiempo mínimo, en concordancia con el RPO.

7.2. Generar el plan estratégico de T.I. (PETI)

Estrategia: El Plan Estratégico PETI 2025-2027 debe incluir como uno de sus pilares la gestión de la continuidad del negocio y la recuperación ante desastres (Plan de contingencia con enfoque de alta disponibilidad). Esto asegura que la continuidad del negocio no sea una acción reactiva, sino una parte integral de la planificación estratégica.

7.3. Definir y consolidar planes, proyectos y programas de T.I.

Estrategia: La Guía Gestión de proyectos TI V1 (intranet IDCP) es el documento base. Cada nuevo proyecto de TI crítico debe incluir desde su concepción un análisis de impacto y un plan de continuidad, garantizando que sus componentes sean recuperables y resilientes a interrupciones. Esto implica que las decisiones de arquitectura, herramientas y proveedores consideren la continuidad del negocio como un requisito fundamental.

7.4. Actualizar el Manual de Políticas de Seguridad y Privacidad de la Información

Estrategia: El Manual de Políticas de Seguridad y Privacidad de la Información debe actualizarse para incluir políticas claras sobre la gestión de la continuidad del negocio. Esto incluye procedimientos para el manejo de incidentes, la gestión de copias de seguridad, el acceso de emergencia a los sistemas y la comunicación durante una crisis. Estas políticas deben ser fácilmente accesibles y comunicadas a todo el personal.

7.5. Realizar seguimiento a los riesgos de seguridad de la información/digital

Estrategia: Como se describe en el Plan de tratamiento de riesgos de seguridad de la información, el seguimiento debe ser un proceso continuo y no un evento único. Se deben utilizar herramientas automatizadas de monitoreo que alerten sobre riesgos potenciales en tiempo real. Esto permite una respuesta proactiva para mitigar amenazas antes de que se conviertan en incidentes con impacto crítico en la continuidad.

7.6. Establecer perfiles para el ingreso, modificación y consulta de la información

Estrategia: El control de acceso es fundamental para la continuidad. Debe implementarse un sistema de gestión de identidades y accesos (IAM) con alta disponibilidad, de modo que, incluso en caso de una falla en el sistema principal, los perfiles de usuario y sus permisos puedan ser restaurados rápidamente para garantizar la continuidad de las operaciones.

7.7. Definir y actualizar los controles para la prevención o mitigación de riesgos asociados a los activos de información

Estrategia: La Declaración de aplicabilidad es clave para este proceso. La estrategia debe basarse en una revisión periódica de los controles existentes, y la implementación de nuevos controles de forma proactiva, como se menciona en los documentos de seguridad. Se deben priorizar los controles que previenen incidentes y reducen el tiempo de recuperación, alineados con el RTO y RPO.

7.8. Garantizar la calidad del software a través de pruebas

Estrategia: Las pruebas de software deben incluir escenarios de interrupción y recuperación. Se deben simular fallas en los sistemas para verificar que el software es capaz de recuperarse de forma automática o con mínima intervención manual, garantizando que el RTO y RPO se cumplan para las aplicaciones críticas.

7.9. Capacitar a los usuarios

Estrategia: La Guía Estrategia de uso y apropiación de TI V2 (Intranet IDPC) destaca la importancia del uso y apropiación de la TI. La continuidad del negocio depende del factor humano. Se debe capacitar al personal de forma regular sobre los procedimientos de emergencia, el uso de las herramientas de recuperación y la comunicación durante un incidente. La concienciación del usuario reduce significativamente la probabilidad de errores humanos que puedan causar interrupciones.

7.10. Desarrollar el Plan de contingencia con enfoque de alta disponibilidad

Estrategia: Este plan, que debe ser la piedra angular de la estrategia de continuidad, debe incluir procedimientos detallados para la recuperación de todos los sistemas y servicios identificados como críticos. El plan debe ser proactivo (alta disponibilidad, sistemas redundantes) y reactivo (pasos de recuperación claros y probados). Debe ser un documento vivo, que se revise y actualice constantemente.

7.11. Administrar la infraestructura de hardware, software base, redes y telecomunicaciones

Estrategia: La Guía de eventos de seguridad y la Política de Tecnologías de la Información son fundamentales para esta actividad. La estrategia es implementar una arquitectura redundante con sistemas de hardware y software en espera (activos-activos o activos-pasivos). Esto garantiza una conmutación por error (failover) rápida en caso de un fallo, cumpliendo con el RTO de dos horas y minimizando el impacto en la operación. El monitoreo constante y el mantenimiento preventivo son también clave para esta estrategia y oportunidad en la protección de datos y la funcionalidad de los servicios en los sistemas de información.

8. Planes de Respuesta y Recuperación por Actividad

A continuación se presentan los planes de respuesta y recuperación para cada actividad crítica, los cuales están diseñados para cumplir con el RTO y RPO establecidos y garantizar la continuidad del negocio:

Identificar las necesidades y requerimientos de los procesos de la entidad

Plan de Respuesta: Ante una interrupción, el equipo debe acceder a la plataforma centralizada y redundante para la recolección de requisitos.

Plan de Recuperación: Se debe restaurar la base de datos de requisitos utilizando los respaldos guardados en un sitio de recuperación. Esto asegura que la información no se pierda y pueda ser restaurada en el tiempo mínimo establecido por el RPO.

Generar el plan estratégico de T.I. (PETI)

Plan de Respuesta: La respuesta inicial es referirse al Plan Estratégico PETI 2025-2027, que debe integrar la gestión de continuidad del negocio y la recuperación ante desastres como pilares fundamentales.

Plan de Recuperación: Se debe seguir el plan de contingencia con enfoque de alta disponibilidad incluido en el PETI para restaurar las operaciones estratégicas. Esto garantiza que las acciones de recuperación sean parte de la planificación estratégica y no una respuesta improvisada.

Definir y consolidar planes, proyectos y programas de T.I.

Plan de Respuesta: En caso de una interrupción, se debe activar el análisis de impacto y el plan de continuidad de cada proyecto de TI crítico, que debe ser una parte inherente de su concepción.

Plan de Recuperación: La Guía de Gestión de Proyectos de TI es el documento base. Se deben utilizar las decisiones de arquitectura, herramientas y proveedores que consideraron la continuidad del negocio como un requisito para restaurar los componentes de los proyectos.

Definir y actualizar el Manual de Políticas de Seguridad y Privacidad de la Información

Plan de Respuesta: El personal debe acceder inmediatamente al Manual de Políticas de Seguridad para seguir los procedimientos de emergencia, manejo de incidentes y comunicación durante una crisis.

Plan de Recuperación: El plan incluye la gestión de copias de seguridad y el acceso de emergencia a los sistemas. El conocimiento de estas políticas permite una respuesta coordinada para la restauración de las operaciones.

Realizar seguimiento a los riesgos de seguridad de la información/digital

Plan de Respuesta: Se activan las herramientas de monitoreo automatizado para detectar riesgos en tiempo real y emitir alertas. Esto permite una respuesta proactiva para mitigar amenazas antes de que escalen a un incidente crítico.

Plan de Recuperación: El plan se basa en el Plan de tratamiento de riesgos de seguridad de la información. La respuesta proactiva derivada del monitoreo continuo ayuda a reducir el impacto de un incidente y el tiempo de recuperación.

Establecer perfiles para el ingreso, modificación y consulta de la información

Plan de Respuesta: En caso de una falla, se debe utilizar el sistema de gestión de identidades y accesos (IAM) con alta disponibilidad para garantizar que los perfiles de usuario y sus permisos puedan ser accedidos.

Plan de Recuperación: La restauración de los perfiles de usuario y los permisos se realiza rápidamente a través del sistema IAM, asegurando la continuidad de las operaciones al restaurar el acceso a los sistemas.

Definir y actualizar los controles para la prevención o mitigación de riesgos asociados a los activos de información

Plan de Respuesta: El plan se centra en la aplicación de la Declaración de Aplicabilidad para identificar y activar los controles existentes que previenen incidentes y reducen el tiempo de recuperación.

Plan de Recuperación: Se priorizan los controles que, en caso de un incidente, ayuden a reducir el tiempo de recuperación, alineándose con el RTO y RPO establecidos. La revisión periódica y la implementación de nuevos controles son clave para la recuperación proactiva.

Garantizar la calidad del software a través de pruebas

Plan de Respuesta: Durante las pruebas de software, se debe simular una interrupción para verificar que el software puede recuperarse automáticamente. Esto es parte del plan de respuesta para asegurar que las aplicaciones críticas cumplan con el RTO y RPO.

Plan de Recuperación: El plan de recuperación para el software crítico se basa en la capacidad del sistema para recuperarse con mínima intervención manual, demostrada durante las pruebas.

Capacitar a los usuarios

Plan de Respuesta: El plan de respuesta se apoya en la Guía de Estrategia de Uso y Apropiación de TI. El personal, previamente capacitado, debe seguir los procedimientos de emergencia y utilizar las herramientas de recuperación.

Plan de Recuperación: La capacitación periódica del personal es fundamental para la recuperación. La concienciación reduce los errores humanos que puedan causar interrupciones, lo que acelera el tiempo de recuperación.

Desarrollar el Plan de contingencia con enfoque de alta disponibilidad

Plan de Respuesta: El plan de contingencia debe ser el documento de referencia principal. Ante un incidente, se deben seguir los procedimientos detallados para la recuperación de todos los sistemas y servicios críticos. El plan debe ser proactivo (alta disponibilidad) y reactivo (pasos de recuperación claros).

Plan de Recuperación: Se deben seguir los pasos de recuperación establecidos en el plan, el cual debe ser un documento vivo que se actualice constantemente para asegurar su eficacia.

Administrar la infraestructura de hardware, software base, redes y telecomunicaciones

Plan de Respuesta: La respuesta inicial es activar la arquitectura redundante con sistemas en espera (activos-activos o activos-pasivos)36. Esto permite una conmutación por error (failover) rápida, cumpliendo con el RTO de dos horas.

Plan de Recuperación: El monitoreo constante y el mantenimiento preventivo son la base de este plan. La conmutación por error es el mecanismo principal de recuperación para minimizar el impacto en la operación.

9.Tipos de Pruebas

Para validar la efectividad de las estrategias de continuidad, se deben realizar los siguientes tipos de pruebas, que van de menor a mayor complejidad y disrupción:

- **Pruebas de revisión:** Consisten en revisar el plan de continuidad, los procedimientos y la documentación asociada en un grupo de trabajo. El objetivo es identificar divergencias o vacíos en los planes sin activar los sistemas.
- **Simulacros de escritorio** (Tabletop Exercises): Se presenta un escenario de crisis hipotético al equipo de respuesta. Se discuten los roles, responsabilidades y los pasos a seguir. No se activan los sistemas, pero se valida el flujo de la comunicación y la toma de decisiones.
- **Pruebas de restauración:** Se prueban los procedimientos de respaldo y restauración de datos para asegurar que los datos críticos puedan ser recuperados dentro del RPO (4 horas).
- **Pruebas de conmutación por error** (Failover): Se simula una interrupción del sistema primario para verificar que los sistemas redundantes tomen el control de las operaciones de manera automática o con mínima intervención, cumpliendo el RTO (2 horas).
- **Pruebas completas de interrupción:** Se simula una interrupción total del servicio para probar todos los procedimientos, desde la notificación inicial hasta la recuperación completa de los sistemas y la infraestructura.

10. Mantenimiento y Actualización de Planes

El plan de continuidad no debe ser un documento estático, sino un documento vivo que se actualice constantemente. Los mecanismos para su revisión y actualización incluyen:

Revisiones periódicas: Se debe programar una revisión anual de todos los planes de continuidad y recuperación. Esta revisión debe ser liderada por el equipo de gestión de continuidad de negocio, en conjunto con los líderes de cada área crítica.

Actualizaciones por cambio: Cualquier cambio significativo en la infraestructura de TI, en los procesos de negocio, o en la estructura organizacional debe disparar una revisión y actualización de los planes de continuidad.

Análisis post-prueba: Después de cada prueba, se debe realizar un análisis de los resultados para identificar las lecciones aprendidas y las áreas de mejora. Los hallazgos deben incorporarse inmediatamente en la actualización de los planes

Capacitación continua: El personal debe ser capacitado de forma regular en los procedimientos de emergencia y el uso de herramientas de recuperación. Esta

capacitación continua es clave para la efectividad de la respuesta humana ante un incidente.

11. Cronograma de Pruebas (1 año)

A continuación, se presenta un cronograma anual para las pruebas y el mantenimiento del plan de continuidad, alineado con los objetivos y estrategias mencionados en la documentación.

Actividad de Pruebas y Mantenimiento	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Revisión de documentación (Todas las actividades)												x
Pruebas de restauración (Todas las actividades)							x					
Simulacros de mesa (PETI, Gestión de Riesgos, Políticas de Seguridad)		x										
Pruebas de conmutación por error (Failover) - (Administración de infraestructura, IAM)										x		
Pruebas de software con escenarios de interrupción						x						

Actividad de Pruebas y Mantenimiento	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Capacitación y concienciación del personal	x					x					x	
Prueba completa de interrupción (Administrar la infraestructura de hardware, software base, redes y telecomunicaciones)												
Análisis post-prueba y actualización de planes		x				x		x		x		x

12. Control de Cambios

Fecha	Versión	Cambios Introducidos	Simplificación o mejora	Origen
29/08/2025	01	Creación del documento.	Mejora	Modelo de seguridad y Privacidad de la Información

13. Créditos

Elaboró	**Revisó**	**Aprobó**
Ángel Antonio Díaz Vega	Mary Rojas	Paulo Cesar Ávila Cantor
Cargo – Rol: Contratista – Oficial de Seguridad de la Información Subdirección de Gestión Corporativa	Cargo – Rol: Profesional Especializado Gestión de sistemas de información y tecnología	Cargo – Rol: Subdirector de Gestión Corporativa
Documento de aprobación	Memorando interno con N° radicado 20255400124043 del 29-08-2025	