AGETIC

agencia de gobierno electrónico y tecnologías de información y comunicación

Lineamientos para la elaboración e implementación de Planes de Contingencia Tecnológica en entidades del sector público

Estado Plurinacional de Bolivia

Estado Plurinacional de Bolivia

SEG-002

Lineamientos para la elaboración e implementación de Planes de Contingencia Tecnológica en entidades del sector público

ctic

CONSEJO PARA LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Lineamientos para la elaboración e implementación de Planes de Contingencia Tecnológica en entidades del sector público

Lineamientos para la elaboración e implementación de Planes de Contingencia Tecnológica en entidades del sector público

SEG-002

Este documento ha sido elaborado por los miembros del Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB).

Coordinación Secretaria Técnica del CTIC-EPB: Patricia López Avendaño, Khantuta Muruchi y Carolina Ovale.

Grupo de Trabajo de Seguridad: Aldo Torrez García, Alejandro Monasterio, Alvaro Gutiérrez Copa, Benjo Huallpa M., Bryan Athea, Boris Cusicanqui H., Cristobal Coarite, Carla Calisaya Choque, Carlos Ramírez García, Cesar Chávez Martínez, Christian Urquidi, Christian Felipe Virreira, Daniel Torrico Álvarez, Daniel Rojas, Daniela Lenz Ardaya, David Gutiérrez, Dania Valenzuela Avendaño, Diego Brayan Alcón Tarqui, Edwin Salcedo Aliaga, Eric Daniel Colquechambi Sánchez, Erock Palenque Ríos, Fernando Choque Alarcón, Fabián Espinoza Valencia, Fidel Rolando Morales Quisbert, Franco Camargo Espejo, Gabriela Murguía Torrez, Gladys Alanoca, Gloria Stephany Chuquimia Nina, Grover Iván Medina Segura, Herian Cameo Ugarte, Hernán Enrique Maidana, Henry Lin Zambrana, Henrry Cenzano Loza, Harold F. Chávez B., Hilder Vladimir Flores León, Jarmila Lejser Halas, Jorge Fabricio Bailey Torrez, José Antonio Jiménez Mancilla, Juan Carlos Canaza, Juan Carlos Patón Mamani, Juan Pablo Conde M., Javier Wilson Condori Machidado, Krissia Stephanie Ferreira Paravicini, Karina Medinaceli, Luis Ariel Huancario Tupa, Luis Calle Blanco, Luis Fernando Catacora Vásquez, Luis Fernando Zegarra Castro, Luz Maribel Garay Quisbert, Luis Fernando Quiroga Altamirano, Luis Freddy Velasco Poma, Marco Mercado Bustillos, Mariel Pizarro Balboa, Miguel Machicao, Miguel Medina, Miguel Fernando Chambi Cari, Miriam Alicia Rosales Rodríguez, Marcelo Romero, Nelson Luna Maidana, Noel Choque Parra, Óscar Álex Villegas Gonzáles, Patricia Mónica Urquiola Torres, Ramiro A. Lazarte Luján, Ranald Soliz Lima, Rodny Escobar, Ramiro Oña, René Cayo Acuña, Ricardo Camacho, Rodrigo Beltrán, Rose Mary Vargas, Rosse Mary Gonzáles A., Rosmery Ana Zegarra Deheza, Roberto Escalante Mendoza, Samuel Wilson Gómez Carranza, Sandra Aileen Macuchapi, Shirley Nahir Pattzi Villavicencio, Stael Candy Alvarez Guzmán, Victor Bernal Rodas, Willy H. Gómez López, Wilfredo Roberto Alarcón, Vladimir Terán Gutiérrez.

Diseño: Orestes Sotomayor

Diagramación: Jorge Dennis Goytia Valdivia

Depósito Legal: 4-1-253-19 P.O.

Impreso: Editorial del Estado

La Paz , Bolivia
2019


ctic
CONSEJO PARA LAS
TECNOLOGÍAS DE INFORMACIÓN
Y COMUNICACIÓN

Contenido

1 Introducción

El Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB) se constituye en una instancia de coordinación técnica para la implementación de Gobierno Electrónico y para el uso y desarrollo de Tecnologías de Información y Comunicación en el país.

Entre las principales funciones asignadas al CTIC-EPB se encuentran:

- Formular propuestas de políticas y normativa relacionada con Gobierno Electrónico, a ser presentadas a la AGETIC;

- Presentar proyectos, programas de Gobierno Electrónico y Tecnologías de Información y Comunicación en el ámbito gubernamental a la AGETIC para su gestión;

- Generar mecanismos de participación para instituciones y organizaciones de la sociedad civil en la proposición, formulación de políticas y acciones relacionadas con Gobierno Electrónico, Tecnologías de Información y Comunicación en el ámbito gubernamental;

- Establecer espacios de coordinación entre las entidades del sector público para el desarrollo conjunto de programas, proyectos o acciones de Gobierno Electrónico, Tecnologías de Información y Comunicación en el ámbito gubernamental;

- Desarrollar y proponer estándares abiertos oficiales del Estado Plurinacional de Bolivia en materia de Gobierno Electrónico y Tecnologías de Información y Comunicación aplicables a las entidades del sector público;

- Establecer espacios de coordinación de comunidades de desarrollo informático, dentro del Estado, con la ciudadanía y a nivel internacional.

El 5 de mayo de 2016 se llevó a cabo la inauguración y la Primera Reunión del Pleno del CTIC-EPB, en la que se conformaron seis grupos temáticos de traba-

jo: Interoperabilidad, Software Libre, Seguridad, Infraestructura, Desarrollo de Software y Datos Abiertos.

Cada Grupo de Trabajo estuvo integrado por servidores públicos de las entidades del nivel central del Estado: Órgano Electoral, Legislativo, Judicial y Ejecutivo, incluyendo sus instituciones descentralizadas, autárquicas, empresas públicas y autoridades de regulación sectorial, Ministerio Público y Procuraduría General del Estado.

Adicionalmente, se invitó a participar, en calidad de miembros adjuntos, a representantes de entidades territoriales autónomas, universidades públicas e indígenas y sociedad civil.

Cada uno de los grupos fue conformado con la finalidad de trabajar y elaborar propuestas a ser presentadas al Consejo para su posible implementación a nivel estatal.

Cabe mencionar que el desarrollo de los Grupos de Trabajo y del Consejo se enmarca en el Reglamento de Funcionamiento del CTIC-EPB, aprobado mediante la Resolución Administrativa N° 024/2016 de la AGETIC, de fecha 31 de mayo de 2016.

Para la gestión 2018, el Grupo de Trabajo de Seguridad se planteó como objetivo la formulación de los lineamientos para que las entidades del sector público del Estado Plurinacional de Bolivia elaboren e implementen Planes de Contingencia Tecnológica.

El Grupo estuvo conformado por los representantes de las siguientes entidades:

- Administración de Aeropuertos y Servicios Auxiliares a la Navegación Aérea (AASANA)
- Administración de Servicios Portuarios – Bolivia (ASP-B)
- Aduana Nacional (AN)

- Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC)[1]
- Agencia Para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB)
- Autoridad de Fiscalización y Control Social de Electricidad (AE)
- Autoridad de Fiscalización del Juego (AJ)
- Autoridad de Fiscalización y Control Social de Empresas (AEMP)
- Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT)
- Autoridad de Fiscalización y Control de Pensiones y Seguros (APS)
- Banco Central de Bolivia (BCB)
- Banco de Desarrollo Productivo (BDP)
- Cámara de Senadores
- Dirección General de Aeronáutica Civil (DGAC)
- Empresa de Apoyo a la Producción de Alimentos (EMAPA)
- Empresa Nacional de Electricidad (ENDE)
- Empresa Pública Nacional Estratégica Lácteos de Bolivia (LACTEOSBOL)
- Escuela de Altos Estudios Nacionales (EAEN)
- Escuela Militar de Ingeniería (EMI)

■

1 En el caso de la AGETIC, los participantes de la mesa son miembros del Centro de Gestión de Incidentes Informáticos (CGII).

- Facultad de Derecho y Ciencias Políticas – Universidad Mayor de San Andrés (UMSA)
- Fondo Nacional de Desarrollo Regional (FNDR)
- Instituto Boliviano de Metrología (IBMETRO)
- Instituto Nacional de Estadística (INE)
- Instituto Nacional de Reforma Agraria (INRA)
- Ministerio de Economía y Finanzas Públicas
- Ministerio de Hidrocarburos
- Ministerio de Justicia y Transparencia Institucional
- Ministerio de Minería y Metalurgia
- Ministerio de Obras Públicas, Servicios y Vivienda
- Ministerio de Trabajo, Empleo y Previsión Social
- Programa Bono Juana Azurduy (BJA)
- Servicio de Impuestos Nacionales (SIN)
- Servicio Estatal de Autonomías (SEA)
- Servicio General de Identificación Personal (SEGIP)
- Servicio Geológico Minero (SERGEOMIN)
- Servicio Nacional de Registro y Control de la Comercialización de Minerales y Metales (SENARECOM)

- Servicio Nacional del Sistema de Reparto (SENASIR)
- Yacimientos Petroleros Fiscales Bolivianos (YPFB)
- Miguel Machicado (sociedad civil)
- Brayan Alcon (sociedad civil)

Asimismo, es importante resaltar la participación de otras entidades u órganos del Estado, a través de sugerencias y acotaciones al documento inicial elaborado por el Grupo. Entre estas se encuentran:

- Agencia Nacional de Hidrocarburos (ANH)
- Autoridad General de Impugnación Tributaria (AIT)
- Boliviana de Aviación (BOA)
- Dirección General del Servicio Civil (DGSC)
- Gobierno Autónomo Municipal de Potosí (GAMP)
- Instituto Geográfico Militar (IGM)
- Ministerio de Educación (MIN-EDU)
- Observatorio Plurinacional de la Calidad Educativa (OPCE)
- Oficina Técnica para el Fortalecimiento de la Empresa Pública (OTFEP)
- Registro Único para la Administración Tributaria Municipal (RUAT)
- Servicio Nacional de Propiedad Intelectual (SENAPI)
- Servicio Nacional de Patrimonio del Estado (SENAPE)

- Unidad de Análisis de Políticas Sociales y Económicas (UDAPE)

Además de todas las instituciones mencionadas y con el fin de desarrollar un trabajo más abierto y participativo, el Grupo incorporó a varios miembros de la sociedad civil.

El resultado de ese trabajo conjunto es el presente documento de "Lineamientos para elaboración e implementación de Planes de Contingencia Tecnológica en entidades del sector público", que recoge las deliberaciones, análisis y sugerencias de todos los miembros del Grupo de Seguridad del CTIC-EPB.

2 Marco normativo referencial

La elaboración del presente documento se enmarca en el mandato institucional respaldado por:

- El artículo 22 del Decreto Supremo N° 29894, de 7 de febrero de 2009, inciso t), de Organización del Órgano Ejecutivo, que establece que: "El Ministerio de la Presidencia es el ente rector de Gobierno Electrónico y de Tecnologías de Información y Comunicación para el sector público del Estado Plurinacional de Bolivia, siendo el encargado de establecer las políticas, lineamientos y normativa específica para su implementación, seguimiento y control".

- El Decreto Supremo Nº 2514, de 9 de septiembre de 2015, en sus siguientes incisos:

  - Artículo 2, de creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), como "una institución pública descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera, legal y técnica y patrimonio propio, bajo tuición del Ministerio de la Presidencia".

  - Artículo 9, párrafo I, de creación del: "Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB), como instancia de coordinación para la implementación de Gobierno Electrónico y para el uso y desarrollo de Tecnologías de Información y Comunicación".

  - Artículo 11, que establece como parte de las funciones del CTIC-EPB: "a) Formular propuestas de políticas y normativa relacionada con Gobierno Electrónico, a ser presentadas a la AGETIC" y "b): Presentar proyectos y programas de Gobierno Electrónico y Tecnologías de Información y Comunicación en el ámbito gubernamental a la AGETIC para su gestión.

  - Artículo 7, que enumera entre las funciones de la AGETIC: "f) Establecer los lineamientos técnicos en seguridad de información para las entidades

del sector público" e "i) Elaborar, proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público; y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática"

El respaldo normativo específico concerniente al Plan de Contingencia Tecnológica incluye:

- El artículo 5 de la Ley N° 164, de 8 de agosto de 2011, Ley General de Telecomunicaciones, que establece como uno de los principios del sector de telecomunicaciones y TIC a la continuidad: "Los servicios de telecomunicaciones y tecnologías de información y comunicación, así como el servicio postal, deben prestarse en forma permanente y sin interrupciones, salvo los casos previstos por norma".

- El artículo 164 (Continuidad del servicio), del Decreto Supremo N° 1391 de Reglamento General de la Ley 164 de Telecomunicaciones, que señala que: "Sin perjuicio de los derechos establecidos en la Ley Nº 164, cuando la ATT tramite reclamaciones, respecto a los servicios de telecomunicaciones disponibles al público; previo análisis podrá ordenar al operador o proveedor que mantenga el servicio o que, en el plazo que el indique, proceda a su re-conexión, según corresponda, mientras resuelva el reclamo presentado".

- Los siguientes artículos del Decreto Supremo N° 1793, de Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, de 13 de noviembre de 2013:

  - Artículo 3 (Definiciones) Parágrafo VI. Respecto a la seguridad informática:

    a. Seguridad informática: Es el conjunto de normas, procedimientos y herramientas, las cuales se enfocan en la protección de la infraestructura computacional y todo lo relacionado con ésta y, especialmente, la información contenida o circulante.

b. Seguridad de la información: la seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

c. Plan de contingencia: Es un instrumento que comprende métodos y el conjunto de acciones para el buen gobierno de las Tecnologías de la Información y Comunicación en el dominio del soporte y el desempeño, contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio y las operaciones de una entidad, en circunstancias de riesgo, crisis y otras situaciones anómalas.

- Artículo 4 (Principios) Parágrafo II. Tratamiento de datos personales, Inciso d) Seguridad: "Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento".

- Artículo 4 (Principios) Parágrafo III. Contenidos digitales: "Los contenidos digitales se rigen con los siguientes principios:

a. Prácticos: Proveer de información práctica y realista;

b. Accesibles: Disponibilidad e intercambio de información en todo momento;

c. Contextualizados: Deben ser acordes a la circunstancia socio-económica, cultural y lingüística de los usuarios;

d. Legibles: Su escritura debe ser concisa, sin ambigüedades, redundancias ni imprecisiones;

e. Ejemplificativos: Deben contener situaciones paradigmáticas, tener ejemplos, casos de estudio y escenarios auténticos y relevantes".

- Artículo 8 (Plan de contingencia), que establece que: "Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad".

3 Objetivo

El objetivo del presente documento es establecer los lineamientos para que las entidades del sector público del Estado Plurinacional de Bolivia puedan elaborar, implementar y actualizar sus Planes de Contingencia Tecnológica, tomando en cuenta los procedimientos, acciones a seguir y recursos a considerar ante la presencia de cualquier evento que dañe una parte o la totalidad de los recursos tecnológicos.

4 Alcance y ámbito de aplicación

En este documento se formulan los lineamientos para la elaboración e implementación de los Planes de Contingencia Tecnológica de las entidades del sector público del Estado Plurinacional de Bolivia.

Los lineamientos contenidos en este documento deberán ser utilizados por todas las entidades del sector público, sin perjuicio del trabajo desarrollado por aquellas entidades que hayan asumido previamente parámetros, rectores, normas y estándares nacionales e internacionales, vigentes o de otra naturaleza, en materia de contingencia tecnológica, siempre y cuando no sean contrapuestas a los lineamientos establecidos en el presente documento.

Las entidades del sector público que ya tengan implementado un Sistema de Gestión de Continuidad del Negocio bajo normas nacionales o internacionales podrán realizar un mapeo o cuadro de equivalencia para la verificación de concordancia con los actuales lineamientos.

5 Términos y definiciones

- **Comité de Seguridad de la Información (CSI):** Equipo de trabajo conformado para gestionar, promover e impulsar iniciativas en seguridad de la información.

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Disponibilidad:** Propiedad de acceso y uso de información a entidades autorizadas cuando estas lo requieran.

- **Entidad del sector público:** Entidades públicas del nivel central del Estado; instituciones descentralizadas, autónomas, estratégicas, empresas públicas; empresas estatales mixtas; empresas estatales intergubernamentales y otras entidades públicas no incluidas en las categorías señaladas precedentemente.

- **Integridad:** Propiedad que salvaguarda la exactitud y completitud de la información.

- **MTD:** (Tiempo máximo de inactividad tolerable) Es el máximo tiempo tolerable sin servicio o caída de servicio que una entidad puede soportar para cumplir con sus objetivos planteados, sin que se produzcan efectos irreversibles.

  También hace referencia al tiempo durante el cual el proceso identificado puede ser inoperable hasta que la entidad empiece a tener pérdidas y colapse.

- **Plan de Contingencia:** Es un instrumento que comprende métodos y el conjunto de acciones para el buen gobierno de las Tecnologías de la Información y Comunicación en el dominio del soporte y el desempeño, contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio y las operaciones de una entidad, en circunstancias de riesgo, crisis y otras situaciones anómalas.

- **Responsable de Seguridad de la Información (RSI):** Servidor público responsable de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información.

- **RTO:** (Tiempo Objetivo de Recuperación): Es el periodo de tiempo real dentro del cual la entidad debe recuperarse después de una interrupción. También hace referencia al tiempo transcurrido entre la interrupción y recuperación e indica el tiempo disponible para recuperar lo interrumpido.

- **RPO:** (Punto Objetivo de Recuperación): Es la tolerancia o sensibilidad que tienen los procesos críticos de la entidad para su operación, respecto a la pérdida de información sensible.

  Hace referencia también al rango de tolerancia que la entidad tiene en relación con la pérdida de datos o información y eventos de desastre.

- **Seguridad de la Información.** La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

- **Seguridad Informática.** Es el conjunto de normas, procedimientos y herramientas que se enfocan en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

6 Lineamientos para la elaboración de planes de contingencia tecnológica en entidades del sector público

Las entidades del sector público deberán elaborar sus Planes de Contingencia Tecnológica conforme a los lineamientos establecidos en el presente documento. El proceso de elaboración incluye las siguientes cuatro partes integrantes:

- **El contexto de la entidad**, que ayuda a identificar los procesos de la entidad, sus factores internos y externos, además de los requisitos legales y reglamentarios para poder elaborar el análisis de riesgos e impactos que permita identificar las necesidades y expectativas de las partes interesadas y determinar el alcance de la contingencia tecnológica.

- **La organización para la contingencia tecnológica**, donde se definirá la política de contingencia que debe seguir la entidad, así como la asignación de roles y responsabilidades necesarios para su aplicación.

- **La planificación de la contingencia tecnológica,** en la que se formularán los objetivos planteados para la contingencia tecnológica además del establecimiento de necesidades y el cronograma para las pruebas del plan de contingencia tecnológica.

- **Los recursos necesarios para la contingencia tecnológica**, donde se definirán aspectos como el personal necesario para la implementación del plan de contingencia, la capacitación y sensibilización necesaria del personal identificado y la documentación de la información.

6.1 Contexto de la entidad

6.1.1 Descripción de la entidad y su contexto

Una adecuada definición de los parámetros básicos a ser considerados para la contingencia tecnológica requiere la descripción del contexto de la entidad y su funcionamiento, que incluye los siguientes elementos: los procesos de la entidad,

sus funciones y servicios, los factores internos y externos, los requisitos legales y reglamentarios.

6.1.1.1 Procesos, funciones y servicios de la entidad

En una primera instancia se deberá realizar un análisis macro a nivel de la entidad del sector público, para lo cual se utilizará la siguiente información:

- **Organigrama:** Documento que permitirá conocer la composición orgánica de la entidad, su estructura interna y jerarquía.

- **Plan Estratégico Institucional (PEI):** Documento que permitirá tomar en cuenta el horizonte a mediano plazo al que apunta la entidad del sector público, sus metas y objetivos trazados, así como su avance alcanzado hasta el momento, su historia y evolución a lo largo del tiempo.

- **Plan Operativo Anual (POA):** Documento que posibilita identificar las metas y objetivos a corto plazo de la entidad del sector público, que deberán aportar al cumplimiento del PEI.

- **Procesos y procedimientos:** Documentación que permitirá conocer los diferentes procesos y procedimientos llevados adelante en la entidad, las áreas que participan, el flujo de información generado, así como el uso o no de sistemas de información.

- **Manuales de puestos y funciones:** Documentación que permite conocer la responsabilidad que cada cargo tiene en la entidad y los procesos en los que participa.

A fin de complementar esta información consultada, se podrán sostener reuniones con las áreas organizacionales pertinentes de la entidad pública.

Con toda la información recopilada, se elaborará un cuadro informativo para la priorización de los procesos, funciones o servicios de mayor relevancia al inte-

rior de la entidad. Para ello, se podrá utilizar como base el siguiente formato de cuadro:

Cuadro 1: Identificación de procesos funciones o servicios

Misión entidad:		
Procesos críticos relacionados	**Funciones**	**Servicios de tecnologías de información relacionados**

6.1.1.2 Factores internos y externos

Una vez identificados los procesos, funciones o servicios que sean relevantes para la contingencia tecnológica, cada entidad del sector público definirá, con base en su jerarquía y funciones, los factores externos e internos de los procesos que pueden generar incertidumbre y ocasionar riesgos.

6.1.1.3 Requisitos legales y reglamentarios

La entidad del sector público debe asegurarse que los requisitos legales de su funcionamiento estén vinculados a la contingencia tecnológica, sean aplicables y puedan ser reglamentados de acuerdo a la normativa vigente en el Estado Plurinacional de Bolivia, además de revisar:

- Los requisitos legales, estatutarios, normativos y contractuales que la entidad del sector público y sus dependencias hayan establecido con los proveedores de servicio o terceros asociados a la entidad, que tengan relación con los procesos, funciones o servicios críticos.

- El conjunto de principios y objetivos, PEI, POA, manuales de funciones, reglamentos internos y cualquier otra fuente documental relacionada a la contingencia tecnológica.

- La evaluación de riesgos previos que la entidad del sector público haya realizado: los informes, reportes de incidentes y/o cualquier documento relacionado a amenazas o vulnerabilidades a las que la entidad del sector público haya sido expuesta.

- Cualquier otra documentación interna o externa que la entidad del sector público determine como apropiada y necesaria para la contingencia tecnológica.

6.1.2 Análisis de riesgos e impactos

Los Planes de Contingencia Tecnológica de las entidades del sector público requieren de la elaboración de un análisis de riesgos e impactos, para lo cual se puede adoptar un estándar o metodología nacional o internacional, vigente o de otra naturaleza, siempre y cuando no sea contrapuesta a los lineamientos establecidos en el presente documento y que se adecúe a los procesos, funciones o servicios identificados como necesarios para la contingencia tecnológica. Los Anexos A y B del presente documento muestran algunas de las posibles metodologías a seguir.

La metodología seleccionada debe establecer, implementar y mantener un proceso formal y documentado en cuanto al análisis de impacto y de riesgos que:

- Considere los requisitos identificados en la descripción de la entidad y el contexto.

- Establezca el marco de la evaluación y defina criterios de categorización.

- Incluya un análisis sistemático para la priorización de los riesgos e impactos. (El Responsable de Seguridad de la Información (RSI) presentará los resultados de la evaluación de riesgos e impactos al Comité de Seguridad de la Información (CSI) para analizar su priorización y tratamiento posterior. La priorización puede ser establecida a partir de lo definido previamente por la entidad del sector público a través del CSI).

La metodología seleccionada debe permitir actualizaciones y revisiones.

6.1.2.1 Análisis de riesgos

Respecto al análisis de riesgos, la metodología debe contener:

- **Identificación del riesgo:** Para la identificación del riesgo se tomarán en cuenta los procesos, funciones o servicios que inciden en la contingencia tecnológica.

- **Valoración del riesgo:** Para esto se evaluarán las posibles consecuencias de la materialización del riesgo.

- **Clasificación del riesgo:** La clasificación del riesgo permitirá definir cuáles son los riesgos que deben tratarse con prioridad.

6.1.2.2 Análisis de impactos

La entidad del sector público debe establecer, implementar y mantener la evaluación y la determinación del análisis de impacto conforme sus procesos, funciones o servicios identificados previamente.

El análisis de impacto en el negocio debe incluir lo siguiente:

- **Identificación:** Se deben identificar todas las actividades que apoyan la provisión de procesos, funciones o servicios necesarios para la continuidad tecnológica.

- **Evaluación de los impactos:** Se deben evaluar los impactos en el tiempo o su frecuencia para determinar los periodos de recuperación, o para medir los tiempos de interrupción de las actividades que apoyan los procesos, funciones o servicios.

- **Establecimiento de plazos:** Es necesario para la reanudación de las actividades a un nivel mínimo aceptable, determinado por la entidad, que incluya los indicadores de continuidad RTO (Tiempo Objetivo de Recuperación), RPO

(Punto Objetivo de Recuperación) y MTD (Tiempo Máximo de Inactividad Tolerable).

6.1.3 Necesidades y expectativas de las partes interesadas

El Plan de Contingencia Tecnológica debe incorporar un relevamiento de las necesidades y expectativas de las partes interesadas, relacionadas a los procesos, funciones y servicios considerados prioritarios para cumplir con la misión, visión y objetivos estratégicos de la entidad del sector público en momentos de contingencia.

En este sentido, dicho relevamiento podrá realizarse con base en los requisitos que se tengan para la continuidad tecnológica, bajo el siguiente formato:

Cuadro 2: Identificación de necesidades y expectativas de las partes interesadas

Partes interesadas	Requisito implícito	Requisito obligatorio	Requisito opcional	Área	Plazo necesario

Sin embargo, la entidad del sector público también podrá hacer uso de otras metodologías, nacionales o internacionales, que considere adecuadas para el relevamiento de las necesidades y expectativas de las partes interesadas.

6.1.4 Alcance de la contingencia tecnológica

La entidad del sector público definirá los alcances relacionados con los procesos, funciones o servicios considerados prioritarios para cumplir con su misión, visión y objetivos estratégicos en situaciones de contingencia tecnológica.

Con base en todo el diagnóstico previo realizado, el RSI propondrá al CSI los alcances de la contingencia tecnológica de la entidad del sector público, para que sean aprobados y revisados.

Una vez aprobados, los alcances quedarán establecidos y serán comunicados a las partes interesadas identificadas en el punto 6.1.3.

6.2 Organización para la contingencia tecnológica

La organización permitirá la definición de la política de contingencia tecnológica y la asignación de roles y responsabilidades en los casos de contingencias.

6.2.1 Definición de la política de contingencia tecnológica

La política de contingencia tecnológica proporciona el marco en torno al cual se diseñan y construyen los Planes de Contingencia Tecnológica y debe ser ajustada a las necesidades de la entidad, de tal forma que apoye al cumplimiento de los alcances propuestos.

En la política se establece claramente lo que deben lograr los planes de contingencia tecnológica; por tanto, su contenido debe ser corto, claro, preciso y conciso.

La política debe ser aprobada por la Máxima Autoridad Ejecutiva (MAE) o la instancia jerárquica que corresponda. La MAE y el CSI deberán demostrar compromiso para la asignación de recursos destinados al cumplimiento de la misma.

La política deberá ser comunicada y socializada a todas las partes interesadas identificadas en el punto 6.1.3. por tratarse de un lineamiento necesario a ser tomando en cuenta para el normal funcionamiento de la entidad ante la contingencia.

El contenido mínimo de la política incluye:

1. Objetivo general
2. Alcance
3. Cumplimiento de normas legales
4. Estrategias de cumplimiento

5. Revisión y aprobación por el Comité de Seguridad de la Información (CSI)

6. Difusión

7. Histórico de cambios

Las estrategias de cumplimiento se refieren a todo lo necesario en cuanto a soluciones para lograr la contingencia tecnológica, con base en lo identificado en el punto 6.1.2. Cada entidad determinará las estrategias más apropiadas para lograr este punto; de forma referencial, se muestran posibles estrategias solo como ejemplo en los Anexos C y D.

6.2.2 Roles y responsabilidades

La MAE de la entidad del sector público debe asegurar la conformación de una estructura adecuada, transversal a todas las partes interesadas, para la administración y funcionamiento del Plan de Contingencia Tecnológica, que incluya la definición de roles y responsabilidades, tanto de los líderes de proceso como de las gerencias.

Esta estructura, formada exclusivamente para el funcionamiento del Plan de Contingencia Tecnológica, deberá tener roles y responsabilidades asignados. De forma referencial, se pueden considerar los siguientes roles:

A. Coordinador de contingencia tecnológica (Requerido).

B. Líder de administración /recuperación de infraestructura física.

C. Líder de recuperación tecnológica (Requerido).

D. Coordinadores de recuperación.

E. Apoyo

F. Comunicación (Requerido)

A. Coordinador de contingencia tecnológica.

El coordinador de Contingencia Tecnológica es el encargado de dirigir y liderar todas las actividades del plan de continuidad. Es el responsable de declarar la contingencia ante el escenario de interrupción en la entidad del sector público, con base en las decisiones tomadas por el Comité de Seguridad de la Información o en situaciones que ameriten su activación inmediata.

Este rol y responsabilidad recaerá en el Responsable de Seguridad de la Información (RSI) designado u otro personal que se considere idóneo y de cargo jerárquico y será designado por el Comité de Seguridad de la Información (CSI) mediante vía formal.

Responsabilidades

- Delegar de manera expresa al CSI la responsabilidad de actualizar, mantener y probar el Plan de contingencia tecnológica.

- Evaluar y aprobar los recursos requeridos para establecer y mantener la estrategia de recuperación y contingencia tecnológica de la entidad.

- Liderar las reuniones del CSI en los temas relacionados con los planes de contingencia tecnológica.

- Advertir sobre nuevos riesgos que afectan a la continuidad de la operación normal de la entidad y que ponen al descubierto debilidades del Plan de Contingencia Tecnológica.

- Establecer los objetivos de recuperación y activar el Plan de contingencia tecnológica ante el escenario de interrupción, teniendo en cuenta el resultado de la evaluación.

- Monitorizar los reportes sobre el estado de recuperación o evaluación durante una contingencia y conocer los daños sufridos (si es que existieran).

- Velar por la seguridad del personal que actúa en el área del evento.

- Velar por la ejecución del debido análisis causa-raíz del evento que ocasione la contingencia tecnológica y sus posibles riesgos.

- Comunicar y coordinar con la MAE o instancia superior correspondiente si el equipo de comunicación debe divulgar la contingencia.

B. Líder de administración / recuperación de infraestructura física

Este rol y responsabilidad será asignado al jefe de dirección, departamento, unidad o área relacionada a sistemas, tecnologías de la información o similares.

El líder administrativo coordinará los aspectos logísticos internos cuando la entidad del sector público se encuentre operando bajo contingencia. También gestionará en cada una de las instalaciones el suministro de elementos esenciales para asegurar el desarrollo de la operación.

Responsabilidades

- Gestionar la ejecución según el Plan de Contingencia tecnológica.

- Coordinar el suministro de elementos esenciales como transporte, recursos de infraestructura y papelería.

- Efectuar una evaluación del daño (si lo hubiera) y notificar al CSI.

- Presentar la información necesaria para efectuar reclamos ante aseguradoras o garantías.

- Mantener informado al coordinador de contingencia tecnológica.

C. Líder de recuperación tecnológica

Es la persona encargada de liderar la recuperación tecnológica, con base enlas estrategias de contingencia tecnológica implementadas; es el contacto directo entre la dirección, gerencia de unidad, la jefatura o departamento de tecnología, sistemas o similares y el Comité de Seguridad de la Información (CSI). Además, apoya las decisiones tomadas por el coordinador de contingencia tecnológica durante la declaración y activación de la contingencia.

Responsabilidades

- Liderar la recuperación tecnológica, con base en las estrategias de contingencia implementadas.

- Identificar los posibles riesgos de aspectos tecnológicos adicionales al estado de contingencia, registrarlos y comunicarlos al coordinador de contingencia tecnológica.

- Colaborar en la comunicación a los proveedores o servicios de su competencia, sobre el estado de contingencia en que se encuentra la entidad del sector público, previa decisión y autorización del coordinador de contingencia tecnológica, mediante comunicado.

- Entregar los reportes correspondientes al CSI sobre el estado de la recuperación.

- Velar por la actualización de la estrategia tecnológica en los casos que se presenten situaciones como cambios en los aplicativos, cambio en la infraestructura, roles y responsabilidades, disponibilidad de los recursos, entre otros.

- Velar por la realización de las pruebas del Plan de Contingencia Tecnológica y revisar los resultados obtenidos en las mismas.

- Verificar que las actividades de ajuste sobre el plan y resultado de las pruebas hayan sido ejecutadas e implementadas.

D. Coordinadores de recuperación

Los coordinadores de recuperación son las personas encargadas de liderar la recuperación de los procesos, funciones o servicios basados en las estrategias de contingencia. Constituyen el contacto directo entre los procesos de negocio y el líder de recuperación tecnológica y además colaboran con las decisiones tomadas por el coordinador de contingencia tecnológica y el comité durante la declaración y activación de la contingencia.

Responsabilidades

- Identificar los posibles riesgos que afectan la contingencia tecnológica de la operación normal de la entidad del sector público.

- Liderar las reuniones para diagnosticar y evaluar las interrupciones que están afectando la prestación del servicio.

- Ejecutar los Planes de Contingencia Tecnológica ante el incidente presentado.

- Mantener comunicación constante durante el estado de contingencia.

- Cubrir las áreas de respuesta en:

    - Software: Solucionar errores en la programación, configuración y fallas de seguridad de código, entre otras.

    - Hardware: Solucionar problemas de mantenimiento o daños en hardware, entre otras.

    - Seguridad: Gestión y respuesta a incidentes de seguridad de la información o informáticos, evaluación de riesgos asociados a la contingencia tecnológica, entre otras.

- Recuperación y restauración de sistemas: Recuperar y restaurar las operaciones de los sistemas, dependiendo del tipo de incidente, o coordinar algún soporte externo si fuera necesario, entre otros.

- Entregar los reportes correspondientes al Comité de Seguridad de la Información, sobre el estado de la recuperación de sus áreas.

- Velar por la realización de las pruebas del Plan de Contingencia Tecnológica y revisar los resultados obtenidos en la misma.

- Verificar que las actividades de ajuste sobre el plan y resultado de las pruebas hayan sido ejecutadas e implementadas.

E. Apoyo

Responsabilidades

- Realizar las actividades que le sean asignadas durante la declaración de contingencia.

- Advertir sobre riesgos que puedan afectar la continuidad en la prestación del servicio o la funcionalidad del Plan de Contingencia Tecnológica.

- Revisar y alertar sobre las implicaciones legales que puede tener, por ejemplo, el apagar un sistema, el infringir los contratos de nivel de servicios, el no apagar un sistema en peligro, la responsabilidad de daños causados por ataques iniciados desde algún sistema interno o externo, entre otros.

- Coordinar toda comunicación con las autoridades legales y organismos de investigación.

F. Comunicación

El servidor público encargado de las comunicaciones institucionales tiene la responsabilidad de asesorar en la comunicación del evento de interrupción a nivel

interno (colaboradores) y a nivel externo (clientes, proveedores, alianzas, organismos de control, entre otros), en situaciones que sean definidas en coordinación con la MAE.

Responsabilidades

- Asesorar a la MAE, al comité y específicamente al coordinador de contingencia tecnológica sobre los temas de comunicación en momentos de contingencia.

6.2.2.1 Delegación de atribuciones por ausencia

De acuerdo a la conformación de la estructura para la Administración de la Contingencia Tecnológica descrita en el punto 6.2.2. de Roles y responsabilidades, la entidad del sector público definirá, de acuerdo a su organización, la designación de delegación en caso de ausencia; es decir, un servidor público de reemplazo para los roles identificados, de tal forma que se garantice el cumplimiento de responsabilidades.

La delegación de atribuciones por ausencia será considerada con base en parámetros de los resultados del análisis de impacto y tiempos de recuperación, además, se debe indicar en este punto cuando una entidad del sector público declara "ausencia".

6.2.2.2 Incumplimiento

De acuerdo a sus normas internas y a las normativa que regula la responsabilidad por la función pública, la entidad del sector público tomará las determinaciones necesarias ante la infracción o incumplimiento de funciones del personal que tiene asignados los roles y responsabilidades de la ejecución de los planes de contingencia tecnológica.

6.2.3 Lista de responsabilidades y autoridades

En función de los resultados de las necesidades y expectativas de las partes interesadas identificadas en el punto 6.1.3, el RSI deberá elaborar una lista de autoridades y responsabilidades de todas las partes interesadas durante la contingencia tecnológica.

Esta lista además deberá tener un plan de llamadas retroalimentado en el cual se establezca la comunicación a las autoridades de la contingencia tecnológica.

6.3 Planificación de la contingencia tecnológica

Como parte integral de los Planes de Contingencia Tecnológica, la parte de planificación tiene los objetivos planteados para la contingencia tecnológica y el establecimiento de necesidades, además de la elaboración del cronograma de pruebas del plan de contingencia tecnológica.

6.3.1 Objetivos planteados para la contingencia tecnológica

Con base en la definición de la Política de Contingencia Tecnológica del punto 6.2.1, se plantearán objetivos que se deberán cumplir durante la contingencia tecnológica:

- Objetivo general: que corresponde al objetivo planteado en el Punto 6.2.1. de la Política de Contingencia Tecnológica.

- Objetivos estratégicos, relacionados a las necesidades y expectativas de las partes interesadas, reflejadas en los puntos 6.1.3 y 6.1.4 de alcance de la contingencia tecnológica.

    - Por ejemplo: Reducir el impacto de incidentes que afecten la contingencia tecnológica, relacionada a hardware, software, equipos y periféricos que soportan los principales procesos, funciones y servicios prestados por la entidad del sector público para el cumplimiento de sus funciones.

- Objetivos tácticos: son aquellos que se formulan con base en los resultados de los tiempos de recuperación establecidos como producto del análisis de impactos del punto 6.1.2.

    - Por ejemplo: Facilitar los procedimientos y capacidades para la recuperación de activos críticos de la infraestructura de tecnologías de información de la entidad para rehabilitar las funciones y procesos identificados en un plazo de 2 horas.

Todos los objetivos deben estar en concordancia con las metas propuestas y considerar lo necesario para la contingencia tecnológica; asimismo, deben ser específicos, medibles, relevantes y temporales.

6.3.2 Establecimiento de necesidades

El establecimiento de necesidades toma en cuenta los requisitos y requerimientos para la ejecución del Plan de Contingencia Tecnológica, que se desprenden de los objetivos planteados.

Las necesidades deben ser claramente identificadas por el RSI y los servidores públicos que tienen asignados los roles y responsabilidades del punto 6.2.2. en un listado que sea aprobado y revisado por el Comité de Seguridad de la Información.

6.3.3 Establecimiento del cronograma de pruebas del plan de contingencia

La entidad deberá realizar todas las pruebas del Plan de Contingencia Tecnológica, para lo cual se establecerán cronogramas, con base en los tiempos establecidos en el Análisis de Impactos y con los escenarios definidos de acuerdo al análisis de riesgos.

El cronograma deberá considerar intervalos planificados donde se establezcan puntos claros de medición que se realicen al menos una vez al año para verificar su eficacia y generar la capacidad técnica y operacional para responder y garantizar que el Plan de Contingencia Tecnológica no presente fallos.

En el ANEXO E se presenta, como ejemplo, un Modelo de Pruebas de Plan de Contingencias Tecnológicas.

6.4 Recursos necesarios para la contingencia tecnológica

La entidad del sector público proporcionará el personal necesario para la implementación, mantenimiento, pruebas controladas y mejora de los planes de contingencia tecnológica, a cuyo efecto deberá contar con presupuesto asignado, así como prever la contratación de personal externo en caso de no contar con los recursos humanos para ello.

A través de las instancias correspondientes, la MAE priorizará y gestionará los recursos económicos para que la infraestructura, en toda su magnitud, esté dispuesta para resistir y darle continuidad a sus operaciones, de conformidad al análisis de riesgos del punto 6.1.2.

6.4.1 Competencias del personal de la entidad

La entidad del sector público determinará las competencias necesarias de su personal, respetando los roles de los responsables de la contingencia tecnológica. Asimismo asegurará, mediante un presupuesto especial, que su personal sea capacitado y esté incluido en su plan o programa anual de capacitaciones.

6.4.2 Capacitación y sensibilización

Para el éxito del Plan de Contingencia Tecnológica, es fundamental contar con la participación y el compromiso del personal involucrado en el mismo. El Comité de Seguridad de la Información debe encargarse de que todos los servidores públicos involucrados reciban capacitación y entrenamiento sobre temas relacionados a los Planes de Contingencia Tecnológica.

Los jefes de las áreas sustantivas, en coordinación con el área de Recursos Humanos y el Responsable de Seguridad de la Información, realizarán, de forma periódica, la capacitación y sensibilización a todo el personal de la entidad del

sector público con el respectivo proceso de evaluación para medir el aprendizaje y desempeño.

Las entidades del sector público también podrán solicitar capacitaciones o sensibilizaciones al Centro de Gestión de Incidentes Informáticos (CGII) de la AGETIC.

6.4.3 Información documentada

Toda la información de los procesos de planificación del Plan de Contingencia Tecnológica, como de los planes y procedimientos que lo componen, deberán ser conservados como información documentada y aprobada por el CSI. En consecuencia, la entidad o empresa pública deberá tener un procedimiento para dicho efecto.

Las entidades del sector público que ya tengan un procedimiento, pueden mantener o seguir, de forma referencial, el modelo del Anexo F.

7 Lineamientos para la implementación de los Planes de Contingencia Tecnológica

Una vez que se ha avanzado en la elaboración del Plan de Contingencia Tecnológica, deben establecerse los lineamientos para su implementación, mismos que deberán incluir:

- **La operación del plan de contingencia tecnológica**, que define el concepto de operaciones y abarca la planificación, control y estrategia del plan mencionado, para un adecuado establecimiento e implementación de procedimientos y estructura de gestión de incidentes y lo realizado en el cronograma de sensibilización, capacitación y entrenamiento.

- **La Evaluación de desempeño** referida al Plan de Contingencia Tecnológica, que verifica la revisión y aprobación por parte del Comité de Seguridad de la Información y el mantenimiento del plan.

- **La mejora del plan de contingencia**, que incorpora su retroalimentación y mejora continua.

7.1 Operación del plan de contingencia tecnológica

En este punto se incluyen la planificación, control y estrategia del Plan de Contingencia Tecnológica, para un adecuado establecimiento e implementación de procedimientos o guías necesarias, además de la estructura de gestión de incidentes, así como todo lo realizado en el cronograma de sensibilización, capacitación y entrenamiento.

7.1.1 Concepto de operaciones

Las operaciones son todas las actividades y acciones realizadas que deben ser llevadas a cabo para lograr superar la contingencia tecnológica.

Es necesario definir claramente lo que la entidad del sector público requiere para cumplir con los puntos 6.2 (Organización) y 6.3 (Planificación). Las acciones lle-

vadas a cabo deben considerar el control de cambios previsto y la revisión de las consecuencias de los cambios no deseados según sea necesario.

7.1.2 Planificación y control del Plan de Contingencia Tecnológica

La planificación de la implementación del Plan de Contingencia Tecnológica debe permitir controlar todo lo identificado en el punto 6.1.2 (Análisis de Riesgos e Impacto) que se encuentre enmarcado en el alcance aprobado por el CSI, minimizando sus consecuencias negativas, y también determinar los requisitos para la seguridad de la información ante situaciones adversas.

Asimismo, debe permitir cumplir con la política definida en el punto 6.2.1 y el uso eficiente de recursos del punto 6.4.

7.1.3 Estrategia del plan de contingencia tecnológica

A partir de la planificación y control establecidos, es necesario tomar en cuenta el punto 6.1.2 del análisis de riesgos e impacto y optimizar la implementación de acciones asumidas frente a los riesgos e impactos contemplados.

La estrategia del Plan de Contingencia Tecnológica corresponde a los procedimientos que restituyan las funciones tecnológicas que fueran afectadas.

Para la implementación de la estrategia propuesta en el punto 6.2.1, se debe contemplar mínimamente lo siguiente:

- Comunicación y sensibilización (cumplimiento del punto 6.4.2)
- Pruebas de implementación de la estrategia de contingencia tecnológica
- Comunicación de resultados de las pruebas
- Procedimiento de gestión de información de la entidad del sector público

7.1.4 Establecer e implementar procedimientos de contingencia tecnológica

La entidad del sector público debe establecer e implementar procedimientos respaldados que permitan verificar acciones u operaciones que se realicen para el Plan de Contingencia Tecnológica, dentro de los cuales se puede incluir de forma no limitativa, los siguientes:

7.1.4.1 Procedimientos o guías de activación y notificación

El procedimiento de activación y notificación considerará a los actores del punto 6.2.2 (Roles y responsabilidades) y a otros actores involucrados, cuando sea necesario u oportuno, con la finalidad de enunciar las causas y justificar el estado de contingencia para activar el Plan de Contingencia Tecnológica elaborado y su forma de notificación.

Para la elaboración de estos procedimientos se deben considerar como base y de forma no limitativa, los siguientes periodos:

- Ante la ocurrencia de un evento (identificación de la presencia de una contingencia).
- Durante la Contingencia Tecnológica (respuesta y restitución).
- Después de la Contingencia Tecnológica (vuelta a la normalidad, evaluación, no conformidades y revisiones posteriores).

7.1.4.2 Procedimientos o guías de escalamiento y comunicación

La entidad del sector público elaborará procedimientos para el escalamiento y comunicación del Plan de Contingencia Tecnológica. El escalamiento debe estar de acuerdo al Plan de Contingencia Tecnológica de cada entidad para su comunicación a las partes interesadas.

Las entidades del sector público deberán reportar la ocurrencia de incidentes informáticos, que activen el Plan de Contingencia Tecnológica, al Centro de Gestión

de Incidentes Informáticos (CGII), de acuerdo al Artículo 17 del Decreto Supremo 2514.

7.1.4.3 Procedimientos o guías de contingencia tecnológica

Los procedimientos o guías que se desprendan de la contingencia tecnológica y su estrategia deben ser elaborados por la entidad del sector público, considerando con claridad los procesos de planificación, preparación, detección, reporte, valoración, decisión, ejecución, respuesta y erradicación para la mejora continua ante la ocurrencia de la activación del Plan de Contingencia Tecnológica.

7.1.5 Estructura de gestión de incidentes

La estructura de la gestión de incidentes podrá considerar como referencia el Anexo C de los Lineamientos para la Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público.

7.1.6 Cronograma de sensibilización, capacitación y entrenamiento

En este punto se debe documentar las capacitaciones y sensibilización que fueron dictadas y las evaluaciones correspondientes que miden el aprendizaje y desempeño, que además muestren el cumplimento de lo planificado en el punto 6.4.2.

7.2 Evaluación de desempeño

La evaluación de desempeño considerará la revisión del Plan de Contingencia Tecnológica por parte del Comité de Seguridad de la Información y el mantenimiento del plan de continuidad con su respectivo seguimiento, medición y análisis de evaluación.

7.2.1 Revisión y aprobación por el Comité de Seguridad de la Información

El Plan de Contingencia Tecnológica deberá ser revisado por el Comité de Seguridad de la Información que impulsará su aprobación ante la Máxima Autoridad Ejecutiva de la entidad del sector público.

En función de las revisiones, se podrán realizar acciones que permitan un mejor seguimiento, medición, análisis y evaluación de estrategia del Plan de Contingencia Tecnológica.

7.2.2 Mantenimiento del Plan de contingencia tecnológica

El RSI deberá promover la realización de pruebas periódicas del Plan de Contingencia Tecnológica, en relación con el cumplimiento y eficacia de las estrategias que se desprenden del mismo.

Si durante las pruebas que se realicen existen servicios de interoperabilidad, se deberá coordinar la colaboración entre instituciones públicas, a objeto de garantizar la continuidad tecnológica.

Los resultados de las pruebas permitirán medir la efectividad y cumplimiento de las estrategias implementadas para que, en función de las mismas, se realice la mejora continua al Plan de Contingencia Tecnológica.

7.3 Mejora del Plan de contingencia tecnológica

La entidad del sector público deberá realizar la mejora continua a fin de mantener la efectividad del Plan de contingencia Tecnológica, considerando como mínimo las siguientes recomendaciones:

- Revisión para eliminar las no conformidades que existieran con respecto al Plan de Contingencia Tecnológica y todo lo inherente a él.

- Controlar y revisar el Plan de Contingencia Tecnológica para implementar cualquier acción necesaria que derive en correcciones o formas de prevención.

- La entidad del sector público deberá conservar la información documentada sobre las correcciones que se realicen, las acciones implementadas y los resultados de lo modificado.

Disposiciones adicionales

Disposición final

Las entidades públicas priorizarán en sus presupuestos institucionales los recursos para el cumplimiento del Plan de Contingencia Tecnológica, en el marco de su asignación presupuestaria y de su POA, previa evaluación y análisis técnico efectuado por cada entidad.

ANEXOS

Anexo A
Guía para la metodología de análisis de riesgos

1 Introducción

Los Lineamientos para la Elaboración e implementación de Planes de Contingencia Tecnológica establecen que cada entidad del sector público puede elegir metodologías de normas y estándares nacionales e internacionales vigentes o de otra naturaleza, siempre y cuando no sean contrapuestas a los lineamientos establecidos en el presente documento con respecto al Análisis de Riesgos.

La metodología de Análisis de Riesgos puede ser alguna de las sugeridas en el presente anexo que tiene como finalidad brindar una guía u orientación al respecto.

2 Objetivo

La presente guía tiene el objetivo de orientar en la metodología de análisis de riesgos a partir de la cual se desarrolla como mínimo las siguientes fases:

Identificación del riesgo: Para la identificación del riesgo se tomarán en cuenta los procesos, funciones o servicios que inciden en la contingencia tecnológica.

Valoración del riesgo: Para la valoración del riesgo se evaluarán las posibles consecuencias de la materialización del riesgo.

Clasificación del riesgo: La clasificación del riesgo permitirá definir cuáles son los riesgos que deben tratarse con prioridad.

3 Primera metodología

La primera metodología se basa en considerar el análisis de riesgos, con base en riesgos y oportunidades (R&O). El proceso general es el siguiente:

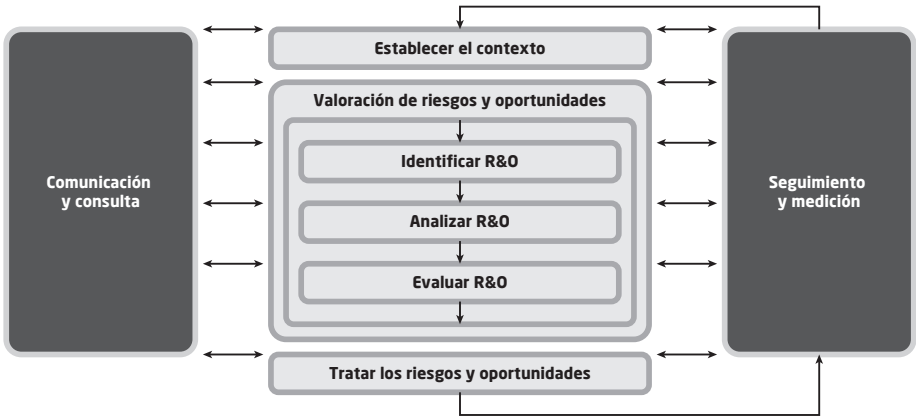
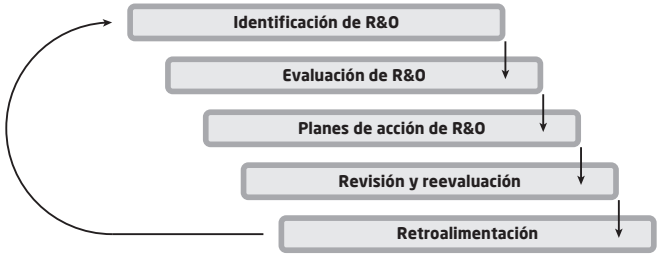


Figura del Proceso para Riesgos



Para el proceso mencionado se define lo siguiente:

- Probabilidad

Nivel	Valor	Calificación	Descripción	Frecuencia
1	1	Baja	Es poco probable que ocurra el R&O De presentarse, se daría en situaciones especiales	Se ha presentado en el último año, una vez o nunca
2	2	Media	Es probable que ocurra el R&O Puede presentarse en algún momento pese a los controles establecidos	Se ha presentado en el último año más de una vez
3	3	Alta	Es altamente probable que suceda el R&O Se va presentar el evento de manera inevitable o favorable	Se ha presentado en el último año más de dos veces

- Impacto

Nivel	Valor	Calificación	Descripción	Frecuencia
1	1	Baja	El impacto es de manera interna o puntual en las partes interesadas, procesos, productos y servicios. De presentarse, se tratarían como correcciones.	Se ha presentado en el último año, una vez o nunca
2	2	Media	El impacto afecta a los procesos, productos y servicios o elementos del sistema de gestión. De presentarse, se tratarían como acciones correctivas o posibles cambios en el sistema de gestión.	Se ha presentado en el último año más de una vez
3	3	Alta	El impacto afecta a la confianza de los procesos, productos y servicios o elementos del sistema de gestión. De presentarse, se tratarían como acciones correctivas y harían cambios importantes en el sistema de gestión.	Se ha presentado en el último año más de dos veces

- Índice de riesgo

El índice del riesgo es la manera cualitativa de medir lo significativo en cada riesgo.

Se calcula a partir de la valoración de la probabilidad de ocurrencia y del impacto del riesgo. Es el producto de la probabilidad (p) e Impacto (i) expresado de la siguiente manera:

$$IR = P * I$$

- La matriz del índice del riesgo se usa para ilustrar los diferentes índices posibles:

Índice del Riesgo		Probabilidad		
		Baja (1)	**Media (2)**	**Alta (3)**
Impacto	Alto (3)	3 MEDIO	6 ALTO	9 ALTO
	Medio (2)	2 BAJO	4 MEDIO	6 ALTO
	Bajo (1)	1 BAJO	2 BAJO	3 MEDIO

- En función a la evaluación efectuada, se tienen las siguientes zonas de riesgos:

Riesgo		
Zona	**Calificación**	**Decisión**
Verde	Bajo (1 a 2)	Asumir Verificar Estimar
Amarilla	Medio (3 a 5)	Repartir Asignar Cambiar
Roja	Alto (≥ 6)	Dominar Evitar Eliminar

  - **Asumir el riesgo:** implica estar expuesto a la probabilidad e impacto que podría derivar en un plan de acción de ser necesario.

  - **Verificar el riesgo:** implica la comprobación de que la probabilidad e impacto permanecen constantes.

  - **Estimar el riesgo:** considera una posible variación en la probabilidad o impacto.

- **Repartir el riesgo:** entre otros procesos internos, por ejemplo: acuerdos entre distintas áreas o unidades organizacionales.

- **Asignar el riesgo:** a otros procesos externos, por ejemplo: incorporar en los términos de referencia.

- **Cambiar el riesgo:** modificando la probabilidad y/o impacto en los términos de referencia.

- **Dominar el riesgo:** asegurando que no cambien la probabilidad y/o impacto, por ejemplo: aplicar algún reglamento o procedimiento.

- **Evitar el riesgo:** implica plantear acciones para prevenir el evento, por ejemplo: optimización del proceso, hacer el seguimiento, uso de tecnologías disponibles.

- **Eliminar el riesgo:** se centra en actuar sobre la fuente de origen, por ejemplo: rediseño del proceso, cambio de tecnología.

• Formulario de registro

Una vez conocidas todas las definiciones, se llenará el siguiente cuadro, con las personas involucradas en la contingencia tecnológica:

Área Organizacional	
Proceso	
Sub Proceso	
Objetivo	

N°	**Gestión del Riesgo / Oportunidad**	**Selección de riesgo y oportunidad**		**Identificación del riesgo / oportunidad**				**Evaluación del riesgo**			
	Fuente (Nivel) estratégico o nivel de operaciones	**Riesgo**	**Oportunidad**	**Denominación del riesgo u oportunidad**	**Descripción**	**Causas**	**Consecuencia o efecto**	**Probabilidad (P)**	**Impacto (I)**	**Índice del riesgo o (P*I)**	**Decisión del Riesgo**

4 Segunda metodología

La segunda metodología se basa en identificar escenarios disruptivos para posteriormente realizar el análisis de riesgo correspondiente, bajo los siguientes pasos:

- Identificación de escenarios disruptivos.
- Análisis del riesgo.
- Identificación de activos de información críticos afectados.
- Identificación de procesos y servicios de TI afectados.

Los cuales se detallan a continuación:

- Identificación de escenarios disruptivos

La identificación de escenarios disruptivos considera el tipo de riesgo, los riesgos y las potencialidades de ocurrencia que, por ejemplo de forma no limitada, pueden ser de las siguientes categorías:

Tipo de riesgo	Riesgo	¿Es un Potencial Riesgo?
Desastres	Sismo /terremoto	Sí
	Tormenta eléctrica	Sí
	Riada	No
Daños Accidentales	Incendio	Sí
	Inundación	No
Tecnológico	Hacking informático	Sí
	Ciberamenazas	Sí
	Ransomware	Sí
Eventos Externos	Fallo de energía	Sí
Eventos Sociales	Conmociones sociales / Saqueos	Sí

- Análisis de riesgos

El análisis de riesgos se realiza bajo las siguientes consideraciones:

Valoración	1	2	3	4	5
Impacto	Insignificante	Menor	Moderado	Severo	Catastrófico
Probabilidad	Raro	Poco Probable	Posible	Probable	Casi Cierto

Rango	(1-4)	(5-8)	(9-12)	(13_18)	(19 a 25)
Nivel de Riesgo	Insignificante	Menor	Moderado	Severo	Catastrófico

Donde, a partir de la tabla de escenarios disruptivos que sí son potenciales, se llena el siguiente cuadro (Por ejemplo):

Tipo de riesgo	Riesgo	Controles existentes	Probabilidad / ocurrencia	Impacto	Riesgo
Desastres	Sismo /terremoto	No se tiene	2	5	10
	Tormenta eléctrica	Pararrayos/conexión a tierra	3	4	8
Daños Accidentales	Incendio	Personal entrenado y extintores	2	5	10
Tecnológico	Hacking informático	Análisis de vulnerabilidades	2	5	15
	Ciberamenaza	Dispositivos de seguridad corta fuegos	2	4	8
	Ransomware	Políticas de seguridad de la información	2	4	8
Eventos Externos	Fallo de energía	UPS y generador	3	1	3
Eventos Sociales	Conmociones sociales / Saqueos	No existe	2	5	10

- Identificación de activos de información críticos afectados

Este paso considera la identificación de activos de información críticos que son afectados, al igual que los procesos o servicios de tecnologías de la información que son afectados (Por ejemplo):

Tipo de riesgo	Riesgo	Activos de información críticos
Desastres	Sismo /terremoto	Servidor A, B y C. Cortafuegos Bases de datos A y B
	Tormenta eléctrica	Servidor A, B y C. Cortafuegos
Daños Accidentales	Incendio	Servidor A, B y C. Cortafuegos Bases de datos A y B
Tecnológico	Hacking informático	Servidor A, B y C. Cortafuegos Bases de datos A y B Computadoras de escritorio
	Ciberamenaza	
	Ransomware	
Eventos Externos	Fallo de energía	Servidor A, B y C. Cortafuegos Bases de datos A y B
Eventos Sociales	Conmociones sociales / Saqueos	Servidor A, B y C. Cortafuegos Bases de datos A y B Computadoras de escritorio

- Identificación de Procesos y Servicios de TI Afectados (Por ejemplo)

Tipo de riesgo	Riesgo	Activos de información críticos	Procesos / servicios de (ti) afectados
Desastres	Sismo /terremoto	Servidor A, B y C. Cortafuegos Bases de datos A y B	Servicio WEB Sistema X y Y Servidor de dominio Servicios de red Servicio de telefonía iP
	Tormenta eléctrica	Servidor A, B y C. Cortafuegos	Servicio WEB Sistema X y Y Servidor de dominio Servicios de red Servicio de telefonía iP
Daños Accidentales	Incendio	Servidor A, B y C. Cortafuegos Bases de datos A y B	Servicio WEB Sistema X y Y Servidor de dominio Servicios de red Servicio de telefonía iP
Tecnológico	Hacking informático	Servidor A, B y C. Cortafuegos Bases de datos A y B Computadoras de escritorio	Servicio WEB Sistema X y Y Servidor de dominio Servicios de red Servicio de telefonía iP
	Ciberamenaza		
	Ransomware		
Eventos Externos	Fallo de energía	Servidor A, B y C. Cortafuegos Bases de datos A y B	Servicio WEB Sistema X y Y Servidor de dominio Servicios de red Servicio de telefonía iP
Eventos Sociales	Conmociones sociales / Saqueos	Servidor A, B y C. Cortafuegos Bases de datos A y B Computadoras de escritorio	Servicio WEB Sistema X y Y Servidor de dominio Servicios de red Servicio de telefonía iP

5 Tercera metodología

El análisis de riesgos es el proceso que permite determinar y categorizar las amenazas potenciales y vulnerabilidades asociadas a activos de información. El resultado de este proceso permitirá un nivel de riesgo sobre el cual se deben implementar soluciones relacionadas a la contingencia tecnológica.

Esta metodología quiere determinar la importancia que tienen las posibles amenazas y vulnerabilidades a las que está expuesta y realizar una descripción del escenario en el cual se puede dar la materialización de la amenaza, asumiendo que el responsable conoce y entiende los riesgos.

Una vulnerabilidad es toda aquella debilidad que se presenta, dada comúnmente por la inexistencia o ineficacia de un control. Está relacionada con la parte interna de la entidad del sector público.

Una amenaza es todo elemento que, haciendo uso o aprovechando una vulnerabilidad, atenta o puede atentar contra la seguridad; está relacionada con la parte externa de la entidad. Las amenazas surgen a partir de la existencia de vulnerabilidades.

La determinación del riesgo para cada activo/amenaza resulta de:

- La probabilidad de que ocurra el incidente, es decir, que la amenaza explote la vulnerabilidad.

- La magnitud del impacto que el evento produce sobre el activo.

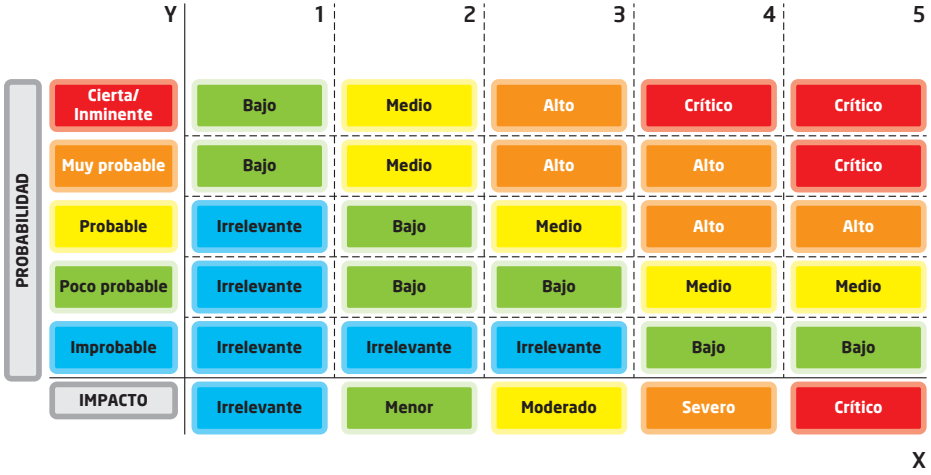
La valoración del riesgo se da en función de la probabilidad y el impacto ocasionado sobre el activo en escalas cualitativas.

Cuadro: Valoración cualitativa

Escalas	
Probabilidad	Impacto
Cierta/Inminente	Crítico
Muy Probable	Severo
Probable	Moderado
Poco Probable	Menor
Improbable	Irrelevante

La probabilidad y el impacto se combinan en una tabla para calcular y valorar el riesgo en una matriz de probabilidad versus impacto.

Figura de la matriz para valorar el riesgo



La valoración cualitativa del riesgo no limita a la entidad del sector público de utilizar valoraciones cuantitativas. Después de los resultados de la valoración, se deben tratar los que caen en la parte superior del gráfico expuesto.

La matriz que se puede utilizar para este efecto es la siguiente:

Figura de la matriz de riesgos

VALORACIÓN DE RIESGOS						
#	**Amenaza**	**Situación**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**

Anexo B
Metodología de análisis de impactos

1 Introducción

Los Lineamientos para la Elaboración e implementación de Planes de Contingencia Tecnológica establecen que cada entidad del sector público puede elegir metodologías de normas y estándares nacionales e internacionales vigentes, o de otra naturaleza, siempre y cuando no sean contrapuestas a los lineamientos establecidos en el presente documento con respecto al análisis de impactos.

En consideración, se puede revisar la ISO 22317, norma internacional que aborda el Análisis de Impacto en el Negocio (BIA).

La metodología de Análisis de Impactos también puede ser alguna de las sugeridas en el presente anexo que tiene como finalidad brindar una guía u orientación al respecto.

2 Objetivo

La presente guía tiene el objetivo de orientar en la metodología de análisis de impactos a partir de la cual se desarrolla como mínimo las siguientes fases:

- **Identificación:** La identificación de todas las actividades que apoyan la provisión de procesos, funciones o servicios que son necesarios para la continuidad tecnológica.

- **Evaluación de los impactos:** La evaluación de los impactos en el tiempo o frecuencia para determinar tiempos de recuperación, o para medir tiempos de interrupción de las actividades que apoyan los productos, funciones o servicios.

- **Establecimiento de Plazos:** El establecimiento es necesario para la reanudación de estas actividades a un nivel aceptable mínimo especificado que

sea determinado por la entidad, que incluyan los indicadores de continuidad RTO, RPO y MTD.

3 Primera metodología

Se define impacto como el grado o la medida de efectos adversos o consecuencias, derivadas de la interrupción de un proceso crítico, existen diferentes tipos de impacto que deben ser valorados de acuerdo a los siguientes criterios, por ejemplo de forma no limitada:

Tipos de Impacto

Tipo de impacto	Descripción
Pérdida económica	Efectos adversos de un incidente disruptivo que ocasiona pérdidas financieras para la entidad
Incumplimiento legal y/o regulatorio	Efectos adversos de un incidente disruptivo que ocasiona el incumplimiento de regulaciones sectoriales o incumplimiento de niveles de servicio con terceras partes interesadas
Daño a la reputación / imagen	Efecto adverso de un incidente disruptivo que ocasiona una pérdida de reputación o compromete la imagen pública de la entidad
Afectación del servicio al cliente	Efecto adverso de un incidente disruptivo que afecta de manera directa a los niveles de servicio prestados a los clientes

Valoración del Impacto

Valoración del impacto	
Valor	**Descripción**
1	Insignificante
2	Menor
3	Moderado
4	Severo
5	Catastrófico

RTO (Tiempo Objetivo de Recuperación)

A continuación se describen los valores RTO: estos valores son definidos por la entidad de acuerdo al análisis previo, por ejemplo, pueden ser de forma no limitada:

Valoración del RPO

TABLA PARA ESTIMAR EL RTO	
VALOR	**DESCRIPCIÓN**
1	El proceso requiere estar restaurado en menos de 15 minutos
2	El proceso requiere estar restaurado en menos de 30 minutos
3	El proceso requiere estar restaurado en menos de 1 hora.
4	El proceso requiere estar restaurado en menos de 2 horas
5	El proceso requiere estar restaurado en menos de 6 horas
6	El proceso requiere estar restaurado en menos de 12 horas
7	El proceso requiere estar restaurado en menos de 24 horas
8	El proceso requiere estar restaurado en menos de 120 horas
9	El proceso requiere estar restaurado en menos de dos semanas

RPO (Punto Objetivo de Recuperación)

A continuación se describen los valores RPO; estos valores son definidos por la entidad de acuerdo al análisis previo, por ejemplo, pueden ser de forma no limitada:

Valoración del RPO

Tabla para estimar el RPO	
Valor	**Descripción**
1	El proceso requiere operar con información actualizada
2	El proceso puede operar con el backup de información de las últimas 4 horas
3	El proceso puede operar con el backup de información de las últimas 8 horas
4	El proceso puede operar con el backup de información de las últimas 12 horas
5	El proceso puede operar con el backup de información de las últimas 24 horas

MTD (Tiempo Máximo de Inactividad Tolerable)

A continuación se describen los valores MTD; estos valores son definidos por la entidad de acuerdo al análisis previo, por ejemplo, pueden ser de forma no limitada:

Estimación del MTD

Tabla para estimar el MTD	
Valor	**Descripción**
1	El proceso estará operativo totalmente en menos de 15 minutos
2	El proceso estará operativo totalmente en menos de 30 minutos
3	El proceso estará operativo totalmente en menos de 1 hora
4	El proceso estará operativo totalmente en menos de 2 horas
5	El proceso estará operativo totalmente en menos de 6 horas
6	El proceso estará operativo totalmente en menos de 12 horas
7	El proceso estará operativo totalmente en menos de 24 horas
8	El proceso estará operativo totalmente en menos de 120 horas
9	El proceso requiere estar restaurado en menos de dos semanas

Niveles Mínimos de Servicio

Son los niveles de servicio, comprometidos por la entidad, para restaurar la operatividad de un proceso crítico después de un incidente disruptivo respecto al RTO definido para el proceso.

Prioridades de recuperación

Los procesos críticos presentan actividades, subprocesos y/o activos de información que tienen mayor criticidad de recuperación para facilitar condiciones operativas al proceso. A continuación, se describen los valores definidos al respecto:

Valoración de las prioridades de recuperación

Prioridad de recuperación	
Valor	**Descripción**
A	Es altamente prioritario para la recuperación del proceso
M	Es medianamente prioritario para la recuperación del proceso
B	Tiene una baja prioridad para la recuperación del proceso

A continuación, se muestran ejemplos del llenado de las tablas BIA de forma referencial:

Análisis del Impacto (BIA)

Proceso	Sub Proceso
Gestión de Telecomunicaciones	Gestión de la infraestructura de redes y comunicaciones (firewalls, switches, vpns, vlans, medios de transmisión)
Prioridad de Recuperación	A

TIPO DE IMPACTO	0-15 Min.	15-30 Min.	30-60 Min.	1-2 Hrs.	2-6 Hrs.	6-12 Hrs.	12-24 Hrs.	1-5 Días	>5 Días
Pérdida económica	Menor	Menor	Menor	Menor	Menor	Menor	Mode-rado	Severo	Catas-trófico
Incumplimiento legal y/o regulatorio	Menor	Menor	Menor	Menor	Menor	Mode-rado	Mode-rado	Severo	Catas-trófico
Daño a la reputación / imagen	Menor	Menor	Menor	Mode-rado	Mode-rado	Mode-rado	Severo	Severo	Catas-trófico
Afectación del servicio a la ciudadanía	Menor	Menor	Menor	Mode-rado	Mode-rado	Severo	Severo	Severo	Catas-trófico
Afectación del Servicio / Usuarios Internos	Menor	Menor	Mode-rado	Mode-rado	Mode-rado	Severo	Severo	Severo	Catas-trófico
MTD : 5 días Máximo Periodo de Interrupción Tolerable	1	2	3	4	5	6	7	8	9
	< 15 Min.	**< 30 Min.**	**< 1 Hr.**	**< 2 Hrs.**	**< 6 Hrs.**	**< 12 Hrs.**	**< 24 Hrs.**	**< 120 Hrs.**	**>120 Hrs.**
								X	
RTO : 12 horas Tiempo Objetivo de Recuperación	1	2	3	4	5	6	7	8	9
	< 15 Min.	**< 30 Min.**	**< 1 Hr.**	**< 2 Hrs.**	**< 6 Hrs.**	**< 12 Hrs.**	**< 24 Hrs.**	**< 120 Hrs.**	**>120 Hrs.**
						X			
RPO : 1 Semana (Archivos de Configuración) Punto Objetivo de Recuperación	1	2	3	4	5	6	7	8	9
	< 15 Min.	**< 30 Min.**	**< 1 Hr.**	**< 2 Hrs.**	**< 6 Hrs.**	**< 12 Hrs.**	**< 24 Hrs.**	**< 120 Hrs.**	**>120 Hrs.**
									X

Proceso	Sub Proceso
Gestión de Telecomunicaciones	Gestión de los enlaces de comunicación
Prioridad de Recuperación	A

TIPO DE IMPACTO	0-15 Min.	15-30 Min.	30-60 Min.	1-2 Hrs.	2-6 Hrs.	6-12 Hrs.	12-24 Hrs.	1-5 Días	>5 Días
Pérdida económica	Menor	Menor	Menor	Menor	Menor	Menor	Mode-rado	Severo	Catastró-fico
Incumplimiento legal y/o regulatorio	Menor	Menor	Menor	Menor	Menor	Mode-rado	Mode-rado	Severo	Catastró-fico
Daño a la reputación / imagen	Menor	Menor	Menor	Mode-rado	Mode-rado	Mode-rado	Severo	Severo	Catastró-fico
Afectación del servicio a la ciudadanía	Menor	Menor	Menor	Mode-rado	Mode-rado	Severo	Severo	Severo	Catastró-fico
Afectación del Servicio / Usuarios Internos	Menor	Menor	Mode-rado	Mode-rado	Mode-rado	Severo	Severo	Severo	Catastró-fico
MTD : 5 días Máximo Periodo de Interrupción Tolerable	1	2	3	4	5	6	7	8	9
	< 15 Min.	**< 30 Min.**	**< 1 Hr.**	**< 2 Hrs.**	**< 6 Hrs.**	**< 12 Hrs.**	**< 24 Hrs.**	**< 120 Hrs.**	**>120 Hrs.**
								X	
RTO : 12 horas Tiempo Objetivo de Recuperación	1	2	3	4	5	6	7	8	9
	< 15 Min.	**< 30 Min.**	**< 1 Hr.**	**< 2 Hrs.**	**< 6 Hrs.**	**< 12 Hrs.**	**< 24 Hrs.**	**< 120 Hrs.**	**>120 Hrs.**
						X			
RPO : n/a : Punto Objetivo de Recuperación	1	2	3	4	5	6	7	8	9
	< 15 Min.	**< 30 Min.**	**< 1 Hr.**	**< 2 Hrs.**	**< 6 Hrs.**	**< 12 Hrs.**	**< 24 Hrs.**	**< 120 Hrs.**	**>120 Hrs.**

Proceso	Sub Proceso
Gestión de los Sistemas de Información	Gestión, administración y producción del [SISTEMA X]
Prioridad de Recuperación	A

TIPO DE IMPACTO	0-15 Min.	15-30 Min.	30-60 Min.	1-2 Hrs.	2-6 Hrs.	6-12 Hrs.	12-24 Hrs.	1-5 Días	>5 Días
Pérdida económica	Menor	Menor	Menor	Menor	Menor	Menor	Mode-rado	Severo	Catastró-fico
Incumplimiento legal y/o regulatorio	Menor	Menor	Menor	Menor	Menor	Mode-rado	Severo	Severo	Catastró-fico
Daño a la reputación / imagen	Menor	Menor	Menor	Menor	Mode-rado	Severo	Severo	Severo	Catastró-fico
Afectación del servicio a la ciudadanía	Menor	Menor	Menor	Mode-rado	Mode-rado	Severo	Severo	Severo	Catastró-fico
Afectación del Servicio / Usuarios Internos	Menor	Menor	Mode-rado	Mode-rado	Mode-rado	Severo	Severo	Severo	Catastró-fico
MTD : 5 días Máximo Periodo de Interrupción Tolerable	1	2	3	4	5	6	7	8	9
	< 15 Min.	**< 30 Min.**	**< 1 Hr.**	**< 2 Hrs.**	**< 6 Hrs.**	**< 12 Hrs.**	**< 24 Hrs.**	**< 120 Hrs.**	**>120 Hrs.**
								X	
RTO : 12 horas Tiempo Objetivo de Recuperación	1	2	3	4	5	6	7	8	9
	< 15 Min.	**< 30 Min.**	**< 1 Hr.**	**< 2 Hrs.**	**< 6 Hrs.**	**< 12 Hrs.**	**< 24 Hrs.**	**< 120 Hrs.**	**>120 Hrs.**
						X			
RPO : 24 horas (Backup Base Datos) Punto Objetivo de Recuperación	1	2	3	4	5	6	7	8	9
	< 15 Min.	**< 30 Min.**	**< 1 Hr.**	**< 2 Hrs.**	**< 6 Hrs.**	**< 12 Hrs.**	**< 24 Hrs.**	**< 120 Hrs.**	**>120 Hrs.**
							X		

4 Segunda metodología

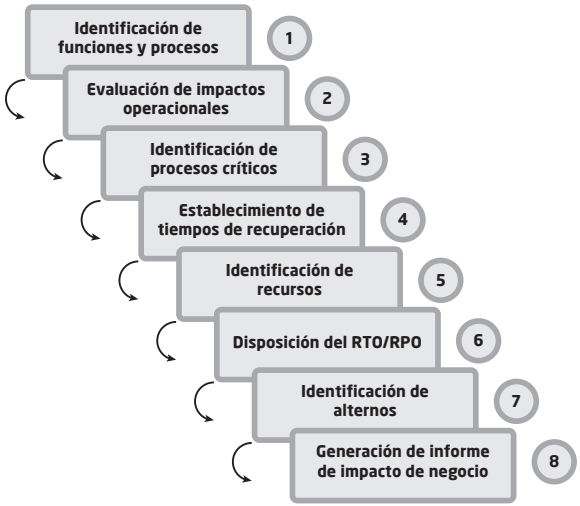
Introducción

El análisis de impactos es parte del plan de continuidad y debe entenderse como un marco conceptual sobre el que las entidades del sector público deben planificar integralmente los alcances y objetivos que protejan la información en todas sus áreas críticas identificadas previamente.

Objetivo

Tener disponible una metodología que especifique y permita identificar las áreas críticas y sus impactos de modo que sea un instrumento para garantizar la correcta medición y magnitud del impacto en una interrupción.

Pasos a seguir para el análisis de impactos



Etapa inicial de requerimientos

Para poder llevar a cabo correctamente un análisis de impactos es necesario considerar los principales puntos:

- Identificar funciones y procesos: es decir, tener en cuenta cuáles de estos procesos son indispensables para que entren en operación rápidamente, asignándoles prioridades para contener el incidente sufrido. Cabe recalcar que todos los procesos deben ser ejecutados dentro del plan de contingencia tecnológica.

- Revisar las consecuencias: es necesario evaluar las consecuencias obtenidas a nivel operacional y financiero en un proceso considerado de alta prioridad.

- Estimar tiempos de recuperación: de acuerdo a las posibles alteraciones de los procesos altamente prioritarios para el funcionamiento de las infraestructuras de TI.

La información para la recopilación de requerimientos debe ser obtenida en primera instancia de las mismas entidades y áreas de la entidad del sector público. Se recurren a recursos como ser:

- Encuestas: conjunto de preguntas cerradas o abiertas que se envían a los interesados o propietarios de procesos e información.

- Entrevistas: son obtenidas de manera personal al entrevistar a los interesados o propietarios de procesos e información.

- Talleres: se obtiene la información requerida al trabajar colectivamente con el grupo de interesados o propietarios de procesos e información.

Al finalizar esta etapa se presenta un informe detallado de las funciones y procesos críticos de la entidad.

En todos los casos la información recopilada debe ser almacenada y comunicada de acuerdo a los reglamentos e instructivas de la entidad del sector público en la que se trabaja.

Requerimientos de tiempo de recuperación

El lapso de tiempo concreto requerido para que la información de la entidad del sector público esté disponible oportuna y ordenadamente tras las interrupciones de los servicios e infraestructura de TI es compuesto principalmente por los componentes:

- MTD (*Maximun Tolerable Downtime*, tiempo máximo de inactividad tolerable): tiempo durante el cual el proceso puede ser inoperable hasta que la entidad empiece a tener pérdidas y colapse.

- RTO (*Recovery Time Objective*, tiempo de recuperación objetivo): tiempo transcurrido entre la interrupción y recuperación; indica el tiempo disponible para recuperar lo interrumpido.

- RPO (*Recovery Point Objective*, punto de recuperación objetivo): es el rango de tolerancia de que la entidad puede tener sobre la pérdida de datos o información y evento de desastre.

- WRT (*Work Recovery Time*, tiempo de recuperación de trabajo): es el tiempo invertido en buscar datos perdidos y realizar las reparaciones necesarias; es el tiempo entre la recuperación del sistema y normalización de los procesos.

Identificación de funciones y procesos paliativos

En este punto se identifican las funciones y procesos de la entidad del sector público útiles para apoyar la misión y objetivos realizables. El resultado de este punto es generar un listado de roles y procesos que analicen el cumplimiento del plan de contingencia tecnológica.

Evaluación de impactos operacionales

Permite evaluar el nivel de la interrupción en varios aspectos, utilizando la siguiente tabla como referencia:

EVALUACIÓN DE IMPACTOS OPERACIONALES	
El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones de la entidad; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C.	
Nivel A	La operación es crítica para un negocio. Una operación es crítica cuando al no contar con esta, la función de la entidad no puede realizarse.
Nivel B	La operación es una parte integral de la entidad, sin esta el negocio no podrá operar normalmente, pero la función no es crítica.
Nivel C	La operación no es una parte integral de la entidad.

Para ejemplificar el desarrollo presentamos la tabla:

VALORACIÓN OPERACIONAL POR NIVELES DE CRITICIDAD				
Categoría (Función de la entidad)	**Procesos (Servicio)**	**Nivel**	**Tolerancia a fallas (Horas)**	**Descripción**
Aplicaciones	Sistema de control de flujo de documentos	B	3	Contenedor de aplicaciones
Web	Sitio web entidad	A	1	Capa de presentación
Base de datos	SQL nómina	A	1	Contenedor de aplicaciones en SQL
Seguridad de información	Firewall	A	1	Servicio de firewall de la entidad
Sistemas de almacenamiento	SAN (Storage Area Network)	A	3	Capacidad de almacenamiento en SAN
Comunicaciones	Acceso local a internet	C	4	Comunicación de internet del usuario local
Cuartos de máquinas	Centro de datos	A	1	Servicio de centro de datos de la entidad
Proveedores de aplicaciones y/o comunicaciones	Interno/externo	B	2	Desarrollo interno o contratado por externos. Canales de comunicación.
Recurso humano	Interno/externo	C	3	Profesionales encargados de administrar las infraestructuras de la entidad.

Identificación de procesos críticos

La identificación de procesos y operaciones críticas para la entidad del sector público tiene base en la clasificación antes propuesta de acuerdo a sus objetivos y metas.

Establecimiento de los tiempos de recuperación

Una vez identificados y clasificados todos los procesos, se analizan los tiempos que tardan en normalizarse sin afectar o colapsar la entidad del sector público, cada entidad determina estos tiempos en función de sus necesidades.

Como ejemplo:

Categoría (Función Crítica)	Proceso Crítico (Servicios)	MTD (en días)	Prioridad de Recuperación
Aplicaciones	Sistema de control de flujo de documentos	2 días	3
Soporte informático	Dispositivos móviles	2 días	3
Aplicaciones	Sistema de nómina	0.5 día*	1
Seguridad de información	Firewall	0.5 día*	1
Sistema de almacenamiento	SAN (Storage Area Network)	1 día	2
Comunicaciones	Servicio WiFi	1 día	2
Cuartos de máquina	Centro de datos	0.5 día*	1
Soporte informático	Equipo PC de usuario	3 días	4

Identificación de recursos

Los recursos y procesos indispensables para normalizar las operaciones y procesos en la entidad del sector público deben ser priorizados, de igual forma los procesos alternos que hacen posible la operabilidad en caso de interrupciones. Para ello, es oportuno que las entidades tengan métodos alternativos temporales que coadyuven a superar las crisis generadas por las interrupciones en cada proceso crítico establecido.

Como ejemplo:

Categoría (Función crítica)	Procesos críticos (Servicios)	Identificación de recursos críticos de sistemas TI
Aplicaciones	Sistemas de nómina	Sistema de entrada de novedades administrativas. Interfaces con el Sistema Financiero.
Seguridad de información	Firewall	Reglas de entrada y salida de puertos. Reglas NAT/PAT. Direccionamiento IP público.
Comunicaciones	Servicio WiFi	Control de identificación de usuarios con Portal Cautivo. Control de usuarios locales vs. invitados.
Cuartos de máquina	Centro de datos	Control de operaciones de Servidores, Equipos de Comunicaciones, Sistemas de Almacenamiento, Sistemas de Backups, Aire Acondicionado, Acometida Electrica.

Documentos Generados

Al culminar el análisis de riesgos es necesario tener aprobado por el Consejo de Seguridad de la información (CSI) y Máxima Autoridad Ejecutiva (MAE) los siguientes documentos y procesos:

- Listado y evaluación de procesos críticos.
- Prioridades de sistemas y aplicaciones.
- Procesos con análisis de tiempos de recuperación.
- Identificación de recursos.

Listado de evaluación y procesos críticos:

Categoría (Función crítica)	Procesos Críticos (Servicios)	Identificación de recursos críticos de Sistema TI	Tiempo de recuperación Objetivo-RTO	Tiempo de recuperación Trabajo-WRT
Cuartos de máquinas	Centro de datos	Control de operaciones de servidores.	1 día	1 día
		Sistemas de almacenamiento.	0.5 día	0.5 día
		Sistemas de backups.	1.5 días	1 día
		Aire acondicionado.	1 día	0.5 día
		Acometida eléctrica.	0.5 día	0.5 día

Generación de Informe de Impacto del Negocio

Con todos los requerimientos y documentos generados elabora un informe donde se establecen también las posibles soluciones y alternativas para minimizar el impacto generado.

Anexo C
Plan de tratamiento de riesgos

Como parte integral se tienen los Planes de Tratamiento de Riesgos para Contingencia Tecnológica, los cuales están diseñados para la respuesta planificada ante el fallo o pérdida de activos de información de la infraestructura de Tecnologías de Información en situaciones de contingencia.

Este plan de tratamiento de riesgos forma parte de las posibles estrategias que se implementen y su uso no es obligatorio, sino de forma condicional a los requerimientos de la entidad del sector público.

1 Objetivos

- Reducir el impacto de incidentes que afecten la contingencia tecnológica de hardware, software, equipos y periféricos que soportan los principales procesos y servicios prestados por la infraestructura de Tecnologías de Información de la entidad.

- Optimizar los esfuerzos y recursos necesarios para atender cualquier contingencia de manera oportuna y eficiente, definiendo las personas responsables de las actividades a desarrollar para la respuesta de incidentes disruptivos relacionados con fallos de la infraestructura de tecnologías de la Información.

- Facilitar los procedimientos y capacidades para la recuperación de activos críticos de la infraestructura de tecnologías de información de la entidad.

2 Metodología

- Descripción de la contingencia.

- Activos de información afectados.

- Medidas de prevención.

- Recursos mínimos asignados para la recuperación.
- Procesos críticos relacionados.
- Convenios realizados para la recuperación.

3 Planificación y ejecución de plan de tratamiento de riesgos

Todo plan de tratamiento de riesgos asociados a la contingencia tecnológica requiere identificar con precisión los siguientes elementos:

- Definir el tipo de contingencia tecnológica a probar.
- Establece el escenario o condiciones de fallo.
- Fecha y hora de la prueba.
- Comunicación sobre la planificación a las partes interesadas
- Recursos necesarios.
- Objetivo de la prueba.
- Procedimiento de prueba.
- Responsable de la ejecución.
- Equipo de validación de pruebas.

4 Procedimientos del plan de contingencia.

Debe tener un procedimiento de la prueba a realizarse; todas las actividades descritas en un procedimiento deben ser superadas para considerar el Plan de Tratamiento de Riesgos de Contingencias Tecnológicas. En caso que alguna de

las actividades especificadas en un procedimiento falle, se considera que la ejecución ha sido fallida.

Todos los planes y procedimientos de contingencia tecnológica deben probarse al menos una vez al año para verificar su eficacia y para crear la capacidad técnica y operacional para responder a incidentes y para garantizar la recuperación de activos de información críticos.

Todo procedimiento debe tener un responsable de su ejecución y una instancia independiente que supervise y evalúe la ejecución exitosa o fallida de pruebas de contingencia.

4.1 Detalle de procedimientos

Detalle de Procedimientos	Descripción
Procedimiento a	[...]
Procedimiento b	[...]
Procedimiento c	[...]
[...]	[...]
Procedimiento n	[...]

4.2 Programación y pruebas

Procedimiento	Estado	Gestión/Año											
		ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
Procedimiento a	ejecutado		x										
Procedimiento b	ejecutado			x									
Procedimiento c	Programado						x						
[...]	Programado								x				
Procedimiento n	Programado											x	

Anexo D
Plan de recuperación de desastre

Los planes de recuperación de desastres en Contingencia Tecnológica proporcionan procedimientos detallados a seguir, paso a paso, para recuperar los sistemas, redes y otros que han sufrido disrupciones para ayudar a resumir la normalidad en las operaciones de la entidad del sector público.

Este plan de recuperación de desastres forma parte de las posibles estrategias que se implementen y su uso no es obligatorio, sino de forma condicional a los requerimientos de la entidad del sector público.

1 Objetivo

El objetivo de estos procesos es minimizar cualquier impacto negativo en las operaciones de la entidad del sector público.

El proceso de recuperación de desastres identifica los sistemas, redes y otros, críticos de tecnologías de la información (con la criticidad); fija las prioridades para su recuperación y dibuja los pasos necesarios para actividades previas al desastre, actividades durante el desastre y actividades después del desastre.

Todo plan integral de recuperación de desastres debería incluir a todos los proveedores relevantes, las fuentes de experiencia para recuperar los sistemas afectados y una secuencia lógica de los pasos a seguir hasta alcanzar una recuperación adecuada de desastre.

2 Estructura del plan

Esta estructura proporciona la orientación necesaria para elaborar un plan de recuperación de desastres efectivo.

Actividades previas al desastre: Actividades de resguardo de información que aseguren una recuperación con el menor costo, realizar o elaborar un plan de acción por cada proceso, función o servicio, que sea identificado en la criticidad.

Actividades durante el desastre: Establecer un programa de prácticas de ejecución de procedimientos ante diferentes siniestros que puedan ocurrir y definir actividades y actores con flujos de contingencias.

Actividades después del desastre: Evaluación de daños, que tenga priorización de actividades del plan con su respectiva ejecución de actividades, la restauración del proceso, función o servicio una evaluación de los resultados de la recuperación y la optimización del plan de recuperación de desastres.

3 Metodología

Se puede seguir de forma no limitativa la siguiente metodología:

1. Establecer el alcance de la acción, como por ejemplo, elementos internos, activos externos, recursos de terceros, enlaces a oficinas, clientes y proveedores, etc.

2. Recopilar toda la documentación relevante de la infraestructura de redes, como los diagramas de las redes, la configuración de los equipos y bases de datos, etc.

3. Obtener copias de los planes de recuperación de redes y de tecnologías de la información existentes.

4. Examinar el historial previo de disrupciones y cómo fueron gestionados.

5. Identificar los activos TI que la dirección considera de importancia crítica. Por ejemplo, procesos, funciones o servicios, servidores, acceso a internet.

6. Determinar el tiempo máximo que está dispuesta a aceptar la entidad del sector público, en caso de indisponibilidad de los equipos de TI, de acuerdo al análisis de impactos.

7. Identificar los procedimientos operativos que se utilizan actualmente para responder a disrupciones y preparar al personal para manejar los sistemas críticos, especialmente en casos de emergencia.

8. Identificar las capacidades de respuesta de los proveedores en casos de emergencia, si se han utilizado alguna vez, si funcionaron correctamente, cuánto paga la compañía por estos servicios, el estado del contrato de servicio, la existencia del acuerdo de nivel de servicio (SLA).

9. Resultados de todas las evaluaciones, que identifique lo que se está haciendo frente a lo que debería hacerse con recomendaciones sobre cómo lograr el nivel requerido en el análisis de impactos.

10. Revisar el plan de recuperación de desastres y mejorarlo.

11. Realizar pruebas de los planes y activos de recuperación de sistemas para validar su operatividad.

Anexo E

Modelo de pruebas plan de contingencias tecnológicas

Objetivo de la prueba:

Fecha y hora de realización de la prueba:

Responsable de ejecución: Líder de recuperación tecnológica y/o listado con prelación.

Descripción contingencia	
Escenario o condiciones de fallo	[Descripción] [Activos de Información Afectados] [Causas] [Efectos]
Comunicación a partes interesadas	Listado de personas a ser comunicadas
Recursos mínimos asignados para la recuperación	Recursos de hardware Recursos de software Recursos de respaldo Facilidades Costo
Procedimiento de la prueba	Fecha de planificación: __/__/__ Fecha de aprobación: __/__/__ [Detalle de procedimientos]
Validación de la prueba	

[Comentarios/observaciones/evidencias]

[Validación del procedimiento]

[Sello/firma] [Departamento Sistemas]	[Sello/firma] [Responsable de Seguridad Información]

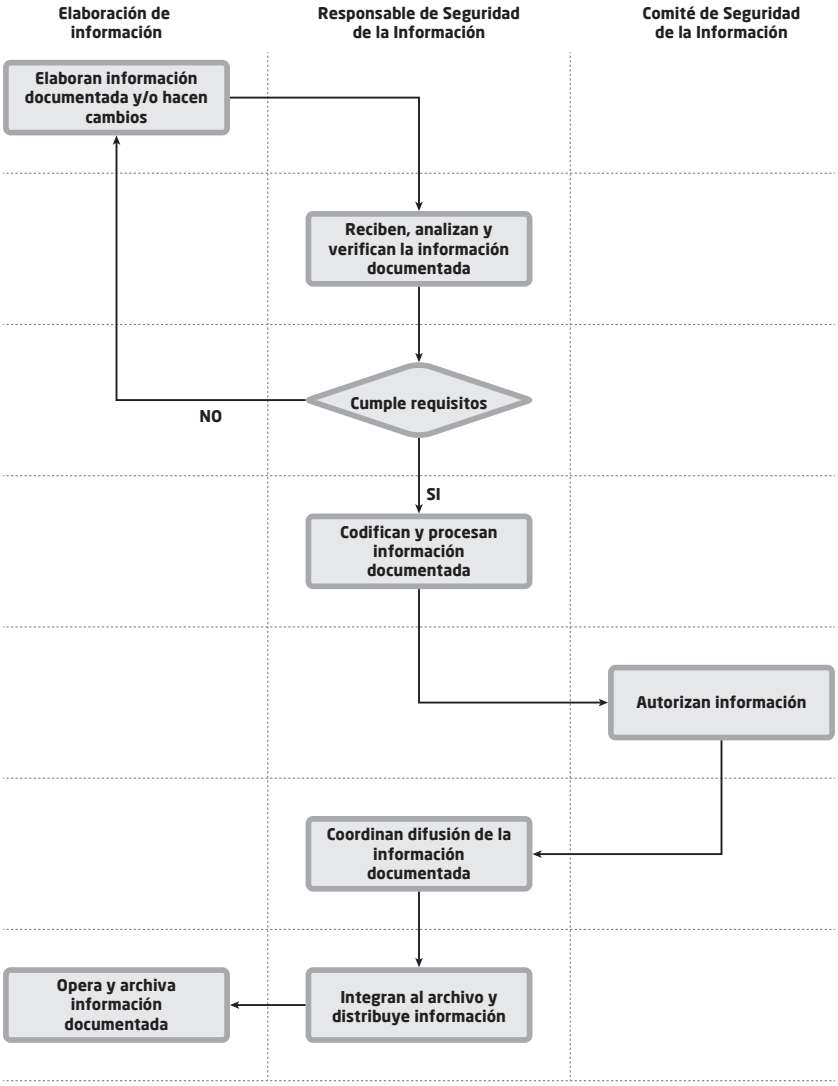
[Aprobación del procedimiento]

[Sello/firma] [Delegado del Comité de Seguridad de la Información]	[Sello/firma] [Delegado de Auditoría Interna]

Resultado: [Prueba exitosa / Prueba fallida]

Comentarios del resultado:

Anexo F
Procedimiento de información documentada




AGETIC
agencia de gobierno electrónico y
tecnologías de información y comunicación