Guía para la preparación de las TIC para la continuidad del negocio

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No 10

17
18
19

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	15/12/2010	Versión inicial del documento

TABLA DE CONTENIDO

PÁG.

1. DERECHOS DE AUTOR

2. AUDIENCIA

Entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

Teniendo en cuenta lo establecido en el Plan Vive Digital, liderado por el Ministerio de las Tecnologías de la Información y las Comunicaciones, en cuanto a la infraestructura, los servicios, las aplicaciones y los usuarios en el marco de un ecosistema digital; las recomendaciones brindadas en el Plan Nacional de Desarrollo 2015-2018 en cuanto a la necesidad de reconocer la seguridad y privacidad de la información, como un factor primordial para la apropiación de las TIC; la constante evolución de los mercados; y la dinámica de las entidades, plantea un marco de seguridad de la información para la prestación de servicios a los ciudadanos a través de las tecnologías de la información, el cual deberá ser respaldado por una gestión, unas políticas y unos procedimientos adecuados, que resalten el papel de las personas como el primer eslabón de una compleja cadena de responsabilidades y que esté orientado a preservar los pilares fundamentales de la seguridad y privacidad de la información.

La implementación de un proceso de preservación de la información pública ante situaciones disruptivas, permite minimizar el impacto y recuperación por perdida de activos de información de la organización, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de eventos disruptivos (desastres, fallas de seguridad, perdida del servicio y disponibilidad del servicio) se deberían ser someter a un análisis del impacto del negocio (BIA). Se deben desarrollar e implementar un plan de continuidad que permita garantizar la restauración oportuna de las operaciones esenciales.

La correcta implementación de la gestión de la continuidad del negocio disminuirá la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, la organización estará preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado por de ese incidente.

4. JUSTIFICACIÓN

La gestión de la continuidad del negocio, es un proceso para holístico a través del cual se identifican los impactos potenciales que amenazan la continuidad de las actividades de las Entidades, proveyendo un marco de referencia para la construcción de la resiliencia y la capacidad de una respuesta efectiva, que le permita proteger los intereses de las Entidades debido a disrupciones.

La guía expuesta en este documento, es un complemento del modelo de seguridad y privacidad de la información y se constituye en un referente de la continuidad del negocio para las entidades del Estado.

5. GLOSARIO

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

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

- **Plan de Continuidad de Negocio.**
  Procedimientos documentados que guían orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel pre-definido de operación debido una vez presentada / tras la interrupción.

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

- **Análisis del impacto al negocio (BIA por sus siglas en ingles).**
  Proceso del análisis de actividades las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas. [Fuente: ISO 22300]

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

- **Interrupción.**
  Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

- **Recuperación de desastres de tecnología y telecomunicaciones (ITCTIC).**
  Habilidad Capacidad de los elementos de tecnología y telecomunicaciones (ITC)de las TIC de la organización para soportar sus funciones críticas a un nivel aceptable dentro de un periodo predeterminado de tiempo después de una interrupción.

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

  NOTA: En algunas organizaciones es llamado el plan de continuidad de tecnología y telecomunicaciones las TIC.

- **Modo de falla.**
  Manera Forma en por la cual se observa una falla es observada.

  NOTA: Esta generalmente describe la manera en que la falla ocurre y su impacto para en la operación del sistema.

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

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

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

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

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

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

  NOTA: También conocido como evento activador.

- **Registro vital.**
  Registro electrónico o en papel que es esencial para preservar, continuar o reconstruir las operaciones de una organización y proteger los derechos de una organización, sus empleados, sus clientes y sus partes interesadas.

6. OBJETIVOS

Para lograr esta visión, se han adoptado los siguientes objetivos:

- Establecer procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones criticas del negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre.
- Identificar las aplicaciones y las plataformas consideradas críticas para la operación del negocio.
- Identificar al personal clave interno y externo requerido para la operación de las actividades críticas del negocio.
- Establecer los tiempos mínimos de recuperación requeridos en los que no se vea afectado el negocio.
- Definir la funcionalidad mínima que requiere el negocio en caso de contingencia.
- Identificar los riesgos presentes para la continuidad.
- Establecer los elementos esenciales requeridos en el plan de recuperación de desastres.
- Desarrollar procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales especificados en el alcance del plan.
- Desarrollar e impartir la capacitación inicial para el correcto funcionamiento del plan.
- Establecer un plan de prueba, gestión y mantenimiento necesarias para garantizar los objetivos del Plan.

7. MARCO PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

El modelo de operación de Continuidad del Negocio para el Modelo de Seguridad y Privacidad de la Información, contempla su implementación las cuatro (4) fases, del ciclo del Modelo para que las Entidades puedan gestionar la seguridad y privacidad de la información, con el fin de fortalecer la protección de los datos y dar cumplimento a lo establecido en la Estrategia de Gobierno en Línea, cubriendo de una manera integral cada uno de sus componentes.

Esta gestión se aplica a todas las fases del desarrollo del modelo, de manera que conserven las expectativas de los grupos de interés de la Entidad, tanto internos como externos. Los insumos para la gestión del modelo están dados por los resultados de las actividades de cada fase, en especial los requeridos por las Entidades, vistos en el marco de seguridad y privacidad de la información.

8. DESCRIPCIÓN DETALLADA DE LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO Y EL MODELO DE OPERACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En el presente capitulo se explica el ciclo de funcionamiento del modelo de operación de continuidad del negocio y su funcionamiento dentro del modelo de operación seguridad y privacidad de la información y la descripción detallada de cada una de las fases. Las cuatro (4) fases que comprenden el modelo de operación contienen objetivos, metas y herramientas que permiten que la continuidad del negocio sea un sistema de sostenible dentro de las entidades.

Ilustración 1 – Marco de Seguridad y Privacidad de la Información

La ilustración 1, muestra el modelo de operación de seguridad y privacidad de la información, del cual solo tendremos en cuenta las fases de planificación, implementación, gestión y mejora continua, como se muestra en la siguiente ilustración.

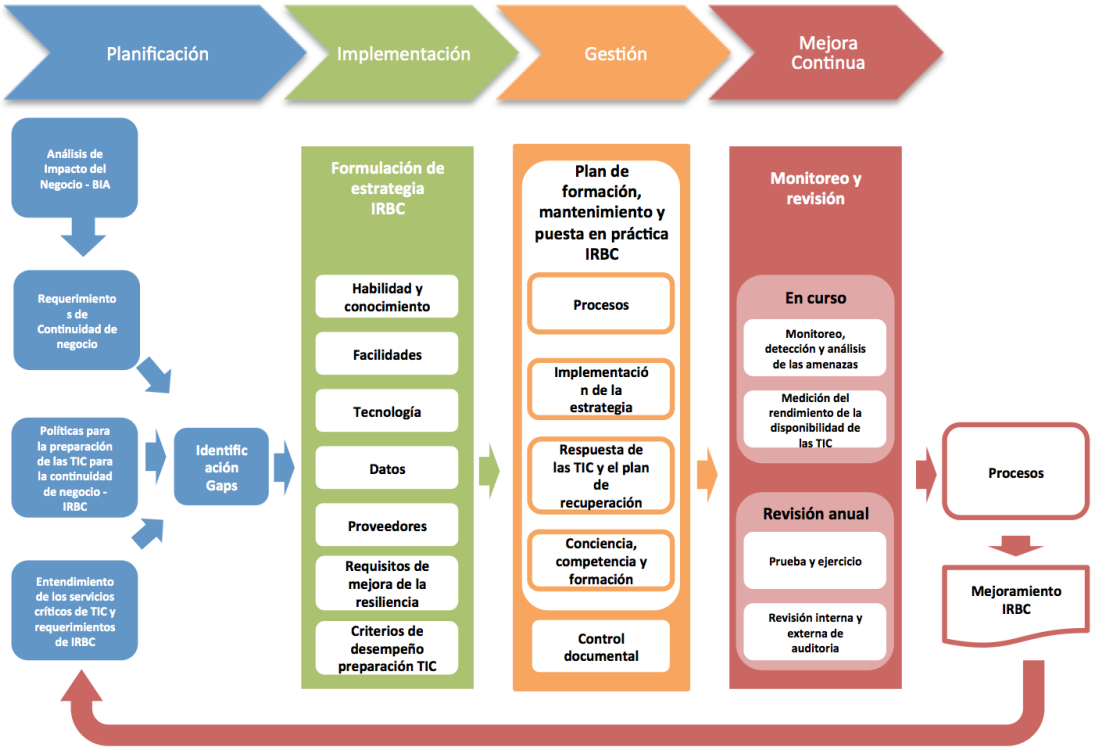

Ilustración 2 – Marco Continuidad del Negocio para Seguridad y Privacidad de la Información

Como parte del proceso de continuidad del negocio, la preparación de las TIC para la continuidad del negocio (IRBC), hace referencia a un sistema de gestión que complementa y suporta la continuidad del negocio de la organización y los programas de Sistemas de Gestión de Seguridad de la Información (SGSI), para mejorar la preparación de la Entidad que le permita:

a) Responder al cambiante ambiente de riesgos.
b) Asegurar la continuidad de las operaciones críticas del negocio soportadas por servicios de TIC.
c) Estar preparado para responder antes de que una disrupción de los servicios de TIC ocurra, identificar los eventos o las serie de eventos relacionados provenientes de incidentes.
d) Responder y recuperarse de incidentes y/o desastres y fallas.

9. COMPONENTE – PLANIFICACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

En este componente, se debe definir la estrategia metodológica, que permita establecer el políticas, objetivos, procesos y procedimientos, pertinentes que le permitan a la Entidad, la preparación de las TIC para la continuidad del negocio (IRBC). La alta dirección debe aprobar los requerimientos de continuidad del negocio de la organización y estos requerimientos darán lugar a un tiempo objetivo de recuperación (RTO) y un punto objetivo de recuperación (RPO) para el objetivo mínimo de continuidad del negocio (MBCO) por producto, servicio o actividad. Estos RTOs comienzan desde el punto en el cual la interrupción ocurrió y va hasta que el producto, servicio o actividad está disponible nuevamente.

Metas	Entregables	Nivel
✓ Objetivos, alcance y limites para la preparación de las TIC para la continuidad del negocio (IRBC). ✓ Política para la preparación de las TIC para la continuidad del negocio (IRBC). (Ver, guía de políticas de seguridad y privacidad de la información) ✓ Asignación de recurso humano competente y capacitado, comunicación de roles y responsabilidades para la preparación de las TIC para la continuidad del negocio (IRBC). ✓ Definición de un plan de requerimientos, categorizando las actividades para la continuidad definiendo el nivel con el cual cada actividad critica necesita para su reanudación, estas actividades deberán contar con un tiempo objetivo de recuperación (RTO) y un punto objetivo de recuperación (RPO) para el objetivo mínimo de continuidad del negocio (MBCO) por producto, servicio o actividad. ✓ Para cada servicio TIC crítico los acuerdos actuales de preparación de TIC – tales como prevención, monitoreo, detección, respuesta y recuperación – deben ser comparados con los requerimientos de continuidad del negocio y cualquier “brecha” debe ser documentada e informada a la alta dirección. ✓ Definir la estrategia de IRBC, la aproximación para implementar la resiliencia requerida de tal manera que los principios de prevención de incidentes, detección, respuesta, recuperación y restauración se pongan en marcha, se deberán contemplar aspectos tales como: habilidades y conocimiento del personal, instalaciones, tecnología, datos, procesos y proveedores, estas deberán ser aprobadas por la alta dirección y sensibilizadas al interior de la Entidad.	Documento con cada uno de los registros e informes a cada una de las metas debidamente aprobado y socializado al interior de la Entidad, por la alta dirección.	**Inicial/ Gestionado**

10. COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

Este componente le permitirá a la Entidad llevar acabo la implementación del componente de **planificación**, teniendo en cuenta los aspectos más relevantes en los procesos de implementación de la estrategia de IRBC, las cuales deberán ser implementadas después de la aprobación de la alta dirección.

La alta dirección debe gestionar y proporcionar los recursos necesarios, procedimientos y operación del IRBC, así como los programas de entrenamiento y concientización. La implementación se debe gestionar como un proyecto a través del proceso de control de cambios formales de la Entidad y de los controles de gestión del proyecto de la Gestión de Continuidad del Negocio con el fin de asegurar visibilidad completa de la gestión y del reporte.

Se deben de tener en cuenta estándares internacionales pertinentes durante la implementación de la detección y respuesta de incidentes y de los componentes de recuperación de desastres, incluyendo los siguientes:

a) ISO/IEC 18043 Para la selección y operación de sistemas de detección de intrusos.
b) ISO/IEC 18044 Para el proceso de respuesta a incidentes.
c) ISO/IEC 24762 Para los servicios de recuperación de desastres.

Metas	Entregables	Nivel
✓ Implementación de los elementos de la estrategia IRBC. • Concientización, habilidades y conocimiento general de la preparación de los elementos de servicios de TIC personas, infraestructura, tecnología, datos, procesos y proveedores, así como sus componentes críticos. • La infraestructura de los sistemas de recuperación de TIC y la información crítica deben, en lo posible, ser físicamente separada del sitio operacional para prevenir que sea afectada por el mismo incidente. • Las estructuras tecnológicas de TIC deben ser implementadas, incluyendo el tipo de implementación y acuerdo, como por ejemplo:	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección. Documentos con los planes para el manejo de interrupciones potenciales, para la habilitación de los servicios TIC y la recuperación de los servicios críticos este debe contemplar el propósito y alcance, roles y responsabilidades, activación del plan y la documentación del plan de respuesta y recuperación de TI propietario y mantenimiento. Documentación del plan de respuesta de TIC y plan de recuperación. Documento con los registros de concientización, competencia y programa	Definido

a. Espera en caliente, donde la infraestructura TIC es replicada a través de dos sitios. b. Espera en tibio, donde la recuperación toma lugar en un sitio secundario donde la infraestructura TIC está parcialmente preparada. c. Espera en frio, donde la infraestructura es construida o configurada a partir de cero en una ubicación alterna. d. Banco de acuerdos, sobre los cuales los proveedores de servicios externos puedan proveer hardware. e. Acuerdos compuestos de las estrategias precedentes: con un enfoque de “escoger y mezclar”. • Los acuerdos para la disponibilidad de los datos deben estar alineados con los requerimientos de la estrategia. • La Entidad debe asegurar que los proveedores críticos están en capacidad de soportar los servicios de la estrategia, conforme a los requerimientos de la Entidad. • Implementar el plan de respuesta de incidentes que permita confirmar la naturaleza y grado del incidente, tomar control de la situación, contener el incidente y comunicar a las partes interesadas.	de pruebas. - Documento con el control de registros del IRBC. - Documento con el control de la documentación que asegure que los documentos son aprobados por su exactitud antes de ser publicados, control de cambios. Nota: Todos los documentos deben ser aprobados por la alta dirección, y se deben encontrar disponibles en los puntos de uso.	

11. COMPONENTE – EVALUACIÓN DE DESEMPEÑO PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

Este componente le permitirá a la Entidad, debe evaluar el desempeño y la eficacia de la implementación , a través de instrumentos que permita determinar la efectividad de la implantación del MSPI.

Para la medición de la efectividad de los procesos y controles del MSPI, se deben tomar los indicadores definidos en el componente de implementación para llevar a cabo el plan de seguimiento, evaluación y análisis del MSPI.

Metas	Entregables	Nivel
✓ Plan de seguimiento, evaluación y análisis para la preparación de las TIC para la continuidad del negocio (IRBC). ✓ Auditoria Interna para la preparación de las TIC para la continuidad del negocio (IRBC). ✓ Evaluación del desempeño de la preparación para las TIC para la continuidad del negocio.	Documento con el plan de seguimiento, evaluación, análisis y resultados del IRBC, revisado y aprobado por la alta Dirección. Documento con el plan de auditorias internas y resultados, de acuerdo a lo establecido en el plan de auditorias, revisado y aprobado por la alta Dirección.	**Gestionado cuantitativamente**

12. COMPONENTE – MEJORA CONTINUA PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

Este componente le permitirá a la Entidad realizar acciones correctivas apropiadas a los potenciales impactos determinados por el análisis de impacto del negocio BIA de la Entidad.

Metas	Entregables	Nivel
✓ Definir las acciones correctivas, identificando las fallas. ✓ Auditoria Interna. ✓ Comunicación de resultados y plan de mejoramiento. ✓ Revisión y aprobación por la alta Dirección.	Documento con el plan de seguimiento, evaluación y análisis para el IRCB, revisado y aprobado por la alta Dirección. Documento con el consolidado de las auditorias realizadas de acuerdo con el plan de auditorias, revisado y aprobado por la alta Dirección.	**Optimizado**

13. ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)

El Análisis de Impacto del Negocio BIA (Bussiness Impact Analysis) Por sus siglas en inglés), permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio.

Cada entidad debe disponer de un documento que permita identificar todas las áreas críticas del negocio y sea un instrumento para garantizar la medición de la magnitud del impacto operacional y financiero de la entidad, al momento de presentarse una interrupción.

En esta etapa, el análisis de impacto del negocio, debe poder clarificar los siguientes requerimientos:

- Identificar las funciones y procesos importantes para la supervivencia de la entidad al momento de la interrupción, esto es tener en cuenta cuales de los procesos son claves para que entren en operación rápidamente asignándoles la mayor prioridad posible, frente a los de menor prioridad; debe quedar claro que para los procesos identificados como no tan prioritarios se deben preparar también planes de recuperación.
- Revisar las consecuencias tanto operacionales como financieras, que una interrupción tendrá en los procesos considerados de alta prioridad.
- Estimar los tiempos de recuperación, en razón a las posibles alteraciones de los procesos considerados de alta prioridad para el funcionamiento de las infraestructuras de TI.

El entregable de esta fase es un informe con el detalle de las funciones y procesos críticos del negocio. Este documento debe contener la información básica de los recursos requeridos y los tiempos de recuperación para que las entidades puedan poner en funcionamiento los servicios y por ende la continuidad del negocio.

13.1. MÉTODOS PARA LA OBTENCIÓN DE INFORMACIÓN

Es recomendable que las entidades posean un método estructurado que facilite la obtención de la información requerida, según (Hiles, 2004) , se debe disponer de encuestas, entrevistas y talleres.

- Encuesta: Conjunto de preguntas que se envían a las distintas entidades de la organización.
- Entrevistas: La información del Análisis de Impacto del Negocio (BIA), se obtiene personalmente, entrevistando a una o más personas. La información detallada puede obtenerse creando preguntas para cada entrevista, de acuerdo a las necesidades de la organización que hace las preguntas.
- Talleres: Permite a un grupo de personas trabajar de forma colectiva para que de esta manera se provea de información para el análisis de impacto del negocio.

13.2. REQUERIMIENTOS DE TIEMPO DE RECUPERACIÓN

Como parte del plan de continuidad del negocio de una organización, es importante poder definir y entender los requerimientos de tiempo necesarios para recuperar a las entidades de servicios que han sido interrumpidos por diferentes motivos dentro de la organización; estos requerimientos obedecen a varios componentes que hacen referencia concreta al tiempo disponible en la cual una organización puede recuperarse oportuna y ordenadamente a las interrupciones en los servicios e infraestructuras de TI. Los componentes se describen a continuación:

- MTD (Maximun Tolerable Downtime) o Tiempo Máximo de Inactividad Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.
- RTO (Recovery Time Objective) o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.
- RPO (Recovery Point Objective) o Punto de Recuperación Objetivo. Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.
- WRT (Work Recovery Time): Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

13.3. METODOLOGÍA DEL ANÁLISIS DE IMPACTO DEL NEGOCIO

La metodología del Análisis de Impacto del Negocio, consiste en definir una serie de pasos interactivos con el objeto de identificar claramente los impactos de las interrupciones y tomar decisiones respecto a aquellos procesos que se consideran críticos para la organización y que afectan directamente el negocio ante la ocurrencia de un desastre, estos pasos se muestran en esta ilustración:

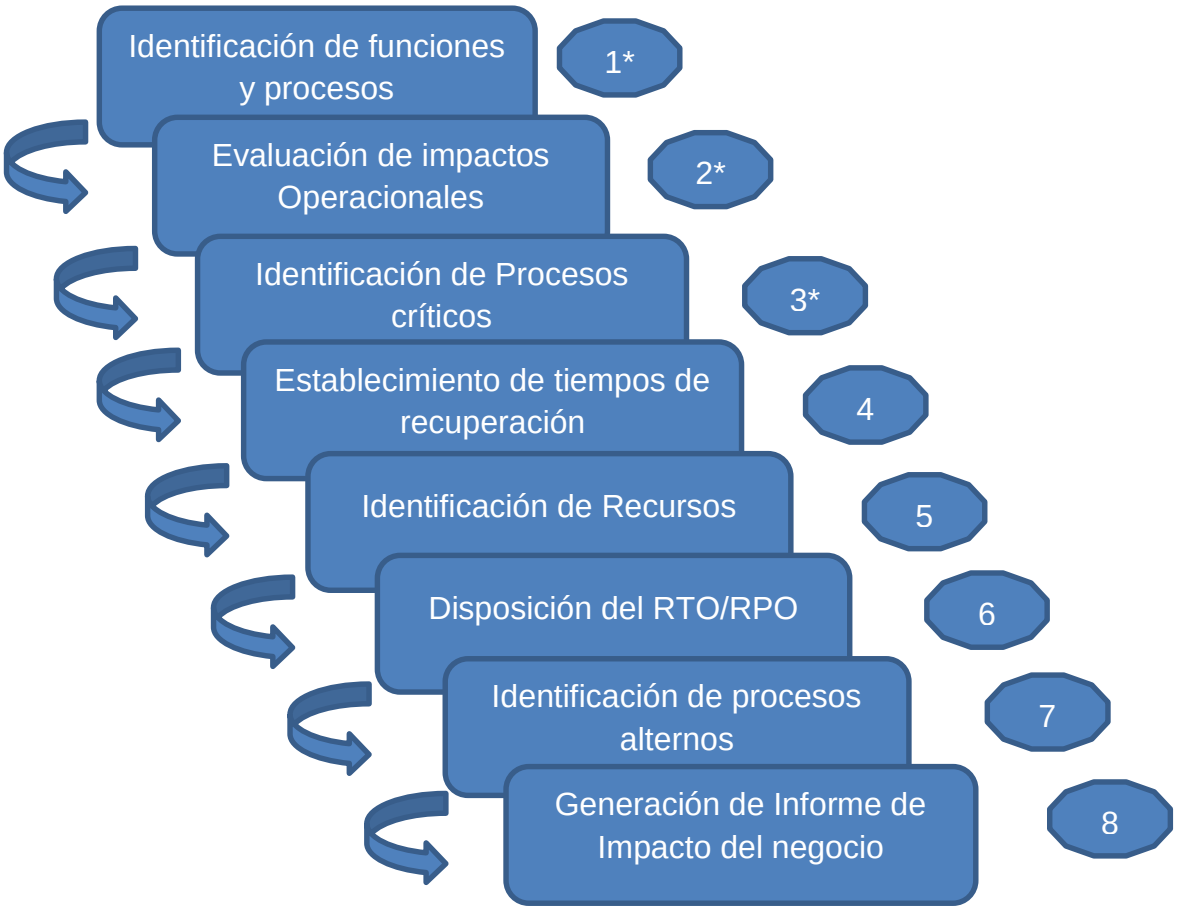

Figura 1. Metodología del Análisis de Impacto del Negocio

13.3.1. Identificación de Funciones y Procesos

En este paso se identifican las funciones del negocio útiles para apoyar la misión y los objetivos a alcanzar en el Sistema de Gestión de Seguridad de Información de la Entidad.

Este punto tiene como resultado generar un listado de roles y procesos, que sirven de análisis para el cumplimiento de los siguientes pasos del BIA.

13.3.2. Evaluación de Impactos Operacionales

Teniendo en cuenta los elementos operacionales de la organización, se requiere evaluar el nivel de impacto de una interrupción dentro de la Entidad.

El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; 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 el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.
- Nivel B: La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.
- Nivel C: La operación no es una parte integral del negocio.

La tabla siguiente muestra un ejemplo con los niveles de criticidad en una Entidad, que contempla un sistema de tolerancia a fallas por horas, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema; por lo tanto la tolerancia a fallas es muy importante en aquellos sistemas que deben funcionar todo el tiempo.

Categoría (Función del Negocio)	Proceso (Servicios)	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	SAN (Storage Área	A	3	Capacidad de

Almacenamiento	Network)			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 comunicaciones
Recurso Humano	Internos/externos	C	3	Profesionales encargados de administrar las infraestructuras de la Entidad

Tabla 1. Valoración Operacional por niveles de criticidad

13.3.3. Identificación de Procesos Críticos

La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones, según esta tabla.

Valor	Interpretación del proceso crítico
A	Crítico para el Negocio, la función del negocio no puede realizarse
B	No es crítico para el negocio, pero la operación es una parte integral del mismo.
C	La operación no es parte integral del negocio.

Tabla 2. Identificación de procesos críticos

13.3.4. Establecimiento de Tiempos de Recuperación

Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios; el entendimiento de estos componentes es fundamental para comprender el BIA. Los tiempos de recuperación de describen a continuación:

Tiempo de Recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

Tabla 3. Descripción de tiempos de recuperación

Una vez identificados los procesos críticos del negocio, función que hace parte del análisis de los impactos operacionales, se procede a identificar el MTD, que corresponde al tiempo máximo de inactividad que puede tolerar una organización antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso (servicio). Esto quiere decir que si por ejemplo un proceso tiene un periodo máximo de tiempo de inactividad (MTD) de un (1) día, este debe tener mayor prioridad para iniciar el evento de recuperación, en razón al poco tiempo de tolerancia de la inactividad, frente a otros que tienen mayor tolerancia.

El siguiente ejemplo ilustra esta situación:

Categoría (Función Crítica del Negocio)	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
Sistemas de Almacenamiento	SAN (Storage Área Network)	1 día	2
Comunicaciones	Servicio WiFi	1 día	2
Cuartos de Máquinas	Centro de Datos	0.5 día*	1
Soporte Informático	Equipo PC de usuario	3 días	4

*: Corresponde al tiempo de inactividad del proceso crítico del negocio, que tomaría menos de un (1) día de tolerancia de inactividad del servicio.

13.3.5. Identificación de Recursos

Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto es clave en este punto, la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomas acciones para medir el impacto del negocio de las Entidades.

La siguiente tabla representa un ejemplo de identificación de recursos críticos de Sistemas de Tecnologías de Información.

Categoría (Función Crítica del Negocio)	Procesos Críticos (Servicios)	Identificación de recursos críticos de Sistemas TI
Aplicaciones	Sistema 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 usuarios con Portal Cautivo. Control de usuarios locales Vs Invitados.
Cuartos de Máquinas	Centro de Datos	Control de operaciones de Servidores, Equipos de Comunicaciones, Sistemas de Almacenamiento, Sistemas de Backups, Aire Acondicionado, Acometida Eléctrica.

Tabla 5. Identificación de recursos críticos de Sistemas TI

13.3.6. Disposición de los RTO/RPO (Recovery Time Objective / Recovery Point Objective)

- RTO: Tiempo de Recuperación Objetivo: Asociado con la restauración de los recursos que han sido alterados de las Tecnologías de la Información; comprende el tiempo disponible para recuperar recursos alterados.

  Adicionalmente, se aplica el WRT, es decir el tiempo que es requerido para completar el trabajo que ha estado interrumpido con el propósito de volverlo a la normalidad.

La siguiente tabla muestra un ejemplo de valores RTO/WRT para el proceso crítico de la operación del Centro de Datos de una organización.

Categoría (Función Crítica del Negocio)	**Procesos Críticos (Servicios)**	**Identificación de recursos críticos de Sistemas TI**	**Tiempo de Recuperación Objetivo – RTO**	**Tiempo de Recuperación de Trabajo – WRT**
Cuartos de Máquinas	Centro de Datos	Control de operaciones de Servidores. Sistemas de Almacenamiento. Sistemas de Backups. Aire Acondicionado Acometida Eléctrica	1 día 0.5 día 1.5 días 1 día 0.5 día	1 día 0.5 días 1 día 0.5 día 0.5 día

Tabla 6. Valores RTO y WRT por cada proceso crítico

- RPO: Punto de Recuperación Objetivo: Este punto es importante para determinar por cada uno de los procesos críticos (servicios), el rango de tolerancia que una Entidad puede tener sobre la pérdida de información y el evento de desastre.

13.3.7. Identificación de Procesos Alternos

La identificación de procesos alternos hace posible que los procesos del negocio puedan continuar operando en caso de presentarse una interrupción; para ello es oportuno que las Entidades tengan métodos alternativos de manera temporal que ayuden a superar la crisis que ha generado una interrupción; por lo tanto para cada proceso crítico que se establezca (en los servicios), se debe poseer un procedimiento manual de continuidad del servicio.

13.3.8. Generación de Informe de Impacto del Negocio

En este punto es necesario presentar un informe de impacto de negocio que corresponde a la guía para el BIA con los siguientes resúmenes:

- Listado de procesos críticos
- Listado de prioridades de sistemas y aplicaciones
- Listado de tiempos MTD, RTO y RPO
- Listado de procedimientos alternos.

13.4. GESTIÓN DEL RIESGO

Ante la posible materialización de algún evento que ponga en riesgo la operatividad de la Entidad y con el fin de establecer prioridades para la mitigación de los riesgos, se hace necesario disponer de metodologías para su evaluación.

La metodología del plan de continuidad del negocio, determina los diversos escenarios de amenazas de una Entidad, el cual permite desarrollar las estrategias de continuidad y los planes para reanudar los servicios que estaban en operación.

La gestión del riesgo debe contemplar el “cálculo del riesgo, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia .

A pesar de la existencia de diversidad de métodos es recomendable iniciar con los más sencillos, que forman parte de lo que denominamos análisis previos. Una primera aproximación es la de establecer un conjunto de causas que pueden generar dificultades, tales como:

Riesgos Tecnológicos:

- Fallas en el Fluido Eléctrico.
- Sabotaje Informático.

- Fallas en el Centro de Datos.
- Problemas Técnicos.
- Fallas en equipos tanto de procesamiento, telecomunicaciones como eléctricos.
- Servicios de Soporte a Sistemas de Producción y/o Servicios.

Riesgos Humanos:

- Robos.
- Acto Hostil.
- Marchas, mítines.
- Artefactos explosivos.
- Problemas organizacionales (huelgas, leyes aceptadas por el congreso, regulaciones gubernamentales, leyes internacionales)
- Problemas de terceros involucrados en la producción o soporte a un servicio.
- Problemas con los proveedores de insumos o subproductos.

Desastres Naturales:

- Sismos
- Tormentas Eléctricas
- Incendios
- Inundaciones

13.5. CLASIFICACIÓN DE ESCENARIOS DE RIESGO

A fin de conocer con precisión los riesgos potenciales de la prestación de servicios de tecnologías de la información en las Entidades, es recomendable clasificar los posibles escenarios de los riesgos potenciales y describir su nivel de impacto por cada función crítica del negocio. La siguiente tabla describe un ejemplo de esta clasificación.

Categorías	Escenarios	Descripción Impacto
Red Eléctrica	Fallas en el fluido eléctrico red normal (no regulada)	Fallas del servicio eléctrico de la entidad que afecta equipos eléctricos normales.
	Fallas en el Fluido Eléctrico red regulada	Fallas en los servicios de Tecnología de Información.

Red Datos, Internet y Seguridad	Problemas dispositivos Red: Falla Parcial	Falla temporal de los servicios de TI de todo un componente por limitación en la comunicación.
	Problemas dispositivos Red: Falla Total	Falla general de los servicios de TI de todos los componentes por ausencia en las comunicaciones
	Problemas en los Dispositivos Seguridad: Falla Parcial	Falla parcial de los servicios de TI de todos los componentes que tiene que ver con elementos de seguridad de TI (Elementos de Hardware Software) y ausencia de políticas y controles de TI.
	Problemas en los Dispositivos Seguridad: Falla Total	Falla general de los servicios de TI de todos los componentes que tiene que ver con elementos de seguridad de TI (Elementos de Hardware, Software) y ausencia de políticas y controles de TI.
	Ausencia servicio del canal de Internet Última Milla: Total	Falla general de los servicios de TI de todos los componentes involucrados en la conexión de última milla por ausencia en la comunicación. No acceso a internet; impacto directo con el proveedor del servicio.
	Perdida conectividad hacia el NAP Colombia: Parcial	Falla parcial de los servicios de TI por ausencia en la conexión hacia el NAP Colombia. Acceso parcial a la red de internet por parte del proveedor del servicio.
Hardware distribuido	Problema de Hardware de Servidores: Falla Total	Falla total de los servicios de los sistemas de información que usan la plataforma de servidores.
	Problema HW Servidores: Falla Parcial	Degradación de la calidad (lentitud) de los servicios de los sistemas de información que usan la plataforma de servidores.
	Problemas en sistema Almacenamiento	Falla de los servicios de los sistemas de Información que usan la plataforma de almacenamiento de información.
	Problemas Hardware de Servidores	Falla de los servicios de los sistemas de información que usan la plataforma de servidores.
Aplicaciones infraestructura distribuida	Problemas Capa de Aplicaciones	Falla o degradación del servicio prestado en el sistema de información afectado por problemas en las aplicaciones.
	Problemas Capa Media	Falla o degradación de la aplicación soportada por las herramientas de software y el sistema de almacenamiento masivo de datos – SAN, por tanto se puede presentar degradación o ausencia del servicio prestado por sistema de información afectado por problemas de la capa media.

	Problemas Capa de Bases de Datos	Falla o degradación de las aplicaciones soportadas por las herramientas y motores de Base de Datos, por tanto se puede presentar degradación o ausencia del servicio prestado por los sistemas de información afectados por problemas de la capa de base de datos.
Recurso Humano	Ausencia de funcionarios, incapacidades y rotación	Disminución de capacidad de atención a los clientes y usuarios, lentitud en la atención a requerimientos e incidentes, como también el retraso en la puesta en marcha de nuevos servicios.
	Errores humanos en operación	Contempla desde la degradación de un servicio hasta la pérdida del mismo, como también la ejecución de procedimientos de manera errada que de cómo resultado la pérdida del servicio de uno o todos los sistemas de información del proyecto.
Desarrollo de aplicaciones	Falla en la aplicación por desarrollo no adecuado de parte de terceros	Contempla la degradación de un servicio por fallas en la funcionalidad de los sistemas de información.
	Falla en la aplicación por desarrollo no adecuado por parte de la Entidad	Contempla la degradación de un servicio por fallas en la funcionalidad en los sistemas de información de la Entidad.

Tabla 7. Clasificación por categorías de escenarios de riesgo

13.6. METODOLOGÍA DEL RIESGO

Es importante determinar los riesgos a los que están enfrentadas las infraestructuras de TI de las organizaciones con base en la identificación tanto de amenazas como de vulnerabilidades.

13.6.1. Identificación de amenazas

Las amenazas son todos los factores que pueden generar daños dentro de la organización y que requieren ser identificados, por lo tanto las amenazas pueden ocasionar riesgos al aprovechar las vulnerabilidades y permitir la afectación de los activos de información.

Las amenazas pueden ser catalogadas dentro de los siguientes tipos:

- Seguridad interna y externa
- Ambiente físico (Instalaciones)
- Protección de activos de información

- Protección de la información
- Protección de recursos humanos

La identificación de amenazas que pueden afectar un activo de información puede clasificarse de la siguiente manera:

- Amenazas a las instalaciones: Caídas de energía, daños de agua, fallas mecánicas, pérdidas de acceso.
- Amenazas tecnológicas: Fallas en las comunicaciones, fallas en el software, fallas en el hardware, virus, spam, hacking, pérdida de datos, entre otros.
- Amenazas naturales: Inundaciones, sismos, huracanes, tormentas, incendios, entre otros.
- Amenazas sociales: Protestas, sabotajes, motines, asonadas, terrorismos, vandalismos, entre otros.
- Amenazas humanas: Problemas de transporte, huelgas, epidemias, pérdida de personal clave.

13.6.2. Identificación de vulnerabilidades

Las vulnerabilidades son las debilidades de seguridad de Información asociadas a los activos de información y se hacen efectivas cuando una amenaza la materializa en los sistemas de información de las Entidades.

Estas no son causa necesariamente de daño, sino que son condiciones que pueden hacer que una amenaza afecte a un activo de información en particular. Para cada amenaza identificada en el punto anterior se debe realizar un análisis de riesgo para identificar la(s) vulnerabilidad(es).

La siguiente tabla muestra un ejemplo de las amenazas y vulnerabilidades por cada Activo de Información.

Sistema TI	Activo de Información	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia	Impacto
Servicio Web de la Entidad	Página Web Entidad	Defacement (desfiguración página web)	Mal diseño del sitio web	Medio	Alto
Servicio de correo electrónico	Correo electrónico Exchange	Virus, listas negras	Carencia de parches de seguridad	Alto	Alto
Sistema de Almacenamiento	SAN o NAS	Falla en el fluido eléctrico	No hay buena acometida eléctrica	Bajo	Alto
Sistema de Base de datos	Bases de datos interna	Usuario no autorizado	Mala configuración	Bajo	Alto

Servicio Red de comunicaciones	Equipos Switches de la Entidad	Falla de comunicaciones	Bloqueo de puertos	Medio	Alto

Tabla 8. Amenazas y Vulnerabilidades por Activo de Información

14. CONCLUSIONES

El análisis de impacto del negocio – BIA, hace parte importante del plan de continuidad del negocio y a su vez presenta consideraciones importantes para la gestión del riesgo dentro de las organizaciones, que establecen un marco de políticas, procedimientos y estrategias que permiten asegurar que las operaciones de carácter crítico puedan ser mantenidas y recuperadas a la mayor brevedad posible, en caso de fallas graves dentro de los sistemas de información y las comunicaciones.

En este sentido, las distintas organizaciones deben considerar que el BIA es un instrumento operacional muy importante que permite la toma de decisiones en momentos críticos de la organización en virtud del cese de operaciones debido a una situación anómala presentada. De esta manera dicho instrumento, contribuye a identificar las operaciones y servicios considerados críticos dentro de la entidad, que contribuyen a restablecer en el menor tiempo posible los servicios y operaciones con el apoyo de un plan de continuidad del negocio de las entidades.

Corroborando lo anterior, el análisis de impacto del negocio - BIA, podrán ayudar a identificar dentro del marco de la seguridad de la información, las vulnerabilidades potenciales de la organización, podrá delimitar las actividades críticas que afectan el negocio y ayudará a las entidades a definir los planes adecuados de recuperación de los servicios que afectan el objeto del negocio; de otro lado las entidades podrán tener mayor información sobre el estado de los procesos contribuyendo favorablemente a mejorar la competitividad y proyectar estrategias adecuadas para una recuperación exitosa de la información.

Finalmente, es responsabilidad de las empresas del gobierno disponer de un recurso humano suficientemente capacitado y especializado, capaz de enfrentarse a los eventos inesperados que atentan con la operatividad, seguridad y disponibilidad de los sistemas de información y las comunicaciones.

15. BIBLIOGRAFIA

- Alexander, A., (2007).Diseño de un Sistema de Gestión de Seguridad de Información, óptica ISO 27001:2005, Alfaomega.
- Hiles, A., (2004). Bussiness Continuity Best Practices, Connecticut: Rothstein Associates, Inc.
- ISO/IEC 27001:2006, Norma Técnica NTC-ISO/IEC Colombiana, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.
- ISO/IEC 27035, Information Technology. Security Techniques. Information Security incident imanagement
- ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary
- ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements
- ISO/IEC 27002, Information Technology. Security Techniques. Code of practice for information security management
- ISO/IEC 27005, Information Technology. Security Techniques. Information security risk Management
- ISO 22301:2012, Sistemas de Gestión y Continuidad del Negocio.
- ISO 27031 – DE198-13, Tecnología de la Información, Técnica de Seguridad, Directrices para la continuidad del negocio.