Guía para realizar el Análisis de Impacto de Negocios BIA

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No 11

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

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	19/01/2015	Versión inicial del documento
2.0.0	12/05/2015	Versión ajustada del documento

TABLA DE CONTENIDO

PÁG.

LISTA DE TABLAS

PÁG.

1. DERECHOS DE AUTOR

2. GLOSARIO

Activo

En relación con la seguridad de la información se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Amenazas

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis del impacto del negocio

Proceso del análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas. (ISO 22301)

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701)

Ciberespacio

Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española).

Plan de Continuidad de Negocio

Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel pre-definido de operación debido a la interrupción. (ISO 22301).

Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Trazabilidad

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

3. INTRODUCCIÓN

La Gestión del plan de impacto del negocio en las entidades del estado debe responder a una variedad de políticas de restablecimiento de actividades y servicios que apoyen el normal funcionamiento de las infraestructuras de TI y minimicen al máximo las interrupciones o fallas presentadas dentro de la organización.

Las entidades deben permanentemente monitorear y reconocer las amenazas más importantes de incidentes que afecten la normal operatividad de los servicios y los sistemas, de tal manera que se debe garantizar la continuidad del negocio a través de mecanismos de recuperación previamente probados y ajustados y que respondan en el menor tiempo posible a las soluciones de los problemas de interrupción generados.

El fin de la implementación del plan de continuidad de TI, es la protección y recuperación de los servicios críticos que se vean afectados por desastres naturales o interrupciones del servicio ocasionadas ya sea por los sistemas de información y comunicación o ya sean por el hombre en virtud de acciones involuntarias o para beneficio propio.

Así mismo, el análisis de impacto de negocios debe convertirse en una herramienta para minimizar los riesgos de indisponibilidad de los servicios e infraestructuras de TI, que afectan las operaciones regulares de las organizaciones, por lo consiguiente debe formar parte de un sistema de gestión de riesgos, que sea utilizado como mecanismo de control para ejecutar tareas de monitoreo de crisis, planes de contingencia, capacidad de marcha atrás y prevención y atención de emergencias.

Las entidades deben contar con un plan de continuidad de Tecnología de Información, que le permita a la organización continuar con sus operaciones, en caso de presentarse fallas o inconvenientes en sus sistemas que le impidan el normal funcionamiento de los servicios de TI, de esta manera, la correcta implementación del plan deberá permitir restaurar en el menor tiempo posible las operaciones de la entidad.

El análisis de impacto del negocio – BIA por sus siglas en inglés (*Bussiness Impact Analysis)*, está determinado por la construcción de un plan de continuidad del negocio para cada organización, que le permita a cada entidad continuar funcionando a pesar de un desastre ocurrido; el documento generado en este análisis deberá cumplir con lo expuesto en los requerimientos de la ISO/IEC 27001,

de este modo el documento *BIA* debe ser validado e implementado bajo las directrices de cada organización,

Se requieren planear las acciones necesarias durante el período en que la infraestructura de TI se encuentra inactiva y en proceso de recuperación y reanudación de los servicios para priorizar cuales actividades y servicios deben entrar en operación inmediatamente dentro de la entidad.

Finalmente, es necesario tener en cuenta que los responsables del negocio deben conocer la importancia de tener una inversión de TI planeada que permita innovar tecnológicamente y que responda adecuadamente a los problemas generados por la interrupción de los servicios y permita que las empresas puedan aplicar exitosamente los criterios de recuperación y reanudación de las operaciones del negocio.

4. OBJETIVO GENERAL

Disponer de un documento guía por medio del cual las Entidades del estado puedan consultar los lineamientos de seguridad ante situaciones de emergencia a fin de mitigar el impacto producido por la interrupción de los servicios de alta criticidad que afectan sensiblemente las operaciones del negocio.

5. FASES DEL PLAN DE CONTINUIDAD DEL NEGOCIO

El Plan de continuidad del negocio, se conforma de un conjunto de directrices y procedimientos plasmados en un documento técnico, para que cada entidad pueda tomar las acciones pertinentes con miras a la recuperación y restablecimiento de los servicios e infraestructuras de TI interrumpidas por situaciones de desastre o emergencias ocurridas en cualquier instante dentro de las organizaciones.

El análisis de impacto del negocio como parte del plan de continuidad del negocio, debe entenderse como un marco conceptual sobre el cual las entidades deben planear integralmente los alcances y objetivos, que permiten proteger la información, en todas sus áreas críticas.

Las entidades deben establecer un análisis de impacto del negocio, que este alineado con el Plan General de Continuidad del Negocio de la Entidad; este debe tener una estrategia de continuidad de TI, que contenga los objetivos globales de la entidad, con respecto a las dimensiones de disponibilidad de datos, infraestructura tecnológica y recurso humano.

Para desarrollar el plan de continuidad del negocio de TI se debe tener en cuenta:

- Diseñar una estrategia de continuidad de los servicios de TI, que tenga como base la reducción del impacto de una interrupción en los servicios críticos de TI del negocio, este debe estar difundido, aprobado y respaldado por los directivos de la entidad.
- Realizar un análisis e identificación de recursos críticos de TI vitales, de esta manera se establece una estrategia que genere prioridades en caso de presentarse una o varias situaciones que causen interrupciones.
- Establecer procedimientos de control de cambio, que permita asegurar que el plan de continuidad de TI, se encuentre actualizado y permita afrontar las amenazas que traen consigo las nuevas tendencias tecnológicas sin perder el alcance de los requerimientos de la Entidad.
- Elaborar un plan de pruebas de continuidad de TI, que permita verificar y asegurar que los sistemas de TI, puedan ser recuperados de forma segura

y efectiva, atendiendo y corrigiendo errores, que atenten contra la disponibilidad de las operaciones.

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

5.1 FASE DE ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)

La fase de 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.

Como se ha venido mencionando, 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.

Al final 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.

5.1.1 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)[1], 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.

[1] Hiles, Andrew. 2004, Bussines Continuity: Best Practices, Connecticut: Rothstein Associates, Inc.

5.1.2 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:[2]

- **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.

5.1.3 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:

[2] Alexander, Alberto. 2007., Diseño de un Sistema de Gestión de Seguridad de Información, pág. 74.

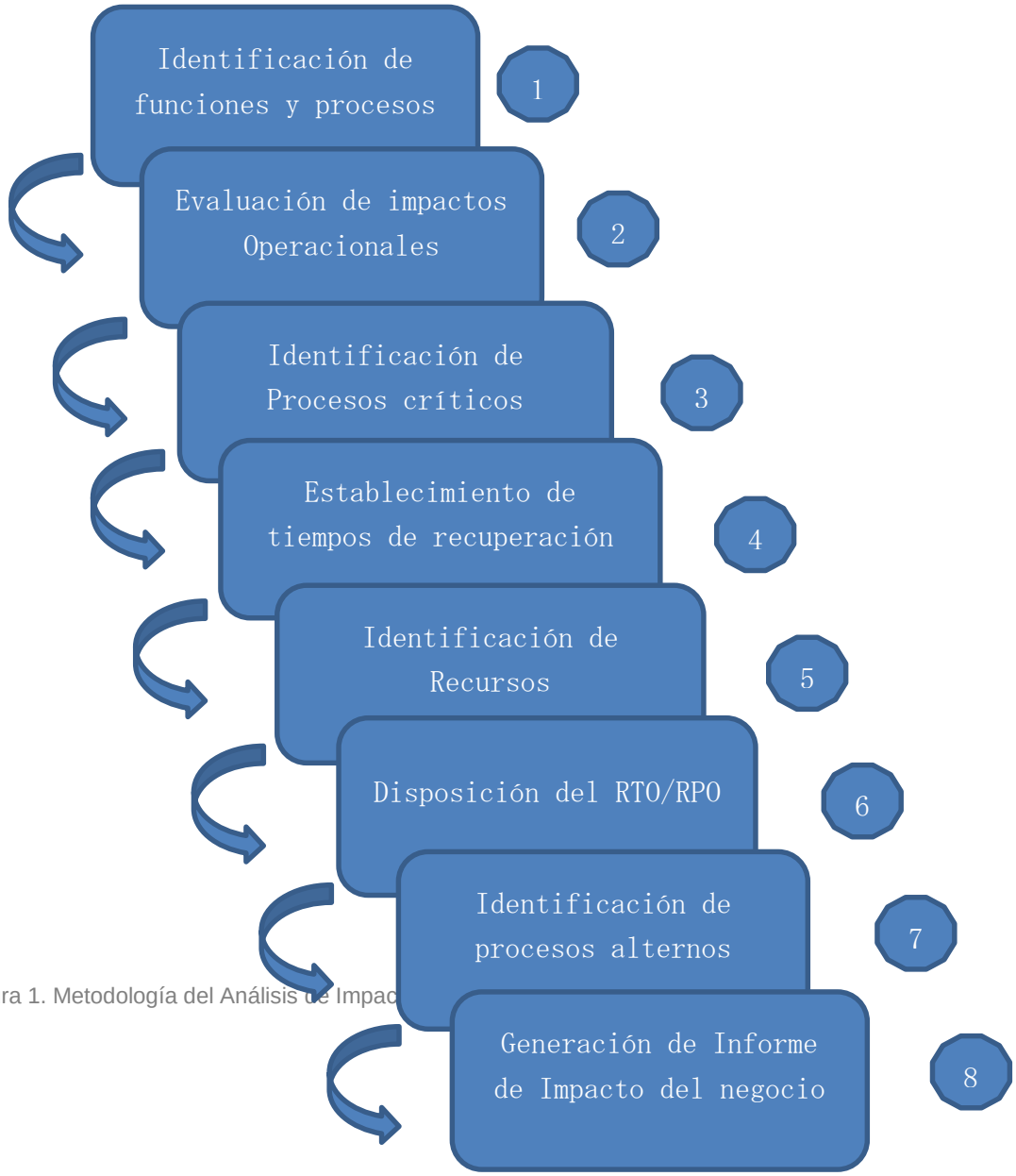

Figura 1. Metodología del Análisis de Impac

5.1.3.1 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*.

5.1.3.2 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 Almacenamiento	SAN (Storage Área 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 comunicaciones
Recurso Humano	Internos/externos	C	3	Profesionales encargados de administrar las infraestructuras de la Entidad

Tabla 2. Valoración Operacional por niveles de criticidad

5.1.3.3 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

5.1.3.4 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

Tabla 4. Prioridades de Recuperación de procesos críticos

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

5.1.3.5 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

5.1.3.6 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.

5.1.3.7 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.

5.1.3.8 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.

6. FASE DE 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[3].

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.

[3] Hiles, Andrew. Business Continuity: Best Practices. Rothstein Associates, Inc. 2004 Connecticut.

Desastres Naturales:

- ✓ Sismos
- ✓ Tormentas Eléctricas
- ✓ Incendios
- ✓ Inundaciones

6.1 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

6.2 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.

6.2.1 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.

6.2.2 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[4]

4 La probabilidad de ocurrencia e impacto de amenazas y vulnerabilidades está sujeta a los diferentes escenarios o campos de aplicación en las entidades, por lo tanto la tabla anterior muestra solo algunos ejemplos de esta situación.

7. 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.

8. 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.