Comfamiliar RISARALDA

POLÍTICAS INSTITUCIONALES

POLÍTICA CONTINUIDAD DEL NEGOCIO

Vigilado Supersubsidio

Introducción:
La Política de Continuidad del Negocio permite a la entidad prevenir, protegerse y reaccionar ante incidentes de seguridad que se puedan presentar y que puedan impactar en las actividades de la entidad. Esta Política describe los principales procesos y tareas que permiten a Comfamiliar Risaralda recuperarse en el caso de que se presente un incidente, garantizando poder dar una respuesta la cual proteja las principales actividades de la entidad.

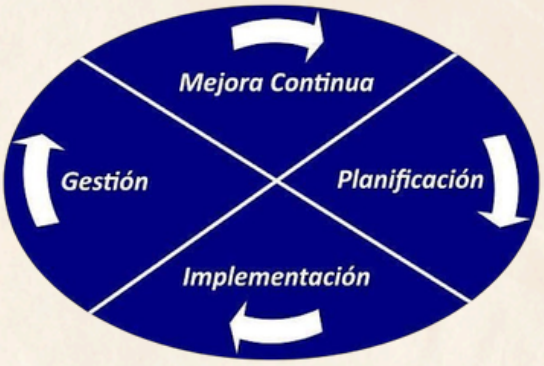
Objetivo:
El presente documento tiene como objetivo principal definir el Plan de Continuidad de Negocio de Comfamiliar Risaralda, el cual define el procedimiento a seguir en el caso de que se lleguen a presentar incidentes que afecten la continuidad de las actividades de la entidad, y así mismo el procedimiento que se debe realizar como respuesta, permitiendo proteger los intereses de la entidad, y asegurar una pronta recuperación en los servicios críticos.

Alcance:
El presente plan abarca a todos los procesos de Comfamiliar Risaralda y deberá ser cumplido por todos los funcionarios, proveedores o terceros que tengan acceso a los sistemas de información e instalaciones físicas de la entidad.

Declaración de Compromiso:
Comfamiliar Risaralda se compromete a implementar la Política de Continuidad del Negocio, la cual permite a la entidad prevenir, protegerse y reaccionar ante incidentes que puedan impactar sobre el negocio.

Marco de Actuación:

Gestión de Continuidad del Negocio:



La ilustración muestra el Modelo de Operación de Seguridad y Privacidad de la Información, del cual, para el Plan de Gestión de Continuidad, solo tendremos en cuenta las fases de:

- Planificación.
- Implementación.
- Gestión.

Planificación
En este componente, se debe definir la estrategia metodológica, que permita establecer las 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.

Implementación
Este componente le permitirá a la Entidad llevar a cabo 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:

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

Gestión
Este componente le permitirá a la Entidad evaluar el desempeño y la eficacia de la implementación, a través de instrumentos que determinen 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.

Mejora continua
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.

Análisis de Impacto del Negocio (BIA):
Comfamiliar Risaralda deberá disponer de un documento que permita identificar todas las áreas críticas de la entidad para garantizar la medición de la magnitud del impacto operacional y

financiero de la entidad, al momento de presentarse una interrupción. Este análisis del impacto del negocio clasificará 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.

Este análisis de impacto del negocio es un informe con el detalle de las funciones y procesos críticos de Comfamiliar Risaralda. El cual contiene la información básica de los recursos requeridos y los tiempos de recuperación para que la entidad pueda poner en funcionamiento los servicios y por ende la continuidad del negocio. Para esto, Comfamiliar Risaralda implementará una metodología del análisis de impacto del negocio, ya sea proporcionado por la MINTIC o por otro ente especializado, para poder identificar los impactos de las interrupciones y tomar decisiones respecto a los procesos considerados críticos para la entidad y que afectan directamente a la continuidad de este. Realizando los siguientes pasos:

- Identificación de funciones y procesos.
- Evaluación de impactos operacionales.
- Identificación de procesos críticos.
- Establecimiento de tiempos de recuperación.
- Identificación de recursos.
- Disposición del RTO/RPO.
- Identificación de procesos alternos.
- Generación de informe de impacto del negocio.

Gestión y Respuesta Ante Incidentes:

Comfamiliar Risaralda realizará ejercicios de pruebas de penetración y simulación de ataques los cuales permitirán a la entidad obtener un balance de posibles configuraciones inadecuada en las aplicaciones de los sistemas informáticos y vulnerabilidades de seguridad en los sistemas de información e infraestructura tecnológica de la entidad, y con esto realizar intervenciones adelantadas que solucionen estas brechas y que permitan mitigar el riesgo en los sistemas.
La realización de pruebas a las defensas de la entidad permite:

- Garantizar que en situaciones que se presenten problemas de seguridad o fallos en los sistemas, la organización pueda recuperarse en los tiempos establecidos, permitiendo la reanudación y continuidad de las actividades de la entidad.
- Incrementar la cohesión del personal implicado ante un posible incidente.
- Evaluar los procesos, herramientas y capacidad de los sistemas de información al momento de responder ante ciberataques.

En el documento **“Test de Penetración”** de Comfamiliar Risaralda se define la metodología completa que se implementa para realizar las pruebas a los sistemas de información de la entidad.

Estrategia de Respaldo:
Comfamiliar Risaralda cuenta con un Plan de contingencia el cual describe detalladamente los servicios tecnológicos de la entidad y la descripción de la contingencia de cada uno de ellos en caso de que se presente algún fallo.
Ver el documento: **“1-OD-073 Plan de Continuidad Sistemas V4”.**

Normatividad Aplicable:

ISO/IEC 27001:2005: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de

la seguridad de la información.

Responsables de Gestión:

Unidad de Sistemas:
Departamento dentro de la organización que vela por los procesos relacionados con utilización y manejo de computadoras, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

Documentos Relacionados:

- 1-OD-073 Plan de Continuidad Sistemas V4.
- Test de penetración.
- Control de Gestión de Incidentes.

Conceptos (Glosario):

ANÁLISIS DE IMPACTO AL NEGOCIO (BIA): proceso del análisis de actividades, las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas. [Fuente: ISO 22300].

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.

PLAN DE CONTINUIDAD DE NEGOCIO: procedimientos documentados que guían orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación debido una vez presentada / tras la interrupción.

PUNTO OBJETIVO DE RECUPERACIÓN (RPO): punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra.

TIEMPO OBJETIVO DE RECUPERACIÓN (RTO): período 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.

la seguridad de la información.

Responsables de Gestión:

Unidad de Sistemas:
Departamento dentro de la organización que vela por los procesos relacionados con utilización y manejo de computadoras, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

Documentos Relacionados:

- 1-OD-073 Plan de Continuidad Sistemas V4.
- Test de penetración.
- Control de Gestión de Incidentes.

Conceptos (Glosario):

ANÁLISIS DE IMPACTO AL NEGOCIO (BIA): proceso del análisis de actividades, las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas. [Fuente: ISO 22300].

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.

PLAN DE CONTINUIDAD DE NEGOCIO: procedimientos documentados que guían orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación debido una vez presentada / tras la interrupción.

PUNTO OBJETIVO DE RECUPERACIÓN (RPO): punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra.

TIEMPO OBJETIVO DE RECUPERACIÓN (RTO): período 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.