



SEGURIDAD DE LA

INFORMACIÓN

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

El Marco de Ciberseguridad es un conjunto de requisitos (requisitos normativos y buenas prácticas) que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.

Usted es libre de copiar, distribuir, comunicar y difundir públicamente este documento, así como hacer obras derivadas, siempre y cuando tenga en cuenta citar la obra de forma específica.

Política de Continuidad de las operaciones y recuperación ante desastres.

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 1.0 | **Categoría** | Política |
| **Última actualización** | 27/06/2022 | **Estado** |  |

# Objetivo

Planificar y gestionar la continuidad operativa de los procesos críticos de la organización ante la eventualidad de ocurrencia de eventos anormales que afecten personas, oficinas y edificios, tecnología, información y proveedores, provocando la disrupción de las operaciones.

Responder adecuada y oportunamente ante estos eventos, asegurando la preservación de datos y funciones esenciales.

Ante la eventualidad de ocurrencia de este tipo de eventos, lograr operar en contingencia durante el tiempo que sea necesario, afectando lo menos posible los servicios, y conseguir una recuperación ante desastres que permita el restablecimiento de las operaciones de la organización a su situación normal en plazos razonables y aceptables.

Establecer las instancias de revisión y mejora de esta política, los planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP), y sus procedimientos operativos.

# Alcance

Esta política aplica a todos los procesos críticos de la organización, los recursos que se utilizan para su ejecución, la información que éstos generan o usan, y las instalaciones donde se desarrollan.

# Responsabilidades

**Dirección** es responsable por generar las condiciones adecuadas para la ejecución y comunicación de la presente política, así como de establecer el alcance para su aplicación. Es responsable de la aprobación de los planes de respuesta, de la designación de un vocero para las comunicaciones externas e internas en ocasión de un incidente disruptivo, y de aprobar el contenido de dichas comunicaciones.

**Gerencias** de la organización son responsables por la identificación de los procesos críticos y los activos y sistemas que los soportan, así como de participar en la creación y pruebas del BCP y DRP. Son responsables de la realización de un análisis de impacto en el negocio (BIA), en el supuesto que los procesos críticos de sus áreas se vieran afectados.

**Equipo responsable de gestión de riesgos** es responsable por la identificación y evaluación de amenazas y vulnerabilidades, la determinación del riesgo y el impacto en la operativa de la organización en caso de ocurrencia.

**Comité de seguridad de la información** es responsable de revisar el plan de contingencia y de recuperación ante desastres, coordinar formalmente a los diferentes actores para la realización de las pruebas y revisar los informes de las pruebas para establecer el plan de mejora.

**Responsable de seguridad de la información** debe velar por el cumplimiento de la presente política. Es responsable por la definición y gestión del plan de contingencia y recuperación ante desastres. Es responsable de la definición de los diferentes equipos de contingencia y de la coordinación de éstos.

**Responsable de tecnología de la información** debe participar en la planificación técnica del plan de contingencia y recuperación en caso de desastres, en coordinación con el Responsable de Seguridad de la Información.

**Personal de la organización** debe cumplir con lo establecido en la presente política y debe participar, previa coordinación con las Gerencias, en las pruebas que se realicen al plan de contingencia y recuperación ante desastres.

# Políticas relacionadas

Política de respaldo
Política de gestión de riesgos
Política de gestión de activos

# Descripción

La Dirección de la organización entiende necesario contar con un plan formal de continuidad operativa y un plan de recuperación en caso de desastres ante eventos anormales, teniendo como premisas fundamentales la seguridad y protección de las personas, los recursos y la información.

El plan de continuidad operativa deberá considerar el riesgo de interrupción de actividades por eventos tecnológicos, humanos y naturales, originados por causas internas o externas, los que estarán debidamente documentados siguiendo lo establecido en la política de gestión de riesgos. El plan deberá definir la contingencia para los procesos críticos incluyendo ventanas de tolerancia, así como un plan de recuperación para el retorno a la operativa normal de la organización.

Anualmente se realizarán pruebas al plan de continuidad operativa y de recuperación en caso de desastres.

El Comité de Seguridad de la Información realizará la coordinación formal de las pruebas a los planes con todas las partes involucradas, facilitando la coordinación que deba realizar el Responsable de Seguridad de la Información. Éste será el encargado, en conjunto con los referentes de las Gerencias que sea necesario, de la ejecución de las pruebas al plan de contingencia y recuperación en caso de desastres, informar a la Dirección de la organización y al Comité de Seguridad de la Información del resultado de las mismas, registrar las lecciones aprendidas y confeccionar el plan de acción para la mejora.

# Cumplimiento

Se destaca que el incumplimiento de la presente política aumenta la exposición de la información y el riesgo de tener un incidente de seguridad de la información. Ante la verificación de un incumplimiento la Dirección podrá tomar las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento.

# Historial de revisiones

|  |  |  |
| --- | --- | --- |
| **Fecha de revisión** | **Responsable** | **Resumen de cambios** |
|  |  |  |

