

Departamento del Valle del Cauca  Gobernación	PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA GOBERNACION DEL VALLE DEL CAUCA	Código: PL-M11-P1-02
		Versión: 1
		Fecha de Aprobación:
		Página: 1 de 11

**PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA
GOBERNACION DEL VALLE DEL CAUCA.**

Secretaría de las Tecnologías de la Información y las Comunicaciones
Gobernación del Valle del Cauca

Contenido

INTRODUCCIÓN	2
OBJETIVOS	3
Objetivo General.....	3
Objetivos Específicos	3
ALCANCE	3
DEFINICIONES	4
CONTENIDO	7
ENTRENAMIENTO	10
FASES	10
Fase de Prevención.....	10
Fase de Administración	11

Departamento del Valle del Cauca  Gobernación	PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA GOBERNACION DEL VALLE DEL CAUCA	Código: PL-M11-P1-02
		Versión: 1
		Fecha de Aprobación:
		Página: 2 de 11

INTRODUCCIÓN.

El objetivo de un plan de continuidad de negocio y recuperación de desastre busca reducir las consecuencias de una interrupción a un nivel aceptable de ejecución y continuidad preestablecida y de recuperación de procesos e información para que el negocio continúe mientras se realizan las acciones de restauración necesarias.

La continuidad y la recuperación de procesos críticos de negocio identificados durante el Análisis de impacto del negocio (BIA) son los principales focos de un plan de continuidad.

La Gobernación del Valle del Cauca reconoce que existen amenazas significativas ante la posibilidad de la ocurrencia de un incidente o desastre que afecte la operación, como también la necesidad de recuperarse en el menor tiempo posible, garantizando la continuidad de la entidad.

La administración del Plan de Continuidad de Negocios y recuperación de desastres hace parte de las políticas de seguridad de la información, el Manual de políticas TIC y el PETIC que La Gobernación del Valle del Cauca implementa, para responder organizadamente a eventos que interrumpen la normal operación de sus procesos y que pueden generar impactos sensibles en el logro de los objetivos.

El Plan de Continuidad del Negocio y recuperación de desastres es una herramienta que mitiga el riesgo de no disponibilidad de los recursos necesarios para el normal desarrollo de las operaciones y como tal hace parte del Sistema de Gestión de Riesgo Operativo, ofreciendo como elementos de control la prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.

Departamento del Valle del Cauca  Gobernación	PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA GOBERNACION DEL VALLE DEL CAUCA	Código: PL-M11-P1-02
		Versión: 1
		Fecha de Aprobación:
		Página: 3 de 11

OBJETIVOS

Objetivo General

Asegurar que La Gobernación del Valle del Cauca esté preparada para responder a emergencias, recuperarse de ellas y mitigar los impactos ocasionados, permitiendo la continuidad de los servicios críticos para la atención de clientes y la operación.

Objetivos Específicos

Lograr un nivel de preparación frente a incidentes, problemas o siniestros que permita asegurar que puede proteger la integridad de las personas, la información y bienes de la entidad en forma adecuada, realizando una buena administración de la crisis.

- Minimizar la frecuencia de interrupciones de la operación de los procesos del negocio.
- Asegurar una pronta restauración de las operaciones afectadas por el evento.
- Minimizar las decisiones a tomar en caso de contingencia para evitar cometer errores.

ALCANCE

La administración del plan de continuidad y recuperación de desastres es una disciplina que prepara a la organización para poder continuar operando durante un incidente, siniestro o desastre, a través del cual contempla los lineamientos, metodologías y actividades para la recuperación y continuidad del negocio, y se realiza de acuerdo con las prioridades establecidas por la Entidad.

Departamento del Valle del Cauca  Gobernación	PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA GOBERNACION DEL VALLE DEL CAUCA	Código: PL-M11-P1-02
		Versión: 1
		Fecha de Aprobación:
		Página: 4 de 11

De la misma manera, el desarrollo de los planes de continuidad y recuperación de desastres se apoya en las capacidades con las que cuenta La Gobernación del Valle del Cauca para enfrentar situaciones que amenacen o afecten la integridad física de sus colaboradores e instalaciones, tales como el Plan de Manejo de Emergencias, los mecanismos de protección y seguridad, Manual de gestión de la comunicación en situaciones de crisis y los demás sistemas de gestión.

DEFINICIONES

Desastre: Un evento que puede interrumpir procesos críticos de negocio y degradar los servicios asociados al punto resultante de que el impacto financiero y operativo se vuelva inaceptable.

Existen niveles de desastre de acuerdo a su impacto, los cuales los vamos a repasar a continuación:

Nivel menor de desastre: Este tipo de desastre puede ocurrir de forma más frecuente durante el día a día operativo, comparado con un desastre de nivel intermedio y/o mayor. Se considera menor porque los efectos se encuentran normalmente aislados a pequeños procesos críticos de negocio.

Las unidades de negocio que dependen de ese proceso, normalmente pueden continuar operando.

Muchos de estos problemas son reanudados mediante políticas de la organización y dependencias que controlan los incidentes operativos y técnicos.

Nivel Intermedio de desastre: Este tipo de desastre puede ocurrir de forma menos frecuente pero con un mayor impacto que el de nivel menor. Este tipo de evento provoca una interrupción de operaciones normales de las empresas, pero no de todas las áreas críticas de la empresa.

Nivel Mayor de desastre: Las posibilidades de que este tipo de desastre ocurra son muy bajas, pero el nivel de impacto de interrupción y daño puede ser muy superior a los niveles medio y menor.

Departamento del Valle del Cauca  Gobernación	PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA GOBERNACION DEL VALLE DEL CAUCA	Código: PL-M11-P1-02
		Versión: 1
		Fecha de Aprobación:
		Página: 5 de 11

Cuando ocurre un evento de este tipo, la operativa es interrumpida e inaccesible para la mayoría de los procesos críticos definidos del negocio. Un ejemplo puede ser: Terremotos, incendios, sabotaje cibernético, casos fortuitos.

Administración del Plan de Continuidad de Negocios: Es un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estrategias, planes de respuesta y demás componentes y actores de la continuidad del negocio. Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca las personas, procesos de negocios, tecnología e infraestructura.

Incidente de Trabajo: Es un evento que no es parte de la operación estándar de un servicio y el cual puede causar interrupción o reducción en la calidad del servicio y en la productividad.

Problema de Continuidad de Negocio: Es un evento interno o externo que interrumpe uno o más de los procesos de negocio. El tiempo de la interrupción determina que una situación sea un incidente o un desastre.

Planes de contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

Plan de Continuidad de Negocio (PCN): Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

Plan de Recuperación de Desastres (DRP): Es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.

Análisis de Impacto del Negocio (BIA): Es la etapa que permite identificar la urgencia de recuperación de cada área, determinando el impacto en caso de interrupción.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, igual que los recursos necesarios para su uso.

Departamento del Valle del Cauca  Gobernación	PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA GOBERNACION DEL VALLE DEL CAUCA	Código: PL-M11-P1-02
		Versión: 1
		Fecha de Aprobación:
		Página: 6 de 11

Amenaza: Persona, situación o evento natural del entorno (externo o interno) que es visto como una fuente de peligro, catástrofe o interrupción. Ejemplos: inundación, incendio, robo de datos.

Vulnerabilidad: Es una debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la Institución. Ejemplos: Deficiente control de accesos, poco control de versiones de software, entre otros.

Riesgo: Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para la Entidad.

Frecuencia: Estimación de ocurrencia de un evento en un período de tiempo determinado. Los factores a tener en cuenta para su estimación son la fuente de la amenaza y su capacidad y la naturaleza de la vulnerabilidad.

Impacto: Es el efecto que causa la ocurrencia de un incidente o siniestro. La implicación del riesgo se mide en aspectos económicos, imagen reputacional, disminución de capacidad de respuesta y competitividad, interrupción de las operaciones, consecuencias legales y afectación física a personas. Mide el nivel de degradación de uno de los siguientes elementos de continuidad: Confiabilidad, disponibilidad y recuperabilidad.

Control: Es el proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo o potenciar oportunidades positivas.

Riesgo inherente: Es el cálculo del daño probable a un activo de encontrarse desprotegido, sin controles.

Riesgo residual: Riesgo remanente tras la aplicación de controles.

Departamento del Valle del Cauca  Gobernación	PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA GOBERNACION DEL VALLE DEL CAUCA	Código: PL-M11-P1-02
		Versión: 1
		Fecha de Aprobación:
		Página: 7 de 11

CONTENIDO

Para la Gobernación del Valle del Cauca el Plan de Recuperación de Incidentes y continuidad del negocio tiene como principales actividades, las siguientes:

- Proceso de superación de la emergencia
- Inicio de los procedimientos de Reanudación y Recuperación de los servicios afectados
- Reanudación y Recuperación de la totalidad de la operación en los lugares y bajo las condiciones que así definió la Secretaria de las TIC una vez concertado con las dependencias afectadas.

Estas tareas se realizan bajo lo establecido en las Normas ISO 27001 e ISO 22301.

El plan de continuidad y recuperación de desastres es una tarea dinámica, y se debe estar actualizando frecuentemente. Los actores que tienen en la Gobernación del Valle del Cauca en la definición del Plan son:

- El líder de programa de TI.
- El funcionario o contratista que realiza las actividades de soporte e infraestructura y se encuentra en segundo lugar bajo la línea jerárquica del Líder de programa de TI.
- El Equipo de Servicios Tecnológicos y eventualmente la mesa de ayuda de los sistemas de información.

Tareas y responsabilidades del equipo de servicios tecnológicos respecto a recuperación de desastres y continuidad del negocio, se ha definido que recae en el Líder de programa de TI, quien coordinará el plan de continuidad y recuperación de desastres, que tienen las competencias, habilidades y educación para desarrollar estas actividades de manera idónea, como lo establece su manual de funciones.

Entre las tareas desarrolladas se incluyen:

- Liderar la ejecución del Plan de continuidad recuperación de desastres, considerando como partes esenciales del plan, cada una de las actividades definidas para el retorno a la normalidad.

Departamento del Valle del Cauca  Gobernación	PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA GOBERNACION DEL VALLE DEL CAUCA	Código: PL-M11-P1-02
		Versión: 1
		Fecha de Aprobación:
		Página: 8 de 11

- Determinar las situaciones que activan el Plan de continuidad recuperación de desastres.
- Definir el personal que participara en el Plan de continuidad recuperación de desastres. En cualquier caso se define un responsable principal, y un responsable suplente para que, en caso de ausencia del principal, este asuma la recuperación de la operación.
- Programar y realizar la(s) prueba(s) del Plan de continuidad recuperación de desastres.
- Activar el equipo GRI (Grupo de Respuesta de Incidentes) para un incidente específico.
- Decidir cuándo un sistema que se vio involucrado en un incidente, debe ser restablecido para operaciones, basándose en el tipo de incidente. Se establece unas acciones para los incidentes que corresponden a la seguridad de la información.
- Establecer formalmente las acciones de comunicación, y los tiempos de respuesta para la interacción entre el líder de Recuperación de desastres y el equipo GRI.

Tareas del Líder del proceso con Respecto a Recuperación de Desastres.

Se incluye entre las tareas del líder:

- Elaborar los borradores para la definición y/o actualización de políticas, directrices, norma, procedimientos y estándares de seguridad de la información.
- Participar en los procesos de difusión y entrenamiento de usuarios respecto al modelo de seguridad de la información de la Gobernación del Valle del Cauca.
- Participar en la actualización y ejecución del Plan de continuidad recuperación de desastres.

Grupo de respuesta de incidentes.

Este grupo tendrá bajo su responsabilidad.

Departamento del Valle del Cauca  Gobernación	PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA GOBERNACION DEL VALLE DEL CAUCA	Código: PL-M11-P1-02
		Versión: 1
		Fecha de Aprobación:
		Página: 9 de 11

- Informar al Líder del proceso de recuperación de desastres sobre la información inicial relacionada al incidente de seguridad y el plan investigativo del equipo GRI.
- Revisar los incidentes de la Gobernación y obtener cualquier información adicional según sea necesario. Esta medición de riesgos será utilizada para determinar el curso de acciones a seguir para asegurar y proteger de esta manera los bienes de la Gobernación del Valle del Cauca, durante el incidente.
- Proveer informes o actas periódicas, a medida que se encuentre información nueva y significativa, relacionada con el incidente de seguridad informática.
- Entregar un reporte final, el cual debe ser el registro oficial del evento y debe incluir los detalles sobre la restauración del servicio.
- Evaluar la necesidad de activar el plan de contingencia con los proveedores de los recursos de información, de ser necesario.
- Realizar la revisión para determinar la causa exacta y el alcance completo del incidente.
- Brindar apoyo en la recuperación del estado operacional y la seguridad de los sistemas comprometidos tan eficientemente como se pueda.

Equipos de Recuperación de desastres estos equipos se encargaran de:

- Realizar la ejecución de las actividades asociadas con entornos de contingencia de acuerdo con los lineamientos establecidos y su rol dentro de la operación de cada una de las áreas que operarán en el Centro Alterno o Datacenter Externo.
- Documentar cada una de las actividades realizadas en el escenario de contingencia con el fin de que sirva como insumo para que una vez restablecida la operación en condiciones normales, se logre evidenciar oportunidades de mejora para actualizar el Plan de continuidad recuperación de desastres.
- Identificar y verificar la disponibilidad de los responsables asignados a los diferentes roles y sus alternos en caso de que estos no puedan asumir las actividades y/o tareas.

Escenario de activación del Plan de continuidad recuperación de desastres.

Departamento del Valle del Cauca  Gobernación	PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA GOBERNACION DEL VALLE DEL CAUCA	Código: PL-M11-P1-02
		Versión: 1
		Fecha de Aprobación:
		Página: 10 de 11

Las actividades de contingencia se definen de acuerdo con las causas de las posibles interrupciones y a partir de ellas se referencian las acciones a seguir en caso que las mismas se presenten. Estas se pueden unificar en los siguientes escenarios:

- No acceso al sitio normal de trabajo: Se presenta cuando por algún evento como desastre natural, actividad terrorista, problemas de transporte, huelgas, siniestros, entre otros, el personal no puede acceder a su lugar de trabajo para desarrollar las actividades propias de su cargo.
- Ausencia de Personal: Se presenta cuando existe un problema significativo porque funcionarios o contratistas que ejecutan procesos no pueden asistir a trabajar para desarrollar las actividades propias de su cargo.
- Caída de los sistemas tecnológicos: Se presenta cuando el hardware y/o software presenta fallas o cuando haya interrupción prolongada de las comunicaciones, ocasionados por: datos corruptos, fallos de componentes, falla de aplicaciones y/o error humano.

ENTRENAMIENTO

En el éxito del Plan de continuidad recuperación de desastres es fundamental contar con la participación y el compromiso del personal involucrado en el mismo. El Sistema de Gestión de Seguridad de la Información debe asegurar que todos los funcionarios involucrados reciban entrenamiento sobre los procedimientos a seguir en caso de incidentes o desastres, lo cual permite tomar conciencia de la importancia del plan, ya que serán los encargados de ponerlos en funcionamiento en caso de presentarse un evento no deseado.

FASES

Fase de Prevención

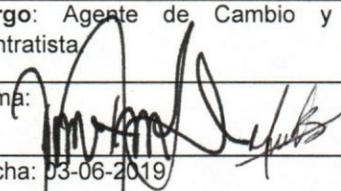
- Fase de prevención; donde se hace una el análisis de impacto en el negocio (BIA), donde se realiza la priorización de la urgencia de recuperación de cada área. Este análisis es dinámico en el tiempo y es revisado periódicamente

Departamento del Valle del Cauca  Gobernación	PLAN DE CONTINUIDAD Y RECUPERACION DE DESASTRES DE LA GOBERNACION DEL VALLE DEL CAUCA	Código: PL-M11-P1-02
		Versión: 1
		Fecha de Aprobación:
		Página: 11 de 11

por Lider de programa de TI. En este proceso se evalúan los procesos críticos de la Gobernación, los recursos que ellos demandan, y la determinación del máximo tiempo que se puede tolerar estar sin este servicio; el análisis de riesgos donde se identifican y analizan las posibles amenazas y/o vulnerabilidades de personas, sistemas, infraestructura y procesos que podrían ocasionar riesgos de continuidad para la Entidad, con el fin de medir el nivel del riesgo; el plan de recuperación, donde se definen las acciones que se deben tomar con el objetivo de restablecer las operaciones del negocio, en el plazo determinado, una vez que ocurra alguna interrupción o falla en los procesos o funciones críticas; el costo de la estrategia y el tiempo de recuperación objetivo (RTO); las pruebas permiten verificar la efectividad de las estrategias diseñadas y permitir el continuo mejoramiento del Plan de continuidad recuperación de desastres de la Gobernación y el mantenimiento de este.

Fase de Administración

- Fase de administración de la crisis; donde se produce la evaluación, activación y retorno a la normalidad.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Ricardo Ramirez Sabogal y Mildred Jimena Gutierrez	Nombre: Frank Alexander Ramirez O. y Oscar Julio Molano Diaz <i>u-</i>	Comité Acta No.
Cargo: Agente de Cambio y Contratista	Cargo: Secretario de las TIC – Lider de programa	
Firma: 	Firma: 	
Fecha: 03-06-2019	Fecha: 04-06-2019	