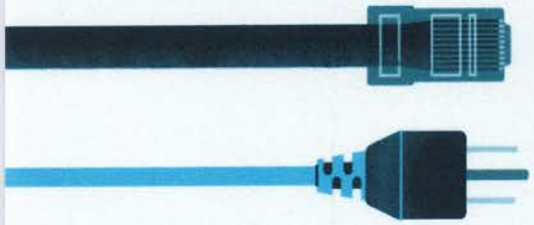
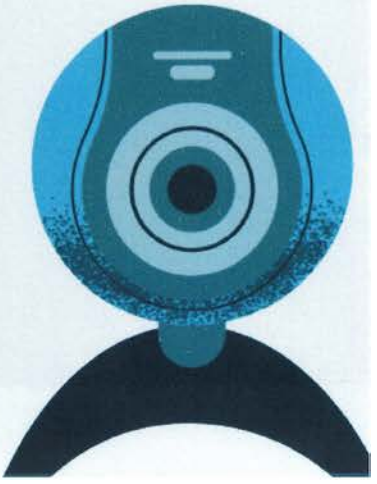


CAMINOS BIENESTAR
DIRECCIÓN DE CAMINOS BIENESTAR

PLAN CONTRA DESASTRES PARA LA RECUPERACIÓN DE DATOS, HARDWARE Y SOFTWARE

CAMINOS BIENESTAR



PLAN CONTRA DESASTRES PARA LA RECUPERACIÓN DE DATOS, HARDWARE Y SOFTWARE.

ELABORÓ

ING. ARELI GARCÍA CRUZ.
JEFA DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DE CAMINOS BIENESTAR.

REVISÓ

COMITÉ DE CONTROL INTERNO DE CAMINOS BIENESTAR.

ING. MOISÉS SALAZAR MARTÍNEZ.
PRESIDENTE.

ING. ALEJANDRO MÉNDEZ ALTAMIRANO.
COORDINADOR.

L.C. NOEL GARCÍA ROJAS.
VOCAL EJECUTIVO.

ING. RAQUEL LÓPEZ CELIS.
VOCAL A.

LIC. EDGAR RÍOS GARCÍA.
VOCAL B.

ING. ARELI GARCÍA CRUZ.
VOCAL C.

AUTORIZÓ

ING. MOISÉS SALAZAR MARTÍNEZ.
DIRECTOR GENERAL DE CAMINOS BIENESTAR.

En la actualidad, la Tecnología de la Información y de la Comunicación (TIC), se ha convertido en una herramienta fundamental para cualquier organización. Su integración es crucial para el desarrollo eficiente de los procesos internos, garantizando el funcionamiento, la continuidad y la seguridad de la información manejada. Por ello, es indispensable implementar medidas adicionales que permitan mitigar los riesgos asociados, asegurando así el cumplimiento de los objetivos organizacionales.

La adopción de las TIC, en los procesos de gestión es clave para incrementar la eficiencia y eficacia de los servidores públicos. Estas tecnologías facilitan el acceso a información crítica en momentos oportunos y optimizan el uso de diversas herramientas, contribuyendo al logro de metas propuestas. Sin embargo, el uso de estas tecnologías también conlleva amenazas que requieren la implementación de controles adecuados para garantizar la prestación de servicios de manera segura y efectiva.

Los planes de recuperación ante desastres son esenciales para asegurar la continuidad de las operaciones en situaciones de interrupción. Un Plan de Recuperación de Desastres (PRD) está diseñado para restaurar servidores y sistemas ante cualquier eventualidad, ya sea un desastre natural, un acto terrorista, un error humano o cualquier evento que perturbe el funcionamiento normal de los procesos tecnológicos.

Este plan seguirá una serie de pasos, para llevar a cabo las actividades de respaldo y recuperación de software y datos. El PRD se fundamentará en las mejores prácticas y en un manejo adecuado de la tecnología, asegurando que se cubran las necesidades de la entidad y se ofrezca un valor agregado de confianza a los servidores públicos. De esta forma, se garantiza un respaldo sólido de la información en manejo dentro del organismo, contribuyendo a la estabilidad y continuidad de sus servicios institucionales.

1. OBJETIVO

Planificar, un plan contra desastres para la recuperación de datos, hardware y software tecnológicos, para que en su momento se actúe de forma correcta ante un evento de desastre tecnológico, interrupción mayor o un evento contingente.

2. ROLES Y RESPONSABILIDADES

Tabla 1. Roles y responsabilidades

Rol	Actividad
Comité de emergencias e institucionales (Director General, Subdirector, directores de área)	• Definir y comunicar los lineamientos generales para el establecimiento y reacción ante eventualidades que impidan la continuidad y el plan de recuperación. • Proveer recursos y atender las necesidades del plan de continuidad y el plan de recuperación.
	• Citar a las personas que conforman el comité de emergencias y activar la contingencia o desastre tecnológico según la alerta. • Tomar decisiones institucionales para la operación del plan de continuidad y del plan de recuperación ante desastres presentadas por los responsables
Jefe del departamento de Tecnologías de la información	• Coordinar la atención organizada y estandarizada de las actividades planificadas ante una eventualidad. Dirigir y comunicar oportunamente las situaciones de riesgo de continuidad, según los canales e instancias definidas. • Asesorar a todo el organismo sobre las acciones a seguir ante un evento de riesgos de continuidad o perdida de la información ante desastres tecnológicos.

	• Adelantar las acciones oportunas ante una eventualidad de continuidad o perdida de información ante desastres tecnológicos. Generar y activar controles para prevenir situaciones de riesgo. • Documentar y conservar la trazabilidad de las acciones adelantadas. • Gestionar y ejecutar los recursos para adelantar las actividades para la activación del plan de continuidad y el plan de recuperación ante desastres.

3. ALCANCE

Esta documentación, establece diversas estrategias para la recuperación y continuidad de los sistemas de información, así como de la infraestructura tecnológica que los respalda, frente a posibles desastres que puedan afectar los procesos y actividades de los servidores públicos del organismo. Las estrategias están orientadas a cumplir con los objetivos institucionales, tanto internos como externos, garantizando la preparación ante cualquier vulnerabilidad. El propósito es restablecer los servicios digitales en el menor tiempo posible y reducir al mínimo la pérdida de recursos tecnológicos.

4. LINEAMIENTOS DE OPERACIÓN

El plan de recuperación ante desastres (DRP), está enfocado a la protección de los sistemas tecnológicos que soporta y almacena información importante de los trabajadores, así mismo, los procesos institucionales de direccionamiento, lo cual, son herramientas importantes que se manipulan en la dependencia. La efectividad en el restablecimiento oportuno de los servicios tecnológicos institucionales se basa en las siguientes premisas:

- Disponer de infraestructura y recursos que soporten las estrategias de contingencia y recuperación de los sistemas críticos.

- Se requiere contar con sitios alternos y operativos dispuestos para la recuperación de las operaciones, procesos y procesamiento de la información.

- Los servidores con responsabilidades asignadas en este plan se capacitarán.

- Se realizarán copias de respaldo de las bases de datos, información y sistemas de información de acuerdo con la política institucional de copias de respaldo.

5. ESCENARIOS DE DESASTRE TECNOLÓGICO

Existen muchas clases de desastres tecnológicos que pueden ocurrir dentro del organismo. A continuación, se explican los escenarios más frecuentes, su causa y solución.

Tabla 2. Escenario de desastre tecnológico

Escenario	Causas potenciales	Soluciones operativas
Indisponibilidad de la información.	Falla de la infraestructura de los servicios esenciales. Fallas tecnológicas en: comunicaciones, hardware, software, bases de datos. Robo o secuestro de datos. Ciberterrorismo. Error humano.	Respaldo de la información clave del proceso (BACKUP). Contar con proveedores de servicios alternos.

		Almacenamiento en la nube.
Pérdida de los servicios TIC.	Fallas en equipos esenciales. Switch Core. Conexión con centro de cableado. Router Core. Switches de piso. Enlaces de comunicación. Firewall. Fallas tecnológicas en: comunicaciones, hardware, software, bases de datos.	Comunicarse con la Dirección General de Tecnologías e Innovación digital para solventar dichos problemas.
Pérdida de información o servicios informáticos por fallas en los servidores	Corrupción de la base de datos. Borrado o perdida de datos. Falla total o parcial del sistema de almacenamiento o del servidor de respaldo. Violaciones de seguridad. Falta de actualización.	Respaldo de la información clave del proceso (Backup). Estrategia DRP.

6. NIVELES DE CONTINGENCIA

Cada escenario de contingencia tiene una respuesta especifica que determina los responsables de los diferentes componentes o sistemas de información. A continuación, se describen de manera general los tipos de contingencia que se cubrirán con el plan de recuperación ante desastres.

Tabla 3. Tipos de contingencia.

Estados de alerta	Definición
Menor	Generada por eventos que afectan a uno o varias áreas por un tiempo superable al tiempo de caída a 2 horas.
Mayor	Interrupción causada por incidentes que afectan el acceso a los sistemas de información, lo que impide la operación normal de la entidad durante un período superior a 24 horas continuas.
Catastrófica	La entidad enfrenta una interrupción total de los sistemas críticos, afectando directamente los procesos misionales que sustentan las actividades principales. La duración del evento supera las 24 horas, lo que compromete seriamente la continuidad operativa.

Por otro lado, es importante precisar, que cuando se determine que la contingencia es mayor o catastrófica, el área de Tecnologías de la Información N es responsable de recomendar al grupo de gestión de emergencias institucionales la activación del plan de recuperación ante desastres.

7. INFRAESTRUCTURA ACTUAL DE SERVICIOS TIC

A continuación, se realiza una descripción de la infraestructura actual que soporta los sistemas de información del departamento de tecnologías de la información.

Centro de datos: Es donde se encuentra alojado la infraestructura, el almacenamiento, las plataformas de procesamiento, que son usadas en el organismo. Cumple con las recomendaciones estándares y un correcto flujo de aire acondicionado, con control interno y extractor para garantizar la disminución de energía en los sistemas de aire y la extracción de calor de estos puntos críticos.

Este centro de datos es administrado por personal de la **Dirección General de Tecnologías e Innovación Digital**.

Cuenta con políticas de administración, mantenimiento, soporte y acceso restringido mediante el instructivo de dato. Su ubicación se encuentra en el primer nivel de la dependencia. En el centro de datos reposa los servidores que funcionan bajo el sistema operativo Linux Debian 9.0.

Sistemas de almacenamiento: Se cuenta con un servidor con capacidad de almacenamiento con un disco de 2 TB, y uno de 500 GB para respaldo y almacenamiento.

Red local: Corresponde a una red de topología ethernet de área local que presta servicios de conectividad a la plataforma de servidores, estaciones de trabajo, servicios de impresión y telefonía. La red local, es administrado por personal de la **Dirección General de Tecnologías e Innovación Digital.**

8. GESTIÓN DE DESASTRES

Preparación frente a desastres tecnológicos

Consiste en planificar y organizar las acciones, así como establecer la estrategia para hacer frente a posibles situaciones de emergencia y desastres. Para el caso de Caminos Bienestar, se debe considerar los siguientes preparativos.

8.1 Evaluación de riesgos

- Generar reportes sobre eventos o emergencias que se hayan presentado en la dependencia con su respecto análisis de riesgo. Identificando los

posibles desastres o amenazas (fallos en el hardware, ataques cibernéticos, incendios, etc.).

- Evaluar el impacto de cada riesgo que podría afectar los sistemas críticos y datos.

- Priorizar los riesgos para enfocar los esfuerzos de prevención y mitigación.

8.2 Respaldo de datos (Backup)

- Copia de seguridad regular: Establecer políticas de copias de seguridad frecuentes (diarias y/o semanales.) Así se asegura que los datos más recientes estén disponibles para la recuperación, enviado correo por electrónico y en la nube.

- Copia de seguridad externa (Backup off-site): Almacenar copias de seguridad en ubicaciones remotas o en la nube, fuera de las instalaciones principales.

- Automatización de backups: Configurar sistemas para que las copias de seguridad se realicen automáticamente, reduciendo el riesgo de errores humanos.

8.3 Recuperación de hardware

- Inventario de hardware: Mantener un inventario detallado de todos los dispositivos, como servidores, área de trabajo, redes y dispositivos de almacenamiento.

- Reemplazo rápido: Establecer contratos con proveedores para la reposición rápida de equipos en caso de fallos.

8.4 Recuperación de software

- Documentación de configuraciones: Mantener un registro actualizado de las configuraciones de software, aplicaciones y sistemas operativos.

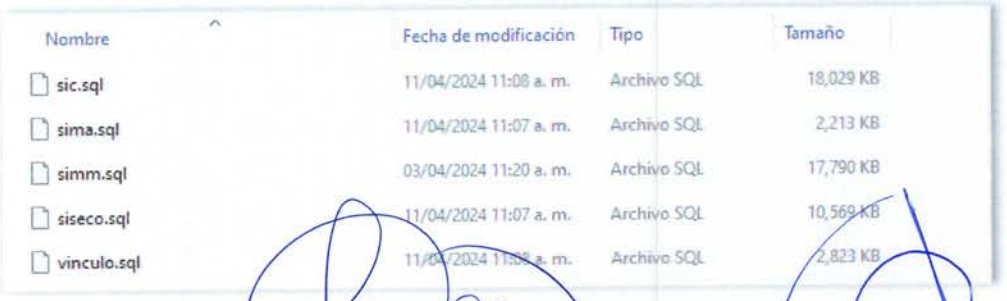
- Licencias y claves de software: Almacenar de manera segura las licencias y claves de software necesarias para reinstalar aplicaciones críticas.

- Testing y validación: Probar regularmente la capacidad de restauración a partir de las copias de seguridad para garantizar su funcionalidad.

8.5 Comunicación y coordinación

- Notificación a los empleados: Definir procedimientos claros de comunicación para informar a los usuarios sobre un desastre y los pasos a seguir.

- Involucrar a terceros: Coordinar con proveedores de servicios, consultores y otros terceros para garantizar que los recursos externos estén disponibles durante la recuperación.



Nombre	Fecha de modificación	Tipo	Tamaño
sic.sql	11/04/2024 11:08 a. m.	Archivo SQL	18,029 KB
sima.sql	11/04/2024 11:07 a. m.	Archivo SQL	2,213 KB
simm.sql	03/04/2024 11:20 a. m.	Archivo SQL	17,790 KB
siseco.sql	11/04/2024 11:07 a. m.	Archivo SQL	10,569 KB
vinculo.sql	11/04/2024 11:08 a. m.	Archivo SQL	2,823 KB

Figura 1. Respaldo de información

Subsistemas de telecomunicaciones

- Router de acceso a internet.
- Canal de acceso a servicios de internet.
- Equipos de seguridad perimetral como firewall y concentrador de VPN.

Subsistemas virtuales y físicos que soportan sistemas de información institucionales

- Sitio web institucional.
- Intranet institucional.

Detención / identificación de desastres

Por consiguiente, una adecuada detección e identificación frente a desastres tecnológicos debe contemplar lo siguiente:

- Identificar las áreas de alto riesgo en el organismo.
- Determinar la situación actual para la respectiva planificación y coordinación para emergencias tecnológicas.
- Identificar los roles y definir responsabilidades.
- Determinar cuál es la capacidad de reacción de los equipos de respuesta existente en cada área.
- Definir estrategias de emergencias ante una eventualidad.

- Establecer los mecanismos de alerta y alarma, así como los canales de comunicación a utilizar, lo anterior con el fin de comunicar a todo el organismo que debe realizar.

- Fortalecer la coordinación interinstitucional para la respuesta ante desastres tecnológicos.

9. ACTIVACIÓN DEL PLAN DE RECUPERACIÓN ANTE DESASTRES

Como parte de las estrategias inmediatas ante una posible crisis, se contemplan las tareas que deben efectuarse lo más rápido posible, después de que se presente el incidente, para reducir posibles impactos. Por ello se contempla el Procedimiento de notificación del plan de recuperación de desastres.

Cuando se presente una emergencia, se debe considerar la notificación de la misma, con el fin de iniciar el proceso de activación del **plan de recuperación de desastres**. Teniendo en cuenta el procedimiento para gestionar la notificación:

- Detectar el incidente
- Informar el evento
- Analizar la situación inicial
- Evaluar los criterios del DRP
- Activación del DRP
- Dar seguimiento correspondiente

Reconocimiento del evento e informar

La identificación o reconocimiento del evento, se realiza cuando se ha presentado un incidente, lo cual, es muy probable que ocurra una interrupción en los servidores afectando a los sistemas tecnológicos que son utilizados en el organismo. Por lo tanto, es aquí en donde se implementa las acciones de recuperación, incluyendo la

notificación y la activación del plan de recuperaciones de desastres, ya que cada factor vulnerable puede suceder al momento.

Analizar la situación inicial

La evaluación de daños en esta actividad se debe efectuar inmediatamente después del incidente, en donde se investiga y se evalúa, así como comunicarse con otras áreas de soporte, para llevar a cabo una evaluación inicial y una valoración de daños. Dependiendo de la magnitud del desastre, se debe elaborar el documento de evaluación del desastre, por lo que se deberá hacer lo siguiente:

- Poner en estado de alerta los procesos críticos que impactan a la entidad.
- Obtener información pertinente con respecto al incidente.
- Descripción del incidente.
- Daño estimado.
- Informar a las áreas afectadas.

Medios de comunicación durante el evento

En este proceso, es importante brindar la información oportuna y clara, a las personas servidoras públicas del organismo, sobre los estados de solución e impactos del incidente, lo cual, tienen responsabilidades funcionales y operativas en los sistemas de información. Esto a través de manera personal, vía telefónica o por medio de un correo electrónico.

10. PROCEDIMIENTOS DE RECUPERACIÓN DE CADA SISTEMA

El plan de contingencia se activa a partir de una falla de la base de datos. El primer paso después de la activación del plan de contingencia es la notificación a los usuarios afectados.

- **Personal interno:** personal administrativo, jefes de departamento, direcciones.
- **Publicación de banner** de notificación de indisponibilidad del sistema de información.

Para asegurar la acertada implementación y gestión de la continuidad del servicio tecnológico se deben establecer roles y responsabilidad que involucren los grupos de gestión en el departamento de tecnologías de la información.

Durante el desastre:

- Evaluar los equipos e instalaciones dañadas, realizar un informe detallado de los equipos que requieren reparación o reemplazo.

- Habilitación de los equipos computacionales con requerimientos mínimos y de comunicaciones para realizar la restauración de los datos previamente respaldados.

11. VUELTA A LA NORMALIDAD

En esta fase, se ve el resultado de cada uno de los procesos que se llevó con el plan de recuperación ante desastres, por lo tanto, de se deben considerar los siguientes aspectos:

- Fecha del retorno a la operación normal.
- Consideraciones especiales para aplicar en el proceso de vuelta a la normalidad.
- Consideraciones especiales con respeto a la recuperación de la información y mantener la integridad de los datos, cuando aplique.

Se definen el retorno a la normalidad, para ello se definen los siguientes aspectos:

- Creación de la incidencia.
- Dia, fecha y hora de la activación de los sistemas de información afectados.
- Realización de una valoración donde explique específicamente si hubo daños y afectaciones a los equipos físicos.
- Sincronización de: Los sistemas de telecomunicaciones, servicios de mensajería electrónica, sistema colaborativo office 365, servidores virtuales físicos que soportan sistemas de información institucionales y físicos, sistemas de almacenamiento masivo.

12. ESTRATEGIA DE PRUEBAS AL DRP

En este proceso es importante poner en práctica los procedimientos ante un incidente o desastre, identificar las áreas que necesitan mejorar y permitir al DRP permanecer activo, actualizado, entendible y usable.

Alcance de las pruebas al DRP

Las pruebas deben ejecutarse por lo menos una vez al año, durante un tiempo en el que las afectaciones de la operación normal sean mínimas, debe comprender elementos críticos y simular condiciones de procesos, dichas pruebas pueden ser en cualquier momento, deben incluir las siguientes actividades:

- Verificar la totalidad y precisión del plan.
- Evaluar el desempeño del personal involucrado.
- Evaluar la coordinación entre los miembros del equipo de emergencia, técnico, proveedores y terceros.
- Identificar la capacidad de recuperar registros e información vital.
- Medir el desempeño de los sistemas de información.

- Es importante disponer y contar de un centro alterno.

OAXACA
GOBIERNO DEL ESTADO

Sistema de Mantenimie
Departamento de Informática MAUR

INICIO Equipos IP Telefonos

CATALOGO DE EQUIPOS DE COMPUTO

Encontrados: 18 Equipos

USUARIO	DEPARTAMENTO	PISO	EQUIPO	MAC
TOMAS ALEJANDRO JIMENEZ	DIRECCION ADMINISTRATIVA	2	Laptop	9C:7B:EF:12:78:68
IMPRESORA ADMINISTRACION DIRECTA	DIRECCION GENERAL	2	Impresora	B4:22:00:BA:A0:DC
LAURA J. NAJERA LOPEZ	DIRECCION ADMINISTRATIVA	3	Laptop	10-1F-74-BA-75-30
DIRECCION ADMINISTRATIVA IMPRESORA	DIRECCION ADMINISTRATIVA	P_B	Impresora	84:34:97:A5:81:29
CANDY SILVA	DIRECCION ADMINISTRATIVA	P_B	PC de Escritorio	00:25:AB:76:51:00
IMPRESORA DIRECCION ADMINISTRATIVA	DIRECCION ADMINISTRATIVA	P_B	Impresora	B4:22:00:BA:A0:D7
ROSA MARIA GARCIA MEDINA	DIRECCION ADMINISTRATIVA	P_B	PC de Escritorio	00:25:AB:5F:D4:08
SIXTA OJEDA LOPEZ	DIRECCION ADMINISTRATIVA	P_B	PC de Escritorio	F4:4D:30:9F:8E:E9
DIRECCION ADMINISTRATIVA	DIRECCION ADMINISTRATIVA	P_B	Laptop	B8:88:E3:BD:F4:1A
ANTONIO ESMERIT ORDAZ MARTINEZ	DIRECCION ADMINISTRATIVA	P_B	PC de Escritorio	E0:D5:5E:14:E8:36
SICTA OJEDA LOPEZ	DIRECCION ADMINISTRATIVA	P_B	PC de Escritorio	
CANDY SILVA	DIRECCION ADMINISTRATIVA	P_B	Laptop	30:F9:ED:A3:22:F1
KARINA AGUILAR FABIAN	DIRECCION ADMINISTRATIVA	P_B	PC de Escritorio	AC:16:2D:11:2C:2E
C.P. HECTOR GUZMAN HERNANDEZ(ASESOR ADMINISTRATIVA)	DIRECCION ADMINISTRATIVA	P_B	Laptop	00:9E:9E:9A:A3:27
LIC. RENATA FELIPE MARTINEZ	DIRECCION ADMINISTRATIVA	P_B	Laptop	D0:37:45:82:C2:45
IMPRESORA CONTABILIDAD	DIRECCION ADMINISTRATIVA	P_B	Impresora	84:25:19:03:09:D0

Figura 2. Sistema de mantenimiento