PLAN DE CONTINGENCIA DEL SISTEMA DE INFORMACION Y COMUNICACIONES DEL DEPARTAMENTO ADMINISTRATIVO DISTRITAL DEL MEDIO AMBIENTE – DADSA –

DIRECTOR GENERAL

SANTA MARTA DTCH 2024

INTRODUCCION

El área de TIC del Departamento Administrativo Distrital de Medio Ambiente – DADSA -, con el propósito de proteger la información y asegurar la continuidad del procesamiento de la información necesaria para el normal desempeño de las funciones propias de la entidad, ha tenido a bien la formulación escrita del Plan de Contingencia para el aseguramiento de la información sistematizadaque circula en la institución.

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que se desarrolló un análisis de los principales riesgos a los que se enfrentala institución, para reducir la probabilidad de ocurrencia y riesgo y estar preparados antes del desastre o contingencia a fin de minimizar los daños y los procedimientos a seguir en caso que se presentara el suceso negativo, y a su vez observar las maneras de restaurar los equipos informáticos y la información dañada o perdida; actuando de manera rápida, eficiente, y oportuna con las menorespérdidas posibles y al menor costo para la Entidad.

Sin embargo, consideramos que no sólo es responsabilidad del área de TIC de la entidad, sino de todas las personas que laboran en esta, proteger la información y los equipos que la contienen; portal motivo, se ha propuesto dentro de este análisis la participación conjunta de todos los funcionariosa fin de ser todos partícipes de la seguridad de la información.

2. OBJETIVOS:

- Contar con una estrategia planificada compuesta por un conjunto de procedimientos que garanticen la disponibilidad de una solución alterna que permita restituir rápidamente los sistemas de información de la Entidad ante la eventual presencia de caídas que los paralicenparcial o totalmente.
- Garantizar la continuidad en los procesos de los elementos críticos necesarios para el funcionamiento de la aplicación web del DADSA.
- Asegurar la integridad del sistema de información, mejorando la capacidad de reacción de los usuarios internos del DADSA, ante eventos que pongan en peligro su funcionamiento.
- Proteger y conservar los activos de la entidad, de riesgos, desastres naturales o actos mal intencionados.
- Reducir la probabilidad de las pérdidas, a un mínimo nivel aceptable, a un costo razonable y asegurar la adecuada recuperación.
- Asegurar que existan controles adecuados para reducir el riesgo por fallas o mal funcionamiento tanto del equipo, como del software, de los datos, y de los medios de almacenamiento.

3. DATOS DE LA ENTIDADD

Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA.
Datos Equipos Oficina:
10 equipos de cómputo para procesos y atención al ciudadano.
4 impresoras.

4. MARCO CONCEPTUAL

En general, se considera que un plan de contingencia es un análisis de los posibles riesgos y eventualeshechos mal intencionados a los que pueden estar expuestos equipos de cómputo, programas, Bases de Datos y archivos.

Por tal motivo, en este manual se hace un análisis de los riesgos y siniestros a los que se halla sujeta la información manejada por el DADSA, para saber cómo reducir las posibilidades de que se presenten estosriesgos y los procedimientos adecuados que se deben ejecutar en dado caso.

El plan de contingencia del Departamento Administrativo Distrital de Medio Ambiente – DADSA – está definido como un conjunto de procesos, procedimientos y recursos físicos, técnicos y humanos que interactúan ante la presencia de un siniestro, teniendo como finalidad garantizar la continuidad de las operaciones automatizadas para reducir su nivel de impacto en la organización y en sus trámites, por tanto, debe estar basado en un proceso dinámico de actualización y de mejoramiento continuo.

El alcance del plan de contingencia incluye los elementos básicos y esenciales, componentes y recursosinformáticos que conforman los sistemas de información que maneja el DADSA, que se relacionan a continuación:

- **Datos**: En general se consideran datos todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (Bases de Datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colecciones de bits.
- **Aplicaciones**: Son los archivos y programas con sus correspondientes manuales de usuario y/o técnicos desarrollados o adquiridos por la entidad.
- **Tecnología**: Incluye los equipos de cómputo como computadores de escritorio, cableados, switches, etc. en general, conocidos como hardware y los programas, archivos, bases de datos, etc. denominados software para el procesamiento de información.
- **Instalaciones**: Lugares físicos de la Entidad donde se encuentren el software.
- **Personal**: Los individuos con conocimientos y experiencia específicos que integran el área de sistemas de la Entidad que dentro de sus funciones deban programar, planificar, organizar, administrar y gestionar los sistemas de información.

5. FUNCIONES DEL AREA DE TIC EN EL PLAN DE CONTINGENCIA

La función del área de TIC, es comunicar a todo el personal activo de la entidad los pasos a seguir en caso de riesgo que presente alguno de los equipos de cómputo, impresoras, e incluso la información manejada por los diferentes entes de trabajo.

5.1 VIGENCIA DEL PLAN

La vigencia de este plan está sujeta a cambios tecnológicos, de equipamiento y de los sistemas informáticos relacionados con la entidad.

6. INFORMACION DE LA OFICINA PRINCIPAL DEL DEPARTAMENTO ADMINISTRATIVO DISTRITAL DE MEDIO AMBIENTE – DADSA -.

La oficina del DADSA se encuentra ubicada en la carrera 12 # 26 – 16 en el Barrio el Bavaria en la ciudad de Santa Marta.

El DADSA tiene como objetivo contribuir y promover el desarrollo sostenible a través de la formulación y adopción de las políticas, planes, programas, proyectos y regulación en materia ambiental, recurso notable renovable, uso de suelos, ordenamiento ambiental territorial, eco-turismo, aguas potables, saneamiento básico y ambiental, desarrollo territorial y urbano.

Ejercemos las funciones de evaluación, control y seguimiento ambiental del uso del agua, el suelo, el aire y los demás recursos naturales renovables, lo cual comprendemos el vertimiento, emisión o incorporación de sustancias o residuos líquidos, sólidos y gaseosos, a las aguas en cualquiera de sus forma, al aire o a los suelos así como vertimiento y emisiones que puedan causar daños o poner en riesgo su normal desarrollo sostenible de recursos naturales renovables o impedir y obstaculizar su empleo para otros usos, estas funciones comprenden la expedición de las respectivas licencias ambientales, permisos, concesiones, autorizaciones y salvoconductos en el perímetro urbano del Distrito de Santa Marta.

La oficina del DADSA cuenta con personal de TIC, quienes prestan soporte a los funcionarios de la entidad, ya sea de manera directa o vía remota a través de un software u otro medio de comunicación, a quien lo requiera en su momento por alguno de los medios mencionados. Igualmente, el encargado del área de TIC debe contar con personal (técnico contratista o empresa contratista encargada de los suministros y mantenimiento, es decir de terceros) a su disposición para proveer soporte a mantenimiento preventivo y correctivo a los equipos de cómputo de la entidad.

7. FORMULACION DEL PLAN DE CONTINGENCIA

Se tendrá en cuenta:

7.1 ANÁLISIS DE RIEGOS.

7.2 EVALUACIÓN DEL RIESGO.

7.3 ASIGNACIÓN DE PRIORIDADES.

7.4 ELABORACIÓN DE UN DOCUMENTO.

7.5 MANTENIMIENTO DEL PLAN DE CONTINGENCIA.

7.6 IMPLEMENTACIÓN DEL PLAN (ACCIONES CORRECTIVAS Y PREVENTIVAS).

7.7 COSTOS DEL PLAN DE CONTINGENCIA.

7.8 DISTRIBUCIÓN Y MANTENIMIENTO DEL PLAN DE CONTINENCIA.

7.1 ANÁLISIS DE RIESGOS

Se tienen en cuenta dos factores:

1. Los que afectan a la seguridad de las plantas físicas.
2. Los que afectan la integridad de los datos.

7.1.1. Los que afectan a la seguridad de la Oficina.

TIPO DE RIESGO	FACTOR DEL RIESGO	PREVENCION Y MITIGACIÓN
Inundación: daños en los equipos.	Bajo	Sistemas de drenaje, buena estructura.
Incendio: destrucción de equipos y archivos.	Medio	Extintores, aspersores automáticos, detectores de humo, pólizas deseguros.
Corte de energía eléctrica:	Alto	Ups, reguladores devoltaje.
Robo: pérdida de equipos y archivos.	Medio	Seguridad en el lugar de trabajo, Cámaras deVideo Vigilancia.

7.1.2. Los que afectan la integridad de los datos:

Pérdida total del servidor	Medio	Contratación de un buen servicio deAcceso a internet. Realización de mínimo un(1) Mantenimiento Preventivo al servidor.
Falla del cableado	Bajo	Medidas exactas del cableado, conexión Debida en los puntos de red. Cambios enlos equipos de red
Pérdida de las estaciones de trabajo	Alto	Hardware en buen estado, Disco Duro con alta capacidad, contar con un buenservicio eléctrico.
Virus informáticos	Alto	Antivirus, cortafuego activo.
Ataques internos	Bajo	Restricciones a usuarios, determinaciónde rol de Administrador.

TIPO DE RIESGO	**FACTOR DEL RIESGO**	**PREVENCION Y MITIGACIÓN**
Cableado eléctrico deestaciones de trabajo	Bajo	Canaletas, tomas corrientes en buen estado
Recursos compartidos por lared	Bajo	Acceso a red directa, restricción en lainformación compartida.
Caída de la base de datos	Bajo	Contratación de un buen servicio.
Caída temporal del servidorpor falla mecánica	Medio	Verificación estado del servidor en espacioDataCenter cedido por la alcaldía distrital.

7.2 EVALUACIÓN DEL RIESGO

7.2.1. Los que afectan a la seguridad de las oficinas:

- Inundación: Ocasionaría pérdidas totales o parciales, por lo tanto, lasactividades serán interrumpidas hasta solucionar el problema. Costo total de Hardware en la entidad aprox.: $2, 800,00. oo por cada Computador, sin incluir impresoras.
- Incendio: Ocasionaría pérdidas totales o parciales. Si la pérdida es total, los costos serían los antes mencionados en el p unto anterior.
- Cortes de energía eléctrica: Discontinuidad e n el trabajo y posibles daños en el hardware. Robo: Pérdidas totales o parciales, según la gravedad de los hechos.
- Costos de Hardware: antes mencionados.

7.2.2. Los que afectan la integridad de los datos

- ✓ Los problemas de comunicación del cliente con los servidores, los problemas en el cableado eléctrico de las estaciones de trabajo, los problemas con los recursos compartidos de la red y la caída de la base de datos: Ocasionarían pérdidas totales o parciales, por lo tanto, se produce una interrupción en las actividades, hasta solucionar el problema. Generaría discontinuidad en el trabajo paralizándose las labores administrativas y de atención en la entidad.
- ✓ Caída temporal del servidor: Ocasionarían pérdidas totales o parciales, p o r lo tanto, se produce una interrupción en las actividadeshasta solucionar el problema.
- ✓ Pérdida total o parcial de las estaciones de trabajo: Ocasionaría pérdidas totales o parciales, por lo tanto, las actividades se encuentraninterrumpidas hasta solucionar el problema, en caso de pérdida total, evaluar costos.
- ✓ Virus informáticos: Generaría molestias en el sistema, ya que lodegradan y lo hacen más lento. No habría pérdidas de la informaciónalmacenada.
- ✓ taques internos: Generaría pérdidas totales o parciales, así como también, vulnerabilidad del sistema.

7.3 ASIGNACIÓN DE PRIORIDADES

Después de que acontezcan el o los problemas antes mencionados, tendremos que establecer un orden de prioridades, para poder restablecer los sistemas y así, poder seguir operando normalmente, teniendo en cuenta que la entidad tiene procesos internos que atender, sin descuidar la atención al ciudadano y empresas que así lo soliciten.

Orden de prioridades:

1. Poner en funcionamiento el o los sistemas afectados en la entidad, una vez reestablecidos se debe permitir el acceso a los funcionarios para continuar conla atención a los ciudadanos.
2. Restablecer los Backup's o copias de seguridad en caso de ser necesario.
3. Poner en funcionamiento los computadores o las impresoras que hayan sido afectadas.
4. Continuar con el trabajo administrativo y de atención al ciudadano en la entidad, haciendo uso de otras herramientas que ayuden a no perder información para luego registrarlas en los sistemas o equipos usados.

7.4 ELABORACIÓN DEL PLAN DE CONTINGENCIA DE TI DEL DADSA.

Se elaboró el esquema del plan de contingencia, con las listas de las personas a notificar, sus números de teléfono, mapas y direcciones. También se relaciona el orden de prioridades, responsabilidades, procedimientos, diagrama de las instalaciones, sistemas, configuraciones y copias de seguridad.

Aclaración: Las áreas encargadas de coordinar las contingencias son:

a) Director(a): Responsable de todos los procesos y, a su vez, el representante legal.
b) Departamento de TI: Encargado de solucionar todo lo relacionado con redes, sistemas, servidor, hardware, software, cableados de red, etc. En coordinación con terceros o técnicos o empresa contratista. c) Área correspondiente, e n caso de incendio o robo.

7.5 MANTENIMIENTO DEL PLAN DE CONTINGENCIA

Cada seis (6) meses realizar un informe sobre el plan de contingencia, teniendo en cuenta las posibles modificaciones que se deben realizar. Algunas de las cosas en las que habitualmente no se piensa a la hora de comprobar, pueden ahorrar mucho tiempo posteriormente. Por eso periódicamente hacer lo siguiente:

- Llamar a los teléfonos de los colaboradores incluidos en la lista del plan de contingencia.
- Verificar los procedimientos que se emplearán para almacenar y recuperar los datos(backup).
- Comprobar el correcto funcionamiento de las unidades donde se guarda lainformación, y del software encargado de realizar dicho backup.
- Realizar simulacros de incendio, capacitando al personal en el uso de los extinguidores; caída de sistemas o fallas de los servicios, para la medición de la efectividad del plan de contingencia.

NOTA
Copias de Seguridad: se realizarán de la siguiente manera: Cada semana la información, es decir la base de datos y archivos necesarios de la entidad, es copiada en una unidad de red (Computadora o Cloud) o disco extraíble diferente al servidor. Esto permite salvar la información, en caso de ruptura parcial o total del servidor, o de la propia base de datos. Además, existe una copia mensual, desde ese disco extraíble a DVD-ROM o a la unidad externa designada para ello, para archivar definitivamente. Esta última copia, que se realiza en forma mensual, podría ser emitida por duplicado, para que, de esta manera, se pueda archivar una dentro de la entidad y otra fuera de la misma. De este modo nos aseguramos que, en caso de un desastre, se cuente con otra copia de la información de la entidad. El responsable es el Ingeniero de Sistemas y/o Técnico capacitado y entrenado para esta tarea. La restauración de la información, disminuye los tiempos de inactividad, en caso de la ruptura parcial o total del servidor o de la base de datos, dado a que se cargaría la instancia con el backup del día, o del mes (según corresponda) para levantar la contingencia.

7.6 COSTOS DEL PLAN DE CONTINGENCIA

Gastos de mantenimiento de la red: Por evento. Extinguidores:
Costo: Consultar con área encargada.
Backup: se encarga el Dpto. de TI: Costo: $2,000.oo/Mes (Valor del DVD-ROM) Costo total por mes del Plan de Contingencia: Costo: $151,083.oo. agregando el valor del disco externo.

7.7 DISTRIBUCIÓN Y MANTENIMIENTO DEL PLAN DE CONTINGENCIA

Distribuir el plan de contingencia a todos los empleados de la entidad. Además, realizar una lista con los nombres, teléfonos y direcciones, de las personas encargadas de llevar a cabo dicho plan.

NOTA
El plan de contingencia se modificará según la retroalimentación periódica, que arroje el análisis de riesgos, El documento del plan se organizará en hojas intercambiables, de tal forma, que permita su actualización periódica. Al principio existirá una hoja de modificación, que explicite la fecha de modificación firmada por el responsable de la modificación. La modificación no requiere acto administrativo adicional de aprobación. Con la firma de los responsables es válido.
ACLARACION
En caso de modificarse el plan de contingencia, actualizar todas las copias de cada uno delos empleados, con la posterior destrucción de la copia anterior, para unificar la información.

8. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La dirección del Departamento Administrativo Distrital de Sostenibilidad Ambiental- DADSA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para del Departamento Administrativo Distrital de Sostenibilidad Ambiental- DADSA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA.
- Garantizar la continuidad del negocio frente a incidentes.
- El Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA y la ciudadanía en general.

Nivel de cumplimiento: Todas las personas cubiertas por el alcance y aplicabilidad deberán dar

cumplimiento un 100% de la política.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA:

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

El Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA, protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activa del riesgo que se genera de los accesos otorgados a terceros, o como resultado de un servicio interno en outsourcing.

El Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA, protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

El Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA, protegerá su información de las amenazas originadas por parte del personal.

El Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

El Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA, controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

El Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA, implementará control de acceso a la información, sistemas y recursos de red.

El Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

El Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA, garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

El Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA, garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

El Departamento Administrativo Distrital de Sostenibilidad Ambiental – DADSA, garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.