PLAN DE RECUPERACIÓN DE DESASTRES - IDPC
PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA
Versión: 2 del 29 diciembre de 2023

Contenido

1. Objetivo

Establecer el plan de recuperación de desastres tecnológicos (DRP) de Sistemas de Información y Tecnología del Instituto Distrital de Patrimonio Cultural IDPC, en caso de la ocurrencia de un evento que impacte los servicios tecnológicos de la entidad, que afecte la Confidencialidad, Integridad y Disponibilidad de la información con el propósito de reestablecer dichas propiedades de la información.

Responsable: Gestión de Sistemas de Información y Tecnología.

2. Alcance

Comprende desde el despliegue de las metodologías utilizadas para la recuperación y estabilidad de los servicios y sistemas de información, a pesar de desastres que perturben los procesos del Instituto Distrital de Patrimonio Cultural – IDPC. En consecuencia, poder estar prevenidos para enfrentar los incidentes y poder reintegrar las funciones y servicios con eficacia y eficiencia, es decir, atenuando el impacto de los eventos no deseados.

3. Definiciones

Activo de Información: Es el activo que contiene o está relacionado con la información y tiene valor para la entidad: personas, sistemas, edificios, etc..

Análisis de Impacto: Marco conceptual sobre el cual las entidades deben planear integralmente los alcances y objetivos, que permiten proteger la información, en todas sus áreas críticas.

Continuidad de Negocio: Entrega de productos y servicios de manera óptima después de ocurrido un evento.

DRP: Cualquier información vinculada Información documentada que define los procedimientos, metodologías, funciones y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de perturbación. Sigla en inglés, Disaster Recovery Plan (Plan de Recuperación ante Desastres).

Interrupción: Incidente anticipado o no, que afecte el normal curso de las operaciones de la entidad, ejemplo: ataques a la infraestructura o al sistema, fallas de potencia, huracanes, etc.

Plan de Continuidad de negocio: Procedimientos que orientan a la entidad para declarar, recuperar, restablecer y reintegrar la operación de forma óptima tras la interrupción.

Plan de Contingencia: Define los procedimientos y las rutas que se deben tomar para que la Entidad pueda continuar funcionando en caso de un evento de desastre.

Plataforma tecnológica crítica: Sistemas de Información vitales para apoyar los servicios y procesos: bases de datos, equipos, enlaces, servidores, etc....

RAS: Texto que plantea las diversas alternativas y soluciones viables para recuperar y reintegrar el sistema de tecnología ante un evento adverso. Sigla en inglés, Response Alternative and Solutions. (Soluciones y Alternativas de Respuesta)

RTO: Tiempo de recuperación para un proceso, servicio, sistema o plataforma tecnológica, después de ocurrido un evento de emergencia. Sigla en inglés, Recovery time Objetive. (Objetivo de Tiempo de Recuperación)

RPO: Masa de Información que puede perder un proceso o servicio por un evento de crisis. Sigla en inglés, Recovery Points Objetive. (Objetivo de Punto de Recuperación).

4. Contenido

a. Política general de plan de recuperación de desastres

La Política General del plan de recuperación de desastres está encaminada a garantizar la conservación, la confidencialidad y la recuperación de todo el sistema de información del Instituto Distrital del Patrimonio Cultural IDPC, asegurando que los controles del SGSI tengan persistencia ante eventos no deseados en la

operación de TI, manteniendo su eficacia y oportunidad en la protección de datos y la funcionalidad de los servicios en los sistemas de información.

Objetivos estratégicos de la política

1. Identificar la infraestructura crítica de los servicios tecnológicos del IDPC que debe recuperarse ante una pérdida o daño a las instalaciones y servicios.

2. Definir los roles y responsabilidades para la ejecución del Plan de recuperación de desastres.

3. Restaurar las actividades, procesos, servicios y sistemas de información en el IDPC.

4. Ofrecer respuestas oportunas y apropiadas a cualquier incidente no planeado, reduciendo así el efecto de una interrupción de los servicios tecnológicos del IDPC.

Políticas específicas de Operación

1. El responsable del Plan de Recuperación de desastres es el líder del Proceso de Gestión de Sistemas de Información y Tecnología, quien debe definir el equipo técnico encargado de la ejecución del Plan.

2. Una vez al año se debe poner a prueba la metodología del DRP para determinar su efectividad, esta debe ser documentada y socializada a la alta dirección y a los funcionarios
y contratistas del IDPC.

3. Se debe socializar como mínimo una vez al año el Plan de Recuperación de Desastres a todos los funcionarios y contratistas del IDPC en el marco del Plan Institucional de Capacitaciones.

4. Es deber de los funcionarios y contratistas que tengan roles definidos en el DRP participar de manera activa en las capacitaciones y actividades de divulgación del plan.

b. Objetivos del MSPI

El Instituto Distrital de Patrimonio Cultural en su propósito de dar cumplimiento a la política de seguridad y privacidad de la información establece los siguientes objetivos:

- Identificar y valorar los activos de información del Instituto Distrital de Patrimonio Cultural.

- Gestionar de manera eficaz los riesgos de seguridad y privacidad de la información identificados en la Entidad.

- Sensibilizar a los colaboradores, contratistas y terceros que tengan acceso a la información del Instituto Distrital de Patrimonio Cultural, sobre el manejo seguro de la información institucional.

- Cumplir con los criterios y requisitos de seguridad atendiendo el marco normativo y legal de la entidad.

c. Alcance /Aplicabilidad

Esta política aplica a todos servidores públicos, contratistas y terceros que tengan acceso a la información del Instituto Distrital de Patrimonio Cultural, en particular a los procesos misionales, gestión documental y gestión de sistemas de información y tecnología.

d. Nivel de Cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a la presente política.

5. Análisis al Impacto (BIA)

A continuación, se analizan los servicios al proceso críticos de TI y el impacto al negocio.

Tabla 1 Análisis de Impacto (BIA)

Categoría (Función Crítica del Negocio)	**Procesos Críticos (Servicios)**	**Identificación de recursos críticos de Sistemas TI**	**Tiempo de Recuperación Objetivo – RTO**	**Tiempo de Recuperación de Trabajo – WRT**
Centro de Datos	Centro de Datos	Control de operaciones de Servidores.	1 día	1 día
		Sistemas de Almacenamiento.	0.5 días	0.5 días
		Sistemas de Backups.	1.5 días	1 día
		Aire Acondicionado	1 día	0.5 días
		Acometida Eléctrica	0.5 días	0.5 días
Comunicaciones	Internet y Red Local	Switches	1 día	0.5 días
		Router	1 día	0.5 días
		Firewall	1 día	0.5 días
Sistemas de información	Orfeo	Servidores	1 día	0.5 días
	Mesa de Ayuda	Servidores	1 día	0.5 días
	Directorio Activo	Servidores	1 día	0.5 días
	Antivirus	Servidores	1 día	0.5 días
	File Server	Servidores	2 días (Sistema de Backup)	1 día
	Página Web	Hosting	2 días	1 día
	SISBIC, SIGO, Correo electrónico	Contratos Proveedores	ANS – Alta disponibilidad de servicio con el proveedor	ANS – Alta disponibilidad de servicio con el proveedor

Categoría (Función Crítica del Negocio)	Procesos Críticos (Servicios)	Identificación de recursos críticos de Sistemas TI	Tiempo de Recuperación Objetivo – RTO	Tiempo de Recuperación de Trabajo – WRT
Fluido Eléctrico	Red Eléctrica Regulada	UPS	1 hora	1 hora

6. Ámbitos de Adversidad

A continuación, se explican algunas situaciones a las que se puede ver enfrentada la entidad:

1. Pérdida total o parcial de información por fallas en infraestructura de bases de datos, almacenamiento y respaldo.
2. Problemas de los servicios.
3. Pérdida total o parcial de servicios informáticos por fallas en los servidores
4. Indisponibilidad de la información.

Tabla 2 Escenarios de adversidad

Escenario	Causas Potenciales	Soluciones Operativas
No disponibilidad de los servicios críticos	Fallas causadas en servicios críticos: Interrupción en el servicio de fluido eléctrico. Ausencia del servicio de comunicaciones. Desastres naturales: Incendios, Inundación, Terremoto.	Plan de DRP UPS Canales de Backup Plan Distrital de gestión del Riesgo de Desastres y del Cambio Climático.
No disponibilidad de los servicios tecnológicos.	Fallas Tecnológicas en: Redes Hardware Software Base de Datos.	Plan del DRP
Ausencia del personal responsable del proceso.	Periodo de vacaciones no planificado. Retiro inesperado. Fallecimiento. Enfermedad.	Fortalecimiento del sistema de gestión documental de los servicios ofrecidos por el proceso de gestión de sistemas de información y tecnología.

Escenario	Causas Potenciales	Soluciones Operativas
Indisponibilidad de la Información.	Desastres naturales Servicios críticos Fallas Tecnológicas en: Comunicaciones Hardware Software Bases de Datos Fuga de información Secuestro de datos Ciberterrorismo Error Humano.	Plan del DRP Plataforma de Backup DLP Google Google Drive Plataforma Antivirus Alta Consejería Distrital de Tic
Problemas de los servicios críticos.	Incendio Terrorismo Fuga de gas Explosión Desastres naturales.	Plan Distrital de Gestión del Riesgo de Desastres y del Cambio Climático.
Pérdida total o parcial de servicios TIC.	Fallas en equipos esenciales: Centro de Datos Casa Pardo Switch Core Fibras ópticas de conexión de cableado entre las sedes Plataforma de almacenamiento Router Switches de las sedes Enlaces de comunicación con ISP ETB Firewall	Plan del DRP
Pérdida total o parcial de información por fallas en infraestructura que soporta las aplicaciones, base de datos, almacenamiento, respaldo conexión Google Suite	Pérdida de integridad en la base de datos. Pérdida de datos Falla total o parcial de sistema de almacenamiento Falla total o parcial del servidor.	Plan del DRP
Pérdida total o parcial de servicios informáticos por fallas en los servidores.	Falla total o parcial de servidor Evadir controles de seguridad Falta de actualizaciones en los sistemas que soportan la infraestructura de TI.	Plan del DRP

7.Identificación de Recursos Críticos

Tabla 3 Recursos críticos

Categoría (Función Crítica del Negocio)	Procesos Críticos	Identificación de recursos críticos de Sistemas TI
Seguridad Perimetral	Firewal	Configuración de Firewal
		Hardware - Dispositivo Appliance
		Diagrama cableado
Antivirus	Protección Antimalware	Consola de antivirus y agente endpoint cliente
Wsus permite a los administradores de tecnologías de la información implementar las actualizaciones de productos de Microsoft más recientes.	Actualizaciones en los sistemas que soportan la infraestructura de TI	Servidor Venus
Comunicaciones	Servicio de Internet	Control de identificación usuarios con doble autenticación
		Control de usuarios locales Vs invitados.
	Servicio MPLS	Servicio de ETB
		Configuración de Firewall
		Configuración de Swiches
Infraestructura de Servidores	Servidores	Servidores Físicos de Cluster.
		Servidores Físicos Aislados
		Configuración de Firewall
		Unidad de Almacenamiento
		Configuración de Unidad de Almacenamiento
		Configuración de Swiches
		Licencia VMWare
		Configuración de Carpetas Compartidas

Categoría (Función Crítica del Negocio)	Procesos Críticos	Identificación de recursos críticos de Sistemas TI
Servidores	Servicio de Carpetas Compartidas	Servidor Venus (Sistema Operativo)
		Servidor de Dominio IDPC
Mesa de ayuda	Gestión de Requerimientos	Servidor Atenea, en caso de falla, el usuario puede utilizar el correo institucional para registrar los Requerimientos.
Servidores	Servidor de Dominio	Configuración de Servidor de Dominio.
		Servidor de Dominio Principal.
		Servidor de Dominio Respaldo IDPC: servicios

8. Niveles de Contingencia

Una contingencia es un suceso o evento que tiene posibilidad de ocurrencia, especialmente un problema que se presenta de forma imprevista.

Cada situación de contingencia tiene un procedimiento de recuperación que debe ser formalizado por los responsables de los diversos sistemas de información. Cuando exista una situación de mayor gravedad, el responsable de Gestión de Sistemas de Información y Tecnología debe armar el grupo de emergencia y activar el plan de recuperación de desastres.

Tabla 4 Niveles de contingencia.

NIVELES DE CONTINGENCIA	
ESTADO DE ALERTA	**DEFINICION**
MENOR	Generada por eventos que afectan a uno o varias sedes por un tiempo superable al tiempo de caída a **1** hora.
MAYOR	Provocada por incidentes que afectan el acceso a los sistemas de Información del IDPC, interrumpiendo la operación normal de la entidad por un período mayor a **4** horas continuas.
CATASTROFICA	Interrupción total al máximo tolerable afectando los procesos misionales y actividades del IDPC por más de **48** horas.

9. Descripción de la Infraestructura Tecnológica

La Arquitectura de Referencia de los servicios tecnológicos del Instituto Distrital de Patrimonio Cultural, la cual está conformada por cinco capas (centro de datos, Infraestructura de almacenamiento y procesamiento, redes y comunicaciones, gestión de servicios y seguridad lógica y física) que se detallan a continuación:

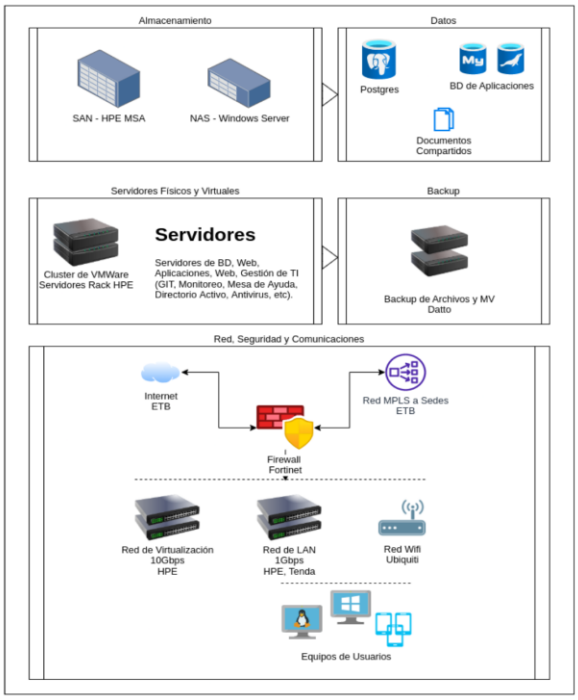

Ilustración 1 Infraestructura IDPC

De acuerdo con el MinTIC, los Servicios Tecnológicos constituyen uno de los dominios del marco de referencia de arquitectura de TI que define estándares y lineamientos para la gestión de la infraestructura tecnológica que soporta los sistemas y los servicios de información, así como los servicios requeridos para su operación. De este modo, la situación actual de la arquitectura de servicios tecnológicos, consolida las vistas y artefactos relacionados con las necesidades que el Instituto Distrital de Patrimonio Cultural busca solucionar por medio de la definición de la arquitectura empresarial. En este sentido, esta comprende la definición de la infraestructura tecnológica, la gestión de la capacidad de los servicios de TI, la gestión de la operación, así como la gestión de los servicios de soporte.

Actualmente se cuenta con un esquema de virtualización en alta disponibilidad con una unidad de almacenamiento central.

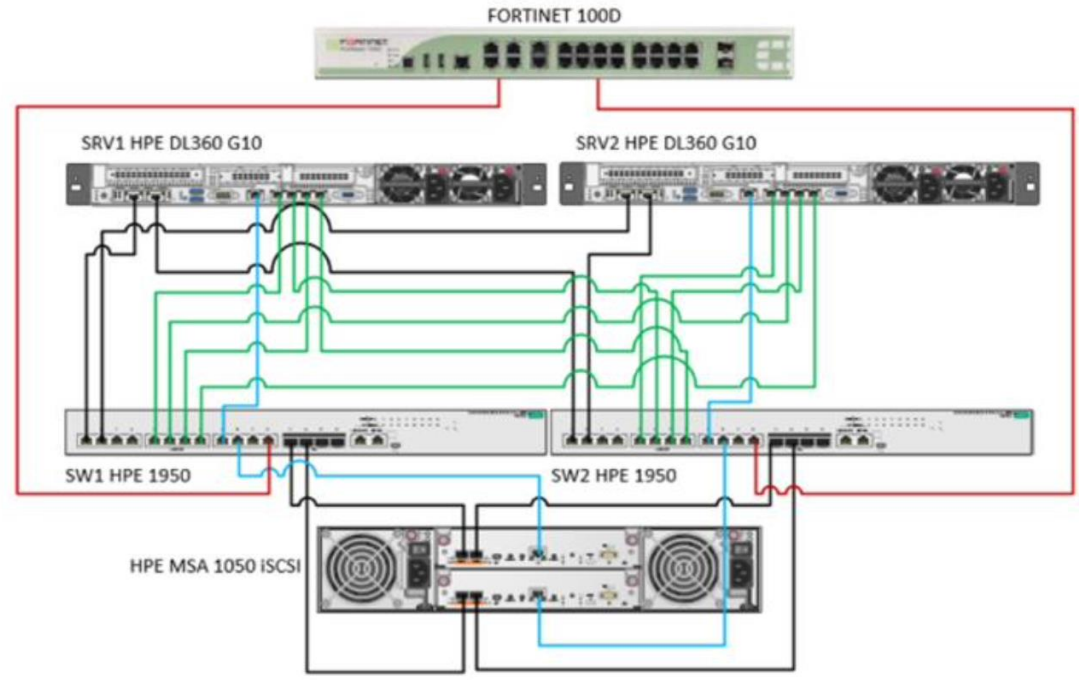

Ilustración 2Diagrama de servidores

10. Administración de Situaciones en Emergencias

a. Planificación ante los Sucesos de Crisis Tecnológica

Determinar los métodos para contrarrestar las diversas circunstancias de emergencia y desastres. En el contexto del Instituto Distrital de Patrimonio Cultural – IDPC, se obliga a atender las sucesivas acciones:

- Elaborar informes diagnosticando los riesgos, sobre los sucesos críticos acontecidos en el pasado o en el presente.
- Sensibilizar a los funcionarios de la entidad en los planes de contingencia de TI.
- Buscar alianzas con diversas entidades, a través de programas de cooperación.

b. Componentes de Información Integrados a los Planes de DRP

Subsistemas de TI

1. Router de acceso a Internet.
2. Canal de acceso a servicios de Internet.
3. Switches de Core y switches de las sedes.
4. Equipos de seguridad perimetral como Firewall y concentrador de VPN
5. Servicios de mensajería electrónica y el sistema colaborativo Google Suite.
6. Servidores virtuales y físicos que soportan sistemas de información institucionales.
7. Sitio web institucional.
8. Intranet institucional.
9. SISBIC
10. SIIGO
11. Sistema de gestión documental Orfeo.
12. Sistema de almacenamiento compartido de archivos Orfeo.
13. Sistemas de almacenamiento.

14. Sistema de virtualización de servidores.
15. Subsistemas de aire acondicionado.
16. Sistema de energía eléctrica, sistema de UPS, bancos de baterías.

c. Reconocimiento de Emergencias

Para el reconocimiento de emergencias se debe tener en cuenta lo siguiente:

1. Planificar y organizar la metodología de desastre a partir del diagnóstico de Entidad.
2. Definir las responsabilidades y sus funciones
3. Establecer los sitios de riesgo inminente en la entidad.
4. Construir tácticas para enfrentarse a los eventos contingentes.
5. Evaluar los equipos y su idoneidad al enfrentarse a circunstancias críticas.
6. Reforzar las relaciones entre Entidades para la respuesta de desastres tecnológicos.
7. Se debe especificar los mecanismos y normas de comunicación, alerta y alarma para que todo los funcionarios y contratistas del Instituto tengan conocimiento de cómo actuar ante una situación de crisis.

d. Escenarios del Plan de Recuperación de Desastres

Los escenarios de activación de DRP alcance de este plan, son aquellos eventos y circunstancias reconocidas en la operación de TI, los cuales, impactan de forma no deseada la prestación de los servicios de TI al IDPC.

Para poner en marcha el plan de recuperación de desastres, se debe seguir los siguientes pasos:

1. Localización del Evento.
2. Análisis del caso.
3. Puesta de marcha del Plan (DRP).
4. Monitoreo.

e. Guía de Activación y DRP

1. Evaluación del alcance e inventario de eventos críticos.
2. Confirmar el tipo de nivel de contingencia de acuerdo con el nivel de alerta (menor, mayor o catastrófico).
3. Comunicar permanentemente a todos los equipos conformados internos y externos sobre los eventos de emergencia.
4. Poner en marcha las alertas concertadas y acordadas en el plan de desastres (menor, mayor o catastrófico).
5. Iniciar el DRP, el plan de recuperación y accionar los procedimientos correspondientes en cada área.
6. Informar y supervisar continuamente desde el principio los eventos críticos.
7. Inicio a la normalidad y comienzo del plan de retorno de contingencia indicado en los procedimientos técnicos de cada plataforma de IT en particular.
8. Comunicado de fin de eventos de emergencia.
9. Ajustes del DRP y de metodologías de prueba.
10. Documentar los eventos aprendidos y formalizar el cierre de incidente de circunstancias críticas.

f. Lineamiento de Avisos del DRP

Es de vital importancia tener en cuenta que, al interior de los procedimientos de la Entidad, debe estar establecido las diferentes causas de circunstancias críticas, por la cual se debe dar aviso a los grupos encargados del DRP.

Para poder distinguir cuando se ha presentado un incidente de emergencia, es porque se sabe claramente que la situación va a provocar una paralización del sistema de información en la entidad.
En ese momento es cuando la respuesta, la acción de recuperación, el aviso y la puesta en marcha del DRP son perentorios.

En ese sentido, se podría decir que los pasos a seguir para informar sobre un evento o circunstancia de emergencia y así poder poner en marcha el DRP son:

1. Localización del Evento.
2. Avisar sobre la existencia del caso.
3. Diagnóstico del caso.

4. Informar a los funcionarios responsables del área y a los funcionarios responsables del DRP.
5. Analizar los criterios para poner en marcha el Plan (DRP).
6. Dar inicio al DRP.

g. Diagnóstico del Caso de Emergencia

Este diagnóstico lo hace el equipo de TI y es escalado al responsable del DRP, una vez declarado un evento de crisis, el funcionario debe comunicar a las áreas comprometidas, con el fin, de hacer un examen y dar la alerta de impacto, detallar el incidente, elaborar información sobre el evento, valorar los daños y delimitar los sitios perjudicados.

h. Protocolos de Llamadas

1. Ante un evento de crisis, corresponde llevar a cabo los siguientes pasos:
2. Se debe informar al responsable de Gestión de Sistemas de Información y Tecnología
3. El responsable de GSIT de debe llamar al subdirector de gestión corporativa
4. El subdirector de gestión corporativa se encargará de comunicar a la dirección y subdirectores de los demás procesos de la entidad.

Los comunicados pueden ser:

a. Personalmente.
b. Vía telefónica.
c. Vía correo electrónico.
d. Grupos de mensajería instantánea.

i. Terminación de la Crisis

Para considerar que se ha llegado a esta fase, hay que tener en cuenta:

1. Fecha de regularización de las funciones.
2. Reflexiones a tener en cuenta en el inicio a la normalidad.
3. Observaciones con respecto a la recuperación de la información, defendiendo la integridad de los datos.

El Coordinador de Gestión de Sistemas de Información y Tecnología debe definir el retorno a la normalidad, definiendo los siguientes aspectos: día, fecha y hora de la activación de los sistemas de información; valoración explicando si hubo daños y afectaciones de los equipos físicos y virtuales; sincronización de sistemas de telecomunicaciones actualización de la matriz de riesgos y gestión de incidentes.

11. Conformación de Equipos del DRP

Las funciones y compromisos deberán ser ejercidos por personal seleccionado. Los equipos conformados son:

1- Equipo Técnico: verifica el incidente, analiza las consecuencias e impactos potenciales, decide la iniciación o no del DRP y avisa al equipo directivo.

2- Equipo de Apoyo: son las personas que soportan la ejecución del DRP, cuando se le requiere. El equipo de apoyo estará conformado por el grupo de servicios de información. procesamiento y almacenamiento de la información.

12. Control de Cambios

Fecha	Versión	Cambios Introducidos	Simplificación o mejora	Origen
1/11/2022	01	Creación del documento.	Mejora	Modelo de seguridad y Privacidad de la Información
29/12/2023	02	Cambio de formato	Mejora	Resultado de revisión y autocontrol

13. Créditos

Elaboró	**Revisó**	**Aprobó**
Nombre(s): Ángel Diaz vega	Nombre(s): Mary Elizabeth Rojas Muñoz	Nombre: Aura Herminda López Salazar
Cargo – Rol: Contratista – Oficial de Seguridad de la Información - Subdirección	Cargo – Rol: Profesional especializado Subdirección de Gestión Corporativa	Cargo: Jefa Subdirección de Gestión Corporativa
Documento de aprobación	Memorando interno con N° radicado 20235600183403 del 29-12-2023	