PROSPERIDAD SOCIAL

PLAN DE CONTINGENCIA DE LAS PLATAFORMAS CRÍTICAS DE PROSPERIDAD SOCIAL

2021 - 2022

GIT INFRAESTRUCTURA Y SERVICIOS DE TI

Departamento Administrativo para la Prosperidad Social
Bogotá, 2022

TABLA DE CONTENIDO

1 INTRODUCCIÓN

Este documento ha sido creado para diseñar, establecer, implementar y probar un plan de contingencia tecnológica para prosperidad Social, de acuerdo con los estándares internacionales correspondientes.

2 OBJETIVO

Establecer las diferentes estrategias de contingencia que permitan garantizar la disponibilidad de la infraestructura tecnológica considerada critica para Prosperidad social.

3 ALCANCE

Este plan aplica para las aplicaciones, sistemas de información y servicios críticos que soportan la operación de los procesos misionales y de apoyo (desarrollo propio) de Prosperidad Social y establece los roles y responsabilidades para probar su efectividad y ponerlo en marcha.

Los sistemas misionales dentro del alcance son:

No	APLICATIVOS	PROCESOS SOPORTADOS	USO Y OBJETO
1	CRONOS	Gestión de Información	Sistema encargado de analizar, visualizar y administrar la información estadística del Sector, manejando y agrupando datos de manera consolidada según la necesidad de cada usuario.
2	LLAVE MAESTRA	Gestión de Información	Permite consolidar la información de todos los beneficiarios de Prosperidad Social y algunas entidades del Sector, permitiendo tener en un solo repositorio los datos básicos de cada Beneficiarios y las ayudas recibidas durante la permanencia de los beneficiarios en el sector de la inclusión social
3	PAGINA WEB	Comunicaciones	Portal de la ENTIDAD. Se registra toda la documentación para informar al público en general
4	SIFA	Gestión para la inclusión social	Sistema de información WEB que permite acceder a las bases de datos del Programa Más Familias en Acción en la cual se encuentra la información de cada una de las familias inscritas y sus beneficiarios
5	SIJA	Gestión para la inclusión social	Sistema de información WEB que permite acceder a las bases de datos del Programa Jóvenes en Acción en la cual se encuentra la información de cada uno de los beneficiarios

No	APLICATIVOS	PROCESOS SOPORTADOS	USO Y OBJETO
6	KOKAN	Gestión para la inclusión social	KOKAN es el sistema de información que soporta la operación de los programas Mi Negocio, Empleabilidad, Iraca, Resa, Familias en su tierra permitiendo consolidar, validar y reportar los datos generados a partir de las acciones realizadas por los programas en el territorio en cuanto a la identificación, caracterización y atención de las personas objeto de intervención, con el fin de producir información veraz y confiable que permita realizar análisis y tomar decisiones para futuros modelos de atención.
7	EQUIDAD DIGITAL – RUFI – Focalizador	Gestión para la inclusión social Gestión y articulación de oferta Gestión de acompañamiento Gestión de Información	Repositorio Único de Fuentes de Información de Equidad Digital, el cual permite la carga y gestión de fuentes tanto externas como internas, utilizadas para los procesos misionales y de gestión de la información de la Entidad.
8	EQUIDAD DIGITAL – RIT	Gestión para la inclusión social Gestión y articulación de oferta Gestión de acompañamiento Gestión de Información	Esta herramienta tecnológica, permitirá a cualquier dependencia de Prosperidad Social que requiera recoger información en territorio, diseñar de una manera amigable, parametrizable y sin necesidad de conocimientos técnicos ni de desarrollo de software, los formularios de encuestas, inscripciones, visitas, caracterización de usuarios o cualquier otro tipo de formulario
9	INGRESO SOLIDARIO	Implementación de Políticas, Programas y Proyectos	Mitigar los impactos derivados de la emergencia sanitaria originada por el Covid-19 en la población en condición de pobreza y de vulnerabilidad económica que no cuenta con ayudas monetarias de los programas del orden nacional (Familias en Acción, Colombia Mayor, Jóvenes en Acción o Compensación de I.V.A.).
10	COLOMBIA MAYOR	Implementación de Políticas, Programas y Proyectos	Aumentar la protección a los adultos mayores que se encuentran desamparados, que no cuentan con una pensión, o viven en la indigencia o en la extrema pobreza, a través de la entrega de un subsidio económico mensual.
11	FAMILIAS EN ACCION	Implementación de Políticas, Programas y Proyectos	Orienta sus acciones a la formación de capital humano, y a la formación de competencias ciudadanas y comunitarias, de las familias en situación de pobreza y pobreza extrema, mediante el apoyo monetario directo y acceso preferencial a programas complementarios a las familias beneficiarias y titulares del Programa Familias en Acción.

No	APLICATIVOS	PROCESOS SOPORTADOS	USO Y OBJETO
12	SISTEMA DE INFORMACIÓN UNIDOS	Gestión de acompañamiento	Sistema Core para administración de operación del programa Unidos Sistema abreviado de levantamiento de información de caracterización Sistema para la administración de postulaciones, vinculaciones, operadores y roles entorno a Unidos.

Los sistemas de información no misionales de la entidad a cargo del GIT Infraestructura y servicios de TI y que están dentro del alcance del *Plan de Contingencia de Plataformas Críticas de Prosperidad Social* son:

No	APLICATIVOS	PROCESOS SOPORTADOS	USO Y OBJETO
1	ASTREA	Gestión Jurídica	Sistema de información para el trámite de tutelas y otras acciones constitucionales interpuestas contra el Departamento Administrativo para la Prosperidad Social.
2	ULISES	Gestión del Talento Humano Gestión Financiera y Contable	Sistema de información financiera y viáticos que soporta la gestión, legalización y liquidación de solicitudes de comisiones de servicios y desplazamientos de los servidores públicos o contratistas de Prosperidad Social.
3	SISGESTION	Gestión Contractual Direccionamiento Estratégico	Sistema de información para la formulación y seguimiento a la planeación institucional y soporte de los procesos internos de gestión contractual: Plan de adquisiciones PAABS, traslados, investigación de mercado, CDP, solicitud PAC, contratación, pagos y retiro de contratistas.
4	SICON	Gestión Contractual	Sistema de información que soporta el proceso contractual del Departamento Administrativo para la Prosperidad Social.
5	Consulta INGRESO SOLIDARIO	Implementación de políticas, programas y proyectos	Aplicación que permite consultar el estado de una persona en la base de datos del Programa Ingreso Solidario.
6	SIGDI	Control Interno Disciplinario	Sistema de Información de gestión disciplinaria para el registro, trámite y seguimiento a procesos disciplinarios relacionados con los funcionarios de Prosperidad Social.
7	ORFEO-Consulta	Gestión Documental	Sistema de Gestión Documental para la consulta de expedientes documentales (anteriores a enero de 2018) de Prosperidad Social.
8	MiIntranet	Comunicación Estratégica	Portal interno de Prosperidad Social para compartir recursos, contenidos y herramientas que facilitan la comunicación, gestión y colaboración de los funcionarios y dependencias de Prosperidad Social.

Este plan no pretende cubrir las operaciones del Equipo de Respuesta a Emergencias estructurado por separado de la Oficina de Talento Humano, grupo de seguridad y salud en el trabajo

4 DEFINICIONES Y SIGLAS

- ✓ **BackEnd:** El backend es la parte “oculta” de un sitio web, ya que los usuarios no pueden acceder a ella libremente. Es donde se almacenan y organizan todos los datos de una página web para garantizar que todo funcione bien de cara al usuario.

- ✓ **Contingencia:** Se refiere a algo que es probable que ocurra, aunque no se tiene una certeza al respecto.

- ✓ **FrontEnd:** Es la parte visible y accesible de una página web. Al frontend también se le conoce comúnmente como el "lado del usuario" e incluye todo lo que el usuario experimenta, incluido el texto, el color, los botones, las imágenes, los menús de navegación, etc.

- ✓ **Nivel de Servicio de TI:** (Service Level Agreement, SLA) describe un servicio de TI, documenta los objetivos de nivel de servicio y especifica las responsabilidades del proveedor de servicios de TI y del cliente.

- ✓ **OpenView Storage Data Protector:** Es un software utilizado principalmente para automatizar la realización y recuperación de copias de seguridad y respaldos de alto rendimiento en discos o cintas a través de distancias ilimitadas y en entornos 24×7. Consta de un servidor central y un agente de backup instalado en los sistemas que van a ser respaldados.

- ✓ **Restore Backup:** Restauración de copias de seguridad.

- ✓ **Servicios en la Nube:** son servicios que se utilizan a través de Internet. Es decir, no están físicamente instalados en un computador. Los servicios en la nube son programas que se alojan en un servidor accesibles desde cualquier dispositivo conectado a Internet.

- ✓ **StorageWorks:** Son equipos de almacenamiento de datos y archivos.

- ✓ **System State:** Es donde se guarda toda la información relacionada al sistema base de Windows

SIGLAS:

EOC: Centro de operaciones de emergencia
EMT: Equipo de administración de emergencias
ERE: Equipo de respuesta a emergencias
OTI: Oficina de Tecnologías de Información
PCP: Plan de Contingencia de la Plataforma Tecnológica
RPO: Recovery Point Objective – Punto de Recuperación Objetivo
RTO: Recovery Time Objective - Tiempo de Recuperación Objetivo
TI: Tecnología de la información

5 ROLES Y RESPONSABILIDADES

Los siguientes roles y responsabilidades son los aplicables para la planificación, ejecución y control de las actividades relacionadas en este documento.

Rol	Responsabilidades en la contingencia
Administrador Servicios de Nube -Azure	Disponer de los recursos de TI necesarios en la Nube, para el traslado de Aplicaciones y Base de Datos On-premise a la Nube. Verificar que los recursos de TI en la nube sean suficientes y acordes a los requerimientos técnicos para que las aplicaciones, bases de datos y repositorios estén disponibles y accesibles.
Administrador de Servidores y Almacenamiento	Verificar que los recursos de TI on-premise sean suficientes y acordes a los requerimientos técnicos para que las aplicaciones, bases de datos y repositorios estén disponibles y accesibles.
Administrador de Bases de Datos	Proceder con el restablecimiento de Bases de Datos en la Nube o en on-premise con el ultimo Back Up disponible y realizar su administración.
Administrador Sitios Web, Videoconferencias,	Proceder con el restablecimiento de las aplicaciones y sitios web en la Nube con el ultimo Back Up disponible y realizar su administración.
Administrador plataforma office 365	Garantizar la disponibilidad de las cuentas de correo y su administración.
Administrador de Redes y Telecomunicaciones	Verificar que se gestione la capacidad y disponibilidad de los recursos respecto a los componentes de las redes de telecomunicaciones
Administrador de Telefonía	Coordinar y administrar la instalación, mantenimiento, soporte, programación y configuración de equipos y software de telefonía.
Administrador de seguridad	Generar alineación entre el plan de contingencia tecnológica y verificar que cumpla con los requisitos establecidos para el Sistema de Gestión de Seguridad de la información.
Coordinador GIT Infraestructura y Servicios de TI	Coordinar la puesta en marcha del presente plan de contingencia tecnológica

El Plan de Contingencia de la Plataforma Tecnológica de Prosperidad Social es responsabilidad del Grupo Interno de Trabajo de Infraestructura y Servicios de Tecnología de la Información.

6 PLAN DE TRABAJO

El siguiente plan de trabajo refiere a las actividades realizadas para definir las estrategias de contingencias de cada uno de los servicios de TI.

ACTIVIDADES	RESPONSABLE
Definir estrategias de contingencias	Administrador de cada servicio.
Contratar o implementar las estrategias definidas	GIT de Infraestructura y servicios de TI
Realizar Pruebas para garantizar las estrategias definidas	Administrador de cada servicio.
Generar el informe de los resultados de las pruebas	Administrador de cada servicio.
Análisis de las pruebas y mejora de las estrategias de contingencia	Administrador de cada servicio.

7 SERVICIOS NUBE AZURE

A continuación, se presentan los escenarios de riesgos y fallas

7.1 Escenarios de activación o riesgos o Supuesto de falla

Las aplicaciones misionales y no misionales (ASTREA, SISGESTION, Consulta INGRESO SOLIDARIO, MiIntranet) relacionadas en el alcance del presente plan están desplegadas en servidores virtuales en la infraestructura de nube Azure; por lo tanto, al ser una plataforma común para todas las aplicaciones, las estrategias de contingencia relacionadas a continuación aplican de igual forma:

ID	Escenarios
Escenario 1	Falla relacionada a daño de uno o varios servidores
Escenario 2	Falla relacionada con el daño de una base de datos
Escenario 3	Falla por catástrofe en el centro de datos en nube.

7.2 Estrategias de Contingencia

A continuación, se definen las estrategias de contingencia para cada uno de los escenarios descritos en el punto anterior

ID	Estrategia de contingencia
Escenario 1	Se tienen backups full diarios de la totalidad de los servidores desplegados en el centro de datos en nube de Azure.
Escenario 2	Se tienen backups full diarios de las bases de datos. Como medida adicional de contingencia se cuanta con backup full de los servidores de base de datos.
Escenario 3	Los backups realizados a servidores quedan geo replicados en dos centros de datos adicionales, en la misma zona geográfica (Estados Unidos).

7.3 RPO (Recovery Point Objective)

Volumen de datos de pérdida que la entidad considera tolerable. Punto de Recuperación.

La política de backups ver Manual se Backups y Recuperación para la Infraestructura Tecnológica de Prosperidad Social (M-GTI-5) el cual establece backups full diarios cada 24 horas para los servidores relacionados con las aplicaciones misionales en la nube de azure; por lo tanto, la perdida de información será desde el último backup hasta máximo 24 horas.

Aplicaciones	Ubicación	Criticidad	Tiempo objetivo de recuperación RPO
Aplicaciones Misionales	Centro de datos de nube azure nube	Critico	24 horas

7.4 RTO (Recovery Time Objective)

Tiempo objetivo de recuperación. Se estipula el tiempo de recuperación de los backups.

En caso de falla se puede generar restablecimiento con el último backup, en un tiempo máximo de 24 horas.

Aplicaciones	Ubicación	Criticidad	Tiempo de inactividad máximo permitido RTO
Aplicaciones Misionales	Centro de datos de nube azure nube	Critico	24 horas

7.5 Niveles de Escalamiento.

Niveles de Escalamiento		
Nivel 1	Mesa de servicios	mesadeayuda@prosperidadsocial.gov.co
Nivel 2	Administrador Servicios de Nube -Azure	Sergio.cante@prosperidadsocial.gov.co
	Administradores de base de datos	Rafael.romero@prosperidadsocial.gov.co Sergio.cante@prosperidadsocial.gov.co
	Administradores de aplicaciones	Sergio.cante@prosperidadsocial.gov.co Juan.leon@prosperidadsocial.gov.co
Nivel 3	Fabricante	Microsoft – ticket de servicios

Matriz de Comunicación Asociada al Servicio

SERGIO ALEJANDRO CANTE
sergio.cante@prosperidadsocial.gov.co
Teléfono 60 (1) 5142060
Móvil 3016155959

8 SERVICIOS ON-PREMISE

8.1 Escenarios de activación o riesgos o Supuesto de falla

Las aplicaciones no misionales o de apoyo a la gestión (ULISES, SICON, SIGDI y ORFEO-Consulta) relacionadas en el alcance del presente plan están desplegadas en servidores virtuales en la infraestructura on-premise; por lo tanto, al ser una plataforma común para todas las aplicaciones, las estrategias de contingencia relacionadas a continuación aplican de igual forma:

ID	Escenarios
Escenario 1	Falla relacionada a daño de uno o varios servidores virtuales
Escenario 2	Falla relacionada con el daño de una base de datos
Escenario 3	Falla relacionada a daño de uno o varios servidores físicos.

8.2 Estrategias de Contingencia

A continuación, se definen las estrategias de contingencia para cada uno de los escenarios descritos en el punto anterior

ID	Estrategia de contingencia
Escenario 1	Se tienen backups full diarios de los servidores virtuales de producción desplegados en el centro de datos on-premise.
Escenario 2	Se tienen backups full diarios de las bases de datos. Como medida adicional de contingencia se cuenta con backup full de los servidores virtuales de base de datos.
Escenario 3	Se tienen dos clusters de servidores físicos, el primer cluster de 3 servidores físicos y el segundo de 4 servidores físicos,.

8.3 RPO (Recovery Point Objective)

Volumen de datos de pérdida que la Entidad considera tolerable. Punto de Recuperación.

La política de backups ver Manual de Backups y Recuperación para la Infraestructura Tecnológica de Prosperidad Social (M-GTI-5) el cual establece backups full diarios cada 24 horas para los servidores relacionados con las aplicaciones de apoyo desplegadas en el centro de datos on-premise; por lo tanto, la perdida de información será desde el último backup hasta máximo 24 horas.

Aplicaciones	Ubicación	Criticidad	Tiempo objetivo de recuperación RPO
Aplicaciones de Apoyo	Centro de datos on-premise	Critico	24 horas

8.4 RTO (Recovery Time Objective)

Tiempo objetivo de recuperación. Se estipula el tiempo de recuperación de los backups.

Para los escenarios descritos en caso de falla se puede generar restablecimiento con el último backup, en un tiempo máximo de 24 horas.

Aplicaciones	Ubicación	Criticidad	Tiempo de inactividad máximo permitido RTO
Aplicaciones de Apoyo	Centro de datos on-premise	Critico	24 horas

8.5 Niveles de Escalamiento.

Niveles de Escalamiento		
Nivel 1	Mesa de servicios	mesadeayuda@prosperidadsocial.gov.co
Nivel 2	Administrador Servicios On-premise	victor.rodriguez@prosperidadsocial.gov.co
	Administradores de base de datos	Rafael.romero@prosperidadsocial.gov.co Sergio.cante@prosperidadsocial.gov.co
	Administradores de aplicaciones	Sergio.cante@prosperidadsocial.gov.co Juan.leon@prosperidadsocial.gov.co
Nivel 3	Fabricante	Hewlett Packard Enterprise – ticket de servicios

Matriz de Comunicación Asociada al Servicio

VICTOR ALFONSO RODRIGUEZ VILLAMIZAR
victor.rodriguez@prosperidadsocial.gov.co
Teléfono 60 (1) 5142060 Ext 7550
Móvil 3133618148

9 REDES DE TELECOMUNICACIONES

A continuación, se presentan los escenarios de riesgos para los equipos de comunicaciones

9.1 Escenarios de activación o riesgos o Supuesto de falla

No disponibilidad de los servicios de comunicaciones por fallas en:

- Switch Core
- Switch Servidores
- Switch de WAN comunicación con regionales e ISP
- Switch de borde
- Switch de una sede
- Enlaces de comunicación Internet
- Enlaces de comunicación con sedes y direcciones regionales

9.2 Estrategias de Contingencia

- **Para la infraestructura administrada por la entidad.**

Configuración del Switch de contingencia en caso de fallas con el switch de Core, switch de servidores y/o Switch Wan.

Switch de contingencia.
Switch CISCO 4500X (2 switch en VSS[i])puede responden a una contingencia en el servicio de CORE, WAN o Servidores.

1. Desconectar las conexiones de fibra.
2. Reconfigurar el Switch en cuestión con la documentación del switch afectado, teniendo en cuenta la velocidad de los conversores de fibra.
3. Encendido del switch de contingencia.
4. Configurar el switch de acuerdo con la configuración backup.
5. Desconexión de servidores y fibras de conexión de los centros de cableado del switch en cuestión y conectarlos al switch de contingencia, de acuerdo con la documentación guía de cada switch.
6. Reinicio de servidores en caso de no tomar configuración y comunicación de red.
7. Verificar comunicación con los servicios y equipos configurados.

Retorno a la Normalidad

1. Obtener la documentación de retorno a la normalidad del Switch programar la fecha de retorno y las consideraciones necesarias para garantizar la disponibilidad de las comunicaciones.
2. Apagar los servidores y otros equipos con sus respectivos servicios.
3. Conectar y prender el Switch de Core y verificar su funcionamiento.
4. Conectar los cables de fibra de los servidores y las fibras de los centros de cableado, de acuerdo con la documentación o verificar su funcionalidad.
5. Comunicar a los funcionarios y personas correspondientes del retorno a la operación normal.

- **Switch de contingencia ante una falla de un switch de piso en Centro de Cableado en la sede de nivel central**

  Switch de contingencia:

Switch CISCO 2960X 4 disponibles en el datacenter.

1. Ubicar el switch de contingencia en el centro de cableado correspondiente.
2. Conectar el switch de contingencia en el Centro de Cableado
3. Conectar con un patchcore un punto de un switch funcional por el frente y desconectar el cable de fibra del switch dañado.
4. Verificar la conectividad con la operación de los lets.
5. Desconectar el cable de stack de la parte posterior del Switch.
6. Conectar todos los puntos del switch que está fallando al switch de contingencia.
7. Verificar conectividad.
8. Si el stack es de 9300 se conecta en cascada por fibra óptica a alguno del switch.
9. Tramitar la garantía del switch defectuoso.

Retorno a la Normalidad:

1. Ubicar y configurar el switch nuevo o ajustado.
2. Conectar el stack y la fibra óptica.
3. Mover los parch core del switch de contingencia al switch nuevo.
4. Verificar conectividad.
5. Desconectar y conectar todos los puntos del switch de contingencia al switch. s.
6. Comunicar el restablecimiento del servicio en contingencia.
7. Programar la fecha de retorno y las consideraciones necesarias para garantizar la disponibilidad de las comunicaciones.

- **Switch de contingencia ante una falla de un switch de sedes diferentes al nivel central**

1. Ubicar y configurar switch de acuerdo con la red de cada sede.
2. Coordinar envío con la subdirección de operaciones y traslado de elemento con el almacén general.
3. Conectar el cable del Router del operador y conectarlo al switch nuevo.
4. Verificar el servicio de comunicaciones.
5. Mover los patch core del switch dañado al de contingencia.
6. Verificar los servicios de comunicaciones.
7. Retirar y Enviar el switch para el arreglo.
8. Configurar el nuevo switch
9. Tramitar garantía o adquisición del switch defectuoso.
10. Realizar el retorno a la operación normal de acuerdo con las recomendaciones correspondientes.

Para la infraestructura NO administrada por la Entidad.

La conectividad de la entidad es operada por CLARO mediante el acuerdo marco de precios para la Prestación de Servicios de Conectividad III CCENEG-024-1-2020[ii] de COLOMBIA COMPRA EFICIENTE la orden de compra actual está vigente hasta el 15 de abril del 2022.

- Enlaces de comunicación Internet

La Entidad cuenta con dos enlaces a internet en configuración activo pasivo con última milla independiente y router independientes con una disponibilidad contratada de 99.98%, todas las fallas se reportan al operador.

- Enlaces de comunicación con sedes y direcciones regionales.

Cada sede regional cuenta con un enlace de comunicación hacia la sede principal y un enlace a internet por WIFI, los dos canales cuentan con última milla independiente y router independiente, todas las fallas se reportan al operador.

9.3 Tiempos de recuperación.

- RPO (Recovery Point Objective)

Volumen de datos de pérdida que la entidad considera tolerable. Punto de Recuperación.

- RTO (Recovery Time Objective)

Tiempo objetivo de recuperación: Tiempo para recuperar la infraestructura tecnológica.

Infraestructura administrada por la Entidad:

Nombre del activo	Tipo	RTO	RPO	Impacto	Orden de recuperación
Swich core	Hardware	1 a 8 hr	0 a 1 hr	Alto	1
Swtich WAN	Hardware	1 a 8 hr	0 a 1 hr	Alto	2
Switch Servidores	Hardware	1 a 8 hr	0 a 1 hr	Alto	3
Switch de borde	Hardware	1 a 12 hr	0 a 4 hr	Alto	4
Swtich Sedes administrativas y regionales	Hardware	*24 a 120 hr	0 a 48 hr	Alto	5

*RTO para Swtich Sedes administrativas y regionales es superior; puesto que, los equipos contingentes no están en estas sedes y adicionalmente no se cuenta con soporte.

Infraestructura NO administrada por la Entidad.

Nombre del Activo	Disponibilidad	RTO	RPO	IMPACTO	Recuperación
Canal de Internet	>=99.98% mensual	<= 8 min	0 a 30 min	**Alto**	**1**
Canales MPLS Redundates	>=99.98% mensual	<= 8 min	0 a 30 min	**Alto**	**2**
Canales MPLS	>=99.9% mensual		0 a 1 hr	**Medio**	**3**

9.4 Niveles de Escalamiento

Para la infraestructura administrada por la Entidad.

Niveles de Escalamiento		
Nivel 1	Mesa de servicios	mesadeayuda@prosperidadsocial.gov.co
Nivel 2	Administrador de redes de telecomunicaciones	Juan.moreno@prosperidadsocial.gov.co
Nivel 3	Fabricante	CISCO– ticket de servicios

Detalles del Nivel 3 de escalamiento

En caso de falla de hardware en el elemento y teniendo en cuenta que la entidad tiene su plataforma LAN y WLAN toda de marca Cisco el soporte técnico es las 24 horas del día, en línea www.cisco.com y por teléfono para Colombia 01-800-5-1-81114 ó 01-800-5-1-81068 - Options 3.

se requieren de los siguientes datos

usuario: juan.moreno@prosperidadsocial.gov.co
contrato y/o número de serie del elemento afectado

Contrato No.	Service Level Description	Contract End	Bill-to Name
203711690	SNTC 8X5X4	31-Dec-2023 02:00 AM	MCO GLOBAL
203711690	SNTC 24X7X4	31-Dec-2023 02:00 AM	MCO GLOBAL
200259680	SNTC 24X7X4	27-Jan-2024 02:00 AM	MCO GLOBAL
201281494	SNTC 24X7X4	16-feb-2023 02:00 AM	TM CONSULTING
203788003	5Y SNTC 24X7X4	21-Jan-2026 02:00 AM	MCO GLOBAL

Reemplazo de hardware:

SNTC 24X7X4: 24 horas diarias, todos los días, cuatro horas de respuesta.
SNTC 8X5X4: 8 horas diarias, 5 días hábiles, cuatro horas de respuesta.

Para la infraestructura administrada por el operador.

MATRIZ DE ESCALAMIENTO CLARO			
NIVEL 1	Gestión de red	clientesespeciales.co@claro.com.co	Bogotá: 7488999 Medellín: 6044456 Cali: 4882456
NIVEL 2	Supervisor NOC	escalamientoclientesespeciales@claro.com.co	320 4882414
NIVEL 3	Líder Operación		323 2802256
NIVEL 4	Coordinador	suzel.torresl@claro.com.co	320 2221939
NIVEL 5	Gerente	juan.verdugo@claro.com.co	320 8382032
Service Account Manager	Shirley Jimena Bermúdez Camelo	shirley.bermudezc@claro.com.co	3144115313

9.5 Matriz de comunicación asociada al servicio

JUAN CARLOS MORENO MORENO
juan.moreno@prosperidadsocial.gov.co
Teléfono 60 (1) 5142060 ext. 7557
Móvil 3118791058

10 DISPOSITIVOS DE SEGURIDAD

Escenarios de activación o riesgos o Supuesto de falla

ID	Escenarios
Escenario 1	Falla relacionada con firewall on-premise primario
Escenario 2	Falla relacionada con firewall entorno de nube
Escenario 3	Falla relacionada con el Web Aplication firewall WAF entorno de nube

10.1 Estrategias de Contingencia

A continuación, se definen las estrategias de contingencia para cada uno de los componentes de seguridad tanto en nube como los componentes de seguridad en on-premise

ID	Estrategia de contingencia
Firewall On-premise	Se cuenta con una contingencia a través de firewalls en alta disponibilidad HA, los cuales se encuentran en estado modo activo-pasivo, siempre uno de los firewalls esta como primario ante la caída de uno, automáticamente ingresa el otro.
Firewall en ambiente de nube	Se tiene copia de la configuración, cada que se realiza un cambio en el firewall, la cuales se encuentran en una cuenta de almacenamiento en la nube. En caso de contingencia se levanta una maquina nuevamente y restaura la configuración
Web aplicatión Firewall en ambiente de nube	Se tiene copia de la configuración, cada que se realiza un cambio en el firewall, la cuales se encuentran en una cuenta de almacenamiento en la nube. En caso de contingencia se levanta una maquina nuevamente y restaura la configuración

10.2 RPO (Recovery Point Objective)

Volumen de datos de pérdida que la Entidad considera tolerable. Punto de Recuperación de recuperación RPO.

Componente de seguridad	Ubicación	Criticidad	Tiempo objetivo de recuperación RPO
Firewall On-premise	Centro de datos on-premise Sede Central	Critico	8 horas
Firewall nube	Centro de datos de nube	Crítico	8 horas
WAF	Centro de datos de nube, Crítico	Crítico	8 horas

10.3 RTO (Recovery Time Objective)

Tiempo objetivo de recuperación. Cuanto tiempo se tiene para recuperar la plataforma:

Componente de seguridad	Ubicación	Criticidad	Tiempo de inactividad máximo permitido RTO
Firewall On-premise	Centro de datos on-premise Sede Central	Critico	8 horas
Firewall nube	Centro de datos de nube	Crítico	8 horas
WAF	Centro de datos de nube, Crítico	Crítico	8 horas

10.4 Niveles de Escalamiento.

Niveles de Escalamiento		
Nivel 1	Mesa de servicios	mesadeayuda@prosperidadsocial.gov.co
Nivel 2	Administrador de equipos de seguridad	Sergio.cante@prosperidadsocial.gov.co
Nivel 3	Fabricante	FORTINET

10.5 Matriz de comunicación asociada al servicio

SERGIO ALEJANDRO CANTE
Sergio.cante@prosperidadsocial.gov.co
Teléfono 60 (1) 5142060
Móvil 3016155959

11 PRUEBAS

Cada una de las estrategias de contingencia definidas para los diferentes componentes de la infraestructura tecnológica deben ser probados mínimo una vez al año, con el fin de validar su efectividad. Los resultados deben ser documentados por medio de un informe y socializados con las partes interesadas.

El proceso de las pruebas inicia con la planificación de las mismas de acuerdo con lo establecido en el Procedimiento Gestión de Cambios (P-GTI-3) y haciendo uso de Formato de Solicitud de Cambios (F-GTI-10), con el fin de evaluar el impacto en los servicios de TI, determinar el tiempo de indisponibilidad, responsables y la infraestructura que va a ser sujeto a pruebas.

Los resultados de las pruebas que no sean efectivas para garantizar la disponibilidad de los servicios de TI, conllevan a un proceso de reevaluación de la estrategia de contingencia definida.

12 INDICADORES

A continuación, se presentan los indicadores asociados al cumplimiento de las pruebas de los escenarios de contingencias definidos y a la ejecución de los mismo en situaciones de crisis.

- Escenarios de estrategia de contingencia probados/ Escenario de estrategia de contingencia Planeadas
- Escenarios de contingencia activados/Eventos de crisis que requieren de activación de los escenarios de contingencia

13 RECURSOS ASIGNADOS

Las funcionarios y contratistas del GIT de Infraestructura y servicios de TI se considera recursos valiosos para realizar las pruebas y puestas en marcha de las estrategias de contingencias planeadas.

CONTROL DE CAMBIOS Y VERSIONES		
VERSIÓN	**FECHA DE APROBACIÓN**	**RAZÓN DE LA MODIFICACIÓN**
1	Liberación Kawak	Creación del Documento
2	Liberación Kawak	Se realiza ajuste de codificación y nombre del proceso como consecuencia de la entrada en vigencia del nuevo mapa de procesos aprobado mediante acta número 04 del 2020 por el Comité Institucional de Gestión y Desempeño en reunión realizada el 24 de noviembre de 2020, el cual crea el proceso Gobierno de las Tecnologías de Información. La nueva codificación del documento es G-GTI-6 que reemplaza al código G-DE-TI-24. Los lineamientos operativos descritos en este documento corresponden íntegramente a los aprobados en la versión 1 de fecha 5 de noviembre de 2020 la cual fue aprobada por Jairo Trujillo Barbosa como líder del proceso Direccionamiento Estratégico – Tecnología de la Información, vigente en ese momento. Teniendo en cuenta que para publicar los documentos en el aplicativo del Sistema de Gestión se debe surtir un proceso de aprobación en dicha herramienta, el Dr. (a) Jairo Trujillo Barbosa actual líder del proceso Gobierno de las Tecnologías de Información, realizará la aprobación atendiendo la contingencia y dejando claridad que su aprobación corresponde únicamente a la nueva codificación y el nuevo nombre del proceso.

3	diciembre 15 del 2021	se actualiza el plan de contingencia a las plataformas críticas de la Entidad, pues se ajustó teniendo en cuenta el nuevo alcance del SGSI a los procesos misionales. Se pasa de formato Guía a Plan.
4	Septiembre de 2022	Se actualiza plan de contingencia al nuevo alcance del SGSI, se incluyen procesos de apoyo (Desarrollo propio). Se incluyeron los sistemas de información no misionales de la entidad a cargo del GIT Infraestructura y servicios de TI y el numeral 8. Servicios On Premise

ELABORÓ:	REVISÓ:	APROBÓ:
Nombre: Samuel Andrés Cordoba Cargo: Contratista Oficina de TI **Nombre: Sergio Alejandro Cante** Cargo: Contratista **Nombre: Victor Alfonso Rodriguez Villamizar.** Cargo: Profesional Especializado **Nombre: Juan Carlos Moreno** Cargo: Contratista	**Nombre: Andrea Eliana Salazar** Cargo: Coordinadora GIT Infraestructura Tecnológica y servicios de TI. **Nombre: Andrés Rodrigo Navia Coloma** Cargo: Coordinador GIT Gobierno de Tecnologías de la Información	**Nombre: Jairo Trujillo Barbosa** Cargo: Jefe Oficina de Tecnologías de la Información.

[i] https://blog.router-switch.com/2014/08/vss-on-cisco-45004500x-switches/
[ii]https://colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/prestacion-de-servicios-de-conectividad-iii