

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS



Bogotá, Diciembre

2024

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

Revisión histórica

Fecha	Versión	Descripción	Autor
18-01-2021	1	Creación documento técnico del plan de continuidad del negocio	Maryury Forero
3-12-2024	2	Actualización documento del plan de continuidad del negocio.	Miguel Torres Lissette Rincón Maryury Forero

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

Tabla de contenido

1. Introducción	5
2. Descripción general	6
2.1 Propósito	6
2.2 Objetivo General	6
2.3 Objetivos Específicos	6
3. Generalidades del plan de continuidad	7
4. Plan de contingencia – Área Sistemas	8
4.1 Clasificación de procesos y servicios	8
5. Estructura Área de Sistemas	11
5.1 Organigrama Área de Sistemas	11
5.2 Condiciones Generales (Esquema General)	12
5.2.1 Criterios Matriz de Riesgos	12
6. Plan de Acción	15
7. Casos de Emergencia	16
7.1 Ausencia o falla del servicio de internet	16
7.2 Garantías de conectividad:	16
7.2.1 Fallo del Proveedor de Servicios de Internet (ISP):	16
7.2.2 Problemas de Hardware o Red Interna	16
7.2.3 Problemas de Configuración de Red	17
7.2.4 Fallo de Equipos de Acceso	17
8.2.5 Recuperación Completa:	17
8.3. Fallos Específicos en Infraestructura:	17
8.3.1 Switch Core, Distribución y Acceso:	17
8.3.2 Falla del Firewall:	18
8.3.3 Falla en Servidores Virtuales:	18
8.3.4 Falla del Servicio Wi-Fi:	19
8.4 Estrategias de Monitoreo y Prevención:	22

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

Tabla de Figuras

Figura 5.1 Organigrama Área de Sistemas

11

Tablas

Tabla 5.1 Cuadro de riesgos generales	12
Tabla 5.2 Matriz de Riesgos	13
Tabla 5.3 Tratamiento del riesgo	13
Tabla 5.4 Tratamiento de riesgo	14
Tabla 5.5 Actividades riesgos generales.....	14
Tabla 5.6 Tiempo Ingenieros de soporte.....	25
Tabla 5.7 Información empresas externas	26

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

1. Introducción

El Plan de Continuidad del Negocio es una herramienta estratégica diseñada para garantizar la capacidad de prevenir y reaccionar eficazmente frente a incidentes que puedan interrumpir las operaciones de Canal Capital. Su propósito es asegurar la continuidad en la prestación de los servicios y el cumplimiento de los compromisos establecidos en la planeación estratégica. Este plan, desarrollado por el área de sistemas, establece una serie de acciones planificadas que buscan responder de manera eficiente ante eventualidades, restablecer los servicios en el menor tiempo posible y minimizar el impacto negativo derivado de la pérdida de recursos.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 <small>ALCALDÍA MAYOR DE BOGOTÁ D.C.</small>
---	---	---	---

2. Descripción general

2.1 Propósito

Establecer un plan de contingencia en Canal Capital para gestionar los riesgos potenciales y existentes derivados de desastres, definiendo actividades específicas respaldadas por los sistemas de información e infraestructura tecnológica disponibles, con el objetivo de garantizar la continuidad operativa y minimizar el impacto de dichos eventos.

2.2 Objetivo General

Definir las actividades preventivas, detectivas y correctivas para reaccionar de manera eficiente y reducir al mínimo, el tiempo de inactividad tecnológica y la pérdida de información ante una eventualidad que comprometa el desarrollo de las actividades cotidianas.

2.3 Objetivos Específicos

- Identificar las actividades críticas, los recursos y los procedimientos necesarios para llevar a cabo las operaciones durante las interrupciones prolongadas del servicio.
- Asegurar una pronta recuperación en los servicios críticos para los grupos de valor.
- Disminuir los tiempos de interrupción de la operación de los procesos.
- Proteger los bienes e información de la entidad de manera adecuada.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

3. Generalidades del plan de continuidad

El Plan de Continuidad reúne un conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento de los servicios administrativos y algunos que afectan la misionalidad de la entidad y la prestación de sus servicios se establece en tres momentos:

- **Preventivo:** Dentro de este aspecto se involucran los recursos humanos, quienes deben estar preparados en caso de presentarse un evento inesperado, y las acciones anticipadas que se puedan articular a la gestión institucional en los diferentes procesos.
- **Reactiva:** Este aspecto va dirigido a fortalecer las políticas internas y comunicarlas oportunamente para ponerlas en marcha una vez detectada la contingencia.
- **Recuperación:** Este aspecto está enfocado en las actividades a desarrollar en el momento de atender una contingencia.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

4. Plan de contingencia – Área Sistemas

El Plan de Contingencia describe los principales procedimientos y medidas a adoptar frente a eventos que pudieran acontecer durante la operación del área de sistemas, a fin de obtener una respuesta, rápida, adecuada y oportuna que pueda mitigar al mínimo el tiempo de inactividad tecnológica de Canal Capital.

En el desarrollo del plan se tiene en cuenta la información como uno de los activos más importantes de la entidad y se realiza una clasificación de los servicios informáticos que se prestan en las operaciones diarias del área, para establecer un procedimiento escrito, que indique las acciones principales para afrontar efectivamente un evento que se presente, a fin de reducir significativamente el impacto negativo en las operaciones.

4.1 Clasificación de procesos y servicios

El presente plan incluye los componentes y recursos informáticos que conforman los sistemas de información que se relacionan a continuación:

- **Datos o Información:** En general se consideran datos todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados o no estructurados.
- **Aplicaciones:** Son los programas, herramientas y medios desarrollados o adquiridos por Canal Capital.
- **Tecnología:** Incluye los equipos de cómputo como computadores de escritorio, periféricos, servidores, servidores virtuales, cableado estructurado, router, firewall, Switches, telefonía IP etc.
- **Instalaciones:** Lugares físicos de Canal Capital donde se encuentre el software.
- **Personal:** Individuos con conocimientos y experiencia específica que integran el área de sistemas de Canal Capital y que dentro de sus funciones deban programar, planificar, organizar, administrar y gestionar los sistemas de información.

Aplicaciones de software

- Sistema de órdenes de pago ORDPAGO.
- Sistema de Inventario KARDEX.
- Sistema de Contabilidad SIIGO.
- Sistema de Contabilidad SIMED.
- Sistema de Nomina NOVASOFT.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 <small>ALCALDÍA MAYOR DE BOGOTÁ D.C.</small>
---	---	---	---

- Sistema de medición de medios IBOPE.
- Software de Intranet.
- Software de gestión documental.
- Software de gestión contractual.
- Software de ERP/ERPC

Tecnología, infraestructura tecnológica

- Un (2) Firewall Fortinet 401E, que provee la seguridad a la red, ya que es el encargado de bloquear el acceso no autorizado a la red, IPS, WEB, APP, Antivirus, SSL, IDS, etc.
- Switch CORE principal, HP 5900 JG510A.
- Switch CORE de respaldo, HP A5120-48G JE069A.
- Servidor HP, tipo Enclosure C3000 con virtualización VmWare 6.5, contiene 54 servidores virtuales en plataformas Microsoft Windows en un 90% y plataforma linux en un 10 %.
- Servidor ThinkSystem SR630, para servicios de servidores de dominio de directorio activo (AD DS), servidor de nombre de dominio (DNS) y servidor de asignación dinámica de host (DHCP).
- Equipo de almacenamiento HP MSA 2050, donde se encuentra la data o información de los servidores virtuales.
- Servidor ThinkSystem SR630, Servidor de Backups.
- Servidor plan de recuperación ante desastres (DRP), Lenovo SR630 V2-7Z71
- Librería HP MSL 2024, la cual cuenta con dos (2) drives de tecnología de escritura para cintas LTO-5; este es el encargado de realizar respaldo de la información a través de Backups.
- HP 1950 - JG961A con conexión en estrella con dispositivos CORES para brindar el servicio de datos y voz.
- Telefonía IP — Contratado con el proveedor ETB
- Aire acondicionado del centro de datos.
- UPS.

Servicios

- Internet: proveedores Canal Principal Level y Canal de respaldo Columbus
- Correo electrónico: Proveedor Xertica
- Streaming.
- Intranet (ERP/ERPC)
- Telefonía IP: Proveedor ETB

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

- Servicios de almacenamiento compartido: MSA 2050
- Backup.
- Servicio de red de área local (LAN)
- Servicio de red de área local inalámbrica (WLAN)
- Servicio de granja de servidores (VmWare)
- Servicio de canal de datos (MPLS)
- Servicio de seguridad perimetral (Firewall)
- Servicio de seguridad endpoint (Antivirus)
- Servicio de monitoreo infraestructura TIC (PRTG)
- Restauraciones.

Software

- Symantec Backup Exec 2020.
- VMWare 6.5. y 7.0
- Windows Server Data Center, standard 2016 and 2019.
- Software de inventarios Assets Invgate.
- Bitdefender Gravityzone V6.56
- Fortinet v7.2.5 build1517
- Aplicación de red Unifi 8.2.93
- Software de monitoreo PRTG Network Monitor 24.3.98.1210 x64
- Site recovery

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

5. Estructura Área de Sistemas

Dentro de las principales funciones del área de sistemas está las de realizar las acciones y proyectos orientados a la consolidación de las iniciativas de Gobierno digital y seguridad digital orientadas a la disponibilidad, acceso a la información pública y seguridad de la información, así como determinar y ejecutar el plan estratégico de la entidad y aquellos proyectos TIC que desde lo administrativo impactan el buen desarrollo de la misión institucional y la continuidad del negocio.

A su vez, para mantener la operatividad de la infraestructura de red y servicios tIC a usuarios finales, cuenta con ingenieros con especialidades diferentes en seguridad de la información, infraestructura de redes y comunicaciones y soporte a usuario final.

5.1 Organigrama Área de Sistemas

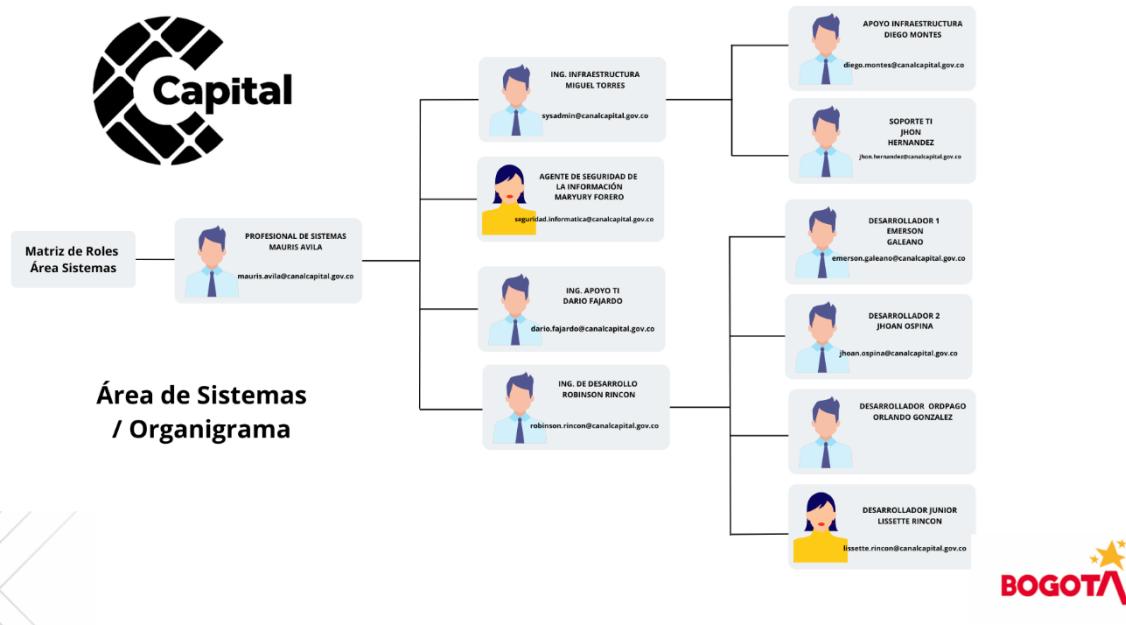


Figura 5.1 Organigrama Área de Sistemas

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 <small>ALCALDÍA MAYOR DE BOGOTÁ D.C.</small>
---	---	---	---

5.2 Condiciones Generales (Esquema General)

El Plan de Recuperación ante Desastres DRP cubre todos los aspectos de la organización que pueden verse afectados por un desastre, tales como:

- **Infraestructura tecnológica:** Servidores, sistemas de respaldo, bases de datos, redes, etc.
- **Personal:** Evacuación, seguridad, asistencia médica.
- **Operaciones:** Continuidad de la producción, ventas, atención al cliente, etc.
- **Recursos físicos:** Suministros esenciales, equipos y maquinaria crítica

A continuación, se relacionan las diferentes definiciones de riesgos generales que pueden afectar el funcionamiento de los servicios actuales de Canal Capital y los cuales se encuentran dentro del Data Center.

Factor Riesgo	Tipo de Riesgo	Prevención y Mitigación
Bajo	Fuego: destrucción de equipos y archivos.	Extintores, detectores de humo, dos (2) Solkaflam, pólizas de seguros.
Bajo	Equivocaciones: daño a los archivos.	Copias de respaldo, Políticas de Seguridad.
Medio	Terremotos: destrucción de equipos y archivos	Seguro contra todo riesgo, Copias de Respaldo.
Medio	Fallas en los equipos: daño a los archivos.	Mantenimiento, garantía y copias de respaldo.

Tabla 5.1 Cuadro de riesgos generales

5.2.1 Criterios Matriz de Riesgos

A continuación, se relacionan las diferentes definiciones de riesgos generales que pueden afectar el funcionamiento de los servicios de TI actuales de Canal Capital y los cuales se encuentran en el Data Center.

Cuadro de riesgos generales

Factor	Tipo de riesgo		Prevención y mitigación
Riesgo			
Bajo	Fuego: destrucción de		Extintores, detectores de humo, dos
	Equipos y archivos.		(2) Solkaflam, pólizas de seguros.
	Equivocaciones: daño a los		Copias de respaldo, Políticas de

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		VERSIÓN: 02	
		FECHA: 02/12/2024	
		RESPONSABLE: SISTEMAS	

Bajo	Archivos.	seguridad
Medio	Terremotos: destrucción	Seguro contra todo riesgo, Copias de
	de equipo y archivos	Respaldo.
Medio	Fallas en los equipos: daño	Mantenimiento, garantía y copias de
	a los archivos	respaldo

Tabla 5.2 Matriz de Riesgos

Se definen los criterios para los riesgos asociados a la continuidad del servicio aclarando que se atenderán y hará parte del mapa de riesgos institucional los de la dimensión 5 x 5 y se identifiquen con nivel extremos:

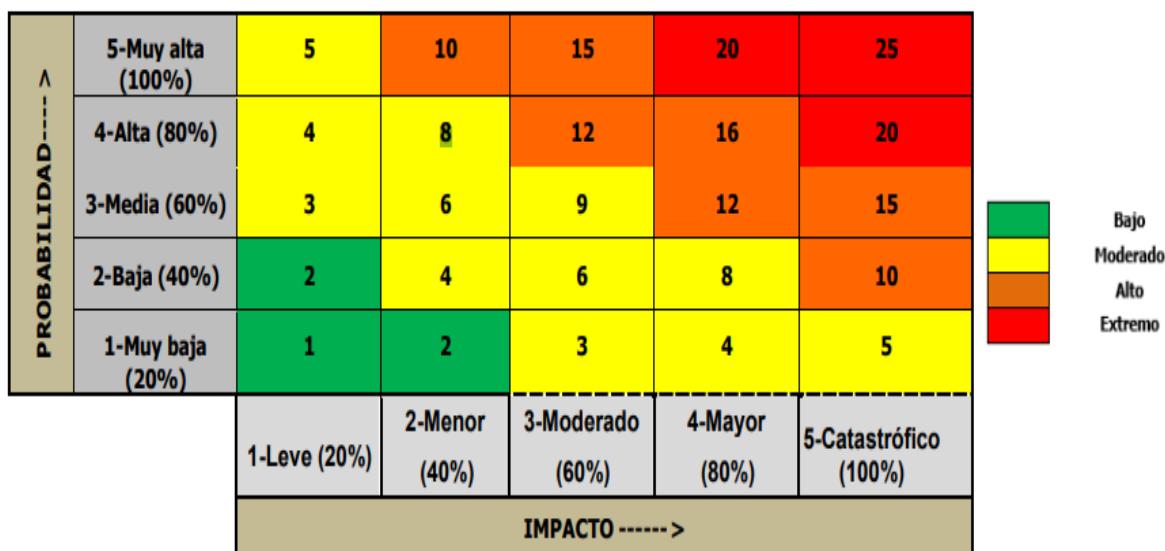


Tabla 5.3 Tratamiento del riesgo

ZONA DE RIESGO	OPCIONES DE TRATAMIENTO DEL RIESGO
Baja	Asumir el riesgo Se administrará a través de las actividades del proceso, proyecto o plan. Se debe adelantar un monitoreo semestralmente por parte de los líderes de proceso con el fin de verificar que estos riesgos no surten cambios en su aceptación que requiera la implementación de actividades de control. El reporte de su gestión se registrará en la herramienta determinada por el proceso.
Moderada	Reducir el riesgo Implementación de acciones de control preventivas que permitan reducir la probabilidad. Su monitoreo se realizará cuatrimestralmente por los líderes de proceso y sus equipos de trabajo con el fin de verificar que estas mitigan la materialización del riesgo identificado, se registrará en la herramienta determinada por el proceso.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		VERSIÓN: 02	
		FECHA: 02/12/2024	
		RESPONSABLE: SISTEMAS	

Alta y Extrema	Manejo a través del mapa de riesgos del proceso e institucional, estableciendo acciones preventivas. Su monitoreo se realizará trimestralmente por parte de los líderes de proceso y la ejecución de esta actividad se registrará en la herramienta determinada por el proceso.
----------------	---

Tabla 5.4 Tratamiento de riesgo

Se relacionan las actividades que se deben realizar con el objeto de prever, mitigar o eliminar los posibles riesgos conocidos:

No	Actividad	Elementos	Resultado
1	Copias de seguridad de la información y documentos residentes en las carpetas compartidas de las diferentes áreas.	Documentos en formatos Word, Excel, PDF e imágenes.	Copias de seguridad, incremental diaria y un full semana a cinta de todos los documentos.
2	Copias de seguridad de los sistemas de información y base de datos.	Aplicaciones WEB e Intranet ERP/ERPC del Canal. Aplicaciones y bases de datos de los procesos y archivos.	Copias de seguridad, incremental diaria y un full semana a cinta de toda la información.
3	Mantener pólizas de seguros vigentes, contra todo riesgo los equipos y bienes, asegurándose por el valor real.	Equipos electrónicos, eléctricos, portátiles, móviles y equipos de comunicación.	Póliza vigente contra todo riesgo de daño y/o pérdida física por cualquier cosa.
4	Mantenimientos preventivos y correctivos de equipos de cómputo y comunicación.	Equipos de cómputo y comunicación, periféricos, sistemas eléctricos, UPS.	Contratos anuales de mantenimiento, garantías vigentes.

Tabla 5.5 Actividades riesgos generales

Estrategias de Recuperación

- Para cada tipo de desastre, se desarrollarán estrategias y procedimientos específicos, tales como:
- Recuperación de datos: Implementación de copias de seguridad diarias/semanales de los datos clave.
- Plan de contingencia para el personal: Procedimientos de evacuación y protocolos de seguridad para empleados.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

- Recuperación de infraestructura tecnológica: Reemplazo o reparación de hardware y recuperación de software y bases de datos.
- Alternativas para las operaciones: Implementar estrategias de trabajo remoto o en sitios alternativos.

6. Plan de Acción

El plan de acción detallado debe incluir:

- **Activación del plan:** Procedimientos para declarar una emergencia y activar el DRP.
- **Rol de los equipos de respuesta:** Establecer responsabilidades claras para los equipos de respuesta ante desastres (comunicación, tecnología, logística, etc.).
- **Recuperación operativa:** Procedimientos para restaurar operaciones clave dentro de un período específico.
- **Restauración de servicios:** Recuperación de servicios esenciales (como comunicaciones, servidores, etc.).
- **Evaluación post-desastre:** Evaluación del impacto, lecciones aprendidas y ajustes al plan.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

7. Casos de Emergencia

Las actividades que se deben realizar con el objeto de prever, mitigar o eliminar los riesgos conocidos para el área de sistemas. Así mismo se informa el procedimiento a seguir en el evento en que fallen equipos críticos al interior de Canal Capital.

7.1 Ausencia o falla del servicio de internet

Actualmente se cuenta con un canal dedicado de internet de 150 MB con el ISP Cirion y canal de respaldo dedicado de internet de contingencia de 90 MB, con el proveedor Liberty Networks. Para garantizar una alta disponibilidad del servicio que presta Canal Capital a la ciudadanía.

7.2 Garantías de conectividad:

Se cuenta con un canal principal de Internet de 150 MB y un canal de respaldo de 90 MB para garantizar la disponibilidad del servicio.

Posibles causas y soluciones:

7.2.1 Fallo del Proveedor de Servicios de Internet (ISP):

- **Verificación del estado del servicio:** Contactar al ISP para identificar si la falla es por mantenimiento, interrupciones o problemas técnicos.
- **Consulta de incidencias:** Revisar alertas emitidas por el ISP.
- **Tiempos de resolución:** Solicitar al ISP un estimado para la restauración del servicio.

7.2.2 Problemas de Hardware o Red Interna

Problemas de Hardware o Red Interna

- **Reiniciar equipos de red:** Reinicia los routers, switches o módems para descartar problemas temporales o errores de configuración que puedan haber causado la falla.
- **Verificar el estado de los cables y conexiones:** Comprobar que todos los cables de red y dispositivos (módem, routers, switches) estén correctamente conectados y funcionando.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 <small>ALCALDÍA MAYOR DE BOGOTÁ D.C.</small>
---	---	---	---

- **Verificar la configuración del router:** Revisar las configuraciones del router o gateway para asegurarse de que esté recibiendo correctamente las direcciones IP, configuraciones de NAT y demás parámetros.
- **Revisar los registros de eventos:** Consultar los logs del router o módem para detectar posibles errores o fallos de conexión.

7.2.3 Problemas de Configuración de Red

- **Revisar la configuración de DNS:** Asegurarse de que los servidores DNS están configurados correctamente. Si es necesario, probar configurando los DNS de Google (8.8.8.8 y 8.8.4.4) o los de Cloudflare (1.1.1.1).
- **Verificar la puerta de enlace predeterminada:** Asegurarse de que la puerta de enlace predeterminada está configurada correctamente en los dispositivos de red.
- **Revisar configuraciones de firewall o filtrado de tráfico:** Verificar que el firewall de la red o el dispositivo de seguridad no esté bloqueando el tráfico saliente.

7.2.4 Fallo de Equipos de Acceso

- **Reemplazo de hardware defectuoso:** Si un dispositivo de acceso (como un router, módem o switch) está fallando, reemplazarlo por uno de repuesto si está disponible.
- **Uso de equipo de respaldo:** Si la organización dispone de equipos de respaldo para la conectividad, como un módem o router de repuesto, utilizarlo temporalmente mientras se diagnostica el problema.

7.2.5 Recuperación Completa:

- Restaurar configuraciones desde copias de seguridad.
- Probar conectividad global y monitorear estabilidad.

7.3. Fallos Específicos en Infraestructura:

7.3.1 Switch Core, Distribución y Acceso:

- Verificar alimentación, enlaces y configuraciones.
- Reiniciar o redirigir el tráfico si no hay recuperación inmediata.
- Utilizar switches de respaldo si el equipo está defectuoso.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

7.3.2 Falla del Firewall:

- **Diagnóstico de la falla:** Identificar si la causa es un error de hardware, software o una configuración incorrecta. Para esto, puede ser necesario revisar los logs del firewall y realizar pruebas de diagnóstico.
- **Reinicio del firewall:** En algunos casos, un simple reinicio o restablecimiento a la configuración predeterminada puede resolver el problema temporalmente.
- **Restauración de la configuración:** Si el firewall está funcionando, pero la configuración se ha perdido o corrompido, restaurar una copia de seguridad de la configuración previa.
- **Sustitución de hardware:** Si se confirma que el fallo es de hardware, proceder a reemplazar el firewall defectuoso por uno nuevo o utilizar una solución temporal hasta que se recupere el dispositivo original.
- **Actualización del firmware:** En caso de que la falla esté relacionada con una vulnerabilidad de seguridad, actualizar el firmware del firewall a la versión más reciente disponible.
- **Validación de la configuración:** Tras la restauración, verificar que las reglas de seguridad del firewall estén configuradas correctamente y que no haya riesgos de exposición.
- Contactar al fabricante para soporte técnico.

7.3.3 Falla en Servidores Virtuales:

- **Reiniciar la máquina virtual:** Intentar reiniciar la máquina virtual desde el hipervisor para descartar problemas temporales en el sistema operativo de la VM.
- **Verificar la integridad del sistema operativo de la VM:** Si la máquina virtual no arranca, acceder a la consola de la VM para diagnosticar el sistema operativo (en busca de errores en el arranque, corrupción de archivos, etc.).
- **Reparación del sistema operativo:** Si se detecta un problema en el sistema operativo (por ejemplo, corrupción de archivos), proceder con la reparación utilizando herramientas como el arranque en modo seguro o la restauración de imágenes del sistema operativo.
- **Verificación del almacenamiento:** Comprobar que el almacenamiento virtual (discos virtuales) esté disponible y sin errores. Si hay problemas con el disco, intentar reparar o recuperar los archivos dañados.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

Recuperación Completa

Si la falla no puede resolverse rápidamente o si la máquina virtual está irremediablemente dañada, es necesario restaurar la máquina virtual desde una copia de seguridad.

7.3.4 Falla del Servicio Wi-Fi:

- **Fallo del hardware:** Daños en los puntos de acceso Wi-Fi (AP), controladores o switches que gestionan la red Wi-Fi.
- **Problemas de configuración:** Errores en la configuración de los puntos de acceso, como cambios en los parámetros de red (SSID, VLAN, etc.), autenticación incorrecta, o problemas con la asignación de direcciones IP.
- **Interferencia de señal:** Interferencia externa (como dispositivos electrónicos cercanos) que afecta la señal Wi-Fi.
- **Problemas con el servidor DHCP:** El servidor que asigna direcciones IP a los dispositivos conectados puede estar fallando.
- **Problemas con el acceso al servidor de autenticación:** Si se utiliza un servidor RADIUS u otro sistema de autenticación, un fallo en el acceso o la configuración de este servidor puede interrumpir el servicio Wi-Fi.

Estrategia de Recuperación

A continuación, se describe un enfoque paso a paso para la recuperación del servicio Wi-Fi en caso de fallo.

Respuesta Inmediata a la Falla

- **Confirmar la falla:** Verificar que la falla del Wi-Fi afecta a varios usuarios o dispositivos dentro de la organización, y no a un único dispositivo o área.
- **Realizar pruebas de conexión:** Intentar conectar diferentes dispositivos al Wi-Fi en diversas áreas para confirmar que el problema es generalizado.
- **Verificar la conectividad:** Comprobar si los dispositivos son capaces de detectar la red Wi-Fi y, si es así, si pueden obtener una dirección IP o establecer la conexión correctamente.
- **Notificar al equipo de TI:** Informar al equipo de soporte técnico, redes e infraestructura sobre la interrupción del servicio Wi-Fi. Si se cuenta con una herramienta de monitoreo de red, revisarla para obtener más detalles.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

Comprobar el estado de los puntos de acceso:

- **Revisar las luces de los puntos de acceso (APs):** Asegurarse de que los APs estén encendidos y funcionando. Si no lo están, comprobar si hay un problema de alimentación o si el dispositivo está fuera de servicio.
- **Comprobar si los APs están sobrecargados:** Verificar si algunos APs están sobrecargados con demasiados dispositivos conectados, lo cual podría estar afectando el rendimiento o la conectividad.

Verificar la red interna:

- **Revisar los switches y routers:** Asegurarse de que los equipos de red que gestionan el tráfico del Wi-Fi, como switches, routers o controladores Wi-Fi, estén funcionando correctamente y que no haya interrupciones en el tráfico de red.

Diagnóstico y Resolución

Fallo de Hardware (Punto de Acceso Wi-Fi o Equipos de Red)

- **Reiniciar los puntos de acceso:** Si los puntos de acceso Wi-Fi no están funcionando correctamente, reiniciarlos para ver si el problema se resuelve. En algunos casos, el reinicio de los equipos puede solucionar problemas temporales de conexión.
- **Reemplazar puntos de acceso defectuosos:** Si un punto de acceso está dañado o defectuoso, reemplazarlo por uno de repuesto. Asegúrate de que los nuevos puntos de acceso estén correctamente configurados y funcionando.
- **Comprobar el controlador Wi-Fi:** Si el sistema de Wi-Fi está gestionado por un controlador central (en lugar de puntos de acceso autónomos), verificar si el controlador está operativo y realizando la gestión adecuada de los puntos de acceso.

Problemas de Configuración

- **Verificar la configuración de la red Wi-Fi:** Asegurarse de que el SSID (nombre de la red) y la configuración de seguridad (contraseña, protocolo de cifrado) sean correctos.
- **Confirmar que los parámetros de red** (por ejemplo, VLAN, DNS) están configurados adecuadamente.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

- **Verificar el servidor DHCP:** Asegurarse de que el servidor DHCP (si se usa) esté funcionando correctamente y que tenga suficiente capacidad para asignar direcciones IP a los dispositivos conectados. Si el servidor DHCP no está respondiendo, reiniciarlo o, si es necesario, cambiar a un servidor DHCP de respaldo.

Interferencia de Señal

- **Cambiar el canal de Wi-Fi:** Si la red Wi-Fi está experimentando interferencias debido a otras redes o dispositivos (microondas, teléfonos inalámbricos, etc.), cambiar el canal de la red Wi-Fi para evitar la congestión del canal. Utilizar herramientas de análisis de espectro o Wi-Fi para identificar interferencias.
- **Optimización de la colocación de puntos de acceso:** Revisar la ubicación de los puntos de acceso para asegurarse de que cubren adecuadamente las áreas de la oficina o la red, evitando zonas muertas o interferencias físicas (como paredes gruesas).

Problemas con el Servidor de Autenticación (RADIUS u Otros)

- **Verificar el servidor de autenticación:** Si se utiliza un servidor de autenticación (como RADIUS), comprobar que esté operativo y que los dispositivos puedan autenticarse correctamente en la red Wi-Fi.
- **Revisar las políticas de acceso:** Verificar que las políticas de acceso Wi-Fi (por ejemplo, 802.1X) no hayan cambiado o no estén impidiendo la autenticación de los usuarios.

Recuperación Completa

- **Restaurar configuración desde copia de seguridad:** Si la falla se debe a una pérdida de configuración o un error en la misma, restaurar la configuración de los puntos de acceso o del controlador Wi-Fi desde una copia de seguridad reciente.
- **Verificar la conectividad completa:** Una vez que los problemas se hayan resuelto, realizar pruebas de conectividad en todas las áreas de la red Wi-Fi para asegurar que todos los dispositivos puedan conectarse correctamente.
- **Monitorear la red:** Implementar monitoreo de red en tiempo real para garantizar que no haya problemas adicionales y que el servicio Wi-Fi sea estable.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

7.4 Estrategias de Monitoreo y Prevención:

- Implementar monitoreo continuo de red para detectar problemas a tiempo.
- Mantener copias de seguridad actualizadas y equipos de respaldo funcionales.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

NOMBRE	DESCRIPCIÓN
	<p>Canal Capital en la actualidad cuenta con Hardware y Software que permite garantizar el respaldo de la información más importante para la entidad de la siguiente manera:</p> <p>Hardware:</p> <p>Se cuenta con un servidor físico y dedicado, para la gestión y operación de salvaguardar la información. Por otro lado se cuenta con una Librería de cintas LTO-5, la cual contiene dos Drive que son los encargados de gestionar el Backup de la información.</p> <p>Software:</p> <p>Se cuenta con el software de gestión y respaldo de la información Backup EXEC, el cual cuenta con soporte y garantía hasta octubre del 2020. Este es el medio actual para gestionar los Backup de información.</p> <p>Funcionamiento:</p> <p>Canal Capital, en aras de validar el funcionamiento, la operación y la continuidad de los servicios estableció la creación de Backup diarios, semanales, quincenales y mensuales en la prioridad full e incremental.</p>
Sistemas de Backup y contingencia de la información.	<p>Canal Capital, cuenta con el servicio de la plataforma de Google la cual administra las cuentas de correo institucional y esta permite un almacenamiento en la nube ilimitado. De esta manera se garantiza que los funcionarios y contratistas puedan contar con acceso a la información en el momento requerido y de esta manera se determina como plan de contingencia.</p>
Sistemas de Almacenamiento en la NUBE.	<p>Canal Capital, cuenta en la actualidad con diversos servidores virtuales a través de la plataforma VmWare y con sistemas operativos Windows y Linux. Esta plataforma cuenta con una configuración de alta disponibilidad soportada sobre un servidor físico el cual garantiza que en el momento que se presente algún incidente o falla sobre algún servidor, entre inmediatamente el que esta como contingencia toda vez que su operación es Activo - Pasivo.</p>
Sistema de Alta Disponibilidad.	<p>Canal Capital, cuenta con un sistema de almacenamiento SAN, el cual garantiza que la información contenida en los diferentes servidores físicos y virtuales repose sobre Discos Duros de tecnología SAS con interconexiones SATA y SCSI. Este garantiza que la información transaccional sobre cada servidor se encuentra alejada solamente sobre la SAN con el fin de que si algún servidor sufre algún incidente se puedan restablecer los servicios a través del respaldo de un servidor físico o virtual.</p>
Sistema de Almacenamiento.	

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

8. Escalamiento Interno

A continuación, se relacionan los nombres y números telefónicos de los responsables del área de sistemas, y los correspondientes turnos.

El Profesional Universitario de sistemas, a su vez informará al Subdirector/a Administrativo/a de la entidad, los hechos y el estado actual de la situación, con el fin de que se escale la información hasta el Secretario/a General y a su vez al Gerente, y de esta manera tener informado a los directivos de los hechos ocurridos.

Personal:

Profesional Especializado de sistemas

Mauris Antonio Ávila Velázquez

Teléfonos: 4578300 Ext. 5000

Celular: 3183726760

Profesional de apoyo TIC

German Darío Fajardo Perilla

Teléfonos: 4578300 Ext. 5050

Celular: 3124569015

Ingeniero de Infraestructura TI

Jose Miguel Torres

Teléfonos: 4578300 Ext. 5050

Celular: 3112829989

Ingeniero de Seguridad de la Información

Maryury Forero Bohorquez

Teléfonos: 4578300 Ext. 5050

Celular: 3164738756

Ingeniero de Software Intranet ERP/ERPC

Robinson Rincon Ramirez

Teléfonos: 4578300 Ext. 5000

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

Celular: 3108775481

Ingenieros de Soporte TI

Diego Montes Duran

Teléfonos: 4578300 Ext. 5050

Celular: 316 8237689

Jhon Hernandez

Teléfonos: 4578300 Ext. 5050

Celular: 3115360215

Ingeniero Soporte Intranet ERP/ERPC

Edith Lissette Rincon

Teléfonos: 4578300 Ext. 5050

Celular: 3192060154

Operación del área de Sistemas

Tiempos	Lunes - Viernes	Sábados - Domingos	Festivos
1	8:00 – 17:30	Por demanda	Por demanda

Tabla 5.6 Tiempo Ingenieros de soporte

Externo

En cualquiera de los siguientes casos debe contactar al ingeniero de soporte de los equipos o servicios afectados:

- Una vez controlada la situación de criticidad.
- Despues de intentar recuperar su estado de funcionamiento normal y no obtener respuesta favorable.
- Como medida de prevención para evaluar daños que no puedan ser detectados con las acciones o levantamientos de servicio rutinario.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		VERSIÓN: 02	
		FECHA: 02/12/2024	
		RESPONSABLE: SISTEMAS	

A continuación, se relacionan los nombres y números telefónicos de los contactos de soporte de los equipos involucrados en operación crítica del área de sistemas.

EMPRESA	CELULAR	CONTACTO	PBX
Help desk ETB	N/A	N/A	18000123737
Ordpago, Kardex	3005646803	Orlando Gonzalez	3005646803
Xertica Correo	187126370	soporte@xertica.com	6228320
GO	3112829989	Miguel Torres	6456062
Cirion	3175182602	Jair Hernandez	18000959493
Liberty	3155611374	Alejandra Muñoz	N/A

Tabla 5.7 Información empresas externas

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

9. Normatividad asociada al Plan

ISO/IEC 22301:2019 (Sistema de Gestión de la Continuidad del Negocio)

- **Descripción:** Esta norma internacional establece los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de la continuidad del negocio. Abarca la gestión de crisis, la gestión de riesgos y la recuperación ante desastres.
- **Relevancia:** La norma ISO/IEC 22301 es fundamental para asegurar que el DRP esté alineado con las mejores prácticas internacionales en cuanto a la continuidad de los negocios y la recuperación ante desastres.
- **Objetivo:** Garantizar que una organización sea capaz de continuar operando durante una crisis o después de un desastre, restaurando sus servicios críticos en el menor tiempo posible.

ISO/IEC 27001:2013 (Sistema de Gestión de Seguridad de la Información)

- **Descripción:** Establece los requisitos para implementar un sistema de gestión de seguridad de la información (SGSI) dentro de una organización. La norma cubre la identificación de riesgos, el tratamiento y la mitigación de esos riesgos, y la protección de la confidencialidad, integridad y disponibilidad de la información.
- **Relevancia:** Un DRP eficaz debe estar alineado con la protección de la información sensible y la continuidad operativa, que es un aspecto clave en la seguridad de la información. Además, esta norma es utilizada por organizaciones que gestionan datos críticos y requieren protección ante desastres.
- **Objetivo:** Asegurar que la infraestructura crítica de TI y los sistemas de información estén protegidos durante un desastre, y que los datos puedan ser restaurados rápidamente.

NIST SP 800-34 (Planificación de la Continuidad del Negocio y Recuperación ante Desastres)

- **Descripción:** Publicado por el National Institute of Standards and Technology (NIST), este documento proporciona un enfoque detallado para la planificación de la continuidad del negocio y la recuperación ante desastres en organizaciones de todos los tamaños.
- **Relevancia:** NIST SP 800-34 es una de las guías más completas para la creación y ejecución de planes de recuperación ante desastres, cubriendo aspectos técnicos, operacionales y organizacionales.
- **Objetivo:** Ayudar a las organizaciones a mantener la continuidad de los servicios esenciales ante un desastre, detallando pasos claros para la recuperación y los recursos necesarios.

	PLAN DE CONTINUIDAD DEL NEGOCIO ÁREA DE SISTEMAS	CÓDIGO: AGRI-SI-PL-002 VERSIÓN: 02 FECHA: 02/12/2024 RESPONSABLE: SISTEMAS	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
---	---	---	---

BS 25999 (British Standard for Business Continuity Management)

- **Descripción:** Es una norma británica que proporciona un marco para la gestión de la continuidad del negocio y la recuperación ante desastres, con un enfoque en la creación, implementación y mantenimiento de un sistema de gestión de continuidad empresarial.
- **Relevancia:** Aunque ha sido reemplazada parcialmente por la ISO 22301, BS 25999 sigue siendo relevante como un conjunto de directrices para gestionar la recuperación ante desastres, especialmente en el contexto de las organizaciones británicas.
- **Objetivo:** Ofrecer un conjunto claro de buenas prácticas para la continuidad del negocio y recuperación ante desastres, ayudando a las organizaciones a proteger sus operaciones críticas.

Normas Relacionadas con la Infraestructura y Tecnologías de la Información

ITIL (Information Technology Infrastructure Library)

- **Descripción:** ITIL es un conjunto de mejores prácticas para la gestión de servicios de TI, que incluye procesos para la continuidad del servicio, la gestión de incidentes y la recuperación ante desastres.
- **Relevancia:** ITIL ofrece una estructura para gestionar el ciclo de vida de los servicios de TI, y dentro de su marco, incluye procedimientos para la recuperación ante desastres que ayudan a restaurar los servicios tecnológicos críticos de manera eficiente.
- **Objetivo:** Asegurar la continuidad de los servicios de TI mediante la implementación de procedimientos efectivos de gestión de incidentes, gestión de cambios y planificación de la continuidad.