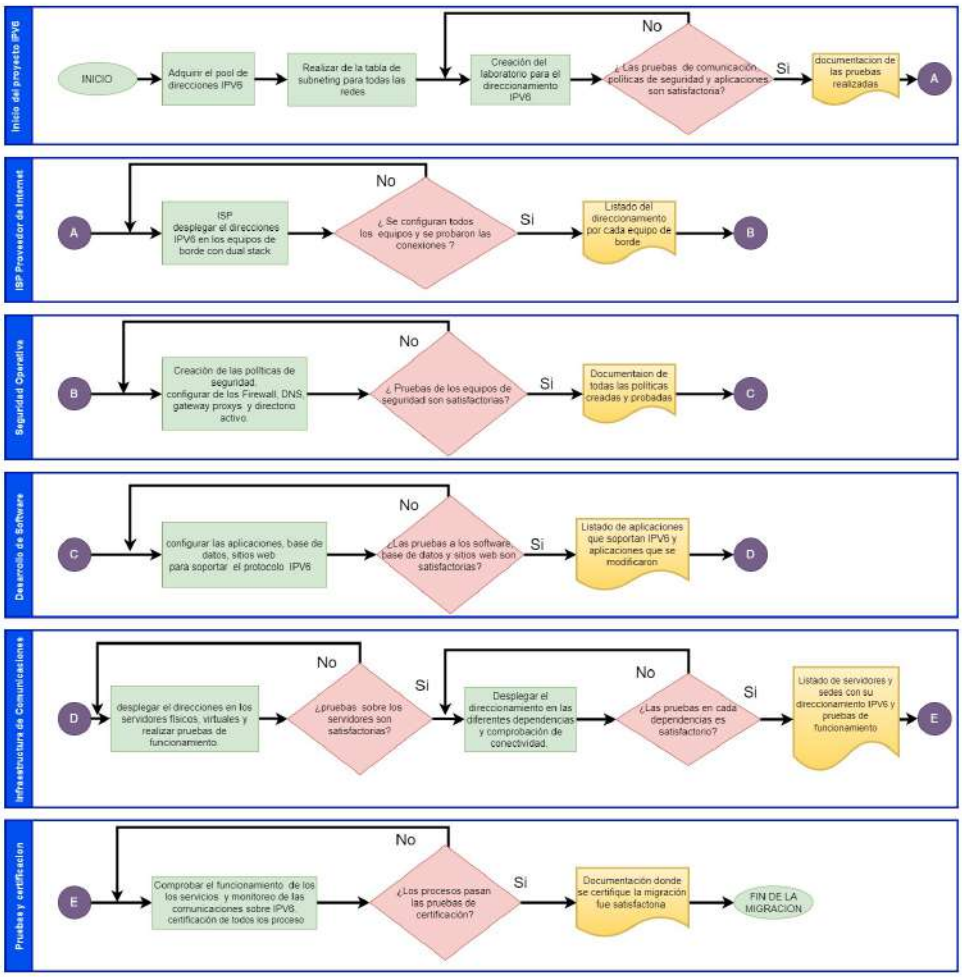
CATÁLOGO DE SERVICIOS DE TI

ID	NOMBRE	DESCRIPCIÓN FUNCIONAL	CATEGORÍA	USUARIOS	HORARIO DE PRESTACIÓN	CANALES DE ATENCIÓN A SOLICITUDES	ACUERDOS DE NIVELES DE SERVICIO (ANS)	ROL APROBADOR SOLICITUDES DE SERVICIO
SER-001	Acceso a internet por WIFI	Acceso a la red de colaboradores de la Entidad de manera inalámbrica a través de dispositivos móviles y computadores portátiles. La velocidad de navegación varia dependeiendo la ubicacion geografica y la cantidad de funcionarios y contratistas con velocidades que opcilan entre 5 Mbps y 120 Mbps	CONECTIVIDAD	Funcionarios y contratistas	24 HORAS, 7 DÍAS A LA SEMANA	Correo electrónico, Software de mesa de servicio (SAUS), Llamada telefonica, Wapp	Horarios de atención: El horario de atención es de lunes a viernes de 8:00 am a 6:00 pm. Excepciones de horario: Estos requerimientos o incidentes que se listan a continuación deberán ser atendidos independientemente del horario en que surjan efectos. Eventos del despacho del alcalde fuera del horario laboral y que se requiera acompañamiento de la oficina asesora de informática. Incidentes que afecten el acceso a servicios tales como caida de servidores, troncales, canales de acceso etc.	Gestor Infraestructura
SER-002	Acceso a la Intranet	La Alcaldia de Cartagena cuenta con una Red de datos interna para el manejo de las aplicaciones que no son de acceso al público.	CONECTIVIDAD	Funcionarios y contratistas	24 HORAS, 7 DÍAS A LA SEMANA	Correo electrónico, Software de mesa de servicio (SAUS), Llamada telefonica, Wapp	Horarios: De Acceso: Lunes a Jueves de 8:00 am a 6:00 PM Viernes de 8:00 am a 5:00 pm De Soporte: Lunes a Jueves de 8:00 am a 6:00 PM Viernes de 8:00 am a 5:00 pm	Jefe de Área
SER-003	Acceso a internet	Acceso a la red de colaboradores de la Entidad. La velocidad de navegación varia dependeiendo la ubicacion geografica y la cantidad de funcionarios y contratistas, con velocidades que opcilan entre 10 Mbps y 400 Mbps	CONECTIVIDAD	Funcionarios y contratistas	24 HORAS, 7 DÍAS A LA SEMANA	Correo electrónico, Software de mesa de servicio (SAUS), Llamada telefonica, Wapp	Horarios: De Acceso: Lunes a Jueves de 8:00 am a 6:00 PM Viernes de 8:00 am a 5:00 pm De Soporte: Lunes a Jueves de 8:00 am a 6:00 PM Viernes de 8:00 am a 5:00 pm	Jefe de Área
SER-004	Correo electrónico	Basado en Microsoft Office 365 con un buzón de almacenamiento de 1TB y acceso desde el cliente Microsoft Outlook o a través del navegador web	SOFTWARE Y APLICACIONES	Funcionarios y contratistas	24 HORAS, 7 DÍAS A LA SEMANA	Correo electrónico, Software de mesa de servicio (SAUS), Llamada telefonica, Wapp	Horarios: De Acceso: Lunes a Jueves de 8:00 am a 6:00 PM Viernes de 8:00 am a 5:00 pm De Soporte: Lunes a Jueves de 8:00 am a 6:00 PM Viernes de 8:00 am a 5:00 pm	Jefe de Área
SER-005	Servicio de entrenamiento y capacitación uso de las soluciones de TI	Servicio que suministra capacitación y entrenamiento sobre las funciones de los sistemas de información que maneja la entidad.	ASESORÍA Y CONSULTORÍA	Funcionarios y contratistas	DE 8:00 AM A 4:00 PM	Correo electrónico, Software de mesa de servicio (SAUS), Llamada telefonica, Wapp	Horarios: De Acceso: Lunes a Jueves de 8:00 am a 6:00 PM Viernes de 8:00 am a 5:00 pm De Soporte: Lunes a Jueves de 8:00 am a 6:00 PM Viernes de 8:00 am a 5:00 pm	Jefe de Área
		SAUS es la nueva herramienta para el manejo y gestión del Departamento						

SE CUENTA CON CATÁLOGO DE SERVICIOS TI

FLUJO-GRAMA DE LA IMPLEMENTACION IPV6

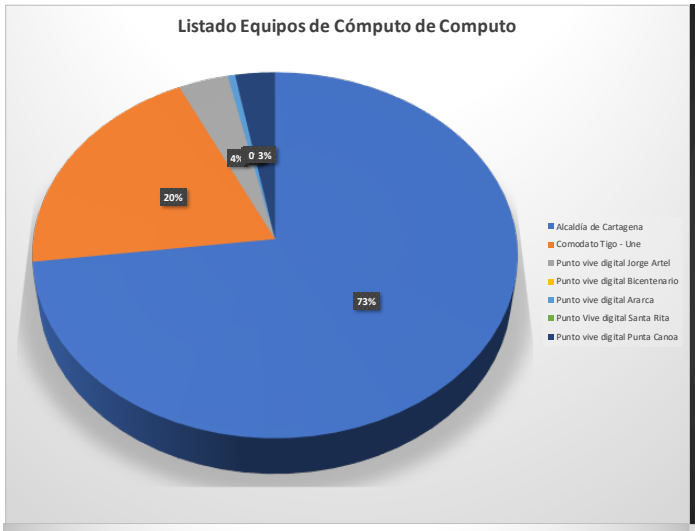


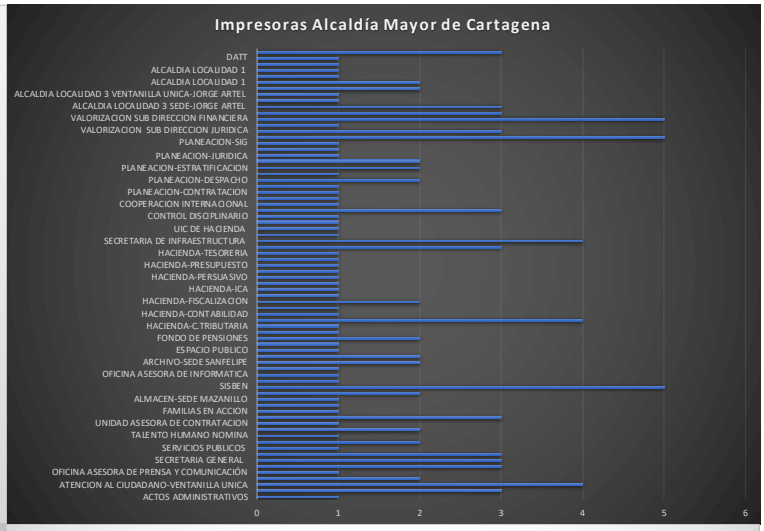
FLUJO-GRAMA DE LA IMPLEMENTACION IPV6			
	Elaborado por:	Revisado por:	Aporbado por :
Nombre	Luis Felipe Boada		
Cargo	Telecomunicaciones		
Fecha	8/08/2022		

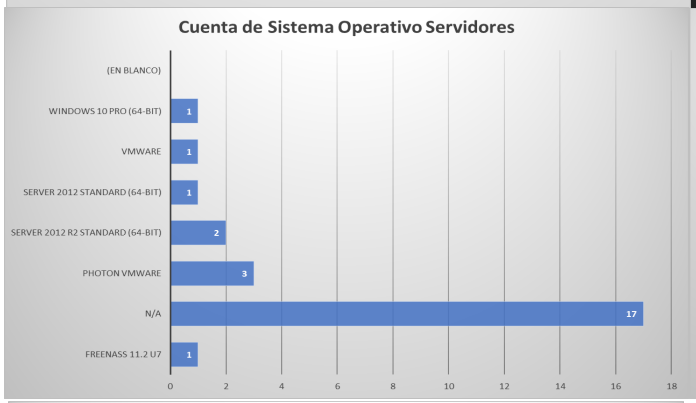
DIRECTORIO INFRAESTRUCTURA TI

ALCALDIA MAYOR DE CARTAGENA DE INDIAS

FECHA DE ACTUALIZACION : 31/12/2021







Planeación de IPv6

- **Tabla de actividades de la Fase I**

Fase I	Actividades Generales	Porcentaje de las actividad
Diagnóstico de la Situación Actual	Construcción del plan de Diagnóstico	100 %
	Inventario de TI (Hardware, Software)	90 %
	Análisis de la nueva topología de la infraestructura actual y su funcionamiento	100 %
	Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos	50%
	Planeación de la transición de los servicios tecnológicos de la Entidad	100%
	Validación de estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes.	98 %
	Identificación de esquemas de seguridad de la información y las comunicaciones	98 %

- **Fase II. Implementación del protocolo IPv6**

Fase II	Actividades Generales	Tiempo en meses de la actividad
Desarrollo del Plan de implementación	Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la Primera Fase.	20 %
	Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.	20 %
	Configuración del protocolo IPv6 en aplicativos, sistemas De Comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear Direccionamiento IP.	20 %
	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6.	30%
	Coordinación con el (los) proveedor (es) de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.	70%

Pruebas de Funcionalidad de IPv6

- **Tabla de actividades de la Fase IIII –**

Fase III	Actividades Generales	Tiempo en meses de la actividad
Pruebas de funcionalidad de IPv6	Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Entidad.	
	Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.	
	Afinamiento de las configuraciones de hardware, software y servicios de la Entidad.	

ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

PLAN DE RECUPERACION DE DESASTRES

VERSION	DESCRIPCION DE CAMBIOS
#.#	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

1. VALIDACION DEL DOCUMENTO

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre: xxxxxxxxxxxxxxx Cargo: xxxxxxxxxxxxxxxx Fecha: ##-##-####	Nombre: xxxxxxxxxxxxxxx Cargo: xxxxxxxxxxxxxxxx Fecha: ##-##-####	Nombre: xxxxxxxxxxxxxxx Cargo: xxxxxxxxxxxxxxxx Fecha: ##-##-####

Contenido

Introducción

El DRP Plan de recuperación de desastres es un plan de responsabilidad del área de Tecnologías de la Información (TI) que busca definir de manera estratégica una serie de acciones a realizar para cuando se ocasiona un desastre de manera tal que se asegure la continuidad de la operación de los activos de TI.

En la medida en que las organizaciones dependen más de sus infraestructuras tecnológicas para con ellas, recopilar, procesar, almacenar y transmitir información, más importancia debería tener su DRP, desde el punto de vista de TI la evaluación de los riesgos debe incluir Ciberataques, ransomware, fallas eléctricas, pérdidas o degradaciones de canales de comunicación, picos de tráfico por condiciones propias del negocio, etc.

Sin importar si la organización cuenta (que debería) con un BCP o si solo tenemos el DRP, estos dos planes deben quedar correctamente alineados, porque desde muchos puntos de vista son complementarios, el ejercicio realizado desde el punto de vista de levantamiento e identificación de los riesgos del negocio sirve para alimentar este plan, al igual que todas las acciones realizadas para el BIA.

Objetivo

Los objetivos que se deben cubrir con el DRP son los siguientes:

- Dar continuidad a los servicios informáticos de la Alcaldía de Cartagena en caso de presentarse una situación de contingencia mayor o catastrófica.
- Reducir al máximo los efectos negativos de un desastre sobre la plataforma de tecnología de la Alcaldía de Cartagena
- Maximizar el tiempo de respuesta, recuperación y disponibilidad de los activos tecnológicos de la Alcaldía de Cartagena.
- Apoyar las estrategias definidas por la organización en cuanto a los planes de continuidad del negocio.
- Proveer un enfoque organizado para el manejo de las actividades de respuesta y recuperación luego de un incidente no planeado o de una interrupción prolongada de los servicios de cómputo, con el objeto de evitar confusión y reducir la probabilidad de error.
- Ofrecer respuestas oportunas y apropiadas a cualquier incidente no planeado, reduciendo así el efecto de una interrupción de los servicios de cómputo.
- Recuperar las aplicaciones críticas del negocio de una manera oportuna, incrementando la habilidad de la compañía para recuperarse de una pérdida o daños a las instalaciones y servicios.

Alcance

Este Plan de Recuperación (DRP) para los Servicios de Cómputo y Comunicaciones en caso de Desastre (DRP), considera a las instalaciones de la Alcaldía de Cartagena ubicadas en el Datacenter Aduana.

El Plan incluye las acciones y procedimientos individuales, así como a los responsables de dar respuesta y recuperación de la operación normal de los servicios de cómputo y comunicaciones ante cualquiera de los siguientes escenarios:

- Cualquier incidente externo que pudiera causar una interrupción de los servicios de cómputo por un tiempo prolongado, como un corte en el servicio de Comunicaciones o fallas en el suministro eléctrico.
- Cualquier incidente que cause daño físico a las instalaciones, como incendio, temblor o inundación.
- Cualquier incidente que afecte indirectamente el acceso a las instalaciones, como una huelga, evacuación urgente a las instalaciones debido a una amenaza de bomba, o una amenaza externa como el incendio de algún edificio contiguo.
- Desastre regional no esperado tal como la erupción de un volcán, un terremoto o una inundación.
- Cierre de las instalaciones por recomendación de la Secretaría de Salud.

En marcaremos el DRP en la protección de los sistemas y plataformas tecnológicas descritas a continuación y que soportan los procesos misionales de la entidad:

Tipo de componentes	**Descripción**	**Tiempo de interrupción Toreable (RTO)**
Aplicaciones	- Sigob - Predis - Mateo - Página Web	24 horas ((1 día hábil)
Mensajería	Correo Electrónico	24 horas ((1 día hábil)
Comunicación	- Switch Core - Enlace con Internet - Enlaces MPLS	24 horas ((1 día hábil)
Servicios	- DNS	24 horas ((1 día hábil)

Infraestructura	-Sistema de Aire Acondicionado - UPS	24 horas ((1 día hábil)

Definición

BCP: Sigla en inglés (Business Continuity Plan) que hace referencia al Plan de Continuidad de Negocio, el cual integra el DRP, planes de contingencia y recuperación de procesos de la entidad, planes de emergencia, y plan de comunicación y administración de crisis.

BIA: Sigla en inglés (Business Impact Analisys), y hace referencia a un documento que identifica la disponibilidad requerida de la plataforma tecnológica para soportar los procesos de la entidad, con el fin de garantizar la continuidad en la prestación del servicio a los usuarios internos y externos.

DRP: Sigla en inglés (Disaster Recovery Plan), que hace referencia al Plan de Recuperación ante Desastres de Tecnología, el cual define los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

RPO: Sigla en inglés (Recovery Point Objetive), que corresponde a la cantidad de datos o información, en términos de tiempo, que tolera perder un proceso o servicio.

RTO: Sigla en inglés (Recovery Time Objetive), que corresponde al tiempo máximo de interrupción tolerable para un proceso, servicio, proveedor, sistema de información o plataforma tecnológica.

PLATAFORMA TECNOLÓGICA CRÍTICA: Hace referencia a los sistemas de información, servidores, bases de datos, sistemas de almacenamiento y respaldo, equipos y enlaces de comunicación que son críticos para soportar los procesos y servicios de la entidad.

Resumen de la Situación

El DRP está enfocado a la protección de la plataforma tecnológica que soporta los procesos misionales de Inspección, Vigilancia y Control.

Supuestos de la Planificación

La efectividad en la ejecución de este documento guía, ante la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente que afecte la plataforma tecnológica, se fundamenta en los siguientes supuestos:

- Se dispone de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación para los sistemas críticos.
- Los funcionarios que ejecutan esta guía, o los administradores de la plataforma, se encuentran Disponibles y no ha sido afectados por el desastre.

- El desastre no afectó simultáneamente el Centro de cómputo principal y el Sitio Alterno (Data Center Principal) donde residen las aplicaciones críticas.
- Se contará con un Centro de Alterno (Server Respaldo En Aduana) y estará habilitado en caso de contingencia.
- Solo el funcionario responsable activará el DRP.
- Se han realizado las pruebas de las estrategias y procedimientos al menos 1 vez al año, y han funcionado.
- Los funcionarios han participado en las pruebas y capacitaciones realizadas.
- La realización de respaldos de las bases de datos e información se realiza de acuerdo a los procedimientos y frecuencias establecidas.

ESCENARIOS DE DESASTRE

Los escenarios de desastre, interrupción mayor o un evento contingente que contempla este documento guía son:

Centro de Cómputo: No disponibilidad del centro de cómputo por:

- ATENTADO TERRORISTA
- INCENDIO
- INUNDACIÓN
- DAÑO SISTEMA AIRE ACONDICIONADO
- DAÑO EN SUMINISTRO ELÉCTRICO

Infraestructura de Comunicaciones: No disponibilidad de los servicios de comunicaciones por fallas en:

- SWITCH CORE
- FIBRAS OPTICAS DE CONEXIÓN
- ROUTER
- ENLACES DE COMUNICACIÓN CON ISP
- FIREWALL

Infraestructura de Servidores: No disponibilidad de la infraestructura por fallas en los servidores identificados como críticos en el inventario actualizado de servidores.

Infraestructura de Bases de datos, Almacenamiento y Respaldo: No disponibilidad de datos e información por:

- CORRUPCIÓN DE LA BASE DE DATOS

- BORRADO O PÉRDIDA DE DATOS
- FALLA TOTAL O PARCIAL DE LA SAN
- FALLA TOTAL O PARCIAL DE LA SAN
- FALLA EN SWITCH CONEXIÓN A LA SAN
- FALLA TOTAL O PARCIAL DEL SERVIDOR DE RESPALDO

Operación

Fase I: Preparación

Para esta fase, una vez tenidas en cuenta las alternativas técnicas que tenemos basadas en las necesidades de nuestra organización, debemos con la lista de recursos a incluir dentro del DRP, una vez esta lista de recursos estén debidamente priorizados bien sea por el equipo del BCP o por el propio ejercicio de DRP y teniendo claro el presupuesto asignado podemos definir cuál va a ser la estrategia que vamos a usar para que nuestros recursos tecnológicos estén preparados de la mejor manera posible para responder en caso de un desastre, la selección de contratar un data center de contingencia y alojar allí copia de mis principales servidores, junto con tener canales de datos redundantes que lleguen a este sitio o generar clúster de los servidores más importantes o tener servidores virtuales On Premise o en la Nube o protecciones de los datos basados en arquitecturas de SAN, NAS o arreglos RAID solo serán características técnicas necesarias para acompañar la estrategia, para los recursos que se han definido como indispensables para proteger por el plan de DRP, su selección dependerán básicamente del tiempo y el presupuesto que puedo invertir en el DRP.

Las opciones técnicas existen, los sistemas que permiten replicaciones de datos en tiempo real requieren capacidades de canales de datos similares o iguales a las de los entornos de producción y capacidades de software y hardware también similares o iguales, si incluimos en esta ecuación las bases de datos, el escenario puede ser complejo desde el punto de vista de presupuesto, pero seguramente encontraremos soluciones que se adecuen a las necesidades técnicas de nuestra organización.

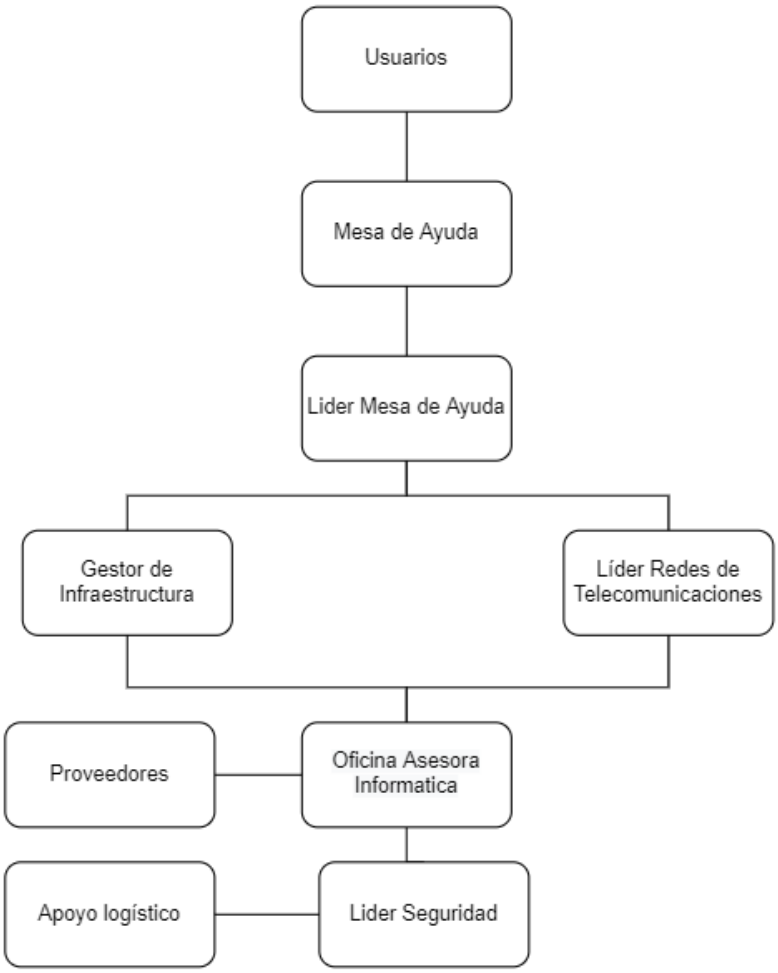
Fase II: Respuesta

El DRP debe contener una lista simple que el personal clave en la atención del DRP pueda seguir en el momento que se declare el desastre o que este sea inminente, y debería existir una lista simple para cada escenario posible de desastre, con las

actividades priorizadas en orden de importancia para que las personas que lo ejecuten tengan clara la prioridad de cada una de las tareas, teniendo en cuenta que la ejecución de las mismas se deberán realizar en medio de la ocurrencia del desastre y que tiene que estar lo más claras posible.

ARBOL DE ATENCION

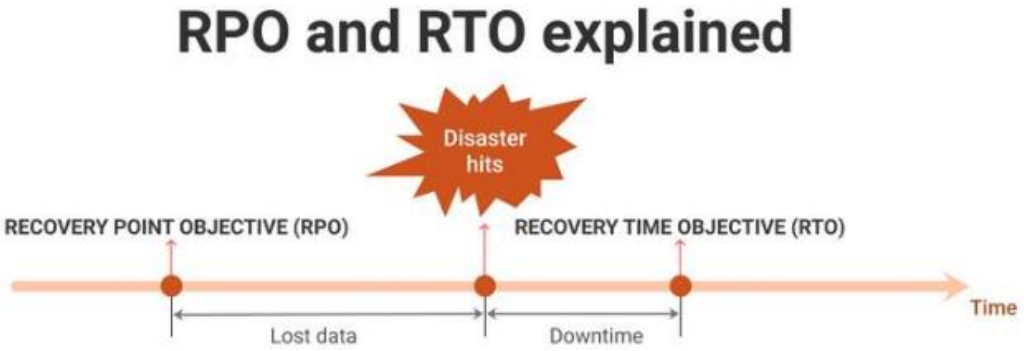
Cuando se presente un desastre, interrupción o evento contingente, se debe seguir la siguiente cadena de llamadas o comunicación:



Los datos de contacto para los funcionarios que ejercen estos roles se encuentran en la oficina de asesora informática.

Fase III: Recuperación

Deben existir dos grupos trabajando activamente, el grupo de recuperación que deberá trabajar en poner los sistemas a disposición de la organización a partir de la estrategia de DRP definida y en curso adicionalmente cumpliendo los tiempos definidos de RPO y RTO, y un equipo de restauración que deberá empezar a trabajar en la recuperación del sitio principal una vez las condiciones de seguridad sean las adecuadas para empezar con esta tarea y para la cual obviamente tendrán más tiempo que el equipo de recuperación, se debe evaluar la posibilidad de volver a las locaciones originales por lo que el equipo de restauración tendrá que hacer un trabajo muy arduo tanto como el montaje inicial de todas las facilidades, el estado de retorno a operaciones normales no se podrá dar hasta que no se vuelva a las instalaciones originales (si las consecuencias del desastre lo hacen factible), el documento de DRP debería contemplar precisamente cuando y en qué condiciones se dará por terminado el desastre y se da el retorno a las operaciones normales.



Fuente: [RTO and RPO: Disaster Recovery Strategy Essentials (msp360.com)]

Aplicativo	Memoria	Disco	S.O	BD	RPO	RTO
.NET 255.11	16,03 GB	156,19 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
.Net TEST 4.19	2,64 GB	163,24 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
255.13 plan B	9,65 GB	1,13 TB	Microsoft Windows Server 2008 (64-bit)		48H	72 H
Acronis Backup ESXI-Host-75	0 B	18,17 GB	Other 3.x Linux (64-bit)		48H	72 H
Acronis Backup VA ESXi host 75	1,53 GB	1,23 TB	Other 3.x or later Linux (64-bit)		48H	72 H
Acronis Backup VA ESXi host 76	1,47 GB	4,02 TB	Other 3.x or later Linux (64-bit)		48H	72 H
AD Connect	16,11 GB	86,24 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H

ALEPMWEBSERVICES 255.3	3,05 GB	114,17 GB	Microsoft Windows Server 2008 (64-bit)		4H	12 H
Aplication-server 1 4.32	4,04 GB	74,19 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
Base De Datos Oracle TEST 4.23	1,69 GB	1,18 TB	Oracle Linux 4/5/6/7 (64-bit)		48H	72 H
BOT	5,02 GB	48,19 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
CaribeTic-1 4.35	1,51 GB	102,16 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
CaribeTic-2 255.18	2,96 GB	303,12 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
COPSIS 255.15	7,15 GB	158,2 GB	Microsoft Windows Server 2008 R2 (64-bit)		48H	72 H
Coronavirus	0 B	106,17 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
DC PPAL 4.215	3,95 GB	44,17 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
DC Principal 4.215	0 B	191,92 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
DC Secundario 4.216	9,59 GB	110,2 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
Digiturno Alcaldia 255.5	11,05 GB	144,23 GB	Microsoft Windows Server 2012 (64-bit)		168H	72 H
drupal recuperado	14,92 GB	299,43 GB	Other 2.6.x Linux (64-bit)		48H	72 H
Drupal test ubuntu	0 B	204,18 GB	Ubuntu Linux (64-bit)		48H	72 H
Drupal Ubuntu Abierta	0 B	206,18 GB	Ubuntu Linux (64-bit)		48H	72 H
ESPACIO P REGISTRO VENDEDORES	4,83 GB	405,24 GB	CentOS 4/5/6/7 (64-bit)		48H	72 H
FEDORA 3.0	0 B	555,19 GB	Red Hat Enterprise Linux 7 (64-bit)		48H	72 H
kali-carlos	3,76 GB	24,17 GB	Debian GNU/Linux 8 (64-bit)		168H	72 H
LYNC 4.201	0 B	260,19 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
MIDAS	10,04 GB	630,21 GB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
Midas 255.4	10,03 GB	2,93 TB	Microsoft Windows Server 2012 (64-bit)		48H	72 H
Moodle	8,43 GB	416,22 GB	Microsoft Windows Server 2012 (64-bit)		72H	72 H
MYSQL 4.8	0 B	204,11 GB	Other 2.6.x Linux (64-bit)	MySQL 4.8	4H	2H
MYSQL TEST 4.25	215 MB	74,17 GB	Other Linux (64-bit)	MySQL 4.25	6H	4H
PAE 2	0 B	4,09 TB	Ubuntu Linux (64-bit)		48H	72 H
PAGINA WEB 255.20 https	0 B	198,67 GB	Red Hat Fedora (64-bit)		4H	4H
Pagina web 255.20 recuperado	0 B	123,74 GB	Other 2.6.x Linux (64-bit)		24H	24H
Pagina web 255.20 recuperado 2	0 B	123,69 GB	Other 2.6.x Linux (64-bit)		72H	72 H

PAGINA WEB NUEVA	1,11 GB	516,2 GB	CentOS 4/5/6/7 (64-bit)		4H	4H
PostgreSQL 4.6	0 B	102,22 GB	Other (32-bit)	PostgreSQL 4.6	4H	2H
PREDIAL 255.17	10,05 GB	210,21 GB	Microsoft Windows Server 2008 R2 (64-bit)		24H	72 H
predial test 4.42	2,15 GB	404,3 GB	Microsoft Windows 7 (64-bit)		72H	72 H
Proxy Inverso	7,98 GB	148,17 GB	Ubuntu Linux (64-bit)		2 H	1 H
SCCM 4.14	6,99 GB	555,2 GB	Microsoft Windows Server 2012 (64-bit)		24H	72 H
Server Backup Oracle	3,91 GB	459,23 GB	Microsoft Windows Server 2012 (64-bit)	Oracle	4H	2H
Server De Archivo 4.45	9,25 GB	610,16 GB	Microsoft Windows Server 2012 (64-bit)		4H	24H
Server Drupal 255.150 sacar info	1,12 GB	415,26 GB	Other 2.6.x Linux (64-bit)		24H	72 H
Server Drupal de Prueba	1,15 GB	405,33 GB	Other 2.6.x Linux (64-bit)		24H	72 H
server print OAI 4.31	3,92 GB	44,19 GB	Microsoft Windows Server 2012 (64-bit)		24H	72 H
Server Versionado	5,09 GB	108,19 GB	Microsoft Windows Server 2012 (64-bit)		24H	72 H
servidor de VOIP	4,02 GB	164,17 GB	Other Linux (64-bit)		24H	72 H
Servidor Web Linux 02-255.21	0 B	212,22 GB	Other (32-bit)		24H	72 H
SISBEN	32,03 GB	282,17 GB	Microsoft Windows Server 2012 (64-bit)		24H	72 H
Sophos Relay 1.4	16,06 GB	316,21 GB	Microsoft Windows Server 2012 (64-bit)		24H	72 H
SQL server 4.41	31,16 GB	5,86 TB	Microsoft Windows Server 2012 (64-bit)	SQL Server 4.41	4H	2H
SQL TEST 4.15	6,2 GB	3,46 TB	Microsoft Windows Server 2012 (64-bit)	SQL Server 4.15	6H	4H
Ubuntu Dadis	6,04 GB	206,24 GB	Ubuntu Linux (32-bit)		24H	72 H
Ubuntu Redmine	0 B	103,17 GB	Ubuntu Linux (64-bit)		24H	72 H
Ubuntu WikiJS	0 B	203,17 GB	Ubuntu Linux (64-bit)		168H	72 H
VCENTER	9,99 GB	354,18 GB	Other 3.x Linux (64-bit)		24H	72 H
VCloud (1)	2,83 GB	24,2 GB	Other 3.x Linux (64-bit)		24H	72 H
web test 254.2	1,15 GB	106,22 GB	Microsoft Windows Server 2012 (64-bit)		168H	72 H
WEBSERVICE TEST 255.7	941 MB	62,18 GB	Microsoft Windows Server 2008 (64-bit)		24H	72 H
webservice 255.9	3,72 GB	144,26 GB	Microsoft Windows Server 2012 (64-bit)		24H	72 H
webservices tomcat 4.7	4,01 GB	54,18 GB	Microsoft Windows Server 2012 (64-bit)		24H	72 H

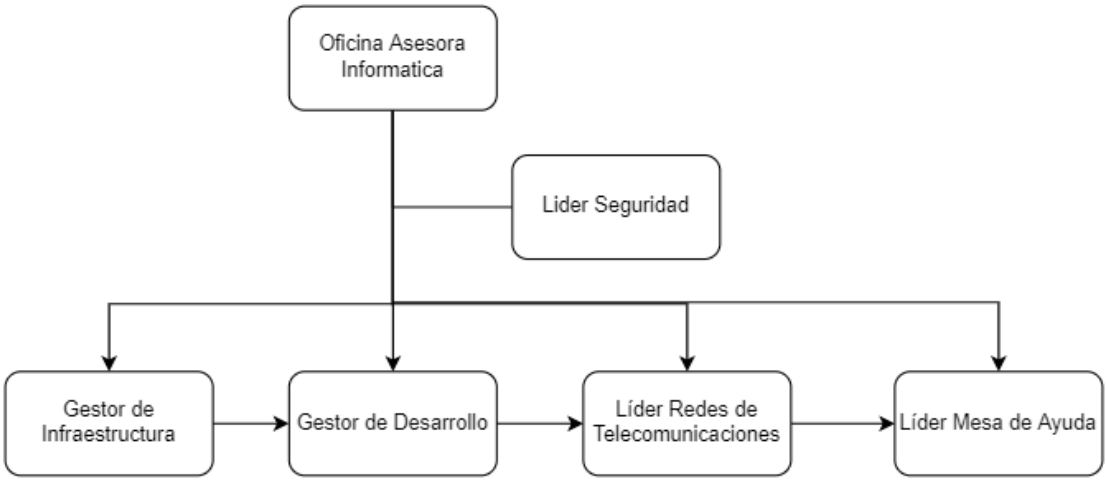
WIN10 ORACLE DBA	9,84 GB	510,21 GB	Microsoft Windows 10 (64-bit)	Oracle	4H	2H
WINDOWS SERVER 2012 DADIS	4 GB	154,2 GB	Microsoft Windows Server 2012 (64-bit)		24H	72 H
Wsus	9,99 GB	310,2 GB	Microsoft Windows Server 2012 (64-bit)		24H	72 H
zabbix red	0 B	42,27 GB	CentOS 4/5/6/7 (64-bit)		168H	24 H
zabbix red db	0 B	84,19 GB	CentOS 4/5/6/7 (64-bit)		168H	72 H

Fase IV: Mitigación

Esta fase del DRP se puede equiparar al proceso de lecciones aprendidas, una vez atendido el DRP y recuperado y restaurados los servicios, la organización debe revisar qué acciones se pueden acometer para mitigar aún más el riesgo que se materializo dentro del DRP, por ejemplo, si el problema fue eléctrico, revisar sus capacidades de UPS's o inclusive la necesidad de contar con generadores de energía propios, los miembros del equipo que atendieron el DRP y la alta dirección necesitan sentarse y revisar porque se dio el DRP y plantear alternativas realistas de mejorar en su infraestructura tecnología y que busque al menos que este tipo de desastre no se vuelva a presentar, si durante la atención del DRP se observan oportunidades de mejora en otros aspectos también se deben discutir y considerar.

Procedimientos detallados y sus responsables

ROLES Y RESPONSABILIDADES: Los roles y responsabilidades definidos en este plan deberán ser ejercidos por el personal seleccionado, de forma tal que se minimice el impacto y se actúe de forma adecuada



Las responsabilidades definidas para cada rol son:

ROL	ANTE DEL EVENTO INTERRUPCION	DURANTE EL EVENTO INTERRUPCION	DESPUES DEL EVENTO DE INTERRUPCION
Oficina Asesora Informática	- Velar por la actualization Del DRP y recursos requeridos. - Velar por la actualización, distribución y pruebas del DRP. - Gestionar la consecución de los recursos para el DRP. - - Comunicar a las personas que corresponda sobre la situación de contingencia.	- Evaluar y activar el DRP y las estrategias de recuperación y contingencia. - Comunicar al secretario general sobre el estado de la operación de Contingencia. - Informar el momento en que opera en contingencia y que puede suceder con la prestación del Servicio - Liderar la operación bajo contingencia. - Comunicar a la dirección el desastre, interrupción o evento contingente. - - Liderar el retorno a la normalidad.	- Velar por la actualización del DRP acorde con los inconvenientes y oportunidades de mejora visualizados durante el evento de interrupción. - Informar al secretario general sobre el retorno a la normalidad y agradecer la comprensión y apoyo de todos en esta situación.
Gestor de Desarrollo, Gestor de infraestructura, Líder de Redes y Telecomunicaciones, y Líder de Mesa de ayuda	- Comunicar necesidades de ajuste - Participar en la ejecución de las pruebas al DRP	- Evaluar el desastre, interrupción o evento contingente. - En caso de no contar con un contrato de mantenimiento vigente se debe tener un listado de posibles proveedores de acciones correctivas de solución. - Notificar al proveedor de Centro de Cómputo Alterno (Datacenter) (si aplica). - Comunicar el evento al Líder del DRP - Verificar disponibilidad y notificar al personal requerido para atender el evento.	

		- Ejecutar las guías de contingencia y recuperación. - Comunicar a los proveedores la activación del DRP. - Solicitar la corrección del componente afectado y realizar seguimiento de la solución. - Estar atentos para dar una correcta información a las personas que lo requieran. - Coordinar con los responsables el desplazamiento al Centro de Cómputo Alterno (Centro Datos Aduana), de los funcionarios que activarán la infraestructura. (Si aplica) - - Mantener informado al Líder del DRP	
Líder de Seguridad	Coordinar actividades de entrenamiento, documentación y actualización del DRP. Coordinar las actividades de pruebas del DRP. Identificar los recursos requeridos para la operación del DRP.	- Proveer soporte a los profesionales especializados. - Gestionar el alistamiento y disponibilidad del Centro de Cómputo Alterno (Centro Datos aduana). - Mantener informado al Líder del DRP	Actualizar el DRP, de acuerdo con los inconvenientes y oportunidades de mejora encontrados.
Apoyo Logístico	Participar en la ejecución de las pruebas al DRP	Apoyar a los involucrados en el DRP, en actividades administrativas y logísticas ante una contingencia, entre otras. Suministro de información de contrato Logística de desplazamiento, si es requerido	Reportar los inconvenientes y oportunidades de mejora del DRP

		Contacto de proveedores, si es requerido	

Integración de los Grupos de Respuesta y Recuperación

Los Grupos de Recuperación han sido creados para el control y la coordinación de las actividades de respuesta y recuperación a un incidente no planeado. Está conformado por personal de las áreas de sistemas y unidades de negocio, a fin de responder a cualquier evento que se presente, mediante la participación en el desarrollo del plan y en las actividades de respuesta y recuperación de los servicios de cómputo y comunicaciones.

Estos Grupos se han integrado con base en las diferentes plataformas y por aplicaciones, de acuerdo a funciones o responsabilidades específicas. Cada uno de estos grupos tiene actividades asignadas a realizarse antes, durante y después de un evento. Sin embargo, cabe resaltar que las actividades previas son parte de una rutina a fin de mantener el plan preparado en cualquier momento. Los grupos definidos son:

- Oficina Asesora informática
- Líder de Seguridad
- Gestor de infraestructura
- Gestor de desarrollo
- Líder redes de telecomunicaciones
- Líder mesa de ayuda

Para cada grupo se requiere la siguiente información:

NOMBRE	CARGO	DEPENDENCIA

Recuperación de los Servicios

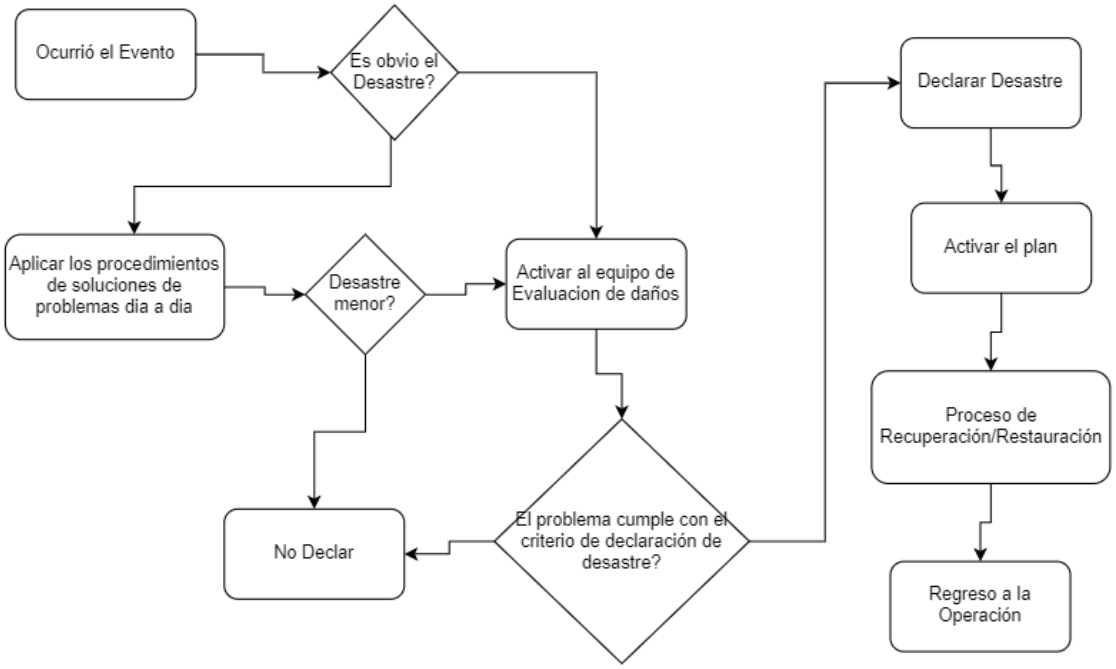
Deben existir dos grupos trabajando activamente, el grupo de recuperación que deberá trabajar en poner los sistemas a disposición de la organización a partir de la estrategia de DRP definida y en curso adicionalmente cumpliendo los tiempos definidos de RPO y RTO, y un equipo de restauración que deberá empezar a trabajar en la recuperación del sitio principal una vez las condiciones de seguridad sean las adecuadas para empezar con esta tarea y para la cual obviamente tendrán

más tiempo que el equipo de recuperación, se debe evaluar la posibilidad de volver a las locaciones originales por lo que el equipo de restauración tendrá que hacer un trabajo muy arduo tanto como el montaje inicial de todas las facilidades, el estado de retorno a operaciones normales no se podrá dar hasta que no se vuelva a las instalaciones originales (si las consecuencias del desastre lo hacen factible), el documento de DRP debería contemplar precisamente cuando y en qué condiciones se dará por terminado el desastre y se da el retorno a las operaciones normales.

Las actividades de los Grupos de Recuperación se dividen en actividades de Preparación y actividades de Respuesta y Recuperación.
Para que un Plan de Recuperación funcione adecuadamente, se requiere seguir ciertos pasos sencillos pero rutinarios con anticipación a lo que pueda suceder. Estas medidas preventivas se verifican y afinan con los procesos de pruebas.

Cada Líder de Grupo deberá ser responsable de que se sigan los pasos aquí indicados, a fin de que se mantengan actualizados los procedimientos y los recursos necesarios para la recuperación.

Autorización para declarar un DRP



Una vez que se haya identificado y reconocido un evento, el tiempo es vital. Los procedimientos que se presentan a continuación incluyen decisiones que son críticas con respecto al tiempo y que pueden estar basadas únicamente en la magnitud de la contingencia, en su evaluación, y en el impacto de éste en las operaciones del negocio.

Planes de pruebas (Con sus evidencias)

Para la realización de las pruebas, se pueden usar cinco tipos de pruebas, checklist test (listas de chequeo), Structured walk-throughs (recorridos estructurados), simulation test, (simulaciones), Parallel Test (Pruebas en paralelo) y full interruption test (pruebas de interrupción completas).

CheckList Test

En este tipo de pruebas se distribuye copias del DRP a los involucrados y se les pide que revisen que todo está en orden, con el propósito de conseguir los tres objetivos siguientes:

- Asegurar que entienden sus responsabilidades en el DRP.
- Ver que la información este actualizada o realizar las modificaciones que hagan falta.
- Ver que todas las responsabilidades del DRP estén cubiertas por los roles actuales de la organización.

Structured Walk-Through

Este tipo de test es referido a veces como ejercicio Table-top, en este tipo de prueba se reúne a todo el equipo de DRP y se le plantea un escenario que regularmente solo se conoce en el momento del ejercicio, y a partir de allí todo el equipo debe revisar el documento, siguiendo sus pasos y discutiendo entre ellos la pertinencia de los pasos declarados en el documento.

Simulation Test

En este tipo de prueba al equipo del DRP se le presenta un escenario y ellos deben ejecutar los pasos del DRP con el fin de verificar que lo que se declaró en el documento responde a las expectativas de la organización, haciendo una simulación de los pasos más representativos del DRP.

Parallel Test

En este tipo de test, las actividades del DRP se realizan como si se hubiera presentado el desastre, con la única diferencia que las actividades en el sitio principal no se interrumpen para no afectar la normal operación del negocio.

Full Interruption Test

En este tipo de prueba opera como la prueba en paralelo, sin embargo, involucra un riesgo alto, porque implica realizar las actividades como en un desastre real, incluyendo inactivar las facilidades del sitio principal para trabajar con las definidas en el DRP. Es el mejor tipo de pruebas, pero requiere madurez en el DRP y haber realizado todas las pruebas anteriores para asegurarnos que todo funcionara correctamente en este último tipo de prueba.
El documento del DRP es un documento vivo, y deberá ir madurando y cambiando basado en los riesgos y evolución de los sistemas de la organización, este tipo de documentos se debe actualizar de manera frecuente al menos una vez al año, y la realización de las pruebas deben ser al menos un par de veces al año o más, algunas regulaciones piden realizar las pruebas, documentarlas y entregarlas como parte del cumplimiento regulatorio.

Bibliografía

- Disaster Recovery Institute https://drii.org/
- https://www.mintic.gov.co/Gestionti/articles5482_G11_Analisis_Impacto.pdf
- MENEZES, A.). (1965-). (1997). Handbook of Applied Cryptography /ALFRED J. MENEZES, PAUL C. VAN OORSCHOT, SCOTT A. VANSTONE. BocaRaton [etc.]: CRC Press.
- Proal, C. (30 de 11 de 2012). Conceptos Básicos - Seguridad Informática. Obtenido de Conceptos Básicos Seguridad Informática:
- http://www.carlosproal.com/seguridad/seguridad01.html
- Cariacedo Gallardo, Justo. Seguridad en Redes Telemáticas. McGraw Hill, 2004.
- Ramió Aguirre, Jorge. Seguridad Informática y Criptografía v 4.1 Dpto. de Publicaciones E.U.I., 2006 (edición impresa). Libro electrónico gratuito disponible en la página Web del autor

El futuro digital es de todos

MinTIC

IMPLEMENTACIÓN DEL PROTOCOLO IPV6

Transformación Digital para TODOS

GOBIERNO DIGITAL

TIC Mejor País

Tabla de Contenido

1. Introducción

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

las redes de telecomunicaciones han venido creciendo exponencialmente generando una mayor demanda de servicios y oportunidades en la red mundial de Internet; con el aumento de las tecnologías computacionales y de comunicaciones, ha aumentado el proceso de innovación tecnológica en los diversos dispositivos tanto alámbricos como inalámbricos, como por ejemplo, celulares, puntos de acceso, tabletas, servidores, equipos de almacenamiento entre otros, que comenzaron a incrementar la conectividad en muchas redes en el mundo y para ello han tenido que hacerlo con direcciones de Internet que permiten establecer conexiones para cada elemento conectado a la red, estas direcciones se conocen como direcciones IP (Internet Protocol Versión 4), que en la actualidad entraron a una fase de agotamiento fi nal, así mismo en el año 1992 la Internet Engineering Task Force IETF a partir de diversos grupos de trabajo, definió el RFC 2460 (Especificaciones del Protocolo Internet Versión 6 (IPv6) que dio origen al nuevo protocolo de conectividad denominado IPv6 o IPng (Next Generation Internet Protocol).

De este modo, el protocolo IPv6, hace posible que todos los dispositivos tecnológicos usados para la conexión a Internet tengan una dirección en IP, la cual facilitará la conectividad en banda ancha, ofreciendo más y mejores servicios poniéndolos al alcance de toda la población a fin de estimular y ofrecer oportunidades para el desarrollo tecnológico y la transformación digital a nivel mundial.

Para cumplir con los objetivos de innovación tecnológica que exige el país, las entidades del país deben entrar en el proceso de transición del protocolo IPv4 hacia el nuevo protocolo IPv6 siguiendo las instrucciones descritas en la

Resolución 2710 del 3 de octubre de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones, que busca promover la adopción de IPv6 en Colombia.

para atender esta necesidad inminente de innovación tecnológica en el país, el MinTIC, mediante este instrumento, desea proyectar los lineamientos para diagnosticar, sensibilizar, desarrollar e implementar el protocolo IPv6 en las entidades del estado, con el propósito de adoptar el nuevo esquema de funcionamiento de manera paralela con el actual protocolo IPv4, de conformidad con la Resolución 2710 de octubre de 2017, garantizando que las infraestructuras de hardware, software y servicios continúen operando normalmente en las distintas instituciones del país.

El objetivo final de esta transición es que toda Internet funcione exclusivamente con IPv6 y la desaparición final de IPv4, manteniendo la coexistencia con ese mientras sea preciso, evitando así costos de nuevas transiciones en el futuro. El IETF ha definido estos mecanismos como “IPv6-only with
IPv4aaS” (sólo IPv6 con IPv4 como servicio), permitiendo con ello que, antiguos dispositivos, servicios o aplicaciones que no puedan ser actualizados a IPv6, sigan funcionando de forma transparente con IPv4, aun cuando las redes intermedias sean exclusivamente IPv6, dada la falta de direcciones IPv4.

2.JUSTIFICACION

IPV4 es el primer protocolo que se creó para el uso de la Internet. Sin embargo, el direccionamiento IP que emplea se ha agotado, lo que limita el crecimiento del internet y dificulta la adecuación de nuevas aplicaciones, aun cuando a nivel mundial se presenta el crecimiento continuo de sitios web, aplicaciones y servicios que requieren una IP pública única, como por ejemplo, los teléfonos con tecnología VoIP, televisión y radio, seguridad, video vigilancia, mercados virtuales, juegos, videoconferencia, redes inalámbricas, etc.

En la actualidad, se necesitan protocolos que garanticen unas

características adecuadas a los tipos de tráfico de datos, pues cada día crece de forma constante el número de usuarios que acceden a la red desde diversos dispositivos. Esta creciente demanda de conectividad ha hecho que cada vez sean más escasas las IP públicas y se necesiten mejores prácticas para salvaguardar el flujo de información.

En consecuencia, los administradores de redes y servicios han explorado múltiples formas de garantizar la seguridad de los usuarios y la calidad del servicio que reciben, por ejemplo, con el uso de Network Address Translación (NAT). No obstante, lograr este propósito no es fácil y más si se consideran dos factores:

1. La falta de disponibilidad de ancho de banda necesario para soportar los servicios actuales.
2. El uso creciente de internet como plataforma de negocios (E-comerce, E-Banking), hace que la seguridad en la red sea necesaria, si se quiere suplir las expectativas de negocio generadas y brindar protección a los distintos actores de los procesos.

Ante el panorama descrito, surge el protocolo IPV6, el cual tiene como objeto subsanar las falencias observadas en el protocolo IPv4, como lo son: el agotamiento de direcciones IP y la seguridad de la información a través del envió cifrado y autenticado de paquetes, lo que permite mantener una transmisión más confiable y segura de la Información. También, posee un sencillo mecanismo de autoconfiguración y velocidad en la transmisión, además entre sus características más importantes se resaltan la cantidad ilimitada de espacio de direcciones IP y la calidad del servicio.

Ahora bien, teniendo en cuenta las bondades de este nuevo protocolo el Ministerio de las TIC emitió la circular 002/2011, mediante la cual busca que todas las entidades que hagan parte del programa de Gobierno en línea, empiecen a llevar a cabo los estudios para la migración al protocolo IPV6.

La Alcaldía mayor de Cartagena, adelanta el programa de la implementación de IPV6 aplicando todas las medidas de seguridad y pautas que dicta MICTIC, para garantizar la mejor implementación en nuestra infraestructura de servicios y telecomunicaciones, para convertirnos un referente para las demás sedes descentralizadas que hacen parte de la Alcaldía mayor de Cartagena.

De igual manera, esto causara una mejora de los servicios que prestamos, beneficiando a sus usuarios y brindando más cobertura y calidad

Por último, se resalta que el camino hacia IPV6 es un paso de evolución e integración necesaria, en particular para la Alcaldía de Cartagena,

asegurándonos así, un futuro frente a las nuevas innovaciones del auge tecnológico que aumenta cada día y su globalización de los servicios hacia los usuarios.

4. OBJETIVOS

4.1 Objetivos generales.

Elaborar propuesta técnica para planear y diagnosticar la adopción del Protocolo IPv6, que permita realizar el despliegue del protocolo en todas las sedes de la Alcaldía mayor de Cartagena y demás entes que hacer parte de la administración del departamento.

4.2 Objetivos Específicos

- Identificar la mejor estrategia que permita adoptar del protocolo IPv6 para la infraestructura tecnológica y de servicios, de tal manera que sea transparente para el usuario y el mejor funcionamiento de los aplicativos y servicios que prestamos.
- Elaborar y validar el inventario de activos de TI de información de servicios tecnológicos de la Entidad y su nivel de cumplimiento con el protocolo IPv6.
- Analizar, diseñar y desarrollar el plan de diagnóstico del protocolo IPv4 a IPv6.
- Proporcionar las recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6, en caso de que aplique.
- Documentar el plan de manejo de excepciones.
- Documentar los lineamientos de Implementación de IPv6 con concordancia con la política de seguridad de la información y los controles de seguridad informática de la entidad.
- Definir las directrices del plan de direccionamiento de IPv6 en la red de la Entidad.
- Realizar el informe de preparación para la adopción de IPv6.

3.BENEFICIOS DE LA TRANSICION

Los siguientes puntos son los beneficios que representa un proceso de transición de IPv4 a IPv6 que son importantes tener presente al momento de adoptar el nuevoprotocolo con éxito, ellos son:

- La posibilidad de tener un mayor número de equipos conectados a la red de lasentidades al ser implementada esta solución.

- Proceso técnicamente transparente para los usuarios de la red de comunicaciones y sus distintos servicios dentro de las organizaciones.

- La posibilidad de incrementar la movilidad de los usuarios al tener un número mayor de direcciones IP para la conectividad.

- Mejora de la seguridad a nivel de direccionamiento IP de la red en virtud de la arquitectura del nuevo protocolo y sus servicios.

- Reducción de los costos al implementar la solución de IPv6, en este sentido los costos podrían ser mayores de no implementarse el nuevo protocolo en las entidades.

- Se facilitará la aparición de nuevas aplicaciones y servicios sobre una gran variedad de plataformas.

- Gran número de direcciones IP para conexiones a Internet con el mundo exterior,facilitando el crecimiento de nuevas tecnologías como el internet de las cosas, las ciudades inteligentes, redes de sensores, entre otras.

- Los Proveedores de Servicio de Internet, tendrán que preparar el proceso de transición de IPv6, mediante la creación de un *Backbone* nativo de IPv6 que apoye a los clientes en el enrutamiento de las nuevas direcciones IPv6 a fin de garantizar la publicación de servicios y aplicaciones que se consideren pertinentes hacia internet para todas las entidades del Gobierno.

- Para el ciudadano en general, la implementación de IPv6 será un proceso gradual cuya responsabilidad no será del gobierno, sino del proveedor del servicio de internet directamente y no deberá generar costos directos.

4.MARCO CONCEPTUAL

TCP/IP (Protocolo de Control de Transporte / Protocolo de Internet)

Este es un conjunto de protocolos de uso extendido y son conocidos como protocolo de control de transmisión / protocolo de Internet o TCP/IP, sirven para conectar redes de todos los tamaños son valorados por su capacidad para permitir comunicaciones entre diferentes equipos.

TCP/IP muestra una arquitectura de red parecida al modelo de red OSI, pero este no establece tantas distinciones como OSI entre las capas superiores del conjuntode protocolos

Figura 1. Capas de TCP/IP

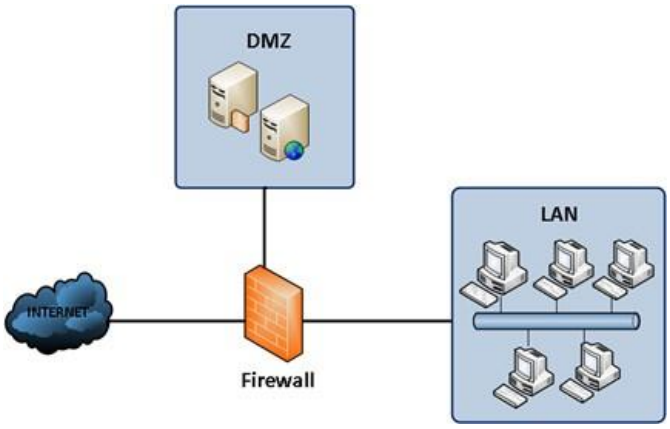
En esta figura se observan las diferentes capas del modelo TCP/IP en donde sus funciones y servicios son variables, cada capa se ocupará de su nivel inferior para solicitar dichos servicios y del nivel superior para devolver los resultados.

IPV4 (Protocolo de Internet Versión 4)

Con el aumento extensivo de internet y los diversos dispositivos interconectados, se ve la necesidad de mejorar el protocolo IP, desarrollándose la versión cuatro de este protocolo (IPV4), el cual utiliza una dirección única de 32 bits para identificar una máquina y la red a la cual está conectada.

DMZ (zona desmilitarizada)

De igual manera se observaron problemas de seguridad, para lo cual se implementaron técnicas como el DMZ (zona desmilitarizada) el cual es un diseño conceptual de red cuyo principal objetivo es proteger la red interna de una organización, separando los servicios privados como son servidor Base de Datos, servidor de aplicaciones, de la red pública (internet); así como asegurar la transferencia de datos.



Esta figura muestra una red donde se tiene un segmento interno que es la LAN de la Organización, y se tiene otro segmento que es la DMZ donde se ubican los servidores de acceso público, al cual se podrá acceder sin exponer la red interna, la cual está protegida por un firewall.

IPV6 (Protocolo de Internet Versión 6)

Los desarrolladores del protocolo IPV4 no previeron la gran acogida que ha tenido internet, generando un crecimiento exponencial y por ende el direccionamiento de IPV4 se ha agotado.

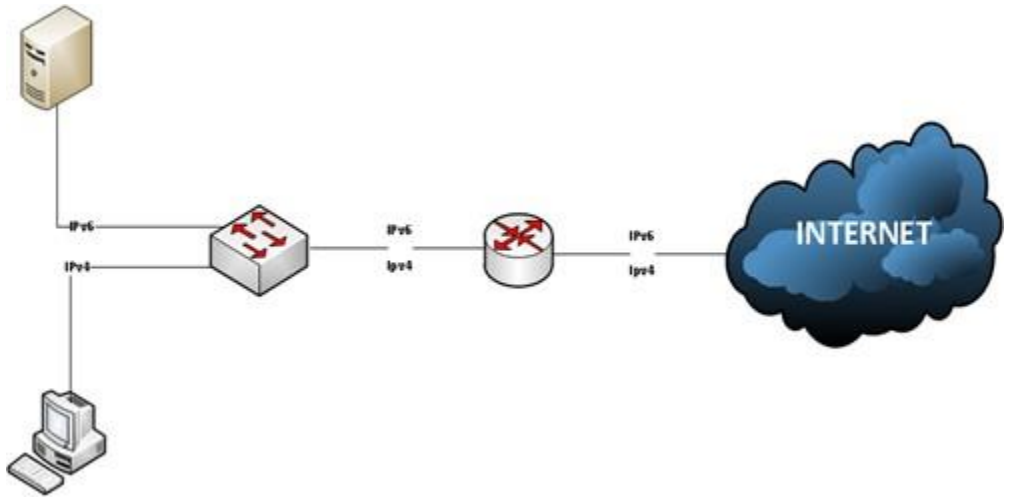
Como solución a esta falencia en el protocolo IPV4, se implementó la versión 6 del protocolo (IPV6) En esta versión se mantuvieron las funciones de Ipv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose

Nuevas características, y lo principal es que IPV6 trabaja con direcciones de 128 bits, lo que hace suponer que a cada persona del planeta se le puede asignar una dirección IP.

Dual Stack (Doble Pila)

El desarrollo de IPV6 será progresivo conviviendo inicialmente con la versión cuatro del protocolo (IPV4) para lo cual se plateo el uso del mecanismo denominado Dual Stack (Doble Pila), este permite a un nodo utilizar un stack Ipv4 y un stack Ipv6 simultáneamente teniendo dos ventajas:

Por un lado, un nodo con Dual Stack puede comunicarse con nodos que solo tienen Stack IPV4 de manera nativa y por el otro también puede comunicarse con nodos que solo tengan habilitado el Stack IPV6 de manera nativa.



En esta figura se observa un mecanismo de transición de IPv4 a IPv6, de una manera en la cual los dos protocolos funcionan simultáneamente hasta lograr un total cambio al protocolo IPv6, esta transición se lleva a cabo de manera suave.

Confidencialidad

Cuando se habla de confidencialidad de la Información, se habla de prevenir el acceso no autorizado ya sea en forma deliberada o no intencional a la información. Se puede perder la confidencialidad de

muchas maneras, un ejemplo común es cuando se publica intencionalmente información confidencial de la organización o ente relacionado que es divulgada a personas, entidades o procesos no autorizados.

Por ende esta propiedad de la información asegura el acceso a la información solo a aquellos individuos o grupos que tengan la correspondiente autorización para el uso y tratamiento de dicha información (NTC-ISO, 2013).

Integridad

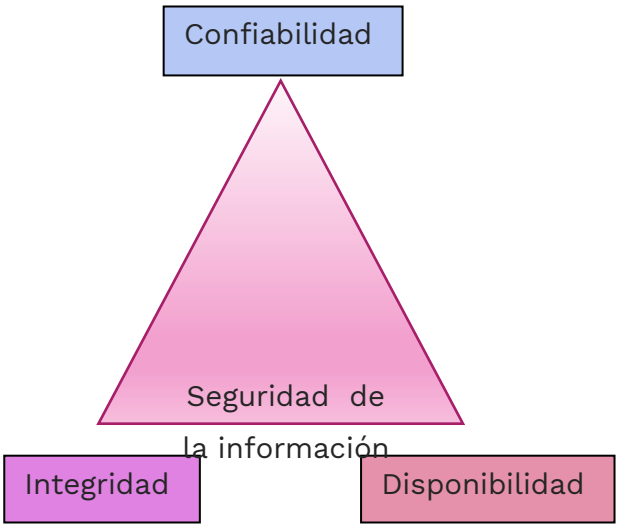
La Integridad de la información es la propiedad que busca asegurar que no se realicen modificaciones a los datos o procesos tanto por personas no autorizadas como por personal autorizado para que estos datos sean consistentes y fidedignos tanto interna como externamente, y así lograr que la información sea exacta, completa y consistente y solo sea modificada cuando sea necesario previa autorización (NTC-ISO, 2013).

Disponibilidad

Esta propiedad, característica o cualidad de la Seguridad de la Información busca asegurar que el acceso a la información sea confiable y oportuna y garantizar de manera efectiva que las personas, aplicaciones y entidades autorizadas tengan acceso a la información y sus procesos asociados cuando lo requieren.

Así mismo la disponibilidad debe asegurar que el sistema se mantiene funcionando eficientemente y es capaz de recuperarse rápidamente en caso de fallo, previniendo la interrupción de los procesos y actividades, previniendo interrupciones no autorizadas de los recursos informáticos (NTC-ISO, 2013).

Pilares de la seguridad



La Confidencialidad, Integridad y Disponibilidad son los tres pilares identificados como fundamentales según la norma ISO 27001:2013 para una correcta administración de la Seguridad de la Información (NTC-ISO, 2013).

Acuerdos de Nivel de Servicio:

EL modelo de Acuerdo de Nivel de Servicios (Service Level Agreement, SLA) consiste en un contrato en el que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes, así, refleja contractualmente el nivel operativo de funcionamiento, penalizaciones por caída de servicio, limitación de responsabilidad (ITIL).

Los principales puntos a cubrir deben ser:

- Tipo de servicio.
- Soporte a clientes y asistencia.
- Provisiones para seguridad y datos.
- Garantías del sistema y tiempos de respuesta.
- Disponibilidad del sistema.
- Conectividad.
- Multas por caída del sistema.

RFC (Request for Comments,)

Las RFC (Peticiones de comentarios) son un conjunto de documentos que sirven de referencia para la comunidad de Internet, que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general. (IPv6Mx)

No repudio

El no repudio es cuando un emisor no puede negar que hizo algún tipo de transacción electrónica, porque el destinatario tiene pruebas suficientes, de que el del origen del envío, lo cual evita que el emisor pueda hacer cualquier tipo reclamación sobre dicha transacción (NTC-ISO, 2013).

COBIT: *(*Objetivos de control de información y tecnologías relacionadas*)*, publicado por ITGI, es un modelo aceptado de buen control de la información, las IT y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno sobre IT y mejorar los controles IT. Contiene objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores de éxito críticos y modelos de madurez (COBIT).

ISO 27000: Es un conjunto de estándares desarrollados o en fase de desarrollo-por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña (NTC-ISO, 2013).

5. MARCO TEORICO

Instituciones públicas y privadas están trabajando mancomunadamente con el fin de (TIC) impulsar la expansión de IPv6, incluyendo Instituciones como la Comisión Europea y el Departamento de Defensa Norteamericano. A nivel de los países de habla Hispana, fue México el precursor en la investigación y experimentación con el protocolo IPv6, seguido de países como España, Chile, Argentina, Uruguay,

Brasil, entre otros. En Colombia lentamente se está comenzando a surgir en la temática de IPv6, con las siguientes entidades la Corporación Autónoma Regional de Boyacá (Corpoboyacá), el Servicio Geológico

Colombiano, el Instituto Nacional Penitenciario (INPEC), Ministerio de Minas y Energías, y el Ministerio de Tecnologías de la Información y las Comunicaciones (TIC, 2014)

La labor de acompañamiento contempla las siguientes actividades:

- Marco de Referencia sobre la importancia de adoptar IPv6.
- Divulgación de los últimos anuncios de LACNIC en materia de agotamiento dedirecciones IPv4 en países de Latinoamérica y del Caribe.
- Explicación del marco legal de soporte sobre IPv6 (Circular 002 de 2011 yManual de GEL 3.1).
- Exposición sobre lineamientos para la transición de IPv4 a IPv6.
- Explicación del impacto de implementar o no el nuevo protocolo en la sentidades.
- Entrega de documentación y aclaración de dudas o inquietudes.

UniNet, una Red Universitaria, sin ánimo de lucro cuyo fin es integrar servicios proporcionados a través de Internet, para ofrecerlos a comunidades virtuales, creadas por personas y organizaciones, lidera un proyecto de implementación de redes basadas en IPv6, del cual ya forman parte la Universidad de Magdalena y la del Cauca, mencionando también a la Universidad de Pamplona con la implementación del túnel con la Universidad Nacional Autónoma de México.

IPv6 es la actualización del Protocolo de Internet, el cual es fundamental para el funcionamiento de las Redes. Desde que se inició el diseño de IPv6 se previó que tendría que coexistir con IPv4 durante un largo período de tiempo por su lenta implementación. En la actualidad existen millones de dispositivos, aplicaciones y servicios, que requieren de una IP pública. Internet ha llegado a ser una infraestructura de un avance exponencial.

Entre los inconvenientes que se presenta al momento de realizar la transición de IPv4 a IPv6 es la incompatibilidad entre los protocolos, por este motivo, IPv6 ha sido diseñado junto a un conjunto de mecanismos de transición, entre ellas encontramos la doble pila de protocolos o Dual Stack, los cuales permiten la coexistencia de ambos protocolos, IPv4 e IPv6, el tiempo necesario que se lleve a cabo los procesos de transición, de igual manera esto dependerá de diferentes aspectos relacionados con las necesidades propias de las organización y países.

Dichos mecanismos de transición contribuyen a la integración de IPv6 en la red Internet que actualmente trabaja con IPv4. IPv6 ha madurado tanto que hoy es posible hacer con esta tecnología de red todo lo que podemos hacer con IPv4 y aun mucho más, mejorando la calidad y la seguridad de la red. Se pueden anunciar mayores desarrollos y mejoras

a los servicios y aplicaciones gracias a la implantación de IPv6.

IPv6 contribuirá a mejorar Internet. En un futuro próximo, veremos toda la red Internet soportando tanto IPv4 como IPv6, e incluso se llegará al punto en que algunas redes dejarán de soportar IPv4. Por supuesto, la comunicación extremo-a- extremo con IPv4 seguirá siendo posible, porque utilizaran mecanismos de transición.

La Unión Europea, a través de la Comisión es una de las instituciones que está apoyando con más fuerza el despliegue definitivo del nuevo protocolo de Internet. Muestra de eso, en enero 2004 se desarrolló un evento en Bruselas (Bélgica), patrocinado por los proyectos de investigación 6Net y Euro6IX, con el fin de presentar de forma oficial el servicio de conectividad global de IPv6 para la comunidad investigadora, que ha contado con la colaboración de la red de investigación paneuropea Géant y de otras redes a escala mundial.

Entre los diferentes antecedentes que se pueden mencionar a nivel mundial se puede encontrar:

- 6SOS: La cual es una organización patrocinada por el Ministerio de Ciencias yTecnología de España que tiene como principal función dar a conocer IPv6 a las PYMES y profesionales facilitándole acceso gratuito a información, preguntas y consultorías con el fin de establecer los mecanismos necesarios para lograr hacer una transición satisfactoria al nuevo protocolo de comunicación. (6SOS)
- IPv6 Task Force Español: se constituye como un grupo de trabajo, al modo del IPv6 Task Force Europeo, y otros grupos similares, con el objetivo básico de estudiar las perspectivas de la tecnología IPv6 y las acciones a tomar para quela implantación de la misma responda a las necesidades del mercado español (IPv6 Task Force).

Características del Datagrama en IPV6

Entre las principales características de IPv6 están:

- Cabecera de longitud fija (40 bytes) conformado por 8 campos.
- Fragmentación de los datagramas sólo es realizada en el host de inicio.
- Eliminación del campo de suma de chequeo.
- La cabecera de extensión, donde se puede implementar nuevas soluciones, está fuera de la cabecera, permitiendo que las aplicaciones puedan ser adaptadas a los nuevos problemas que se presenten.
- Direcciones lógica o IP de 128 bits, permitiendo disponer 340sextillones de direcciones IP.

Cabecera del protocolo IPV4

VERS	HLEN	TIPO DE SERVICIO	LONGITUD TOTAL	
IDENTIFICACION			BANDERAS	DESPLAZAMIENTO DE FRAGMENTO
TIEMPO DE VIDA		PROTOCOLO	SUMA DE VERIFICACION DEL ENCABEZADO	
DIRECCION IP DE LA FUENTE				
DIRECCION IP DEL DESTINO				
OPCIONES (en caso de existir)				RELLENO

	Nombre del campo se mantiene
	Campo eliminado en IPv6
	Se cambió nombre y ubicación
	Nuevo campo en IPv6

Esta figura muestra cómo se encuentra compuesta la cabecera del protocolo deIPv4 y cada uno de los campos que componen el datagrama.

Cabecera del protocolo IPV6

VERSION	DS	ETIQUETA DE FLUJO
LONGITUD DE CARGA UTIL	CABECERA SIGUIENTE	LIMITE SALTO
DIRECCION DE ORIGE		
DIRECCION DE DESTINO		
CABECERA EXTENSIÓN 1		
CABECERA EXTENSIÓN 2		

Al comparar las dos imágenes se puede observar que en el datagrama IPv6 no se introducen los campos de Helen, Banderas, Desplazamiento de fragmentos, Suma de verificación de encabezado, Opciones y Relleno, del protocolo de IPv4, con el fin de reducir el tiempo de procesamiento de los paquetes manejados y limitar el coste en ancho de banda de la cabecera de IPv6

Campos del protocol IPv6:

- **Campo VER (Versión)**: Este campo tiene una longitud de 04 bits y especifica la versión del protocolo, tomando el valor de 0110. Recordar que el protocolo IPv4 también cuenta con el campo VER y su valor en este caso es de 0100. Hoy en día, los sistemas operativos de los Router soportan ambos protocolos (dual stack) y los Router pueden identificar que versión de protocolo IP llega al Router por una de sus interfaces analizando este campo.

- **Campo DS (Differnet Service)**: Este campo tiene una longitud de 08 bits y de ellos 06 bits definen el nivel de prioridad que presente el protocolo IP, subcampo denominado DSCP (se definen 64 niveles de prioridad). Este campo define la arquitectura de Internet de Servicios Diferenciados o *DiffServ*.

- **Campo Etiqueta de Flujo**: Este campo tiene una longitud de 20 bits y permite que una aplicación asigne un número que identifique a todos los paquetes IPv6 perteneciente a esta aplicación. Antes que se envíen los paquetes IPv6 a red, el host emisor envía a la red el protocolo de señalización RSVP para informar a todos los nodos de la red que reserve recursos para ésta aplicación identificado por el valor del campo Etiqueta de Flujo. Este campo define la arquitectura de Internet de Servicios Integrados o *IntServ*.)

- **Campo Longitud de carga útil**: Este campo tiene una longitud de 16 bits y define el tamaño en bytes de la carga útil (incluyendo la cabecera de extensión).

- **Campo Cabecera Siguiente**: Este campo tiene una longitud de 8 bits y define el tipo de carga útil que encapsula el protocolo IPv6. Existe la posibilidad de que el protocolo IPv6 esté llevando información específica en la región denominado *cabecera de extensión*; si este es el caso, ésta región *cabecera de extensión* deberá contener como primer campo *cabecera siguiente* para indicar que tipo de información corresponde a continuación.

➢ **Cabecera Límite de Salto**: Este campo tiene una longitud de 08 bits y define la cantidad máxima de saltos que un paquete IPv6 puede transitar antes de que sea considerado que está en un bucle. Cada router disminuye en la unidad el valorde este campo antes de enviar al router siguiente. Un protocolo IPv6 es eliminado de la red si un router detecta que este campo está en cero.

•

➢ **Campo Dirección IP de origen y Dirección IP de destino**: Cada uno deestos campos tiene una longitud de 128 bits y define 2^{128} direcciones IP de origeny 2^{128} direcciones IP de destino. Debido a la longitud de estos campos, se dispone de un número incalculable de direcciones IP; esto permitirá que los diversos nodos y equipos terminales cuenten con direcciones IPv6 públicas, eliminando mecanismos innecesarios como el NAT.

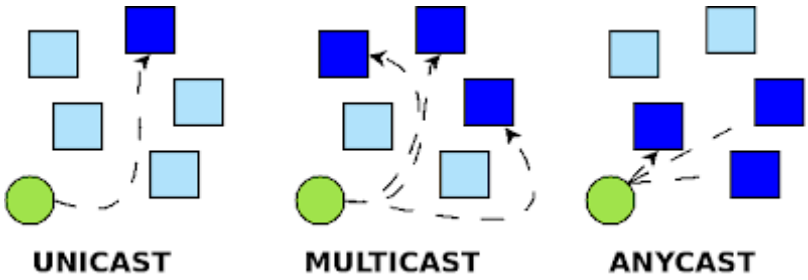
Tipos de Direccionamiento en IPv6

➢ Unicast: Identifica a una interfaz y pueden ser de tres tipos. ***Global Unicast*** que son reconocidas en la Internet; son los equivalentes a las direcciones públicas en IPv4. ***Site-Local Unicast*** no son reconocidas en la Internet y sirven para asignar una dirección IPv6 a un interfaz dentro de una red LAN; es equivalente a las direcciones privadas en IPv4. ***Link-Local Unicast*** no son reconocidas en la Internet y sirven para asignar una dirección IPv6 a una interfaz dentro de un segmento de red; es útil para aplicar la autoconfiguración en IPv6.

➢ Multicast: Identifica a varias interfaces y son utilizados por algunos protocolos, como RIP y OSPF para IPv6. Se identifica porque los primeros ocho bits de este tipo de direcciones están en uno (FFh).

- Identifican a un grupo de hosts
- Un paquete dirigido a una dirección multicast se entrega a todos los hosts
  Identificados con esa dirección.
- Implementan también el tráfico broadcast

Anycast: En una dirección que permite identificar a varias interfaces (similar a una dirección multicast) pero se accede a una sola interfaz.



Se muestra las tres clases posibles en las cuales el protocolo de IPv6
Pueden ser direccionados.

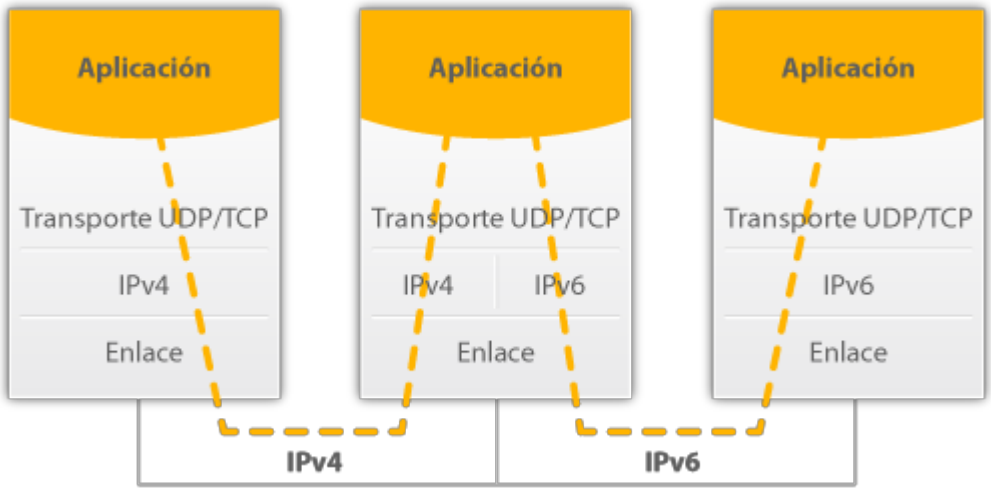
Mecanismos de Implementación de redes en IPv6:

- **DUAL STACK:** Una de las maneras conceptualmente más fáciles de introducirIPv6 en una red, es el denominado "mecanismo de pila doble" que es describe en el RFC 2893 (Microsystem, 2000) . Por este método un host o un Router tendrán ambas pilas de protocolos, IPv4 e IPv6, provistas directamente como un componente del sistema operativo. Cada nodo, denominado "nodo IPv4/IPv6", se configura con ambas direcciones IPv4 e IPv6. Por consiguiente, las dos pilas envían y reciben datagramas que pertenecen a ambos protocolos y así podrán comunicarse con cada nodo IPv4 e IPv6 en la red. Ésta es la manera más simple ymás deseable de coexistencia para IPv4 e IPv6 y es, en general, el próximo paso en la evolución, antes de una transición más profunda, hacia una Internet mundial solo IPv6.

No existe un mecanismo de transición real usado en el escenario dual stack, debido a que “Dual Stack” integra en sí mismo el soporte IPv6. Para construir un nodo de pila dual, solo es necesario habilitar en el sistema operativo el soporte IPv6. De esta manera el nodo se convierte en un nodo "híbrido" y dependiendo de

la resolución de nombres será el protocolo que usará para cada requerimiento enparticular.

Dual Stack



Esta figura muestra el mecanismo de interacción entre protocolo IPv4 y el IPv6, con el fin de interactuar simultanea durante el proceso de transición cuando se establece una conexión hacia un destino sólo IPv4, se utilizará la conectividad IPv4 y si es hacia una dirección IPv6, se utilizará la red IPv6. En caso que el destino tenga ambos protocolos, normalmente se preferirá intentar conectar primero por IPv6 y en segunda instancia por IPv4.

6. Fases I. Etapa de transición al protocolo IPV6

6.1 INVENTARIOS

-

7. DIAGNOSTICO DE LA INFRAESTRUCTURA

Diagnóstico de los equipos de comunicación, comunicaciones y aplicativos

El presente diagnóstico se elaboró en base a los inventarios de los equipos de comunicación, equipos de cómputo, aplicativos y servidores, que se encuentra en servicio, resaltando el funcionamiento, el estado físico del equipo, el soporte al nuevo protocolo de IPv6.

Para este análisis se desarrollaron los inventarios de equipo instalado, su estado físico, el soporte al protocolo IPv6, tipo de cableado instalado al que le presta la conectividad, tipos rack, cantidad de usuarios soportados y el ambiente en el que se encuentra.

1. Equipos de comunicaciones.

ITEM	EQUIPO	CANT.	CAPA	ROL	GESTIONA IPV6
1	3COM 4500G-24	6	3	ACCESO	NO
2	3COM 4500G-48	1	3	CORE	NO
3	3COM 5500G-24	0	3	CORE	NO
4	3COM 2226-SFP PLUS	8	2	ACCESO	NO
5	D-LINK DES-1024D	1	2	ACCESO	NO
6	MIKROTIK CRS125-24G-1S	43	3	ACCESO	SI
7	ARUBA 2530-24G	13	3	ACCESO	SI
8	ARUBA 2530-48G	11	3	ACCESO	SI
9	CISCO SG200-18 PORT	0	3	ACCESO	SI
10	CISCO SF220-24	2	3	ACCESO	SI
11	CISCO SG300-52	2	3	ACCESO	SI
12	HP 1920-48G	2	3	ACCESO	SI

13	HP 1920S 24G 2SFP PoE+ (370W)JL385A	1	3	ACCESO	SI
14	HP 2530-48G-PoEP Switch (J9772A)	7	3	ACCESO	SI
15	HP 2530-24G-PoEP Switch (J9773A)	8	3	ACCESO	SI
16	HP 1910-24 Switch (JG538A)	12	3	ACCESO	SI
17	3COM 4210	2	2	ACCESO	NO
18	CAMBIUM NETWORK	1	3	ACCESO	SI
	CANTIDAD DE EQUIPOS	120			

En este inventario se observan solo Switch de core y de acceso principales, pero la realidad es que la población de Switch es superior, debido al crecimiento sin programación, por daños en los equipos, por fallas en el cableado y falta de una política de actualización de equipos.

Encontramos Switch de diferentes fabricantes a lo largo de todas las sedes, que no cumple con los estándares para el tipo de operación empresarial que se requieren, la mayoría son Switch tipo hogar, que no dan las prestaciones que se requieren, esto ocasiona las repetidas llamadas al servicio técnico, como por ejemplo tenemos:

Oficinas de talento humano: se encuentran 3 Switch marca tp-link de 8 puertos, se instalaron por la necesidad de conectar la cantidad de usuarios que laboran en la oficina, debido a que los puntos que llegan del data center no son suficientes, además el cableado que se utilizó para la conexiones, es un cable que presenta averías y oxidación en su estructura interna, el sitio donde se encontraba instalado había presencia de agua, este cableado está pendiente para su reemplazo.

Oficina de jurídica: presenta el mismo panorama que talento humano.

Sede de santa Rita, casa de justicia el country: los Switch presenta algunos puertos dañados, se requiere el cambio del Switch y el cableado presenta daños por envejecimiento y daños por roedores.

Gestión de riesgo: esta oficina tiene una cableado categoría 6 en buenas condiciones, pero el Switch de acceso principal presenta daños en algunos puertos y falla intermitentes.

Edif. Portus: la alcandía tiene arrendados los pisos del 17 al piso 23, esta cableado es categoría 6A esta en óptimas condiciones y los Switch son de última generación, pero los AP instalados son de marca TP-Link y no están dando el cubrimiento deseado.

Edif. antiguo de empresas públicas: los rack de cada piso se encuentra en buen estado, pero se presentan alguna averías en el cableado, debido a las remodelaciones donde se dañaron algunos cableado, los Switch son de marca Mikrotik de los cuales ya se han dañado varios y no se han podido reemplazar, en la actualidad se encuentran dañados 4 Switch en piso 2, 6 ,3.

Alcaldía menor de Chiquinquirá: presenta problemas con el cableado, este ha sido dañado por roedores en varios sectores por esta razón se ha implementado la instalación de sw tipo hogar en varios sitios para dar el conectividad a usuarios, este escenario se repite en muchas sedes que han crecido. Se han anexado nuevas oficinas o por daños en el cableado.

2. **Equipos de cómputo e impresoras**:

En este cuadro comparativo están los computadores de escritorio y portátiles, con su ubicación y convenios con la alcaldía.

EQUIPOS INSTALADOS Y PROVEEDORES

Nº	Entidad	Tipo de equipo				Cantidad Total	%
		Escritorio	%	Portátil	%		
1	Alcaldía de Cartagena	656	82,93%	29	19,73%	685	73,03%

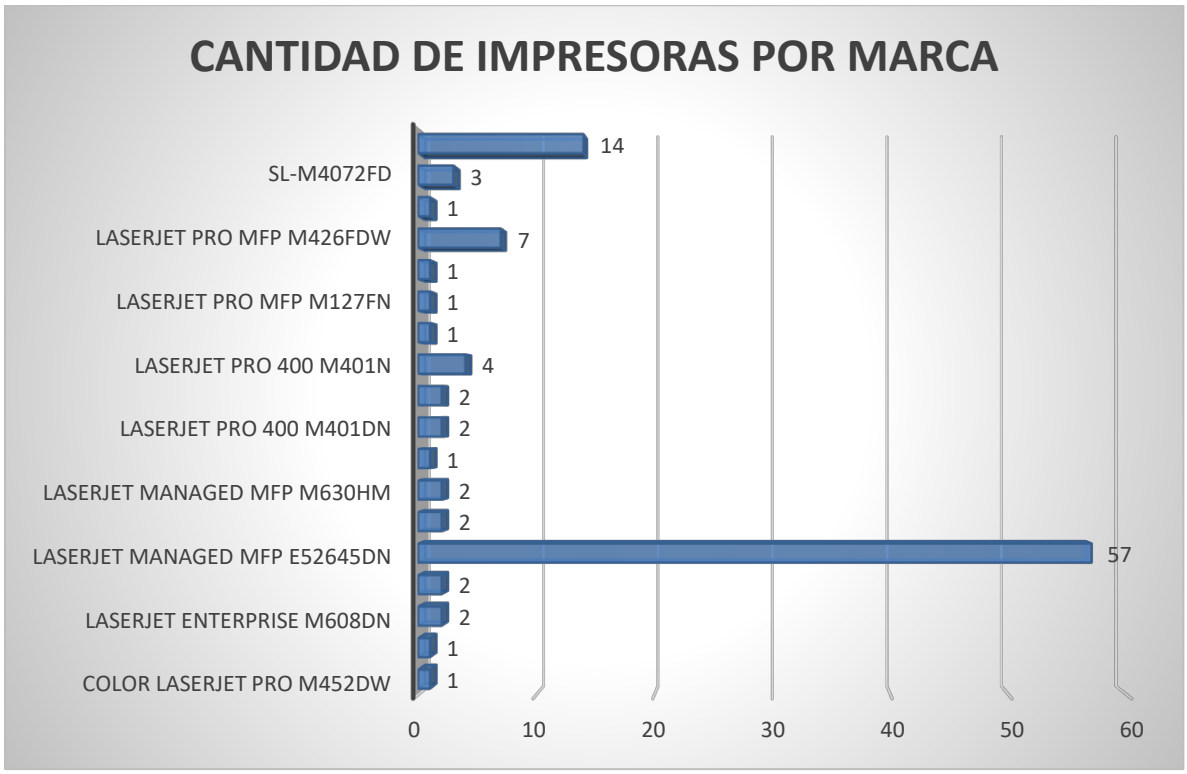
2	Comodato Tigo - Une	125	15,80%	62	42,18%	187	19,94%
3	Punto vive digital Jorge Artel	5	0,63%	29	19,73%	34	3,62%
4	Punto vive digital Bicentenario	0	0,00%	0	0,00%	0	0,00%
5	Punto vive digital Ararca	2	0,25%	3	2,04%	5	0,53%
6	Punto Vive digital Santa Rita	0	0,00%	0	0,00%	0	0,00%
7	Punto vive digital Punta Canoa	3	0,38%	24	16,33%	27	2,88%
TOTAL		**791**	**100%**	**147**	**100%**	**938**	**100%**

Tabla que indica los tipos de sistema operativos instalados en los equipos

Nº	Entidad	Sistema Operativo								Cantidad Total	%
		Win XP	%	Win 7	%	Win 8	%	Win 10	%		
1	Alcaldía de Cartagena	1	0%	180	83%	231	90%	273	59%	685	72,95%
2	Comodato Tigo - Une	0	0%	0	0%	0	0%	187	40%	187	19,91%
3	Punto vive digital Jorge Artel	0	0%	34	16%	0	0%	0	0%	34	3,62%
4	Punto vive digital Bicentenario	0	0%	0	0%	0	0%	0	0%	0	0,00%
5	Punto vive digital Ararca	0	0%	3	1%	0	0%	2	0%	5	0,53%
6	Punto Vive digital Santa Rita	0	0%	0	0%	0	0%	0	0%	0	0,00%
7	Punto vive digital Punta Canoa	0	0%	0	0%	27	10%	0	0%	27	2,88%
TOTAL		**1**	**0%**	**217**	**100%**	**258**	**100%**	**462**	**100%**	**938**	**100%**

Memoria Instalada	Alcaldía de Cartagena	UNE	%	Total general
1,024 MB	1		0%	1
2,048 MB	82		0%	82
3,072 MB	45		0%	45
3,982 MB	2		0%	2

4,002 MB	2		0%	2
4,096 MB	433	99	53%	532
6,144 MB	12		0%	12
8,088 MB	1		0%	1
8,192 MB	107	88	47%	195
10,240 MB	1		0%	1
16,384 MB	1		0%	1
Total general	**685**	**187**		**872**



Contamos con una población de 938 computadores donde el 70% son propios, el 30% restante son suministrados en convenios con la alcaldía.

Los sistemas operativos que tiene instalados los computadores son Windows. Como es sabido las versiones de Microsoft Windows desde la versión 7 en adelante, traen

implementado el protocolo ipv6 en su programación, pero se requiere la actualización del 40% de los equipos propios, realizando el aumento de la memoria RAM, actualizando la cantidad de memoria a 4MG como mínimo de memoria RAM.

Tenemos una población de 104 impresoras instaladas en todas las dependencias de la alcaldía, al ser impresoras de última generación, el protocolo IPV6 viene incluido en su sistema operativo.

Con esto podemos concluir, que los computadores de usuario final y las impresoras, no presentaran ningún inconveniente a la hora de implementar IPV6,

Actualmente se adelanta con TIGOUNE y VENEPLAS, la ampliación de los contratos de computadores nuevos e impresoras para las diferentes sedes de la alcaldía.

3. **Servidores físicos y virtuales**:

De acuerdo con los inventarios realizados por infraestructura, podemos resumir que en la alcaldía cuenta con los siguientes servidores así:
Servidores físicos ubicados en el Datacenter y algunos en varias sedes, un total de 30 servidores de los cuales hay 18 equipos apagados y 12 encendidos.

Servidores virtuales instalados en TITANIUN, la nube de TIGOUNE, a la fecha del 12 de noviembre del 2021. Se encuentran virtualizados 22 servidores y en el Datacenter, hay 27 servidores en funcionamiento.

Conclusiones del diagnóstico de la infraestructura de telecomunicaciones.

1. La población de Switch en un 50% no soportaría la adopción del protocolo IPV6, 30% debe ser reemplazados por envejecimiento y un 20% de equipos soporta el protocolo IPV6, pero se requeriría una actualización del sus versiones de firmware. Se debe realizar una inversión para la adquisición de nuevos equipos de comunicaciones (Switch, Router), debido a que la gran mayoría de los equipos de comunicaciones son obsoletos o no soportan el protocolo IPV6.

2. Los Computadores de propiedad de la alcaldía, en su mayoría se requiere la actualización de hardware y software, los computadores e impresoras que están en comodato no presentan problemas porque se exigen equipos de última generación.

3. Los servidores físicos manejan un sistema operativo de virtualización VMWARE ESXI, tenemos servidores con WINDOWS server 2012 y 2008.
   VMWARE es un sistema de virtualización que proporciona un ambiente de ejecución de diferentes sistemas operativos, compartiendo su CPU, memoria RAM, BIOS, su tarjeta gráfica etc., soporta el protocolo ipv6.
   WINDOWS SERVER 2012, 2008, como se comentó anteriormente, todo los sistemas operativos desde el Windows 7 tiene incluido el soporte para IPV6, podemos confirmar que no habrá problemas a la hora de la adopción del protocolo IPV6 en nuestra infraestructura de comunicaciones.

Comentarios de las conclusiones: se requiere la actualización de todo el sistema de comunicaciones como los Switch, cableado estructurado y todo sus accesorios como Patch panel, Patch Cord, conectores etc.

Tenemos una deficiencia en protección eléctrica, tenemos UPS que se encuentran dañadas, otras necesitan cambios de baterías y un mantenimiento semestral, se elabora un plan de mantenimiento para todos los equipos

Con respecto a los computadores e impresoras no deberíamos de tener problemas en la implementación, aparte de los equipos que se requiere su actualización.

Los servidores por su nivel de tecnología no tendrían problemas con la implementación, como todos saben, la meta es que todos los servidores queden alojados en la nube TIGOUNE antes de finalizar el año.

Como se puede observar podemos hacer la implementación del protocolo IPV6, realizando las actualizaciones que se requieren, estas actualizaciones se harán progresivamente, por tal motivo se debe implementar el método de Dual Stack para poder convivir con los dos protocolos IPV4 y IPV6 hasta que se pueda desactivar el protocolo IPV4, en el tema de las comunicaciones es urgente el cambio de equipos debido a su antigüedad, en este momento tenemos problemas en varias sedes porque muchos equipos está fallando.

FASE II
IMPLEMENTACION IPV6

Actividades de Fase II

Para efectuar la implementación se deben realizar las siguientes actividades y en el siguiente orden. Lo anterior basado en los resultados del Análisis de la información de activos de TI recopilada. La priorización para la implementación se define de acuerdo con los siguientes parámetros:

- Prioridad a los servicios con criticidad Alta, Media y Baja.
- Orden de implementación por Capa (0. Planeación, 1. Red, 2.SO, 3.BD, 4.APP)
- Solicitar el direccionamiento global al organismo regulador o proveedor de servicios de internet.

Revisión del Servidor DNS y Servidor DHCP IPv4

Para una apropiada adopción del protocolo IPv6, se debe hacer una revisión sobre el servidor de DNS, el cual consistente en:

1. Verificación de correspondencia de nombres con direcciones IPv4.
2. Eliminación de registros DNS duplicados y obsoletos.
3. Creación de objetos DNS que no estén registrados o que tengan problemas de registro DNS.

Así mismo, teniendo en cuenta que se tendrá una coexistencia entre dos protocolos, es necesario hacer la revisión del servidor de asignación automática de direcciones IPv4 (servidor DHCP), en los siguientes aspectos.

4. Verificación de los registros de direcciones IPv4 duplicados.
5. Verificación de registros de direcciones IPv4 obsoletos.
6. Eliminación de registros no coherentes.
7. Verificación de asignación correcta de los hosts en sus VLAN correspondientes.
8. Revisión de las asignaciones estáticas

Preparación de los dispositivos con conexión a internet.

La preparación de los dispositivos requiere tener presente varias de las consideraciones expuestas hasta ese momento, estas son:

- Haber adquirido un direccionamiento IP global.
- Contemplar el mecanismo de transición seleccionado.
- Haber definido el plan de direccionamiento IPv6.
- Contemplar que en este momento la mayoría de los sitios de internet en América Latina aún se comunican con direccionamiento IPv4, por lo tanto, es necesario mantener activo el protocolo IPv4.

Para la configuración de enrutadores, se debe tener en cuenta los siguientes aspectos:

Direccionamiento Global entregado por el RIR (Regional Internet Registry). En este se debe contemplar los siguientes aspectos:

- Solicitar al ISP realizar la configuración global asignada por el RIR(LACNIC).
- Realizar Backup de la configuración en el enrutador pasivo.
- Mantener el direccionamiento IPv4 actual, para evitar incidentes con los servicios publicados.
- Realizar pruebas de conectividad sobre IPv6.

Para la configuración del Firewall, se deben tener en cuenta los siguientes aspectos:

- Activar las características IPv6 para el dispositivo.
- De acuerdo con el plan de direccionamiento, asignar direcciones IPv6 estáticas a las interfaces de red del dispositivo.
- Verificar la gestión del dispositivo a través del direccionamiento IPV6 asignado. Se puede usar una interfaz de prueba para la administración y gestión del dispositivo, una vez las pruebas por esta interfaz sean satisfactorias, se puede realizar la configuración en la interfaz principal.
- Realizar la configuración para la comunicación con los enrutadores del ISP.

- Configurar ACL (Access Control List) de prueba para conectividad a Internet a través de IPv6.
- Realizar pruebas de conectividad IPV6 Firewall / enrutador y viceversa.
- Realizar Backup de la configuración del Firewall.

Nota: En este instante, aún no se hace publicación de los servicios sobre IPv6, por lo tanto, se deben mantener aseguradas las ACL tanto para IPv6 como para IPv4.

Preparación del servidor de direccionamiento DHCP IPv6.

Para la preparación del servidor de direccionamiento IPv6 (DHCP IPv6) se deben tener en cuenta las siguientes consideraciones:

- Haber adquirido un direccionamiento global (temporal o definitivo) emitido por su RIR https://www.lacnic.net/ (LACNIC).
- Tener pre-configurados los dispositivos de conexión a internet (Router, Firewall, entre otros).
- Haber definido un plan de direccionamiento IPv6 acorde con la topología de red de la entidad.
- Depurar previamente el DNS y el servidor DHCP IPv4.

Teniendo en cuenta que la Alcaldía Mayor de Cartagena, maneja el direccionamientos a través de los Router de Core locales, donde se alojan las configuraciones de las VLan de las entidades, integrado a un directorio activo en Windows server 2019 y el DNS.
La configuración del servidor debería ser integrado dentro de la misma solución y se debe tener en cuenta las siguientes consideraciones:

ACTIVIDAD	ESTADO
Activar las características IPv6 en el servidor.	

Asignar una dirección IPv6 estática, acorde con el plan de direccionamiento IPv6.	
Registrar la dirección IPv6 estática en el servidor de DNS (Esta dirección no es modificable ya que a través de esta los clientes de la red encontraran la dirección del servidor DNS IPv6).	
Revisar si la configuración del servidor DHCP de los Router de Core de las diferentes entidades, cuenta con ámbitos activos de IPv6.	
Cree un ámbito DHCP IPv6 de pruebas en todos los Router de Core de la topología de red.	
Crear un entorno de pruebas para validar la correcta asignación de direcciones IPv6. Si las pruebas son satisfactorias crear los ámbitos necesarios de acuerdo con su topología y el plan de direccionamiento.	
Establecer los dispositivos que son manejados por el DHCP IPv6 que requieran direccionamiento estático.	
De acuerdo con el plan de direccionamiento y la topología actual de red, se deben crear las VLAN IPv6 en cada uno de los Switch de Core para que permitan el tráfico a través de ellas y se verificara que los equipos puedan navegación hacia internet.	

Luego de las pruebas y/o correctivos, realizar Backup la configuración en los demás Switch Core en toda la red.	
Realizar una activación temporal del protocolo IPv6 en equipos de manera aleatorios de la red en una VLAN seleccionada, para la verificación de conectividad IPv6, esto requiere desactivación temporal de IPv4 en esos mismos equipos.	
Hacer un monitoreo del comportamiento de la conectividad en IPv6 durante un tiempo que se considere prudente.	

Para las soluciones Wireless:

ACTIVIDAD	ESTADO
Configurar la controladora Inalámbrica para su gestión a través de IPv6.	
Activar las características que permitan el uso del mecanismo de transición.	
Configurar una dirección IPv6 estática en la controladora.	
Realizar pruebas de conectividad IPv6 hacia el dispositivo.	
Mantener activa la configuración IPv4 del dispositivo.	
Configurar las VLAN correspondientes en IPv6 para los clientes inalámbricos.	

Configurar los puertos de la controladora para permitir el tráfico de las VLAN IPv6.	
Realizar pruebas de conectividad de los clientes inalámbricos y verificar la correcta asignación de direcciones IPv6 en dicho cliente.	

Preparación de servidores.

Siendo los servidores la columna vertebral de la infraestructura, donde se soportan las operaciones críticas de la entidad, es necesario tener consideraciones especiales para esta:

DESCRIPCIÓN	ESTADO
Verificar que los dispositivos de red de los servidores sean compatibles y se encuentran actualizados para su operación en IPv6	
Se necesita establecer un plan ordenado de asignación de direcciones para estos dispositivos.	
Validar la compatibilidad de los sistemas operativos de los servidores con IPv6.	
Verificar la correcta asignación de direcciones en los servidores de DNS y DHCP IPv4.	
Activar las características de IPv6 en cada uno de los sistemas operativos de los servidores	
Asignar una dirección IPv6 estática, de acuerdo con el plan de direccionamiento.	

Verificar la conectividad del servidor en IPv6.	
Verificar el correcto registro del servidor en el DNS con su correspondiente dirección en IPv6 y en el Servidor DHCP IPv6	

Nota: Siempre se deberá mantener activo el protocolo IPv4 durante las pruebas.

- Para los servidores virtuales las recomendaciones son similares, sin embargo, se debe considerar la activación de las características IPv6 en los servidores físicos que soportan las máquinas virtuales (Oracle VM).

  Otras consideraciones: gran parte de la infraestructura de servidores soporta las aplicaciones de la entidad, bases de datos, archivos e información crítica para la entidad, es por ello que la activación de las características IPv6 se realizará de manera gradual evitando impactos en la continuidad del negocio, por lo tanto, se deben abrir ventanas de mantenimiento específicas para estas configuraciones y pruebas.

Preparación de equipos de usuarios final y otros tipos de host.

DESCRIPCIÓN	ESTADO
Verificar que los dispositivos de red, de los equipos cliente, soportan, son compatibles y se encuentran actualizados para su operación en IPv6.	
Acorde al análisis de criticidad IPv6 (Bajo/Medio/Alto), es necesario establecer un plan ordenado de asignación de direcciones para estos dispositivos.	
Validar la compatibilidad de los sistemas operativos de los equipos cliente con IPv6.	

Verificar la correcta asignación de los equipos cliente en los servidores de DNS y DHCP IPv4.	
Activar las características de IPv6 en cada uno de los sistemas operativos de los equipos cliente.	
Asignar una dirección IPv6 automática, de acuerdo al plan de direccionamiento.	
Verificar la conectividad de los equipos cliente en IPv6.	
Verificar el correcto registro de los equipos cliente en el DNS con su correspondiente dirección en IPv6 y en el Servidor DHCP IPv6.	

Preparación de los Sistemas de Información y Bases de Datos

Para los sistemas de información

Iniciar el proceso de actualización de aplicaciones desarrolladas en lenguajes de programación NO compatibles con IPv6. Sin embargo, cada vez que se vaya a desarrollar una aplicación se deben tener en cuenta las mejores prácticas de desarrollo para incluir IPv6.

En los escenarios donde las aplicaciones no puedan trabajar IPv4 e IPv6 simultáneamente (Capa de Aplicación), se deben separar los entornos de la aplicación para que cada uno se comunique mediante su respectivo protocolo. Recordar: La actualización de la aplicación debe hacerse en ambos entornos.

Antes de poner en producción una aplicación modificada para IPv6, crear un ambiente de pruebas y cerciórese que arroja los resultados esperados.

Evitar alterar las aplicaciones en producción.

Crear copias de respaldo antes de cualquier modificación.

Para Bases de Datos

DESCRIPCIÓN	ESTADO
Crear una copia de seguridad de las bases de datos.	
Actualizar la tabla de Host, con las direcciones IPv6 correspondientes.	
Actualizar los Jobs, Procedimientos almacenados y toda configuración de base de datos que invoque a una aplicación, modificando acorde a la tabla de Host actualizada.	
Para las Bases de Datos, crear una copia de seguridad, realizar las configuraciones para IPv6 en un entorno de pruebas, modificando acorde a la tabla de Host actualizada.	
Validar los modelos de bases de datos con el fin de determinar si existen campos dentro de las tablas que deban modificarse, ya sea en su tamaño o en su tipo. Lo anterior para el almacenamiento de variables que tengan datos de dirección IPv6.	

Para las conexiones Cliente / Aplicación

De acuerdo con la manera en que se invoque a la aplicación, tener en cuenta:

- Para las Aplicaciones WEB, hacer el llamado a través del nombre del Host, ya que a través de la dirección IP puede generar inconvenientes. Es importante tener en cuenta

que si se desea acceder a una aplicación por su dirección IPv6 se debe usar la sintaxis adecuada de la dirección entre corchetes: [ ].

- Para las Aplicaciones Cliente/Servidor, actualizar orígenes de datos, documentos conexión o cualquier otro tipo de conector que la aplicación tenga, para que esta se realice a través de nombre de Host. En caso de que los clientes compilados ya tengan direcciones IP quemadas en el código, se recomienda recompilar la aplicación con el nombre del servidor en vez de la dirección IP.
- Para las unidades mapeadas, hacer el llamado de las unidades de red compartidas invocando directamente el nombre del Host donde se encuentra el recurso.

RECOMENDACIONES GENERALES

- Capacitar a todo el personal implicado en la gestión y manejo del protocolo IPv6.
- Socializar ante la organización el plan de implementación de IPv6.
- Todos los procesos de adquisición tecnología a futuro deben exigir la compatibilidad con IPv6.
- Aunque el porcentaje de compatibilidad de los equipos con IPv6 es importante, se deben tener en cuenta que todos los nuevos equipos deben adquirirse con compatibilidad en IPv6.

Dado que la entidad cuenta con infraestructura a la nube, se recomienda tener en cuenta los siguientes aspectos:

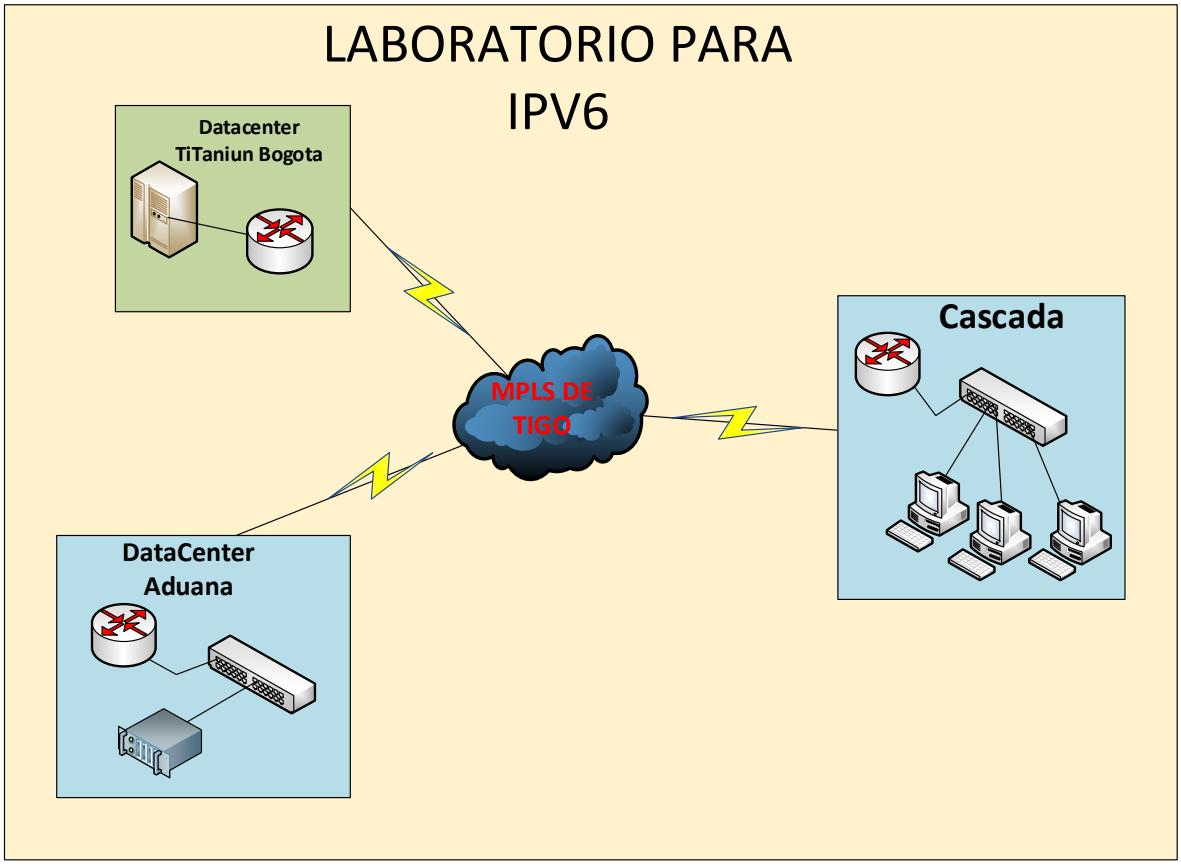
- Se debe contarse con el direccionamiento de la entidad propio para poderlo entregar al proveedor.
- Debe seleccionarse el segmento de red IPv6 que se asignará a las direcciones IP que se migrarán a la nube con el fin de que no se traslape con el direccionamiento interno. Estas direcciones serán anunciadas por el proveedor en su nube, por lo tanto, el rango debería ser único para los servicios que son públicos.
- Definir junto con el proveedor de servicios el mejor esquema de direccionamiento y segmentación de acuerdo con las condiciones adquiridas de la nube privada o pública.

RECOMENDACIONES DE ADQUISICIÓN

Como resultado del diagnóstico a continuación se presentan las recomendaciones de adquisición de infraestructura o software que permiten complementar el proceso de transición a IPv6.

- Adquirir una herramienta de control de IPv6. Esto permite gestionar el direccionamiento IPv6 de la entidad y administrarlo adecuadamente. Si bien inicialmente la asignación se realizará partiendo del plan de direccionamiento, es importante que a futuro se contemple la adquisición de dicha herramienta.
- Se recomienda que todos los contratos de adquisición de nuevas tecnologías, hardware y software incluyan la política de IPv6, la cual debe exigir que todos los equipos y software sean compatibles y desplegados en IPv6 cumpliendo con los requisitos técnicos mínimos que defina la Alcaldía de Mayor de Cartagena, así como los lineamientos de seguridad de IPv6 en general.

Diagrama Del laboratorio de prueba



Tareas para el laboratorio de Prueba.
Fase 1.

1. Adquisición del pull de direcciones o solicitar un pull de direcciones para realizar pruebas de comunicación
2. Informar a TIGO, la habilitación del protocolo IPV6 en todos los Router de borde donde se presta el servicio de comunicaciones.
3. Solicitar a seguridad la creación de varias VLans en IPV6 para habilitarlas en los sitios donde se van a realizar las pruebas.
4. Descripción del ejercicio: instalación de una Vlan en aduana y otra en cascada en el protocolo IPV6, y comenzar a hacer el despliegue del direccionamiento en cascada y en aduana.
5. Habilitar un servidor con el protocolo IPV6 para realizar pruebas de comunicación y ejecución de algunos programas en línea,

Fase 2

1. Configuración de los Firewall y tareas de seguridad.

Fase 3

1. Comenzar a realizar pruebas con base de datos.
2. Verificación el funcionamiento de los micrositios

Fase 4.

1. Despliegue del direccionamiento en toda la red, recordando que debe de trabajar simultáneamente los protocolos IPV4 y IPV6.