

 <p>Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p>	 <p>Gobernación del Archipiélago</p>
<p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>		

PLAN DE CONTINUIDAD Y DISPONIBILIDAD

GOBERNACIÓN SAN ANDRÉS
PROVIDENCIA Y SANTA CATALINA
Secretaria TIC

2023

 <p>Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p> <p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>	 <p>Gobernación del Archipiélago</p>
--	---	--

INTRODUCCION

Para efectos de implementar en el departamento un modelo de Seguridad y privacidad de la información, se requiere de la definición y aplicación de un proceso dirigidos a la preservación e la información pública, ante la presencia de eventos disruptivos (desastres, fallas de seguridad, perdida del servicio y disponibilidad del servicio) que generen consecuencias que pongan en riesgo la información e la entidad, así como señalar las medidas y acciones con que se abordarían con el fin de minimizar el impacto mediante la combinación de controles preventivos y de recuperación.

El anterior proceso conocido como Gestión de Continuidad del Negocio, requiere de la implementación efectiva el mismo, ante la presencia y ocurrencia de incidentes disruptivos, para que, frente a una ocurrencia de los mismo, la capacidad de respuesta de la Gobernación de San Andrés Providencia y Santa Catalina se de en forma adecuada y oportuna, de esa manera se minimice de manera significativa un daño potencial que pueda ser ocasionado por un incidente.

Con la aplicación de la Gestión de Continuidad del negocio, una vez se identifican los impactos potenciales que amenazan la continuidad de las actividades de la Entidad, y se diseña y construye un plan de acción, que permita la resiliencia y la capacidad de respuesta efectiva por parte e entidad, para garantizar desarrollo de los procesos de la Entidad y el cumplimiento de su misión y propósitos institucionales.

Por tanto, la correcta implementación de la Gestión de continuidad del negocio es necesario poner a disposición recurso humano, financiero, físico y tecnológico, los cuales son identificados en este documento.

este documento servirá como herramienta, para la prevención y las respuestas oportunas frente a cualquier evento que ponga en riesgo la seguridad de la información el ente Departamental, por lo que en el se establecen las acciones pertinentes, para enfrentar cualquier situación que ponga en riesgo la continuidad de los servicios que prestas la entidad.

 <p>Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p> <hr/> <p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>	 <p>Gobernación del Archipiélago</p>
---	---	---

Objetivo General

Definir el conjunto de actividades, roles y responsabilidades que permitan el restablecimiento de la operación normal de las plataformas tecnológicas de la entidad, en caso de la ocurrencia de un evento o la materialización de un riesgo de TI, que pueda alterar el normal funcionamiento de los sistemas de información críticos y los servicios tecnológicos de la Gobernación Archipiélago de San Andrés Providencia y Santa Catalina.

Objetivos específicos

- ✓ Establecer procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones críticas del negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre.
- ✓ Identificar las aplicaciones y las plataformas consideradas críticas para la operación del negocio.
- ✓ Optimizar los esfuerzos y recursos necesarios para atender cualquier contingencia de TI, de manera oportuna y eficiente, definiendo las personas responsables de las actividades a desarrollar antes, durante y después de la emergencia.
- ✓ Establecer los tiempos mínimos de recuperación requeridos en los que no se vea afectado el negocio.
- ✓ Definir la funcionalidad mínima que requiere el negocio en caso de contingencia.
- ✓ Identificar los riesgos presentes para la continuidad.
- ✓ Establecer los elementos esenciales requeridos en el plan de recuperación de desastres.
- ✓ Desarrollar procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales especificados en el alcance del plan.
- ✓ Desarrollar e impartir la capacitación inicial para el correcto funcionamiento del plan.
- ✓ Establecer un plan de prueba, gestión y mantenimiento necesarias para garantizar los objetivos del Plan.

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Alcance

El plan de continuidad del negocio de TI de la Gobernación Archipiélago de San Andrés Providencia y Santa Catalina, descrito en este documento busca definir roles y responsabilidades, así como actividades para tomar control frente a situaciones que puedan afectar la continuidad de las operaciones que involucren infraestructura tecnológica identificada en el Análisis de Impacto (BIA), delimitado en la protección y funcionalidad mínima de los sistemas de información y servicios tecnológicos que soportan los procesos críticos de la entidad.

Marco Legal

Tabla 1 Marco Normativo

TIPO DE NORMA	FECHA	DESCRIPCIÓN
Decreto 767 de 2022	16-05-2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 1008 de 2018	15-06-2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 612 de 2018	04-abr-2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 2157	20-dic-2017	Por medio del cual se adoptan directrices generales para la elaboración del plan de gestión del riesgo de desastres de las entidades públicas y privadas en el marco del artículo 42 de la ley 1523 de 2012.
Decreto 728 de 2017	05-may-2017	Por el cual se adiciona el capítulo 2 al

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

		título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
CONPES 3854 - 2016	11-Abr-2016	Política Nacional de Seguridad Digital.
CONPES 3701-2011	14 - jul - 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa Estrategia Nacional de Ciberseguridad y Ciberdefensa.
ISO 22301:2019	01-oct-2019	Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio. Requisitos.
GTC-ISO/IEC 27031:2016	07-dic-2016	Tecnología de la información. Técnicas de seguridad. Directrices para la preparación de la tecnología de información y las comunicaciones para la continuidad de negocio
ISO 22317:2015	01-sep-2015	Seguridad social - Sistemas de gestión de la continuidad del negocio - Directrices para el análisis de impacto empresarial (BIA)
NTC-ISO/IEC 27001:2022	25-oct-2022	Norma Técnica Colombiana NTC-ISO-IEC 27001. Sistemas de Gestión de la Seguridad de la Información. Requisitos

Fuente: Elaboración propia

MARCO PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

De acuerdo a los lineamientos del MINTIC se tienen en cuenta para la elaboración de este plan. Las cuatro (4) fases que comprenden el modelo de operación contienen objetivos, metas y herramientas que permiten que la continuidad del negocio sea un sistema de sostenible dentro de las entidades

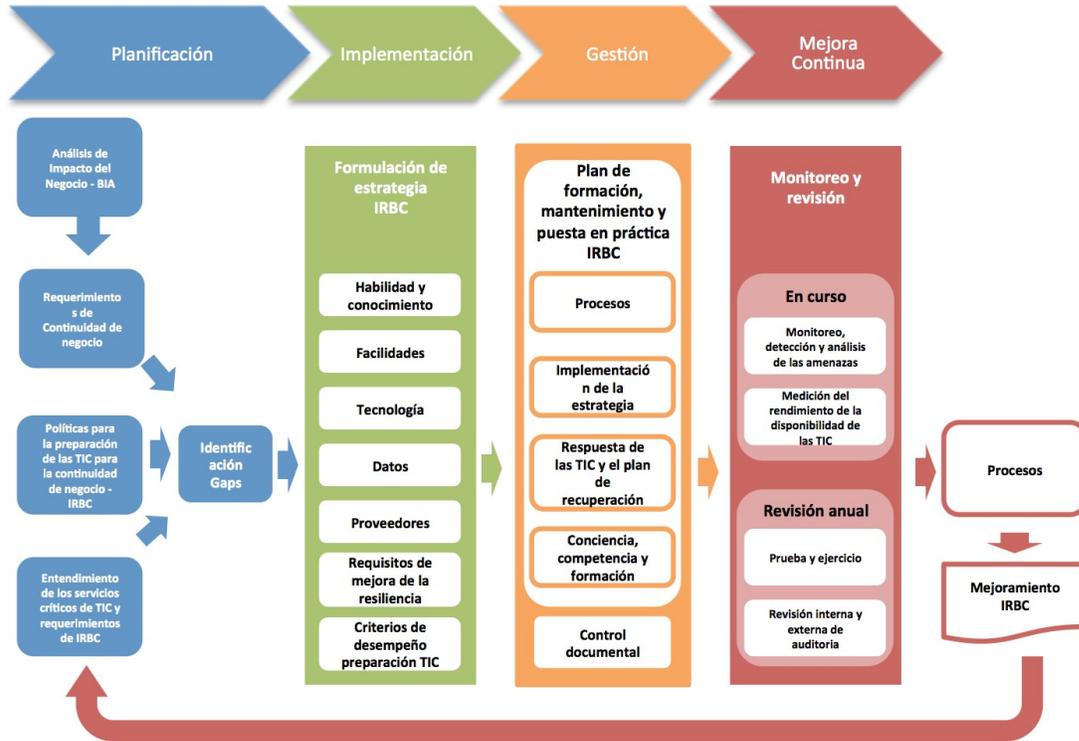
 <p>Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p>	 <p>Gobernación del Archipiélago</p>
<p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>		



Ilustración 1 – Marco de Seguridad y Privacidad de la Información

Fuente MINTIC

De acuerdo a este modelo de operación de seguridad y privacidad de la información, nos indica solo tener en cuenta las fases de planificación, implementación, gestión y mejora continua, como se muestra en la siguiente ilustración.



Fuente MINTIC

Como parte del proceso de continuidad del negocio, la preparación de las TIC para la continuidad del negocio (IRBC), hace referencia a un sistema de gestión que complementa y soporta la continuidad del negocio de la organización y los programas de Sistemas de Gestión de Seguridad de la Información (SGSI), para mejorar la preparación de la Entidad que le permita:

- a) Responder al cambiante ambiente de riesgos.
- b) Asegurar la continuidad de las operaciones críticas del negocio soportadas por servicios de TIC.
- c) Estar preparado para responder antes de que una interrupción de los servicios de TIC ocurra, identificar los eventos o las serie de eventos relacionados provenientes de incidentes.
- d) Responder y recuperarse de incidentes y/o desastres y fallas.

La secretaria TIC dentro de sus funciones tiene la responsabilidad de

Control:

Verificar el inventario de activos críticos

Verificar y valorar los activos críticos

 <p>Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p> <hr/> <p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>	 <p>Gobernación del Archipiélago</p>
---	---	---

Impacto de los activos críticos

Verificación idoneidad del comité de gestión del riesgo

Verificar costos de alternativas de continuidad

La Secretaría de las TIC tiene la responsabilidad de custodiar, administrar las bases de datos y todo el recurso tecnológico que apoya los procesos de información de la Gobernación, realiza la implementación de toda tecnología a nivel de hardware (servidores, sistemas de cableado estructurado, virtualización de máquinas, adquisidor de servicios de internet y correo electrónico)

Equipo de emergencias y recuperación el cual está conformado por:

- Gobernador
- La Secretaria de las TIC
- Los Administradores de los diferentes Sistemas de Información
- Administrador de la Base de Datos
- Encargado de la Seguridad Informática
- Equipo de Soporte y Mantenimiento
- Secretaria General (Almacen)
- Secretario de Hacienda
- Secretario de Gestión del Riesgo y Atención de Desastres

PLANIFICACION

Análisis del Impacto del Negocio.

El Análisis del Impacto del Negocio permite identificar con claridad los procesos misionales de la entidad y analizar el nivel de impacto con relación a la gestión del negocio.

En esta fase se identificaron las áreas críticas del negocio para garantizar la medición de la magnitud del impacto operacional y financiero de la entidad, al momento de presentarse una interrupción. Con esto se clarifican los siguientes requerimientos:

 <p>Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p> <hr/> <p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>	 <p>Gobernación del Archipiélago</p>
---	---	---

Identificar las funciones y procesos importantes para la supervivencia de la entidad al momento de la interrupción, esto es tener en cuenta cuales de los procesos son claves para que entren en operación rápidamente asignándoles la mayor prioridad posible, frente a los de menor prioridad; debe quedar claro que para los procesos identificados como no tan prioritarios se deben preparar también planes de recuperación.

Revisar las consecuencias tanto operacionales como financieras, que una interrupción tendrá en los procesos considerados de alta prioridad.

Estimar los tiempos de recuperación, en razón a las posibles alteraciones de los procesos considerados de alta prioridad para el funcionamiento de las infraestructuras de TI.

Evaluación de Impactos Operacionales

Teniendo en cuenta los elementos operacionales de la organización, se requiere evaluar el nivel de impacto de una interrupción dentro de la Entidad. El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C.

- Nivel A: La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.
- Nivel B: La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.
- Nivel C: La operación no es una parte integral del negocio.

Establecimiento de Tiempos de Recuperación

Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios; el entendimiento de estos componentes es fundamental para comprender el BIA. Los tiempos de recuperación se describen a continuación:

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Tiempo de Recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso

IDENTIFICACIÓN DE RECURSOS

Se realiza la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomar acciones para medir el impacto del negocio de la Gobernación.

Categoría (Función Crítica del Negocio)	Procesos Críticos (Servicios)	Identificación de recursos críticos de Sistemas TI
Nodo físico	Base de datos Entidad	Oracle Database Appliance X8-2-HA
Nodo físico	Base de datos Entidad	Oracle Database Appliance X5-2-HA
Nodo físico	VMware vSphere Essential Plus	Proliant DL190 Gen9
Nodo físico	VMware vSphere Essential Plus	DELL EMC Power Edge R940
Nodo físico	VMware vSphere Essential Plus	Powe Vault ME4012
Nodo físico	VMware vSphere Essential Plus	System x 3550 M5
Nodo físico	Respaldo de Base de datos y Máquinas virtuales	Oracle Storagetex SL 150
Nodo físico	Hyper-V	HP Proliant DL380 G7

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

DISPOSICIÓN DE LOS RTO/RPO (RECOVERY TIME OBJECTIVE / RECOVERY POINT OBJECTIVE)

RTO: Tiempo de Recuperación Objetivo: Asociado con la restauración de los recursos que han sido alterados de las Tecnologías de la Información; comprende el tiempo disponible para recuperar recursos alterados.

Adicionalmente, se aplica el WRT, es decir el tiempo que es requerido para completar el trabajo que ha estado interrumpido con el propósito de volverlo a la normalidad.

Categoría (Función Crítica del Negocio)	Procesos Críticos (Servicios)	Identificación de recursos críticos de Sistemas TI	Tiempo de Recuperación Objetivo – RTO	Tiempo de Recuperación de Trabajo – WRT
Nodo físico	Base de datos Entidad	Oracle Database Appliance X8-2-HA		
Nodo físico	Base de datos Entidad	Oracle Database Appliance X5-2-HA		
Nodo físico	VMware vSphere Essential Plus	Proliant DL190 Gen9		
Nodo físico	VMware vSphere Essential Plus	DELL EMC Power Edge R940		
Nodo físico	VMware vSphere Essential Plus	Powe Vault ME4012		
Nodo físico	VMware vSphere Essential Plus	System x 3550 M5		
Nodo físico	Relpaldo de Base de datos y Mauinas virtuales	Oracle Storagetex SL 150		
Nodo físico	Hyper-V	HP Proliant DL380 G7		
Nodo físico	Base de datos Entidad	Oracle Database Appliance X8-2-HA		

GESTIÓN DEL RIESGO

Ante la posible materialización de algún evento que ponga en riesgo la operatividad de la Entidad y con el fin de establecer prioridades para la mitigación de los riesgos, se hace necesario disponer de metodologías para su evaluación.

 <p>Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p> <hr/> <p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>	 <p>Gobernación del Archipiélago</p>
---	---	---

La metodología del plan de continuidad del negocio, determina los diversos escenarios de amenazas de una Entidad, el cual permite desarrollar las estrategias de continuidad y los planes para reanudar los servicios que estaban en operación. La gestión del riesgo debe contemplar el “cálculo del riesgo, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia . A pesar de la existencia de diversidad de métodos es recomendable iniciar con los más sencillos, que forman parte de lo que denominamos análisis previos. Una primera aproximación es la de establecer un conjunto de causas que pueden generar dificultades, tales como:

Riesgos Tecnológicos:

Fallas en el Fluido Eléctrico.

- Sabotaje Informático.

Fallas en el Centro de Datos.

- Problemas Técnicos.
- Fallas en equipos tanto de procesamiento, telecomunicaciones como eléctricos
- Servicios de Soporte a Sistemas de Producción y/o Servicios

Riesgos Humanos:

- Robos.
- Acto Hostil.
- Marchas, mítines.
- Artefactos explosivos.
- Problemas organizacionales (huelgas, leyes aceptadas por el congreso, regulaciones gubernamentales, leyes internacionales)
- Problemas de terceros involucrados en la producción o soporte a un servicio.
- Problemas con los proveedores de insumos o subproductos.

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Desastres Naturales:

- Sismos
- Tormentas Eléctricas
- Incendios
- Inundaciones
- Huracanes

CLASIFICACIÓN DE ESCENARIOS DE RIESGO

A fin de conocer con precisión los riesgos potenciales de la prestación de servicios de tecnologías de la información en la Gobernación, es recomendable clasificar los posibles escenarios:

Categorías	Escenarios	Descripción Impacto
Red Eléctrica	Fallas en el fluido eléctrico red normal (no regulada)	Fallas del servicio eléctrico de la entidad que afecta equipos eléctricos normales.
	Fallas en el Fluido Eléctrico red regulada	Fallas en los servicios de Tecnología de Información.

Red Datos, Internet y Seguridad	Problemas dispositivos Red: Falla Parcial	Falla temporal de los servicios de TI de todo un componente por limitación en la comunicación.
	Problemas dispositivos Red: Falla Total	Falla general de los servicios de TI de todos los componentes por ausencia en las comunicaciones
	Problemas en los Dispositivos Seguridad: Falla Parcial	Falla parcial de los servicios de TI de todos los componentes que tiene que ver con elementos de seguridad de TI (Elementos de Hardware Software) y ausencia de políticas y controles de TI.
	Problemas en los Dispositivos Seguridad: Falla Total	Falla general de los servicios de TI de todos los componentes que tiene que ver con elementos de seguridad de TI (Elementos de Hardware, Software) y ausencia de políticas y controles de TI.

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

	Ausencia servicio del canal de Internet Última Milla: Total	Falla general de los servicios de TI de todos los componentes involucrados en la conexión de última milla por ausencia en la comunicación. No acceso a internet; impacto directo con el proveedor del servicio.
	Perdida conectividad hacia el NAP Colombia: Parcial	Falla parcial de los servicios de TI por ausencia en la conexión hacia el NAP Colombia. Acceso parcial a la red de internet por parte del proveedor del servicio.
Hardware distribuido	Problema de Hardware de Servidores: Falla Total	Falla total de los servicios de los sistemas de información que usan la plataforma de servidores.
	Problema HW Servidores: Falla Parcial	Degradación de la calidad (lentitud) de los servicios de los sistemas de información que usan la plataforma de servidores.
	Problemas en sistema Almacenamiento	Falla de los servicios de los sistemas de Información que usan la plataforma de almacenamiento de información.
	Problemas Hardware de Servidores	Falla de los servicios de los sistemas de información que usan la plataforma de servidores.
Aplicaciones infraestructura distribuida	Problemas Capa de Aplicaciones	Falla o degradación del servicio prestado en el sistema de información afectado por problemas en las aplicaciones.
	Problemas Capa Media	Falla o degradación de la aplicación soportada por las herramientas de software y el sistema de almacenamiento masivo de datos – SAN, por tanto se puede presentar degradación o ausencia del servicio prestado por sistema de información afectado por problemas de la capa media.

	Problemas Capa de Bases de Datos	Falla o degradación de las aplicaciones soportadas por las herramientas y motores de Base de Datos, por tanto se puede presentar degradación o ausencia del servicio prestado por los sistemas de información afectados por problemas de la capa de base de datos.
	Ausencia de funcionarios, incapacidades y rotación	Disminución de capacidad de atención a los clientes y usuarios, lentitud en la atención a requerimientos e incidentes, como también el retraso en la puesta en marcha de nuevos servicios.

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Recurso Humano	Errores humanos en operación	Contempla desde la degradación de un servicio hasta la pérdida del mismo, como también la ejecución de procedimientos de manera errada que de cómo resultado la pérdida del servicio de uno o todos los sistemas de información del proyecto.
Desarrollo de aplicaciones	Falla en la aplicación por desarrollo no adecuado de terceros	Contempla la degradación de un servicio por fallas en la funcionalidad de los sistemas de información.
	Falla en la aplicación por desarrollo no adecuado por parte de la Entidad	Contempla la degradación de un servicio por fallas en la funcionalidad en los sistemas de información de la Entidad.

METODOLOGÍA DEL RIESGO

IDENTIFICACIÓN DE AMENAZAS

Las amenazas son todos los factores que pueden generar daños dentro de la organización y que requieren ser identificados, por lo tanto las amenazas pueden ocasionar riesgos al aprovechar las vulnerabilidades y permitir la afectación de los activos de información. Las amenazas pueden ser catalogadas dentro de los siguientes tipos:

Las amenazas pueden ser catalogadas dentro de los siguientes tipos:

- Seguridad interna y externa
- Ambiente físico (Instalaciones)
- Protección de activos de información
- Protección de la información
- Protección de recursos humanos

La identificación de amenazas que pueden afectar un activo de información puede clasificarse de la siguiente manera:

- Amenazas a las instalaciones: Caídas de energía, daños de agua, fallas mecánicas, pérdidas de acceso.
- Amenazas tecnológicas: Fallas en las comunicaciones, fallas en el software, fallas en el hardware, virus, spam, hacking, pérdida de datos, entre otros.
- Amenazas naturales: Inundaciones, sismos, huracanes, tormentas, incendios, entre otros.
- Amenazas sociales: Protestas, sabotajes, motines, asonadas, terrorismo, vandalismo, entre otros.
- Amenazas humanas: Problemas de transporte, huelgas, epidemias, pérdida

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

de personal clave.

Identificación de vulnerabilidades

Las vulnerabilidades son las debilidades de seguridad de Información asociadas a los activos de información y se hacen efectivas cuando una amenaza la materializa en los sistemas de información de las Entidades.

Sistema TI	Activo de Información	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia	Impacto
Servicio Web de la Entidad	Página Web de la Entidad	Defacement (desfiguración página web)	Mal diseño del sitio web	Medio	Alto
Servicio de correo electrónico	Correo electrónico Exchange	Virus, listas negras	Carencia de parches de seguridad	Alto	Alto
Sistema de Almacenamiento	SAN o NAS	Falla en el flujo eléctrico	No hay buena acometida eléctrica	Medio	Alto
Sistema de Base de datos	Bases de datos interna	Usuario no autorizado	Mala configuración	Medio	Alto

Servicio Red de comunicaciones	Equipos Switches de la Entidad	Falla de comunicaciones	Bloqueo de puertos	Medio	Alto
--------------------------------	--------------------------------	-------------------------	--------------------	-------	------

APROBACIÓN Y ACTUALIZACIÓN

El Plan de continuidad y disponibilidad de TI deberá ser aprobado en sesión de Comité de MIPG y las actualizaciones a que haya lugar, serán aprobadas por las mismas instancias y se realizarán con una periodicidad de un año o cuando se requiera de acuerdo con las siguientes situaciones:

- ✓ Cambios en la infraestructura o aplicativos y/sistemas de TI.
- ✓ Resultados de análisis de riesgos que cambien los escenarios descritos para las contingencias de TI.
- ✓ Evaluación de los resultados de las pruebas al Plan de Continuidad y disponibilidad de TI.
- ✓ Recomendaciones y/u oportunidades de mejora identificadas en auditorías u otro proceso de revisión y mejora.

 <p>Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p> <hr/> <p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>	 <p>Gobernación del Archipiélago</p>
---	---	---

COMUNICACIÓN Y DISTRIBUCIÓN DEL PLAN

A continuación, se presentan algunas pautas para la comunicación y distribución del plan y sus componentes.

- ✓ Publicación de información de manera continua y accesible. En la Intranet de la Gobernación este medio se debe utilizar para difundir el plan de Continuidad de TI. Por otro lado, en el sitio del Sistema de Gestión de Seguridad de la Información – SGSI.
- ✓ Boletines internos de comunicación a fin de establecer conciencia sobre la importancia del tema.
- ✓ Charlas y talleres. Incluir el tema del manejo de contingencias de TI dentro de la estrategia de sensibilización del SGSI.
- ✓ La Gobernación debe comunicar a los funcionarios su compromiso de salvaguardar la información y el plan de continuidad de la entidad, para lo cual utilizará los medios necesarios.

ROLES Y RESPONSABILIDADES DENTRO DEL PLAN DE CONTINUIDAD Y DISPONIBILIDAD DE TI

Para la activación del Plan de Continuidad de TI en alguno de sus escenarios, es importante destacar que el proceso de Gestión Administrativa y Financiera es quien en primera instancia deberá establecer los protocolos de comunicación primarios con la empresa de Seguridad y Vigilancia a fin de establecer los canales de comunicación al interior de la entidad en caso de presentarse alguna contingencia como la caída del fluido eléctrico, inundación, Huracanes, o en el evento de la programación o ejecución de actividades de mantenimiento que afecten el fluido eléctrico de la entidad, en días laborales y no laborales y/o cuando se encuentren o no servidores en las sedes de la entidad

Dependiendo la criticidad de la situación de contingencia, la Secretaria de las Tecnologías y las Comunicaciones TIC, serán los encargados de difundir las comunicaciones oficiales tanto internas o externas (si los servicios afectados involucran servicios a la ciudadanía o los sujetos de control), donde se indiquen

 <p>Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p> <hr/> <p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>	 <p>Gobernación del Archipiélago</p>
---	---	---

las acciones y/o noticias frente a los temas que están afectando el servicio o el restablecimiento de los mismos.

De igual manera, se deberá priorizar la comunicación entre los procesos de Gestión Administrativa y Financiera y Gestión de Tecnologías de la Información y las Comunicaciones, en cuanto la organización y requerimientos de logística. Por su parte la secretaria de las Tecnologías, la información y las comunicaciones TIC procederá a poner en marcha los protocolos de atención de la contingencia de acuerdo al escenario materializado. De otra parte, es fundamental el compromiso de los servidores públicos de la Gobernación, en especial los de la secretaria TIC debido a que son ellos quienes tienen la responsabilidad de comunicar y gestionar de forma adecuada el incidente tecnológico (prevención, mitigación, preparación, alertas, respuestas, rehabilitación y/o reconstrucción), que afecte la operación normal de la Gobernación, desde el momento que se declare la interrupción hasta la vuelta a la normalidad, buscando siempre reducir al mínimo el impacto sobre la prestación del servicio.

NIVELES DE GESTIÓN DEL PLAN DE CONTINUIDAD

Nivel Estratégico: A este nivel corresponde la planeación del logro de los objetivos del Plan de Contingencias de TI, se basa en decidir y asignar las políticas, directrices y los recursos para lograr su efectividad en caso de presentarse una interrupción tecnológica no planeada en la Gobernación.

Nivel Táctico: Llevará a cabo la coordinación de las actividades que se deriven del Plan de Continuidad de TI, así como la evaluación de las situaciones de interrupción y dará lineamientos para la operación de mismos, a su vez es el encargado de escalar al nivel estratégico en un lenguaje claro las necesidades de la operación de TI y brindará los insumos para la evaluación.

Nivel Operativo: Este nivel realiza las tareas puntuales en el momento de presentarse un incidente o evento inesperado que activa el Plan de Continuidad de TI de la Gobernación. Se ejecuta a partir de los lineamientos proporcionados por los niveles estratégico y táctico.

SEGUIMIENTO Y EVALUACION

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Para garantizar que el plan de continuidad de negocio es eficaz, es necesario que se realicen pruebas periódicas y simulacros de recuperación, razón por la cual se establece el plan de pruebas.

Cuando ocurriera un evento ya sea natural o provocado, se activará el plan de continuidad del negocio, el cual estará bajo la dirección y coordinación de la Secretaría de las TIC, quien contará con el apoyo logístico y estratégico de la Dirección de Recursos Físicos junto con el Comité de atención a desastres e incidentes informáticos y demás grupos de atención conformados.

FORMULACION DE PLAN DE ACCIÓN

ACTIVIDAD	RESPONSABLE	PERIODICIDAD
Mantener actualizado el inventario de activos de información (Sistemas de información, infraestructura física que soporta los sistemas de información, Backups, Manual de Políticas y Procedimientos de realización y restauración de Backups, Servicios.	Secretaria TIC	Anual
Realizar Copias de Seguridad de acuerdo al plan de Backups establecido por la Entidad, de: Sistemas Operativos, Software aplicativo, programas fuentes, programas ejecutables, bases de datos, reglas del firewall, Software licenciado.	Secretaria TIC	Diario
Asignar recursos en el presupuesto para la atención del desastre o incidente informático	Secretaria TIC	Anual
Gestionar los riesgos informáticos. (analizar factores internos y externos, Identificar los riesgos, analizar y valorar los riesgos, Evaluar los riesgos, Formulara plan de manejo de riesgos)	Secretaria TIC	Semestral
Realizar auditoría para identificar los datos sensibles e información crítica para el desarrollo de los procesos de la Entidad	Secretaria TIC	Semestral

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Realizar pruebas periódicas de vulnerabilidad y de la efectividad del plan de reacción o plan de respuesta a incidentes	Secretaria TIC	Semestral
Implementar y monitorear las políticas y controles de seguridad informática	Secretaria TIC	Trimestral
Verificar periódicamente el estado de las instalaciones eléctricas asegurándose que permanezcan en perfecto estado y evitar las múltiples conexiones con el uso de multitomas, a fin de evitar sobre carga eléctrica.	Secretaria TIC	Mensual
Verificar periódicamente las condiciones de extintores e hidratantes y orientar capacitaciones permanentes para su manejo, asegurándose que en el área del datacenter se encuentren ubicados extintores adecuados y los funcionarios conozcan su manejo	Secretaria TIC	Semestral
Diseñar el procedimiento para el reporte de eventos de seguridad y socializarlo a todos los funcionarios y contratistas	Secretaria TIC	Semestral

 <p>Gobernación del Archipiélago</p>	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 <p>Gobernación del Archipiélago</p>
<p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>		:

ANEXOS

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Servicio de TI	Descripción del servicio
Internet	Servicio de internet cableado e inalámbrico a los funcionarios de la entidad
Correo electrónico	Servicio de mensajería por correo electrónico para los funcionarios de la entidad
Soporte aplicaciones	Soporte técnico a usuario final sobre las aplicaciones y sistemas de información registradas en el catálogo de aplicaciones
Mesa de servicio	Soporte técnico a usuario final sobre los dispositivos de cómputo y periféricos
Centro de datos	Servicio de alojamiento de servidores y servicios de cómputo para soportar los sistemas de información y demás servicios tecnológicos
Inventario tecnológico	Adquisición, distribución y mantenimiento de elementos y equipos de tecnología informática.
Trámites y servicios digitales	Consultoría, promoción y soporte tecnológico para la disposición de trámites y servicios digitales
Implementación sistemas de información	Análisis, diseño, desarrollo e implementación de los sistemas de información, las aplicaciones y el soporte técnico que requiera la ejecución de los programas y proyectos de las diferentes dependencias de la Administración Central
Lineamientos TIC	Formulación, articulación y seguimiento de las políticas, lineamientos y directrices departamentales sobre Tecnologías de Información y Comunicación TIC
Uso y apropiación de TI	Formular los planes, programas y proyectos necesarios para promover el acceso a las Tecnologías de la Información y la comunicación en el orden departamental
Sitio web de la entidad	Disponer de la página web de la entidad y definir las directrices para su manejo

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Catálogo de Servicios Tecnológicos Gobernación del Archipiélago

Nombre	Sigla	Descripción	Versión	Categoría
Office Standard	OS2013	Paquete de oficina de Microsoft en su versión 2013 que incluye herramientas para desarrollar presentaciones, elaborar documentos, crear hojas de calculos, gestión de cuentas de correo, entre otras herramientas de la suite.	2013	Sistema de apoyo
Office Standard	OS2016	Paquete de oficina de Microsoft en su versión 2016 que incluye herramientas para desarrollar presentaciones, elaborar documentos, crear hojas de calculos, gestión de cuentas de correo, entre otras herramientas de la suite.	2016	Sistema de apoyo
Office 365 E1	365 E1	Se integra con office 365 y su fin es apoyar el trabajo colaborativo por medio de la gestión de documentos en línea de aplicaciones como Excel, Word, Power Point, OneNote entre otras.	2016	Sistema de apoyo
Office 365 E3	365 E3	Se integra con office 365 y su fin es apoyar el trabajo colaborativo por medio de la gestión de documentos en línea para desarrollar presentaciones, elaborar documentos, crear hojas de calculos, gestión de cuentas de correo, entre otras herramientas de la suite.	2016	Sistema de apoyo
Office Professional	OP2013	Paquete de oficina de Microsoft en su versión 2013 que incluye herramientas para desarrollar presentaciones, elaborar documentos, crear hojas de calculos, gestión de cuentas de correo, entre otras herramientas de la suite.	Plus 2013	Sistema de apoyo

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Office Professional	OP2010	Paquete de oficina de Microsoft en su versión 2010 que incluye herramientas para desarrollar presentaciones, elaborar documentos, crear hojas de calculos, gestión de cuentas de correo, entre otras herramientas de la suite.	Plus 2010	Sistema de apoyo
Office Professional	OP2007	Paquete de oficina de Microsoft en su versión 2007 que incluye herramientas para desarrollar presentaciones, elaborar documentos, crear hojas de calculos, gestión de cuentas de correo, entre otras herramientas de la suite.	Plus 2007	Sistema de apoyo
Outlook Messenger	chat	Aplicativo usado para el envío de mensajería instantánea, comunicación interna entre las diferentes dependencias o áreas de la Gobernación del Archipiélago	6.0.50	Sistema de apoyo
GDATA	GDATA	Antivirus para equipos finales para detección de amenazas para combatir eficazmente troyanos, malware y virus en general.	2019	Sistema de apoyo
VMware Vsphere 6	VMWAR	Hipervisor VMWare ESXi 5.X para virtualización de servidores.	2008 Release 2	Sistema de Infraestructura TI
SQL Server - Standard	SQL		2012 R2	Sistema de Infraestructura TI
Windows Server - Enterprise	WSE2008	Microsoft Windows Server 2008 R2	2008 Release 2	Sistema de Infraestructura TI
Windows Server - Standard	WSS2012	Microsoft Windows Server	2008	Sistema de Infraestructura TI

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Windows Server - Standard	WSS2008	Microsoft Windows Server	4/5/6 (64 Bit)	Sistema de Infraestructura TI
Windows Server - User CAL	WSUCAL		6 (64 Bit)	Sistema de Infraestructura TI
CentOS	CENT	CentOS	4/5/6 (64 Bit)	Sistema de Infraestructura TI
Debian	deb	Debian GNU/Linux	6 (64 Bit)	Sistema de Infraestructura TI
Oracle Linux	oraclin	Oracle Linux	12C	Sistema de Infraestructura TI
Servidor - VPN	vpn	Red Hat Enterprise Linux	1	Sistema de Infraestructura TI
Hyper-V Manager	hiperv	Complemento de MMC (Microsoft Management Console) el cual es usado para administrar, configurar y gestionar máquinas virtuales	I	Sistema de Infraestructura TI
Oracle Enterprise Edition	OEE	Base de Datos con capacidades de autoprotección y reparación autónoma, segura, inteligente y de alta disponibilidad con características de implementación en la Nube	2011	Sistema de Infraestructura TI
Oracle Database Appliance X5-2 ODA_X5-2	ORAC	base de datos de clústeres con una arquitectura de caché compartida que supera las limitaciones de los enfoques tradicionales de disco compartido y de nada compartido para proporcionar soluciones de base de datos altamente escalables y disponibles para todas las aplicaciones empresariales, proporciona Escalabilidad, Disponibilidad, Data Base As a Service.	2019	Sistema de Infraestructura TI

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Servidores

IP	Aplicativo	DESCRIPCION	FUNCION
192.168.1.90	HYPER-V	SERVIDOR HP CON 5 DISCOS DUROS DE 300 GB CADA UNO, 10000 RPM.	SERVIDOR QUE ALOJA 3 MAQUINAS VIRTUALES HYPER V, EL CONTROLADOR DE DOMINIO Y EL SOFTWARE LUNGSOFT (UTILIZADO POR LA OCCRE PARA HACER CONSULTAS)
192.168.1.95	ACTIVE DIRECTORY	SERVIDOR DE DOMINIO	ADMINSTRADOR DEL DOMINIO
192.168.1.101	LUNGSOFT SQL SERVER 2008	SERVIDOR DE APLICACIÓN Y BASE DE DATOS SQL SERVER 2008	LUNGSOFT (UTILIZADO POR LA OCCRE PARA HACER CONSULTAS)
192.168.1.23	VMWARE ESXI vSphere 6 Essentials Plus	SERVIDOR IBM CON 3 DISCO DUROS SAS CADA UNO DE 600 GB, 10000 RPM Y UN SAN STORWISE 3700 V2 CON 8 DISCO DUROS SAS DE 1.8TB 10K 12Gb Y 2 DISCO DURO DE 400GB SSD SAS 12 Gb	SERVIDOR QUE ALOJA 37 MAQUINAS VIRTUALES VMWARE (Aplicaciones Gobierno en Linea, Backup-Imágenes, balancing-webcity, ConstruControl, Control Datacenter, Control_Tiempo, dirsinc_new, DjangonBPM, Edx_Lms, emisora, fundamar-rgpsai, obstrio-mujer, servercity, Servidor-vpn, sistraff, Srv_cpartes_prueba, SrvAplicaciones, Srvaplicaciones_2, SrvAplicaciones_3, srv-geovisor.gobsai.co, srvsalud, System_Backup, vps-vpn, webcity-a, webcity-b, webcity-movilidad, wirelles lan manager, wsus)

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

192.168.1.10		Maquina virtual VMware version 11 con las siguientes especificaciones 4 Vcpu, 12GB Ram, tarjeta de red E1000E y dos unidades de disco de 60GB y 50GB	Complemento de digifile para el escaneo de documentos
192,168,1,47	opengnsys, pbackup	Maquina virtual VMware version 11 con las siguientes especificaciones 4 Vcpu, 4GB Ram, dos tarjeta de red VMXNET 3 y dos unidades de disco de 40GB y 250GB	Contiene aplicación opengnsys para la gestion de imágenes de pc, pbackup para gestionar backup de los pc de la gobernacion
192.168.1.252	Nginx, Bind 9	Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 4GB Ram, dos tarjeta de red VMXNET 3 y una unidades de disco de 16GB	Servidor web nginx, Balancea los dos nodos de webservice de hacienda, Servidor dns bind para el dominio de sanandres.gov.co, para red local
192.168.1.62	IIS 10, Cplan y Humano	Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 20GB Ram, una tarjeta de red VMXNET 3 y dos unidades de disco de 20GB ssd y 220GB	Servidor web IIS 10, contine las apliaciones de infraestructura Cplan(estimacion de presupuesto de obra) y Humano(Gestion de Nomina recurso humano de la gobernacion)
192.168.1.44	Zkaccess 3.5 Security System	Maquina virtual VMware version 11 con las siguientes especificaciones 1 Vcpu, 2GB Ram, una tarjeta de red E1000E y una unidades de disco de 60GB	Maquina virtual para el acceso al datacenter por huella digital
192.168.1.17	ZKTime 5, PLSQLDeveloper 14, SQL Server 2008 R2	Maquina virtual VMware version 8 con las siguientes especificaciones 2 Vcpu, 4GB Ram, una tarjeta de red VMXNET 3 y una unidades de disco de 60GB	Maquina virtual para el control de acceso del personal de la gobernacion de recursos humano, maquina de acceso utilizada por el proveedor Infortributo, para acceso a soporte por anydesk

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

192.168.1.4	Azure AD Connect	Maquina virtual VMware version 11 con las siguientes especificaciones 1 Vcpu, 4GB Ram, una tarjeta de red E1000E y una unidades de disco de 80GB	Maquina virtual para sincronizar office 365 con el Active Directory
192.168.1.16		Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 4GB Ram, una tarjeta de red VMXNET 3 y una unidades de disco de 120GB	Maquina virtual con entorno BPM para crear proceso de gestion de la gobernacion
192.168.1.24		Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 4GB Ram, una tarjeta de red VMXNET 3 y dos unidades de disco de 32GB y 50GB	
192.168.1.18	Joomla	Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 4GB Ram, una tarjeta de red VMXNET 3 y una unidades de disco de 120GB	Aplicativo para cargas de informacion estadistica de la oficina de la mujer
192.168.1.201	Oracle 12c	Maquina virtual VMware version 8 con las siguientes especificaciones 4 Vcpu, 8GB Ram, una tarjeta de red VMXNET 3 y tres unidades de disco de 140GB, 500GB y 900GB	Servidor de base de datos de prueba de infotributo (city), servidor de archivo para el aplicativo city y replicacion de backup de la oda de oracle
192.168.1.12	Sistrapp	Maquina virtual VMware version 8 con las siguientes especificaciones 2 Vcpu, 4GB Ram, una tarjeta de red VMXNET 3 y dos unidades de disco de 60GB, 480GB	Sistema de gestion de movilidad vehicular del departamento

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

192.168.1.78	cpartes	Maquina virtual VMware version 8 con las siguientes especificaciones 2 Vcpu, 4GB Ram, una tarjeta de red E1000 y una unidades de disco de 140GB	Sistema de gestion de pensionados del fips de la gobernacion
19.168.1.7	Tomcat 6, Tomcat 7, ISS 7	Maquina virtual VMware version 11 con las siguientes especificaciones 4 Vcpu, 4GB Ram, una tarjeta de red E1000 y una unidades de disco de 120GB	Servidor de Aplicaciones (PCTWebiTransparencia, bici y humano viejo)
192.168.1.207	IIS 7, Isolucion	Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 4GB Ram, una tarjeta de red E1000 y dos unidades de disco de 520GB y 80GB	Servidor de Aplicaciones (Isolucion y Outlook Messenger)
192.168.1.5	SysAid	Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 8GB Ram, una tarjeta de red E1000 y dos unidades de disco de 60GB y 60GB	Servidor de mesa de ayuda de la gobernacion
192.168.1.80		Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 4GB Ram, una tarjeta de red E1000 y una unidades de disco de 60GB	
192.168.1.81		Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 6GB Ram, una tarjeta de red E1000 y dos unidades de disco de 60GB y 120GB	Servidor de aplicación de secretaria de salud
192.168.1.32	Django, control	Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 4GB Ram, una tarjeta de red E1000 y dos unidades de disco de 40GB y 300GB	Servidor de aplicación (control)

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

192.168.1.9	openvpn	Maquina virtual VMware version 8 con las siguientes especificaciones 2 Vcpu, 8GB Ram, una tarjeta de red E1000 y una unidad de disco de 120GB	Srvidor de OpenVPN de la gobernacion
192.168.105.250	Tomcat 8.5	Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 16GB Ram, una tarjeta de red VMXNET 3 y dos unidades de disco de 60GB y 20GB	Servidor web service nodo 0 de la secretaria de hacienda para la liquidacion y recaudacion de impuestos por la web
192.168.1.249	Tomcat 8.5	Maquina virtual VMware version 11 con las siguientes especificaciones 2 Vcpu, 16GB Ram, una tarjeta de red VMXNET 3 y dos unidades de disco de 60GB y 20GB	Servidor web service nodo 1 de la secretaria de hacienda para la liquidacion y recaudacion de impuestos por la web
192.168.15.140		Maquina virtual VMware version 8 con las siguientes especificaciones 2 Vcpu, 4GB Ram, una tarjeta de red VMXNET 3 y una unidad de disco de 80GB	Software para gestionar los access point Inalambricos
192.168.1.66	wsus	Maquina virtual VMware version 11 con las siguientes especificaciones 4 Vcpu, 12GB Ram, una tarjeta de red VMXNET 3 y una unidad de disco de 500GB	Servidores de actualizaciones de microsoft
192.168.1.2	VMWARE ESXI vSphere 5.1 Essentials Plus	SERVIDOR HP TIENE UN PROCESADOR DE 6 CORES A 1.7 GHz, MEMORIA RAM DE 44 GB 4 DISCO DUROS SAS CADA UNO DE 1 TB, 7200 RPM	GESTION DOCUMENTAL APLICACION
192.168.1.25	Digifile	Maquina virtual VMware version 11 con las siguientes especificaciones 4 Vcpu, 20GB Ram, una tarjeta de red VMXNET 3 y una unidad de disco de 1TB	Sistema de Gestion Documental de la Gobernacion

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

Software base

Nombre	Sigla	Descripción	Versión
VMware Vsphere 6	VMWAR	Hipervisor VMWare ESXI 5.X para virtualización de servidores.	2008 Release 2
SQL Server - Standard	SQL		2012 R2
Windows Server - Enterprise	WSE2008	Microsoft Windows Server 2008 R2	2008 Release 2
Windows Server - Standard	WSS2012	Microsoft Windows Server	2008
Windows Server - Standard	WSS2008	Microsoft Windows Server	4/5/6 (64 Bit)
Windows Server - User CAL	WSUCAL		6 (64 Bit)
CentOS	CENT	CentOS	4/5/6 (64 Bit)
Debian	deb	Debian GNU/Linux	6 (64 Bit)
Oracle Linux	oraclin	Oracle Linux	12C
Servidor - VPN	vpn	Red Hat Enterprise Linux	1
Hyper-V Manager	hiperv	Complemento de MMC (Microsoft Management Console) el cual es usado para administrar, configurar y gestionar máquinas virtuales	I
Oracle Enterprise Edition	OEE	Base de Datos con capacidades de autoprotección y reparación autónoma, segura, inteligente y de alta disponibilidad con características de implementación en la Nube	2011
Oracle Database Appliance X5-2 ODA_X5-2	ORAC	base de datos de clústeres con una arquitectura de caché compartida que supera las limitaciones de los enfoques tradicionales de disco compartido y de nada compartido para proporcionar soluciones de base de datos altamente escalables y disponibles para todas las aplicaciones empresariales, proporciona Escalabilidad, Disponibilidad, Data Base As a Service.	2019

Infraestructura de red del centro de datos

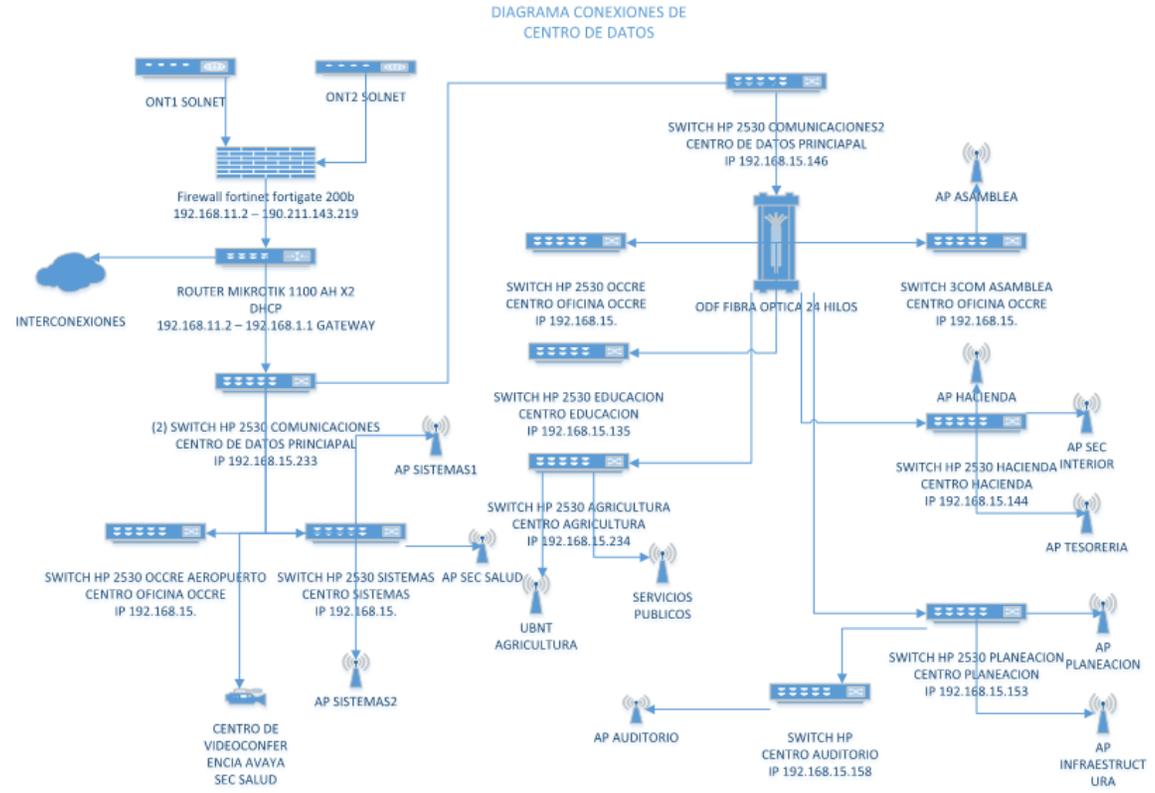


Diagrama de Infraestructura centro de datos



GOBERNACIÓN DEPARTAMENTO
ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA
Y SANTA CATALINA



Gobernación
del Archipiélago

PLAN DE CONTINUIDAD Y DISPONIBILIDAD

Infraestructura de red inalámbrica interna

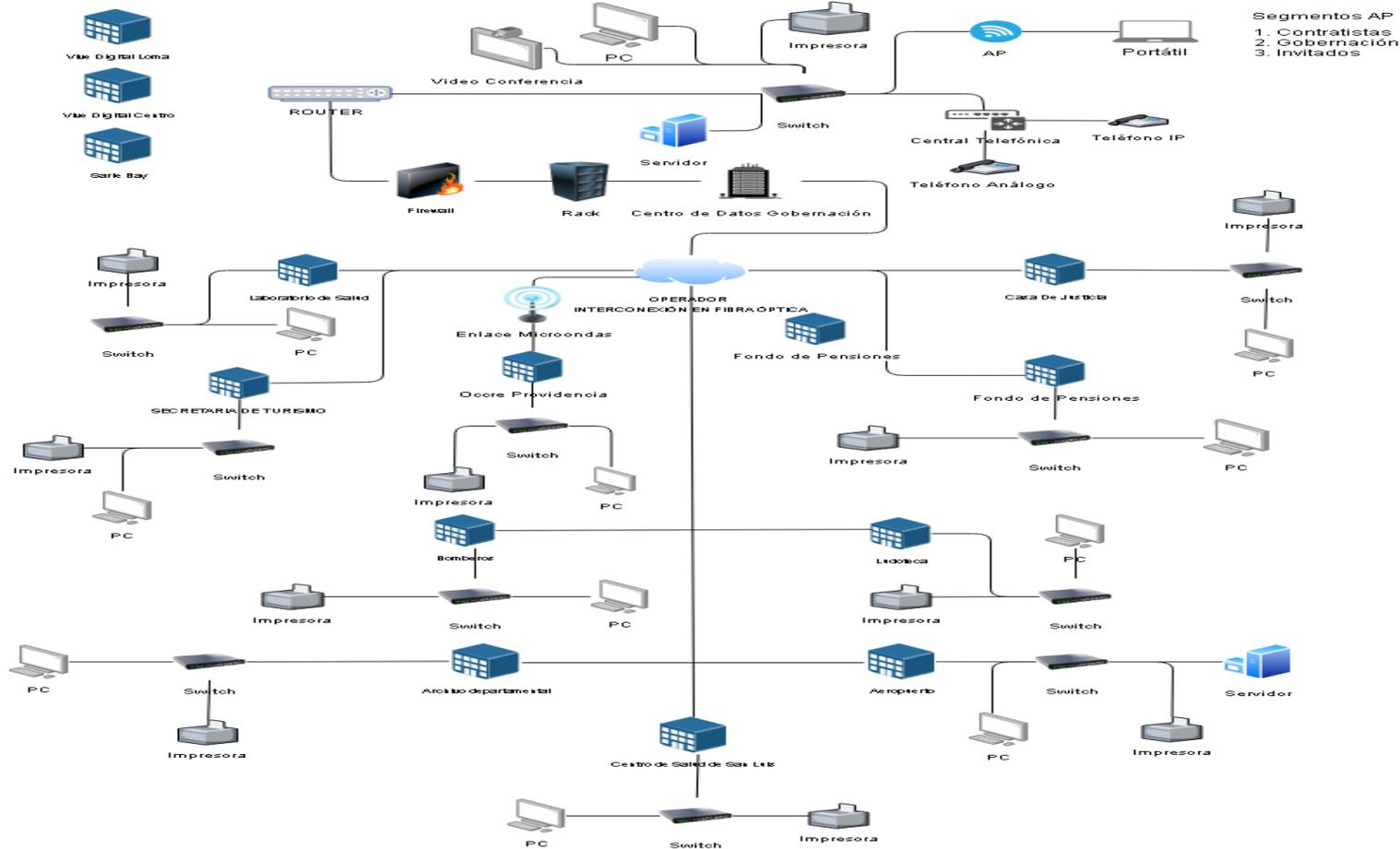


Diagrama general de red inalámbrica interna



Directorio de elementos de infraestructura de TI

No.	Tipo de hardware	Nombre / Referencia	Fabricante	Modelo	Responsable	Ubicación
1	Servidor	VMWBASEDATOS	HP	Proliant DL 380 G5	Manuel Espitia	NOC-SISTEMAS
2	Servidor	srvaplic	HP	Proliant DL 160 G9	Manuel Espitia	NOC-SISTEMAS
3	Servidor	wmaplicaciones	HP	Proliant DL 380 G6	Manuel Espitia	NOC-SISTEMAS
4	Servidor	srvservicios2	IBM	System x3550	Manuel Espitia	NOC-SISTEMAS
5	Servidor	srvservicios	HP	Proliant DL 180 G6	Manuel Espitia	NOC-SISTEMAS
6	Servidor	HPVSAI01	HP	Proliant DL 380 G7	Manuel Espitia	NOC-SISTEMAS
7	Servidor	sai1dom0	ORACLE	ODA X5-2	Manuel Espitia	NOC-SISTEMAS
8	Servidor	sai2dom0	ORACLE	ODA X5-2	Manuel Espitia	NOC-SISTEMAS
9	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-SISTEMAS
10	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-SISTEMAS
11	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-SISTEMAS
12	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-SISTEMAS
13	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-AGRICULTURA
14	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-AGRICULTURA
15	Switch	3com 4500 26 port	3COM	3com 4500	Grupo TIC	NOC-AGRICULTURA
16	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-HACIENDA

 <p style="font-size: small;">Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p>	 <p style="font-size: small;">Gobernación del Archipiélago</p>
<h2 style="margin: 0;">PLAN DE CONTINUIDAD Y DISPONIBILIDAD</h2>		

17	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-HACIENDA
18	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-HACIENDA
19	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-PLANEACION
20	Switch	3com 4500 26 port	3COM	3com 4500	Grupo TIC	NOC-PLANEACION
21	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-PLANEACION
22	Switch	HP V1910-24G Switch JE006A	HP	1910-24G	Grupo TIC	NOC-AUDITORIO
23	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-OCCRE
24	Switch	HP V1910-24G Switch JE006A	HP	1910-24G	Grupo TIC	NOC-OCCRE
25	Switch	HP 2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	NOC-EDUCACION
26	Firewall	FORTINET - FORTIGATE 200B	FORTINET	FORTIGATE	Grupo TIC	NOC-SISTEMAS
27	Router	MIKROTIK - RB1100 AH	MIKROTIK	1100 AH	Grupo TIC	NOC-SISTEMAS
28	Router	MIKROTIK - CCR-103G 8G- 2S+	MIKROTIK	103G	Grupo TIC	NOC-SISTEMAS
29	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-SISTEMAS
30	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-SISTEMAS
31	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-AGRICULTURA
32	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-AGRICULTURA
33	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-AGRICULTURA
34	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-AGRICULTURA

 <p style="font-size: small;">Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p>	 <p style="font-size: small;">Gobernación del Archipiélago</p>
<h2 style="margin: 0;">PLAN DE CONTINUIDAD Y DISPONIBILIDAD</h2>		

35	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-AGRICULTURA
36	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-AGRICULTURA
37	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-AUDITORIO
38	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-HACIENDA
39	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-HACIENDA
40	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-HACIENDA
41	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-PLANEACION
42	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-PLANEACION
43	Acces Point	UBIQUITI UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	NOC-SALUD PUBLICA
44	Switch	baseline 2024	3COM	N/A	Grupo TIC	NOC-SECULTURA
45	Acces Point	DAP-2590	N/A	DAP-2590	Grupo TIC	SEC TURISMO
46	Acces Point	DAP-2590	N/A	DAP-2590	Grupo TIC	CASA DE JUSTICIA
47	Switch	2530-24G J9776A	HP	HP 2530-24G	Grupo TIC	AEROPUERTO
48	Switch	2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	AEROPUERTO OFI PRINCIPAL
49	Switch	2530-48G Switch(J9775A)	HP	2530-48G	Grupo TIC	AEROPUERTO SALIDA NACIONAL
50	Switch	HPV1910	HP	V1910	Grupo TIC	AEROPUERTO ENTRADA INTERNACIONAL
51	Switch	SG300-10	CISCO	10 PORT GIGABIT	Grupo TIC	ASAMBLEA
52	Acces Point	UNIFI UAP-PRO	UBITIQUI	UNIFI	Grupo TIC	ASAMBLEA
53	Media	TP-LINK GIGABIT	TP-LINK	MC210CS	Grupo TIC	ASAMBLEA

 <p style="font-size: small;">Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p>	 <p style="font-size: small;">Gobernación del Archipiélago</p>	
<h2 style="margin: 0;">PLAN DE CONTINUIDAD Y DISPONIBILIDAD</h2>			

	Converter					
54	Firewall	FORTIANALYZER-100C	FORTINET	FAZ-100C	Grupo TIC	NOC-SISTEMAS
55	Media Converter	TP-LINK GIGABIT	TP-LINK	MC210CS	Grupo TIC	NOC-SISTEMAS
56	Media Converter	TP-LINK GIGABIT	TP-LINK	MC210CSI	Grupo TIC	NOC-SISTEMAS
57	Media Converter	TP-LINK GIGABIT	TP-LINK	MC210CS	Grupo TIC	NOC-SISTEMAS
58	Media Converter	TP-LINK GIGABIT	TP-LINK	MC210CS	Grupo TIC	NOC-SISTEMAS
59	Media Converter	TP-LINK GIGABIT	TP-LINK	MC210CS	Grupo TIC	NOC-SISTEMAS
60	Media Converter	TP-LINK GIGABIT	TP-LINK	MC210CS	Grupo TIC	NOC-SISTEMAS
61	Media Converter	CTC	CTC	MC210CS	Grupo TIC	NOC-SISTEMAS
62	Firewall	CYBEROAM	CYBEROAM	CR 500ING-XP	Grupo TIC	NOC-SISTEMAS
63	Switch	HP-A5120-JE068A 24PUERTOS	HP	JE068A	Grupo TIC	NOC-SISTEMAS
64	Controladora	RUCKUS	RUCKUS	ZONEDIRECTOR 3000 - NAR5520	Grupo TIC	NOC-SISTEMAS
65	Router	TP-LINK	TP-LINK		Grupo TIC	
66	Acces Point	Ruckus T710	RUCKUS	T710	Grupo TIC	DESPACHO
67	Acces Point	Ruckus T710	RUCKUS	T710	Grupo TIC	PASILLO 2DO PISO

 <p>Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p>	 <p>Gobernación del Archipiélago</p>	
<p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>			

						GOBERNACION
68	Switch	CISCO SG300-10	CISCO	SG300-10	Grupo TIC	FONDO DE PENSIONES
69	Switch	ENCORE ENH916P-NWY	ENCORE	ENH916P-NWY	Grupo TIC	CASA DE JUSTICIA
70	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	ESQUINA MICKEY MOUSE
71	Acces Point	RUCKUS	RUCKUS	r710	Grupo TIC	AEROPUERTO EMBRUJO - PROVIDENCIA
72	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	BAHIA SARDINA
73	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	SECRETARIA DE TURISMO
74	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	CASA DEL RELOJ
75	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	HOTEL TIUNA
76	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	MUELLE
77	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	ESQUINA CAFÉ-CAFÉ
78	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	BANCO DE BOGOTA
79	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	MANAWAR
80	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	AV 20 DE JULIO CON AV AMERICAS
81	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	HOTEL TONE
82	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	SEC. TURISMO/PROVIDENCIA
83	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	ALTOS DE NATANIA
84	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	HOTEL ISLEÑO

 <p style="font-size: small;">Gobernación del Archipiélago</p>	<p>GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA</p>	 <p style="font-size: small;">Gobernación del Archipiélago</p>	<p>PLAN DE CONTINUIDAD Y DISPONIBILIDAD</p>
--	--	---	--

85	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	LOMA BARACK
86	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	PARQUE NEWBALL
87	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	BARRACUDA
88	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	AEROPUERTO-SEGUNDO PISO - SAI
89	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	AEROPUERTO-SAI SALA DE ESPERA
90	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	PESCADERO (CAÑÓN DE MORGAN)
91	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	MUELLE CATAMARAN- EDIFICIO AURY-PROVIDENCIA
92	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	ALCALDIA - PROVIDENCIA
93	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	PUENTE ENEAMORADOS - PROVIDENCIA
94	Acces Point	RUCKUS	RUCKUS	zf7782	Grupo TIC	AGUA DULCE - PROVIDENCIA
95	Router	CISCO	CISCO		Grupo TIC	LUDOTECA
96	Switch	3COM	3COM	3CFSU08	Grupo TIC	LUDOTECA
97	Switch	3COM BASELINE	3COM	3C16471	Grupo TIC	SEC CULTURA
98	Switch	CISCO SG300-10	CISCO	SG300-10	Grupo TIC	INSPECCION POLICIA LOMA
99	Switch	CISCO SG300-10	CISCO	SG300-10	Grupo TIC	CRUE
100	Switch	PULPO	3BUMEN	PULPO8	Grupo TIC	LABORATORIO DE SALUD
101	Firewall	USG6000	HUAWEI	Secospace USG6620	Grupo TIC	NOC-SISTEMAS

 Gobernación del Archipiélago	GOBERNACIÓN DEPARTAMENTO ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA	 Gobernación del Archipiélago
	PLAN DE CONTINUIDAD Y DISPONIBILIDAD	

102	Planta Telefónica	UNIFY OPEN SCAPE BUSINESS	SIEMENS	X8 BASE BOX	Grupo TIC	NOC-SISTEMAS
103	Planta Telefónica	UNIFY OPEN SCAPE BUSINESS	SIEMENS	X8 EXPENSION BOX	Grupo TIC	NOC-SISTEMAS
104	UPS	SYSKAB	SIEMENS	S30122-K5950-F300-3	Grupo TIC	NOC-SISTEMAS
105	UPS	BACKUPS	APC	ES 550	Gobernación	USUARIOS
106	Repositorio	ONE DIVE	MICROSOFT	ONE DIVE	Gobernación	USUARIOS



Gobernación
del **Archipiélago**

GOBERNACIÓN DEPARTAMENTO
ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA
Y SANTA CATALINA



Gobernación
del **Archipiélago**

**PLAN DE CONTINUIDAD Y
DISPONIBILIDAD**

: