1. OBJETIVO

Dar trámite a los requerimientos de copias de respaldo de los datos de los sistemas operativos, de las bases de datos, de las soluciones tecnológicas que permita salvaguardar la información de los componentes On-Premise de la Plataforma Tecnológica de la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales - UAE DIAN.

2. DOCUMENTOS RELACIONADOS

Tipo de documento	Código	Titulo	Modo de uso	Clasificación documento
Procedimiento	PR-IIT-0460	Gestión de requerimientos	Digital	Interno
Formato	FT-IIT-2207	Diagrama para toma de copias de respaldo	Digital	Interno

3. DEFINICIONES Y SIGLAS

- **Administrador de Servicio**. Es la forma en que los equipos de TI administran la prestación de servicios de TI, de extremo a extremo, a los clientes. Esto incluye todos los procesos y actividades para diseñar, crear, ofrecer y dar soporte a los servicios de TI.

  Fuente: Consultado en https://inlogiq.com/que-es-la-administracion-de-servicios-de-ti-itsm/

- **Administrador de Servidor**. Es una consola de administración que ayuda a los profesionales de TI a aprovisionar y administrar servidores locales y remotos desde sus escritorios, sin necesidad de tener acceso físico a los servidores

  Fuente: Consultado en https://learn.microsoft.com/es-es/windows-server/administration/server-manager/server-manager

- **Archivos UCS (Compressed User Configuration).** Sistema de Caracteres Unicode. Referencia del juego de caracteres estándar internacional que es parte del estándar Unicode. La versión existente del estándar **UCS** más aceptada es *UCS-2*, que especifica valores de caracteres de 16 bits aceptados y reconocidos para usarse en la codificación de la mayor parte de los idiomas del mundo

  Fuente: https://www.glosarioit.com/UCS

- **Cartucho**. Elemento extraíble que funciona como una memoria con información de solo lectura.

  Fuente: Consultado en https://definicion.de/cartucho/

- **Cintoteca.** Almacén donde se depositan las cintas magnéticas que no se encuentran en uso en tareas de respaldo o en custodia externa.

  Fuente: Función Pública – Colombia. Página 4. Política de respaldo, custodia y recuperación de la información. Consultado en https://www.funcionpublica.gov.co/documents/34645357/34703081/Politicas_respaldo_custodia_informacion.pdf/cdadd3ea-31f5-4154-be6a-f8227b3cc47e?t=1544198825391

- **Consola Symantec**. Se refiere al producto Symantec Client Management Suite (CMS), el cual permite administrar, parchear y corregir configuraciones de aplicaciones y sistemas operativos para computadoras de escritorio, computadoras portátiles y servidores a lo largo de su ciclo de vida para fortalecer la seguridad de los endpoints.

  Fuente: Consultado en https://www-east.symantec.com/content/dam/symantec/docs/data-sheets/client-management-suite-en.pdf

- **Copia de respaldo**. Una copia de todo o parte del software o archivos de datos en un sistema preservado en medios de almacenamiento, como cinta o disco, o en un sistema separado para que los archivos puedan restaurarse si los datos originales se eliminan o dañan.

  Fuente: Libro: A Glossary of Archival and Records Terminology. Autor: Richard Pearce-Moses. Página: 45

- **COS - IBM (Cloud™ Object Storage)**. Permite almacenar cantidades ilimitadas de datos, de forma sencilla y rentable. Se utiliza comúnmente para archivar datos y copias de seguridad, para aplicaciones web y móviles, y como almacenamiento escalable y persistente para la analítica. La opción integrada de transferencia de datos de alta velocidad de IBM Aspire® facilita la transferencia de datos hacia y desde Cloud Object Storage, y la funcionalidad de consultas en el sitio permite ejecutar analíticas directamente en los datos.

  Fuente: Consultado en https://www.ibm.com/co-es/cloud/object-storage

- **Diagrama.** Formato que indica la ubicación de las cintas, según el consecutivo de cada una, en la cintoteca.

  Fuente: UAE DIAN – Dirección de Gestión de Innovación y Tecnología

- **Direcciones IP**. Es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa “protocolo de Internet”, que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local.

  Fuente: Consultado en https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address

- **Esquema**. Exposición ordenada de los puntos o cuestiones esenciales de un asunto o materia; en especial la escrita en que dichos puntos se relacionan con líneas, números u otros signos gráficos para indicar su interdependencia.

  Fuente: Consultado en https://languages.oup.com/google-dictionary-es/

- **Hash**. Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos, en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud**.**

  Fuente: Choosing Best Hashing Strategies and Hash Functions. Publicado en: 2009 IEEE International Advance Computing Conference.

- **Hyper-V**. Es el producto de virtualización de hardware de Microsoft. Permite crear y ejecutar una versión de software de un equipo, denominada máquina virtual. Cada máquina virtual actúa como un equipo completo, ejecutando un sistema operativo y programas.

  Fuente: Consultado en https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/hyper-v-technology-overview

- **IBM COS Object Storage (COS)** es un sistema de almacenamiento que se puede utilizar para almacenar datos no estructurados que son flexibles, rentables y escalables.

  Fuente: Consultado en https://cloud.ibm.com/docs/node?topic=node-object-storage&locale=es

- **Instancias.** Se llama instancia a todo objeto que derive de algún otro. De esta forma, todos los objetos son instancias de algún otro, menos la clase Object que es la madre de todas.

  Fuente: Consultado en https://www.glosarioit.com/Instancia

- **McAfee Web Gateway.** Es un Gateway (puerta) web seguro de alto rendimiento, que ofrece una protección frente a amenazas inigualable en una arquitectura unificada de appliance de software.

  Fuente: McAfee Web Gateway. Consultado en https://www.mcafee.com/enterprise/es-es/products/web-security-products.html

- **MGMT**. Se refiere a la plataforma de gestión de seguridad en el centro de datos principal con el producto Smart-1 de Check Point. Este producto es una solución de gestión de seguridad todo en uno, con gestión de políticas integrada, visibilidad de amenazas, flujo de trabajo y orquestación, que permite la consolidación de la seguridad en cualquier entorno de TI.

  Fuente: Smart-1 Security Management Platforms DATASHEET. Autor: Check Point. Consultado en https://www.checkpoint.com/downloads/products/smart-1-security-management-platform-datasheet.pdf

- **Paths**. Camino que toma un programa para acceder a los datos contenidos en la unidad de almacenamiento o de la memoria externa al ordenador.

  Fuente: Consultado en https://www.glosarioit.com/Path

- **RACK**. Es un armario metálico cuya función es guardar los equipos informáticos, equipamiento electrónico y el de comunicaciones

  Fuente: Consultado en https://www.vertiv.com/

- **SAN - Storage Area Network / Sistema de Almacenamiento Masivo**. Una red de área de almacenamiento (SAN, Storage Area Network) es un tipo especial de red de área local de alta velocidad destinada a conectar numerosos bancos de dispositivos de almacenamiento (discos) a las computadoras que utilizan los datos.

  Fuente: Fundamentos de Bases de Datos, 5a, Edición. Autor: Abraham Silberschatz / Henry F. Korth / S. Sudarshan. Página: 667

- **Servidor Central**. El servidor central es responsable de entregar la lógica de la aplicación, procesar y proporcionar recursos informáticos (tanto básicos como complejos) a las máquinas cliente conectadas.
  Fuente: Centralized Computing. Autor: techopedia. Consultado en https://www.techopedia.com/definition/26507/centralized-computing

- **Sistemas de archivos**. Un sistema de archivos, sistema de ficheros o file system es el conjunto de procesos y normas que se llevan a cabo para el almacenamiento de un dispositivo de memoria. Este sistema le permite al usuario identificar la ubicación de los archivos y poder acceder a ellos de una forma rápida

  Fuente: Consultado en https://keepcoding.io/blog/que-es-un-sistema-de-archivos

- **Spectrum Protect**. IBM Spectrum Protect permite replicar los datos de copia de seguridad en una base de nivel incremental y granular de un servidor de IBM Spectrum Protect a otro. La réplica se basa en políticas, así que las políticas respectivas locales y externas pueden ser diferentes. Además, esta replica se puede realizar con datos des duplicados y cifrados, lo que mejora la eficiencia y la seguridad de la red.

  Fuente: Consultado en https://www.ibm.com/co-es/products/data-protection-and-recovery/details

- **TRD – Tabla de retención documental**. Se define como el listado de series, con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos, es decir se considera como el Instrumento que permite establecer cuáles son los documentos de una entidad, su necesidad e importancia en términos de tiempo de conservación y preservación y que debe hacerse con ellos una vez finalice su vigencia o utilidad.

  Fuente: Archivo General de la Nación – Colombia https://www.archivogeneral.gov.co/transparencia/gestion-informacion-publica/Tablas-de-Retencion-Documental-TRD

- **V5000 - IBM® Storwize® V5000**. IBM® Storwize® V5000 solución de almacenamiento robusta para proporcionar servicios de almacenamiento integrales, una escala extraordinaria y una administración simplificada con opciones todo flash o flash híbrido, todo diseñado para apoyar iniciativas comerciales clave.

  Fuente: IBM Storwize V5000. Consultado en https://www.ibm.com/downloads/cas/AJPNKQGV

4. DESARROLLO DEL TEMA

4.1 Condiciones Generales

- Las copias de respaldo se realizan con frecuencia diaria, mensual, semestral y anual.

- El tiempo de retención preestablecido en todos los casos, con excepción de aquellos en los que el administrador del servicio disponga diferente, será así:

  - ✓ Incrementales, son aquellas copias diarias tomadas de lunes a domingo y su retención es de 60 días.

- ✓ Mensuales, son aquellas copias tomadas al final del mes, y su retención es de un (1) año.
- ✓ Semestral, son aquellas copias tomadas cada 30 de junio y su retención es de cinco (5) años.
- ✓ Anuales, son aquellas copias tomadas cada 31 de diciembre y su retención es de cinco (5) años.
- ✓ No programado y a solicitud, son aquellas copias tomadas cada vez que se necesita y su retención es máximo de 5 años.
- ✓ La información de SIGLO XXI se respalda diariamente y su retención es de 10 años.
- ✓ Las Máquinas Virtuales Hyper-V se respaldan diariamente y su retención es de 60 días.

4.2 Descripción de actividades

4.2.1 Programar copias de respaldo para Servidores de BD, de soluciones tecnológicas y de Files

- La base de datos de Spectrum Protect es la única Base de datos que se respalda en Disco y también en Cartucho; este proceso es alternado y se ejecuta a diario

- El responsable o administrador de cada servidor debe solicitar al administrador de la herramienta de respaldo Spectrum Protect incluir dicha maquina dentro del esquema de Backup definido por la Subdirección de Infraestructura Tecnológica y de Operaciones o quien haga sus veces. Para esto debe informar:

  - ✓ Si la copia de respaldo requerida corresponde a una base de datos Oracle deberá indicarse la versión, si está alojado en RACK y las direcciones IP de los servidores donde se encuentran las instancias de dicha base de datos.
  - ✓ Si la copia de respaldo requerida corresponde a uno o varios sistemas de archivos deberá indicar los paths o rutas de la información a respaldar.

- El funcionario responsable de la administración de la herramienta Spectrum Protect realiza las siguientes tareas, de acuerdo a las indicaciones técnicas recibidas por parte del proveedor:

  - ✓ Instalar localmente en el servidor cliente el agente de la herramienta de acuerdo con el sistema operativo y tipo de archivo o base de datos a respaldar.
  - ✓ Configurar localmente el agente en el servidor cliente.
  - ✓ Configurar lo pertinente del servidor cliente en el servidor Spectrum Protect ..
  - ✓ Hacer pruebas manuales de funcionamiento de la copia de respaldo
  - ✓ Programar la ejecución automática de la copia de respaldo del servidor cliente en el servidor Spectrum Protect, especificando el tiempo de retención.

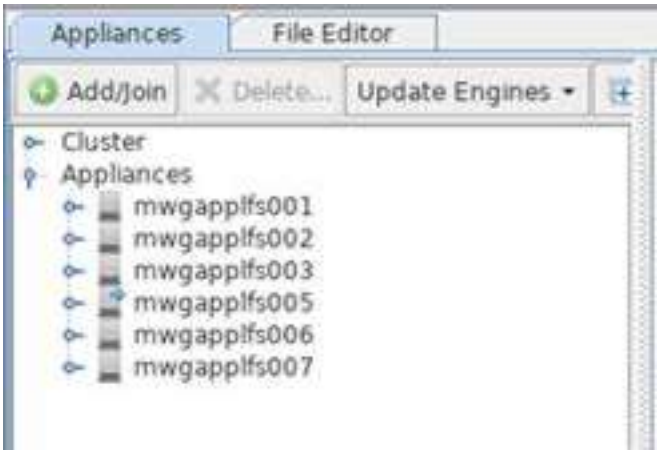
4.2.2 Ejecutar la copia de respaldo

El sistema Spectrum protect escanea su agenda cada minuto y ejecuta los backups que estén programados en ese momento.

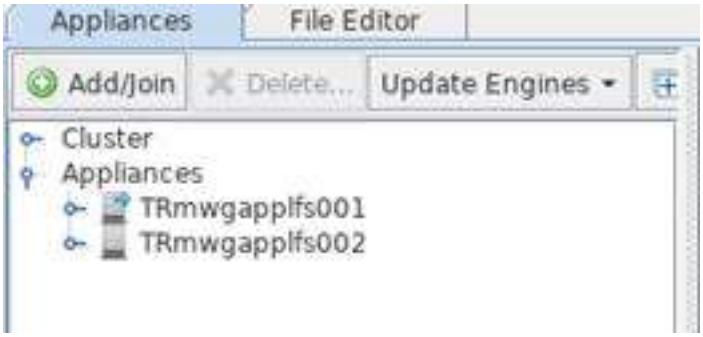
4.2.3 Copias de respaldo de las herramientas de seguridad informática

A. McAfee web Gateway

- Se realiza la configuración en cada uno de los Gateway donde se le envían los logs al servidor de la base de datos SQL, este es un proceso que se realiza mientras se configura por primera vez cada Gateway.



Appliances para funcionarios



Appliances para WIFI

- Se verifica que la base de datos quede conectada y prestando servicio a los Gateway.

Default internal database

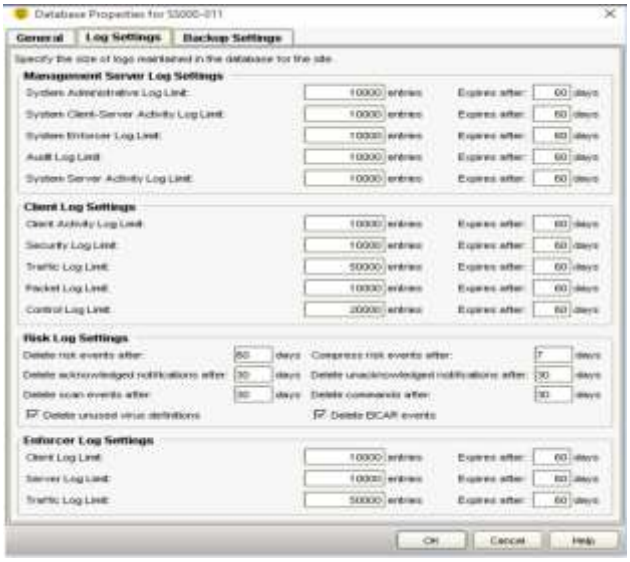
This external database : Microsoft SQL Server 2012

Database settings	
Database address:	10.255.33.14
Database port:	1433
Logon name:	reporter
Password:	**********
Instance name (if any):	
Database name:	Reporting

- Se toma copia de respaldo de la configuración de los Gateway y se almacena en el disco denominado *Datos (F:)* del servidor de la base de datos, al cual se le está realizando el respaldo con la herramienta Spectrum Protect.

B. Symantec

- Se realiza la configuración de las consolas de administración para que se observe la base de datos SQL y se envíen los logs a la misma. Este es un proceso interno que se realiza mientras se configura por primera vez las consolas.



- Se verifica que la base de datos quede conectada y prestando servicio a las consolas.

- Se toma copia de respaldo de la configuración de las consolas y se almacena en el disco (E:) de los servidores a los cuales se les realiza el respaldo con la herramienta Spectrum Protect.

Programación TSM Semanal

C. Logs y configuración en firewall CheckPoint

- Se desarrollan scripts en Basic Shell para realizar la compresión y transmisión de los logs y de las copias de respaldo que se generan en las consolas MGMT-SA1 y MGMT-ALT2, de forma automática hacia un disco en la SAN, con el propósito de incluir el respaldo de la información correspondiente en cintas.

- Los scripts mencionados anteriormente, se realizan de la siguiente forma:

  - ✓ Para la compresión diaria de los archivos de log, se ejecuta el script a las 11:30 PM.
  - ✓ Para la transmisión de los logs empaquetados, se ejecuta el script a las 1:00 AM.
  - ✓ Para el borrado de los logs empaquetados, se ejecuta el script a las 1:30 AM.

- A continuación, se muestran imágenes de la programación de los scripts correspondientes:

```
SHELL=/bin/bash
MAILTO=""
#
# mins  hrs     daysinm months  daysinw command
#

##__backup__Backup_Day
00      4       *       *       *       /bin/scheduled_backup Backup_Day

##__backup__MGMT_backup
30      22      *       *       5       /bin/scheduled_backup MGMT_backup


##Copia de logs comprimidos
00     01       *       *       *       /usr/lbin/copiaLog.sh

## Genera Logs Comprimidos
30      23      *       *       *       /usr/lbin/comprimeLog.sh

## Depuracion de Logs
30      01      *       *       0       /usr/lbin/borraLog.sh
```

```
[Expert@MGMT-ALT2:0]# date
Tue Sep 29 12:25:43 COT 2015
[Expert@MGMT-ALT2:0]# crontab -l
#  This file was AUTOMATICALLY GENERATED
#  Generated by /bin/cron_xlate on Thu Jun  4 10:48:31 2015
#
#  DO NOT EDIT
#
SHELL=/bin/bash
MAILTO=""
#
# mins  hrs     daysinm months  daysinw command
#

##Copia de logs comprimidos
00     01       *       *       *       /usr/lbin/copiaLog.sh

## Genera Logs Comprimidos
30      23      *       *       *       /usr/lbin/comprimeLog.sh

[Expert@MGMT-ALT2:0]#
```

En cualquiera de los dos (2) casos anteriores, se deja un rastro localmente de la ejecución de los scripts en la ruta /tmp/copiaLogs.txt.

D. Logs y configuración de la plataforma F5

La toma de backup de la plataforma F5 se realiza a los Chasis y guest del Sitio 1 y Sitio 2 por medio de tarea programada diaria a los archivos UCS (Compressed User Configuration) que contiene la configuración. Así mismo, los domingos de cada semana se ejecuta una tarea programada a la carpeta de log's (/var/log) de la plataforma, con el fin de mantener un registro de copia de respaldo semanal.

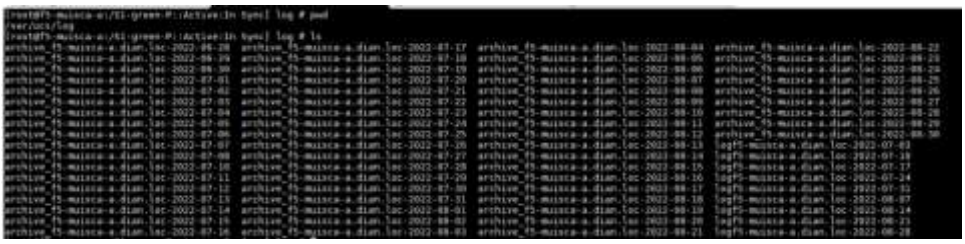
Para el caso de la toma del archivo UCS se ejecuta una tarea cron todos los días a las 11:00 PM horas que contiene lo siguiente:

Luego en la misma tarea el archivo UCS es enviado a la subcarpeta /backuptsm1/No_Borrar/F5/$hostname del guest o chasis correspondiente en el servidor CENTRAL (10.255.32.131).

Los archivos de log's de la plataforma se ejecutan semanalmente los domingos a las 11:30 PM horas, con el scritp que está en la ruta /usr/tmp/backup_to_central.sh en los guest o chasis de la Plataforma. El script contiene lo siguiente:

Se hace un archivo tar de la carpeta /var/log con el nombre del host del guest o chasis, incluyendo la fecha en el formato (YYYY-MM-DD) y se envía al servidor CENTRAL (10.255.32.131).

Todos los log's de la evidencia de la toma de los backups se encuentran en la carpeta /var/ucs/log ubicada en cada guest o chasis. Los archivos que contienen la evidencia de la toma de backup de los archivos UCS tienen el formato archive_$hostname-YYYY-MM-DD.log y la de la toma de los archivos de log el formato logF5_$hostname-YYYY-MM-DD.log. A estos archivos no se les hace backup ni tienen tiempo de retención. A continuación, se muestra un ejemplo para el guest f5-muisca-a.



4.2.4 Equipos de comunicaciones

Los backups de configuración de los switches a nivel nacional, se toman automáticamente con la herramienta orión todos los 27 de cada mes y se guardan en un repositorio, al cual tiene acceso todo el grupo de Comunicaciones si requiere realizar la recuperación de alguno de ellos.

E. Core con IMC

El servidor se respalda como Máquina Virtual y su retención es de 60 días.

4.2.5 Respaldos de servicios en NUBE Azure, Sharepoint, correo

La retención de los documentos en SharePoint online se establece en la Orden de Compra y/o contrato con los proveedores del servicio, en el momento está establecido de cinco años. Las áreas que requieran una duración mayor deberán solicitarlo a través de un caso en Soporte TIC, para análisis de la Dirección de Gestión de Innovación y Tecnología.

4.3 Verificar ejecución de la copia de respaldo

El funcionario responsable de la administración del sistema de respaldos verificará que la copia de respaldo se haya ejecutado correctamente; en caso de que no se haya ejecutado correctamente la hace manualmente (Bajo demanda) o vuelve a programar la ejecución en un horario alterno.

Disposición de la copia de respaldo

En la plataforma de respaldo Spectrum Protect , la información es guardada en el almacenamiento IBM V5000 y después de dos (2) meses las copias de respaldo históricas (mensuales, semestrales, anuales) son transferidas automáticamente al almacenamiento IBM COS donde permanecerán hasta que expire el tiempo de retención.

(Para terminar de organizar las cintas de respaldos históricos – en disco se tiene desde 2020) Cuando exista la necesidad de retiro de cartuchos, una vez éstos se encuentren en el bolsillo de la librería, se solicita el retiro y la identificación del medio al buzón centrocomputo@dian.gov.co. Dichos medios se deben identificar por el operador del centro de cómputo conforme al siguiente rotulo, quien entrega los medios al funcionario responsable de la cintoteca:

<table>
<tr><th colspan="2">LIBRERÍA / EQUIPO</th><th>MEDIO MAGNETICO</th></tr>
<tr><td colspan="2">Nombre librería
Periodicidad de la copia de respaldo (tipo de copia)
Contenido</td><td rowspan="3">Consecutivo de la cinta</td></tr>
<tr><td>Fecha retiro</td><td>Secuencia</td></tr>
<tr><td colspan="2"></td></tr>
</table>

4.4 Almacenar cintas para su custodia en la entidad

El funcionario responsable de la cintoteca registra en el formato "*FT-IIT-2207 Diagrama para toma de copias de respaldo*" el consecutivo de los medios junto con su ubicación en la cintoteca, y almacena los medios durante el tiempo de retención establecido por el administrador del servicio.

5. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de Cambios	Tipo de información
	Desde	Hasta		
1	10/09/2021	14/11/2022	Versión inicial, Se deroga el procedimiento: • PR-SI-0343 Toma y custodia de copias de respaldo	No aplica

			Se derogan los siguientes instructivos: • IN-SI-0172 Toma de Copias de Respaldo MCAFEE WEB GATEWAY • IN-SI-0173 Toma de Copias de Respaldo SYMANTEC • IN-SI-0174 Respaldo de Logs y Configuración en FIREWALL CHECKPOINT	
2	15/11/2022		Versión 2 que reemplaza lo establecido en la versión 1. Se modifica Objetivo, Numeral 3. *Definiciones y Siglas* y Numeral 4. *Desarrollo del Tema.* Se actualiza la plantilla del presente documento, de acuerdo con la versión 5 del procedimiento "*PR-PEC-0001 Documentación del sistema de gestión*".	Esta versión corresponde a información pública

Elaboró:	Gilbert Dario Ortega Samboni **Elaboración técnica**	Gestor III	Subdirección de Infraestructura Tecnológica y de Operaciones
	Claudia Marcela Lucena Pérez **Elaboración técnica**	Gestor III	Subdirección de Infraestructura Tecnológica y de Operaciones
	Juan Pablo Serna Botero **Elaboración técnica**	Gestor IV	Coordinación Centro de Gestión de Proyectos de Innovación y Tecnología CENIT
	Tito Alejandro Menjura **Elaboración Metodológica**	Gestor II	Coordinación de Procesos y Riesgos Operacionales
	Alfredo A. Ahumada A. **Elaboración Metodológica**	Gestor II	Coordinación de Procesos y Riesgos Operacionales
Revisó:	Juan Carlos Vizcaino	Inspector IV	Subdirección de Infraestructura Tecnológica y de Operaciones
	Olga Lucía Hurtando Hurtado	Inspector III	Subdirección de Infraestructura Tecnológica y de Operaciones
Aprobó:	Héctor Leonel Mesa Lara	Subdirector	Subdirección de Infraestructura Tecnológica y de Operaciones