1. OBJETIVO

Asegurar la correcta operación, disponibilidad y seguridad de la plataforma tecnológica alojada en los centros de datos de la UAE DIAN, a través del cumplimiento de las políticas de seguridad, el monitoreo físico y ambiental, haciendo uso de las herramientas de hardware y software dispuestas para ello.

2. DOCUMENTOS RELACIONADOS

Tipo de documento	Código	Titulo	Modo de uso	Clasificación documento
Procedimiento	PR-IIT-0460	Gestión de requerimientos	Digital	Interno
Procedimiento	PR-ADF-0018	Egreso de bienes muebles	Digital	Interno
Procedimiento	PR-IIT-0457	Gestión de cambios	Digital	Interno
Instructivo	IN-ADF-0139	Reintegro de bienes a bodega	Digital	Interno
Formato	FT-ADF-1557	Autorización de salida de elementos	Digital	Interno
Formato	FT-IIT-1877	Solicitud de cambio en la infraestructura tecnológica	Digital	Interno
Formato	FT-IIT-1878	Control de ingreso a los centros de datos - Operadores	Digital	Interno
Formato	FT-IIT-1879	Control de ingreso a los centros de datos - Vigilancia	Digital	Interno
Formato	FT-IIT-1880	Solicitud de ingreso a los centros de datos	Digital	Interno
Formato	FT-IIT-2635	Compromiso de confidencialidad y no divulgación de la información reservada o clasificada	Digital	Interno
Formato	FT-IIT-2714	Bitácora de eventos	Digital	Interno

3. DEFINICIONES Y SIGLAS

- **Administrador de servicio**. Funcionarios de la UAE DIAN responsables de administrar componentes de la plataforma (grupo comunicaciones, grupo base de datos, grupo despliegue, grupo seguridad y administrador técnico centros de datos).

  Fuente: UAE DIAN - Subdirección Infraestructura Tecnológica y Operaciones**.**

- **Activos de información**. Se entiende cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio. Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización. (ISO/IEC 27000). Son los recursos del Sistema de Seguridad de la Información indispensables para que una empresa funcione y consiga los objetivos que se ha propuesto la alta dirección.

  Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones (2017), Glosario de Términos. Consultado en http://www.mintic.gov.co/portal/604/w3-article-4013.html

- **Aire acondicionado de precisión**. Son equipos diseñados para lograr un ambiente, donde, en forma simultánea y continua, se controlan la temperatura, la humedad, la circulación y la limpieza del aire, a la vez que se mantiene una presión positiva en la sala, en relación con otros ambientes,

para una exigencia de trabajo de 24 horas al día durante los 365 días del año, por un tiempo de vida útil entre 15 y 20 años.

Fuente: Consultado en https://www.mundohvacr.com.mx/2014/01/aa-de-precision-vs-aa-de-confort/

- **Alta disponibilidad**. Es la capacidad de un sistema o componente del sistema para estar continuamente operando durante un período deseablemente largo; es decir, sin interrupciones por fallos. La alta disponibilidad funciona como un mecanismo de respuesta a fallas para la infraestructura. La forma en que funciona es bastante simple conceptualmente, pero generalmente requiere un software y configuración especializados.

  Fuente: Libro - Data Center Handbook. Consultado en https://ciberseguridad.com/guias/alta-disponibilidad/

- **Base de datos**. Recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático. Una base de datos está controlada por un sistema de gestión de bases de datos (DBMS). En conjunto, los datos y el DBMS, junto con las aplicaciones asociadas a ellos, reciben el nombre de sistema de bases de datos, abreviado normalmente a simplemente base de datos.

  Fuente: Consultado en https://www.oracle.com/co/database/what-is-database/

- **Centro de datos**. Espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización a través de un sistema informático especializado de hardware de alta potencia y disponibilidad en un ambiente controlado con la finalidad de almacenar, resguardar y procesar datos a gran escala. Estos datos son distribuidos a otros sistemas o personal autorizado para consultarlos y/o modificarlos.

  Fuente: Consultado en https://www.ecotec.edu.ec/documentacion/investigaciones/docentes_y_directivos/articulos/5816_TRECALDE_00226.pdf -

- **Centro de datos Site1**. En condiciones normales de operación de la plataforma de TI de la entidad que presta los servicios informáticos electrónicos, atiende las peticiones realizadas por los usuarios tanto internos como externos de la entidad; en el evento que se detecte una falla que genere una indisponibilidad en los servicios informáticos electrónicos prestados por el centro de datos Site1, el centro de datos Site2 asume la operación, garantizando la prestación de los mismos de cara a los usuarios; esto es posible porque la configuración de operación de los centros de datos de la UAE DIAN se encuentran dispuestos en la topología para recuperación de desastres y continuidad del negocio en modo ACTIVO/ACTIVO.

  Fuente: High availability and disaster recovery for your on-premises app. Consultado en https://www.ibm.com/garage/method/practices/manage/hadr-on-premises-app/

- **Centro de datos Site2.** En condiciones normales de operación de la plataforma de TI de la entidad que presta los servicios informáticos electrónicos, el centro de datos Site2, actúa como respaldo de la operación del centro de datos Site1, debido a que los centros de datos se encuentran dispuestos en la topología para recuperación de desastres y continuidad del negocio en modo ACTIVO/ACTIVO. En una eventual indisponibilidad del centro de datos Site1, asume toda la operación garantizando la continuidad de los servicios.

Fuente: High availability and disaster recovery for your on-premises app https://www.ibm.com/garage/method/practices/manage/hadr-on-premises-app/

- **Centro de Datos**. Un Centro de Datos debe ofrecer la garantía de que el negocio siga funcionando de manera correcta sin importar los eventos que se susciten por una indisponibilidad en el servicio.

  Fuente: Consultado en https://www.optical.pe/blog/que-es-un-data-center-y-cual-es-su-importancia/

- **Cintoteca o Archivos Magnéticos**. Área física donde se almacenan, custodian y resguardan las cintas o medios magnéticos que no se encuentran en uso, en tareas de respaldo o en custodia externa.

  Fuente: 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)

- **Control de acceso físico**. Sistema electrónico que restringe o permite el ingreso de un usuario a un área específica validando la identificación por medio de diferentes tipos de lectura (clave por teclado, tags de proximidad o biometría) que a su vez controla un recurso de acceso (puerta, torniquete o talanquera) por medio de un dispositivo eléctrico como un electroimán, cantonera, pestillo o motor.

  Fuente: NTC - ISO / IEC 27001. Consultado en https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso

- **Componente**. Elemento, pieza o accesorio indispensable que forma parte de un sistema. Un componente puede ser hardware y/o software y puede estar subdividido en otros componentes.

  Fuente: IEEE Standard Glossary of Software Engineering Terminology. Consultado en https://www.significados.com/componentes/

- **Componente de enfriamiento de precisión**. Equipo o equipos de aire acondicionado de precisión que conforman un sistema de climatización de un centro de datos.

  Fuente: Aires acondicionados de precisión. Consultado en https://www.logisa.com/aires-acondicionados-de-precision

- **Componente de redes de telecomunicaciones**. Conjunto de ordenadores, computadoras o dispositivos interconectados que permite intercambiar información y recursos de uno a otro, tales como impresoras, discos duros terminales, nodos y medios de interconexión que pueden incluir líneas o troncales, satélites, microondas, radio de onda media y larga, entre otros. En general, una red es una colección de recursos utilizados para establecer y cambiar rutas de comunicación entre sus terminales.

  Fuente: Dictionary of Computer Science - Oxford Quick Reference, 7a. Edición

- **Componente redes eléctricas**. Un circuito eléctrico básico está formado por un conjunto de componentes, que ordenados y conectados adecuadamente permiten el paso de la corriente. Los componentes básicos de una red eléctrica son: Fuente de energía que se encarga de proporcionar

la energía, conductores eléctricos que la transportan, la carga (equipos y artefactos conectados) y los medios conexión y desconexión que permiten energizar o desenergizar las cargas.

Una red eléctrica es la encargada generar, transmitir y distribuir la energía eléctrica desde los centros de generación a los consumidores finales.

Fuente: Consultado en https://www.electricasas.com/elementos-basicos-instalacion-electrica/

- **Gabinete o Rack**. Mueble metálico diseñado para alojar los elementos de conectividad de red y los equipos de servicio. Su diseño permite alojar diversos dispositivos que prestan diferentes servicios (Switches, enrutadores, servidores, entre otros).

  Fuente: Consultado en https://www.monografias.com/docs/gabinete-de-telecomunicaciones

- **Infraestructuras críticas**. Son las infraestructuras estratégicas, que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales de la organización. En ellas están incluidos todos los activos vitales para cualquier país que su destrucción o degradación tendría un efecto debilitante en las funciones primordiales del gobierno, la seguridad nacional, la economía nacional o la salud pública.

  Fuente: Critical Infrastructure Protection Plans.Autor: Gabriel J. Correa / José M. Yusta. Publicado en: VII Simposio Internacional sobre Calidad de la Energía Eléctrica - Colombia - Consultado en https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas

- **Nivel de redundancia**. El principio de redundancia en sistemas es proporcionar un cambio de funcionalidad a un componente en espera o de respaldo en caso de que falle un componente primario. Esta acción ocurre automáticamente y no requiere un operador para la conmutación. Aunque la redundancia asegura una mayor confiabilidad, tiene profundos impactos en la inversión inicial y los costos operativos continuos.

  Existen varios tipos de redundancia (N, N + 1, 2N, 2 [N + 1]) que generalmente se refieren al número de componentes de alimentación y refrigeración que conforman los sistemas de respaldo en la infraestructura de un centro de datos.

  - ✓ N: Cumple con los requisitos básicos. La falla de cualquier componente causará una interrupción.
  - ✓ N + 1: Proporciona una unidad / módulo / ruta adicional más que el requisito básico; la falla en una sola unidad no interrumpirá las operaciones.
  - ✓ N + 2: Proporciona dos unidades / módulos / rutas o sistemas adicionales más que el requisito básico; la falla en una sola unidad no interrumpirá las operaciones.
  - ✓ 2N: Se requieren dos unidades / módulos / rutas o sistemas completos para la operación. La falla de un sistema completo no interrumpirá las operaciones ni afectará el rendimiento. Tanto N + 1 como 2N representan niveles crecientes de redundancia.
  - ✓ 2 (N + 1): Dos unidades / módulos / trayectorias completas (N + 1); la falla de un sistema completo aún deja un sistema completo con redundancia (N + 1)

  Fuente: Data Center Handbook, Editorial: John Wiley & Sons, Autor: Hwaiyu Geng, Página: 9. Consultado en https://www.mdcdatacenters.com/es/company/blog/avoid-risks-and-go-for-2n-power-redundancy/

- **Redundancia**. Duplicación de componentes críticos para aumentar la seguridad del sistema y garantizar su disponibilidad total. La redundancia en TI es muy importante, por ejemplo, si solo hay un servidor web en un momento de falla, el servicio que soporta no se podría utilizar.

  Fuente: Data Center Handbook, Editorial: John Wiley & Sons, Autor: Hwaiyu Geng, Página: 9. Consultado en https://www.mdcdatacenters.com/es/company/blog/avoid-risks-and-go-for-2n-power-redundancy/

- **SAN (Storage Area Network)**. Red dedicada de alta velocidad que brinda acceso al almacenamiento a nivel de bloque. Las SAN se adoptaron para mejorar la disponibilidad y el rendimiento de las aplicaciones al segregar el tráfico de almacenamiento del resto de la LAN, permitiendo así la conexión de numerosos bancos de dispositivos de almacenamiento (discos).

  Fuente: Fundamentos de Bases de Datos, 5. Consultado en https://www.computerworld.es/networking/que-es-una-san

- **Seguridad física y del entorno**. Dentro de la Seguridad Informática, la Seguridad física y del entorno hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático para proteger el hardware y las instalaciones de amenazas físicas.

  Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC - Procedimientos de seguridad de la información. Consultado en https://sites.google.com/a/istpargentina.edu.pe/exposicion-areas-seguras/seguridad-fisica-y-del-entorno

- **Servidor.** Ordenador o equipo informático que se encarga de alojar, procesar o transmitir información a otros ordenadores que estén conectados a él. Además, esta transmisión de información también puede ser de ordenador a personas. Los datos que transmiten pueden ser de diversos tipos de acuerdo con los aplicativos que se manejen.

  Fuente: Diccionario de la Lengua Española. Consultado en https://dle.rae.es/ - https://desafiohosting.com/que-es-un-servidor/

- **SIE**. Servicios informáticos electrónicos

- **Sistema de climatización**. Sistema de regulación que controla los niveles de humedad y temperatura dentro de un centro de datos, manteniendo condiciones ambientales precisas para la integridad de los servidores, y, por lo tanto, de la información que en ellos se almacena.

  Fuente: Consultado en https://www.kionetworks.com/blog/data-center/importancia-de-la-climatizaci%C3%B3n-de-un-data-center

- **Switch, Equipo Activo o Conmutador.** Dispositivo de interconexión utilizado para conectar equipos en red (formando junto con el cableado lo que se conoce como red de área local – LAN), con especificaciones técnicas que siguen el estándar Ethernet (IEEE 802.3), cuyo trabajo es transmitir paquetes entre las computadoras conectadas a él, y utiliza una dirección en cada paquete para determinar a qué computadora se lo debe enviar.

- Fuente: Redes de computadores, 5a. Edición. Consultado en https://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/

- **Termohigrómetro**. Es un instrumento electrónico utilizado para el monitoreo constante de la temperatura (T) y la humedad relativa (HR) de un ambiente especifico.

  Fuente: Thermo Hygrometer. Consultado en https://www.pce-instruments.com/english/measuring-instruments/test-meters/thermo-hygrometer-kat_151815.htm) - https://www.solerpalau.com/es-es/blog/termohigrometro/

- **UPS (Uninterruptible Power Supply) o SAI (Sistema de Alimentación Ininterrumpida)**. Dispositivo que permite mantener la alimentación eléctrica regulada mediante baterías cuando falla el suministro o se produce una anomalía eléctrica (por ejemplo, una sobretensión). Sirven para proteger por tanto los dispositivos que tienen conectados y mantenerlos en funcionamiento ante cortes o fluctuaciones en el suministro eléctrico.

  Fuente: Libro: Data Center Handbook, Editorial: John Wiley & Sons, Autor: Hwaiyu Geng, Página: 495. Consultado en https://www3.gobiernodecanarias.org/medusa/ecoblog/fmorherj/files/2014/04/Sistema-de-alimentacion-ininterrumpida.pdf

4. DESARROLLO DEL TEMA

4.1 Condiciones generales

- El personal técnico y de ingeniería de la entidad y de las firmas contratistas que dan soporte y mantenimiento a las diferentes plataformas de TI instaladas en los centros de datos de la UAE DIAN son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la entidad.

- La totalidad de las tareas a ejecutar en los centros de datos de la UAE DIAN, tanto a nivel de software como a nivel de hardware deben ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control. Cada grupo cuenta con un líder que es el responsable de cada actividad.

- En los centros de datos de la UAE DIAN, debe existir una persona de seguridad privada, adscrita a la compañía de vigilancia contratada por la entidad, para controlar el ingreso del personal a los centros de datos Site1 y Site2.

- Tanto el personal técnico de la entidad como las firmas contratistas que prestan soporte y mantenimiento a las diferentes plataformas de TI instaladas en los centros de datos de la UAE DIAN, que garantizan la disponibilidad de los servicios y soluciones tecnológicas prestados a través de los centros de datos Site1 y Site2, son responsables del cumplimiento de este documento y se comprometen a no divulgar la información de hardware, de software e instalaciones dentro del área blanca de los centros de datos.

- El Subdirector de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, es el responsable de administrar los centros de datos, y por consiguiente es el encargado de hacer cumplir el presente documento. Para coadyuvar a la administración de los centros de datos el Subdirector podrá designar a un funcionario como Administrador Técnico de los centros de datos.

- El Subdirector de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, se reserva el derecho de autorizar los respectivos ingresos, de monitorear las actividades realizadas en los centros de datos y detallar actividades que presenten un comportamiento inusual o sospechoso. El Administrador de los centros de datos deberá verificar, controlar y autorizar el ingreso al personal técnico y de Ingeniería de la entidad y de las firmas contratistas que dan soporte y mantenimiento a las diferentes plataformas de TI instaladas en los centros de datos de la UAE DIAN.

- Toda persona; funcionario de la entidad o personal de una firma contratista, al momento de ingresar a cualquiera de los centros de datos, acepta y reconoce la existencia de un documento denominado Acuerdo de Confidencialidad (documento que reposa a la entrada de cada uno de los centros de datos), mediante el cual se compromete a la no divulgación de información de infraestructura de clientes, de diseños, de datos al interior de equipos y visualmente desplegada en monitor, sensores, puertas, gabinetes de equipos, entre otros. Asimismo, reconoce y acepta la prohibición de NO intervenir, introducir, extraer, copiar, manipular, alterar, compartir, fotografiar, filmar, duplicar, respaldar, entre otras, sobre equipos de terceros. Al funcionario de la entidad o del proveedor que ingresa por primera vez a los centros de datos, se les hace leer y firmar el documento.

4.2 Administración de los centros de datos

- Para controlar el ingreso y garantizar la seguridad en los centros de datos Site12 y Site2 de la UAE DIAN, se debe tener en cuenta el cumplimiento de las políticas de seguridad consignadas en los formatos que aplican para el ingreso, permanencia y ejecución de actividades permanentes u ocasionales en los centros de datos:

  - ✓ *FT-IIT-1877 Solicitud de cambio infraestructura tecnológica*", en él se registran todas las actividades y cambios en la plataforma de TI instalada.

  - ✓ *FT-IIT-1878 Control de ingreso a los centros de datos – Operadores*", registro de entrada del personal técnico y de ingeniería de la entidad y de las firmas contratistas que dan soporte y mantenimiento a las diferentes plataformas de TI instaladas en los centros de datos de la UAE DIAN; contiene hora y descripción de la actividad a realizar y es responsabilidad del operador de turno.

  - ✓ "*FT-IIT-1879 Control de ingreso a los centros de datos – Vigilancia",* registro de entrada del personal técnico y de ingeniería de la entidad y de las firmas contratistas que dan soporte y mantenimiento a las diferentes plataformas de TI instaladas en los centros de datos de la UAE DIAN; contiene hora y descripción de la actividad a realizar y es responsabilidad del vigilante de turno.

  - ✓ *FT-IIT-1880 Solicitud de ingreso a los centros de datos:* El administrador de cada servicio solicita el ingreso del personal técnico y de ingeniería de la entidad y de las firmas contratistas que va a ingresar y es quien asume la responsabilidad de la actividad.

- Para asegurar la instalación y el correcto funcionamiento de los componentes relacionados con: sistemas eléctricos, sistema de climatización de precisión, sistema redes de telecomunicaciones, sistema de video vigilancia, sistema de monitoreo videowall, sistema de control de acceso, sistema de detección y extinción de incendios y sistema de iluminación, cada componente debe cumplir con los estándares técnicos mínimos para su instalación y correcto funcionamiento. La instalación y/o mantenimiento de dichos sistemas debe ser realizado por personal especializado (contratistas o terceros) con la supervisión de funcionarios de la entidad; las características técnicas de los

componentes de cada sistema son estipuladas en los pliegos de condiciones de los respectivos procesos de adquisición, instalación y puesta en funcionamiento; así como en los contratos de mantenimiento de cada sistema.

- Para la identificación de los equipos dentro del área blanca de los centros de datos, se define la siguiente nemotecnia: se genera un plano “XY” donde se ubican los gabinetes del cómputo, definiendo el eje “X” con números y el eje “Y” con letras. (Agregar lo de número de rack y ubicación del servidor dentro del gabinete)

  Los gabinetes ubicados en el área blanca de los centros de datos son de 42RU (unidades de rack), generalmente un servidor ocupa 1RU. Ejemplo: el servidor de un aplicativo se encuentra ubicado F11418 y se acompaña con el nombre que le haya asignado el administrador del servidor, donde:

  F: Ubicación vertical,
  11: Ubicación horizontal,
  4: Número de rack
  18: Ubicación del servidor dentro del gabinete.

  Todo cambio de ubicación, distribución y disposición de los equipos de TI que se encuentran alojados en el área blanca de los centros de datos, se registra en la bitácora de operación del centro de datos y el operador se encarga de informar al administrador del servicio y al administrador técnico del centro de datos para que se realice la actualización en el sistema de archivo el cual se encuentra en medio digital.

- El operador de turno de cada centro de datos es el encargado de monitorear continuamente el correcto funcionamiento de la plataforma de TI instalada en las áreas blancas de los centros de datos, revisando temperatura, humedad relativa, alarmas de UPS, estado de las alarmas de los servidores y equipos de TI. Adicionalmente, a través de la herramienta de monitoreo, debe verificar el acceso, operación y almacenamiento de los aplicativos, bases de datos y la disponibilidad del servicio.

  La temperatura y la humedad relativa son censadas y verificadas continuamente por los equipos de aire acondicionado de precisión que forman parte del sistema de climatización, estas medidas se visualizan en los respectivos paneles de control de cada equipo; adicionalmente se cuenta con termohigrómetros instalados sobre los pasillos fríos del área blanca de los centros de datos para tener un mejor control de la temperatura y la humedad relativa. Los rangos de temperatura y humedad relativa establecidos para el correcto funcionamiento de los equipos alojados en el área de los centros de datos oscilan entre 18°C - 23 °C y la humedad relativa de 45% - 55%, valores de operación para la ciudad de Bogotá, D.C.; este valor depende de la altura sobre el nivel del mar donde se encuentre operando el centro de datos. La cantidad de humedad relativa máxima que puede contener el aire a la altura de Bogotá debe oscilar entre el 40% y 60% para disipar la carga térmica producida por los equipos de TI alojados en el área blanca de los centros de datos Site1 y Site2.

- El centro de datos Site 1 cuenta con una capacidad máxima de cien (100) Toneladas de Refrigeración (100 TR), las cuales están dispuestas en una conexión cíclica que permite que trabajen cincuenta (50) TR y cincuenta (50) TR se encuentren en reposo, dado que la configuración de equipos del centro de datos es de una disipación de cincuenta TR (50 TR). Cada quince (15) días los martes a las 09:00 horas el sistema hace la conmutación y los equipos que se encontraban en reposo comienzan a trabajar y los que estaban trabajando entran en reposo. El sistema está

compuesto por cuatro (4) equipos de aire acondicionado de precisión de 20 TR y dos (2) equipos de aire acondicionado de precisión de diez (10) TR. Se encuentran identificados así:

- Aire Acondicionado No. 1 de 20 TR
- Aire Acondicionado No. 2 de 20 TR
- Aire Acondicionado No. 3 de 20 TR
- Aire Acondicionado No. 4 de 20 TR
- Aire Acondicionado No. 5 de 10 TR
- Aire Acondicionado No. 6 de 10 TR

Los aires acondicionados de precisión impares (1, 3 y 5) conforman un subsistema de 50 TR y los aires acondicionados de precisión pares (2, 4 y 6) conforman el otro subsistema de 50 TR.

- El centro de datos Site2, cuenta con una capacidad máxima de cincuenta y cinco Toneladas de Refrigeración (55 TR), las cuales están dispuestas en una conexión cíclica que permite que treinta (30) TR estén trabajando y veinticinco (25) TR en reposo, dado que la configuración de equipos del centro de datos es de una disipación de treinta (30) TR. Los martes cada quince días a las 09:00 horas el sistema hace la conmutación y los equipos que se encontraban en reposo comienzan a trabajar y los que estaban trabajando entran en reposo. El sistema está compuesto por dos (2) equipos de aire acondicionado de precisión de quince (15) TR, dos (2) equipos de aire acondicionado de precisión de diez (10) TR y un equipo de aire acondicionado de precisión de cinco (5) TR. Se encuentran identificados así:

  - Aire Acondicionado No. 1 de 15 TR
  - Aire Acondicionado No. 2 de 10 TR
  - Aire Acondicionado No. 3 de 15 TR
  - Aire Acondicionado No. 4 de 10 TR
  - Aire Acondicionado No. 5 de 5 TR

  Los aires acondicionados de precisión impares (1 y 3) conforman un subsistema de veinticinco (25) TR, los aires acondicionados de precisión pares (2 y 4) conforman otro subsistema de veinticinco (25) TR y el aire acondicionado No. 5 forma otro subsistema.

  El operador de turno realiza ronda de inspección cada hora y verifica el estado de operación de los equipos de aire acondicionado de precisión y toma un reporte donde registra la temperatura y la humedad relativa observadas, las registra en el formato "*FT-IIT-2714 Bitácora de eventos"* y los manifiesta al operador que recibe en la entrega de turno. Toda anomalía debe ser consignada en el mismo documento.

- Todo incidente que se presenta en el turno debe quedar consignado en el formato "*FT-IIT-2714 Bitácora de eventos*" y reportado directamente al personal técnico y de Ingeniería de la entidad y de las firmas contratistas que dan soporte y mantenimiento a las diferentes plataformas de TI instaladas en los centros de datos de la UAE DIAN. En los casos en que un evento no se resuelve por no ser de su competencia se escala al administrador del servicio correspondiente (Grupo Comunicaciones, Grupo Base de Datos, Grupo Despliegue, Grupo Seguridad, Administrador Técnico Centros de datos, entre otros).

- La gestión de incidentes relacionados con los centros de datos Site1 y Site2, se lleva a cabo a través del sistema gestión de incidentes (ARANDA), gestionando o escalando con los administradores de

los servicios correspondientes. Cuando se requiera una modificación en cualquiera de los equipos de la plataforma de TI alojada en los centros de datos, de acuerdo al diagnóstico realizado producto del reporte de un incidente, ya sea que estos afecten o no la disponibilidad del servicio en los centros de datos, se deberá llevar a cabo el control de cambios diligenciando el formato "*FT-IIT-1877 Solicitud de cambios infraestructura tecnológica*", teniendo en cuenta lo establecido en el procedimiento "*PR-IIT-0457 Gestión de cambios*".

Cuando se requiera dar de baja algún elemento de los centros de datos, ya sea por obsolescencia o por cambio de tecnología, es necesario contar con la información de este para realizar copia de respaldo de la información correspondiente y migración de la misma al equipo nuevo, posteriormente se debe proceder a la destrucción de discos duros y procesadores para entregar el equipo al almacén general.

Se debe informar al administrador del sistema del equipo sobre el cual se efectuarán los cambios para proceder a su desconexión, hacer la destrucción de discos duros y procesadores para después ser retirados del área blanca del centro de datos. Cuando se realice algún cambio en la infraestructura de TI instalada en los centros de datos, se debe registrar en el formato "*FT-IIT-2714 Bitácora de eventos*" para modificar y actualizar los archivos planos de distribución y distribución de servidores cuando aplique.

- Una vez destruidos los discos duros, se reintegran a la Coordinación de Inventarios para la disposición final mediante entrega a la firma contratada por la entidad para tal fin, quien a su vez entregará el certificado de disposición final. Instructivo "*IN-ADF-0139 Reintegro de bienes a bodega*", procedimiento "*PR-ADF-0018 Egreso de bienes muebles*".

- Las rutinas de mantenimiento preventivo de los equipos de TI que conforman la plataforma tecnológica de la Entidad, deben realizarse periódicamente conforme al Anexo "Cronograma mantenimiento de la plataforma tecnológica y parque computacional", el cual debe ser actualizado por la Subdirección de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, mínimo una (1) vez cada seis (6) meses y conforme al vencimiento de los contratos que amparan los mantenimientos o garantías.

4.3 Ingreso a los centros de datos

- Debe enmarcarse en los siguientes escenarios y ser exclusivamente para realizar actividades que tengan que ver con la función de la UAE DIAN y previa autorización:

  a) Ingreso para realizar procedimientos de monitoreo.
  b) Ingreso para realizar procedimientos de mantenimiento y aseo
  c) Ingreso para realizar procedimientos implementación y cambios en la infraestructura
  d) Ingreso para levantamientos de información de terceros o internos

- Igualmente, para el ingreso a los centros de datos está prohibida la entrada bajo las siguientes condiciones:

  a) Porte celulares o equipos de comunicación.
  b) Equipos de cómputo portátiles no indispensables.
  c) Ingreso de llaves, destornilladores, monedas
  d) Porte de armas de fuego, armas blancas o similares
  e) Bajo estado de embriaguez o consumiendo bebidas alcohólicas

f) Bajo el efecto de cualquier droga o sustancia alucinógena
g) Porte de cámaras fotográficas y filmadoras
h) Con vestimenta inapropiada (pantalones cortos, camisas sin mangas, chancletas) o fumando

- Para ingresar a los centros de datos Site1 y Site2 de la entidad, se debe solicitar el ingreso mediante el diligenciamiento y envío vía correo electrónico del formato "*FT-IIT-1880 Solicitud de ingreso al centro de datos*" al Subdirector de Infraestructura Tecnológica y de Operaciones o quien haga sus veces y al Administrador Técnico de los centros de datos. Así mismo, previo al primer ingreso al centro de datos se debe firmar el formato *"FT-IIT-2635 Compromiso de confidencialidad y no divulgación de la información reservada o clasificada".* Por considerarse información clasificada y de seguridad estas solicitudes sólo deben ser registradas en los centros de datos y consignadas en el formato "*FT-IIT-2714 Bitácora de eventos*".

- Los trabajos que se realizan en los centros de datos son de dos tipos: preventivos y correctivos. Cuando se trata de un trabajo preventivo este se hace de manera programada, el personal técnico y de ingeniería de la entidad o del contratista encargado de realizar el trabajo debe diligenciar y enviar el "*FT-IIT-1880 Solicitud de ingreso a los centros de datos*" como mínimo veinticuatro (24) horas antes de la ejecución de los trabajos. Cuando se trata de un trabajo correctivo o imprevisto, se debe diligenciar y enviar el "*FT-IIT-1880 Solicitud de ingreso a los centros de datos*" en lo posible treinta minutos (30) antes de la ejecución de los trabajos.

  Al momento del ingreso al centro de datos, el personal autorizado (técnico y de ingeniería de la entidad y de los contratistas que prestan el servicio de mantenimiento a la plataforma de TI instalada en los centros de datos de la UAE DIAN), debe conocer el acuerdo de confidencialidad que reposa en el puesto del vigilante al ingreso de cada centro de datos; con la lectura del acuerdo se da por hecho que el personal autorizado conoce y está de acuerdo con lo consignado y por ende se considera firmado por él.

- El Subdirector de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, o el Administrador Técnico de los Centros de datos, deberá llevar a cabo las siguientes tareas:

  a) Verificación de los datos de las personas que van a ingresar
  b) Verificación de las tareas que se van a realizar
  c) Asignación de los recursos necesarios para llevar a cabo la actividad
  d) Notificar la autorización a través de correo electrónico o medio físico a los operadores de los centros de datos
  e) Firmar el formato "*FT-IIT-1880 Solicitud de Ingreso a los centros de datos*" para dar autorización.

  El operador de turno de cada centro de datos debe guardar copia física de la autorización y registrarla en el formato *"FT-IIT-1878 Control de ingreso a los centros de datos – Operadores*". Igualmente debe informar al guardia de seguridad privada los nombres de las personas que están autorizadas para ingresar al Centro de datos y solicitarle su registro en el "*FT-IIT-1879 Control de ingreso a los centros de datos – vigilantes*". El operador solicitará a los funcionarios autorizados el diligenciamiento de los formatos y dará a conocer el acuerdo de confidencialidad al momento de ingresar.

- Para el desarrollo de las actividades que aseguren la alta disponibilidad y máxima seguridad de la información, infraestructura y hardware de los centros de datos, se requiere del ingreso permanente de personal técnico y de Ingeniería de la entidad y de las firmas contratistas que dan soporte y

mantenimiento a las diferentes plataformas de TI instaladas en los centros de datos de la UAE DIAN, se debe diligenciar el formato "*FT-IIT-1878 Control de ingreso a los centros de datos – Operadores*". y "*FT-IIT-1879 Control de ingreso a los centros de datos – vigilantes*". En estos casos se deben tener en cuenta las siguientes consideraciones:

a) Autorización por parte del Subdirector de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, o el Administrador Técnico de los Centros de datos; dicha autorización debe ser de conocimiento de todos los operadores de los centros de datos y deben tener un listado de personas autorizadas permanentemente.
b) El listado, de personal preautorizado o con ingreso permanente a los centros de datos de la entidad debe ser un documento formal el cual se renueva mensualmente y es tramitado por el Subdirector de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, o el Administrador técnico de los centros de datos y debe contener la información que permita identificar al personal autorizado para el ingreso permanente.
c) Cuando se requiera autorizar el retiro de equipos, elementos o accesorios de los centros de datos estos deben llevar el visto bueno del Subdirector de Infraestructura Tecnológica y de Operaciones o quien haga sus veces, o el Administrador Técnico de los Centros de datos, se debe tramitar el formato "*FT-FI-1557 – Orden Salida de Elementos"* el cual debe ir firmado por el Subdirector de Infraestructura Tecnológica y de Operaciones o por quien tenga la firma autorizada para permitir la salida de elementos.
d) El ingreso de personal preautorizado o permanente a los centros de datos será en el horario de 7*24*365 (las veinte cuatro (24) horas del día, los siete (7) días de la semana, los trescientos sesenta y cinco (365) días del año), según sea el caso.

5. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de Cambios	Tipo de información
	Desde	Hasta		
1	21/09/2022	14/11/2022	Versión inicial. Se deroga el procedimiento PR-SI-0134 Administración del Centro de datos. Se deroga el Instructivo IN-SI-0010 Seguridad al ingreso en el centro de datos.	No aplica
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:	Miguel Arturo Cuesta Buitrago **Elaboración Técnica**	Gestor III	Subdirección de Infraestructura Tecnológica y de Operaciones
	Said Alfonso García Salazar **Elaboración Técnica**	Inspector I	Subdirección de Infraestructura Tecnológica y de Operaciones
	Diego Mauricio Calderón Pérez **Elaboración Técnica**	Inspector II	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 Murcia **Elaboración metodológica**	Gestor II	Coordinación de procesos y riesgos operacionales
	Alfredo Antonio Ahumada Ahumada **Elaboración metodológica**	Gestor II	Coordinación de procesos y riesgos operacionales
Revisó:	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