PLAN DE RECUPERACIÓN ANTE DESASTRES

(APLICACIONES OPERATIVAS)

Agencia Nacional de Tierras

AGENCIA NACIONAL DE TIERRAS

SECRETARÍA GENERAL

Equipo de Infraestructura y Soporte Tecnológico

OCTUBRE DE 2021

TABLA DE CONTENIDO

LISTA DE TABLAS

1 INTRODUCCIÓN

Todas las organizaciones o entidades independiente de su naturaleza, función, rol o core de negocio deben preocuparse por mantener de manera constante e ininterrumpida la prestación de sus productos y/o servicios. La Agencia Nacional de Tierras ha establecido su Misión "*Como máxima autoridad de tierras, consolidar y mantener el ordenamiento social de la propiedad rural, para mejorar las condiciones de vida de la población*" y por lo tanto debe garantizar una serie de componentes transversales basados en estudios, procesos, procedimientos, infraestructura física y tecnológica, recurso humano y presupuesto que respalden la gestión de los sistemas de información y facilite oportunidad y eficiencia en la operación diaria de la entidad.

Actualmente la ANT no cuenta con un proceso estructurado, sistemático, medible y repetible que permita reaccionar ante las innumerables y significativas amenazas que pueden materializarse afectando la operación y el normal funcionamiento de la entidad y que pueda recuperarse en el menor tiempo posible para responder organizadamente a eventos que interrumpen la normal operación de sus procesos y que pueden generar impactos sensibles en el logro de los objetivos estratégicos institucionales.

Por lo tanto, la ANT debe prepararse para enfrentar la posibilidad de la ocurrencia de un evento, incidente o desastre que afecte la operación y establecer los mecanismos y recursos para recuperarse en el menor tiempo posible garantizando la prestación de los servicios primordiales institucionales, es por esto, que el plan de recuperación ante desastres (DRP) es una herramienta orientada a la mitigación de los riesgos para el desarrollo normal de las operaciones y detalla una serie de actividades de control y prevención ante posibles emergencias, administración de crisis, planes de contingencia y capacidad de retorno a la operación normal.

2 SIGLAS Y DEFINICIONES

- ✓ **Análisis de Impacto en el negocio (BIA- Business Impact Analisys):** Documento para estimar la afectación que puede padecer una empresa como resultado de la ocurrencia de algún incidente o un desastre.

- ✓ **DDoS - Ataque de denegación distribuida de servicio**: Este tipo de ataque aprovecha los límites de capacidad específicos que se aplican a cualquier recurso de red, tal como la infraestructura que habilita el sitio web de la empresa. El ataque DDoS envía varias solicitudes al recurso web atacado, con la intención de desbordar la capacidad del sitio web para administrar varias solicitudes y de evitar que este funcione correctamente.

- ✓ **DNS sistema de nombres de dominio**: Es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominio asignados a cada uno de los participantes.

- ✓ **Emergencia:** Asunto o situación imprevistos que requieren una especial atención y deben solucionarse lo antes posible

- ✓ **Interrupción**: Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

- ✓ **LDF - Log Database Files** (Archivos de registros de bases de datos): Es un archivo de base de datos de Microsoft SQL Server, que almacena todos los registros de transacciones / eventos, que se ejecuta en la base de datos. El propósito principal del uso de archivo de registro en SQL Server es revertir la base de datos en caso de pérdida de datos.

- ✓ **Manejo de crisis:** El proceso mediante el cual una organización enfrenta un acontecimiento de importancia que podría generar daño a la organización, sus stakeholders, o al público en general.

- ✓ **MDF - Master Database Files (**Archivo maestro de bases de datos): contiene las filas, columnas, campos y datos creados por una aplicación o usuario. La creación de una columna de base de datos, las modificaciones e información de la creación de los registros, todo está almacenado en este archivo para el uso las aplicaciones y de búsquedas.

- ✓ **NetBIOS - Network Basic Input/Output System**: Es una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.

- ✓ **Nivel de Criticidad.** Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.

- ✓ **Plan de continuidad de negocio (BCP - Business continuity Plan):** Es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre

- ✓ **Plan de Recuperación ante desastres (DRP**): Plan claramente definido y documentado el cual permite recuperar las capacidades de tecnología cuando se presenta una interrupción.

- ✓ **Plataforma tecnológica crítica**: Entiéndase como el conjunto de elementos compuestos por los sistemas de información core del negocio, servidores, bases de datos, medios de almacenamiento, equipos, redes y comunicaciones que son críticos para la prestación de los servicios de la Agencia.

- ✓ **Riesgo:** Es la combinación de la probabilidad de que algo suceda y las consecuencias que puedan tener. efecto de la incertidumbre sobre la consecución de los objetivos

- ✓ **RPO - Recovery Point Objective**: Es la cantidad de datos que una empresa puede permitirse perder y aun así seguir funcionando si sufre un tiempo de inactividad ("downtime").

- ✓ **RTO - Recovery Time Objective:** Describe el intervalo de tiempo que puede pasar antes de que la interrupción comience a impedir las operaciones normales del negocio (continuidad de negocio).

3 NORMATIVIDAD APLICABLE

- ✓ Norma ISO/IEC 22301:2012 Sistema de Gestión de Continuidad de Negocio.
- ✓ Norma NTC-ISO/IEC 27001:2013 Sistema de Gestión de Seguridad de la Información.

4 REVISIÓN Y ACTUALIZACIÓN

Es responsabilidad del Líder de Infraestructura y Soporte Tecnológico acatar las sugerencias realizadas por los responsables de la implementación de este plan una vez se hayan ejecutado actividades de pruebas donde se pueden evidenciar oportunidad de mejora que fortalezcan su aplicabilidad ante un evento. Los ajustes se realizarán una vez al año o cuando se considere necesario debido a cambios en la normatividad, modo de ejecución de las actividades operativas de la agencia, cambios en la plataforma tecnológica y cambio de responsables, entre otros.

5 PLAN DE RECUPERACIÓN ANTE DESASTRES

5.1 Objetivo General

Establecer las actividades necesarias que permitan mantener la continuidad de los servicios críticos establecidos en la plataforma tecnológica de la ANT en caso de la ocurrencia de una catástrofe, desastre, evento, contingencia o interrupción mayor.

5.2 Objetivos Específicos

1. Contar con los lineamientos establecidos para la activación del DRP de acuerdo con los riesgos potenciales que puedan ocasionar interrupción en la operación de los servicios críticos de la entidad.
2. Regresar a un estado operativo normal después de la interrupción del servicios y aplicaciones de las actividades detalladas en este plan.
3. Minimizar el impacto de los posibles riesgos materializados.
4. Identificar los recursos críticos de la infraestructura tecnológica con sus riesgos asociados.
5. Determinar el RTO (Recovery Time Objective) y el RPO (Recovery Point Objective)
6. Establecer los roles y responsabilidades para la gestión de la plataforma tecnológica.
7. Realizar simulacros tendientes a probar los planes de recuperación y ajustarlos si es necesario.
8. Concienciar a funcionarios, contratistas y colaboradores en los planes adoptados para la recuperación ante cualquier desastre.

5.3 Alcance

Este plan aplica para la plataforma crítica tecnológica de la Agencia Nacional de Tierras y los sistemas de información que se describen a continuación:

COMPONENTE	SERVICIO ASOCIADO	RTO	RPO
Aplicaciones y bases de datos	Orfeo	4 horas	2 horas
	Klic	4 horas	2 horas
	PAABS	4 horas	2 horas
	Ulises	4 horas	2 horas

COMPONENTE	SERVICIO ASOCIADO	RTO	RPO
Infraestructura	Centro de Atención y Servicios CAS	4 horas	2 horas
	Directorio Activo	4 horas	2 horas
	DNS	4 horas	2 horas
	DHCP	4 horas	2 horas
	Servidores	4 horas	2 horas

Tabla 1. Alcance DRP

El RPO y RTO se establece acorde con la experiencia de los especialistas que administran la infraestructura tecnológica y aplicaciones operativas, sin embargo, este plan será verificado una vez se realicen las pruebas correspondientes.

5.4 Supuestos

El plan de recuperación ante desastre (DRP) detallado en este documento está orientado en garantizar la protección y estabilidad de la plataforma tecnológica y las aplicaciones operativas de la Agencia para reanudar las operaciones cuando sea necesario, por lo tanto, se identifican los siguientes **supuestos** frente a la ocurrencia de un evento catastrófico, desastre, contingencia o interrupción mayor:

- ✓ Se tiene el apoyo de la dirección General, Secretaría General y las áreas impactadas.
- ✓ Se cuenta con los recursos financieros en caso requerido.
- ✓ Se han realizado mínimo una vez por año, los ejercicios de reconocimiento e implementación de este plan.
- ✓ Los funcionarios, contratistas o colaboradores que hacen parte de los roles y perfiles detallados en este plan, se encuentran disponibles para apoyar la situación presentada.
- ✓ Los servicios, aplicaciones y bases de datos instalados en Azure se encuentran disponibles y actualizados.
- ✓ Las copias restauradas se encuentran validadas y funcionan correctamente.
- ✓ Se han aplicado los controles a los riesgos identificados en la plataforma crítica tecnológica.
- ✓ Se identificaron los recursos críticos de la infraestructura tecnológica, los riesgos asociados y sus controles.
- ✓ Se realizaron capacitaciones y socializaciones a funcionarios, contratistas y colaboradores de la ANT sobre los planes adoptados ante la recuperación de un desastre.

5.5 Escenarios previstos

Dentro de este plan como escenarios previstos se contempla que por alguna situación crítica no se pueda acceder a los servicios de tecnologías de la información, instalaciones físicas del centro de cómputo y/o sedes de la entidad por un período de tiempo indeterminado identificando las siguientes situaciones, eventos o incidentes que ocasionan indisponibilidad:

a) Bases de datos:

- ✓ Accidente humano: borrado de datos, actualizaciones indebidas, formateo accidental de particiones, robo de datos, restauraciones defectuosas de información, no generación de backups, abuso de privilegios, elevación de privilegios no autorizados y autenticación débil.
- ✓ Auditoría débil.
- ✓ Vulnerabilidad de la plataforma y protocolos de las bases de datos.
- ✓ Fallas o daño de los componentes del almacenamiento.
- ✓ Falta de capacidad de almacenamiento.
- ✓ Denegación de servicio.
- ✓ Inyección de SQL.
- ✓ Datos sensibles sin cifrar.
- ✓ Desactualización del motor de bases de datos.
- ✓ Estados anómalos de la base de datos.

b) Almacenamiento y respaldo de la información

- ✓ Robo de cintas o backups de bases de datos.
- ✓ Daños físicos de los medios de almacenamiento.
- ✓ Herramienta de backups desactualizada o defectuosa.
- ✓ Restauraciones de backups sin seguimiento ni validaciones.
- ✓ Daños físicos y lógicos.
- ✓ Datos sobrescritos en la LUN´s del almacenamiento.
- ✓ Particiones y sistemas de archivos corruptos.
- ✓ Almacenamiento de cintas y backups de información internos.

c) Servidores:

- ✓ Accidentes humanos: mantenimiento inadecuado de máquinas, no actualizaciones del software, extracción no autorizada y controlada de dispositivos, accesos no autorizados.

- ✓ Ataque distribuido de denegación del servicio (DDoS).
- ✓ Infecciones de virus.
- ✓ Espacio insuficiente en almacenamiento.
- ✓ Problemas de red.
- ✓ Problemas de hardware en el Enclosure.
- ✓ Fallas eléctricas

d) Centro de cómputo:

- ✓ Desastres naturales: inundación, incendio, rayo o terremoto.
- ✓ Vandalismo: destrucción ocasionada por terceros en eventos de protestas.
- ✓ Fallas del suministro eléctrico.
- ✓ Daño del sistema de refrigeración.
- ✓ Obsolescencia de los equipos.
- ✓ Accidente aéreo.

e) Redes y comunicaciones:

- ✓ Ataque de denegación de servicio.
- ✓ Infección de virus, malware o ransonware.
- ✓ Fallas en los switches o routers.
- ✓ Conexión errónea de equipos.
- ✓ Daño de hardware o de software.

Es de anotar que la ANT cuenta con diversas sedes a nivel nacional, sin embargo, el centro de datos se encuentra ubicado en la sede principal Calle 43 No. 57-41 en Bogotá y, por tanto, es la única sede que respaldas las operaciones tecnológicas on premise. En caso de cualquier eventualidad mayor con el centro de datos, la contingencia se aplicará sobre la infraestructura Azure para aquellos servicios de misión crítica.

f) No ingreso del recurso humano a las instalaciones:

Debido a eventos como inundaciones, incendio, terremoto, vandalismo, paros o pandemia, los profesionales, contratistas o colaboradores de la ANT no puedan acceder a las instalaciones de alguna de las sedes, se hará uso del trabajo remoto accediendo a través de una conexión VPN de los aplicativos webs o de la plataforma Cloud Microsoft 365. Adicionalmente se podrá contemplar la posibilidad de reubicar algunas personas dentro de otras sedes alternas que permitan ejecutar funciones primordiales que así de demande.

Nota 1: para aquellas situaciones no contempladas anteriormente podrán incluirse al momento de su presentación previa validación de su remediación haciendo uso de la infraestructura Cloud que soporta este DRP.

5.6 Estrategia prevista

Teniendo en cuenta cada uno de los escenarios mencionados en el numeral 4.5 de este documento es necesario establecer una estrategia orientada a la mitigación de los eventos presentados y la recuperación de los servicios de la Agencia para lo cual se considera:

1. **Evento informático:** el funcionario, contratista o colaborador que identifique el evento deberá comunicar a través de la mesa de servicios de TI cuando:
    a. No haya servicio de correo electrónico
    b. No haya internet
    c. No pueden acceder a las plataformas tecnológicas o sistemas de información internos.
    d. No puedan acceder a las carpetas compartidas.
    e. Pérdida de información en el file server.
    f. Almacenamiento no contenga espacio.

2. **Evento de la naturaleza, vandalismo, paros otros:** el personal de vigilancia, servicios generales que identifique el evento deberá comunicar a su superior y/o al líder de Infraestructura y Soporte Tecnológico cuando:
    a. Inundación del centro de datos o cualquier piso.
    b. Destrucción parcial o total del centro de datos por causas vandálicas o terremoto.
    c. Sustracción de equipos de personas no autorizadas.
    d. Incendio del centro de datos o cualquier piso.
    e. Presentación de humedades o goteras en el centro de datos.
    f. Cualquier otro evento que afecte el centro de datos no contemplado en este numeral.

3. **Atención de incidentes, evento, contingencia o interrupción mayor:** los especialistas de la mesa de servicios de TI, deberán atender los incidentes reportados por los usuarios acorde con el numeral 7.3 Gestión de Incidentes Tecnológicos que hace parte del Instructivo de Buenas prácticas en ITIL para la Gestión de la mesa de servicios de TI GINFO-I-005, mediante el cual se evalúa, categoriza, prioriza e investiga el incidente para posteriormente solucionarlo o si es necesario escalarlo.

4. **Activar la contingencia:** el Líder de Infraestructura y Soporte Tecnológico valida si el evento afectó el centro de datos o algún sistema de información crítico y su solución tarda más de 4 horas procede a activar el centro de cómputo alterno en Azure previa validación y autorización por parte del Secretario General.

5. **Recuperar la plataforma, sistema de información o base de datos en Azure**: el Líder de Infraestructura y Soporte Tecnológico debe:

a. Notificar al Secretario General la activación del Centro de cómputo alterno.
b. Disponer del recurso humano necesario para apoyar las actividades.
c. Comunicar al proveedor de internet para reapuntar los servicios al centro de datos alterno.
d. Verificar la disponibilidad de los servicios que respaldan el DRP en Azure.
e. Validar la información en Azure y si es necesario replicar los datos requeridos.
f. Activar el servicio de bases de datos y aplicaciones en caso requerido.

6. **Comunicar el incidente, evento, contingencia o interrupción mayor:** el Líder de Infraestructura y Soporte Tecnológico en conjunto con el Secretario General definen si amerita notificar a la Dirección General el incidente sucedido para la ejecución de actividades para el manejo de crisis. Si el evento es de seguridad de la información debe tratarse como se menciona en el procedimiento Gestión de Incidentes de Seguridad de la Información de la entidad.

7. **Activar la estrategia al interior de la Agencia:** el Líder de Infraestructura y Soporte Tecnológico debe garantizar que los servicios activados en Azure estén disponibles para toda la comunidad, para lo cual debe ejecutar las siguientes actividades:
   a. Validación de alta disponibilidad de Azure.
   b. Validación de acceso a los sistemas de información, bases de datos y carpetas compartidas.
   c. Validación de la información almacenada en los repositorios de información.
   d. Si el evento impactó la seguridad de la información:
      i. Eliminar las causas del incidente.
      ii. Mejorar los esquemas de seguridad y protección actuales tanto a nivel de hardware como de software en caso necesario.
      iii. Fortalecer la seguridad de los equipos involucrados.
      iv. Poner en alerta a la comunidad.
   e. Si el evento impactó las redes y comunicaciones:
      i. Validar los servicios de red.
      ii. Validar los equipos de seguridad.
      iii. Escalar al proveedor en caso de fallas no solucionables por especialista de la ANT.
   f. Si el evento afectó la infraestructura de servidores:
      i. Validar recursos de hardware y ejecutar la acción necesaria.
      ii. Validar los servidores físicos y virtuales, almacenamiento y demás componentes que hacen parte del data center.
      iii. Validar daños en el almacenamiento.
      iv. Validar el funcionamiento de la red SAN.
      v. Revisar los backups de las máquinas virtuales.
      vi. Configurar un servidor de contingencia y restaurar la información.
   g. Si el evento afectó las bases de datos:

i. Restauración copia de seguridad en caso de pérdida o borrado de datos.
ii. Ejecutar los scripts de estructuras de las bases de datos.
iii. Truncar y reducir el registro de transacciones de bases de datos.
iv. Ampliar los recursos de almacenamiento o presentación de un nuevo disco.
v. Migrar los archivos MDF y LDF a un disco con mayor espacio.
vi. Revisar los archivos de metadata y log data.
vii. Activar la contingencia sobre Azure.

h. Si el evento afecto el almacenamiento y respaldo:
   i. Si la SAN Falla se escala al proveedor.
   ii. Activar la contingencia en Azure.

8. **Comunicar la solución**: el Líder de Infraestructura y Soporte Tecnológico debe notificar la solución a la comunidad ANT a través de correo electrónico.

9. **Retorno a la normalidad**: el Líder de Infraestructura y Soporte Tecnológico junto con el Secretario General y profesionales involucrados en resolver el incidente, deciden la fecha de retorno a la normalidad y bajo las consideraciones necesarias que garanticen la recuperación del hardware y software intervenido en el evento.

10. **Documentar el incidente, evento, contingencia o interrupción mayor:** las personas que intervinieron en el incidente deberán participar en la construcción del documento de oportunidades de mejora que deberán ser incluidas en el DRP en caso requerido, de lo contrario se tendrá en cuenta como lecciones aprendidas.

11. **Cierre del incidente, evento, contingencia o interrupción mayor:** el Líder de Infraestructura y Soporte Tecnológico, a través de la mesa de servicios de TI, realiza el cierre del caso y documenta las acciones preventivas y correctivas.

Nota 2: en caso de ser necesario el Líder de Infraestructura y Soporte Tecnológico previa aprobación por el Secretario General, deberá contratar los servicios o bienes que permitan solucionar el incidente para el regreso de la prestación de los servicios normales al punto original.

5.7 Árbol de llamadas y comunicaciones

5.7.1 Comunicación interna

Para la activación de este plan (DRP) frente a una catástrofe, desastre, evento, contingencia o interrupción mayor, se debe comunicar con las personas que ocupan los cargos mencionados en la siguiente matriz antes durante y después de la presentación del evento:

Rol/Cargo	Dependencia
Líder Equipo de Infraestructura y Soporte Tecnológico	Secretaría General
Secretario General	Secretaría General
Director(a) General	Dirección General
Oficial de seguridad	Subdirección de Sistemas de Información de Tierras
Responsable de redes y comunicaciones	Secretaría General
Responsable de Bases de datos	Secretaría General

Tabla 2. Árbol de llamadas

Nota 3: esta matriz aplica también para la realización de pruebas del DRP.

5.7.2 Comunicación externa

En caso de que el evento requiera comunicarse externamente para soportar la solución del incidente, se relacionan los siguientes datos:

Empresa	Teléfono
Emergencias generales	123
Empresa de Acueducto y alcantarillado	116
Gas natural	164
Codensa	115
Bomberos	119
Policía de transito	127
Policía nacional	911
Dijin	157
Defensa civil	144
CAI la Esmeralda	2222673

Tabla 3. Directorio Empresas Extrenas

5.7.2.1 Para evento de seguridad de la información

En dado caso que el incidente sea identificado como de seguridad de la información, deberá seguir los lineamientos mencionados en el procedimiento gestión de incidentes de seguridad de la información de la Agencia.

A continuación, se relaciona las empresas del gobierno para el reporte de incidentes de seguridad de la información según sea el caso:

Empresa	Teléfono	Otro medio de comunicación
COLCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia)	(+571) 2959897 Opción 1	http://www.colcert.gov.co/?q=contenido/reportar-un-incidente. contacto@colcert.gov.co Si es un phishing: phishing-report@colcert.gov.co
CCIRT GOBIERNO	(+571) 390 79 50 018000-910742 opc.2	csirtgob@mintic.gov.co Coordinador CSIRT: Email Andrés Mena Palacios emena@mintic.gov.co https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/
Policía Nacional	(571)5159090/ 5159586	ponal.csirt@policia.gov.co https://cc-csirt.policia.gov.co www.policia.gov.co
Delitos informáticos	018000-910112	https://adenunciar.policia.gov.co/adenunciar/Login.aspx?ReturnUrl=%2fadenunciar%2f

Tabla 4. Directorio Entidades del Gobierno

5.8 Roles y responsabilidades del DRP

Los roles y responsabilidades que se definen a continuación deberán ser tenidos en cuenta antes, durante y después del evento de la interrupción:

ROL	RESPONSABILIDADES		
	ANTES	DURANTE	DESPUÉS
Líder de Infraestructura y Soporte Tecnológico	▪ Mantener actualizado el DRP. ▪ Realizar pruebas de implementación del DRP con el recurso requerido. ▪ Activar el plan del DRP cuando se considere necesario previa aprobación del Secretario General. ▪ Informar las actualizaciones del DRP, roles y responsabilidades. ▪ Comunicar la contingencia.	▪ Notificar al Secretario General el evento sucedido. ▪ Identificar y evaluar el evento y/o desastre presentado. ▪ Evaluar las posibles soluciones, esto incluye la contratación de recursos externos. ▪ Activar la plataforma Azure para la Contingencia en caso de ser necesario. ▪ Ejecutar el DRP.	▪ Informar al Secretario General la recuperación de la operación y el retorno normal de las actividades. ▪ Aplicar las oportunidades de mejora identificadas en durante la implementación del DRP. ▪ Actualizar el DRP con las oportunidades de mejora identificadas

ROL	RESPONSABILIDADES		
	ANTES	DURANTE	DESPUÉS
	▪ Validar las necesidades tecnológicas para la implementación de un DRP. ▪ Disponer de la plataforma tecnológica, recursos de hardware y software necesarios para la implementación del DRP. ▪ Coordinar y apoyar la realización pruebas del DRP. ▪ Mantener actualizados los componentes y servicios ofrecidos en Azure. ▪ Velar porque el hardware y software se encuentre en óptimas condiciones. ▪ Monitorear contantemente la infraestructura tecnológica en búsqueda de eventos anómalos para corregirlos.	▪ Comunicar a los roles el evento sucedido. ▪ Solicitar la remediación al rol responsable del evento sucedido. ▪ Hacer seguimiento de la remediación o corrección aplicada. ▪ Liderar las actividades necesarias para el retorno de la operación.	por los roles durante la presentación del evento.
Oficial de Seguridad	▪ Documentar los procedimientos y formatos asociados a seguridad de la información. ▪ Participar en la búsqueda de soluciones y realización de pruebas del DRP. ▪ Sugerir actualizaciones al DRP.	▪ Seguir los lineamientos mencionados en el procedimiento de seguridad de la información. ▪ Analizar el incidente presentado. ▪ Notificar a entes de control externo y del gobierno el evento sucedido. ▪ Mantener informado al líder de Infraestructura y Soporte Tecnológico. ▪ Documentar los hechos, soluciones e impacto del evento.	▪ Resguardar la documentación generada a partir del evento y de acuerdo con lo establecido en el procedimiento de incidentes de seguridad de la información. ▪ Analizar y socializar las lecciones aprendidas. ▪ Recomendar actualizaciones del DRP acorde con las lecciones aprendidas y oportunidades de mejora identificadas.
Líder de redes y comunicaciones	▪ Mantener actualizada las seguridades de hardware y software.	▪ Iniciar el DRP sobre Azure. ▪ Ejecutar el plan de despliegue en Azure. ▪ Iniciar el cargue de máquinas sobre Azure.	▪ Reportar los inconvenientes y oportunidades de mejora identificadas. ▪ Desactivar el DRP

ROL	RESPONSABILIDADES		
	ANTES	DURANTE	DESPUÉS
Responsable de bases de datos	▪ Disponer del recurso humano para la creación, seguimiento y control de copias de seguridad de la información. ▪ Garantizar la restauración aleatoria de copias de seguridad para confirmar su validez. ▪ Actualizar los motores de bases de datos y parches de seguridad. ▪ Validar que los usuarios no posean permisos sysadmin sobre las bases de datos y si lo tienen documentar la razón. ▪ Establecer planes de mantenimiento de bases de datos. ▪ Establecer procesos de auditoría de bases de datos. ▪ Gestionar el crecimiento de las bases de datos.	▪ Monitoreo de bases de datos. ▪ Restauración de backups en caso necesario. ▪ Reestablecer el servicio. ▪ Validar accesos a usuarios y respuestas a peticiones de información. ▪ Validar la integración de aplicaciones y servicios.	▪ Aplicar las oportunidades de mejora identificadas en durante la implementación del DRP.
Responsable mesa de servicios de TI	▪ Participar activamente en las pruebas de ejecución del DRP. ▪ Documentar las inconsistencias encontradas.	▪ Informar el evento a los usuarios de la comunidad ANT. ▪ Presentar un canal de comunicación único para atender cualquier inquietud sobre el evento. ▪ Comunicar al Líder de Infraestructura y Soporte Tecnológico las situaciones adversas que se presenten con el usuario frente al incidente.	Aplicar las oportunidades de mejora identificadas en durante la implementación del DRP.

Tabla 5. Roles y Responsabilidades

6 MANEJO DE CRISIS

Ante la presentación de una ocurrencia catastrófica, desastre, evento, contingencia o interrupción mayor, requiere planeación, organización y control de las actividades que se deben ejecutar a fin de reducir el riesgo reputacional, pérdida de recursos y de la imagen institucional.

A continuación, se presentan las actividades para tener en cuenta:

Responsable de informar	Aspectos generales	Informa a
Líder del equipo de Infraestructura y Soporte Tecnológico	▪ Tipo de evento ▪ Servicios afectados ▪ Acciones para realizar ▪ Tiempo estimado para la normalización ▪ Riesgos contemplados y mitigación.	Dirección General y Secretaría General.
Dirección General y Secretaría General	▪ Comunicar la situación presentada. ▪ Validar y gestionar los recursos necesarios.	Delegados (funcionarios, contratistas o colaboradores) de la ANT.
Delegados (funcionarios, contratistas o colaboradores) de la ANT	▪ Evaluar el impacto que puede tener para la imagen y reputación de la entidad. ▪ Validar la información a comunicar interna y externamente. ▪ Revisar qué información está pendiente por validarse antes de emitir cualquier comunicación. ▪ Validar quiénes son los afectados. ▪ Mantener informado al usuario interno y externo permanentemente. ▪ Comunicar en un lenguaje claro para generar confianza. ▪ Realizar monitoreo de medios para su pronunciamiento. ▪ Análisis del impacto de la información que circula en medios de comunicación, interno y externo a la entidad.	▪ Usuarios internos y externos. ▪ Medios de comunicación. ▪ Entidades gubernamentales ▪ Terceros que tengan relación con la Agencia.

Tabla 6. Actividades para el manejo de crisis

Se recomienda conformar un equipo para el manejo de crisis el cual debe estar integrado por personas de las diferentes oficinas de la ANT que tengan poder de decisión, manejo de medios de comunicación, manejo jurídico y conocimiento de la agencia. Este equipo debe reunirse una vez al año para validar si los integrantes continúan en la entidad o si deben reemplazarse. Igualmente deben revisar las responsabilidades y si es necesario se hacen los ajustes correspondientes.

7 PRUEBAS DEL DRP

Se establece que la realización de las pruebas para este DRP debe ser mínimo una vez al año donde se incluyan a todos los responsables designados para validar la ejecución de actividades aquí planteadas, oportunidades de mejora y ajustes a este plan.

8 ANEXOS

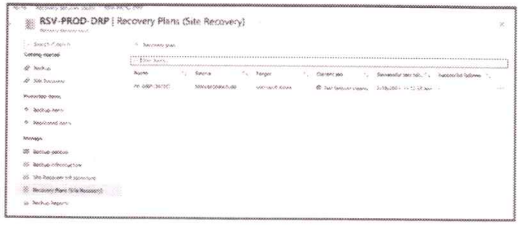
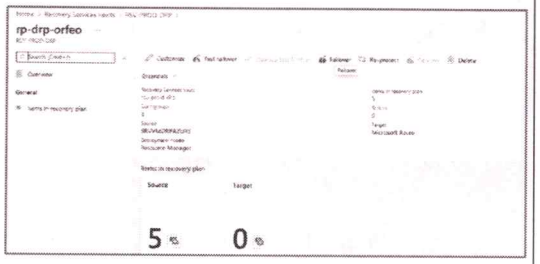
- **ANEXO 1: PASOS PARA ACTIVAR DRP.**
- **ANEXO 2: ARQUITECTURA DEL CENTRO DE DATOS**
- **ANEXO 3: MANUAL DE SINCRONIZACIÓN DE DATOS PARA ORFEO**
- **ANEXO 4: MANUAL DE RESERVA DE RADICADOS DE ORFEO EN AZURE**

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
22/10/2021	01	Primera versión del documento.

Elaboró: Alexandra Ruiz Bedoya	**Revisó:** Fabián Augusto Patarroyo Morales	**Aprobó:** Raúl Alberto Badillo Espitia
Cargo: Contratista - Secretaría General	**Cargo:** Contratista - Secretaría General	**Cargo**: Secretario General
Firma:	**Firma:**	**Firma:**

ANEXO 1: PASOS PARA ACTIVAR DRP

RESPONSABLE	ACTIVIDADES PREVISTAS	RESULTADO ESPERADO	DURACIÓN DE LA ACTIVIDAD MINUTOS	OBSERVACIONES
Líder de Infraestructura y Soporte Tecnológico	Notificar al Secretario General el evento sucedido	Comunicación efectiva	15	La notificación puede ser telefónica o de manera presencial
Líder de Infraestructura y Soporte Tecnológico	Pedir aprobación al Secretario General para activación del DRP	Aprobación otorgada		
Líder de Infraestructura y Soporte Tecnológico	Comunicar el evento a los roles del DRP y miembros de la comunidad	Colaboradores enterados del Incidente Incidente radicado en la mesa de servicios de TI	15	La notificación puede ser telefónica o de manera presencial
Líder de Infraestructura y Soporte Tecnológico	Contar con el apoyo de los especialistas de infraestructura	Especialistas disponibles para apoyar el incidente		
Administrador de Infraestructura	Ingresar al portal Azure (Autenticación)	Ingreso realizado exitosamente.	2	
Administrador de Infraestructura	Seleccionar el plan de Recuperación a Activar 	Plataforma Azure disponible. Plan de recuperación seleccionado y activado en Azure.	2	

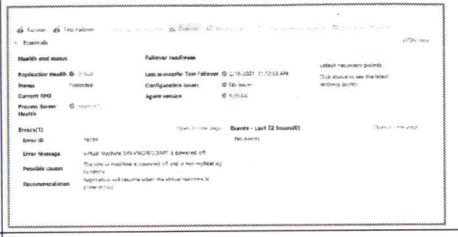
Administrador de Infraestructura	Ingresar al plan de despliegue del DRP y desplegar el Failover  	Despliegue del plan ejecutado sin contratiempos Provisión de los recursos solicitados	2	
Administrador de Infraestructura	Aprovisionar los recursos de cómputo para el DRP	Las máquinas se creen correctamente Validación el funcionamiento de los servicios	120	
Líder de desarrollo	Validación de funcionalidad de los servicios en azure	Acceso probado y validado	5	

DBA	Reservar consecutivos por tipo de radicado en caso necesario: 1. Ejecutar los pasos mencionados en el anexo 3 Manual de sincronización de datos Orfeo y 4 **Manual de reserva de radicados de orefo en Azure.**	Consecutivos reservados por tipo	30	Para el caso de Orfeo y de acuerdo con análisis previamente realizado, se deben reservar en azure algunos consecutivos de radicados de orfeo ya que los datos en azure se están actualizando cada 30 minutos y entre la caída de servidor en on premise y la última actualización de azure pueden existir diferencias entre radicados, es decir, que en azure no están todos los radicados que pudo tener el servidor on premise. Las estadísticas fueron generadas con base en el análisis de radicación del año 2020. Estos radicados se reservan con el fin de restaurar la información cuando se regrese a la normalidad: TIPO DE RADICADO / Promedio Mensual / Promedio Día (calculado sobre 20 días / Promedio Hora / Promedio 30 minutos SALIDA 11.842 592 74 37 ENTRADA 8.498 424 53 27 INTERNA 2.683 134 17 8 RESOLUCIONES 82 4 1 0 PLANILLAS 30 1 0 0 CERTIFICADOS - EDICTOS 19 1 0 0 AUTOS - ACTOS 14 1 0 0 23.159 1.158 145 72
Líder de Infraestructura y Soporte Tecnológico	El registro tipo A se debe reapuntar al cname de Azure	Servicio reapuntado correctamente	30	

Líder de Infraestructura y Soporte Tecnológico	Notificar a los usuarios la activación del servicio a través de correo electrónico	Usuarios Informados de la activación del servicio	5	
		MINUTOS	**226**	
		HORAS	**3,77**	

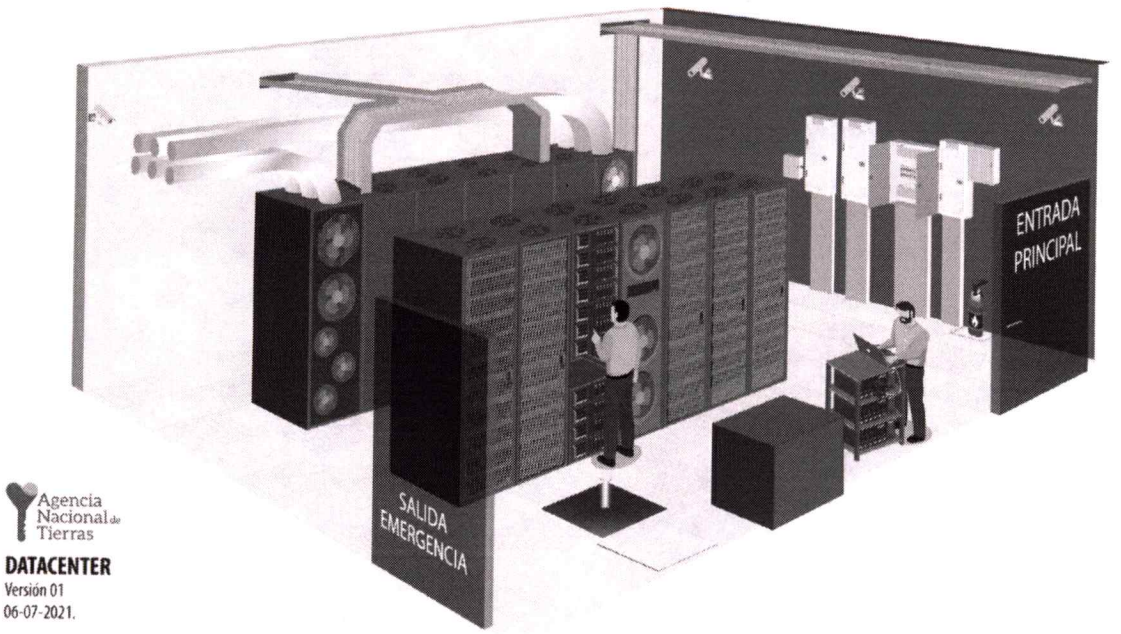
El regreso a la normalidad dependerá de los análisis del evento presentado y las acciones ejecutadas para la subsanación.

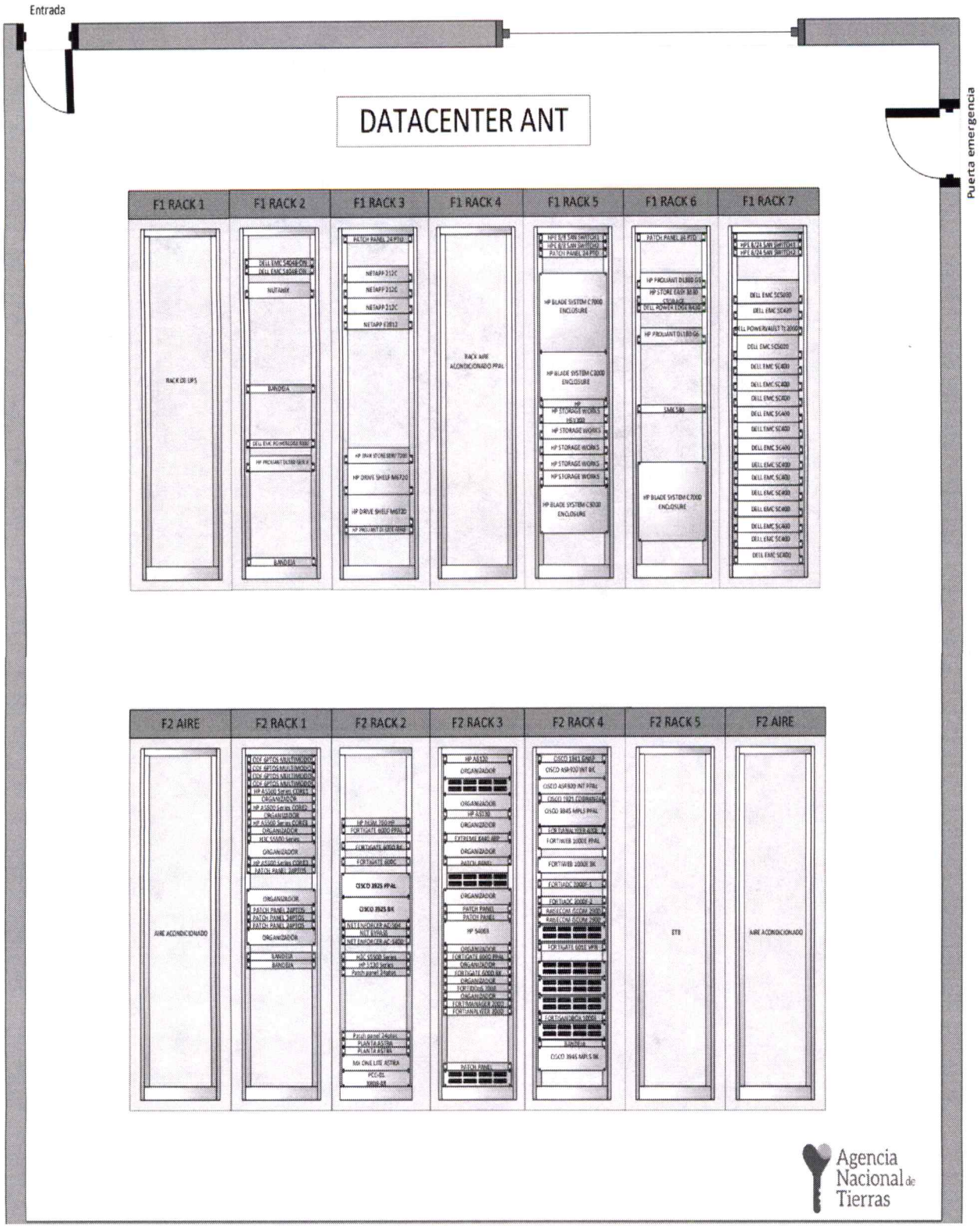
REGRESO A LA NORMALIDAD				
RESPONSABLE	**ACTIVIDADES PREVISTAS**	**RESULTADO ESPERADO**	**DURACIÓN DE LA ACTIVIDAD MINUTOS**	**OBSERVACIONES**
Líder de Infraestructura y Soporte Tecnológico	Comunica al secretario General la disponibilidad de regreso a la normalidad y acuerda la fecha para el regreso a la normalidad	Secretario notificado y fecha establecida para el regreso a la normalidad	15	La notificación puede ser telefónica o de manera presencial
Líder de Infraestructura y Soporte Tecnológico	Notificar ventana de mantenimiento	Ventana de mantenimiento programada e informada a los usuarios	10	Nota: se actualiza pieza de mantenimiento y se envía correo electrónico
Administrador de Infraestructura	Bajar servicios de cara al usuario	Servicios apagados para el usuario	5	
DBA	Sincronizar y notificar los radicados que no fueron cargados a Azure e insertar la diferencia de datos que existe entre on premise y Azure sobre las BD de azure para lo cual se deben seguir los lineamientos mencionados en el anexo 3 y 4.	Datos sincronizados en azure	45	Nota: Este tiempo puede ser variante acorde con la cantidad de registros para sincronizar.

Administrador de Infraestructura	Finalizar el DRP para que se repliquen los datos sobre On Premise - haciendo commit. Posteriormente la información nueva registrada en la plataforma Azure regresa a On premise automáticamente. 	Comando ejecutado correctamente	45	Nota: este tiempo depende de la cantidad de registros que se descarguen en su momento. Aquí se registró el tiempo de las pruebas ejecutadas.
Usuario Final	Validación de funcionalidades de la aplicación.	Aplicación y base de datos funcionando correctamente	15	
Líder de Infraestructura y Soporte Tecnológico	Notificar a la comunidad el regreso a la normalidad y el acceso a la aplicación	Usuarios notificados a través de correo electrónico	10	
Líder de Infraestructura y Soporte Tecnológico - Usuario final	Acta de radicados reservados Versus radicados utilizados.	Acta firmada por las partes interesadas	60	
DBA-líder de Desarrollo	Anulación de radicados sobrantes	Radicados anulados por tipo	10	Esta opción aplica en caso requerido.
FIN DE LA CONTINGENCIA				

MINUTOS	**215**
HORAS	**3,6**

ANEXO 2: ARQUITECTURA DEL CENTRO DE DATOS




Entrada
DATACENTER ANT
Puerta emergencia
F1 RACK 1
F1 RACK 2
F1 RACK 3
F1 RACK 4
F1 RACK 5
F1 RACK 6
F1 RACK 7
F2 AIRE
F2 RACK 1
F2 RACK 2
F2 RACK 3
F2 RACK 4
F2 RACK 5
F2 AIRE
Agencia Nacional de Tierras

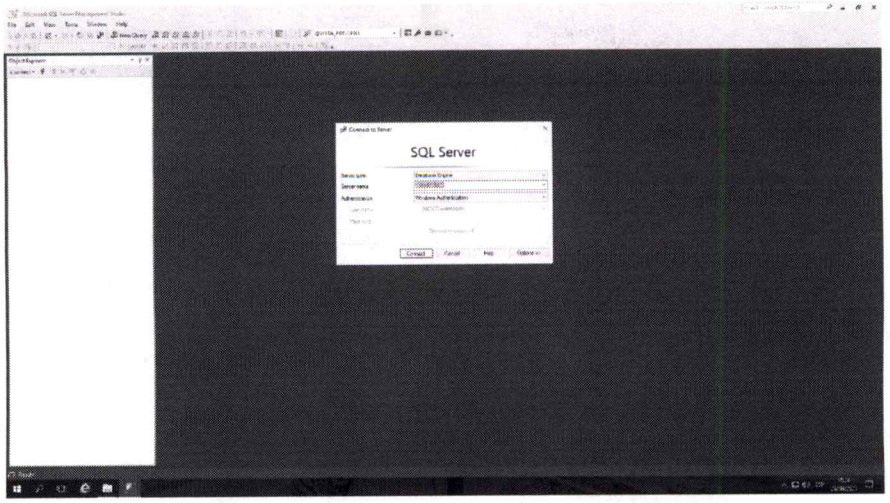
ANEXO 3: MANUAL DE SINCRONIZACIÓN DE DATOS PARA ORFEO

1. Ejecución de software de administración de base de datos SQL Server Management Studio.

Al ser motores de bases de datos SQL Server, es importante ejecutar los procesos con los programas nativos de Windows para garantizar la correcta ejecución de los procedimientos, por lo tanto, se recomienda ejecutarlos desde el SQL Server Management Studio.

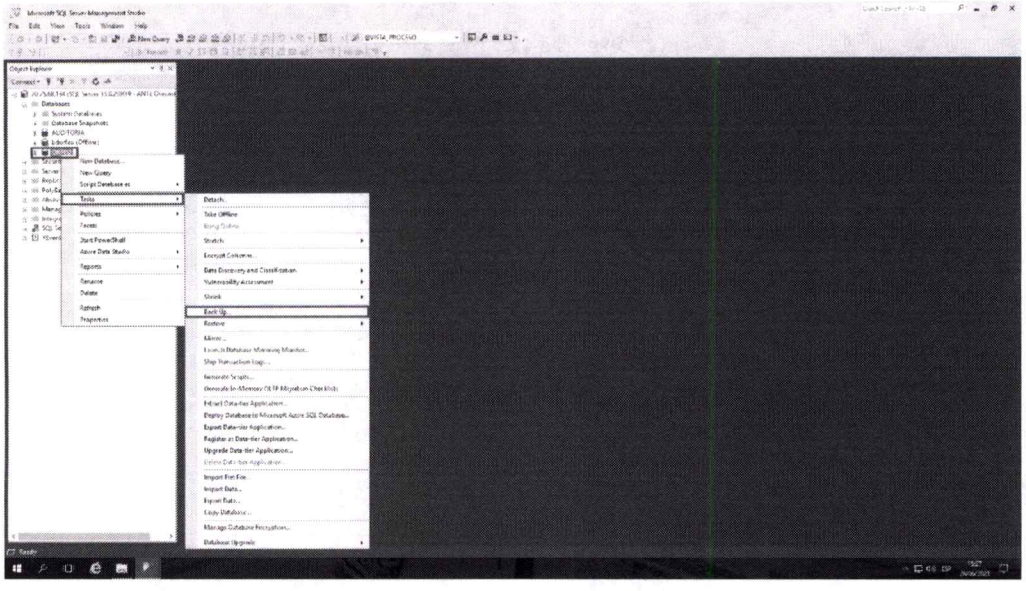
2. Conexión a la base de datos ORFEO sobre servidor AZURE (20.75.68.134)

Se debe realizar diversos procesos sobre la base de datos desplegada en el servidor de AZURE. Para ello, se inicia con la conexión a la base de datos de ORFEO localizada en la dirección IP de servidor **20.75.68.134**.



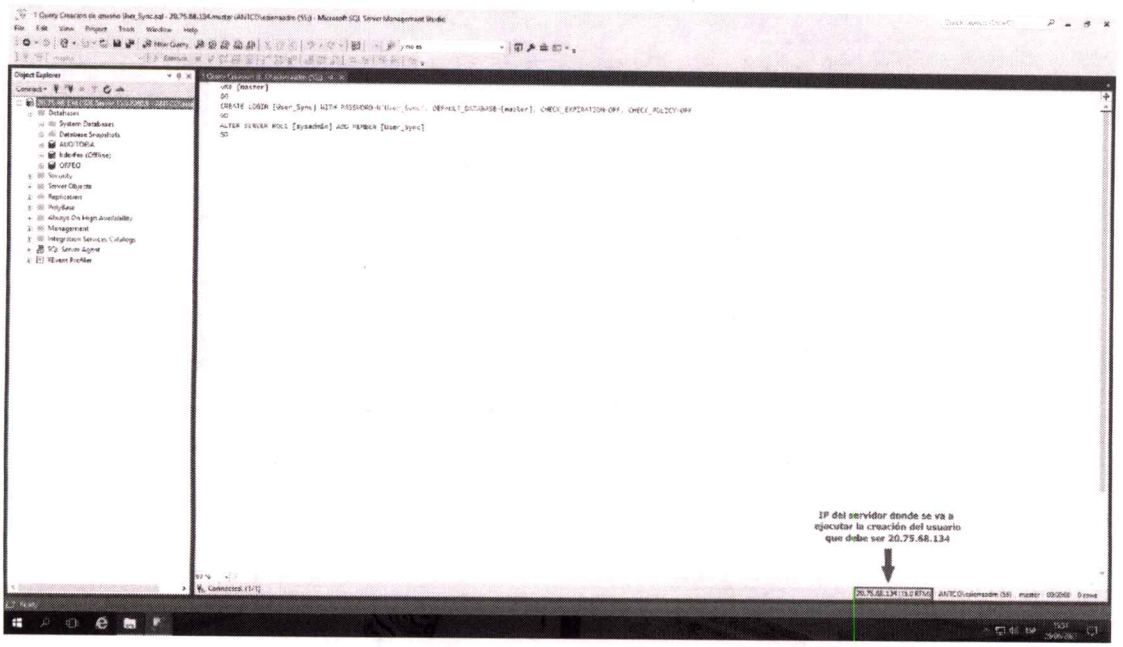
3. Ejecución de backup de la base de datos actual

Antes de realizar cualquier ajuste o actualización de secuencia, es recomendable realizar tareas de copia de seguridad de base de datos, para ser restaurada en caso de alguna falla en la ejecución, para ello, dentro de Management Studio, sobre las opciones de la basede datos, buscar la opción "**Copia de seguridad**" o "**BackUp**" y siguiendo los pasos tradicionales.



4. Creación de usuario de sincronización "User_Sync" sobre ORFEO en el servidor AZURE

Antes de iniciar la sincronización de datos, como requisito fundamental se debe hacer el enlace entre las bases de datos de ORFEO de AZURE y On-Premise, sobre la base de datos de ORFEO localizada en AZURE, se debe ejecutar el archivo "**1 Query Creacion de usuario User_Sync**".



Posterior a la carga de archivo, se debe proceder a la ejecución del código ya sea dando clic sobre el botón "**Ejecutar**" o en su defecto oprimir la tecla **F5.**

5. Proceso de sincronización

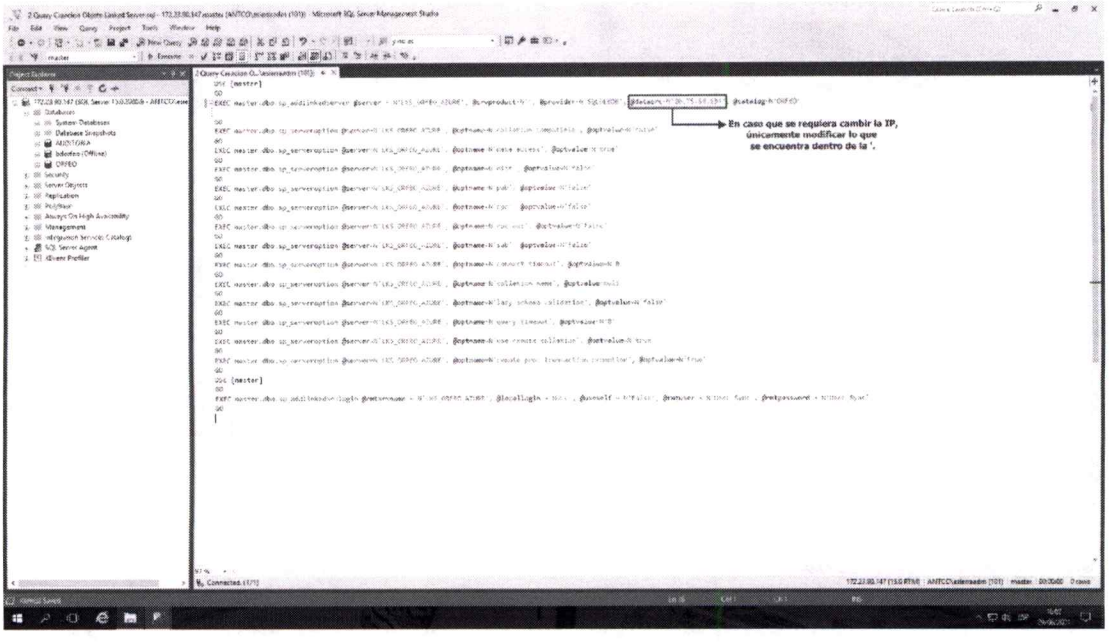
Para ejecutar este paso, se debe tener en cuenta que debe existir conectividad entre los servidores On-Premise y Azure, con el fin de sincronizar los registros faltantes de labase de datos de la base de datos sobre AZURE que están en On-Premise.

En este paso, la ejecución se hace desde la base de datos de ORFEO localizada en el servidor **ON-PREMISE**. Es importante que quien ejecute este procedimiento, tenga conocimientos básicos de SQL para garantizar una correcta realización:

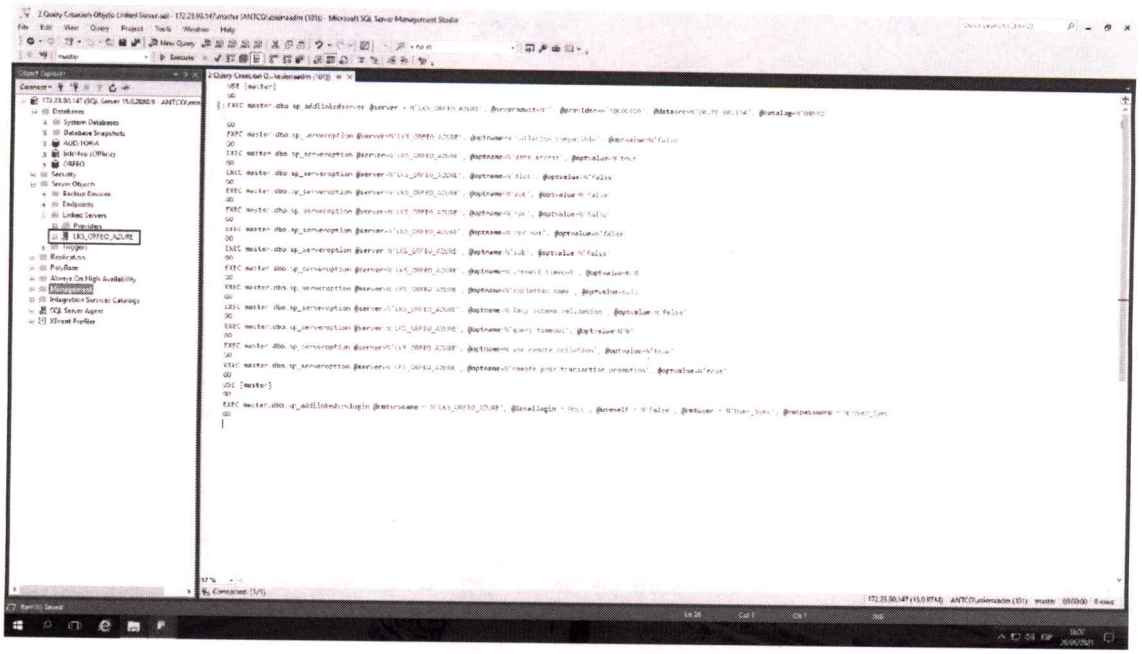
a) Creación de enlace entre las bases de datos ORFEO

Como primera acción para poder realizar la sincronización de datos faltantes a la base de datos ubicada en ambiente AZURE, se deberá crear el enlace entre las dos bases de datos. Este enlace se hace configurando un objeto de tipo Linked Server, ejecutando el archivo "**2 Query Creacion Objeto Linked Server.sql**".

Es importante que sobre este objeto se verifique la IP del servidor remoto, que, para este caso, la dirección IP del servidor de AZURE es **20.75.68.134**. En caso de que sea diferente, se debe digitar la correspondiente.

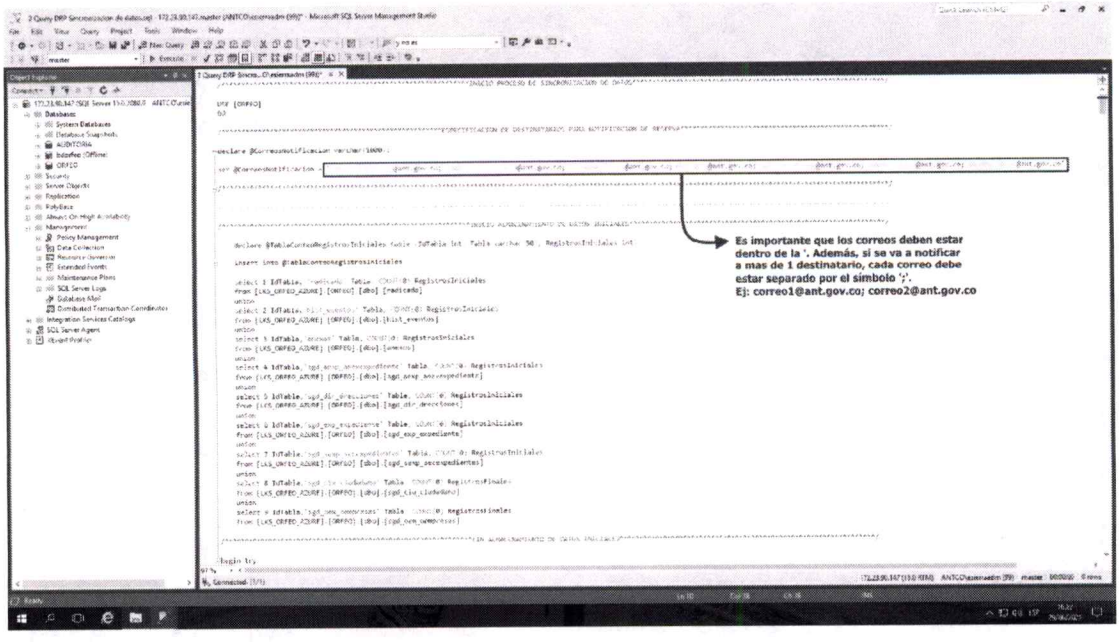


Posterior a la configuración de los datos remotos, se debe proceder a la ejecución del código ya sea dando clic sobre el botón "**Ejecutar**" o en su defecto oprimir la tecla **F5**. Como último paso, se debe verificar la correcta creación del objeto sobre el árbol del Explorador de Objetos de SQL Server Management Studio.

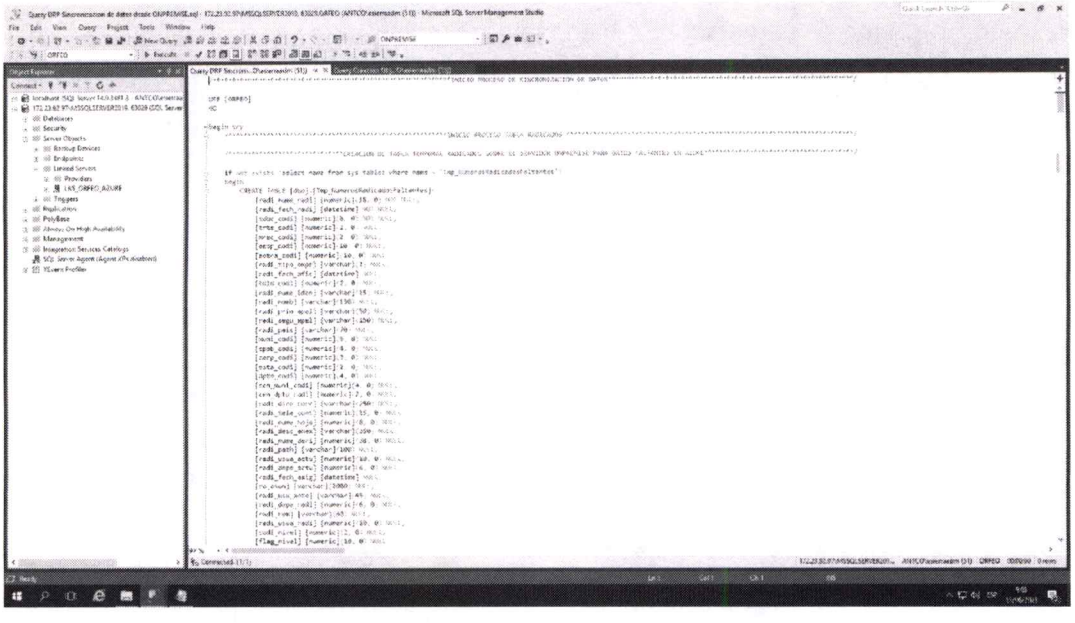


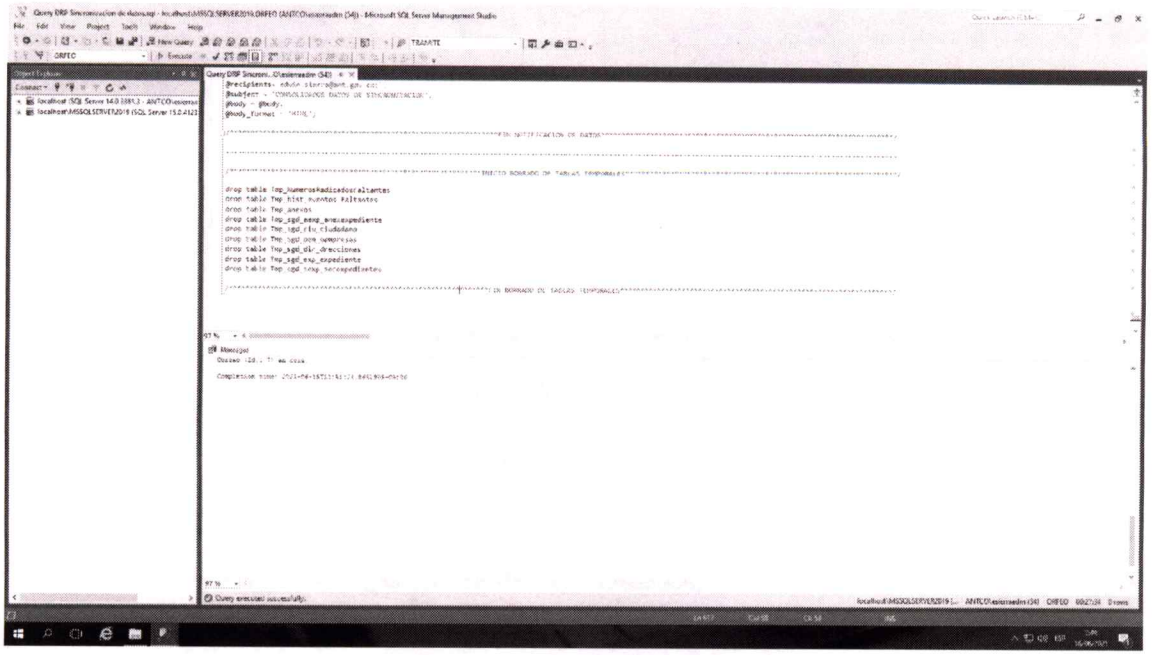
b) Ejecución de código de sincronización de datos.

Una vez se tiene la conectividad entre las dos bases de datos, se debe proceder a la ejecución del proceso de sincronización. Esto se hace a través del código de archivo denominado "**3 Query DRP Sincronizacion de datos.sql**". Es importante tener en cuenta que los procesos ejecutados en este paso, generan una notificación por correo electrónico, es por ello que se debe especificar el o los correos de los destinatarios que recibirán esta información. Esto se hace en la sección "ESPECIFICACION DE DESTINATARIOS PARA NOTIFICACION DE RESERVA" en donde se especificarán los correos.

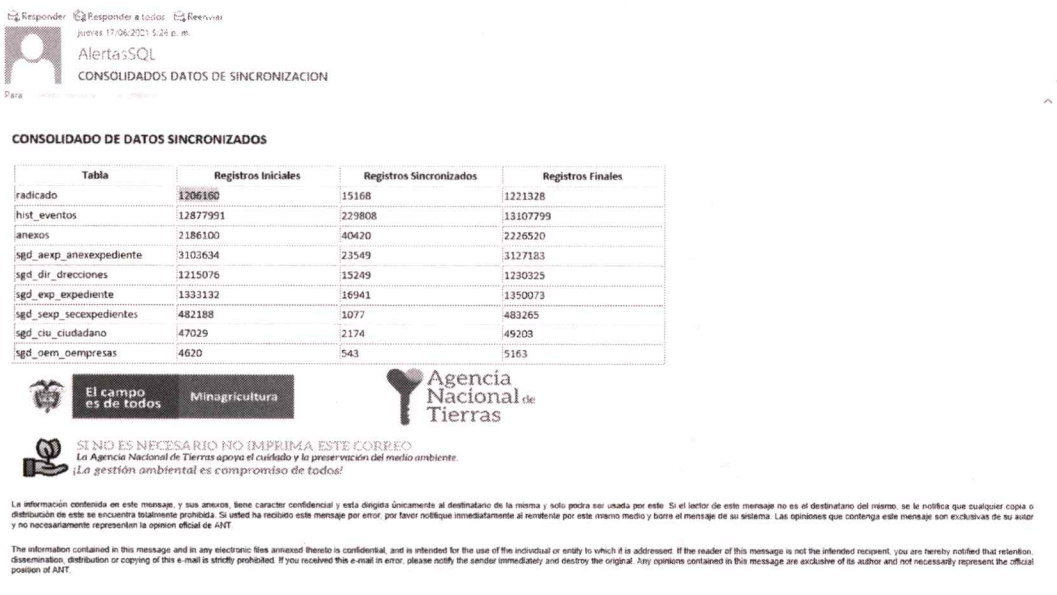


Posterior al ajuste de los correos electrónicos, se debe proceder a la ejecución del código ya sea dando clic sobre el botón "**Ejecutar**" o en su defecto oprimir la tecla **F5**.





Al final del proceso de carga, se emitirá un correo que informa la cantidad de registros iniciales, cantidad de registros cargados y cantidades finales posteriores a la ejecución.



Responder Responder a todos Reenviar

jueves 17/06/2021 5:24 p. m.

AlertasSQL

CONSOLIDADOS DATOS DE SINCRONIZACION

Para

CONSOLIDADO DE DATOS SINCRONIZADOS

Tabla	Registros Iniciales	Registros Sincronizados	Registros Finales
radicado	1206160	15168	1221328
hist_eventos	12877991	229808	13107799
anexos	2186100	40420	2226520
sgd_aexp_anexexpediente	3103634	23549	3127183
sgd_dir_drecciones	1215076	15249	1230325
sgd_exp_expediente	1333132	16941	1350073
sgd_sexp_secexpedientes	482188	1077	483265
sgd_ciu_ciudadano	47029	2174	49203
sgd_oem_oempresas	4620	543	5163

El campo es de todos | Minagricultura

Agencia Nacional de Tierras

SI NO ES NECESARIO NO IMPRIMA ESTE CORREO

La Agencia Nacional de Tierras apoya el cuidado y la preservación del medio ambiente.

¡La gestión ambiental es compromiso de todos!

La información contenida en este mensaje, y sus anexos, tiene caracter confidencial y esta dirigida únicamente al destinatario de la misma y solo podra ser usada por este. Si el lector de este mensaje no es el destinatario del mismo, se le notifica que cualquier copia o distribución de este se encuentra totalmente prohibida. Si usted ha recibido este mensaje por error, por favor notifique inmediatamente al remitente por este mismo medio y borre el mensaje de su sistema. Las opiniones que contenga este mensaje son exclusivas de su autor y no necesariamente representan la opinion oficial de ANT.

The information contained in this message and in any electronic files annexed thereto is confidential, and is intended for the use of the individual or entity to which it is addressed. If the reader of this message is not the intended recipient, you are hereby notified that retention, dissemination, distribution or copying of this e-mail is strictly prohibited. If you received this e-mail in error, please notify the sender immediately and destroy the original. Any opinions contained in this message are exclusive of its author and not necessarily represent the official position of ANT.

También se notificará una comparación entre las bases de datos de ORFEO, localizados en On-Premise y Azure, que permitirá tener una relación entre los datos de las tablas sincronizadas y verificar si son consistentes los datos o tienen alguna diferencia entre cantidades de registros.

Responder Responder a todos Reenviar

miercoles 23/06/2021 3:55 p. m.

AlertasSQL

CONSOLIDADODE DATOS DE TABLAS

Para

CONSOLIDADO DE DATOS DE TABLAS

Tabla	Registros Azure	Registros OnPremise	Comprobación
radicado	1221328	1221328	OK
hist_eventos	13107799	13107799	OK
anexos	2226520	2226520	OK
sgd_aexp_anexexpediente	3127183	3127183	OK
sgd_dir_drecciones	1230325	1230325	OK
sgd_exp_expediente	1350073	1350073	OK
sgd_sexp_secexpedientes	483265	483265	OK
sgd_ciu_ciudadano	49203	49203	OK
sgd_oem_oempresas	5163	5163	OK

El campo es de todos Minagricultura

Agencia Nacional de Tierras

SI NO ES NECESARIO NO IMPRIMA ESTE CORREO

La Agencia Nacional de Tierras apoya el cuidado y la preservación del medio ambiente.

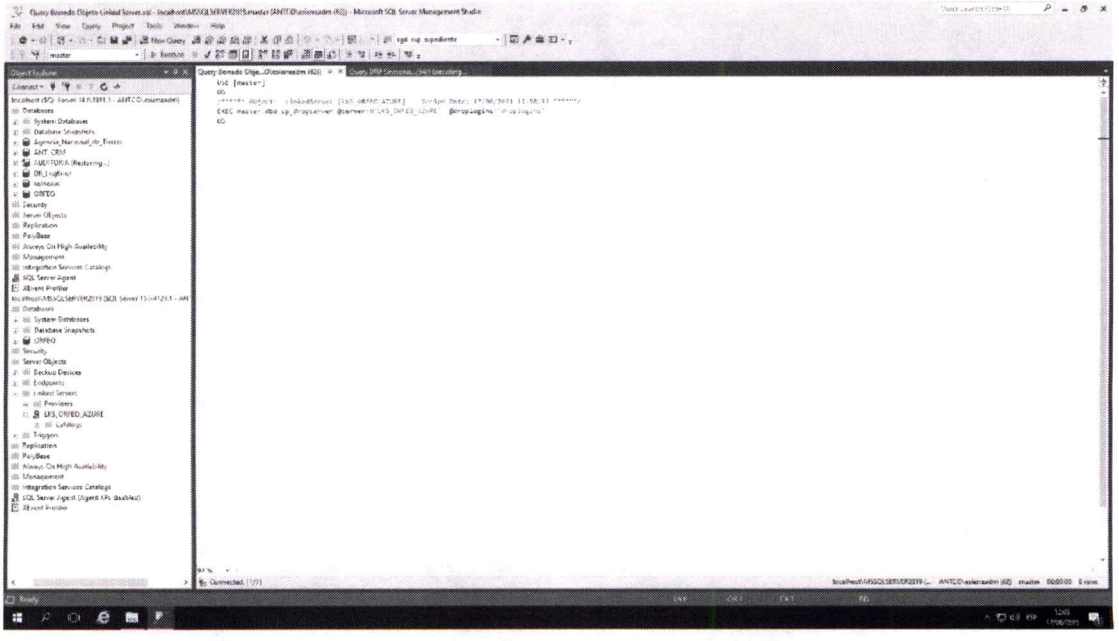
¡La gestión ambiental es compromiso de todos!

La información contenida en este mensaje, y sus anexos, tiene caracter confidencial y esta dirigida únicamente al destinatario de la misma y solo podra ser usada por este. Si el lector de este mensaje no es el distinatario del mismo, se le notifica que cualquier copia o distribucion de este se encuentra totalmente prohibida. Si usted ha recibido este mensaje por error, por favor notifique inmediatamente al remitente por este mismo medio y borre el mensaje de su sistema. Las opiniones que conferga este mensaje son exclusivas de su autor y no necesariamente representan la opinion oficial de ANT.

The information contained in this message and in any electronic files annexed thereto is confidential, and is intended for the use of the individual or entity to which it is addressed. If the reader of this message is not the intended recipient, you are hereby notified that retention, dissemination, distribution or copying of this e-mail is strictly prohibited. If you received this e-mail in error, please notify the sender immediately and destroy the original. Any opinions contained in this message are exclusive of its author and not necessarily represent the official position of ANT.

c) Eliminación de objeto linked server

Después de haber hecho el proceso de sincronización y garantizar el proceso de sincronización, se procede a realizar la eliminación del objeto linked server creado, llamado "**LKS_ORFEO_AZURE**". Eso se hace a través del archivo .sql denominado "**4 Query Borrado Objeto Linked Server.sql**". Este, se debe realizar sobre el servidor On-Premise, solo cargándolo y ejecutándolo sin realizar ninguna modificación.

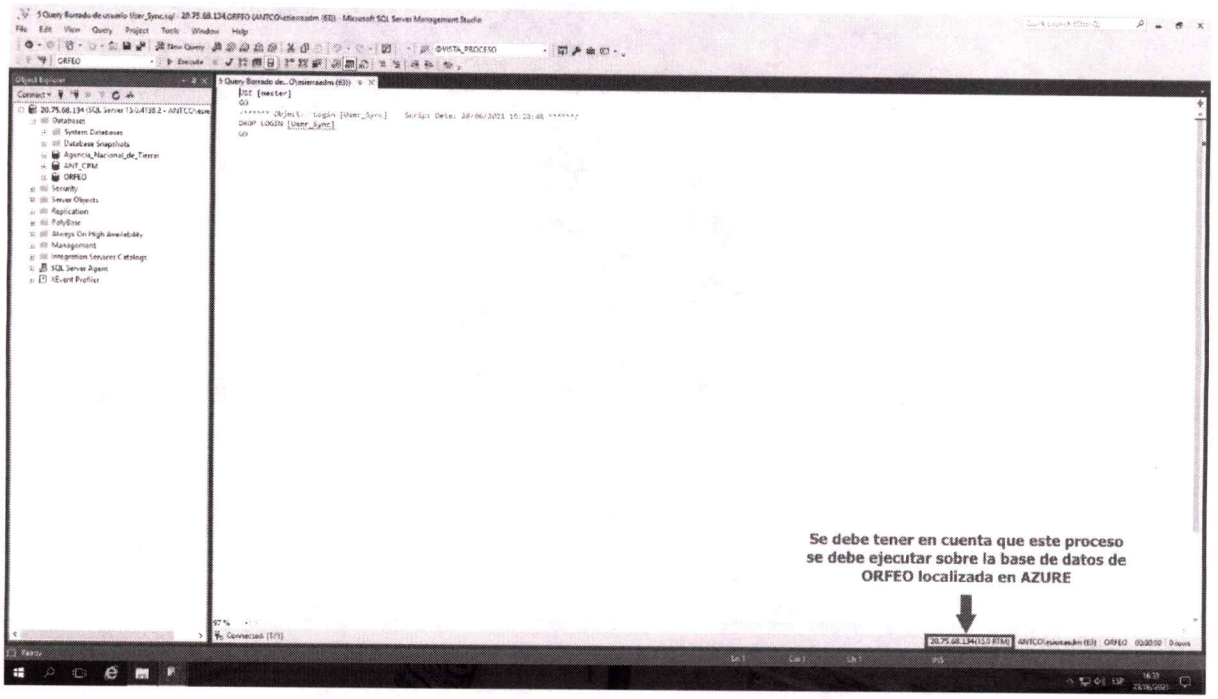


Posterior a la carga del código, se debe proceder a la ejecución del código ya sea dando clic sobre el botón "**Ejecutar**" o en su defecto oprimir la tecla **F5**.

6. Borrado de usuario de sincronización sobre base de datos AZURE

Posterior a la ejecución de la sincronización de datos, es necesario la eliminación del usuario creado para el enlace entre las bases de datos. Para ello, se debe recurrir al archivo "**5 Query Borrado de usuario User_Sync**".

Nota: Este proceso se debe ejecutar sobre la base de datos localizada en AZURE.



Posterior a la carga del código, se debe proceder a la ejecución del código ya sea dando clic sobre el botón "**Ejecutar**" o en su defecto oprimir la tecla **F5**.

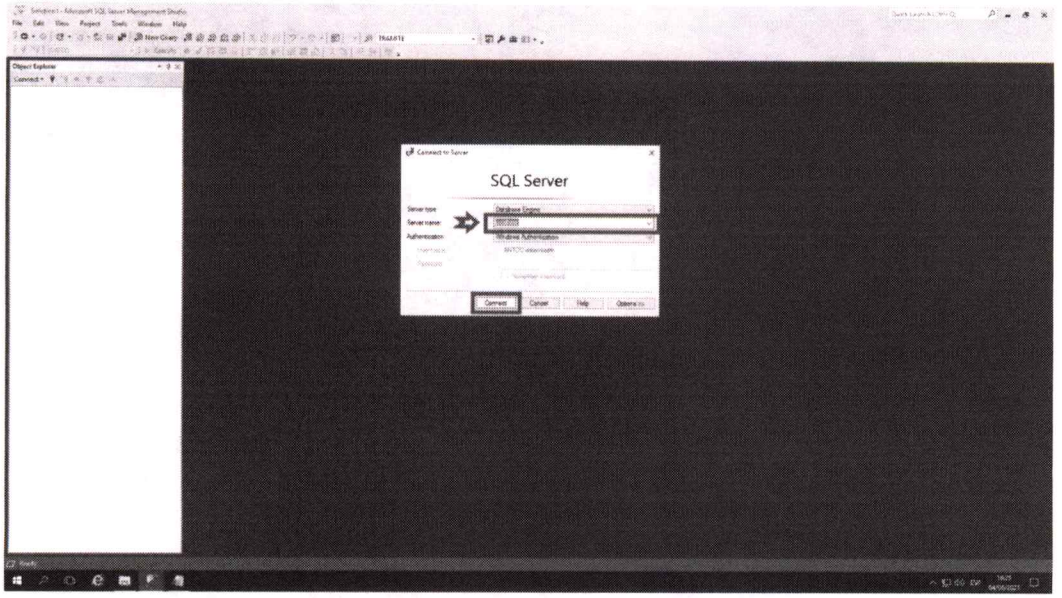
ANEXO 4. MANUAL DE RESERVA DE RADICADOS DE ORFEO EN AZURE

1. Ejecución de software de administración de base de datos SQL Server Management Studio.

Al ser motores de bases de datos SQL Server, es importante ejecutar los procesos con los programas nativos de Windows para garantizar la correcta ejecución de los procedimientos, por lo tanto, se recomienda realizarlos desde el SQL Server Management Studio.

2. Conexión a la base de datos

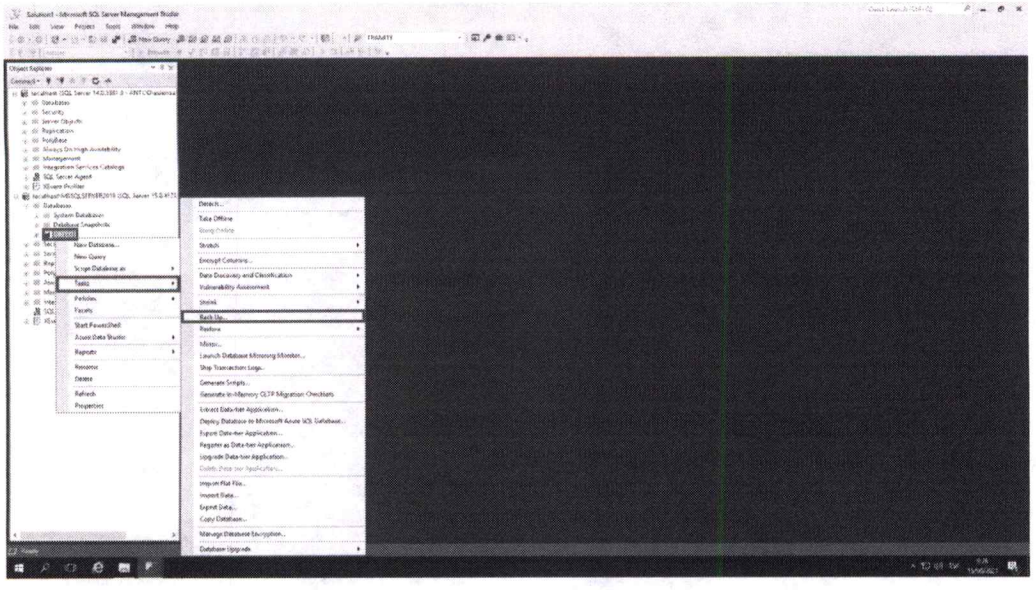
Al realizar la ejecución localmente, se debe realizar con el nombre de servidor **localhost** (solo si el Management Studio se ejecuta sobre el servidor de AZURE), en caso de que la conexión se realice desde otro servidor, sobre el campo "**Server name**" se ingresa la IP **20.75.68.134,** con esto, se garantiza la conexión a la base de datos que se requiere modificar.



Nota: Para este ejemplo, se ejecutó el Management Studio sobre la máquina virtual del DRP (20.75.68.134)

3. Ejecución de backup de la base de datos actual

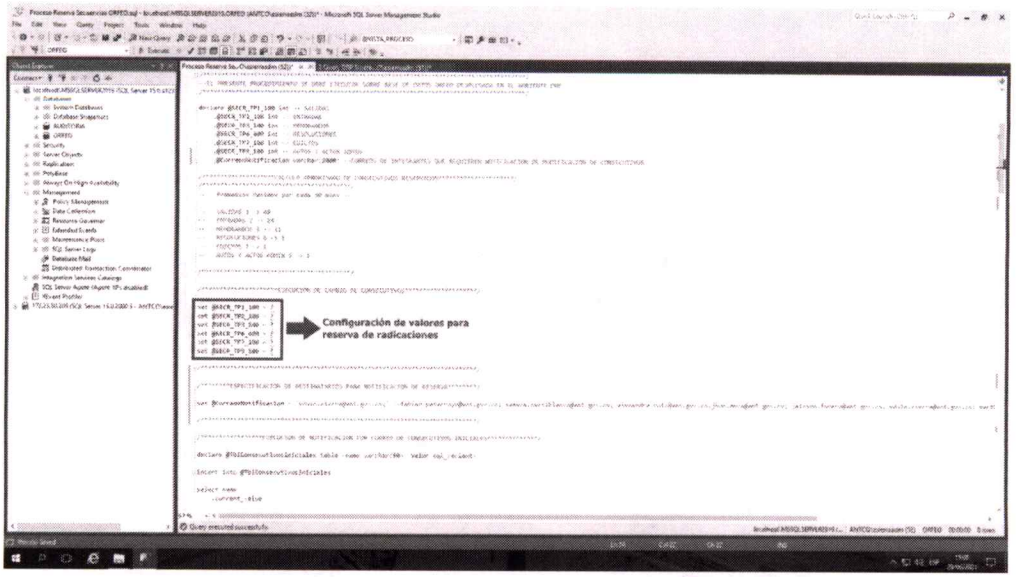
Antes de realizar cualquier ajuste o actualización de secuencia, es recomendable realizar tareas de copia de seguridad de base de datos, para ser restaurada en caso de alguna falla en la ejecución, para ello, dentro de Management Studio, sobre las opciones de la basede datos, buscar la opción "**Copia de seguridad**" o "**BackUp**" y siguiendo los pasos tradicionales.



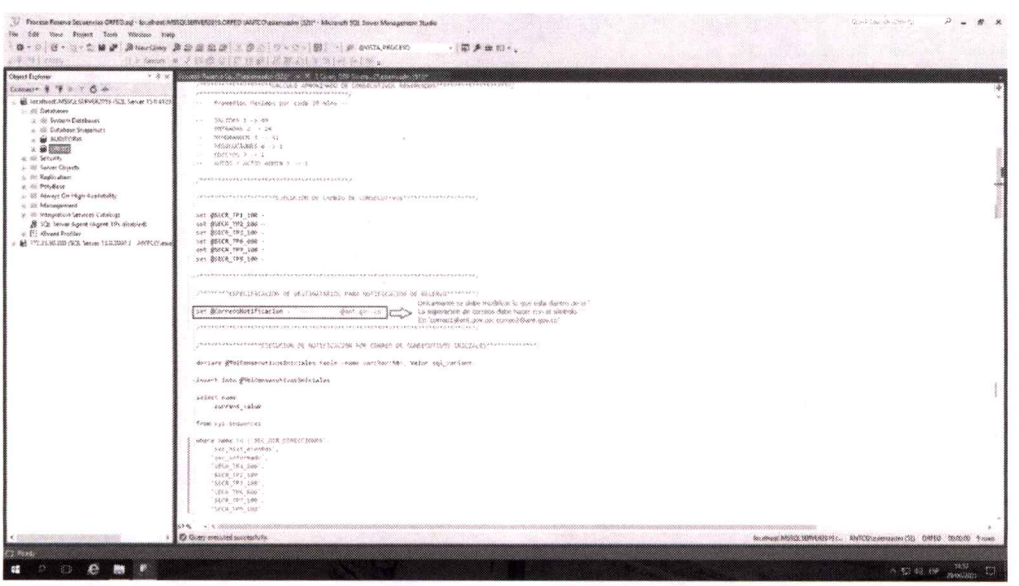
4. Ejecución del proceso de reserva de secuencias.

Para la ejecución del ajuste de reserva de consecutivos de radicación, se debe ejecutar el archivo "**Proceso Reserva Secuencias ORFEO.sql**". En Este proceso hace una modificación en consecutivos utilizados por el sistema.

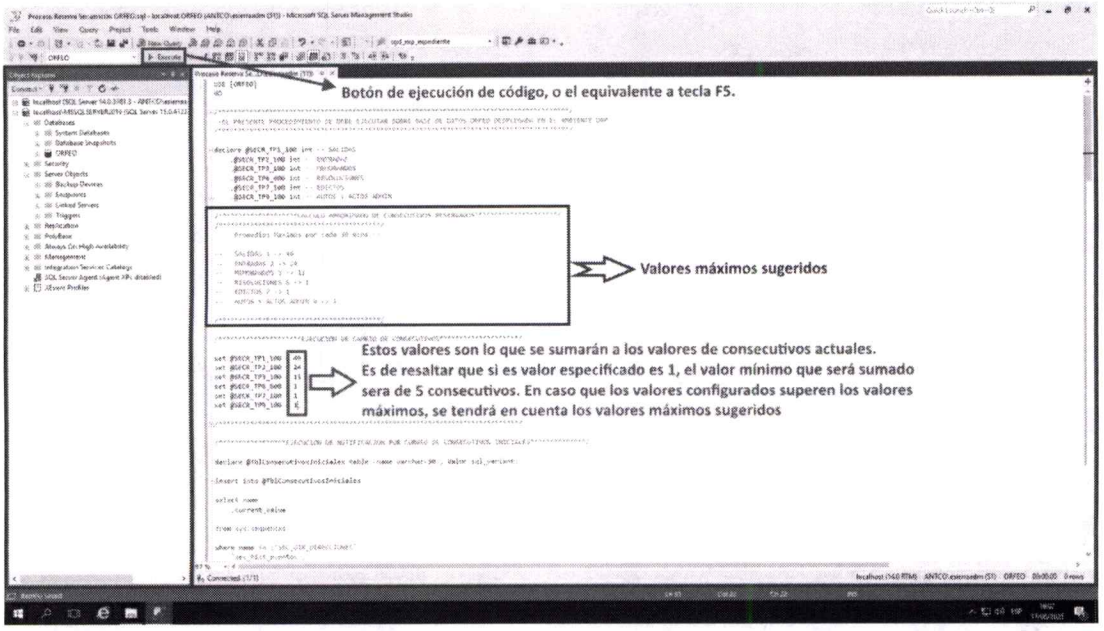
En el código que contiene el archivo, se debe buscar la sección "**EJECUCIÓN DE CAMBIO DE CONSECUTIVOS**". Allí se especificarán los valores que se sumarán a los con consecutivos actuales para iniciar la operación reemplazando el signo "**?**" por el valor requerido.



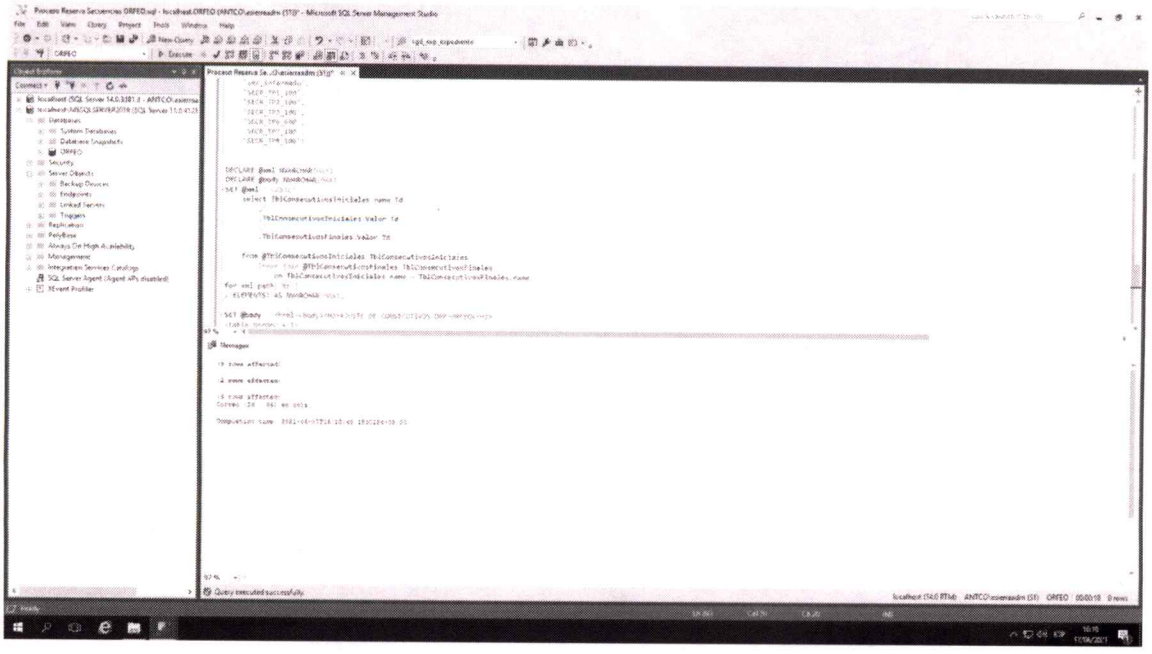
Posterior a la especificación de valores iniciales de los consecutivos con lo que se desea iniciar, se debe especificar los correos de quienes van a recibir la notificación de los ajustes, mínimo se debe especificar 1 persona. Para especificar más de 1 correo, sebe separar mail con el símbolo "**;**". Esta configuración se hace en la sección "**ESPECIFICACION DE DESTINATARIOS PARA NOTIFICACION DE RESERVA**".



Una vez realizado las configuraciones de reserva de consecutivos y destinatarios de notificación, se debe dar clic sobre el botón "**Ejecutar**" o presionar la tecla "**F5**".



La ejecución de este código, hará el ajuste automático de los consecutivos iniciales, suman los valores especificados en el query. Posterior a la ejecución, se recibirá un correo de notificación con los valores anteriores y nuevos de las secuencias.



Responder | Responder a todos | Reenviar

jueves 17/06/2021 4:13 p. m.

AlertasSQL

Consecutivo Inicial pre-ajuste

Para

AJUSTE DE CONSECUTIVOS DRP-ORFEO

Consecutivo	Secuencia Inicial	Secuencia Final
SEC_DIR_DIRECCIONES	152407454	152407541
sec_hist_eventos	19313878	19314139
sec_informado	9697	9717
SECR_TP1_100	235	285
SECR_TP2_100	52902	52926
SECR_TP3_100	13790	13801
SECR_TP6_600	6455	6456
SECR_TP7_100	417	6457
SECR_TP9_100	2630	2631

Fecha tentativa del último registro on-premise: 17/may./2021 19:00:28

El campo es de todos | Minagricultura

Agencia Nacional de Tierras

SI NO ES NECESARIO NO IMPRIMA ESTE CORREO
La Agencia Nacional de Tierras apoya el cuidado y la preservación del medio ambiente.
¡La gestión ambiental es compromiso de todos!