


RESOLUCIÓN SEN Nº 779/2021

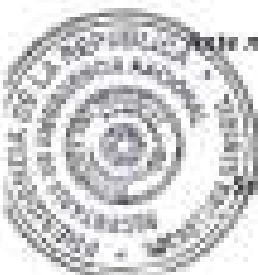
POR LA CUAL SE APRUEBA LA POLÍTICA Y PROCEDIMIENTOS PARA LA UTILIZACIÓN DEL CORREO INSTITUCIONAL EN LA NUBE Y PARA LA UTILIZACIÓN DEL SERVICIO DRIVE EN LA NUBE DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, DE LA SECRETARÍA DE EMERGENCIAS NACIONALES (SEN), DEPENDIENTE DE LA PRESIDENCIA DE LA REPÚBLICA.

Asunción, 17 de septiembre de 2021

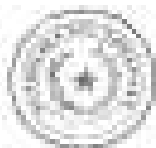
Artículo 4º.- Creación e quince corresponden y correlación, archivar.



  
Joaquín D. Ros Burgos  
Ministro Secretario Ejecutivo  
Secretaría de Emergencias Nacionales



  
María del Pilar Castro  
Secretaría General  
Secretaría de Emergencias Nacionales



ESTADO  
PARAGUAY  
GOBIERNO  
NACIONAL

■ TETĀ REKUĀI  
■ GOBIERNO NACIONAL

*Paraguay  
de la gente*

# POLÍTICAS

PARA LA UTILIZACIÓN

DEL

# SERVICIO DRIVE

EN LA NUBE



ESTADO  
PARAGUAY  
GOBIERNO  
NACIONAL

Secretaría de Emergencia Nacional

Dirección de Tecnología, Información y Comunicaciones (DTIC)

Departamento de Administración de Redes (DPAR)

*[Handwritten signature]*



Año 2021

ESTADO PARAGUAY, ASÍ SE SERVE

CONSEJO DE LA ECONOMÍA

Y FINANZAS

SECRETARÍA DE EMERGENCIA NACIONAL

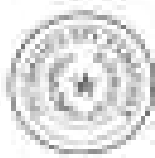


ESTADO PARAGUAY, ASÍ SE SERVE

CONSEJO DE LA ECONOMÍA

Y FINANZAS

SECRETARÍA DE EMERGENCIA NACIONAL



CONTENIDO

1.- Introducción	3
2.- Habilitación de Cuentas	4
2.1.-Administrador Nube Institucional	4
2.2.-Administrador Drive Institucional	4
2.3.-Usuario Drive Institucional	4
3.- Responsabilidad de los Usuarios	5
3.1.-Administrador Nube Institucional	5
3.2.-Administrador Drive Institucional	5
3.3.-Usuario Drive Institucional	5
4.- Seguridad de Acceso	6
4.1.-Contraseña	6
4.2.-Precauciones	6
5.- Seguridad de la Información	6
5.1.-Respaldo	6
5.1.-Difusión	6
6.- Políticas de Uso	7
6.1.-Archivos	7
6.2.-Limitaciones	7
6.3.-Montos	7



REPUBLICA PARAGUAY  
GOBIERNO NACIONAL



## I. INTRODUCCIÓN

Ante los requerimientos actuales de infraestructura adecuada para el manejo de servicios, aplicaciones y resguardo de la información pública como patrimonio intangible, disponible y accesible desde cualquier punto, se realizaron las gestiones ante el Ministerio de Tecnología, Información y Comunicaciones (MITIC), para la habilitación de una Nube Institucional.

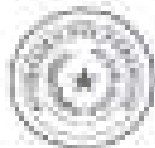
Con el objetivo de contar con una plataforma digital, que pudiera sostenerse en el tiempo y salvaguardar los datos estadísticos e históricos de la administración de esta Secretaría. A partir de la habilitación de este servicio el 25 de agosto de 2021, para su goceamiento, a través de la Dirección de Tecnología, Información y Comunicaciones (DTIC) y su Departamento de Programación y Administración de Redes (DPAAR) como punto focal y técnico ante el Ministerio de Tecnología, Información y Comunicaciones (MITIC).

Siendo posible contar con un servicio más que nos brinda la posibilidad de realizar fácilmente el respaldo de datos institucionales que pueden servir de respaldo a proyectos y programas de ayuda humanitaria y así como transparentarla gestión de la misma administración actual.

Es importante la utilización de este tipo de servicios, para las Direcciones y Dependencias que manejan todo tipo de informaciones que sirven de apoyo estadístico, consulta o de resguardo digital de documentaciones, concernientes a las actividades de la institución, evitando el riesgo interno de su pérdida por daños del equipo informático.



  
ENCUENTRO LOS SERVIDORES  
Ministerio de Tecnología, Información y Comunicaciones  
San Pedro de Ycuá Ypané



## 2. HABILITACIÓN DE CUENTAS

### 2.1 ADMINISTRADOR NUBE INSTITUCIONAL

Para la habilitación del administrador de la Nube, Conforme a la solicitud de la máxima autoridad de la institución, designando a un funcionario técnico del área TIC, a través del formulario de Servicios, ante el Ministerio de Tecnología, Información y Comunicaciones (MITIC). Este paso se realiza de forma única para habilitar el servicio. En caso de la designación de un nuevo administrador, se debe comunicar vía nota oficial al MITIC.

### 2.2 ADMINISTRADOR DRIVE INSTITUCIONAL

Para la habilitación del administrador del Drive Institucional, se realiza previa solicitud del servicio en la Nube y designación del funcionario técnico del área TIC, por parte de la máxima autoridad de la Institución por medio del formulario de Servicios, ante el Ministerio de Tecnología, Información y Comunicaciones (MITIC). Este paso se realiza de forma única para habilitar el servicio. En caso de la designación de un nuevo administrador, se debe comunicar vía nota oficial al MITIC.

### 2.3 USUARIO DRIVE INSTITUCIONAL

Para la habilitación de usuarios en el Drive Institucional, se realiza por solicitud vía correo o memorándum del superior inmediato del área, a la Dirección TIC y esta al Departamento de Programación y Administración de Redes, mencionando los usuarios que podrán utilizar el servicio y el nombre de la carpeta asignada para uso de esa dependencia, a efectos de resguardar los archivos, base de datos o multimedios institucionales de importancia. Así mismo la dependencia deberá comunicar al Administrador Drive, la baja del usuario que ya no tendrá acceso a la plataforma.



ESTADO PARAGUAY  
PRESIDENCIA NACIONAL



### 3. RESPONSABILIDAD DE LOS USUARIOS

#### 3.1 ADMINISTRADOR NUBE INSTITUCIONAL

Encargado técnico TIC de la Nube Institucional y punto focal designado por la máxima autoridad para realizar las gestiones en el portal de servicios ante el Ministerio de Tecnología, Información y Comunicaciones (MITIC). Por solicitud de algún servicio vía correo electrónico o memorándum de alguna dependencia que lo requiera.

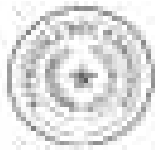
#### 3.2 ADMINISTRADOR DRIVE INSTITUCIONAL

Responsable del servicio drive institucional en la nube para gestionar las altas, bajas, creación de carpetas para grupos de trabajo y reseteo de contraseñas de usuarios, conforme a la solicitud realizada por correo o memorándum de alguna dependencia para lo mencionado.

#### 3.3 USUARIO DRIVE INSTITUCIONAL

Encargado de gestionar los archivos y carpetas del grupo de trabajo designado, para la carga digital en el drive institucional, así como el resguardo e integridad de la información correspondiente a la Dirección o Dependencia al cual pertenece.





## 4. SEGURIDAD DE ACCESO

### 4.1 CONTRASEÑA

Todos los usuarios de diversos niveles de acceso deberán colocar contraseñas seguras de por lo menos 8 caracteres combinando letras mayúsculas y minúsculas, números y caracteres especiales para mayor seguridad. Cambiar la contraseña cada cierto tiempo. En caso de pérdida o olvido, se podrá solicitar el reseteo del mismo al administrador del Drive Institucional por correo memorándum.

### 4.2 PRECAUCIONES

Evitar exponer la contraseña en medios legibles como agendas, mensajerías instantáneas, redes sociales o archivos digitales sin contraseña. No recordar la contraseña en el navegador que utilice. No ingresar a la cuenta en presencia de extraños o en equipos informáticos de uso casual o público. No ceder la contraseña a terceros.

## 5. SEGURIDAD DE LA INFORMACIÓN

### 5.1 RESPALDO

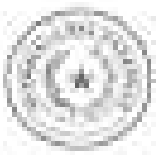
Las Direcciones o Dependencias tendrán a su cargo el manejo de los datos institucionales que generen para su respaldo en el Drive Institucional bajo la carpeta única o del grupo habilitado con los usuarios designados que ha sido solicitado con anterioridad. Así como su respaldo en unidades extraíbles como disco duro externo.

### 5.2 DIFUSIÓN

La socialización de la información Institucional (opción de compartir o descarga) queda bajo responsabilidad de los usuarios. El mismo deberá ser solicitado por correo o memorándum a la dependencia que lo administra de forma interna y si fuera externa la solicitud será autorizada por la superioridad.







## 6. POLÍTICAS DE USO

### 6.1 ARCHIVOS

Los datos o archivos resguardados en el Drive, deberán ser referentes a la gestión de la institución para su respaldo, evitando el uso del espacio para archivos personales o sin fines institucionales.

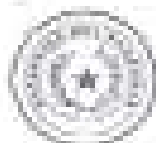
### 6.2 LIMITACIONES

Las limitaciones de espacio para los archivos digitales serán establecidas de acuerdo a la necesidad de cada dependencia, pudiendo ser limitada o ampliada por solicitud al administrador del Drive institucional y conforme a los estándares de la misma plataforma.

### 6.3 MONITOREO

Las actividades de los usuarios sobre el uso del drive y/o acciones realizadas quedan registradas en la plataforma como **Historial en la plataforma (actividad)** para los fines que hubieren lugar.



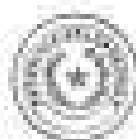


REPUBLICA  
PARAGUAY  
SISTEMA  
NACIONAL  
DE EMERGENCIAS

■ TETĀ REKUĀI  
■ GOBIERNO NACIONAL

Paraguay  
de la gente

POLÍTICAS  
Y  
PROCEDIMIENTOS  
PARA LA UTILIZACIÓN  
DEL  
CORREO INSTITUCIONAL  
EN LA NUBE



REPUBLICA  
PARAGUAY  
SISTEMA  
NACIONAL  
DE EMERGENCIAS

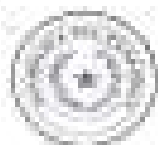
Secretaría de Emergencia Nacional

Dirección de Tecnología, Información y Comunicaciones (DTIC)

Departamento de Administración de Redes (DFAR)

Año 2021

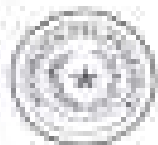




## CONTENIDO

1.- Introducción	3
2.- Habilitación de Cuentas	4
2.1.-Administrador Nube Institucional	4
2.2.-Administrador Correo Institucional	4
2.3.-Usuario Correo Institucional	4
3.- Responsabilidad de los Usuarios	5
3.1.-Administrador Nube Institucional	5
3.2.-Administrador Correo Institucional	5
3.3.-Usuario Correo Institucional	5
4.- Seguridad de Acceso	6
4.1.-Contraseña	6
4.2.-Precauciones	6
4.3.-Correos o Mensajes	6
5.- Seguridad de la Información	6
5.1.-Respaldo	6
5.1.-Difusión	6
6.- Políticas de Uso	7





## I. INTRODUCCIÓN

La comunicación institucional es uno de los requerimientos más importantes para realizar las gestiones dentro de la administración pública así como la plataforma que se utiliza para ello. Es el medio oficial ante otros organismos nacionales e internacionales para el envío y la recepción de informaciones. Teniendo como ente rector de la Tecnología y Comunicación de las instituciones del estado, al Ministerio de Tecnología, Información y Comunicaciones (MITIC). Por lo que fue tramitado, la habilitación del correo electrónico institucional en la Nube como primer servicio indispensable. En ese sentido es de suma importancia que las dependencias de esta Secretaría, realicen los trámites a través de este servicio como canal institucional, formalizando toda gestión.

El fortalecimiento tecnológico dentro de las entidades públicas, es fundamental para las relaciones interinstitucionales, a fin de mejorar la eficiencia de los servicios públicos que ofrece al gobierno. Este medio de comunicación, ayuda a facilitar las actividades internas y externas, así como la transferencia de datos, planes y proyectos. Haciendo un seguimiento a los mismos y poder llegar a concluir los objetivos propuestos.

El Departamento de Programación y Administración de Redes está comprometido a mantener y gestionar los servicios y portales dentro de la Nube como contacto técnico interinstitucional.





## 1. HABILITACIÓN DE CUENTAS

### 1.1 ADMINISTRADOR NUBE INSTITUCIONAL

Para la habilitación del administrador de la Nube. Conforme a la solicitud de la máxima autoridad de la institución, designando a un funcionario técnico del área TIC, a través del formulario de Servicios, ante el Ministerio de Tecnología, Información y Comunicaciones (MITIC). Este paso se realiza de forma única para habilitar el servicio. En caso de la designación de un nuevo administrador, se debe comunicar vía nota oficial al MITIC.

### 1.2 ADMINISTRADOR CORREO INSTITUCIONAL

Para la habilitación del administrador del correo institucional, se realiza previa solicitud del servicio y designación del funcionario técnico del área TIC, por parte de la máxima autoridad de la institución por medio del formulario de servicios, ante el Ministerio de Tecnología, Información y Comunicaciones (MITIC). Este proceso se realiza de forma única para habilitar el servicio. En caso de la designación de un nuevo administrador, se debe comunicar vía nota oficial al MITIC.

### 1.3 USUARIO CORREO INSTITUCIONAL

La habilitación de los usuarios para el uso del correo institucional. Se realiza por solicitud vía correo o memorándum del superior inmediato del área, a la Dirección TIC y este al Departamento de Programación y Administración de Redes, detallando el nombre del correo que tendrá a su cargo la dependencia. El mismo será habilitado por el administrador con una contraseña temporal para que el usuario lo pueda reemplazar de forma segura.





### 3. RESPONSABILIDAD DE LOS USUARIOS

#### 3.1 ADMINISTRADOR NUBE INSTITUCIONAL

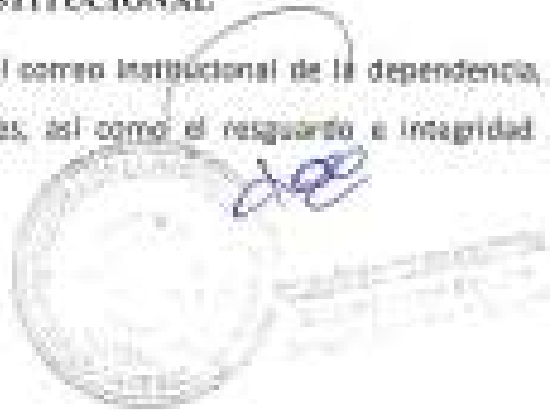
Encargado técnico TIC de la Nube Institucional y punto focal designado por la máxima autoridad para realizar las gestiones en el portal de servicios ante el Ministerio de Tecnología, Información y Comunicaciones (MITIC). Por solicitud de algún servicio vía correo electrónico o memorándum de alguna dependencia que lo requiera.

#### 3.2 ADMINISTRADOR CORREO INSTITUCIONAL

Responsable del servicio de correo institucional en la nube para gestionar las altas, bajas y reseteo de contraseñas de usuarios, conforme a la solicitud realizada por correo-memorándum de alguna dependencia.

#### 3.3 USUARIO CORREO INSTITUCIONAL

Encargado de gestionar el correo institucional de la dependencia, para el envío y la recepción de los mensajes, así como el resguardo e integridad de la información recepcionada y remitida.





## 4. SEGURIDAD DE ACCESO

### 4.1 CONTRASEÑA

Todos los usuarios de diversos niveles de acceso deberán colocar contraseñas seguras de por lo menos 8 caracteres combinando letras mayúsculas, minúsculas, números y caracteres especiales para mayor seguridad. Cambiar la contraseña cada cierto tiempo. En caso de pérdida o olvido, se podrá solicitar el reseteo del mismo al administrador del correo institucional por medio electrónico o memorándum.

### 4.2 PRECAUCIONES

Evitar exponer la contraseña en medios legítimos como agendas, mensajes instantáneos, redes sociales o archivos digitales sin contraseña. No recordar la contraseña en el navegador que utilice. No ingresar a la cuenta en presencia de extraños o en equipos informáticos de uso casual o público. No ceder la contraseña a terceros.

### 4.3 CORREOS O MENSAJES

Al recibir un correo electrónico, deberá evitar abrirlo o descargarlo si no es posible identificar al remitente, pues podría ser un virus, malware o spam que podría dañar el equipo, robar información o ingresar a una lista negra. Comunicar este hecho al administrador del servicio.

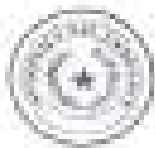
## 5. SEGURIDAD DE LA INFORMACIÓN

### 5.1 GESTIÓN

Las Dependencias tendrán a su cargo la gestión del correo institucional asignado para la recepción y remisión de datos institucionales. Así como su respaldo en el drive institucional y en unidades extraíbles como disco duro externo.

### 5.2 DIFUSIÓN

La socialización de la información institucional, a través del correo electrónico oficial queda bajo responsabilidad de los usuarios, previa autorización de la superioridad.



## 6. POLÍTICAS DE USO

- 1- El correo electrónico institucional, se utilizará exclusivamente para los trámites referentes a la institución, teniendo en cuenta que representa a esta Secretaría, a la dependencia o al funcionario remitente por su extensión [sen.gov.py](mailto:sen.gov.py).
- 2- El correo electrónico institucional, no se utilizará para cuestiones personales que puedan dañar la imagen, la integridad institucional, de sus autoridades o hechos que puedan ser pasibles de sanciones.
- 3- Se podrá acceder al correo electrónico institucional, a través del portal de la Secretaría, [www.sen.gov.py](http://www.sen.gov.py), en la pestaña institucional>correo institucional con el nombre del usuario designado (Ej: [mesadeentrada@sen.gov.py](mailto:mesadeentrada@sen.gov.py)) y la contraseña definida por el usuario.
- 4- El reclamo por la falta de este servicio, deberá ser comunicado al administrador del correo institucional, a fin de realizar las gestiones ante el Ministerio de Tecnología de la Información y Comunicación (MITIC).







Secretaría General

**Ratificación Resolución SEN N° 738/2021**

FORO DE DIALOGO DE APERTURA LA NÚMÉRICA Y PROCESAMIENTOS PARA LA GESTIÓN DEL TERCER INSTITUCIONAL EN LA RUMI Y PARA LA  
MODERNIZACIÓN DEL SERVICIO DE TRÁMITE DE LA RUMI DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, DE LA  
SECRETARÍA NACIONAL, COMO COMPONENTE DE LA REFORMA DE LA REPÚBLICA

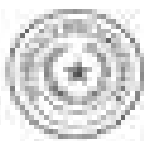
➤ **Mesa de Dependencias Ejecutivas**

- 1. Secretaría Privada (SP) \_\_\_\_\_
- 2. Departamento de Protocolo y Ceremonial (DPC) \_\_\_\_\_
- 3. Centro de Operaciones de Emergencia (COE) \_\_\_\_\_
- 4. Unidad Anticorrupción (UAC) \_\_\_\_\_
- 5. Dirección General de Reducción de Riesgos (DGR) \_\_\_\_\_
- 6. Secretaría General (SG) \_\_\_\_\_
- 7. Coordinación MDCP: \_\_\_\_\_
- 8. Jefatura de Gabinete: \_\_\_\_\_
- 9. Dirección de Relaciones Internacionales e Interacción (DRI) \_\_\_\_\_
- 10. Dirección de Auditoría Interna \_\_\_\_\_
- 11. Dirección de Consultoría e Información Pública (DCIP) \_\_\_\_\_
- 12. Dirección de Planificación y Sistematización (DPS) \_\_\_\_\_

➤ **Mesa de Dependencias de Apoyo**

- 13. Dirección de Asesoría Jurídica \_\_\_\_\_
- 14. Dirección de Tecnologías de la Información y la Comunicación (DTIC) \_\_\_\_\_
- 15. Coordinación de Asuntos Lingüísticos (CAL) \_\_\_\_\_
- 16. Dirección General de Logística (DGL) \_\_\_\_\_
- 17. Dirección General de Administración y Finanzas (DGLAF) \_\_\_\_\_
- 18. Dirección Operativa de Contrataciones Públicas (DOCP) \_\_\_\_\_

**Misión:** Operar y robustecer los canales de diálogo en el país a través de instancias, con espíritu siempre participativo, que brinden un reconocimiento y justicia.  
**Visión:** Ser el más reconocido y valorado canal de comunicación de la gestión pública de todos los niveles de gobierno.



Secretaría General

18. Dirección de Gestión y Desarrollo de las Personas (DGDPE)

↳ Nivel de Dependencias Misionales:

19. Dirección General de Gestión de Riesgos (DGGG)

19. Comisión Nacional de  
Asesoría - Gestión de Riesgos  
2024 - 2025

**Misión:** Gestionar y reducir los riesgos de desastres de el país a través de políticas, los planes, normas y procedimientos, apoyados en la tecnología y ciencia.

**Visión:** Ser el líder nacional en el país y alcanzar normativas y procedimientos de la gestión y reducción de riesgos de desastres.



Secretaría General

**Notificación Resolutive SEM N° 770/2021**

POR LA CUAL SE APRUEBA LA POLÍTICA Y PROCEDIMIENTOS PARA LA OPERACIÓN DEL COMANDO INSTITUCIONAL EN LA VIGILANCIA Y PARA LA ATENCIÓN DEL SERVIDOR PÚBLICO EN LA VIGILANCIA DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, DE LA SECRETARÍA NACIONAL, DEPENDIENTE DE LA PRESIDENCIA DE LA REPÚBLICA.

**Nivel de Dependencias Estratégicas**

19. Departamento de Auditoría de Gestión:

*[Handwritten signature]*

Delmarita González  
Jefe de Auditoría de Gestión  
Departamento de Auditoría de Gestión

20. Asesoría Técnica

• Ricardo Alcides Nolasca Gardo:

*[Handwritten signature]*

• Aldo César Echeverría Amarilla:

21. Departamento de Prensa:

José JORDAN MARTÍNEZ

Jefe de Prensa - SEM

22. Departamento de Acceso a la Información Pública:

*[Handwritten signature]*

23. Departamento de Archivo:

24. Departamento de Servicios Tácticos:

Roberto R. Rodríguez  
Jefe de Planeación y Análisis  
Departamento de Servicios Tácticos

25. Dirección de Transporte Terrestre, Agua y Naval:

26. Departamento de Operaciones, Mantenimiento y Admisión:

27. Coordinación Administrativa:

Henry Quiroga  
Jefe de Planeación Operativa  
Departamento de Operaciones, Mantenimiento y Admisión

28. Dirección de Planificación Operativa:

29. Departamento de Depósitos de Bienes e Insumos Estratégicos:

• Belarmino Arbórizo Galeano Medina:

• Daniel Alfredo Mendoza Castro:

30. Dirección Financiera

*[Handwritten signature]*

31. Departamento de Contabilidad:

Roberto López Portillo  
Jefe de Contabilidad de Gestión  
Departamento de Contabilidad

32. Departamento de Rendición de Cuentas:

23-09-2021

33. Departamento de Tesorería:

ANA ANA GALBANO  
Jefe de Tesorería  
Departamento de Tesorería

23-09-2021

**Misión:** Gestionar y reducir los riesgos de default de la población, en su nivel, recursos y patrimonio, a través de innovaciones y tecnologías.

**Visión:** Ser el más seguro de la población económica y comercial de la gestión y producción de riesgos de default.



SINERGIA NACIONAL  
SISTEMA NACIONAL DE EMERGENCIAS  
NACIONAL

■ TETĀ REKUĀI  
■ GOBIERNO NACIONAL

Paraguay  
de la gente

34. Dirección Administrativa:

*[Handwritten signature]*  
Secretaría General

SONIA ARCE

Jefe

35. Departamento de Patrimonio:

*[Handwritten signature]*

Jefe de Depto.

36. Departamento de Servicios Generales e Infraestructura:

*[Handwritten signature]*

37. Departamento de Depósitos de Útiles de Oficina:

*[Handwritten signature]*

38. Dirección General de Gestión de Riesgos (DGGG):

*[Handwritten signature]*

28/09/2021

39. Coordinación de Control Interno:

*[Handwritten signature]*

23/09/2021

40. Departamento de Control de Cumplimiento Contractual:

*[Handwritten signature]*

23/09/2021

41. Departamento de Proceso de Contratación:

*[Handwritten signature]*

28/09/2021

42. Departamento de Personal:

*[Handwritten signature]*

EDUARDO FERRARI GARCIA ACOSTA

Jefe de Depto.

20/09/2021

43. Departamento de Médicos:

*[Handwritten signature]*

Jefe de Depto.

44. Departamento de Capacitación del Personal:

*[Handwritten signature]*

45. Departamento del Bienestar del Personal:

*[Handwritten signature]*

46. Dirección de Fortalecimiento y Asistencia Técnica:

Jefe de Depto.

47. Departamento de Alerta Temprana:

Jefe de Depto.

48. Departamento de Recuperación Temprana:

Jefe de Depto.

49. Dirección de Preparación:

*[Handwritten signature]*

50. Departamento de Operaciones en Terreno:

*[Handwritten signature]*

51. Departamento de Pre-qualificación:

Diego Daniel Cardozo

Jefe de Depto.

52. Departamento de Evaluación de Daños y Análisis de Necesidades (DAN):

*[Handwritten signature]*

Misión: Decidir y reducir los riesgos de desastres en el país a través de políticas con acciones concertadas y participativas, que utilicen asociaciones y tecnología.

Visión: Ser el más eficaz del país; reducir material e intencional de la gente e reducción de riesgos de desastres.