TABLA DE CONTENIDO

1. INTRODUCIÓN 2

2. DEFINICIONES 2

3. OBJETIVO 5

4. ALCANCE 5

5. DESARROLLO 6

5.1 POLÍTICA CONTROL DE ACCESO 6

5.2 POLÍTICA DE COPIAS DE SEGURIDAD 8

5.3 POLÍTICA GESTIÓN DE LLAVES CRIPTOGRÁFICOS 10

5.4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES 11

5.5 POLÍTICA DISPOSITIVOS MÓVILES 14

5.6 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA 16

5.7 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS 17

5.8 POLÍTICA ACCESO REMOTO 18

5.9 POLÍTICA TRANSFERENCIA DE LA INFORMACIÓN 20

5.10 **POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES** 22

5.11 TRANSPARENCIA DE INFORMACIÓN PÚBLICA BAJO LA LEY 1712 DE 2014 29

5.12 CONTROL OPERACIONAL PARA LA SEGURIDAD DE LA INFORMACIÓN 39

1. INTRODUCIÓN

En el presente documento se establecen las políticas y procedimientos que serán pilar de cumplimiento para la Unidad Nacional para la Gestión del Riesgo de Desastres (UNGRD), de acuerdo a lo establecido en los requisitos de la NTC:ISO:27001:2013, así como la Ley de Protección de Datos Personales - 1581 de 2012; "Por el cual se dictan disposiciones generales para la protección de datos personales[i]" y el decreto 1377 de 2013; "Por el cual se reglamenta parcialmente la Ley 1581 de 2012", sancionados por el Congreso de la República de Colombia.

Entendiendo lo anterior, y teniendo en cuenta que la UNGRD tiene la misión de dirigir, orientar y coordinar la Gestión del Riesgo de Desastres en Colombia, fortaleciendo las capacidades de las entidades públicas, privadas, comunitarias y de la sociedad en general y su visión es empoderar a las autoridades nacionales e internacionales, entidades públicas o privadas y a la sociedad; siendo referente en estándares de calidad y cooperando a la definición y construcción de una sociedad en paz, próspera y equitativa; la Unidad es responsable del tratamiento de los datos personales obtenidos en desarrollo de su objeto como entidad, dando garantía integral a ejercer el derecho de Habeas Data a todos los titulares de la información personal que se maneje al interior de la misma.

2. DEFINICIONES

Acceso Remoto: [1] En redes de computadoras acceder desde una computadora a un recurso ubicado físicamente en otra computadora, a través de una red local o externa (como internet).

Archivo. Es el conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de los datos personales.

Aviso de privacidad: Comunicación verbal o escrita generada por la UNGRD, dirigida al titular, para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables por la unidad, la forma de acceder y las finalidades del tratamiento que se pretende dar a sus datos personales.

Base de datos: Conjunto organizado de datos personales que sean objeto de tratamiento en la UNGRD.

Causahabiente: Persona que ha sucedido a otra por causa del fallecimiento de ésta (heredero).

Cifrado Asimétrico[2]: Uso de dos claves las cuales se denomina pública y privada. **La clave pública** es aquella que puede ser conocida por todos los usuarios; **la clave privada** está en custodia por su propietario y no debe ser conocida por nadie más.

[1] https://manualdeserviciosdelaweb.wikispaces.com/****ACCESO+REMOTO****

Cifrado Simétrico[3]**:** Dos o más usuarios cuentan con una sola clave secreta, está cifrará o descifrará la información transmitida a través del canal de ingreso seguro.

Clave o Contraseña: Toda forma de autenticación secreta para controlar el acceso a sistemas de información y/o red de la entidad.

Cobián Backup: Es un programa multitarea capaz de crear copias de seguridad en un equipo o en una red local. Se ejecuta sobre Windows y consume muy pocos recursos.

Contratistas de prestación de servicios: Vinculación de una persona natural en forma excepcional, para suplir actividades o labores relacionadas con la administración o funcionamiento de la entidad, o para desarrollar actividades especializadas que no puede asumir el personal de planta.

Copia de Respaldo (Backup): Es un proceso donde se copian todos los archivos que han sido modificados desde la copia de seguridad anterior.

Copia Incremental: Es un proceso donde se copian todos los archivos que han sido modificados desde la copia de seguridad anterior.

Copia Total: Es un proceso donde se copian todos los archivos y directorios seleccionados.

Criptografía: Es una técnica mediante la cual a través de una función matemática se transforman los datos con el objetivo de salvaguardar la confidencialidad, integridad, autenticidad y no repudio de la información.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas.

Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.

Dato público. Es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.

Dato semiprivado. Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.

Dato Sensible: Es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación.

Datos Abiertos. Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

---

[2] Ibíd.

[3] https://support.microsoft.com/es-co/kb/246071

Disco Duro: Dispositivo de almacenamiento de datos que emplea un sistema de grabación magnética para almacenar datos digitales.

Dispositivo Móvil: Equipos de procesamiento de información que por su tamaño permiten que sean transportados fácilmente, entre algunos se encuentran los ordenadores portátiles, teléfonos inteligentes, Tablet, entre otros.

Documento de archivo. Es el registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones.

Documento en construcción. No será considerada información pública aquella información preliminar y no definitiva, propia del proceso deliberatorio de un sujeto obligado en su calidad de tal.

Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del Responsable del Tratamiento.

Gestión documental. Es el conjunto de actividades administrativas y técnicas tendientes a la planificación, procesamiento, manejo y organización de la documentación producida y recibida por los sujetos obligados, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación.

Habeas Data: Derecho de cualquier persona a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en el banco de datos y en archivos de entidades públicas y privadas.

Hardware HSM (Hardware Security Module)[4]: Procesador de cifrado para la protección del ciclo de vida de las claves de cifrado.

Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

Información pública reservada. Es aquella información " que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

Información Pública. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Proveedor de Bienes y Servicios: Persona natural o jurídica o empresa que suministra bienes y/o presta servicios a la entidad, para su funcionamiento.

---

[4] http://www.safenet-inc.es/data-encryption/hardware-security-modules-hsms/

Publicar o Divulgar. Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión.

Responsable del tratamiento: Persona natural o jurídica, pública o privada, que por si misma o en asocio con otros, decida sobre las bases de datos y/o en tratamiento de los datos.Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.

Servidor: Es un computador cuyo propósito es proveer datos o servicios de modo que otros computadores los puedan utilizar.

Sujetos obligados. Se refiere a cualquier persona natural o jurídica, pública o privada incluida en el artículo 50 de la ley 1712 de 2014.

Teletrabajo o Trabajo Remoto:[5] Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio especifico de trabajo.

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos de carácter personal tales como la recolección, procesamiento, publicidad, almacenamiento, uso, circulación o supresión.

Usuario Especial: Es el usuario que por sus necesidades de interacción con las aplicaciones requiere de accesos o permisos especiales para acceder a las aplicaciones.

Usuario: Funcionarios y/o contratistas de la UNGRD a quien se le entrega un dispositivo móvil para la ejecución de sus labores.

3. OBJETIVO

Establecer políticas de operación para la implementación de las estrategias de seguridad de la información de la Unidad Nacional para la Gestión del Riesgo de Desastres.

4. ALCANCE

La aplicabilidad del presente manual, está definido por el alcance establecido en cada una de las políticas que lo integran.

[5] Artículo 2, Ley 1221 de 2008

5. DESARROLLO

5.1 POLÍTICA CONTROL DE ACCESO

Propósito:
Definir los lineamientos relativos al control de acceso lógico de los usuarios de la Unidad Nacional de Gestión de Riesgos de Desastres – UNGRD.

Alcance:
La política aplica a todos los funcionarios, asesores, personal de contratistas, empleados temporales y terceros que tienen acceso a los servicios de red, aplicaciones y sistemas de información de la UNGRD.

Generalidades
En esta política se definen las condiciones sobre las cuales los funcionarios, contratistas o terceros tienen acceso a la red, sistemas operativos y aplicativos de la UNGRD.

ACCESO A LA RED

- Son usuarios de red de la entidad todos los funcionarios, contratistas y terceros que se encuentren en la UNGRD.
- El acceso a la red por parte de terceros debe estar estrictamente restringido y permisible únicamente con previa autorización del profesional responsable de Soporte e Infraestructura Tecnológica.
- La gestión de contraseñas para el acceso a la red se realiza por medio de autorización del profesional responsable de Soporte e Infraestructura Tecnológica.

ACCESO A LAS APLICACIONES

- El jefe de cada dependencia de la UNGRD es quien debe realizar la solicitud de creación o asignación del usuario de las aplicaciones que requiera el funcionario o contratista.
- El responsable del Proceso de Gestión de Sistemas de Información será el encargado de la creación, modificación y desactivación de cuentas de los usuarios de acuerdo a lo establecido en el *Procedimiento de Administración de Usuarios PR-1300-GSI-02*
- La asignación y gestión de cambios de claves y/o contraseñas de cuenta, se encuentra a cargo del Administrador de la aplicación y/o Profesional responsable de Gestión de Sistemas de información.

INGRESO A LA RED CORPORATIVA

La gestión de los usuarios para el ingreso a la red corporativa de la entidad se realiza a través del Directivo Activo de Windows Server.

El ingreso a la red corporativa se encuentra protegido, mediante el inicio seguro de sesión; los funcionarios tendrán acceso a la red corporativa en función de la operación, así mismo es

responsabilidad de los funcionarios de la UNGRD que se cumpla y se asegure formalmente el acceso a los sistemas.

GESTIÓN DE CONTRASEÑAS

Con el fin de evitar el acceso no autorizado a los sistemas informáticos de la UNGRD, las contraseñas utilizadas deben cumplir con las siguientes condiciones:

- **Longitud de Contraseñas.** La longitud de las contraseñas de ingreso a equipos de cómputo debe ser mínimo de ocho caracteres, para dispositivos móviles (Teléfonos inteligentes y portátiles) se debe contar con una contraseña de cuatro números
- **Uso de Combinaciones.** Las contraseñas utilizadas por los usuarios de la red corporativa de la UNGRD deben cumplir con las siguientes condiciones:
  - Contar con al menos 8 caracteres.
  - Contener caracteres Alfabéticos (a-z, A-Z)
  - Numéricos (0-9)
  - Caracteres especiales (!@#$%^&*()_+|~- =\`{}[]:";'<>?,./) (Opcional)

RESTRICCIONES DE USO DE CONTRASEÑAS

Las contraseñas utilizadas para el acceso a los equipos de cómputo y sistemas informáticos de la UNGRD no deben utilizar cadena de caracteres duplicados, nombre de usuario del equipo, fechas de nacimiento o cualquier otro dato personal, conjuntos de letras o caracteres de fácil identificación (abcd1234).

PRIVACIDAD DE LAS CONTRASEÑAS

La contraseña de acceso a los equipos de cómputo y sistemas informáticos de la UNGRD de cada usuario, es personal e intransferible, por tanto, cada usuario se compromete a no revelar, prestar, transferir y difundir sus claves de acceso.

PERIODICIDAD DE LAS CONTRASEÑAS

Las contraseñas de acceso a los equipos de cómputo y sistemas informáticos de la UNGRD, deben ser cambiadas cada 45 días por el usuario.

No podrá coincidir con ninguna de las 5 contraseñas anteriormente definidas por el usuario.

REVISIÓN Y RETIRO DE LOS DERECHOS DE ACCESO A USUARIOS

- Los derechos de acceso a usuarios se revisan periódicamente, si se presentan cambios en los roles y/o funciones de los empleados, estos deben ser modificados por parte del Profesional responsable de Gestión de Sistemas de Información.
- La eliminación, bloqueo o retiro de acceso a usuarios en el caso de funcionarios: en vacaciones, licencias o terminación de contrato laboral, se realiza de acuerdo a lo establecido en el *Procedimiento de Administración de Usuarios PR-1300-GSI-02,*

NORMA ISO/IEC 27001:2013 ANEXO A 9.1.1
VER PROCEDIMIENTO DE ADMINISTRACIÓN DE USUARIOS SIPLAG DEL PROCESO

VER FORMATO DE SOLICITUD DE CREACIÓN O MODIFICACIÓN DE USUARIOS DE SISTEMAS DE INFORMACIÓN SIPLAG DEL PROCESO

5.2 POLÍTICA DE COPIAS DE SEGURIDAD

Propósito:
Establecer las directrices para la ejecución y restauración de las copias de seguridad de la información que se encuentra en el servidor de archivos de la UNGRD.

Alcance:
La política aplica para el respaldo de la información que se encuentra en los servidores de archivos, la cual es ingresada o modificada por todos los funcionarios, contratistas y terceros de la UNGRD.

Generalidades

Con el fin de mantener la integridad y disponibilidad de la información, las copias de respaldo se ponen a prueba mediante la restauración aleatoria de algún archivo al que se le haya realizado la copia de respaldo. Si la restauración del backup es exitosa, se documenta en la bitácora de respaldo.

La **UNGRD** ha establecido los siguientes lineamientos generales para el resguardo de la información de la entidad:

COPIAS DE SEGURIDAD SERVIDOR DE ARCHIVOS, BASE DE DATOS Y SISTEMAS OPERATIVOS

- Realiza y verifica que las copias de seguridad se actualicen con la periodicidad y los requerimientos definidos.
- Para toda la información que se encuentra en el servidor de archivos, se realiza una copia de respaldo o backup de forma incremental de acuerdo a lo establecido en el *Procedimiento de Copias De Seguridad Incremental Y Total Pr-1603-Sis-01*
- Para las copias de seguridad la UNGRD utiliza la herramienta *Cobian Backup.*
- Se realiza copia de respaldo total mensual por medio de la herramienta *Cobian Backup* contenida en el servidor de archivos a un disco duro externo.
- El disco duro externo se identifica por medio de la fecha en la cual se realizó la copia total del archivo, con el fin de contar con la información necesaria para identificar cada una de ellas y administrarlas de forma adecuada.
- Los discos duros externos se almacenan en un lugar seguro designado por la entidad, el cual debe cumplir con las condiciones de seguridad y ambientales que permitan mantener la confidencialidad e integridad de las mismas y a su vez se encuentren disponibles cuando sean requeridas.

RESTAURACIÓN DE LAS COPIAS DE RESPALDO

- El funcionario y/o contratista de la UNGRD que requiera de un archivo a restaurar, deberá realizar la solicitud directamente al Profesional del área de (Soporte) Gestión de Infraestructura Tecnológica por medio de correo electrónico.
- La restauración de las Bases de Datos y Sistemas Operativos, se debe tener en cuenta lo establecido en el *Procedimiento de Continuidad de la Operación y Seguridad de la Información.*

COPIAS DE SEGURIDAD CORREO ELECTRÓNICO

- Las copias de seguridad de correo electrónico corporativo de la UNGRD, se realiza cuando el funcionario y/o contratista finaliza la relación contractual con la entidad.
- La ejecución de la copia de seguridad se realiza por medio del software SYLPHEED utilizando la licencia OPEN SOURCE GNU GPL.
- Para el respaldo de los archivos (Documentos de cada usuario y archivos PST del correo electrónico) de los funcionarios, se crea un archivo con el nombre del usuario.

NORMA ISO/IEC 27001:2013 ANEXO A 12.3.1
VER PROCEDIMIENTO DE COPIAS DE SEGURIDAD INCREMENTAL Y TOTAL SIPLAG DEL PROCESO

5.3 POLÍTICA GESTIÓN DE LLAVES CRIPTOGRÁFICOS

Propósito:
Definir las normas que se deben aplicar para la generación, protección y tiempo de vida de las llaves criptográficas utilizadas por la UNGRD.

Alcance:
La política aplica para todos los equipos móviles (portátiles y teléfonos inteligentes) pertenecientes a la UNGRD.

CONTROLES CRIPTOGRÁFICOS

La UNGRD ha establecida una herramienta de cifrado, con el fin de salvaguardar la confidencialidad e integridad de la información contenida en los computadores portátiles que pertenecen a la entidad y son utilizados fuera de ella. Para esto cuenta con un inventario de equipos portátiles cifrados.

Los propietarios de los activos individuales sobre los cuales se aplican controles criptográficos, son los responsables por la correcta aplicación de los controles criptográficos particulares.

GENERACIÓN DE LLAVES

El software de cifrado genera una primera clave de forma aleatoria al momento de su instalación y el usuario del equipo asigna una segunda clave.

Todos los funcionarios que tengan a su cargo equipos portátiles de la UNGRD deben al momento de asignar la clave al software de cifrado tener en cuenta las condiciones para la asignación de contraseñas según *Política de Dispositivos Móviles.*

ALMACENAMIENTO

El software de cifrado se almacena local y temporalmente en el disco del equipo portátil.

GESTIÓN DE CLAVES CRIPTOGRÁFICAS TELÉFONOS INTELIGENTES

- El mecanismo a través del cual se cifraran los teléfonos inteligentes pertenecientes a la entidad que poseen sistema operativo android, será el que por defecto tengan dichos dispositivos.
- El usuario del teléfono inteligente perteneciente a la UNGRD debe configurar un patrón, garantizando la confidencialidad e integridad de la información contenida dentro del dispositivo donde maneje información sensible de la entidad.

NORMA ISO/IEC 27001:2013 ANEXO A 10.1.2
POLÍTICA DE DISPOSITIVOS MÓVILES

5.4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES

Propósito:
Definir los requisitos de seguridad de la información entre la UNIDAD NACIONAL DE GESTIÓN DE RIESGOS DE DESASTRES – UNGRD sus proveedores y contratistas con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

Alcance:
La política aplica a todos los proveedores, contratistas y terceros que tengan relación con la Unidad.

Generalidades

Para la mitigación de los posibles riesgos asociados con el acceso de proveedores a los activos de información de la entidad, deben ser acordados y documentados entre la UNGRD los proveedores o contratistas, los requisitos de seguridad de la información con el fin de asegurar la protección de dichos accesos.

- Los proveedores y contratistas tendrán acceso limitado a información reservada y confidencial de la UNGRD. Si fuese necesario el suministro de esta información, se deberá cumplir con medidas de seguridad que garantice la no divulgación y/o modificación de dicha información.
- Los contratistas no podrán tener acceso a áreas o zonas donde se encuentre información sensible en la entidad. Sí fuera necesario su ingreso a determinadas áreas, será necesaria la autorización de un funcionario de la entidad, el cual debe acompañar al contratista durante el tiempo que este permanezca en dicha área.

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN CON PROVEEDORES

- Los proveedores y contratistas que tengan relaciones contractuales con la entidad, se les incluirá dentro de su contrato una cláusula de confidencialidad de la información.
- Para la contratación de los proveedores y contratistas se realizará según lo establecido en el *Manual de Contratación Resolución Número 807 de 2014.*
- Los proveedores deberán ser evaluados según el formato de *Criterios para la Evaluación de Proveedores y Contratistas FR- 1604-GCON-13.*

TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON LOS PROVEEDORES

- Los controles físicos y lógicos con los cuales el proveedor y contratista de la UNGRD debe cumplir, tendrán que estar documentados y aprobados, además de ser de conocimiento de ambas partes.
- La UNGRD tiene establecida una lista detallada del personal autorizado por el proveedor especificando quienes puedan tener acceso a la información de la entidad o recibirla de ella.
- Para la modificación y/o adquisición de software el proveedor deberá realizar pruebas con el solicitante del nuevo desarrollo o cambio en alguna aplicación existente con el fin de validar la funcionalidad y disponibilidad de la aplicación. Adicionalmente el desarrollador deberá entregar un manual de usuario con las especificaciones técnicas y funcionales de la aplicación.
- Los proveedores notificarán al oficial de seguridad de la información o quien haga sus veces sobre los incidentes de seguridad de la información que hayan sucedido o materializado en el marco del servicio prestado, así mismo reportará a la entidad la gestión y acciones tomadas para el cierre del incidente.
- La UNGRD mantendrá actualizada la información correspondiente de la persona de contacto que los proveedores tenga asignada con respecto a seguridad de la información.

CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

- Para toda adquisición de software y hardware realizada por la UNGRD, el comité de seguridad de la información, es el responsable de definir los requisitos de seguridad, los cuales deben quedar documentados y aprobados por las partes en el contrato u acuerdo.
- Los proveedores y contratistas que acuerdan externamente servicios de otras compañías, y que estén relacionados con el suministro de tecnología de información y comunicación que prestan a la UNGRD, deberán proporcionar información sobre los requisitos y prácticas de seguridad, a quienes se les realizará el respectivo seguimiento por parte de la UNGRD, según los acuerdos iniciales establecidos con el proveedor del servicio.

SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES

Asegura que los términos y condiciones de seguridad de la información en los acuerdos realizados entre la UNGRD con los proveedores y contratistas se cumplan, así como los incidentes y problemas de seguridad que se generen y que se deben gestionar oportunamente para lo cual:

- Se realizará seguimiento y revisión a los productos y servicios prestados por los proveedores de acuerdo a las condiciones iniciales establecidas dentro del contrato.
- De acuerdo al proveedor o contratista, se definirá los mecanismos que permitan realizar el seguimiento, dependiendo de la criticidad de la información que maneja, evaluando criterios de seguridad física y lógica, así como algunos requerimientos del estándar ISO/IEC 27001.
- De ser posible y si aplica, para proveedores de alto impacto en seguridad de la información se evalúa el plan de continuidad del proveedor.
- El seguimiento o auditoria a los procesos y controles a los proveedores se realizará con una periodicidad no mayor a un año.

GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES

Cuando se presentan cambios como:

- Acuerdos con los proveedores; tanto el proveedor o contratista como la UNGRD deben establecer y notificar los cambios que se generen o se estimen realizar con respecto a los acuerdos contractuales iniciales.
- Con respecto a los cambios que la UNGRD requiera implementar como: mejoras al servicio ofrecido; desarrollo de nuevas aplicaciones y sistemas; actualizaciones o modificaciones a las políticas de la entidad, será el comité de seguridad de la información quien definirá los lineamientos de seguridad que se deben aplicar para cumplir con los requisitos del SGSI.
- Todo cambio en el servicio que el proveedor o contratista desee o requiera implementar como: uso de nuevas tecnologías, cambios y mejoras en las redes, versiones o ediciones recientes, herramientas nuevas y ambientes de desarrollo, deben ser informados a la UNGRD antes de ser implementados.

NORMA ISO/IEC 27001:2013 ANEXO A 15
VER MANUAL DE CONTRATACIÓN RESOLUCIÓN 807 DE 2014 SIPLAG PROCESO DE CONTRATACIÓN
VER FORMATO DE CRITERIOS PARA LA EVALUACIÓN DE PROVEEDORES Y CONTRATISTAS

5.5 POLÍTICA DISPOSITIVOS MÓVILES

Propósito:
Establecer las normas sobre el uso de los dispositivos móviles (computadores portátiles y teléfonos inteligentes) institucionales de la Unidad Nacional para la Gestión del Riesgo de Desastres -UNGRD, velando por su uso adecuado, responsable y sus mejores prácticas.

Alcance:
La política aplica para todos los funcionarios y/o contratistas de la UNGRD que tengan asignado dispositivos móviles (computadores portátiles y teléfonos inteligentes) pertenecientes a la entidad para el desarrollo de las actividades propias de su función.

Generalidades

La **UNGRD** proporciona las condiciones para el manejo de los dispositivos móviles (computadores portátiles y teléfonos inteligentes) Institucionales y personales que hagan uso de los servicios de la entidad. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la entidad.

La asignación de los dispositivos móviles a los funcionarios y/o contratistas se realiza según el *Procedimiento de Asignación de Equipos De Cómputo PR-1603-Sis-02* y por medio del *Formato Solicitud de Materiales FR-1603-GBI-04.*

USO DE CONTRASEÑAS

- Todos los dispositivos móviles pertenecientes a la UNGRD que se encuentren asignados a algún funcionario y/o contratista, debe contar con una contraseña o clave (password) que impida el acceso directo a la información que este contiene.
- Las contraseñas utilizadas para el acceso a los dispositivos móviles no deben utilizar cadena de caracteres duplicados, nombre de usuario del equipo, fechas de nacimiento o cualquier otro dato personal, conjuntos de letras o caracteres de fácil identificación (abcd1234).

PROTECCIÓN FÍSICA

- Todos los dispositivos móviles de la UNGRD deben estar registrados e inventariados.
- Los dispositivos móviles asignados a funcionarios y/o contratistas de la unidad son personales e intransferibles.
- Los usuarios de equipos portátiles que pertenezcan a la UNGRD deben mantener una seguridad física dentro de las instalaciones de la entidad, por medio del uso de guayas de seguridad.
- En caso de pérdida o robo del equipo, el funcionario deberá informar inmediatamente al comité de seguridad o quien haga sus veces quienes tomarán las medidas de seguridad necesarias.
- Los equipos asignados en particular aquellos que almacenen información sensible no deben ser entregados a terceros

INSTALACIÓN Y CONFIGURACIÓN DE APLICACIONES

- Está prohibida la instalación de aplicaciones en los dispositivos móviles que pertenezcan a la UNGRD por parte de los funcionarios o terceros, de ser necesario el uso de las aplicaciones realizará la solicitud por medio de su jefe inmediato y firmara el documento correspondiente donde se define la responsabilidad sobre el uso de las mismas.
- El proceso de instalación y configuración de las aplicaciones en los dispositivos móviles, solo puede ser realizado por los profesionales designados por el Grupo de Apoyo Administrativo previa evaluación y pertinencia de la misma.
- El aseguramiento de la administración de los dispositivos móviles, pertenecientes a la UNGRD, será administrado por el profesional designado del Grupo de Apoyo Administrativo.

SEGURIDAD DEL SISTEMA OPERATIVO

- Para garantizar la disponibilidad, confidencialidad e integridad de la información contenida en los dispositivos móviles, el profesional designado del Grupo de Apoyo Administrativo será quien otorgará los respectivos permisos.

SINCRONIZACIÓN DE CORREO ELECTRÓNICO EN DISPOSITIVOS MÓVILES

- Está prohibido sincronizar la cuenta de correo electrónico corporativo en el equipo móvil de uso personal, excepto con autorización expresa del Coordinador o Jefe del área, en dado caso de tener el permiso correspondiente se debe firmar el documento donde se establecen las políticas sobre el uso del mismo.

REGISTRO DE INGRESO Y SALIDA DE EQUIPO DE CÓMPUTO

- Los equipos de cómputo que ingresen o salgan de las instalaciones de UNGRD por parte de personal externo deben ser registrados en la planilla de ingreso y salida de visitantes.

NORMAS DIRIGIDAS A TODOS LOS USUARIOS

- No dejar desatendidos los equipos.
- No llamar la atención acerca de portar un equipo valioso.
- No colocar identificaciones de la Organización en el dispositivo, salvo los estrictamente necesarios.
- No colocar datos de contacto técnico en el dispositivo.
- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles asignados.

NORMA ISO/IEC 27001:2013 ANEXO A 6.2.1
VER PROCEDIMIENTO DE ASIGNACIÓN DE EQUIPO DE COMPUTO SIPLAG DEL PROCESO
VER FORMATO SOLICITUD DE MATERIALES

5.6 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

Propósito:
Establecer por parte de la Unidad Nacional Gestión de Riesgos de Desastres- UNGRD, normas de escritorios limpios para proteger documentos físicos y dispositivos de almacenamiento removibles, del mismo modo normas de pantallas limpias para toda la entidad, a fin de reducir los riesgos de acceso no autorizado, perdida o daño de la información; y de esta manera responsabilizar a todos los funcionarios de la entidad sobre el cuidado de los activos de Información de la entidad.

Alcance:
La presente política aplica a todos los funcionarios, contratistas y terceros que tengan acceso a la información de la UNGRD.

Generalidades
Con el fin de garantizar la confidencialidad e integridad de la información todos los funcionarios personal contratista y empleados temporales, deben cumplir con las siguientes disposiciones:

ESCRITORIOS LIMPIOS

- Todos los funcionarios deben mantener su estación de trabajo organizada.
- El funcionario debe mantener su escritorio libre de información, propia de la UNGRD, susceptible de ser alcanzada, copiada o utilizada por terceros o por personal sin autorización para su uso o conocimiento.
- Todo documento, medio magnético u óptico removible que contenga información confidencial o sensible, debe ser almacenado en lugares seguros.
- En las áreas de atención al público, la información interna debe tener el mismo tratamiento de la información confidencial o sensible.
- Al finalizar la jornada de trabajo, el funcionario o externo debe guardar en un lugar seguro los documentos o medios que contengan información reservada, confidencial o de uso interno.
- Toda información impresa confidencial o sensible, debe ser retirada de manera inmediata de la impresora y no se debe dejar en el escritorio sin custodia.

PANTALLA LIMPIA

- El funcionario debe Bloquear el equipo de cómputo cuando sea necesario ausentarse del puesto de trabajo, para esto se recomienda el uso de los comandos: CTRL + ALT + SUPR o WINDOWS + L.
- Los funcionarios no deben almacenar información sensible en el escritorio de los equipos de cómputo.
- Los equipos de cómputo deben tener aplicado un fondo de pantalla corporativo establecido por la UNGRD
- Todos los equipos de cómputo deben tener configurado bloqueo automático por inactividad, en la UNGRD el periodo de inactividad está definido en 3 minutos.
- Los funcionarios deben Almacenar la información de forma ordenada, haciendo uso de carpetas y jerarquías de almacenamiento.
- En lo posible los funcionarios de la UNGRD deben evitar almacenar videos, fotografías o información personal en los equipos de cómputo asignados.

NORMA ISO/IEC 27001:2013 ANEXO A 11.2.9

5.7 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

Propósito:
Determinar los lineamientos para el uso de controles criptográficos con el fin de proteger la confidencialidad, integridad y autenticidad de la información de la Unidad Nacional para la Gestión de Riesgos de Desastres - UNGRD.

Alcance:
La política aplica para los controles criptográficos utilizados como mecanismo de autenticación ante los dispositivos móviles (portátiles y teléfonos inteligentes) pertenecientes a la UNGRD.

Generalidades:

La UNGRD utiliza técnicas criptográficas para proteger la información confidencial y reservada de la entidad, salvaguardando de esta manera la confidencialidad e integridad de la información en los dispositivos móviles suministrados a los funcionarios de la entidad.

- Los computadores portátiles que pertenezcan y estén autorizados para salir de la entidad deben contar con una herramienta de cifrado, con el fin de proteger la información almacenada en los discos duros de estos equipos, salvaguardando así la confidencialidad de la información almacenada.
- Los usuarios de equipos portátiles que pertenezcan a la UNGRD deben mantener una seguridad física dentro de las instalaciones de la entidad, por medio del uso de guayas de seguridad.
- Se realiza la configuración de una herramienta de cifrado seleccionando la partición del disco que se quiere cifrar y donde se almacenaran los archivos a resguardar.
- Los usuarios autorizados se autenticaran a través de contraseñas las cuales deben cumplir con las reglas sobre la gestión de claves (longitud mínimo de 8 caracteres, inclusión mayúsculas y minúsculas, incluya caracteres especiales como (*?\!°/&%$) entre otros, no incluya nombre propios, números de identificación)
- Para los dispositivos móviles tipo teléfonos inteligentes, se recomienda usar patrones de bloqueo definidos por el usuario asignado del dispositivo y bajo su total responsabilidad**.**

NORMA ISO/IEC 27001:2013 ANEXO A 10.1.1 //POLÍTICA DE DISPOSITIVOS MÓVILES //POLÍTICA DE GESTIÓN DE LLAVES CRIPTOGRÁFICAS

5.8 POLÍTICA ACCESO REMOTO

Propósito:
Determinar las condiciones y medidas de seguridad para el acceso remoto de los funcionarios de la Unidad Nacional para la Gestión del Riesgo de Desastres - UNGRD.

Alcance:
Está política comprende el cumplimiento por parte de los funcionarios autorizados por la UNGRD para realizar conexiones remotas con el fin de ejecutar tareas relacionadas con sus responsabilidades ante la unidad.

Generalidades:

- La conexión remota, se encuentra restringida para todos los funcionarios de la UNGRD, excepto aquellos usuarios que justifican esta necesidad a través del coordinador y/o jefe de área y obtienen la autorización correspondiente por parte del comité de seguridad de la información y/o Grupo de Apoyo Administrativo de la Unidad.
- Se tiene definido un listado de los funcionarios aprobado por el comité de seguridad y/o Grupo de Apoyo Administrativo, que tienen derecho a este acceso para el desempeño de sus actividades, de igual manera el funcionario diligencia el Formato de *FR-GSI-1300-02 usuarios especiales.* Este listado se debe estar revisando y actualizando de forma frecuente con el fin de mantener la información de conexiones remotas lo más actualizada posible.

CONDICIONES DE ACCESO

- Los funcionarios o usuarios autorizados con el acceso remoto, deben firmar el formato *FR-GSI-1300-02* donde se establece la autorización del acceso, responsabilidades y condiciones de uso necesarias para su conexión.
- Todo funcionario con autorización de acceso remoto posee un usuario y contraseña para el acceso al equipo y los sistemas de información.
- Las contraseñas utilizadas para el acceso remoto al servidor remoto y sistemas informáticos de la UNGRD no deben utilizar cadena de caracteres duplicados, nombre de usuario del equipo, fechas de nacimiento o cualquier otro dato personal, conjuntos de letras o caracteres de fácil identificación (abcd1234).
- El soporte y mantenimiento del equipo del funcionario autorizado con trabajo remoto, se realiza por medio del área de soporte e infraestructura tecnológica de la unidad.

RESTRICCIONES

- Toda conexión remota a la plataforma tecnológica de la entidad se hará mediante un método de conexión segura, equipos previamente identificados y privados.
- Se tiene prohíbe, sin excepción alguna, la conexión remota desde redes públicas (cafés internet, hoteles sin acceso controlado, centro comerciales, entre otros)
- La contraseña de acceso a los equipos de cómputo y sistemas informáticos de la UNGRD de cada usuario, es personal e intransferible, por lo anterior, cada uno de los usuarios se compromete a no revelar, prestar, transferir ni difundir sus claves de acceso.

COPIAS DE RESPALDO
Las copias de respaldo o backup se realizan por medio de la sincronización del equipo al momento de conectarse a la red de la UNGRD, se utiliza una copia de respaldo o backup incremental.

REVISIONES

Las conexiones remotas asignadas se revisaran por lo menos cada seis meses para renovar los permisos asignados, por parte de comité de seguridad de la información.

En caso que el funcionario cambie de roles y/o responsabilidades dentro de la entidad, el comité de seguridad de la información de la UNGRD revisará los respectivos accesos, los revocará, actualizará o mantendrá según sea el caso.

NORMA ISO/IEC 27001:2013 ANEXO A 6.2.2

VER ACTA O FORMATO DE ASIGNACIÓN DE EQUIPOS

5.9 POLÍTICA TRANSFERENCIA DE LA INFORMACIÓN

Propósito:
Definir los lineamientos y controles necesarios para llevar a cabo una correcta transferencia de información dentro de la entidad y/o con partes externas, con el fin de mantener la seguridad de la información, a través de los diferentes tipos de comunicación o transferencia definidos por la UNGRD.

Alcance:
La política aplica a todos los funcionarios, contratistas y terceros, va desde la necesidad de transferir información hasta cuando llega al destinatario de la información.

Generalidades
Con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información en los diferentes medios de transferencia de información, en la UNGRD se definió el manejo de información a través del Directorio Activo, que tiene las siguientes condiciones:

CONTROL DE REDES

Ningún colaborador de la UNGRD puede establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la entidad, sin la previa autorización del Oficial de Seguridad de la Información o Profesional Responsable.

CORREO ELECTRÓNICO

- Los colaboradores de la UNGRD son responsables de las actividades realizadas con su cuenta de correo institucional.
- Solamente se podrá enviar correos a través de la cuenta de correo institucional.
- Todos los mensajes generados o manejados a través de la plataforma de correo electrónico Google Apps con que cuenta la UNGRD, incluyendo las copias de respaldo, se consideran propiedad de la UNGRD.
- Está prohibido utilizar el sistema de correo para el desarrollo de actividades políticas, comerciales o de entretenimiento o para la transmisión de mensajes vulgares u obscenos.
- Como política del directorio activo está prohibido el uso de correos personales (Hotmail, Yahoo, entre otros), con el principal objetivo de gestionar el riesgo de fuga de información.
- En el caso de recibir un correo electrónico de un destinatario desconocido, este no debe ser abierto y se debe notificar por medio de correo al Oficial de Seguridad de la información o quien haga sus veces en la entidad, de manera inmediata, para evitar una posible afectación de un malware, rootkit o cualquier tipo de infección en el sistema, en caso de contener algún virus.
- Los colaboradores de la UNGRD en caso de ser necesarios, están sujetos a un monitoreo del uso de correo electrónico por parte del Oficial de Seguridad de la Información o quien haga sus veces en la entidad.
- Es de obligatorio cumplimiento configurar la cuenta de correo electrónico utilizando el protocolo IMAP4.
- Como adjunto en cada correo electrónico se incluye un aviso de confidencialidad, de manejo de datos personales de acuerdo a la ley 1581 del 2012 y 1266 del 2008 de Habeas Data.

INTERNET

- El acceso a internet suministrado a los funcionarios y/o contratistas de la UNGRD es de uso exclusivo para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.
- Todos los accesos a Internet de los funcionarios y/o contratistas deben ser realizados a través de los canales de acceso suministrados por la UNGRD, en caso de necesitar una conexión a Internet alterna o especial, se debe solicitar la autorización del Oficial de Seguridad de la Información o quien haga sus veces en la entidad.
- Es prohibido el uso del internet para acceder, crear, copiar, distribuir material o enviar mensajes obscenos, pornográficos, entre otros o mensajes que instiguen violencia o amenaza de cualquier tipo.
- Los funcionarios, contratistas y terceros al acceder a internet están sujetos a un monitoreo de las actividades que realizan, a través del Oficial de Seguridad de la Información o quien haga sus veces en la Unidad.
- Los usuarios que tienen acceso a Internet a través de los recursos de la entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.

TRANSFERENCIA DE INFORMACIÓN CON TERCEROS

- Para el envío de información confidencial de la entidad por medio electrónico se enviará en formato PDF o un archivo comprimido .ZIP con clave, la cual será por defecto el número de identificación del tercero a quien se le envié la información. Para lo cual se tiene definida una guía donde se enumera el paso a paso para comprimir los archivos según el tipo de información a transferir.
- Los funcionarios y contratistas no deben enviar correos electrónicos a partes externas sin tener la firma establecida.
- Los terceros deben cumplir con las políticas de seguridad de la información, que tengan algún tipo de relación con la transferencia de información en medios físicos.
- Todo correo electrónico y/o medio físico con destino a terceros que contenga información confidencial y/o reservada, no debe tener ningún contenido en el cuerpo del correo que haga referencia a la clave de acceso. Esta contraseña podrá ser suministrada a través de contacto telefónico y/o correo electrónico posterior a su envío sin ningún adjunto.
- Para los Acuerdos de Confidencialidad establecidos entre la UNGRD y terceros, el Oficial de Seguridad de la Información realizará una revisión anual, evaluando la pertinencia de los mismos, con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

NORMA ISO/IEC 27001:2013 ANEXO A 13.2.1
VER MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA SIPLAG DEL PROCESO

5.10 POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES

Alcance:
La presente política será aplicable a los datos personales recibidos y registrados en cualquier base de datos de LA UNGRD cuyo titular sea una persona natural, que requiere la atención de una solicitud, la presentación de una queja o reclamo, o para acceder a los mecanismos interactivos que posee la Entidad. Así mismo, otra fuente de recepción de datos personales proviene de la información recolectada en cumplimiento de las funciones asignadas a la Entidad, con motivo de la atención de las emergencias causadas por los eventos naturales o antropogénicos no intencionales.

5.10.1 PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES

Para dar cumplimiento a la política de Protección de Datos Personales, se tendrán en cuenta los siguientes principios, en los procesos de recolección, uso y tratamiento de datos personales.

Acceso y Circulación
El contenido de las bases de datos no será publicado en internet sin el control respectivo, u autorización en caso de requerirla, a no ser que este sea de naturaleza pública.

Confidencialidad
Las personas que participen en el proceso de tratamiento de datos personales, deben garantizar la reserva de la información, inclusive después de la relación con la entidad, o de acuerdo a como este establecido en el Sistema de Gestión de Seguridad de la Información de la UNGRD.
El incumplimiento de este principio será sancionado de acuerdo a lo establecido en el numeral 7.2.3 del Anexo A de la norma técnica colombiana NTC-ISO27001:2013.

Finalidad
En la UNGRD, el tratamiento de los datos personales recogidos obedece a una finalidad, de la cual se informar al titular de los mismos.
En lo referente a la recolección de datos personales, la UNGRD se limitará a los datos estrictamente necesarios.

Legalidad
En la UNGRD, el tratamiento de los datos personales, estan sujetos a lo descrito por la Ley 1581 de 2012.

Libertad
El tratamiento de los datos personales será realizado bajo consentimiento previo, expreso e informado del titular de la información, garantizando los derechos estipulados en la Constitución de Colombia.

Seguridad
La información sujeta de tratamiento se protege mediante el uso de medidas técnicas, humanas y administrativas necesarias para evitar adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la misma.

Transparencia
El titular tiene derecho a obtener la información en el momento que este lo requiera sin restricción alguna, bajo los parámetros establecidos en la Ley de Protección de Datos Personales.

Veracidad o Calidad
La información sujeta de tratamiento tratada es veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de información parcial e inexacta de los titulares.

5.10.2 TRATAMIENTO DE DATOS PERSONALES

Con el fin de dar cumplimiento a lo establecido en la Ley 1581 de 2012 y al Decreto reglamentario 1377 de 2013, la UNGRD establece los siguientes tratamientos:

Tratamiento de datos públicos
La UNGRD, solo publica en sus canales de comunicación, los datos personales que se encuentren contemplados en la Ley con el fin de no incurrir en incumplimento del derecho fundamental de Habeas Data.

Tratamiento de datos sensibles
La UNGRD realizará el tratamiento de datos personales sensibles para lo estrictamente necesario, solicitando consentimiento previo y expreso a los titulares informándoles sobre la finalidad exclusiva para su tratamiento.
La Unidad cataloga datos como sensibles, según lo establecido en la ley.
La Unidad no realizará el tratamiento de datos personales de acuerdo a las prohibiciones descritas en la ley.

Tratamiento de datos de menores de edad.
La UNGRD realizará el tratamiento de datos personales de menores de edad respetando sus derechos y únicamente se hará uso de los mismos cuando estos sean definidos como de naturaleza pública o cuenten con la autorización respectiva.
Para el tratamiento de datos de menores, la UNGRD se compromete a capacitar al interior de la Unidad respecto de los riesgos de la publicación no indebida de información relacionada con menores de edad, con el fin de dar cumplimiento estricto a lo definido por la Ley 1581 de 2012 y el Decreto 1377 de 2013, garantizando el derecho fundamental de estos.

5.10.3 DERECHOS DE LOS TITULARES

En virtud de la política de tratamiento y protección de datos personales, la UNGRD garantiza a los titulares de los datos personales los siguientes derechos:

- Acceder, conocer, actualizar y rectificar sus datos personales frente a la Unidad en su condición de responsable del tratamiento de datos personales.
- Solicitar prueba de la existencia de la autorización otorgada a la Unidad, salvo los casos exceptuados por la Ley.
- Ser informado por Unidad, previa solicitud, respecto del uso que le ha dado a sus datos personales.
- Presentar ante la Super-Intendencia de Industria y Comercio, las quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y normas referentes al derecho de habeas Data.
- Modificar, revocar la autorización y/o solicitar la supresión de los datos personales, cuando el tratamiento no respete los principios, derechos y garantías constitucionales y legales vigentes.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

5.10.4 DEBERES DE LA UNIDAD NACIONAL PARA LA GESTIÓN DEL RIESGO DE DESASTRES RESPECTO AL TRATAMIENTO DE LOS DATOS PERSONALES.

En virtud del cumplimiento de la presente política de tratamiento de datos personales, son deberes de la UNGRD, los siguientes, sin prejuicio de las disposiciones previstas por la Ley.

- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- Solicitar y conservar, copia de la respectiva autorización otorgada por el titular;
- Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
- Actualizar la información, notificando oportunamente, todas las novedades respecto de los datos solicitados.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente.
- Respetar las condiciones de seguridad y privacidad de la información del titular.
- Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;
- Informar a solicitud del titular sobre el uso dado a sus datos;
- Informar a la autoridad de protección de datos (Superintendencia de Industria y Comercio – Delegatura de Protección de Datos -) cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- Adoptar esta política y procedimiento para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;
- Cumplir los requerimientos e instrucciones que imparta la Superintendencia de Industria y Comercio (SIC).
- La UNGRD, hará uso de los datos personales del titular sólo para aquellas finalidades para las que se encuentre facultada respetando lo establecido en la normativa vigente.

5.10.5 POLITICA DEL TRATAMIENTO DE LA INFORMACION.

- La UNGRD, en cumplimiento de su objeto y funciones, recolecta información por diferentes canales (escrito, presencial, telefónico y virtual), durante su jornada de Lunes a Viernes, garantizando la atención a la ciudadanía.
- La UNGRD únicamente suministrará información personal a los titulares o causahabientes después de demostrada su condición o a terceros autorizados por el titular o por la Ley.
- La UNGRD suministrará información a entidades públicas o privadas si esta es requerida por con orden judicial.
- La UNGRD utilizará la información recolectada por los titulares de la información, únicamente para diseñar e implementar programas y proyectos relacionados con su objeto social y misionalidad.
- La UNGRD no entregará información recolectada a terceros sin previa autorización de los titulares de la información.
- La UNGRD establecerá un aviso al ingreso de la entidad, dando a conocer a su política de tratamiento de datos personales.

- La UNGRD establecerá dentro del procedimiento de ingreso a la entidad, indicaciones que permitan obtener autorización expresa por parte de los visitantes (proveedores, contratistas, empleados etc) para el manejo de los datos personales.
- La UNGRD establecerá en cada uno de los contratos firmados con la entidad, una leyenda indicando el conocimiento de la política de tratamiento de los datos personales y la autorización expresa para el tratamiento de los mismos dentro de las bases de datos de la entidad.
- La UNGRD, establecerá dentro de los formatos del Sistema Integrado de Gestión, donde se solicita información personal una leyenda que indique el conocimiento de la política de tratamiento de datos personales.
- La UNGRD, dará a conocer a sus clientes internos y externos la política de tratamiento de datos personales, la cual estará publicada en la intranet y pagina web de la entidad.
- La UNGRD, garantiza tener los mecanismos de seguridad necesarios para salvaguardar la información allí contenida respetando los principios de confidencialidad, integridad y disponibilidad de acuerdo a lo establecido en el manual del SGSI.
- La UNGRD, garantiza que todos los funcionarios al interior de la entidad, entienden la importancia de realizar el tratamiento de la información personal, entendiendo que más que un tema normativo es un tema de concienciación y cultura. Para lo anterior establece dentro de los planes de sensibilización, talleres para permear el tema en toda la entidad.
- La UNGRD, establece que revisará la política de tratamiento de datos personales una vez al año o en el momento que existan modificaciones de Ley. Para lo anterior garantiza que los canales de comunicación se encuentran debidamente actualizados.
- CONSULTAS
- Los titulares o causahabientes podrán consultar la información personal recolectada por la UNGRD, previa solicitud. A lo anterior la Unidad suministrará toda la información relacionada con la identificación del titular en un término no mayor a 10 días hábiles contados a partir de la recepción de la petición. En el evento que no se pueda atender la solicitud del titular dentro del los términos establecidos, se informará vía correo electrónico los motivos de la demora y se establecerá nuevo plazo de entrega de información que no puede ser superior a 5 días hábiles siguientes al vencimiento del primer término.

5.10.6 RECLAMOS

El titular o sus causahabientes que consideren que la información recolectada por la UNGRD, respecto de sus datos personales debe ser objeto de corrección, actualización o supresión, viendo vulnerados sus derechos contenidos en la Ley, debe presentar un reclamo ante a Unidad el cual será tramitado de la siguiente manera:

1. El reclamo realizado por el titular debe ser dirigido a la UNGRD, al correo electrónico contactenos@gestiondelriesgo.gov.co, incluyendo en el asunto: Reclamación Habeas Data y en el detalle la siguiente información: Nombre del titular o su causahabiente, identificación, reclamo (identificación de los hechos sujetos del reclamo), correo electrónico, dirección y teléfono de notificación. De no contar con la información completa, se notificará vía correo electrónico al titular, quien tendrá 2 días hábiles para subsanar el requerimiento solicitado por la Unidad.
2. Recibido el trámite, este será catalogado como “Reclamo en trámite”.
3. El término para la atención del reclamo será no mayor a 15 días hábiles contados a partir del siguiente día de la fecha de recibo del reclamo. En el evento que no se pueda atender la solicitud del titular dentro de los términos establecidos, se informará vía correo electrónico los motivos de la demora y se establecerá nuevo plazo de entrega de información que no puede ser superior a 5 días hábiles siguientes al vencimiento del primer término.

5.10.7 PETICIONES DE ACTUALIZACIÓN, RECTIFICACIÓN Y SUPRESIÓN DE DATOS
La UNGRD rectificará y actualizará, a solicitud del titular, la información que resulte ser incompleta o inexacta para lo cual el titular debe realizar la solicitud al correo contactenos@gestiondelriesgo.gov.co indicando en el detalle la solicitud a realizar.

5.10.8 REVOCATORIA DE AUTORIZACIÓN Y/O SUPRESIÓN DE DATOS
Los titulares pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no exista una restricción contractual. Para o anterior la UNGRD dispone el correo electrónico contactenos@gestiondelriesgo.gov.co.
Si vencido el término, la UNGRD no ha realizado la eliminación de la información, el titular puede elevar solicitud a la Super-Intendencia de Industria y Comercio para que se ordene la supresión de la información.

5.10.9 TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES

- La UNGRD, no realiza transferencia o transmisión de datos personales a terceros países, sin previa autorización expresa por parte del titular.
- La UNGRD, no realizará transferencia o transmisión a terceros países que no tengan un nivel de protección de la información adecuado.

5.10.10 FUNCION DE PROTECCION DE DATOS PERSONALES EN LA UNGRD.

- Responsable del Tratamiento de Datos Personales

El responsable del tratamiento de datos personales es la UNGRD, apoyada en la oficina asesora de planeación e información y jurídica, dependencias que vigilarán el debido cumplimiento del presente documento y de las demás normas que regulen el buen uso de los datos personales de acuerdo a lo establecido en la 1581 de 2012 y normas referentes.
El correo electrónico de contacto al cual el titular o su causahabiente deben enviar sus solicitudes es el siguiente: contactenos@gestiondelriesgo.gov.co

- Encargado del Tratamiento de Datos Personales

Es encargado del tratamiento de datos personales cualquier persona natural o jurídica, pública o privada, que realice el tratamiento de datos personales por cuenta del responsable del tratamiento de la UNGRD.

La UNGRD define que los encargados del tratamiento de los datos personales sean los subdirectores de área y coordinadores de grupos así:

- Subdirector de Manejo de desastres
- Subdirector de Conocimiento de Riesgo
- Subdirector de Reducción de Riesgo
- Coordinador del Grupo de Cooperación Internacional
- Coordinador del Grupo de Apoyo Financiero y Contable
- Coordinador Grupo de Apoyo Administrativo
- Coordinador del Grupo de Talento Humano
- Coordinador del Grupo de Contratación

Y como labor de control y monitoreo el responsable será el área de control interno de la entidad.
Los deberes de los encargados del tratamiento de los datos personales, serán los descritos en la Ley 1581 de 2012 o normas referentes que la actualicen.

5.10.11 REGISTRO NACIONAL DE BASES DE DATOS

De acuerdo con el Art. 25 de la Ley 1581 de 2012 y sus decretos reglamentarios, el responsable del tratamiento de datos personales de la UNGRD aportará a la SuperIntendencia de Industria y Comercio (SIC), el presente documento de políticas y procedimientos para el tratamiento de datos personales y de la misma manera realizará el proceso de identificación de las bases de datos contenidas en la UNGRD, para su posterior inscripción en la RNBD, de acuerdo a lo establecido en la Circular Externa No. 02 del 3 de Noviembre de 2015 emitida por la SIC.

5.10.12 AUTORIZACIONES Y CONSENTIMIENTO DEL TITULAR

Para el tratamiento de datos personales, la UNGRD mediante sus mecanismos electrónicos (página web, correo electrónico) en la opción de aceptación de términos y condiciones, solicitará al titular la autorización expresa para manejar y recolectar sus datos personales. Esta autorización puede ser tramitada por cualquier medio electrónico sin perjuicio de lo establecido por la Ley.

De la misma manera, la UNGRD y de acuerdo a los términos dispuestos por la Ley generará un aviso en el cual comunica a los titulares que pueden ejercer su derecho de Habeas Data a través de su página web portal.gestiondelriesgo.gov.co o por medio del correo electrónico contactenos@gestiondelriesgo.gov.co

5.10.13 VIGENCIA

El presente documento rige a partir del primero (01) de Diciembre de 2016 y estará publicada en la página web portal.gestiondelriesgo.gov.co

Los cambios a los que esté sujeta la presente política, serán revisados y actualizados por el personal encargado al interior de la entidad, quienes una vez aprueben, se realiza la publicación en la página web portal.gestiondelriesgo.gov.co. Si los cambios en la política son suntanciales, estos serán comunicados vía web a los titulares de los datos personales.

5.10.14 MECANISMOS DE ATENCIÓN DE CONSULTAS Y RECLAMOS

La UNGRD ha designado como área responsable de velar por el cumplimiento de la atención de consultas y reclamos por parte de los titulares a la oficina asesora de planeación de información con el apoyo de la oficina asesora jurídica, subdirecciones, coordinaciones y encargado de la seguridad de la información en la entidad.
Esta área estará atenta para resolver peticiones, consultas y reclamos por parte de los titulares y realizar las actualizaciones pertinentes de acuerdo a lo establecido en la Ley.
Para realizar peticiones, consultas o reclamos con el fin de ejercer el derecho de Habeas Data, la UNGRD, ha dispuesto para los titulares son siguientes canales de comunicación

Medio Telefónico: Tel: (57-1) 5529696
Medio Virtual: Email: contactenos@gestiondelriesgo.gov.co
Chat virtual
Medio Presencial: Dirección: Avenida Calle 26 No. 92-32 - Edificio Gold 4 - piso 2, Bogotá, Colombia.

5.10.15 REFERENCIA A OTROS DOCUMENTOS

El presente documento relacionado con la Protección de Datos Personales ha sido elaborado en concordancia con las siguientes normas y documentos:

- Ley 1581 de 2012
- Decreto Reglamentario 1377 de 2013
- Ley 1266 de 2008

5.11 TRANSPARENCIA DE INFORMACIÓN PÚBLICA BAJO LA LEY 1712 DE 2014

A continuación, se definen las políticas y procedimientos que serán pilar de cumplimiento para la Unidad Nacional para la Gestión del Riesgo de Desastres (UNGRD), de acuerdo a lo establecido en la Ley de Transparencia - 1712 de 2014; “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”, sancionados por el Congreso de la República de Colombia.

5.11.1 PRINCIPIOS PARA LA TRANSPARENCIA Y ACCESO A LA INFORMACION PÚBLICA

En la UNGRD, para interpretar el derecho de acceso a la información, aplica los siguientes principios establecidos en la Ley.

Principio de máxima publicidad para titular universal
Toda información en posesión, bajo control o custodia de la UNGRD, es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley.

Principio de Transparencia
Toda la información en poder de la UNGRD definida en el esta ley, se presume pública, en consecuencia de lo cual la Unidad está en el deber de proporcionar y facilitar el acceso a la misma en los términos posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.

Principio de buena fe
La UNGRD, cumpliendo con las obligaciones derivadas del derecho de acceso a la información pública, lo hará con motivación honesta, leal y desprovista de cualquier intención dolosa o culposa.

Principio de facilitación
La UNGRD, debe facilitar el ejercicio del derecho de acceso a la información pública, excluyendo exigencias o requisitos que puedan obstruirlo o impedirlo.

Principio de discriminación
La UNGRD, debe entregar información a todas las personas que lo soliciten, en igualdad de condiciones, sin hacer distinciones arbitrarias y sin exigir expresión de causa o motivación para la solicitud.

Principio de Gratitud
La UNGRD, tiene conocimiento que el acceso a la información pública es gratuito y no se podrá cobrar valores adicionales al costo de reproducción de la información.

Principio de Celeridad
La UNGRD garantiza la agilidad en el trámite y la gestión administrativa, como parte del cumplimiento de las tareas a cargo de entidades y servidores públicos.

Principio de Eficacia

Este principio impone el logro de resultados mínimos con relación a las responsabilidades confiadas a la UNGRD, con miras a la efectividad de los derechos colectivos e individuales.

Principio de la Calidad de la Información

Toda la información de interés público que sea producida, gestionada y difundida por la UNGRD, será oportuna, objetiva, veraz, completa, reutilizable, procesable y estar disponible en formatos accesibles para los solicitantes e interesados en ella, teniendo en cuenta los procedimientos de gestión documental de la respectiva entidad.

Principio de la Divulgación proactiva de la Información

La UNGRD, debe promover y generar una cultura de transparencia al interior, lo que conlleva la obligación de publicar y divulgar documentos y archivos que plasman la actividad estatal y de interés público, de forma rutinaria y proactiva, actualizada, accesible y comprensible, atendiendo a límites razonables del talento humano y recursos físicos y financieros.

Principio de la responsabilidad del uso de la Información

La UNGRD, entiende que cualquier persona que haga uso de la información proporcionada por la Unidad, lo hará atendiendo a la misma.

5.11.2 POLÍTICAS GENERALES DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN EN LA UNGRD

- La UNGRD, establece que las subdirecciones y coordinaciones de la entidad son las encargadas de revisar si la información manejada por estas dependencias es pública, clasificada o reservada de la entidad.
- La UNGRD, establece que cada subdirección o coordinación de la entidad será la encargada del registro de activos de información de la información que se maneja en la dependencia.
- La UNGRD, establece que la oficina jurídica es la encargada del proceso de consolidación del registro de activos de información y el índice de información clasificada y reservada de la entidad.
- La UNGRD, establece que la oficina de planeación e información es l encargada del proceso de consolidación del registro de activos de información y el índice de información clasificada y reservada de la entidad.
- La UNGRD, establece que el Sistema Integrado de Gestión definirá dentro de los formatos lo requerido para identificar si la información contenida es de tipo público, clasificado o reservado de acuerdo a lo establecido por la Ley.
- La UNGRD, establece que la política de transparencia y acceso a la información será revisada cada año o cuando existan modificaciones en la Ley o sus normas referentes.
- La UNGRD, establece dentro de sus planes de sensibilización, dar a conocer al interior de la entidad, la política de transarencia y acceso a la infrmación, sus cambios y la importancia de la misma.
- La UNGRD, garantiza que actualizará la información publicada en la página web con una periodicidad semestral o cuando las modificaciones de la Ley así lo requieran.

5.11.3 PUBLICACIÓN Y CONTENIDO DE LA INFORMACION

Para dar tratamiento a la Política y cumplir con el procedimiento de Transparencia y derecho de acceso de la Información y las obligaciones impartidas por la Ley 1712 de 2014, desde la UNGRD, se debe tener en cuenta lo siguiente.

Disponibilidad de la información
La UNGRD, pondrá a disposición del público la información a la que hace referencia la presente ley, a través de cualquier medio de comunicación electrónica. La UNGRD, tendrá a disposición de las personas interesadas dicha información en la Web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.

Accesibilidad
Con el objeto de facilitar que las poblaciones específicas accedan a la información que particularmente las afecte, la UNGRD, a solicitud de las autoridades de las comunidades, divulgarán la información pública en diversos idiomas y lenguas y elaborarán formatos alternativos comprensibles para dichos grupos. Deberá asegurarse el acceso a esa información a los distintos grupos étnicos y culturales del país y en especial se adecuarán los medios de comunicación para que faciliten el acceso a las personas que se encuentran en situación de discapacidad.

- **Información mínima obligatoria respecto a la estructura de la UNGRD.**

La UNGRD, publicará y actualizará con una periodicidad no mayor a 6 meses, la siguiente información mínima obligatoria de manera proactiva en los sistemas de información del Estado o herramientas que lo sustituyan:

a. La descripción de su estructura orgánica, funciones y deberes, la ubicación de sus sedes y áreas, divisiones o departamentos, y sus horas de atención al público;
b. Su presupuesto general, ejecución presupuestal histórica anual y planes de gasto público para cada año fiscal, de conformidad con el artículo 74 de la ley 1474 de 2011;
c. Un directorio que incluya el, cargo, direcciones de correo electrónico y teléfono del despacho de los empleados y funcionarios y las escalas salariales correspondientes a las categorías de todos los servidores que trabajan en la Unidad, de conformidad con el formato de información de servidores públicos y contratistas.
d. Todas las normas generales y reglamentarias, políticas, lineamientos o manuales, las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos y los resultados de las auditorñias al ejercicio presupuestal e indicadores de desempeño.
e. Su respectivo plan de compras anual, así como las contrataciones adjudicadas para la correspondiente vigencia en lo relacionado con funcionamiento e inversión, las obras públicas, los bienes adquiridos, arrendados y en caso de los servicios de estudios o investigaciones deberá señalarse el tema específico, de conformidad con el artículo 74 de la ley 1474 de 2011. En el caso de las personas naturales con contratos de prestación de servicios, deberá publicarse el objeto del contrato, monto de los honorarios y direcciones de correo electrónico, de conformidad con el formato de información de servidores públicos y contratistas;
f. Los plazos de cumplimiento de los contratos;
g. Publicar el Plan Anticorrupción y de Atención al Ciudadano, de conformidad con el artículo 73 de la ley 1474 de 2011.

h. La UNGRD, garantiza que la información publicada será de fácil uso y comprensión para las personas asegurando su calidad, veracidad, oportunidad y confiabilidad.
i. Para el reporte de información de los funcionarios de la UNGRD, se hará uso del forato de información dispuesto por el Departamento Administrativo de la Función Pública.
j. La UNGRD, validará lo requerido por la Estrategia de Gobierno en Línea respecto a los términos de publicación y divulgación de la información.

- **Publicidad de la contratación.**

La UNGRD, publicará en el medio electrónico institucional sus contrataciones en curso y un vínculo al sistema electrónico para la contratación pública o el que haga sus veces, a través del cual podrá accederse directamente a la información correspondiente al respectivo proceso contractual, en aquellos que se encuentren sometidas a dicho sistema, sin excepción.

- **Información mínima obligatoria respecto a servicios, procedimientos y funcionamiento de la UNGRD**

La UNGRD, publicará la siguiente información mínima obligatoria de manera proactiva:

a. Detalles pertinentes sobre todo servicio que brinde directamente a las entidades del sector minero, energético e hidrocarburos, además del público en general, incluyendo normas, formularios y protocolos de atención;
b. Toda la información correspondiente a los trámites que se pueden agotar en la entidad, incluyendo la normativa relacionada, el proceso, los costos asociados y los distintos formatos o formularios requeridos;
c. Una descripción de los procedimientos que se siguen para tomar decisiones en las diferentes áreas;
d. El contenido de toda decisión política que haya adoptado y afecte a las entidades adscritas o interesadas, así como al público en general, junto con sus fundamentos y toda interpretación autorizada de ellas;
e. Todos los informes de gestión, evaluación y auditoría a las que está vinculado;
f. Todo mecanismo interno y externo de supervisión, notificación y vigilancia pertinente;
g. Sus procedimientos, lineamientos, políticas en materia de adquisiciones y compras, así como todos los datos de adjudicación y ejecución de contratos, incluidos concursos y licitaciones;
h. Todo mecanismo de presentación directa de solicitudes, quejas y reclamos a disposición del público en relación con acciones u omisiones de la Unidad. Junto con un informe de todas las solicitudes, denuncias y los tiempos de respuesta del sujeto obligado;
i. Todo mecanismo o procedimiento por medio del cual el público pueda participar en la formulación de la política o el ejercicio de las facultades de ese sujeto obligado;
j. Un registro de publicaciones que contenga los documentos publicados de conformidad con la presente ley y automáticamente disponibles, así como un Registro de Activos de Información, el cual se encuentra asociado al SGSI – Sistema de Gestión de Seguridad de la Información.
k. Los sujetos obligados deberán publicar datos abiertos, para lo cual deberán contemplar las excepciones establecidas en el titulo 3 de la presente ley. Adicionalmente, para las condiciones técnicas de su publicación, se deberán observar los requisitos que establezca el gobierno nacional a través del Ministerio de las Tecnologías de la Información y las Comunicaciones o quien haga sus veces.

- **Adopción de esquemas de publicación en la UNGRD.**

La UNGRD, adoptará y difundirá de manera amplia su esquema de publicación, dentro de los seis meses siguientes a la entrada en vigencia de la presente ley. El esquema será difundido a través de su sitio Web, y en su defecto, en los dispositivos de divulgación existentes en su dependencia, incluyendo boletines, gacetas y carteleras. El esquema de publicación debe establecer:

a. Las clases de información que UNGRD publicará de manera proactiva y que en todo caso deberá comprender la información mínima obligatoria;
b. La manera en la cual publicará dicha información;
c. Otras recomendaciones adicionales que establezca el Ministerio Público;
d. Los cuadros de clasificación documental que faciliten la consulta de los documentos públicos que se conservan en los archivos de la Unidad, de acuerdo con la reglamentación establecida por el Archivo General de la Nación.
e. La periodicidad de la divulgación, acorde a los principios administrativos de la función pública.

- **Registros de Activos de Información en la UNGRD.**

La UNGRD debe actualizar el inventario de activos de información de su SGSI, con los requerimientos establecidos en esta Ley, teniendo en cuenta:

a. Todas las categorías de información publicada;
b. Todo registro publicado;
c. Todo registro disponible para ser solicitado por el público;
d. El Ministerio Público podrá establecer estándares en relación a los Registros Activos de Información.

La Unidad debe asegurarse de que sus Activos de Información cumplen con los estándares establecidos por el Ministerio Público y con aquellos dictados por el Archivo General de la Nación, en relación a la constitución de las Tablas de Retención Documental (TRD) y los inventarios documentales.

- **Información publicada con anterioridad.**

La UNGRD debe garantizar y facilitar a los solicitantes, de la manera más sencilla posible, el acceso a toda la información previamente divulgada. Se publicará esta información en los términos establecidos por la Ley.
Cuando se dé respuesta a una de las solicitudes aquí previstas, esta deberá hacerse pública de manera proactiva en el sitio Web de la Unidad, y en defecto de la existencia de un sitio Web, en los dispositivos de divulgación existentes en su dependencia.

- **Programa de Gestión Documental.**

La UNGRD, adopta el Programa de Gestión Documental en el cual se establezcan los procedimientos y lineamientos necesarios para la producción, distribución, organización, consulta y conservación de los documentos públicos. Este programa se integra con las funciones administrativas de la Unidad.

Deberán observarse los lineamientos y recomendaciones que el Archivo General de la Nación y demás entidades competentes expidan en la materia.

- **Archivos**

La UNGRD, se asegura que existen procedimientos claros para la creación, gestión, organización y conservación de sus archivos. Los procedimientos adoptados por la Unidad, cumplen con los lineamientos que en la materia sean producidos por el Archivo General de la Nación.

- **Sistemas de Información.**

Para asegurar que los sistemas de información electrónica sean efectivamente una herramienta para promover el acceso a la información pública, la UNGRD asegura que estos:

a. Se encuentran alineados con los distintos procedimientos y articulados con los lineamientos establecidos en el Programa de Gestión Documental de la entidad;
b. Gestionan la misma información que se encuentre en los sistemas administrativos de la Unidad;

5.11.4 EXCEPCIONES EN EL ACCESO A LA INFORMACION.

- **Información exceptuada por daño de derechos a personas naturales o jurídicas.**

Esta información es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos:

a. El derecho de toda persona a la intimidad, bajo las limitaciones propias que imponen la condición de servidor público, en concordancia con lo estipulado.
b. El derecho de toda persona a la vida, la salud o la seguridad.
c. Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la ley 1474 de 2011.

- **Información exceptuada por daño a los intereses públicos.**

Se refiere a toda aquella información pública reservada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional.

a. La defensa y seguridad nacional;
b. La seguridad pública;
c. Las relaciones internacionales;
d. La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según sea el caso;
e. El debido proceso y la igualdad de las partes en los procesos judiciales;
f. La administración efectiva de la justicia
g. Los derechos de la infancia y la adolescencia;
h. La estabilidad macroeconómica y financiera del país;
i. La salud pública;

- **Índice de información clasificada y reservada**

La UNGRD, mantendrá un índice actualizado de los actos, documentos e informaciones calificados como clasificados o reservados, de conformidad a esta ley.
El índice incluirá sus denominaciones, la motivación y la individualización del acto en que conste tal calificación.

- **Divulgación parcial y otras reglas**

En aquellas circunstancias en que la totalidad de la información contenida en un documento no esté protegida por una excepción contenida en la presente ley, debe hacerse una versión pública que mantenga la reserva únicamente de la parte indispensable. La información pública que no cae en ningún supuesto de excepción deberá ser entregada a la parte solicitante, así como ser de conocimiento público. La reserva de acceso a la información opera respecto del contenido de un documento público pero no de su existencia.

Ninguna autoridad pública puede negarse a indicar si un documento obra o no en su poder o negar la divulgación de un documento.

Las excepciones de acceso a la información contenidas en la presente ley no aplican en casos de violación de derechos humanos o delitos de lesa humanidad, y en todo caso deberán protegerse los derechos de las víctimas de dichas violaciones.

- **Excepciones temporales**

La reserva de las informaciones amparadas por el artículo 19 de la Ley 1712 de 2014, no deberá extenderse por un período mayor a quince (15) años.

5.11.5 GARANTIAS AL EJERCICIO DEL DERECHO DE ACCESO A LA INFORMACION.

- **Funciones del Ministerio Público**

El Ministerio Público será el encargado de velar por el adecuado cumplimiento de las obligaciones estipuladas en la presente ley. Para tal propósito, la Procuraduría General de la Nación tiene las siguientes funciones y atribuciones:

a. Desarrollar acciones preventivas para el cumplimiento de la ley 1712 de 2014.
b. Realizar informes sobre el cumplimiento de las decisiones de tutelas sobre acceso a la información.
c. Publicar las decisiones de tutela y normatividad sobre acceso a la información pública.
d. Promover el conocimiento y aplicación de la presente ley y sus disposiciones entre los sujetos obligados, así como su comprensión entre el público, teniendo en cuenta criterios diferenciales para su accesibilidad, sobre las materias de su competencia mediante la publicación y difusión de una guía sobre el derecho de acceso a la información.
e. Aplicar las sanciones disciplinarias que la presente ley consagra.
f. Decidir disciplinariamente, en los casos de ejercicio de poder preferente, los casos de faltas o mala conducta derivada del derecho de acceso a la información.
g. Promover la transparencia de la función pública, el acceso y la publicidad de la información de las entidades del Estado, por cualquier medio de publicación.

h. Requerir a la UNGRD para que ajusten sus procedimientos y sistema de atención al ciudadano a dicha legislación.
i. Realizar, directamente o a través de terceros, actividades de capacitación de funcionarios públicos en materia de transparencia y acceso a la información.
j. Efectuar estadísticas y reportes sobre transparencia y acceso a la información de I los órganos de la administración del Estado y sobre el cumplimiento de esta ley.
k. Entregar en debida forma las respuestas a las peticiones formuladas con solicitud de identificación reservada a las que se refiere el parágrafo del artículo 4° de la 11 presente ley.
l. Implementar y administrar tres sistemas de información en el cumplimiento de sus funciones para lo cual establecerá los plazos y criterios del reporte por parte de las 11 entidades públicas que considere necesarias.

Las entidades del Ministerio Público contarán con una oficina designada que dispondrá de los medios necesarios para el cumplimiento de las anteriores funciones y atribuciones.

- **Del Derecho de Acceso a la Información**

Toda persona tiene el derecho a solicitar y recibir información de la UNGRD, en la forma y condiciones que establece la ley aplicable y la Constitución Nacional. Para lo anterior la UNGRD, dispone de todos sus canales de comunicación.

- **Solicitud de Acceso a la Información**

La UNGRD, garantiza que cualquier persona podrá realizar una solicitud de información, de forma oral o escrita, incluida la vía electrónica, para acceder a la información pública. Para lo anterior la UNGRD, dispone de todos sus canales de comunicación.

- **Respuesta a la Solicitud de Acceso a la Información**

La UNGRD, mediante una comunicación escrita o vía electrónica, de forma oportuna, veraz, completa, motivada y actualizada, responderá a cualquier persona que haya presentado una solicitud de acceso a información pública. Su respuesta se dará en los términos establecidos en la Ley.
La respuesta a la solicitud es gratuita o sujeta a un costo que no supere el valor de la reproducción y envío de la misma al solicitante. Se preferirá, cuando sea posible, según los sujetos pasivo y activo, la respuesta por vía electrónica, con el consentimiento del solicitante.
La UNGRD, designa que el área encargada para dar respuesta a las solicitudes de información será la oficina asesora jurídica apoyada de las subdirecciones y coordinaciones de la entidad.
La UNGRD, establece el siguiente procedimiento para da respuesta a las solicitudes de acceso a la información:

- Recibir la solicitud por cualquiera de los canales dispuestos por la Unidad. Dentro de los canales dispuestos se encuentran; vía telefónica, presencial en las instalaciones de la Unidad; Correo físico; correo electrónico institucional; formulario dispuesto para la ciudadanía en la página web de la Unidad.
- Identifica si se trata de una solicitud de información; Una vez recibida la información, la persona encargada define si la solicitud es de información o corresponde a un derecho de petición, con el fin de dar curso en los términos establecidos en cada caso. De no ser clara la solicitud, el encargado deberá informar al solicitante de la situación parra que esta sea subsanada en un término no mayor a 2 días hábiles.

- Determina si la UNGRD tiene competencia para dar respuesta: En caso que la UNGRD, no sea la entidad competente para dar respuesta a la solicitud de información, el encargado debe informar en un término no mayor a 5 días al solicitante de la información.
- Asegura la existencia de la información en la Unidad: El encargado debe validar si la información solicitada existe o debe ser creada, para lo cual debe revisar el registro de activos de información.
- Establece si la información es reservada o clasificada: El encargado debe establecer si la información solicutada es reservada o clasificada y continuar con el trámite de acuerdo a lo establecido por la Ley. Para lo anterior debe revisar el Indice de Información clasificada y reservada donde se indica la clasificación de la información de la Unidad.
- Envia respuesta al solicitante: Independientemente como se haya recibido la solicitud, la UNGRD debe responder por escrito sea por medio electrónico o físico de acuerdo a las preferencias del solicitante.

- **Recursos del Solicitante**

Cuando la respuesta que entregada por la UNGRD, invoque la reserva de seguridad y defensa nacional o relaciones internacionales, el solicitante podrá acudir al recurso de reposición, el cual deberá interponerse por escrito y sustentando en la diligencia de notificación, o dentro de los tres (3) días siguientes a ella.
Negado el recurso corresponde al Tribunal Administrativo con jurisdicción en el lugar donde se encuentren los documentos, si se trata de autoridades nacionales, departamentales o del Distrito Capital de Bogotá, o al juez administrativo si se trata de autoridades distritales y municipales, decidir en única instancia si se niega o se acepta, total o parcialmente, la petición formulada.
Para ello, el funcionario respectivo enviará la documentación correspondiente al tribunal o al juez administrativo en un plazo no superior a tres (3) días. En caso de que el funcionario incumpla esta obligación el solicitante podrá hacer el respectivo envío de manera directa.
El juez administrativo decidirá dentro de los diez (10) días siguientes. Este término se interrumpirá en los siguientes casos:

- Cuando el tribunal o el juez administrativo solicite copia o fotocopia de los documentos sobre cuya divulgación deba decidir, o cualquier otra información que requieran, y hasta la fecha en la cual las reciba oficialmente.
- Cuando la autoridad solicite, a la sección del Consejo de Estado que el reglamento disponga, asumir conocimiento del asunto en atención a su importancia jurídica o con el objeto de unificar criterios sobre el tema. Si al cabo de cinco (5) días la sección guarda silencio, o decide no avocar conocimiento, la actuación continuará ante el respectivo tribunal o juzgado administrativo.

- **Carga de la prueba**

Le corresponde a la UNGRD aportar las razones y pruebas que fundamenten y evidencien que la información solicitada debe permanecer reservada o confidencial.
En particular, el sujeto obligado debe demostrar que la información debe relacionarse con un objetivo legítimo establecido legal o constitucionalmente. Además, deberá establecer si se trata de una excepción contenida en los artículos 18 y 19 de la ley 1712 de 2014 y si la revelación de la información causaría un daño presente, probable y especifico que excede el interés público que representa el acceso a la información.

- **Responsabilidad Penal**

Todo acto de ocultamiento, destrucción o alteración deliberada total o parcial de información pública, por parte de la UNGRD, una vez haya sido objeto de una solicitud de información, será sancionado en los términos del artículo 292 del Código Penal.

5.11.6 VIGENCIA

El presente documento rige a partir del primero (01) de Diciembre de 2016 y estará publicada en la página web portal.gestiondelriesgo.gov.co

Los cambios a los que esté sujeta la presente política, serán revisados y actualizados por el personal encargado al interior de la entidad, quienes una vez aprueben , se realiza la publicación en la página web portal.gestiondelriesgo.gov.co. Si los cambios en la política son sustanciales, estos serán comunicados vía web a los titulares de los datos personales.

5.11.7 INFORMACIÓN DE CONTACTO

Si tiene alguna duda respecto a lo definido en la presente política, la UNGRD, ha dispuesto para los titulares son siguientes canales de comunicación

Medio Telefónico: Tel: (57-1) 5529696
Medio Virtual: Email: contactenos@gestiondelriesgo.gov.co
Chat virtual
Medio Presencial: Dirección:Avenida Calle 26 No. 92-32 - Edificio Gold 4 - piso 2, Bogotá, Colombia

5.11.8 REFERENCIA A OTROS DOCUMENTOS

El presente documento relacionado con la Protección de Datos Personales ha sido elaborado en concordancia con las siguientes normas y documentos:

- Ley 1581 de 2012
- Ley 1712 de 2014
- Manual del SGSI de la UNGRD.

5.12 CONTROL OPERACIONAL PARA LA SEGURIDAD DE LA INFORMACIÓN

Con el fin de dar cumplimiento al numeral de la norma 12.1.1 Procedimientos de operación documentados de procesamiento de información, la UNGRD cuenta con los siguientes procedimientos operacionales dentro de los siguientes documentos:

- **Política y Procedimiento de copias de seguridad PR- 1603- SIS-02**

Determina como realizar las copias de seguridad de la información del servidor de archivos, correo electrónico al servidor de copia, la restauración y custodia de las mismas, con el fin de garantizar la recuperación en caso de pérdida de la información.

- **Procedimiento de Monitoreo de aplicaciones PR-1300-GSI-06**

Identifica como monitorear, controlar y realizar seguimiento a los sistemas de información de la UNGRD, para garantizar el óptimo funcionamiento y uso de los recursos tecnológicos que soportan el funcionamiento y operación de los sistemas de información de la UNGRD.

- **Procedimiento de Control de Cambios.**

Establece e implementa las actividades necesarias para registrar y evaluar los posibles cambios en las instalaciones de procesamiento y aplicaciones de la UNGRD

- **Procedimiento de Continuidad de Seguridad de la Información.**

Define las estrategias de recuperación ante situación de desastres que afecten las operaciones misionales y que permita la continuidad de la seguridad de la información de la UNGRD.

- **Procedimiento de Gestión de Incidentes.**

Define las actividades que se deben realizar cuando se presente algún tipo de incidente que pueda afectar la seguridad de la información de la UNGRD.

- **Procedimiento de Gestión de Proveedores.**

Define el alcance y responsabilidades para la seguridad de la información de la UNGRD, por parte de los proveedores de servicios para la Unidad.

- **Política de Uso de Dispositivos Móviles.**

Establece e implementa las políticas del uso de dispositivos móviles (Discos Duros Externos, USB, Tablets, Computadores Portátiles y Smarthphone, entre otros, en la Unidad), conectados a la Red de la UNGRD.

- **Política de Acceso Remoto.**

Establece las condiciones que se deben considerar en el marco de la seguridad de la información de la UNGRD, para poder realizar trabajo correspondiente a los aspectos de la Unidad, de forma remota.

- **Protocolo de Contingencias página web – PT-1300-GSI-01.**

Determina una serie de tareas y actividades para cuando se presente una situación adversa que afecten la prestación del servicio de la página Web de la UNGRD, que involucra el accionar de diferentes áreas al interior de la UNGRD así como la coordinación de tareas con terceros que prestan diferentes servicios que soportan el funcionamiento de la página web.

- **Manual de Contingencia Informático M- 1603 SIS-02.**

Tiene como base la infraestructura tecnológica de red, comunicaciones e internet y elementos o activos complementarios que soportan la información o datos críticos para la función de la Entidad. Este manual identifica los problemas que pueden suceder en nuestra infraestructura y los procedimientos que se tienen que realizar por el personal a cargo de soporte para restablecer los servicios que sean interrumpidos por estas fallas.

- **Manual de Políticas de Seguridad Informática M- 1603- SIS-01.**

Establece como Administrar la Infraestructura tecnológica y la seguridad de las redes informáticas para lo cual se prestará el soporte y se proporcionarán las herramientas adecuados a los funcionarios de la UNGRD, actuando como un centro de servicios para la solución de diferentes problemas informáticos y promoviendo el uso de las buenas prácticas para el manejo de la infraestructura tecnológica.

- **Política de Control de Acceso.**

Define los lineamientos relativos al control de acceso lógico de los usuarios de la UNGRD.

- **Procedimiento de Control de Cambios.**

Define los lineamientos relativos al control de acceso lógico de los usuarios de la UNGRD

- **Política de Uso de Llaves Criptográficas.**

Determina los lineamientos para el uso de controles criptográficos con el fin de proteger la confidencialidad, integridad y autenticidad de la información.

- **Política de Gestión de Llaves.**

Identifica las normas que se deben aplicar para la generación, protección y tiempo de vida de las llaves criptográficas utilizadas por la UNGRD.

- **Política de Transferencia de Información.**

Define las normas a considerar relacionadas con las maneras como se debe transferir o recibir la información que tiene una relación directa con la UNGRD.

Para el subproceso de gestión de infraestructura tecnológica, se encuentran establecidos los siguientes procedimientos, actualmente como soporte a la operación de TI en la UNGRD:

- Procedimiento de Asignación de Equipos.
- Procedimiento de envío de Equipos a Bodega.

Para el proceso de Gestión de Sistemas de Información se cuenta además de lo ya descrito, los siguientes procedimientos:

- Procedimiento de Gestión de Proyectos de TI.
- Procedimiento de Monitoreo de Aplicaciones.

Gestión de vulnerabilidades técnicas

La Unidad Nacional para la Gestión del Riesgo de Desastres (UNGRD), realiza un análisis de vulnerabilidades y pruebas técnicas de penetración, de forma anual a través de un tercero especializado, con el fin del evaluar las posibles brechas de seguridad que existen y puedan afectar la

confidencialidad, integridad y disponibilidad de la información de la Unidad y aquella que la Entidad custodia de sus partes interesadas.

ELABORÓ	REVISÓ	APROBÓ
VER LISTADO DE DOCUMENTOS EN LA HERRAMIENTA TECNOLÓGICA NEOGESTIÓN.		
Nombre: Luis Javier Barrera	Nombre: Paula Contreras / Yanizza Lozano Orjuela	Nombre: Ángela Patricia Calderón
Cargo: Profesional Especializado UNGRD	Cargo: / Profesionales Especializados OAPI	Cargo: Coordinadora Grupo de Apoyo Administrativo

1. CONTROL DE CAMBIOS DEL DOCUMENTO

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
01	Emisión inicial	20/12/2016
02	Ajustes al Procedimiento	21/12/2016
03	Ajuste al Alcance del Documento	04/05/2018

[i] Ley 1581 de 2012