CONTENIDO

1. INTRODUCCIÓN

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, el Modelo de Seguridad y Privacidad de la Información-MinTIC, 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 " 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****

[2] Ibíd.

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.

[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 sí 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

PROPOSITO

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 del Grupo de Tecnologías de la Información.
- La gestión de contraseñas para el acceso a la red se realiza por medio de autorización del profesional responsable del Grupo de Tecnologías de la Información.

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 PR-1101-GTI-02 GESTIÓN DE USUARIOS
- 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 del Grupo de Tecnologías de la 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 del Grupo de Tecnologías de la 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 PR-1101-GTI-02 GESTIÓN DE USUARIOS.

NORMA ISO/IEC 27001:2013 ANEXO A 9.1.1

5.2 POLÍTICA DE COPIAS DE SEGURIDAD.

PROPOSITO

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 SISTEMA DE ALMACENAMIENTO, 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 sistema de almacenamiento, se realiza una copia de respaldo o Backup de acuerdo a lo establecido en el Procedimiento *PR-1101-GTI-07 PROCEDIMIENTO DE COPIAS DE SEGURIDAD INCREMENTAL Y TOTAL.*
- Para las copias de seguridad la UNGRD utiliza la herramienta *Networker.*

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 Grupo de Tecnologías de la Información por medio de correo electrónico.
- La restauración de las Bases de Datos y Sistemas Operativos, se debe tener en cuenta lo establecido en el *PR-1101-GTI-08 PROCEDIMIENTO DE CONTINUIDAD DE 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 de la plataforma de administración de correo electrónico Workspace.

- Para el respaldo de los correos y drive de cada usuario, se crea un archivo con el nombre del funcionario.

NORMA ISO/IEC 27001:2013 ANEXO A 12.3.1
VER PROCEDIMIENTO DE COPIAS DE SEGURIDAD INCREMENTAL Y TOTAL.
VER PROCEDIMIENTO DE CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

5.3 POLÍTICA GESTIÓN DE LLAVES CRIPTOGRÁFICAS

PROPOSITO

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 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 cifrado del disco local de almacenamiento de información será configurado con las llaves criptográficas por solicitud previa del colaborador que requiera confidencialidad en la información que maneja.

GTI será responsable de la activación, recepción y la distribución de las llaves criptográficas a los usuarios autorizados y velará porque la llave se encuentre activa en el periodo de tiempo previsto. Cada clave deberá tener un ciclo de vida, el cual dependerá de la información del equipo que se desea proteger, pudiendo tener un periodo de expiración de horas o días, se definirán las fechas de activación y desactivación para cada clave generada.

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. 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 colaboradores 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 *POLITICA DE DISPOSITIVOS MOVILES.*

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 cifrarán 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

PROPOSITO

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 M-1604-GCON-01 MANUAL DE CONTRATACIÓN

- Los proveedores deberán ser evaluados.

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

5.5 POLÍTICA DISPOSITIVOS MÓVILES

PROPOSITO

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 PR-1101-GTI-09 ASIGNACIÓN DE EQUIPOS DE COMPUTO.*

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).

- Los funcionarios deben de aplicar el método de bloqueo recomendado por la UNGRD, para la protección de los dispositivos móviles que les sean entregados. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo por usuario y contraseña.

CIFRADO

- Los funcionarios deben activar la opción de cifrado en los dispositivos móviles haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo. El cifrado de los dispositivos móviles pertenecientes a la UNGRD, será direccionado por el profesional designado.

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 Tecnologías de la Información con 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 Tecnologías de la Información.

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 Tecnologías de la Información será quien otorgará los respectivos permisos.

SINCRONIZACIÓN DE CORREO ELECTRÓNICO EN DISPOSITIVOS MÓVILES

- 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 EQUIPOS 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.

- Los equipos de cómputo que ingresen o salgan de las instalaciones de UNGRD frecuentemente por parte de los colaboradores deben ser registrados en el formato FR-1101-GTI-10 Registro equipos frecuentes.

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.
- Evitar hacer uso de redes inalámbricas de uso público.
- Evitar conectar los dispositivos móviles institucionales asignados, por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- Dado que la mayor parte de los dispositivos móviles permiten habilitar y deshabilitar las funciones de geoposicionamiento, según las preferencias y necesidades del usuario, los funcionarios deberán deshabilitar esta funcionalidad siempre que no sea estrictamente necesario.

NORMA ISO/IEC 27001:2013 ANEXO A 6.2.1.
VER PROCEDIMIENTO DE ASIGNACIÓN DE EQUIPO DE COMPUTO

5.6 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

PROPOSITO

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 del comando: TECLA 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

PROPOSITO

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 autenticarán a través de contraseñas las cuales deben cumplir con las reglas sobre la gestión de claves (longitud mínima de 8 caracteres, inclusión mayúsculas y minúsculas, incluya caracteres especiales como (*? \! °/&%$) entre otros, no incluya nombre propio, 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

PROPOSITO

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 Tecnologías de la Información.

- Se tiene definido los funcionarios aprobado por el comité de seguridad y/o Grupo de Tecnologías de la Información, que tienen derecho a este acceso para el desempeño de sus actividades. 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 que tengan que ingresar remotamente a equipos de cómputo deben estar autorizados a través de correo electrónico por parte del coordinador y/o jefe de área donde se establece la solicitud para la conexión.

- Los funcionarios o usuarios autorizados con el acceso remoto a sistemas de información, reciben la notificación 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 de las personas designadas en el grupo de tecnologías de la información.

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 prohibido, sin excepción alguna, la conexión remota desde redes públicas (cafés internet, hoteles sin acceso controlado, centros 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.

REVISIONES

Las conexiones remotas asignadas se revisarán por lo menos cada seis meses para renovar los permisos asignados, por parte de comité de seguridad de la información y/o personal técnico del Grupo de Tecnologías 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 y/o personal técnico del Grupo de Tecnologías 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 DE TELETRABAJO

PROPOSITO

Definir los lineamientos relativos al ejercicio del teletrabajo por parte de los funcionarios de la Unidad Nacional de Gestión de Riesgos de Desastres – UNGRD.

ALCANCE

La política aplica a todos los funcionarios de la UNGRD.

GENERALIDADES

En caso de formalizarse y definirse el Teletrabajo para los funcionarios con responsabilidades dentro de la UNGRD, se dará cumplimiento a la legislación vigente en Colombia en materia de teletrabajo, teniendo en cuenta:

- La seguridad física existente en el sitio, teniendo en cuenta la seguridad física de la edificación y del entorno local.
- El entorno físico de teletrabajo propuesto
- Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la UNGRD, la sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación y la sensibilidad del sistema interno.
- La amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo alojamiento, por ejemplo, familia y amigos
- El uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica
- Acuerdos para evitar disputas acerca de derechos de propiedad intelectual desarrollados en equipos de propiedad privada
- Requisitos de firewall y de protección contra software malicioso.

Las directrices y acuerdos que se consideren deberían incluir:

- El suministro de equipo adecuado y de muebles de almacenamiento para las actividades de teletrabajo, cuando no se permite el uso del equipo de propiedad privada que no está bajo el control de la institución
- Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el teletrabajador está autorizado a acceder

- El suministro de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto
- La seguridad física
- Las reglas y la orientación sobre el acceso de la familia y los visitantes a los equipos y a la información
- El suministro de soporte y mantenimiento del hardware y el software
- El suministro de seguros
- Los procedimientos para copias de respaldo y continuidad del negocio
- Auditoría y seguimiento de la seguridad
- La revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades del teletrabajo finalicen.

NORMA ISO/IEC 27001:2013 ANEXO A 6.2.2

5.10 POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS

PROPOSITO

Establecer las normas sobre el uso aceptable de los activos de información (computadores portátiles y teléfonos inteligentes, entre otros) 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/FNGRD que tengan asignado activos de información pertenecientes a la entidad para el desarrollo de las actividades propias de sus funciones u obligaciones.

GENERALIDADES

La UNGRD como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su nube, otorgará responsabilidad a los diferentes procesos sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos como estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos inteligentes, entre otros, propiedad de la UNGRD, son activos de la entidad y se proporcionan a los funcionarios y terceros autorizados, para cumplir con sus propósitos.

Toda la información sensible de la UNGRD, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con la

legislación aplicable y los requerimientos propios de la entidad cumpliendo con la metodología de gestión de activos y riesgos. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

- El proceso de Gestión de tecnologías de la información es el propietario de los activos de información almacenados en la nube institucional de la UNGRD y bajo su control técnico, en consecuencia, debe asegurar su apropiada operación y administración.

- El proceso de Gestión de tecnologías de la información es el propietario en conjunto con el Comité de Control de Cambios, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la nube institucional de la UNGRD, bajo el control técnico de dicho proceso.

- El proceso de Gestión de tecnologías de la información debe establecer una configuración adecuada para los recursos tecnológicos bajo su control técnico, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

- El proceso de Gestión de tecnologías de la información es responsable de preparar los requerimientos técnicos necesarios, incluyendo necesidades de hardware y software para incorporar a los procesos de compra y contratación de las estaciones de trabajo fijas y/o portátiles de los funcionarios.

- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, entre otros. Estos cambios pueden ser realizados únicamente por el personal asignado por el proceso de Gestión de tecnologías de la información.

- En caso tal de que algún funcionario requiera para el desempeño de sus funciones realizar instalación de software y/o cambios en la configuración del equipo se debe documentar la autorización caso por caso, indicando la duración de la autorización.

- Todos los equipos de cómputo de la UNGRD, deben ser bloqueados por el funcionario responsable al momento de retirarse de su puesto de trabajo.

- Las claves de acceso a los sistemas de información de la UNGRD son personales e intransferibles, cada funcionario debe responder por las actividades que se lleven a cabo con sus datos de identificación.

- Todo problema mecánico, eléctrico o electrónico sobre los equipos de cómputo de la universidad, debe ser atendido únicamente por el personal asignado por el proceso de Gestión de tecnologías de la información.

- Todas las estaciones de trabajo deben apagarse o dejarse en estado de hibernación al finalizar la jornada laboral.

- Los equipos de cómputo (CPU y monitor), servidores, teléfonos IP y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados.

- Los recursos tecnológicos de la UNGRD, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la entidad.

- Los recursos tecnológicos de la UNGRD entregados a funcionarios y proveedores, son proporcionados con el único fin de llevar a cabo las labores definidas por la entidad; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

- Los funcionarios deben de privilegiar el uso de las herramientas y equipos institucionales para el desarrollo de sus actividades.

- Los funcionarios no deben utilizar software no autorizado o de su propiedad en los equipos entregados por la UNGRD para el desempeño de sus funciones.

- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

- El sistema de correo debe ser utilizado solamente para propósitos de la UNGRD y evitarse su uso para tratar asuntos personales.

- Evitar acceder desde redes inalámbricas públicas, pues estas redes al compartir el canal de Internet con todos los usuarios que simultáneamente se conectan a ellas, son altamente inseguras ante ataques de espionaje.

- Es muy importante no abrir correos que provengan de destinatarios desconocidos o que tengan asuntos o archivos adjuntos sospechosos.

- Se deben evitar las acciones en Internet a nombre de la UNGRD que no estén previamente aprobadas y no se relacionen con el cumplimiento de objetivos contractuales, pues de esta manera, se podría estar comprometiendo negativamente el nombre de la entidad y su reputación.

- La información contenida en las herramientas y equipos asignados por la UNGRD para el cumplimiento de sus responsabilidades son de propiedad de la entidad y podrán ser revisadas en el momento en que ésta lo determine.

5.11 POLÍTICA TRANSFERENCIA DE LA INFORMACIÓN

PROPOSITO

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 Workspace 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.
- 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

5.12 POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES

Se acoge lo establecido en la POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES de la entidad.

VER RG-1200-OAJ-07 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

5.13 POLÍTICA PARA EL USO DE INTERNET

PROPÓSITO

El propósito de esta política es establecer normas que aseguren la adecuada utilización del acceso a internet, con lo cual se optimiza el buen funcionamiento del recurso

ALCANCE

La política aplica a todos los funcionarios, asesores, personal de contratistas, empleados temporales y terceros que usen equipos dentro de la UNGRD.

USO DE INTERNET

Debe entenderse que Internet es una herramienta estrictamente de trabajo y no debe tener otros fines ajenos a las funciones del usuario, por lo anterior se realizarán monitoreos periódicos por parte del área de sistemas de la UNGRD con el fin de verificar su acertado uso.

Uso del Internet:

- El usuario no debe entrar a Páginas Web con contenido pornográfico.
- El usuario no debe bajar ningún programa (software), sin la debida autorización del área de Tecnología de la UNGRD, tales como: Shareware, software de evaluación, ya que estos no poseen licencia para su uso en la UNGRD y en su mayoría traen código oculto que daña los navegadores (internet explorer, mozila, chrome, etc)
- El usuario no puede utilizar redes sociales salvo sean autorizados por el director de la UNGRD. autorizados por su jefe directo y/o el oficial de seguridad de la información.
- No se puede realizar ningún tipo de compras a través de páginas establecidas para tal fin.
- El usuario dentro de la UNGRD no debe utilizar el internet con fines comerciales, políticos o con propósitos ilegales.
- Es prohibido el uso de acceso a internet para acceder, crear, copiar, distribuir material o enviar mensajes obscenos, pornográficos, etc, o mensajes que instiguen violencia o amenaza de cualquier tipo.
- 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.

AUDITORÍA DE INTERNET

El área de tecnología estará auditando los equipos con el fin de verificar el buen uso del internet. Al ser encontrado algún usuario dando un indebido uso a esta herramienta, se procederá a comunicarle al Jefe del área, sobre el mal uso que se le está dando a la herramienta.

5.14 POLITICA PARA EL USO DEL CORREO ELECTRONICO INSTITUCIONAL

PROPÓSITO

El propósito de esta política es establecer normas que aseguren la adecuada utilización del correo electrónico institucional, con lo cual se optimiza el buen funcionamiento del recurso

ALCANCE

La política aplica a todos los funcionarios, asesores, personal de contratistas, empleados temporales y terceros que usen equipos dentro de la UNGRD.

USO DEL CORREO ELECTRONICO

- Todos los mensajes generados o manejados a través de la plataforma de correo electrónico Workspace con que cuenta la UNGRD, incluyendo las copias de respaldo, se consideran propiedad de la UNGRD.
- El uso del sistema de correo electrónico institucional está restringido a asuntos oficiales.
- Su empleo para asuntos personales está autorizado siempre y cuando consuma una mínima parte de los recursos y no interfiera con el cumplimiento de las obligaciones del funcionario.
- 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.
- Por seguridad no se debe dar la clave para acceder al servicio a terceras personas.
- No se debe utilizar el correo electrónico para participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares.
- El manejo de las claves de seguridad y la información que se tramita en cada cuenta es responsabilidad única del funcionario.

PRIVACIDAD

Excepto en casos especiales y autorizados, se prohíbe a los funcionarios interceptar o divulgar los mensajes de terceras personas.

SANCIONES POR MAL USO DEL CORREO ELECTRONICO

Al ser encontrado algún usuario dándole mal uso al Correo Electrónico institucional se procederá a comunicar al Director o Jefe del área. De volver a incurrir se aplicarán sanciones que amerite el caso.

5.15 POLITICA PARA INSTALACION DE SOFTWARE

PROPÓSITO

El propósito de esta política es establecer normas que aseguren que el software que se encuentra instalado en los computadores cumplan con los respectivos licenciamientos y de acorde a la propiedad intelectual.

ALCANCE

La política aplica a todos los funcionarios, asesores, personal de contratistas, empleados temporales y terceros que usen equipos dentro de la UNGRD.

SOFTWARE EN LOS COMPUTADORES

- Todo software que se utilice en la UNGRD será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.
- En los equipos de cómputo, de comunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento.
- Apropiado y de acorde a la propiedad intelectual.
- El usuario no debe instalar ningún programa para escuchar MP3, RA, WAV, o emisoras de radio vía Internet tales como Winamp, real audio, Music match, etc.
- El usuario no debe instalar ningún programa para ver vídeos o emisoras de televisión vía Internet tales como real audio, Bwv, etc.
- La instalación de software que desde el punto de vista del área de Sistemas pudiera poner en riesgo los recursos de la institución no está permitida.
- El usuario no debe instalar ningún programa diferente a los previamente instalados por el área de sistemas, los cuales están debidamente legalizados.

5.16 POLITICA PARA ALMACENAMIENTO DE INFORMACION EN LA RED

PROPÓSITO

El propósito de esta política es establecer normas que aseguren que la información que se almacene en el servidor de archivos cumpla y este acorde con los lineamientos del almacenamiento de archivos dentro de la red.

ALCANCE

La política aplica a todos los funcionarios, asesores, personal de contratistas, empleados temporales y terceros que usen equipos dentro de la UNGRD.

ALMACENAMIENTO DE ARCHIVOS DENTRO DE LA RED

• Información personal tal como fotos, archivos, publicaciones, etc no deben ser guardados en carpetas en el servidor de archivos. Se debe utilizar para tal fin el disco duro local del PC.

• El usuario no debe guardar ningún programa para escuchar MP3, RA, WAV, o emisoras de radio vía Internet tales como winamp, real audio, music match, etc, en el servidor de archivos.

• El usuario no debe guardar ningún programa para ver vídeos o emisoras de televisión vía Internet tales como real audio, bwv, etc, en el servidor de archivos.

• El usuario no destruirá, dañará o borrará el trabajo de otros funcionarios. El uso indebido deliberado de los archivos de la red y de su equipo se considerará como un acto de vandalismo y podrá ser causa de una acción disciplinaria.

5.17 POLITICA DE ACCESO AL CENTRO DE DATOS

PROPÓSITO

El propósito de esta política es la de establecer las reglas para el acceso al centro de datos con el objeto de mantener la seguridad, integridad y apariencia del mismo.

ALCANCE

La política está dirigida a todos los visitantes y clientes que tienen equipos instalados en el centro de datos de la UNGRD ubicado en el edificio Gold 4 Piso 2.

SOLICITUD Y AUTORIZACION DE VISITAS

- Todo tipo de visitas al Centro de Datos, deberá tener un agendamiento previo con anticipación al menos de 24 horas respecto de la hora de vista y deberá ser solicitada al área Administrativa y/o Grupo de Tecnologías de la Información.

- Únicamente las áreas anteriormente mencionadas podrán dar permiso para el acceso al centro de Datos.

- No se acepta el ingreso de personas diferentes a los visitantes autorizados.

VISITAS AUTORIZADAS

Si la visita fue autorizada, entonces el ingreso del visitante debe seguir las siguientes Instrucciones que dependen del horario en que se realice.

- Horario Hábil: En este caso el cliente debe dirigirse a la recepción de la UNGRD informando de su visita e indicando la persona que lo atenderá por parte del Grupo de Tecnologías de la Información.

- Horario No hábil: El cliente debe dirigirse al guardia del edificio, quien confirma el acceso con el soporte correspondiente enviado por el Área Administrativa, una vez confirmado el acceso se permite el ingreso del cliente.

Para los casos anteriormente descritos el visitante debe ser registrado en el formato *FR-1101-GTI-09 INGRESO DATA CENTER*, para ello deberá identificarse con algún documento válido y vigente, que concuerde plenamente con la información indicada en la solicitud de visita (los documentos válidos son cédula de identidad, licencia de conducir o pasaporte todos vigentes al momento de ser presentado).

Si la documentación del visitante no es coincidente con la solicitud de visitas, o no es vigente al momento de la visita, entonces no se le permitirá el acceso al Centro de Datos. Si la visita fue realizada en horario no hábil, entonces el guardia conducirá al visitante hacia el exterior del edificio.

ACCESO AL CENTRO DE DATOS

Toda persona que ingrese al centro de Datos debe hacerlo acompañado por lo menos al inicio y al fin de sus actividades por un funcionario del Grupo de Tecnologías de la Información quién será la persona que le indicará el área específica donde el cliente tiene instalado sus equipos o donde los podrá instalar, y tendrá como obligaciones para con la entidad las siguientes, las cuales serán indicadas previamente al ingreso del mismo:

- No podrá ingresar: Bajo los efectos de alcohol, drogas o cualquier sustancia alucinógena; Portando armas de fuego o similares; fumando.

- No podrá introducir ninguno de los siguientes elementos: Explosivos, elementos inflamables o corrosivos, Armas, Químicos, Drogas ilegales, Materiales radioactivos, Comidas ni bebidas.

- No se permite tomar fotos, ni el uso de cámaras fotográficas o cámaras de video, a menos que se tenga permiso para ello.

- El cliente solo podrá conectar sus equipos a las salidas asignadas a sus respectivos gabinetes.

FINALIZACION DE LAS LABORES

- Al finalizar cualquier trabajo en el centro de datos, deberá asegurarse que todos los cables utilizados estén debidamente conectados e instalados dentro de los gabinetes respectivos.

- Se deben sacar todas las cajas y desechos antes de salir de las instalaciones. El Centro de Datos debe mantenerse limpio y ordenado en todo momento.

- La UNGRD se reserva el derecho de remover y descartar cualquier basura o desechos dejados en él.

- No se puede arrastrar equipos sobre el piso falso del Centro de Datos. Se debe utilizar carretillas con llantas de caucho, en caso de ser necesario para el ingreso o salida de algún equipo pesado.

  VER FORMATO INGRESO DATA CENTER

5.18 POLÍTICA DE PRUEBAS DE ACEPTACIÓN

PROPOSITO

Establecer los lineamientos básicos para las pruebas de aceptación realizadas a todos los sistemas de información de la Unidad Nacional para la Gestión del Riesgo de Desastres - UNGRD.

ALCANCE

Esta política aplica para todos los sistemas de información con los que cuenta la Unidad Nacional para la Gestión del Riesgo de Desastres - UNGRD

GENERALIDADES

El equipo de Gestión de Tecnologías de la Información debe diseñar pruebas y criterios de aceptación para todas las aplicaciones, software, bases de datos y demás sistemas de información nuevos, actualizados o nuevas versiones, elaboradas por la entidad o adquiridos por terceros, no solo en función de sus requisitos comerciales, sino también relacionadas al cumplimiento de cara a los requisitos y criterios de seguridad de la información. Lo anterior con el fin de garantizar los datos procesados en los sistemas de información con los que cuenta la Unidad Nacional para la Gestión del Riesgo de Desastres - UNGRD.

5.19 POLITICA PARA DATOS DE PRUEBA

PROPOSITO

Definir las medidas y directrices necesarias para salvaguardar los datos utilizados en entornos de pruebas para los Sistemas de Información de la Unidad Nacional para la Gestión del Riesgo de Desastres - UNGRD.

ALCANCE

La presente política aplica para todos los datos utilizados en la realización de pruebas por parte del equipo de Gestión de Tecnologías de la Información.

GENERALIADES

- Con el fin de propender siempre la confidencialidad, integridad y disponibilidad de la información de la entidad, en la medida de lo posible los datos utilizados para entornos de pruebas deben ser NO reales, es decir, datos genéricos.

- En caso de que por la naturaleza de la prueba (pruebas precisas) sea necesario usar datos reales, estos deberán ser cuidadosamente seleccionados, monitoreados y autorizados por el líder del proceso de Gestión de Tecnologías de la Información, garantizando su seguridad durante el periodo de prueba.

- Una vez terminada la prueba se debe borrar los datos de forma segura, de manera que no se vuelvan a recuperar.

5.20 TRAE TU PROPIO DISPOSITIVIO (TTPD)

PROPOSITO

El propósito de esta política es establecer requerimientos que aseguren la adecuada utilización de los dispositivos (Tablets, portátiles) personales.

ALCANCE

La política aplica a todos los colaboradores que usen dispositivos personales en atención a sus funciones laborales, dentro y fuera de las instalaciones de la UNGRD

GENERALIADES

Los dispositivos personales (portátiles, tablets) que ingresen a las instalaciones de la UNGRD frecuentemente deben ser registrados en el formato FR-1101-GTI-10 Registro equipos frecuentes y el usuario debe firmar el formato FR-1101-GTI-16 FORMATO CONSENTIMIENTO INFORMADO.

CONDICIONES QUE DEBE CUMPLIR EL DISPOSITIVO

- Tener instalado Antivirus actualizado
- Sistema operativo actualizado
- Los dispositivos deben estar protegidos mediante claves, lectores biométricos, etc.

CONDICIONES QUE DEBEN CUMPLIR LOS USUARIOS

- No permitir el acceso a cualquiera que no sea propietario del dispositivo.
- La información de la UNGRD solo deber ser compartida a través de la VPN.
- Cuando se utilicen los dispositivos personales dentro y fuera de las instalaciones de la UNGRD, no deben ser dejados desatendidos.
- Cuando se utilizan los equipos en lugares públicos, el propietario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- No transferir información de la UNGRD a otros dispositivos no permitidos.
- Reportar incidentes de seguridad con GTI.
- En caso de pérdida, robo del dispositivo, reportarlo a la entidad como incidente de Seguridad.

- Toda la información contenida en los Dispositivos TTPD inherente a la ejecución de las funciones u obligaciones contractuales de los colaboradores debe estar almacenada en las carpetas asignadas del servidor.

SENSIBILIZACIÓN

El grupo TI estará a cargo de la sensibilización a los colaboradores de la entidad sobre el uso adecuado de los dispositivos TTPD, así como también de concientizar sobre las amenazas y riesgos más comunes a los que se expone la entidad al permitir el acceso a sus recursos tecnológicos a través de este tipo de dispositivos.

REVISIONES

- Se realizarán inspecciones mensuales sobre el escaneo del código QR para verificar su validez

- El Grupo TI mensualmente revisará la periodicidad de los registros, y la duración del registro es hasta la finalización del contrato del usuario.

6. CONTROL DE CAMBIOS DEL DOCUMENTO

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
01	Emisión Inicial - Este documento tenía el código M–1603-SIS-03 - versión 05 con fecha 23/07/2020 , se realizó actualización de formato y de codificación, se actualizan las políticas de seguridad de la información.	24/11/2021
02	Se agregó la política de prueba de aceptación y la política para datos de prueba	14/02/2022
03	Se agregó la política de TTPD, se hicieron ajustes respecto a la vida útil de las claves en la política de gestión de llaves criptográficas y se agregaron formatos nuevos.	25/08/2022

ELABORÓ	REVISÓ	APROBÓ
Nombre: Luis Javier Barrera / Javier Edgardo Soto	Nombre: Catherine Pérez	Nombre: Carolina Jiménez Zapata
Cargo: Profesionales Especializados GTI	Cargo: Contratista GTI	Cargo: Coordinadora Grupo de Tecnologías de la Información