1. TABLA DE CONTENIDO

2. INTRODUCCION

La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que confrontan las entidades hoy día en lo que se refiere a la protección de sus activos de información frente a peligros externos e internos.

La políticas de seguridad son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos.

A menudo las políticas van acompañadas de normas, instrucciones y procedimientos. Las políticas son obligatorias, mientras que las recomendaciones o directrices son más bien opcionales. De hecho, las declaraciones de políticas de seguridad pueden transformarse fácilmente en recomendaciones reemplazando la palabra "debe" con la palabra "debería".

Por otro lado las políticas son de jerarquía superior a las normas, estándares y procedimientos que también requieren ser acatados. Las políticas consisten de declaraciones genéricas, mientras las normas hacen referencia específica a tecnologías, metodologías, procedimientos de implementación y otros aspectos en detalle.
.
Una declaración sobre políticas describe sólo la forma general de manejar un problema específico, pero no debe ser demasiado detallada o extensa, en cuyo caso se convertiría en un procedimiento.

Las políticas también son diferentes de las medidas de seguridad o de los mecanismos de control. Un ejemplo de esto último sería un sistema de cifrado para las comunicaciones o para los datos confidenciales guardados en discos y cintas. En muchos casos las políticas definen metas o objetivos generales que luego se alcanzan por medio de medidas de seguridad.

En general, las políticas definen las áreas sobre las cuales debe enfocarse la atención en lo que concierne a la seguridad. Las políticas podrían dictar que todo el software desarrollado o adquirido se pruebe a fondo antes de utilizarse. Se necesitará tomar en cuenta varios detalles

sobre cómo aplicar esta política. Por ejemplo, la metodología a usar para probar el software.

3. DEFINICIONES

Activos: Son todo elemento que compone el proceso de la comunicación, la cual la componen: la información, el emisor, el medio que la transporta y finalmente el receptor.

Administrador: Es la persona o programa encargado de gestionar, realizar el control, conceder permisos, en un sistema informático o red de ordenadores.

Adware: Los programas de tipo adware muestran publicidad asociada a productos y/o servicios ofrecidos por los propios creadores o por terceros.

Autorización: Es el proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.

Amenaza: Es cualquier actividad que represente posible daño a su información. Las amenazas pueden tomar muchas formas.

Confidencialidad: Es el acceso a los activos del sistema está limitado a usuarios autorizados.

Cookies: Las cookies son pequeños archivos de texto que el navegador de Internet guarda en el ordenador del usuario cuando se visitan páginas web. Pueden derivar en una amenaza para la privacidad del usuario.

Generación: Es un ataque contra la autenticidad, se da cuando una entidad no autorizada inserta objetos Falsificado en el sistema.

Gusanos: Los gusanos son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser colapsar los ordenadores y las redes.

Integridad: Los activos del sistema sólo pueden ser borrados o modificados por usuarios autorizados.

Interrupción: es un ataque contra la disponibilidad, se da cuando un componente del sistema informático es destruido o se vuelve no disponible.

Intercepción: Es un ataque contra la confiabilidad, se da cuando una entidad (persona, programa u Ordenador) no autorizada consigue acceso a un recurso.

Modificación : Es un ataque contra la integridad , se da cuando una entidad no autorizada no solo accede al recurso , sino que es capaz de modificarlo cambiando en parte o en todo el funcionamiento del sistema.

Organización: En este grupo se incluyen los aspectos que componen la estructura física y organizativa de las empresas

Riesgo: Es que la información de tu compañía esté disponible para terceros, lo cual causará pérdidas a la compañía, tiempo, dinero y reputación.

Scams: Es un tipo de correo electrónico fraudulento que pretende estafar económicamente al usuario presentado como donación a recibir, lotería o premio al que se accede previo envío de dinero.

Seguridad informática: Es un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas.

Spyware: El spyware o programas espías son aplicaciones que recopilan información sobre una persona u organización sin su consentimiento ni conocimiento.

Troyanos: El principal objetivo de este tipo de malware es introducir e instalar otras aplicaciones en el equipo infectado, para permitir su control remoto desde otros equipos

Virus: Es un programa informático diseñado para infectar archivos. Suelen venir dentro del código de otros programas. Los objetivos de los virus suelen ser los programas ejecutables.

Vulnerabilidad: Es una debilidad en la seguridad de la información que puede ser explotada por una amenaza; que podría ser, una debilidad en su sistema de seguridad de red, procesos, y procedimientos

4. OBJETIVO

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.

5. ALCANCE

Las políticas aplican a todos los funcionarios, asesores, personal de contratistas, empleados temporales y terceros que usen equipos dentro de la UNGRD.

6. DESARROLLO

1. POLITICAS 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.
- 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.

2. POLITICAS 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 Google Apps 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 Electrónico.

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 aplicaran sanciones que amerite el caso.

3. POLITICAS 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.

4. POLITICAS ALMACENAMIENTO 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. POLITICAS 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 Soporte e Infraestructura Tecnológica, enviando un correo electrónico a Fanny.torres@gestiondelriesgo.gov.co ó luis.barrera@gestiondelriesgo.gov.co, o realizando una llamada telefónica para su programación al 5529696 ext. 826 u 833.
- 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 área de soporte e infraestructura tecnológica.

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

Para los casos anteriormente descritos el visitante debe ser registrado en el Sistema de Registro de visitas, 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 área de soporte e infraestructura tecnológica 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:

- Todo ingreso al centro de datos debe ser registrado en el formato “Registro Ingreso al Centro de datos”. Anexo No. 1.

- 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, Quimicos, 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 el.

- 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.

ELABORO	REVISO	APROBO
Ver formato de aprobación de documentación SIPLAG del proceso. Ver listado de documentos en la herramienta tecnológica Neogestión.		
Nombre: Luis Javier Barrera Naicipa.	Nombre: Fanny Torres Estupiñan.	Nombre: Carlos Iván Márquez Pérez
Cargo: Profesional Especializado-UNGRD	Cargo: Coordinadora Grupo de Apoyo Administrativo- UNGRD	Cargo: Director General UNGRD

7. CONTROL DE CAMBIOS DEL DOCUMENTO

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
02	Inclusión políticas de acceso al Centro de datos	08/06/2016

ANEXO No. 1

UNIDAD NACIONAL PARA LA GESTION DEL RIESGO DE DESASTRES
REGISTRO INGRESO AL CENTRO DE DATOS

Nombre	Organización	Motivo Ingreso	Ingreso		Salida		Observaciones
			Fecha	Hora	Fecha	Hora	

Obligaciones del Visitante:

NO PODRA INGRESAR	NO PODRA INTRODUCIR	OTRAS OBLIGACIONES
• Bajo los efectos de alcohol, drogas o cualquier sustancia alucinógena; • Portando armas de fuego o similares; • fumando	• Explosivos, • elementos inflamables o corrosivos, • Armas, • Químicos, • Drogas ilegales, • Materiales radioactivos, • Comidas ni bebidas	• 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. • 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. • No se permite tomar fotos, ni el uso de cámaras fotográficas o cámaras de video, a menos que se tenga permiso para ello. • solo podrá conectar sus equipos a las salidas asignadas a sus respectivos gabinetes.