MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO

Establecer las medidas organizacionales, técnicas, físicas y legales, necesarias para proteger los activos de información contra acceso no autorizado, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir en forma intencional o accidental, asegurando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información

ALCANCE

Este MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, es aplicable a todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de la organización.

Las políticas de seguridad descritas en este manual, se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001:2013.

LÍNEA BASE DE LA POLÍTICA

RESPONSABILIDAD

Es responsabilidad de la organización hacer uso de la MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, como parte de sus herramientas de gobierno y de gestión, de definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento.

CUMPLIMIENTO

El cumplimiento de la MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN es obligatorio. Si los colaboradores, consultores, contratistas, terceras partes violan estas políticas, la organización se reserva el derecho de tomar las medidas correspondientes.

EXCEPCIONES

Las excepciones a cualquier cumplimiento de MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN deben ser aprobadas por la dirección de la organización. Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas.

ADMINISTRACIÓN DE LAS POLÍTICAS

Las modificaciones o adiciones al MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN serán propuestas por el encargado de hacer cumplir las políticas presentes previa autorización de la gerencia de la organización. Estas políticas deben ser revisadas como mínimo una vez al año o cuando sea necesario.

POLÍTICA CONTROL DE ACCESO

Propósito:

Definir los lineamientos relativos al control de acceso lógico de los usuarios de la **KEEP NET SAS**

Alcance:

Esta 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 **KEEP NET SAS**

Generalidades:

En esta política sesta basada en NORMA ISO/IEC 27001:2013 ANEXO A 9.1.1 y definen las condiciones sobre las cuales los funcionarios, contratistas o terceros tienen acceso a la red, sistemas operativos y aplicativos de **KEEP NET SAS**

ACCESO A LA RED

- Son usuarios de red de la organización todos los funcionarios, contratistas y terceros que se encuentren en **KEEP NET SAS**
- El acceso a la red por parte de terceros debe estar estrictamente restringido y permisible únicamente con previa autorización del profesional responsable de

KEEP NET SAS

- La gestión de contraseñas para el acceso a la red se realiza por medio de autorización de **KEEP NET SAS**

ACCESO A LAS APLICACIONES

- La persona encargada de **KEEP NET SAS** 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 aplicable.*

- La asignación y gestión de cambios de claves y/o contraseñas de cuenta, se encuentra a cargo del responsable del Proceso 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 organización se realiza a través de contraseña segura de red.

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 **KEEP NET SAS** 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 **KEEP NET SAS,** 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 **KEEP NET SAS** 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 **KEEP NET SAS** 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 **KEEP NET SAS** 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 **KEEP NET SAS**, deben ser cambiadas cada 90 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 responsable del Proceso 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 *Procedimiento aplicable*,

POLÍTICA DISPOSITIVOS MÓVILES

Propósito:

Establecer las normas sobre el uso de los dispositivos móviles (computadores portátiles y teléfonos inteligentes) propiedad de **KEEP NET SAS,** velando por su uso adecuado, responsable y sus mejores prácticas.

Alcance:

Esta política aplica para todos los funcionarios y/o contratistas de **KEEP NET SAS** 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

KEEP NET SAS basado en NORMA ISO/IEC 27001:2013 ANEXO A 6.2.1 proporciona las condiciones para el manejo de los dispositivos móviles (computadores portátiles y teléfonos inteligentes) tanto corporativos como personales los cuales hacen uso de los servicios de la organización. 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 aplicable*.

USO DE CONTRASEÑAS

- Todos los dispositivos móviles pertenecientes a KEEP NET SAS 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 basarse en lo consignado en la POLÍTICA CONTROL DE ACCESO en el apartado GESTIÓN DE CONTRASEÑAS.

PROTECCIÓN FÍSICA

- Todos los dispositivos móviles de **KEEP NET SAS** deben estar registrados e inventariados.

- Los dispositivos móviles asignados a funcionarios y/o contratistas de **KEEP NET SAS** son personales e intransferibles.
- Los usuarios de equipos portátiles que pertenezcan a **KEEP NET SAS** deben mantener una seguridad física dentro de las instalaciones de la entidad, por medio del uso de guayas de seguridad o similares.
- En caso de pérdida o robo del equipo, el funcionario deberá informar inmediatamente a quien haga las veces de responsable de seguridad informática quien tomará 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 **KEEP NET SAS** 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 **KEEP NET SAS** previa evaluación y pertinencia de la misma.
- El aseguramiento de la administración de los dispositivos móviles, pertenecientes a **KEEP NET SAS** será administrado por el profesional designado por la dirección de la organización

SEGURIDAD DEL SISTEMA OPERATIVO

- Para garantizar la disponibilidad, confidencialidad e integridad de la información contenida en los dispositivos móviles, el profesional designado por **KEEP NET SAS** 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 un 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 **KEEP NET SAS** 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.

USO DE DISPOSITIVOS MOVILES

Para los dispositivos móviles (teléfono celular, tabletas, iPad, discos duros extraíbles, dispositivos de almacenamiento masivo USB, etc.) asignados por **KEEP NET SAS** de ser posible deberán estar debidamente cifrados por la herramienta suministrada por la entidad o fabricante, de no ser posible deberán estar habilitados los controles de aseguramiento y criptografía suministrados por el fabricante del dispositivo.

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 los servidores de archivos de **KEEP NET SAS**

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 **KEEP NET SAS**

Generalidades

Con el fin de mantener la integridad y disponibilidad de la información, esta política se basa en NORMA ISO/IEC 27001:2013 ANEXO A 12.3.1 donde 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 debe documentar en la bitácora de respaldo.

KEEP NET SAS 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.*
- Para las copias de seguridad **KEEP NET SAS** por el momento se realizan de manera manual, donde los funcionarios son responsables de realizar y actualizar los respaldos de la información que tiene en el equipo asignado mínimo cada 30 días

RESTAURACIÓN DE LAS COPIAS DE RESPALDO

- El funcionario y/o contratista de **KEEP NET SAS** que requiera de un archivo a restaurar, deberá realizar la solicitud directamente al personal designado por la organización para que este contacte a la persona de soporte técnico encargada de realizar esta función.
- La restauración de las Bases de Datos y Sistemas Operativos, solo lo debe realizar el personal designado por la organización para que este contacte a la persona de soporte técnico encargada de realizar esta función.

COPIAS DE SEGURIDAD CORREO ELECTRÓNICO

- Las copias de seguridad de correo electrónico corporativo de **KEEP NET SAS**, se realiza cuando el funcionario y/o contratista finaliza la relación contractual con la entidad.
- La ejecución de la copia de seguridad se realiza cuando la dirección de la organización autorice al personal designado para que este contacte a la persona de soporte técnico encargada de realizar esta función
- 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.
-

DIAGRAMA DE RED