1. OBJETIVO

Determinar los lineamientos sobre el uso de la información garantizando la confidencialidad, integralidad y protección de esta, mitigando los posibles riesgos en las tecnologías (Equipos de cómputo, sistemas de información); procurando el mejoramiento continuo de los procesos, concientizando al colaborador sobre la importancia de la información, el uso laboral adecuado y uso de las herramientas de trabajo.

2. ALCANCE

Abarca desde la configuración de la conexión de accesos remotos o servicios de red para usuarios autorizados por la entidad, garantizando el acceso seguro, hasta la desconexión de dichos servicios conforme a las directrices de seguridad establecidas por la institución.

3. DEFINICIONES

3.1. **Acceso remoto**: Conexión a las redes y sistemas informáticos, establecida desde sitios externos (ej. estaciones de teletrabajo, equipos móviles, dispositivos inalámbricos, entre otros).

3.2. **Antivirus**: Programa informático que tiene el propósito de detectar virus y otros programas que pueden afectar la integridad del equipo antes o después que ingresen al sistema de tu computador.

3.3. **Cortafuegos**: Sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

3.4. **Equipo informático ajeno autorizado**: Todo aquel equipo (ej. computadores personales, computadores portátiles, agendas electrónicas, organizadores personales, teléfonos inteligentes, de nueva generación; dispositivos de almacenamiento masivo, tablets, palmtops, entre otros). En el caso que el equipo no sea propiedad de la empresa, es utilizado bajo previa autorización, en actividades de su interés.

3.5. **Personal usuario o usuarios**: Funcionarios, contratistas, vendedores, consultores, Administrados, proveedores y/o aliados de la empresa, a los que se les ha asignado el uso de Recursos Informáticos o se les ha proporcionado acceso a los sistemas de información.

3.6. **Política**: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

3.7. **Recursos informáticos**: Son recursos, sistemas, servicios, aplicaciones y/o medios de comunicación, que son propiedad de la empresa y de su interés directo por ser utilizados para las labores propias de éste o en la ejecución de sus objetivos. Estos comprenden entre otros:

a) **Recursos de información**: Documentación de sistemas, archivos y bases de datos, manuales técnicos de usuario, material de capacitación, procedimientos operativos y de soporte, disposiciones relativas a sistemas de emergencia para la reposición de información, planes de continuidad, diagramas de red, información archivada.

b) **Equipo informático**: Activos físicos (equipos reproductores, procesadores, monitores, computadores de todo tipo, tablets, dispositivos electrónicos, equipos de comunicaciones (routers, centrales telefónicas, máquinas de fax, teléfonos de todo tipo, contestadores automáticos, redes y enlaces de comunicaciones), medios magnéticos y ópticos; otros equipos técnicos (suministro de electricidad, sistemas de aire acondicionado), mobiliario;

3.5. **Red inalámbrica**: Conexión de nodos sin necesidad de una conexión física (cables).

3.8. **Software**: Es un programa o conjunto de programas de cómputo que incluye datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático.

3.9. **Servidores**: Un servidor es un conjunto de computadoras capaz de atender las peticiones de un cliente y devolverle una respuesta.

4. RESPONSABLES

- ✓ Técnico de Sistemas
- ✓ Todos los colaboradores

5. CONDICIONES GENERALES

5.1. **Lineamientos de seguridad de la información**:

5.1.1. No se debe divulgar información confidencial a personas no autorizadas y/o personas fuera de la entidad.

5.1.2. No se permite ni se facilita el uso de los sistemas informáticos a personas no autorizadas (No se permite acceso remoto de ningún tercero sin ser autorizado y vigilado por el equipo de sistemas).

5.1.3. La interconexión a la red interna no es permitida a ninguna persona que no sea colaborador de la empresa, con la salvedad de los funcionarios externos que provengan de entes de regulación control y vigilancia, entre otros (Debidamente identificados), y solo con la autorización del área sistemas.

5.1.4. No se debe usar los recursos informáticos (hardware, software, datos, entre otros) y de telecomunicaciones para otras actividades que no estén directamente relacionados con la labor que se deba desarrollar en la institución.

5.1.5. Los usuarios y contraseñas son únicos e intransferibles, solo serán compartidos en los casos en que por cualquier periodo de tiempo un colaborador se encuentre por fuera de sus labores; para lo cual, requiere realizar una entrega de cargo al Jefe Directo o quien haga sus veces.

5.1.6. Se debe reportar al Jefe Inmediato o a quien haga sus veces cualquier evento que pueda comprometer la seguridad y los recursos informáticos, como por ejemplo contagio de virus, intrusos, modificaciones o perdida de datos o equipos. A su vez el Jefe Inmediato o quien haga sus veces debe enviar un correo electrónico al área de sistemas con detalle de información y los demás procesos que se consideren relevantes para tomar acciones.

5.1.7. El equipo de sistemas cuenta con la autorización de ingresar remotamente a cualquier equipo para brindar apoyo a cualquier novedad que se haya presentado con el equipo.

5.1.8. Es responsabilidad del área de sistemas reportar anomalías de violaciones de seguridad al Director Administrativo y al Ingeniero en sistemas, para realizar las correcciones necesarias.

5.1.9. En los equipos de la institución no se debe copiar programas informáticos, para uso personal.

5.2. **Servidores**

5.2.1. El acceso a los RACK; compete única y exclusivamente a los colaboradores del proceso de sistemas, la cual concederán autorización vigilada cuando se requiera.

5.2.2. Cada uno de los servidores tiene configurados tareas de backup, las cuales, se realizan de manera diaria y se almacenan en sus respectivas NAS.

5.3. **Instalación de software**

5.3.1. Todas las licencias para uso de software deben ser entregadas al área de sistemas, quien las mantendrá custodiadas almacenadas y vigilará el uso adecuado.

5.3.2. No se debe despegar o quitar los sticker de identificación que soportan la licencia del software.

5.3.3. El área de sistemas es la encargada de asesorar, instalar, configurar y supervisar software.

5.3.4. Esta prohibido el uso de software descargados de internet o fuentes no confiables, a menos que haya sido comprobado y aprobado por el área de sistemas.

5.3.5. En caso de que el software sea libre, se respeta la propiedad intelectual y derechos de autor.

5.3.6. Para prevenir acciones legales, se prohíbe estrictamente la instalación de software no autorizados, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita, a menos que haya sido previamente aprobado por el área de sistemas.

5.4. **Software de seguridad e internet**

5.4.1. El área de sistemas se encarga de instalar, configurar y administrar el software de seguridad y control, restringiendo permisos de sitios permitidos y/o negados para la navegación.

5.4.2. El Jefe de área autoriza que páginas se requiere para el buen trabajo de sus colaboradores.

5.5. **Antivirus**

5.5.1. Todos los equipos deben tener instalados antivirus, para su protección.

5.5.2. Cada vez que se realice mantenimiento preventivo, el equipo de sistemas debe verificar que todos los hardware cuenten con antivirus.

5.6. **Licenciamiento**

5.6.1. Es responsabilidad del área de compras, adquirir todas las aplicaciones de Software con su respectiva licencia, certificación, contrato, vigencia y/o su factura.

5.6.2. Si se encuentra algún software sin su licencia, el personal de sistemas deberá desinstalar inmediatamente.

5.7. **Uso de contraseñas**

5.7.1. El área de sistemas se encarga de asesorar a los usuarios sobre el correcto uso de las contraseñas y se informa sobre el alto grado de confidencialidad de estas, ya que, son únicas

e intransferibles y que cada colaborador es responsable de las actividades realizadas con su usuario.

5.7.2. Los permisos de los usuarios son restringidos dependiendo el perfil y a las funciones que desempeña.

5.7.3. El usuario no debe guardar su contraseña en una forma legible en archivos en discos y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada.

5.8. **Política de seguridad para las comunicaciones**

5.8.1. Está prohibido el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

5.8.2. La navegación del internet para fines personales no debe hacerse a costo tiempo de la empresa y recursos de estas, y si se requiere deben usarse en las horas no laborales.

5.9. El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

6. DOCUMENTOS DE REFERENCIA Y ANEXOS

NA.

6.1. Bibliografía

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Obtenido de Elaboración de la política general de seguridad y privacidad de la información. : https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Elaboró	Revisó	Aprobó
Miguel Ángel Peña Técnico de Sistemas	Ingrid Yovanna Mosquera Ingeniero de Mejoramiento Continuo	Lina Villarraga Jefe de Mejoramiento Continuo