1. OBJETIVO

Establecer las normas y procedimientos que deben seguirse para la seguridad en el servicio de acceso remoto y de los servicios de red; protegiendo la información electrónica de la empresa.

2. ALCANCE

Inicia con la conexión de accesos remotos o servicios de red a usuarios autorizados por la entidad, hasta la desconexión de los servicios por directrices de la empresa.

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 propieda 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. **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;

3.7. **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.

3.10. **VPN o red privada virtual**: Crea una conexión de red privada entre dispositivos a través de Internet. Las VPN se utilizan para transmitir datos de forma segura y anónima a través de redes públicas.

4. RESPONSABLES

- ✓ Técnico de Sistemas
- ✓ Todos los colaboradores

5. CONDICIONES GENERALES

5.1. La empresa está en la obligación de proteger la información que le pertenece y/o que se encuentra en su custodia de accesos no autorizados. Para ello, deberá asegurar no sólo las conexiones internas, sino también las externas.

5.2. La información de los procesos de la organización se encuentra protegidos bajo restricciones de acceso emitidas por los principales responsables del proceso, mediante mecanismos de validación manejados con credenciales, entre otras estrategias y herramientas.

5.3. Todos los usuarios deben de pedir autorización al área de sistemas para el ingreso a la red local.

5.4. Estrategias y herramientas

- ✓ **Antivirus**: Servidores y equipos de cómputo de las estaciones de trabajo tienen instalado un antivirus debidamente licenciado, el cual se encuentra programado para que analice el equipo y genere bloqueos con alertas.

- ✓ **UTM**: Los equipos informáticos tienen configurado “políticas de red”, las cuales garantizan la seguridad de las comunicaciones vía internet bloqueando el acceso a páginas no autorizadas.

- ✓ **Software Legal**: Los softwares instalados en los equipos provienen de una fuente conocida y segura, además, se encuentran licenciados. Ningún usuario tiene permitido instalar, descargar, utilizar algún software sin la administración de un técnico en sistemas.

- ✓ **Administrador y usuario estándar**: Cada equipo tiene configurado un usuario Administrador y un usuario estándar con permisos limitados. La contraseña del administrador es conocida exclusivamente por la personal del área de sistemas, este usuario posee todos los permisos propios del administrador y el usuario estándar cuenta con permisos restringidos según su perfil y las tareas diarias. Si necesita los privilegios de administrador para realizar alguna tarea como instalar o desinstalar aplicaciones, el sistema pedirá la contraseña del administrador.

- ✓ **Contraseñas seguras**: Se recomienda a los usuarios utilizar contraseñas alfanuméricas, cambiarlas periódicamente y diferentes para cada acceso; además se le responsabiliza de las actividades realizadas por su usuario en cada aplicación.

- ✓ **Red local**: El área de sistemas es la única encargada administrar, mantener y actualizar la infraestructura de esta, además de restringir el acceso a los usuarios. Cada equipo tiene asignada su IP, el cual, se le otorgan permisos y restricciones de acceso a internet de acuerdo con lo establecido por la empresa.

- ✓ **Servidores**: Se encuentran ubicados en el área de sistemas, en un cuarto aislado bajo la supervisión del personal autorizado, los cuales, cuentan con acceso físico a estos. Cada servidor tiene un antivirus licenciado con un usuario administrador y uno invitado con sus respectivas

claves. El invitado solo tiene acceso a consultar y la clave del administrador la posee personal autorizado.

- ✓ **Red Inalámbrica WI-FI**: El área de sistemas es la encargada de la administración y asignación de las claves a los usuarios autorizados por el Director Administrativo e Ingeniero de Sistemas, las redes inalámbricas deben utilizarse exclusivamente para actividades laborales y es responsabilidad del usuario hacer buen uso de la red inalámbrica.

- ✓ **VPN**: El área de sistemas asigna el uso de las VPN a los equipos autorizados por el Director Administrativo para tener conexión interna a los servicios de red, es responsabilidad del usuario el buen uso de esta.

6. DOCUMENTOS DE REFERENCIA Y ANEXOS

N/A

6.1. Bibliografía

AWS. (s.f.). Obtenido de ¿Qué es una red privada virtual (VPN)?: https://aws.amazon.com/es/what-is/vpn/#:~:text=Una%20VPN%20o%20red%20privada,a%20trav%C3%A9s%20de%20redes%20p%C3%BAblicas.

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 en Sistemas	Ingrid Mosquera Ingeniero de Mejoramiento Continuo	Lina Villarraga Jefe de Mejoramiento Continuo