**Objetivo**

Establecer criterios que permitan mantener un entorno informático seguro y controlado para el desarrollo de las actividades de la organización.

**1 Red**

1. Las redes tienen como propósito principal servir en la transformación e intercambio de información entre usuarios, departamentos, oficinas y hacia afuera a través de conexiones con otras redes.
2. El Área de Tecnología no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.
3. Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.
4. No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de La Empresa.
5. Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de La Empresa y se usarán exclusivamente para actividades relacionadas con la labor asignada.
6. Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.
7. El uso de analizadores de red es permitido única y exclusivamente por el personal de IT para monitorear la funcionalidad de las redes, contribuyendo a la consolidación del sistema de seguridad bajo las Políticas de Seguridad.
8. No se permitirá el uso de analizadores para monitorear o censar redes ajenas a La Empresa y no se deberán realizar análisis de la Red desde equipos externos a la entidad.
9. Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

**2 Servidores**

**2.1 Configuración e instalación**

El Administrador de infraestructura tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

1. Los servidores que proporcionen servicios a través de la red e Internet deberán:
   1. Funcionar 24 horas del día los 365 días del año.
   2. Recibir mantenimiento preventivo mínimo una vez al año
   3. Recibir mantenimiento Lógico semestral que incluya depuración de logs.
   4. o Recibir mantenimiento anual que incluya la revisión de su configuración.
   5. o Ser monitoreados por el personal de infraestructura designado para dicha actividad.
2. La información de los servidores deberá ser incluida en el plan de respaldo del servidor o servicios.

**2.2 Correo Electrónico**

1. El equipo de infraestructura se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.
2. Para efecto de asignarle su cuenta de correo al usuario se debe contar un procedimiento para solicitar la cuenta de correo el momento del alta.
3. La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.
4. La longitud mínima de las contraseñas será igual o superior a ocho caracteres.

**2.3 Bases de Datos**

1. Ningún miembro del IT debe o puede eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

**3 Recursos de Cómputo**

**3.1 Seguridad de cómputo**

El equipo de infraestructura es el encargado de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas, así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo. Sin embargo, debido a la cantidad de usuarios y a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.

El equipo de IT debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.

Únicamente el equipo de IT está autorizado para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la red.

**3.2 Ingenieros de Soporte**

Los Ingenieros de Soporte tendrán las siguientes atribuciones y/o responsabilidades:

Podrán ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.

Deberán utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.

Deberán realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.

Deben actualizar la información de los recursos de cómputo de La Empresa, cada vez que adquiera e instale equipos o software.

Deben registrar cada máquina en el inventario de control de equipos de cómputo.

Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, música, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.

Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.

Reportar a la Gerencia los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

**3.3 Renovación de equipos**

Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.

Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al área de Tecnología a fin de que se seleccione el equipo adecuado. Sin el visto bueno de Tecnología no podrá liberarse una orden de compra.

**4 Uso de Servicios de Red**

**4.1 Servicios de red**

La Gerencia de informática definirá los servicios de Internet a ofrecer a los usuarios y se coordinará con el equipo de infraestructura para su otorgamiento y configuración.

El equipo de infraestructura es el responsable de la administración de contraseñas de redes y deberán guardar su confidencialidad.

No se darán equipo, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas profesionales en La Entidad, excepto por orden expresa del Gerente de Informática.

**4.2 Usuarios**

***4.4.2.1 Identificación de Usuarios y contraseñas***

Todos los usuarios con acceso a un sistema de información o a la Red, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recurso que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por Las Gerencias.

El usuario deberá notificar a IT en los siguientes casos:

Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.

Si tiene problemas en el acceso a los servicios proporcionados por el servidor.

Si un usuario viola las políticas de uso de los servidores, IT podrá cancelar totalmente su cuenta de acceso a los servidores, notificando a La Gerencia correspondiente.

***4.4.2.2 Responsabilidades Personales***

Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar a IT.

Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

Los usuarios sólo podrán crear archivos que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco del equipo de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

***4.4.2.3 Uso Apropiado de los Recursos***

Los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para cumplir las obligaciones y propósito de la operativa para la que fueron diseñados e implantados.

4.4.2.3.1 Queda Prohibido

El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.

Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de La Entidad.

Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.

Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos.

Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.

Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.

Cualquier fichero introducido en la Red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas Políticas y, en especial, las referidas a propiedad intelectual y control de virus.

**5 Antivirus**

Todos los equipos de cómputo de la entidad deberán tener instalada una aplicación de Antivirus.

Es responsabilidad del Administrador de Infraestructura mantener la consola de antivirus con definiciones actualizadas.

El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.

**6 SEGURIDAD PERIMETRAL**

La seguridad perimetral es método de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

El objetivo de la seguridad perimetral es:

Rechazar conexiones a servicios comprometidos

Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).

Proporcionar un único punto de interconexión con el exterior.

Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).

Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet

Auditar el tráfico entre el exterior y el interior.

Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

**6.1 Firewall**

La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.

Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.

El Administrador de Infraestructura gestiona las reglas en el Firewall necesarias bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.

El firewall debe bloquear las “conexiones extrañas” y no dejarlas pasar para que no causen problemas.

El firewall debe controlar los ataques de “Denegación de Servicio” y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.

Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

**6.3 Redes Privadas Virtuales (VPN)**

Los usuarios móviles y remotos de La Entidad podrán tener acceso al a red interna privada cuando se encuentren fuera de La Empresa alrededor del mundo en cualquier ubicación con acceso al Internet público, utilizando las redes privadas VPN IPSec habilitadas por el Área de Tecnología.

El equipo de infraestructura será el encargado de configurar el software necesario y asignar las claves a los usuarios para poder acceder a través de la VPN.

**6.4 Conectividad a Internet**

La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de La Entidad tienen las mismas responsabilidades en cuanto al uso de Internet.

El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.

.

Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

**6.5 Red Inalámbrica (WIFI)**

**6.5.1 Acceso a Funcionarios de La Entidad:**

La Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura de La Entidad. Donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.

Las condiciones de uso presentadas definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, Ipod, celulares, etc.) con capacidad de conexión Wireless.

El equipo de infraestructura es el encargado de la administración, habilitación y/o bajas de usuarios en la red inalámbrica de La Entidad.

**6.6 Restricciones/prohibiciones de acceso a Internet**

Con la finalidad de hacer un buen uso de la red inalámbrica, se aplicarán las siguientes prohibiciones:

El uso de programas para compartir archivos (Peer to Peer).

El acceso a páginas con cualquier tipo de contenido explícito de pornografía.

Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.

Uso de JUEGOS "on line" en la red.

**7. Vigencia y Revisión**

La presente política queda vigente desde el momento de su aprobación y debe revisarse en un período de 12 a 18 meses.