1 POLITICAS GENERALES

1.1. Velar por los recursos informáticos y servicios de red del MSP

1.2. La Dirección Nacional Administrativa es la responsable de la entrega y custodia de equipos

1.2.1. Las jefaturas serán las únicas autorizadas para el pedido de recursos informáticos

1.2.2. Solo el área de TIC's es la autorizada de realizar soporte y cambio en configuración de equipos del MSP

1.2.3. Los mantenimientos contratados deberán ser aprobados por la el departamento de Tecnologías de la Información y Comunicaciones.

Ministerio de Salud Pública

2. POLÍTICAS PARA EQUIPOS INFORMÁTICOS

2.1.	Efectuar mantenimientos preventivos y correctivos una vez al año
2.2.	La Dirección Administrativa es la responsable de la asignación de equipos informáticos
2.3.	La gestión de compra de equipos es responsabilidad de la Dirección Administrativa
2.4.	La generación del pedido para compras de equipos informáticos es responsabilidad de la TIC's.
2.5.	La conexión de equipos externos a la red del MSP requiere autorización de la TIC's
2.6.	En caso de hurto, robo o extravío de equipos informáticos se notificará a la Dirección Administrativa
2.7.	En caso de daño de equipos informáticos se notificará a la TIC's
2.8.	Solo la TIC's está autorizada a abrir los equipos informáticos
2.9.	Todos los equipos del MSP deben contar con un software antivirus OBLIGATORIAMENTE (licenciado o gratuito)
2.10.	Todos los equipos del MSP deben contar con un firewall personal
2.11.	Todos los equipos del MSP deben tener actualizados los parches de seguridad
2.12.	Todos los equipos del MSP deben tener el fondo definido por la Dirección Nacional de Comunicación, Imagen y Prensa

Ministerio de Salud Pública

3. ACCESO A SERVIDORES Y CENTROS DE DATOS

3.1. El acceso al centro de datos es exclusivo del personal informático de redes, comunicaciones, infraestructura y seguridad informática
3.2. Las claves de acceso a los servidores son de exclusiva administración del personal informático de redes, comunicaciones, infraestructura y seguridad informática
3.3. Las configuración de los servidores son de exclusiva administración del personal informático de redes, comunicaciones, infraestructura y seguridad informática
3.4. El monitoreo de enlaces y continuidad de los servicios y comunicaciones son responsabilidad del personal informático de redes, comunicaciones, infraestructura y seguridad informática

Ministerio de Salud Pública

4. PROPIEDAD DE LA INFORMACIÓN

4.1. Toda información generada y almacenada en cualquier equipo o medio electrónico dentro del MSP es propiedad de la Institución

4.2. La TIC's es la encargada de resguardar la información generada al interior de la Institución

Ministerio de Salud Pública

5. USOS INADECUADOS

5.1.	Violar los derechos de autor, software, patentes
5.2.	Difusión de información confidencial
5.3.	Instalación de software malware
5.4.	Utilizar la infraestructura tecnológica con ánimos de lucro
5.5.	Prohibido el uso de la tecnología de la Institución para generación de actividad hostil
5.6.	Prohibido realizar actividades que contravengan en la seguridad del software y/o sistemas de la Institución
5.7.	Prohibido realizar el monitoreo de puertos o análisis de tráfico, evaluación de seguridades y vulnerabilidades al interior de la Institución sin contar con la respectiva autorización de Gerencia
5.8.	Prohibida la violación de mecanismos de seguridad para evadir accesos
5.9.	Prohibido el ingreso a cuentas de usuarios no autorizados
5.10.	Prohibido interferir o negar el servicio de redes y comunicaciones tecnológicas
5.11.	Prohibida la instalación de cualquier tipo de software sin la autorización de la TIC's
5.12.	Prohibido cambiar los permisos en los recursos compartidos en la red
5.13.	Prohibido la descarga de música y videos (radio online)

Ministerio de Salud Pública

6. Excepciones

6.1. Los funcionarios que desempeñen funciones especiales, pueden solicitar accesos especiales mediante memorando sin que violen las políticas de la TIC's

Ministerio de Salud Pública

7. POLÍTICAS DE CONTRASEÑAS - USUARIOS

7.1. Las contraseñas deberán ser cambiadas al menos una vez cada tres meses / seis meses cuenta correo
7.2. Ante la sospecha de robo de contraseñas se debe efectuar el cambio inmediato y notificar el incidente a la TIC's
7.3. Las cuentas de usuario que tengan privilegios de sistemas deben ser distintas al resto de cuentas
7.4. Las contraseñas de acceso a los servicios serán proporcionadas por la TIC's previa la confirmación por parte de Talento Humano
7.5. La desactivación de contraseñas de ex funcionarios será realizada por la TIC's previa la confirmación por parte de Talento Humano.

Ministerio de Salud Pública

8. Selección de contraseñas

8.1.	Contraseñas mayores a 8 caracteres
8.2.	Mezclar caracteres alfanuméricos y símbolos
8.3.	No utilizar nombres ni información personal ni de familiares cercanos

Ministerio de Salud Pública

9. PROHIBICIÓN USUARIOS

9.1. Revelar o compartir contraseñas
9.2. Escribir o guardar la contraseña sin que sea encriptada
9.3.Comunicar las contraseñas por vía electrónica o telefónica
9.4. Utilizar el correo institucional para actividades comerciales
9.5. Participar en propagación de propagandas
9.6. Enviar o reenviar mensajes difamatorios
9.7. Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad el emisor
9.8. Distribuir mensajes con contenidos inapropiados

Ministerio de Salud Pública

10. INTERNET Y CORREO ELECTRÓNICO

10.1. El proveedor deberá garantizar mínimo el 99.6% de disponibilidad
10.2. La TIC's monitoreará las actividades de red, correo electrónico, internet y uso de red de datos
10.3. El acceso a estos recursos estará condicionado a la aceptación de la Política de Uso
10.4. El acceso al servicio de correo se lo realizará por medio de la página institucional
10.5. Las comunicaciones institucionales solo podrán ser efectuadas por medio del correo institucional
10.6. Los buzones de correo electrónico son propiedad de la Institución

Ministerio de Salud Pública

11. RESPONSABILIDAD DE LOS USUARIOS

11.1. Los usuarios son los únicos responsables de las actividades realizadas desde sus cuentas y buzones

11.2. La cuenta de correo es instranferible

11.3. Los correos deben ser marcados como urgentes únicamente cuando lo sean

11.4. La información recibida de manera personal y confidencial no podrá ser distribuida sin autorización del remitente

11.5. Un correo será impreso cuando sea indispensable tener un registro físico

Ministerio de Salud Pública

12. SEGURIDAD PARA LA INSTITUCIÓN

12.1. El usuario se compromete a crear contraseñas de características fuertes
12.2. El usuario debe notificar inmediatamente cualquier fallo de seguridad en su cuenta.
12.3. El usuario debe notificar cualquier mensaje sospechoso de origen desconocido
12.4. El usuario se compromete a notificar la recepción de cualquier mensaje con archivos sospechoso
12.5. No se utilizará el internet de la Institución para la distribución de actividades o materiales que vayan contra la Ley.
12.6. La TIC's asignará perfiles y roles de navegación para uso de los usuarios
12.7. Si se utiliza un dispositivo móvil (USB móvil) para conexión a Internet se deberá desconectar el equipo de la red de la Institución (cable o acceso inalámbrico)

Ministerio de Salud Pública

13. SOFTWARE

13.1. Mantener bajo resguardo las licencias de uso de software de la Institución
13.2. Mantener actualizado el catálogo de software (libre y licenciado), DESINSTALAR el software que no posea licencias o que no sea autorizado por la DNTIC's
13.3. La instalación de cualquier software libre deberá ser autorizado y verificado por la TIC's según decreto 1014
13.4. El software licenciado será utilizado cuando no exista software libre que supla las necesidades
13.5. Mantener un estándar del software permitido que deberá ser instalado en cada computador antes de entregar a los usuarios finales
13.6. Mantener un estándar del software permitido de uso exclusivo para la TIC's
13.7. No está autorizada la instalación de software pirata
13.8. No está autorizada la instalación de software descargado del Internet
13.9. No está autorizada la instalación de software de entrenamiento