ALCANCE:

El presente documento define las reglas y directrices para los miembros de la organización que permitan garantizar la seguridad Informática de CEDIMED S.A.S bajo los lineamientos del GRUPO QUIRONSALUD y, en consecuencia, tener unas políticas homogéneas para proteger las entidades conectadas en la red, así como la información contenida en las mismas.

La presente norma es aplicable a todos los usuarios que tienen una relación laboral con el Grupo, ya sea como usuario interno o externo que acceden a la red de la organización y que utilizan recursos informáticos.

CUMPLIMIENTO:

Toda práctica que vaya en contra de estas políticas o acción que comprometa la seguridad de la información de la organización, será causal de acciones disciplinarias.

DEFINICIONES:

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

POLITICA PARA EL USO DE LOS RECURSOS TECNOLOGICOS:

- Los empleados de CEDIMED S.A.S utilizarán únicamente software licenciado e instalado por la Empresa para el cumplimiento de las funciones de su cargo.

- Ningún usuario podrá instalar software diferente al autorizado para sus funciones, si fuese necesario algún software nuevo para el desempeño de sus labores, deberá ser solicitado al Departamento de Sistemas de Información.

- Los Equipos de cómputo solo deberán tener información laboral para el desempeño diario de su trabajo. El Departamento de Sistemas verificará periódicamente la información almacenada en su computador por medio de auditorías sin previo aviso.

- Queda expresamente prohibido copiar para uso personal o para terceros, información o software de propiedad de la empresa, tampoco modificar las configuraciones del software que puede alterar su funcionalidad.

- Los equipos de cómputo y/o equipos de oficina asignados para sus labores, no deberán moverse a otros puestos de trabajo sin la autorización del Departamento de Sistemas.

- Los empleados conservarán y restituirán en buen estado, salvo el deterioro natural, los equipos de cómputo y accesorios que se les haya sido asignados.

- Los Backup de los empleados no deberán contener información diferente a la laboral; Solo se realiza backup de la información solicitada por el usuario en los casos que aplique.

- Ningún usuario está autorizado para abrir o intervenir los equipos de cómputo y/o manipular sus componentes internos. Esta actividad solo debe ser realizada por el Departamento de Sistemas.

- CEDIMED S.A.S Prohíbe el uso de dispositivos de almacenamiento USB para evitar la infección de virus informáticos en el equipo y la red lógica corporativa a excepción de cargos que así lo requieran.

- Ningún proveedor, cliente o empleado podrá conectar a la red de CEDIMED S.A.S dispositivos informáticos (Portátiles, Celulares, Tablet, entre otros) sin la debida autorización del Departamento de Sistemas y con las validaciones que considere pertinentes.

- La única herramienta autorizada por la organización para la conexión de acceso remoto aprobada por excepción es la VPN corporativa, a través del agente Forticlient, quedando prohibido el uso de cualquier otra herramienta alternativa de conexión remota.

POLITICAS DE NAVEGACION SEGURA (INTERNET)

- El acceso a internet se brindará únicamente a aquellos usuarios que por requisitos específicos de sus funciones así lo requieran. Dicho acceso se debe utilizar sólo con el fin de ejecutar las actividades laborales que requiera su puesto de trabajo.

- Los usuarios no deberán realizar descargas a través de internet ya que estos pueden ser portadores de virus informáticos; En caso de requerirse la instalación de algún software, este deberá solicitarse al Departamento de Sistemas.

- Consultar páginas no autorizadas y realizar descargas de sitios no controlados puede suponer un peligro para los sistemas de información de la organización. El acceso a Internet desde equipos de la empresa será moderado y filtrado a través de herramientas de monitoreo.

- Se encuentra prohibido el acceso a páginas de contenido ilícito o que atenten contra la dignidad humana: aquellas que realizan apología del terrorismo, páginas con contenido xenófobo, para adultos, de ciber acoso, racista, o de contenido violento, etc.

- Se encuentra prohibida la creación de reglas automáticas de reenvío desde buzones de correo corporativos a correos externos (Ejemplo: Gmail, Hotmail, entre otros).

- Se encuentra prohibido el uso de correos personales para uso corporativo (Ejemplo: Yahoo, Hotmail, entre otros). El único dominio autorizado por la organización es @cedimed.com

- Se encuentra prohibida la descarga de ficheros, programas o documentos que contravengan las normas de la compañía sobre instalación de software y propiedad intelectual.

A continuación, se detallan los filtros habilitados y permitidos por la organización para la navegación:

Servicios	Regla
• **Correo electrónico**	
o Corporativo	✓
o Gmail	✓
o Hotmail / Yahoo	✗
o Otros	✗
• **Web Browsing**	
o Deportes	✓
o Salud y medicina	✓
o Drogas y alcohol	✓
o Noticias y actualidad	✓
o Banca, seguros y finanzas	✓
o Administración Pública	✓
o Investigación y ciencia	✓
o Tecnología e informática	✓
o Redes sociales	✗ *(Aprobado sólo: Facebook Twitter Instagram y LinkedIn para el área de Comunicaciones, Jefes y Directores)*
o Contenido para adultos	✗

Servicios	Regla
o Páginas de contenido ofensivo	✗
o Juegos y apuestas	✗
o Acoso cibernético	✗
o Video y Streaming	✗ *(Aprobado sólo para Médicos, Comunicaciones, Jefes y Directores*
o File sharing / Compartir archivos	*(Aprobado sólo: Dropbox y OneDrive Corporativo)*
o Malware o virus	✗
o Violencia, odio o racismo	✗
o Conexiones remotas	✗ *(A excepción de la VPN corporativa)*

✓ Acceso permitido ✗ Acceso no permitido

POLITICA DE USO DEL CORREO ELECTRÓNICO

- El correo es estrictamente para uso laboral, alineado al cumplimiento de las funciones y actividades del usuario, y sólo deberá ser utilizado para este fin.
- No se deben publicar las direcciones de correo corporativas en páginas web ni en redes sociales.
- Está prohibido el reenvío de correos corporativos a cuentas personales en la organización.
- No se permite la transmisión o reenvío cadenas o spam.
- Se encuentra prohibido el envío masivo o no justificado de cualquier tipo de información que no sea de carácter público.
- No utilizar el correo personal para fines laborales. Si se requiere una cuenta de correo esta deberá ser solicitada al Departamento de Sistemas, para que esta contenga el dominio @cedimed.com
- Borre “cadenas” de correo electrónico y correos con propaganda (spam) de su buzón, pueden generar riegos de seguridad y privacidad.
- Los usuarios deberán identificar correos fraudulentos y no abrir sus adjuntos cuando:

    - El cuerpo del mensaje presente cambios de aspecto (logotipos, pie de firma, etc.) con respecto a los mensajes recibidos anteriormente por ese mismo remitente
    - El mensaje contiene una «llamada a la acción» que nos urge, invita o solicita hacer algo no habitual.
    - Soliciten el envío de credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.).
    - El correo contenga cobros o multas sospechosas.
    - El remitente del correo no sea de una procedencia recurrente o cercana.

RECOMENDACIONES:

Al recibir un mensaje con un adjunto, este se debe analizar cuidadosamente antes de abrirlo.

Estas son algunas medidas para identificar un adjunto malicioso:

- Tiene un nombre que nos incita a descargarlo, por ser habitual o porque creemos que tiene un contenido atractivo.
- El icono no corresponde con el tipo de archivo (su extensión), se suelen ocultar ficheros ejecutables bajo iconos de aplicaciones como Word, PDF, Excel, etc.
- No se reconoce la extensión del adjunto y puede que se trate de un archivo ejecutable (hay muchas extensiones con las que no estamos familiarizados).
- Al recibir un mensaje con un enlace, antes de hacer clic el usuario deberá revisar si es una URL legítima, situándose sobre el texto del enlace, para visualizar la dirección antes de hacer clic en él.

POLITICAS PARA EL USO DE MENSAJERIA INSTANTANEA

- Para CEDIMED S.A.S el chat de mensajería instantánea es un mecanismo de comunicación formal dentro de la empresa, por lo tanto, esta información queda almacenada en la base de datos y podrá ser consultada si un ente superior así lo requiere.

- No se podrá utilizar programas de CHAT diferentes al corporativo para enviar y recibir mensajes dentro de la red interna. El único programa autorizado por la organización para la comunicación interna será el que los funcionarios del área de TI instalé en los diferentes equipos de la empresa. No se permite la instalación de ninguna otra aplicación de mensajería interna o externa.

- No está permitido el acceso, transmisión y retransmisión de cartas en cadena cualquiera sea su naturaleza, publicidad, ventas, mercadeo, promociones, videos y música al menos que estén relacionados con el trabajo en la organización.

- Para evitar congestiones y optimizar el uso de la red, se debe aplicar criterio en el tamaño de los archivos que se envían y el número de destinatarios. Además, evaluar la necesidad o no de enviar archivos gráficos, de audio o de video y cerciorarse de no enviar información con virus, verificando tener la versión más reciente del antivirus.

POLITICAS DE ANTIVIRUS

- Todos los equipos de la organización deben tener instalada una versión actualizada del software antivirus debidamente licenciado, capaz de proteger en tiempo real y de actualizarse de forma automática.

- Se deberá comunicar al Departamento de Sistemas de cualquier infección por virus o sospecha del mismo.

- Los usuarios no podrán desinstalar o cambiar el producto de antivirus existente en su equipo.

- Todos los dispositivos extraíbles como USB, CDs, Discos duros externos entre otros, antes de ser utilizados deben ser escaneados con el antivirus.

- No se permitirá conexión remota a la red de la organización ningún dispositivo sin el antivirus debidamente licenciado.

EXCEPCIONES:

Si por consideraciones técnicas de algunos recursos tecnológicos y/o proveedores no es posible instalar el software antivirus en los equipos de la red de la organización, estos deberán ser informados al Departamento de Sistemas de información indicando la justificación y en conjunto analizar las opciones para la mitigación del riesgo.

Las excepciones a esta directiva requerirán documentación del motivo y el razonamiento de la excepción. Dicha excepción también requiere la aprobación formal de una autoridad apropiada dependiendo del alcance de la excepción, además de la del Departamento de sistemas.

POLITICA PARA EL USO DE CONEXIONES REMOTAS

- Los equipos que se conecten a la red de la organización deberán cumplir con los siguientes requerimientos:

    - Antivirus vigente y activo.
    - Agente de monitorización instalado
    - Bloqueo de puertos

Estos requerimientos serán verificados por el responsable de TI. No obstante, en caso que el usuario detecte algún problema o ausencia de estas medidas deberá reportarlo a el responsable de TI para la verificación y subsanación correspondiente.

- CEDIMED S.A.S ha implementado una Red Privada Virtual o VPN que cuenta con una serie de controles y medidas que garantizar la seguridad de las comunicaciones para conexiones a la red fuera de la oficina. Esto ofrece una serie de ventajas, tales como:

    - Toda la información se transmite de manera segura gracias al cifrado de datos y de conexión.
    - Confidencialidad e integridad de la información: al ir cifrada, la información no puede ser leída, modificada o alterada durante la transmisión.
    - Restricción de acceso: a través de usuario y contraseña necesitando una previa autorización.
    - Control de estado de seguridad e instalaciones de actualizaciones.
    - Actualización a instalación de parches de seguridad.

En tal sentido, el uso de conexiones VPN es obligatorio bajo cualquier de las siguientes circunstancias:

- Uso de sistemas corporativos, portales internos o recursos de almacenamiento corporativos (servidores, bases de datos, etc.).
- Soporte remoto en caso de atención de incidencias.

- Ejecución de operaciones confidenciales: acceso a bases de datos, banca online o facturación, que impliquen la transmisión de usuarios, contraseñas, o cualquier otra información confidencial.
- Trabajo remoto y soporte y monitoreo de proveedores.

Dado todo lo anterior no está autorizado ningún otro software de conexión remota en la institución.

- En el caso que la organización detecte alguna actividad maliciosa o anómala por parte del usuario, se procederá a la desactivación inmediata del acceso VPN a fin de proteger la red interna y realizar las investigaciones de seguridad necesarias.

- Para que el túnel VPN funcione se recomienda como mínimo 20 megas de navegación, para un funcionamiento óptimo y eficiente se recomiendan 30 megas en adelante.

- Cualquier proveedor que requiera conectarse a la red de la organización deberá justificar y realizar la solicitud de esta conexión al personal de TI, el cual realizara su respectivo análisis y aprobación.

EXCEPCIONES:

Las excepciones a esta directiva requerirán documentación del motivo y el razonamiento de la excepción. Dicha excepción también requiere la aprobación formal de una autoridad apropiada dependiendo del alcance de la excepción, además de la del Departamento de sistemas.

POLITICA PARA EL USO DE CONTRASEÑAS

- Todas las claves de acceso a equipos de cómputo, software y/o sistemas de información son personales e intransferibles, por lo tanto, cada empleado será responsable de mantener la confidencialidad sobre ellas. Para garantizar la seguridad de la información las contraseñas deberán ser cambiadas periódicamente.

- Las contraseñas de los equipos de cómputo deben estar compuestas por caracteres alfanuméricos (números y letras), Las cuales deben contener 6 caracteres, como mínimo, No podrán reusarse ninguna de las contraseñas utilizadas y la contraseña deberá cambiarse de forma obligatoria cada 30 días.

- Bloquee su computador en el momento en que se retire del puesto de trabajo o se ausente por periodos indeterminados de tiempo.

- Para el acceso a los aplicativos Misionales Asistenciales (Historia Clínica, PACS-RIS y Laboratorio Clínico) se cuentan con los respectivos perfiles de acceso modularizados de cada una de las aplicaciones, en los cuales se limita el acceso dependiendo del perfil del usuario; se recomienda manejar contraseñas independientes por cada una de las aplicaciones.

POLITICA PARA ÁREAS SEGURAS Y PERÍMETRO DE SEGURIDAD FÍSICA

- Las áreas identificadas como sensibles para CEDIMED SAS deben tener un perímetro claramente definido, el cual restringe el acceso solo a usuarios autorizados. Por ejemplo, instalaciones de procesamiento de información crítica, centros de datos u oficinas de de TI e ingeniera Biomedica y áreas críticas de servidores.

- Las oficinas y Data Centers de TI son zonas de acceso restringido exclusivo para miembros autorizados de TI e Ingenieria Biomedica, solo se proporcionará acceso ocasional a personal externo por motivos de mantenimientos y actividades previamente concertadas.

- Los tiempos de estadía de personal externo en Oficinas de TI y Data Centers debe contar con el acompañamiento exclusivo de uno de los miembros del equipo de TI, en su defecto por un personal de Seguridad dispuesto por la Institución.

POLITICAS PARA EL RETIRO DE UN EMPLEADO

Con el objetivo de garantizar la Integridad, confidencialidad y disponibilidad de la información a continuación se detallan las normas que deben cumplirse estrictamente cuando la división de Gestión Humana notifica al departamento de sistemas el retiro de un empleado:

- Es responsabilidad del jefe inmediato el control y custodia del equipamiento asignado al empleado retirado. A través de la lista de chequeo de egreso, el jefe inmediato debe solicitar todos los insumos y equipo en buen estado que le fueron asignados para su labor, como diademas, equipo de oficina, tarjetas de ingreso entre otros.

- Inmediatamente se recibe el correo por parte de la división de Gestión Humana informando el personal retirado, se procede a realizar el bloqueo de todas sus cuentas:

    - Correo electrónico,
    - Usuario del computador y de red,
    - Usuario de Spark,
    - Acceso a Servinte,
    - Acceso a Historia Clínica
    - Acceso PACS, RIS, Kawak.
    - Acceso a aplicaciones diferenciales por cargo y funciones.