CONTROL DE CAMBIOS			
Act.	**Fecha**	**Páginas**	**Descripción**
01	2006.may.16	-	Lanzamiento
02	2008.feb.10	-	Actualización año 2008
03	2009.mar.19	-	Cambio de Formato. Se reorganiza el documento agregándole el aparte “Gestión de la Seguridad Informática”. Se revisan, ajustan y actualizan las políticas para el año 2009.
04	2010.abr.11	Todas	Asignación de código al manual. Se realiza revisión, ajuste y actualización de las políticas para el año 2010.
05	2011.mar.21	Todas	Se agregan políticas de acuerdo a la Norma Internacional ISO 27001. Se realiza revisión, ajuste y actualización de las políticas para el año 2011.
06	2012.abr.22	Todas	Se armoniza el manual con el panorama general de seguridad informática, incluyendo los Planes de Contingencia y el Plan de Continuidad del Negocio. Se actualizan los nombres de los cargos de quien elabora y revisa el Manual. Se realiza revisión, ajuste y actualización de las políticas para el año 2011.
07	2012.ago.13	22-28	Se incluye el ítem políticas de uso de las red de COOSALUD
08	2013.abr.02	6	Se incluye dentro del punto 2 “Manejo de Información” el siguiente ítem, teniendo presente que el tiempo de implementación es de 1 año “Todos los equipos pertenecientes a COOSALUD deberán estar sujetos al control de Aranda, cualquier equipo que no cumpla con lo indicado solo podrá acceder a internet a través de la red de invitados y no podrá tener acceso a los programas de trabajo.”
09	2013.abr.02	-	Se actualiza el documento
10	2013.dic.20	6	Se incluyeron dentro del punto 2 “Manejo de Información” las siguientes políticas: • Queda prohibido el uso de dispositivos de almacenamiento masivo para escritura de archivos. Se restringe el uso de unidades de CD/DVD regrabable
11	2016.feb.08	-	Se actualiza de acuerdo a la operación actual
12	2017.may.19	Todo	Se actualiza el documento

13	2021.abr.29	7,10,11,14 y 15	• Se agregó políticas de trabajo en casa (8.16) • Se actualizo el numeral dispositivo móviles y de proveedores • Se actualizo el numeral nombre de usuarios y contraseñas respecto a parámetros de SAP. • Se actualizo el numeral de responsabilidades del usuario. • Se actualizo el numeral de confidencialidad de la información.
14	2021.jun.17	-	• Se revisa y ajusta el documento
15	2021.jun.24	-	• Se revisa y ajusta el documento
16	2023.mar.01	-	• Se revisa y ajusta de acuerdo a la operación actual

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Enfocados en la protección de la plataforma tecnológica de COOSALUD, se ha estructurado el siguiente documento cuyo objetivo principal es definir una política de seguridad informática, en la cual se establezcan las reglas, normas, controles y procedimientos que regulen la forma en que COOSALUD prevenga, proteja y maneje los riesgos de seguridad informática en diversas circunstancias.
Las normas y políticas expuestas en este documento son de estricto cumplimiento, salvo en los casos donde la Alta Gerencia establezca las excepciones que considere necesarias. Esta normativa será revisada anualmente y podrá ser actualizada en cualquier momento, siempre y cuando se tengan presentes los estándares de seguridad de la información, los cuales serán notificados en forma pertinente a los usuarios de la plataforma tecnológica de COOSALUD.
Todo usuario que utilice los servicios que ofrece la red de COOSALUD y sus sistemas de información, debe conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

2. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Adware: Adware es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.
Alarma: Sonido o señal visual que se activa cuando se produce una condición de error.
Alerta: Notificación automática de un suceso o un error.
Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).
Amenaza Externa: Amenaza que se origina fuera de una organización.
Amenaza Interna: Amenaza que se origina en una organización.
Antispam: Es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios.
Antivirus: Es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.
Áreas seguras COOSALUD: áreas de tecnología donde se encuentran ubicados los servidores y equipos de red.
Ataques multi-etapas: Es una infección que normalmente implica un ataque inicial, seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un troyano que descarga e instala adware.
Ataques Web: Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.
Autenticación: Garantía de que una parte de una transacción informática no es falsa. La autenticación normalmente lleva consigo el uso de una contraseña, un certificado, un número de identificación personal u otra información que se pueda utilizar para validar la identidad en una red de equipos.
Blacklisting o Lista Negra: Es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.
Bot: Es una computadora individual infectada con malware, la cual forma parte de una red de bots (botnet).
Botnet: Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio.
Caballo de Troya: Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos.
Certificado: Los sistemas criptográficos utilizan este archivo como prueba de identidad. Contiene el nombre del usuario y la clave pública.
Ciberdelito: Es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Contraseña: Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales.
Cuarentena: Aislar archivos sospechosos de contener algún virus, de modo que no se pueden abrir ni ejecutar.
Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
Encriptación: La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos.
Exploits o Programas intrusos: Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.
Firewall: Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.
Grooming: Es una nueva forma de acoso y abuso hacia niños y jóvenes que se ha venido popularizando con el auge de las TIC, principalmente los chats y redes sociales.
Gusanos: Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, a diferencia de un Virus.
Ingeniería Social: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.
Keylogger: Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.
Malware: Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras.
Negación de servicio (DoS): La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o red para los usuarios. Un ataque distribuido de negación de servicio (DDoS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque.
Plataforma Tecnológica COOSALUD: Comprende todos los equipos de computo, sistemas operativos, software, medios de almacenamiento, redes, servicios de apoyo, aplicaciones, servidores, servicios de internet, camaras, kit de audio, dispositivos moviles, equipos de red, kit biometrico, servicio de impresión y servicio de digitalización
Pharming: Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del re-direccionamiento e ingresen información personal, como la información bancaria en línea, en el sitio fraudulento.

Phishing: Método más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.
Redes punto a punto (P2P): Red virtual distribuida de participantes que hacen que una parte de sus recursos informáticos estén a disposición de otros participantes de la red, todo sin necesidad de servidores centralizados. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware.
Riesgo: Posibilidad de que ocurra un evento negativo.
Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios.
Spyware o Software Espía: El software espía consta de un paquete de software que realiza un seguimiento y envía información confidencial o personal a terceros.
Virus: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario.
Vulnerabilidad: Es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.

3. ¿QUÉ ES SEGURIDAD DE LA INFORMACIÓN?

La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.
El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.
La seguridad de la información se encarga de garantizar la integridad, confidencialidad, disponibilidad de nuestra información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006].
Disponibilidad: Propiedad de que la información siempre sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006].
Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC5411- 1:2006].

4. OBJETIVOS

- Dar a conocer los lineamientos dispuestos para todos los usuarios, de modo que los procesos de negocios de COOSALUD se realicen de forma segura y por personal autorizado.
- Asegurar que la información gestionada a través de la plataforma tecnológica, cumpla con los principios de disponibilidad, autenticidad, integridad, confiabilidad y confidencialidad.
- Proteger la plataforma tecnológica de COOSALUD mediante una política de seguridad de la información que permita minimizar los riesgos de ocurrencia de una violación de la seguridad y detectar oportunamente intentos de violación, evitando los impactos adversos que puedan generarse de la misma.
- Concientizar a los usuarios finales de la plataforma tecnológica de COOSALUD, en el buen uso de los recursos tecnológicos que esta pone a su disposición para el desempeño de sus funciones.

5. VIGENCIA

La documentación presentada como normativa de seguridad entrará en vigencia desde el momento en que ésta sea aprobada como documento técnico de seguridad informática por la alta dirección de COOSALUD. Esta normativa debe ser revisada y actualizada anualmente, o en el momento en que haya la necesidad de realizar cambios sustanciales en la plataforma tecnológica de la COOSALUD.

6. MISIÓN

Establecer las directrices necesarias para el correcto funcionamiento de un sistema de gestión para la seguridad de la información, enmarcando su aplicabilidad en un proceso de desarrollo continuo y actualizable, apegado a los estándares de la 27001 desarrollados para tal fin.

7. ALCANCE

- Las políticas de seguridad descritas en el presente documento establecen los lineamientos para proteger, controlar y mantener la plataforma tecnológica de COOSALUD.
- Las políticas de seguridad aplican a cualquier activo que hace parte de la Plataforma tecnológica de COOSALUD y a todos los usuarios que hagan uso de la misma, entre los cuales se encuentran empleados, proveedores, socios de negocio o terceros. Estas políticas también cubrirán cualquier equipo que no sea propiedad de COOSALUD y requiera conectarse, ingresar o acceder a la Red de Corporativa.
- En caso de incumplimiento de esta normativa, COOSALUD se reserva el derecho de veto sobre el personal que haya cometido la infracción, así como la adopción de las medidas sancionatorias que se consideren pertinentes.

8. POLÍTICAS

8.1 CAPACITACIÓN DE USUARIOS

- Los usuarios de los servicios de la plataforma tecnológica de COOSALUD serán capacitados para que tengan conocimiento de las políticas de seguridad y manejo de la información.
- Los usuarios firmaran documento de aceptación y conocimiento de la política de seguridad y manejo de la información de COOSALUD.

8.2 CONFIDENCIALIDAD DE LA INFORMACIÓN

- La información que se maneja en COOSALUD solamente podrá ser utilizada con fines empresariales.
- Toda persona, ya sea empleado o un tercero que tenga acceso a la información de COOSALUD deberá considerar que dicha información, por defecto, es de carácter confidencial y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.
- Toda relación laboral o comercial que Coosalud establezca con empleados o terceros debe incluir en el contrato o en otro documento una cláusula de acuerdo de confidencialidad de la información.
- El área de gestión humana en el proceso de contratación se encargará de hacer firmar un acuerdo de confidencialidad con el funcionario.
- Todo usuario que tenga acceso a información confidencial, deberá protegerla contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso.
- Se utilizará el menor número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.
- Las herramientas y servicios informáticos asignados a cada usuario son para uso limitado a la función empresarial.
- La información confidencial de terceros que por cualquier circunstancia se conozca por parte de COOSALUD, debe ser tratada bajo los mismos lineamientos establecidos para el tratamiento de la información confidencial de COOSALUD.
- No usar la información con el fin de obtener beneficio propio o de terceros.
- El acceso físico a las “áreas seguras” está permitido sólo para personal autorizado.
- Todo trabajo ejecutado en áreas seguras, por personal interno o externo, deberá realizarse bajo supervisión del personal de sistemas.
- Se acompañará a los visitantes en áreas seguras y se registrará la fecha y hora de su entrada y salida.

- Está prohibido dentro de las áreas seguras el uso de medios de almacenamiento de información tales como memorias USB, discos duros portables, CD-ROM, DVD-ROM, discos BLU-RAY o cualquier otro dispositivo magnético, salvo previa autorización del área de tecnología.
- Es responsabilidad del área de Sistemas la supervisión y mantenimiento de los equipos ubicados en las áreas seguras.
- Se prohíbe el consumo de alimentos o bebidas en las áreas seguras.
- El acceso a servidores y el uso de equipos de trabajo de la compañía por parte de terceros solo podrá realizarse con la autorización del Área de Sistemas.

8.3 CONTROL DE ACCESO A APLICACIONES

- El area de gestión humana debe realizar la solicitud de creación de usuarios de acceso a la plataforma tecnologica de cada funcionario, especificando las aplicaciones y el perfil.
- El area de sistemas de Coosalud debe crear los usuarios y perfiles, asignando un ID o nombre de usuario y una contraseña única para cada funcinario interno o externo.
- El area de sistemas de Coosalud debe desactivar los usuarios y perfiles, una vez el empleado firma su retiro (paz y salvo) previa notificación y autorización del area de gestion humana.
- El area de sistemas debera mantener registro de cada una de las solicitudes de acceso.

8.4 USO APROPIADO DE LOS RECURSOS

La plataforma tecnológica que COOSALUD pone a disposición del personal, está disponible exclusivamente para el cumplimiento de las obligaciones laborales y propósito de la operatividad para la que fue diseñada e implementada. En relación a la plataforma tecnológica, , se estableceran reglas de seguridad informatica para evitar lo siguiente:

- Utilizarla para actividades no relacionadas con el propósito del negocio.
- Utilizarla para acceder a recursos externos con propósitos ilegales o no autorizados.
- Hacer mal uso, reubicar o modificar sin la debida autorización, hurtar o dañarla a propósito.
- Utilizar equipos y/o aplicaciones que no estén permitidos en COOSALUD.
- Publicar o divulgar contenidos obscenos, discriminatorios, ilegales, fraudulentos, amenazadores, inmorales u ofensivos, cualquier tipo de virus, dispositivo lógico, dispositivo físico u otras amenazas que puedan causar alteración o daño.
- Realizar copias no autorizadas de software de COOSALUD, dentro y fuera de sus instalaciones.

- Descargar, instalar o compartir algún tipo de software que no esté autorizado por el área de sistemas de COOSALUD.
- Falsificar y duplicar un producto informático de COOSALUD.
- Capturar sin autorización la información de los accesos de otros usuarios.
- Transgredir o burlar los controles de acceso u otros mecanismos de seguridad implementados en COOSALUD.
- Violar cualquier ley o regulación nacional o internacional respecto al uso de sistemas de información.

8.5 PROTECCIÓN FRENTE A VIRUS Y AMENAZAS SIMILARES

La seguridad de la infraestructura de hardware y software de Coosalud se describe en el documento "TIC-M-16 MANUAL DE INFRAESTRUCTURA Y SEGURIDAD DE TICS".

- Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles.
- El software antivirus se deberá instalar, mantener siempre habilitado y actualizado en todos los servidores y equipos de cómputo para reducir el riesgo operacional asociado con los virus u otro software malicioso.
- Todos los equipos y servidores de oficinas o centros de datos, sus redes estaran protegidas con Firewall para tener seguridad periferica.

8.6 INTERCAMBIO DE INFORMACIÓN

- Los usuarios no deben ocultar o manipular su identidad bajo ninguna circunstancia.
- La distribución de información ya sea en formato digital o papel se realizará mediante herramientas facilitadas por COOSALUD para las funciones del cargo. COOSALUD se reserva, en función del riesgo identificado, la implementación de medidas de control e inspección sobre estas herramientas.
- Se estableceran reglas de seguridad informatica para evitar lo siguiente:
    - Transmisión o recepción de material protegido por Copyright o cualquier otra ley de propiedad intelectual.
    - Transmisión o recepción de archivos que infrinjan la Ley de Protección de Datos de Carácter Personal o directrices de COOSALUD.

- Uso de dispositivos de almacenamiento externos (USB, CDs, DVDs, entre otros) sin previa autorización del área de sistemas. (Crear documento de exclusiones)
- Todas las actividades que puedan dañar la buena reputación e imagen de la COOSALUD.
- Compartir recursos (Carpetas, Archivos, etc.) con permiso de control total a los roles y perfiles. Al compartir recursos se debe configurar usuario(s) y permisos específicos (Lectura o Escritura).

8.7 USO DEL CORREO ELECTRÓNICO

- Se considerará al correo electrónico como una herramienta más de trabajo provista al empleado con el fin de ser utilizada para propósitos laborales.
- El área de sistemas está en la facultad de implementar sistemas de control destinados a velar por la protección y el buen uso de este recurso.
- El sistema de correo electrónico de COOSALUD no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores, publicitarios, piramidales u otro tipo de comunicados similares.
- Las cuentas de correo son personales e intransferibles. El propietario de la cuenta es el único responsable de la privacidad de la clave de acceso a su cuenta, cualquier acción efectuada desde ésta cuenta será atribuida a dicho propietario. Salvo el caso cuando sea autorizado por el área de gestión humana.
- La apertura de archivos adjuntos debe hacerse siempre y cuando se conozca con claridad el remitente y el asunto. Es responsabilidad del usuario el cuidado de ejecutar archivos de fuentes desconocidas, o ciertos archivos como fotos o imágenes reenviadas vía email.
- Los usuarios de los correos electrónicos institucionales que adjunten documentos que no son propios deberán citar siempre la fuente de origen con la finalidad de respetar los derechos de propiedad intelectual.
- La Presidencia de COOSALUD, con el apoyo del área de sistemas, se reserva el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para su seguridad.
- La creación de los correos electrónicos institucionales es responsabilidad del área de sistemas de COOSALUD, quien define los nombres, estructura y plataforma que se utilizará.

8.8 CONECTIVIDAD A INTERNET

- Los usuarios no deben ingresar a sitios en Internet que no sirvan como soporte al cumplimiento de su trabajo diario.
- El acceso a Internet desde la red corporativa se restringe por medio de dispositivos y reglas de control incorporado en la misma.

- La utilización de otros medios de conexión a Internet diferentes a los asignados por COOSALUD deberán ser autorizados por el área de sistemas.
- Los usuarios no deberán usar el nombre, símbolo o logotipo de COOSALUD en ningún elemento de Internet no justificado o autorizado por actividades estrictamente laborales.
- Se estableceran reglas informaticas para evitar la descargar programas, juegos, archivos multimedia o cualquier información de Internet que no esté relacionada con actividades laborales.
- Los usuarios no podrán utilizar cualquier software o dispositivo tecnológico, para violar u omitir la seguridad.

8.9 RESPONSABILIDADES DE USUARIOS

- Cada usuario es responsable de su Nombre de Usuario (Login) y contraseña, el cual es asignado para el acceso a la plataforma tecnológica de COOSALUD, por lo que es imprescindible que este sea únicamente conocido por el propio usuario, no deberá revelarse al resto del personal.
- Los archivos del usuario deberán ser guardados en la carpeta definida para sincronizar con ONEDRIVE, para que se pueda realizar backups automáticos de dicha información.
- Todo funcionario al finalizar su jornada laboral, deberá apagar los recursos tecnológicos que utilizó durante la misma.
- Los usuarios deberán seguir las siguientes directivas en relación a la gestión de las contraseñas:
    - Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
    - Seleccionar contraseñas de calidad, cumpliendo las características descritas en la política de Nombres de usuario y contraseñas que se presenta en este documento.
    - Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
    - Cambiar las contraseñas temporales en el primer inicio de sesión (“login”).
    - Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función, macro o cache del navegador.
    - Notificar cualquier incidente de seguridad relacionado con sus contraseñas como pérdida, robo o indicio de pérdida de confidencialidad.
    - Los usuarios deberán velar por que los equipos queden protegidos cuando vayan a quedar desatendidos. Bloquear la pantalla cuando se ausenten del puesto de trabajo.
    - El parametro login/fails en SAP se configura en 2, lo cual se bloquea automaticamente el acceso al SAP despues de 2 intentos fallidos de la contraseña.
    - El parametro rdisp/gui_auto_logout de SAP se configura en 1790 segundos, lo cual se bloquea el acceso al SAP por inactividad en la sesion por 1790 segundos.

8.10 NOMBRES DE USUARIOS Y CONTRASEÑAS

- El personal que accede a la plataforma tecnológica de COOSALUD, es responsable de asegurar que ésta sea para el propósito para el cual fue creada e implementada.
- Para ingresar a la plataforma tecnológica de COOSALUD, el usuario debe disponer de un acceso autorizado (Nombre de usuario y contraseña), sobre el que deben seguir los siguientes procedimientos de actuación:
  - Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
  - La contraseña debe cumplir la siguiente directiva:
    - ✓ longitud mínima de la contraseña deberá ser de 8 caracteres.
    - ✓ No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.
    - ✓ Incluir caracteres de tres de las siguientes categorías:
      - ❖ Mayúsculas (de la A a la Z)
      - ❖ Minúsculas (de la a a la z)
      - ❖ Dígitos de base 10 (del 0 al 9)
    - ✓ Caracteres no alfanuméricos (¡por ejemplo, !, $, #, %)
    - ✓ No repetir ninguna de las 5 contraseñas anteriores.
    - ✓ Como recomendación, la contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos, etc.
    - ✓ No utilizar la misma contraseña para propósitos profesionales y no profesionales.
  - En el primer inicio de sesión, el usuario está obligado a cambiar la contraseña asignada.
  - En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 60 días.
  - Los usuarios no deben revelar bajo ningún concepto su contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
  - Si un usuario tiene sospechas de que su nombre de usuario está siendo utilizado por otra persona, debe proceder al cambio de su contraseña y notificar al área de sistemas.
  - Cada usuario es responsable de su Nombre de Usuario (Login) y contraseña, el cual es asignado para el acceso a la plataforma tecnológica de COOSALUD, por lo que es imprescindible que este sea

únicamente conocido por el propio usuario, excepto que sea autorizado por Gestión Humana o la Gerencia de la Sucursal cuando el usuario no está activo en sus funciones indicando a quien se le da acceso y por cuanto tiempo a través de un correo electrónico al subdirector de sistemas.

- El parametro login/min_password_specials se configura en 1, lo cual exige que la contraseña tenga al menos 1 carácter especial.
- El parametro login/min_password_digits se configura en 1, lo cual exige que la contraseña tenga al menos 1 carácter numerico.

8.11 PUESTO DE TRABAJO LIMPIO

Se establecen las siguientes políticas de puesto de trabajo limpio con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información:

- Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- No dejar información confidencial expuesta en la pantalla de los equipos.
- Proteger los puntos de recepción y envío de información (correo postal, máquinas de scanner, fax, fotocopiadoras e impresoras).
- La reproducción o envío de información con este tipo de dispositivos, queda bajo la responsabilidad del usuario.
- Al imprimir una información confidencial se debe resguardar.

8.12 EQUIPOS DE USUARIOS

Sobre el equipamiento informático asociado al puesto del personal se establecerán las siguientes políticas:

- Todos los recursos informáticos con acceso a la información de COOSALUD estarán controlados por la compañía. Los recursos externos deberán contar con la debida autorización del área de sistemas.
- Se prohíbe la captura de tráficos de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de monitoreo expresamente autorizadas por el área de sistemas.
- El usuario no podrá retirar de las instalaciones de COOSALUD, cualquier equipo tecnológico sin la debida autorización del área de sistemas.
- Ningún usuario podrá manipular, sustraer y modificar las configuraciones de los equipos de cómputo.

8.13 SOFTWARE

- Todo el personal que accede a la plataforma tecnológica de COOSALUD debe utilizar únicamente las versiones de software facilitadas y vigentes aprobadas por el área de sistemas.
- Se prohíbe borrar o eliminar cualquiera de los programas instalados, sin la debida autorización del área de sistemas.

8.14 ACCESO A LA RED

- Las conexiones externas a la red se realizarán requiriendo la autenticación previa del usuario mediante la utilización de redes privadas virtuales VPN o líneas dedicadas.
- No se deberá conectar a ninguno de los recursos de COOSALUD equipos de comunicaciones (tarjetas, módems, switche, router, AP, repetidor, etc.) que posibiliten conexiones alternativas no controladas a la red corporativa.
- Nadie deberá conectarse a la plataforma tecnológica a través de otros medios que no sean los definidos por el área de sistemas.
- La conexión a la plataforma tecnológica por parte de los empleados de la organización solo podrá realizarse a través del equipo que le ha sido asignado por el área de sistemas. En caso de requerir acceso en un equipo ajeno a la compañía, se deberá conectar a la red de invitados.
- Se prohíben los cambios en cualquier configuración de recursos de red por parte de cualquier empleado que puedan causar inestabilidad en el acceso a la plataforma tecnologica.
- En cualquier momento se podrá monitorear el uso de servicios de red a un empleado para establecer si los recursos se están usando de manera adecuada.
- Los empleados no podrán utilizar los servicios de red para actividades que no estén relacionadas con las obligaciones laborales. Está prohibido el uso de los servicios de red para activar y utilizar clientes p2p, conexión a enjambres de datos ajenos a la compañía como servidores de Torrent, redes de blockchain, mineria de datos, entre otros.
- Está prohibido el uso de sistemas operativos diseñados para actividades que atenten contra la seguridad informática.
- Está prohibido las siguientes acciones:
    - Acceso, uso, puesta a prueba, exploración o escucha no autorizada de la plataforma tecnologica de COOSALUD.
    - Bombardeo de correo (uso de mail bombers), inundación de tráfico (TCP Syn Flooding), intentos de denegación de servicio y/o difusión de virus o cualquier otro tipo de software malicioso que se ejecuten o afecten la plataforma tecnologica de COOSALUD.

- Realizar cualquier tipo de suplantación mediante información falsa a nivel de direcciones MAC, encabezados IP o TCP, y/o encabezados a nivel de datos de protocolos de aplicación.
- Activación, sin previa autorización, de programas que consuman de manera no controlada tiempo de procesamiento en servidores y equipos institucionales.

8.15 DISPOSITIVOS MÓVIL Y DE PROVEEDORES

En el caso de que algún usuario tenga configurado en sus dispositivos móviles (Smartphone, Tablets) aplicaciones que tengan acceso a la informacion de la empresa como el correo electrónico corporativo, programas para compartir archivos como One Drive, deberá seguir las siguientes recomendaciones:

- Es responsabilidad del usuario hacer buen uso del dispositivo móvil, el usuario debe asegurar la información que enviará a través de canales inalámbricos y abstenerse de utilizar estos recursos para enviar información confidencial o crítica que pueda poner en riesgo los activos de información de la compañía.
- Activar mecanismos de bloqueo de teléfono automáticamente, después de un periodo de tiempo, para evitar realizar acciones accidentales por presionar teclado o transferencia de información táctil.
- Evitar acceder a conexiones WI-FI no cifradas, pues el tránsito de información en esos casos no está asegurado y puede ser accesible a terceros.
- No responder mensajes de dudosa procedencia que hacen referencia a haber ganado premios de concursos desconocidos o que incitan a hacer llamadas a números telefónicos sospechosos.
- Evitar utilizar el dispositivo en zonas peligrosas como el transporte público, la calle o centros comerciales, pues se hace atractivo para robos.
- Evite abrir correos electrónicos de dudosa procedencia en el dispositivo y descargar archivos adjuntos que no esté esperando.
- No dejar el bluetooth encendido si no se está usando.

8.16 POLITICA DE TRABAJO EN CASA

- La conexión remota a la red de área local de Coosalud debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, configurada y auditada, por el Área de TICs.
- Los perfiles de acceso remoto de la VPN a los sistemas informáticos y activos de información de la Entidad, se autorizan de acuerdo a las necesidades específicas del área solicitante. Sin embargo el área de tecnología debe evaluar de acuerdo al principio del menor privilegio la limitación de los accesos.
- Se recomienda que mientras se haga uso de VPN desde un equipo personal, éste tenga instalado y actualizado el antivirus y que el sistema operativo cuente con las actualizaciones de seguridad.

- El área de Tecnología proporcionará el acceso a herramientas colaborativas de tipo corporativo tales como chat persistente y videoconferencia; para que los empleados puedan comunicarse entre sí. Estas herramientas sirven como medio de confirmación directo ante solicitudes que ingresen por correo electrónico catalogadas con caracter de urgencia y que induzcan a la ejecución de tareas sensibles tales como una transferencia inmediata de fondos.

8.17 POLÍTICA DE BACKUP

- Toda información crítica de Coosalud EPS almacenada dentro de la infraestructura tecnológica, se le debe hacer backup con la frecuencia necesaria soportada por el procedimiento TIC-P-16 GESTION DE BACKUPS.
- Se deben hacer pruebas periódicas de restauración para garantizar el buen estado de la información almacenada.