Tabla de Contenido

1. Macroproceso

Gestión Tecnología

2. Responsables de la Política

Generación de la Política: Jefe de Tecnologías e Información
Actualización, socialización y verificación del cumplimiento de la política: Analista de Seguridad Informática
Autorizador de la Política: Gerente de SAVIA SALUD EPS.

3. Introducción

Las políticas de seguridad de la información tienen como objeto construir las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) que se utilizan en SAVIA SALUD EPS.

Este documento describe las políticas de seguridad de la información definidas por la EPS. Para la elaboración del mismo, se toman como base el Modelo de Seguridad y Privacidad de la Información, que a su vez se basa en la norma ISO 27001:2013, las recomendaciones del estándar ISO 27002:2013 y la normatividad colombiana sobre privacidad de la información, en especial la ley 1581 de 2012, la ley 1712 de 2014 y sus decretos reglamentarios respectivos.

4. Justificación

Las políticas incluidas en este manual se constituyen como parte fundamental de los sistemas de información de la EPS y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La seguridad de la información es una prioridad para SAVIA SALUD EPS y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia de cada una de estas políticas.

5. Alcance

Las Políticas de seguridad de la Información son aplicables a toda la EPS, sus empleados, contratistas, practicantes, consultores incluyendo a todo el personal externo y afiliados (de ahora en adelante integrantes de la EPS) que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica y sus canales de comunicación.

6. Objetivo general

Establecer las políticas necesarias para los integrantes de la EPS para proteger la información de SAVIA SALUD a través de normas y acciones de aseguramiento teniendo

en cuenta los requisitos legales, operativos y tecnológicos de la entidad alineados con el contexto de direccionamiento estratégico.

7. Público objetivo

- Todos los integrantes de SAVIA SALUD EPS.

8. Marco Legal

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC Colombiana 27001:20013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos

LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República

DECRETO 1377 DE 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012

LEY 1712 DE 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

DECRETO 103 DE 2015 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

9. Políticas

9.1. Vigencia

Cada día las amenazas están en continuo proceso de expansión, lo que, unido al progresivo aumento de los sistemas de información, hace que todos los sistemas y aplicaciones estén expuestos a riesgos cada vez mayores, que sin una adecuada gestión de los mismos, pueden ocasionar que su vulnerabilidad se incremente y por consiguiente los activos se vean afectados, es por este motivo que los integrantes de la EPS son responsables del cumplimiento de las políticas de seguridad de la información. Cabe destacar que este nivel de responsabilidad va a ser conocido por las diferentes áreas quienes serán las garantes de que esta información sea conocida por cada integrante de área.

El manual presentado como Políticas de Seguridad de la Información entrará en vigencia desde el momento en que sea aprobado por la Gerencia.

9.2. Revisión de la política

Las Políticas de Seguridad de la Información se deberán revisar y actualizar anualmente conforme a las exigencias de la EPS o en el momento en que haya la necesidad de realizar cambios sustanciales en su contenido motivados por identificación de nuevos riesgos, vulnerabilidades y/o se hayan generado cambios significativos en la infraestructura tecnológica de la entidad.

9.3. Política general de seguridad de la información

La gerencia de SAVIA SALUD EPS, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Modelo de Seguridad y Privacidad de la información (MSPI) buscando establecer un marco de confianza en el ejercicio de sus deberes con sus afiliados, empleados y proveedores, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad. Para SAVIA SALUD EPS, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus empleados, practicantes, proveedores y afiliados, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del MSPI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus afiliados, socios, proveedores y empleados.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los empleados, proveedores, practicantes y afiliados de SAVIA SALUD EPS.
- Garantizar la continuidad del negocio frente a incidentes.

SAVIA SALUD EPS ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación se establecen 12 principios que soportan el Modelo de Seguridad y Privacidad de SAVIA SALUD EPS:

- Las responsabilidades frente a la seguridad y privacidad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, practicantes, proveedores y afiliados.

- SAVIA SALUD EPS protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros, o como resultado de un servicio en outsourcing.

- SAVIA SALUD EPS protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- SAVIA SALUD EPS protegerá su información de las amenazas originadas por parte del personal.
-
- SAVIA SALUD EPS protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- SAVIA SALUD EPS controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- SAVIA SALUD EPS implementará control de acceso a la información, sistemas y recursos de red.
-
- SAVIA SALUD EPS garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
-
- SAVIA SALUD EPS garantizará, a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.
-
- SAVIA SALUD EPS garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

-
- SAVIA SALUD EPS garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

9.4. Gestión de Activos de Información

Es necesario, para una eficiente gestión de seguridad de la información, realizar una adecuada identificación, clasificación, devolución y disposición de los activos de información de la entidad, tanto los tangibles (p. ej. hardware) como intangibles (p. ej. software e información), procurando que su descripción se encuentre siempre actualizada. A continuación se exponen las principales directrices para desarrollar estas labores:

- *Identificación y Clasificación de Activos*. Para la descripción y clasificación de los activos de información se debe desarrollar un documento denominado *Registro de Activos de Información*, de acuerdo con los lineamientos establecidos en la Ley 1712 de 2014 y el Decreto 103 de 2015. Este documento se debe revisar y si es del caso actualizar al menos 1 vez al año, o cuando se identifiquen necesidad de reflejar cambios en este.

- *Etiquetado o rotulado de Activos*. En el caso de activos tangibles, tales como equipos de cómputo, impresoras, dispositivos móviles, dispositivos extraíbles, etc, se deberá realizar un etiquetado de tal manera que se identifique inequívocamente cada uno de estos. En el caso de que estos pertenezcan a algún proveedor, se deberá exigir esta actividad en el contrato respectivo.

  Devolución de Activos. Cuando un integrante de SAVIA SALUD EPS se retira de esta, debe devolver los activos de información que hayan sido asignados a El. La recepción debe ser realizara por la dependencia que le asignó dicho activo.

- *Disposición de Activos*. Se debe contar con un procedimiento para realizar la baja de un activo de información, teniendo en cuenta la conservación de la información allí almacenada y los lineamientos entregados por el programa Gobierno Digital (Decreto 10018 de 2018).

- *Gestión de Medios Removibles*. Los medios removibles son dispositivos electrónicos que pueden ser insertados y/o extraídos de los equipos de cómputo, y son usados para el almacenamiento de información. Para su uso, el jefe respectivo de quien lo usará debe realizar la solicitud a la Mesa de Ayuda, informando las características del dispositivo, tipo de uso que se le dará, tiempo de uso, etc. La

Jefatura de Tecnologías e Información, a través de la Coordinación de Infraestructura, deberá tener control sobre el uso de estos en todos los equipos de cómputo usados en la entidad.

- *Protección de datos personales*. Savia Salud EPS se compromete con el cumplimiento de la Ley 1581 de 2012 y el Decreto 1377 de 2013.

- *Confidencialidad*. Para procurar un alto nivel de confidencialidad en el manejo de la información relacionada, por una parte con datos personales en especial los que hacen parte de la historia clínica y/o de la situación de salud de una persona, orientación sexual o religiosa de un afiliado, o de datos personales de menores de edad, entre otros datos sensibles, y de otra parte e información transaccional de la Entidad, Savia Salud EPS deberá firmar un acuerdo de confidencialidad en el contrato laboral, o de prestación de servicios. Adicionalmente, deberá establecer los adecuados controles tecnológicos que minimicen el riesgo de la ruptura de la confidencialidad respectiva.

- *Alcance del uso de los activos de información*. Los integrantes que desarrollen actividades laborales para SAVIA SALUD, deben garantizar que el acceso a la información y la utilización de la misma sea exclusivamente para actividades relacionadas con funciones propias de la EPS y que ésta sea utilizada de acuerdo con los criterios de seguridad.

- *Configuración, Soporte y Mantenimiento de activos*. Los integrantes de la EPS no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. El personal del área de Tecnología e Información o delegados por ellos, son los únicos autorizados para realizar la instalación y mantenimiento de cualquier tipo de software o hardware en los equipos de cómputo.

- *Administración remota*. Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información. Todo uso de aplicaciones de conexión remota por parte de los integrantes de SAVIA SALUD EPS deberá ser previamente solicitado por el respectivo jefe inmediato a la Mesa de Ayuda. La Jefatura de Tecnologías e Información, por medio de la Coordinación de Infraestructura, deberá tener el control y seguimiento al uso de dichos aplicativos.

- *Almacenamiento de activos intangibles*. Toda la información propia de la gestión de SAVIA SALUD debe residir en las bases de datos, en la red (unidad de red de área), en medios de almacenamiento externo entregado y/o respaldado por tecnología, nunca en los discos duros de las estaciones de trabajo. Esta acción hará responsable en caso de presentarse pérdida de información, al respectivo usuario.

- *Dudas sobre el manejo de activos*. Los integrantes de SAVIA SALUD deberán solicitar apoyo al área de Tecnología e Información por medio de los canales dispuestos por la mesa de ayuda (línea y correo electrónico) ante cualquier duda en el manejo de los recursos de cómputo de la EPS.

9.4.1. Mensajería en la nube

Savia Salud EPS gestiona la mensajería electrónica a través de la suite de Google G Suite, la cual tiene incorporadas múltiples aplicaciones, entre las que se destacan el correo electrónico, el calendario, el drive, herramientas ofimáticas, entre otras.

Para la autenticación a G Suite se cuenta con una única contraseña y un usuario bajo el dominio @saviasaludeps.com.

El servicio de correo ha sido concebido como medio formal de comunicación y es una herramienta de uso institucional, por lo tanto, debe darse un uso racional mediante el envío de comunicaciones cortas y precisas. Las comunicaciones electrónicas deben tener las características básicas de cordialidad, respeto, deben observarse los conductos regulares y seguir los siguientes lineamientos:

- Se debe proteger el servicio de correo electrónico frente a problemas que se materializan por estos medios tales como: correo no solicitado (en su expresión inglesa “spam”), programas dañinos constituidos por virus, gusanos, troyanos, espías, código móvil, entre otros.

- El correo electrónico no se debe usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la EPS, tales como cadenas, publicidad y propaganda comercial, política, social, etcétera).

- Los integrantes de SAVIA SALUD deben evitar abrir correos con archivos adjuntos desconocidos o con mensajes sugestivos.

- No se debe utilizar el correo para realizar inscripciones en redes sociales, foros entre otros, excepto para inscripciones institucionales.

- La Jefatura de Tecnología e Información por medio de la Mesa de Ayuda será la única área encargada de crear las cuentas de G Suite a los usuarios para el uso de correo electrónico. Para efecto de asignarle la cuenta al usuario, la Jefatura de Gestión Humana deberá informar a la Mesa de Ayuda el ingreso del funcionario a la EPS, y deberá ser su respectivo jefe directo quien solicite la creación de la cuenta

- La cuenta será activada en el momento en que el usuario ingrese por primera vez a G Suite y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.

- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán deberán estar constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

- La Mesa de Ayuda, con el apoyo de la Oficina de Comunicaciones, promoverá buenas prácticas de seguridad entre los usuarios. Igualmente publicará tips de G Suite que faciliten su uso, lo que incluye la inscripción del número de celular, registro de cuenta de correo de recuperación, pasos para la recuperación de la contraseña, entre otros.

- El retiro de los colaboradores de la entidad deberá ser notificado por el respectivo jefe. La Mesa de Ayuda deberá generar el respectivo respaldo, incluyendo el correo, las conversaciones de Hangout (chat) y los archivos de herramientas de oficina (Hoja Electrónica, Procesador de Texto y Presentador de Diapositivas) y luego proceder a la eliminación de la respectiva cuenta de G Suite.

- El rol de administrador y superadministrador de G Suite se entregará exclusivamente a los miembros de la Mesa de Ayuda, a través de los cuales se gestionarán todas las cuentas, incluyendo la creación, inactivación y reactivación, eliminación, creación y eliminación de grupos, agregar miembros a grupos, asignar alias a una cuenta, recuperación de cuentas eliminadas, generación de informes, entre otras labores.

- En el cuerpo de los correos deberá incorporarse un mensaje alusivo a la importancia de guardar la confidencialidad de la información contenida en el respectivo mensaje.

9.4.2. Internet

Internet es un servicio importante de comunicación y consulta, por lo tanto se requiere darle un uso eficiente al mismo, adoptando los siguientes lineamientos:

- Quienes tengan acceso a esta herramienta deben utilizarlo de manera efectiva, ética, legal y solo para fines laborales concernientes a la EPS. Todos los integrantes de SAVIA SALUD tienen las mismas responsabilidades en cuanto al uso de Internet.

- Las páginas de Internet a las que se tiene acceso son las validadas y definidas por la Jefatura de Tecnología e Información, basándose en las políticas laborales establecidas por la Gerencia de la entidad.

- 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.

- La transmisión, distribución, reproducción o almacenamiento de cualquier tipo de información, dato o material en violación de la ley o regulación al respecto, está estrictamente prohibido.

- Sólo puede haber transferencia de datos o de Internet en conexión con actividades propias del trabajo desempeñado.

- La red inalámbrica es un servicio que permite conectarse a la red de la EPS e Internet de manera controlada sin la necesidad de algún tipo de cableado. La Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura de la EPS. Al personal miembro de la EPS definido y autorizado por la jefatura de TI.

- No está autorizada la descarga de Internet de programas informáticos no autorizados por la Jefatura de Tecnología e Información.

- El área de Tecnología e Información se reserva el derecho de llevar un registro de los eventos asociados a la conexión de los diferentes usuarios para asegurar el uso apropiado de los recursos de red.

9.4.3. Servicio de impresión

En el servicio de impresión se debe asegurar la operación correcta y segura.

- Los documentos que se imprimen deben ser de carácter institucional.
- Las estaciones de trabajo deberán tener configurada la impresión retenida, de tal forma que luego de enviar un documento a impresora, se requiera dar la orden directamente en el panel de control de esta para la impresión. Con esto se garantiza que un documento impreso pueda ser visto solo por su dueño.

- No imprimir correos electrónicos a menos que sea estrictamente indispensable. En caso de necesitar la impresión, revisar el documento y eliminar el contenido que no se requiere.

9.5. Control de acceso

9.5.1. Gestión de acceso

- Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la EPS y se usarán exclusivamente para actividades relacionadas con la labor asignada.

- Los integrantes con acceso a un sistema de información o a la red, dispondrán de una única cuenta de acceso compuesta de identificador de usuario y contraseña definida de acuerdo a los lineamientos de estas.

- 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.

- El área de Tecnología e Información cancelará la cuenta o se desconectará temporal o permanentemente cuando se detecte un uso no aceptable de usuarios de acceso a la red de acuerdo con las políticas aquí establecidas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

- Los integrantes de la EPS tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por la Jefatura de Tecnología e Información y la autorización de su jefe inmediato. Los integrantes de SAVIA SALUD EPS no deben intentar sobrepasar los controles de los sistemas, examinar los computadores y redes de la entidad en busca de archivos de otros sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.

- En el caso del aplicativo misional INTEGRA, los permisos de acceso serán establecidos de acuerdo con la configuración previa de los roles. Esta configuración, en la cual se determinan los permisos y elementos del menú al que tendrá acceso, se debe realizar en conjunto con los usuarios y la aprobación del respectivo jefe inmediato, identificando necesidades y potenciales conflictos, y teniendo siempre en cuenta los impactos que generan dichos permisos. La configuración de un nuevo rol deberá hacerse por solicitud expresa del jefe del área y/o usuario interesado. La asignación de un rol a un usuario, así como su nivel de autorización, para el caso de usuarios que deberán autorizar servicios médicos y/o medicamentos, se deberá realizar previa solicitud y/o autorización del jefe inmediato.

- La filosofía expresada en el ítem anterior se aplica igualmente para el acceso al ERP SAP, con la excepción de los niveles de autorización que son un concepto exclusivo de INTEGRA.

9.5.2. Registro y cancelación de usuarios.

Para la gestión de usuarios (solicitudes de creación, modificación, inactivación, o eliminación) en los diferentes sistemas de información, será el coordinador de gestión humana o quien éste delegue de dicha área, quien vía correo electrónico envíe el aval al área de tecnología por medio de la mesa de ayuda, los empleados que ingresen, se retiren o se les dé por terminado el contrato laboral, para crear o deshabilitar de manera oportuna los usuarios en la red y aplicativos (máximo un día hábil luego de generada la novedad). Así mismo para los contratistas deberá ser el jefe inmediato (jefe con vinculación en la EPS) quien realice y acate dicha política.

9.5.3. Uso de contraseñas

- No revelar las contraseñas ya que son personales e intransferibles, por lo tanto son de carácter confidencial.

- No deben estar escritas ni disponibles donde otros puedan tener acceso fácilmente a ellas.

- No revelar las contraseñas por vía telefónica, correo electrónico o por ningún otro medio.

- Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.

- Cambiar las contraseñas según los requerimientos de seguridad definidos.

- Construir las contraseñas cumplimiento con los siguientes lineamientos:

  - ✓ Con 8 o más caracteres
  - ✓ Utilizar caracteres especiales (¡!$%&/+]), alfanuméricos, mayúsculas y minúsculas.
  - ✓ Efectuar cambios de contraseña periódicas.
  - ✓ No repetir la contraseña anterior.

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.

- En caso que el sistema no lo solicite automáticamente, se debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días.

9.5.4. Acceso a redes y servicios en red

- Las redes de datos y los recursos de red deben estar debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico
- Solo se debe permitir acceso de los usuarios a los servicios de red para los que hayan sido autorizados específicamente.

- Para la autorización de acceso a la información se debe contemplar un análisis previo de la justificación de la necesidad de uso de la misma y las actividades a realizar con el acceso a la información.

- Está prohibido en las redes y servicios de red:

  - ✓ Instalar o conectar sus portátiles o dispositivos personales a la red de SAVIA SALUD para realizar sus labores no institucionales.

- ✓ Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos
- ✓ Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- ✓ Albergar datos de carácter personal en las unidades de red y en las unidades locales de disco de los computadores de trabajo.

9.6. Seguridad física y del entorno

9.6.1. Áreas seguras

Se debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información o cuartos de telecomunicaciones de la EPS.

9.6.2. Seguridad De los Equipos

9.6.2.1. Ubicación y protección de los equipos

Los equipos que hacen parte de la infraestructura tecnológica tales como equipos de comunicaciones y seguridad electrónica, UPS, plantas telefónicas, impresoras multifuncionales, estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que almacenen o procesen deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. Para tal fin se deben tener en cuenta los siguientes lineamientos:

- Al finalizar la jornada laboral, es necesario salir de las aplicaciones que se estaban usando y apagar el computador.

- Por ningún motivo se puede conectar en las instalaciones eléctricas soportadas por la fuente de poder ininterrumpida UPS (tomas naranjados) cualquier tipo de artefacto que no sea el computador, esto con el fin de evitar un posible corto circuito que llegue a afectar los equipos soportados en ella.

- Se deben adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética, vandalismo, entre otros.

- Todos los dispositivos que conforman la infraestructura tecnológica de SAVIA SALUD EPS, deben contar con planes anuales de mantenimiento preventivo y se debe llevar el registro de las actividades adelantadas sobre los mismos.

9.6.2.2. Seguridad del cableado

El cableado de energía y telecomunicaciones que transporta datos o brinda apoyo a los servicios de información deben estar protegidos contra la intercepción o daño. Para tal fin se deben tener en cuenta los siguientes lineamientos:

- El cableado de energía y telecomunicaciones se debe proteger mediante canaletas.
- Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas. Deben existir planos que describan las conexiones del cableado.
- El acceso a los centros de cómputo y cuartos técnicos debe estar limitado y protegido.

9.6.2.3. Equipos desatendidos

- Siempre se debe bloquear las estaciones de trabajo o terminar todas las sesiones establecidas cada vez que se retire del sitio de trabajo.

- Sin perjuicio de lo anterior, y transcurridos un periodo de inactividad, de forma automática el equipo se encontrará bloqueado, exigiendo que el empleado ingrese su usuario y contraseña para desbloquear el equipo.

9.6.2.4. Escritorios y pantallas limpias

- En el escritorio de Windows no se debe almacenar información, para ello se debe utilizar la respectiva carpeta de datos en la red.

9.7. Seguridad de las operaciones

9.7.1. Gestión de cambios

Todos los cambios que se realicen a la plataforma tecnológica deben realizarse considerando que tanto el software, los accesos y las versiones son adecuadamente controlados, debidamente autorizados y no disminuya los niveles de seguridad existentes.

9.7.2. Gestión de capacidad

Se debe hacer seguimiento al uso de recursos, los ajustes, y las proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.

9.7.3. Separación de los ambientes de desarrollo, pruebas y producción

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad. Los programas que se encuentren en el ambiente de producción, pueden ser modificados únicamente por personal autorizado.

9.7.4. Protección contra software malicioso

Para prevenir posibles contagios se deben seguir los siguientes lineamientos:

• Todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad que brindan protección contra software malicioso y permiten detectar, prevenir y recuperar posibles fallos causados por los mismos.

• De presentarse el contagio de un virus informático, los daños que alcance a realizar y las consecuencias, serán atribuidos a la persona que hizo caso omiso de las políticas de seguridad.

• No ejecutar los archivos anexos al correo electrónico, si no provienen de una fuente segura.

• No utilizar medios de almacenamiento de procedencia desconocida.

• No escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier computador o red de SAVIA SALUD.

9.7.5. Respaldo de la información

• Se deben realizar copias de respaldo (Backup) que permitan recuperar datos perdidos accidental o intencionadamente de las bases de datos y unidades de red; las copias de respaldo deben contar con la misma seguridad que los datos originales Los datos incluyen pero no se limitan a archivos de información, fuentes y objetos de los programas del aplicativo, bases de datos, equipos de comunicaciones, software y documentación de SAVIA SALUD. La Coordinación de Infraestructura de la Jefatura de Tecnologías e Información debe diseñar e implementar un plan de respaldo, de acuerdo con la criticidad de la información a respaldar, que incluya pruebas frecuentes de recuperación.

9.8. Seguridad de las comunicaciones

9.8.1. Controles de redes

• Se deben mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.

• Las plataformas tecnológicas que soportan los sistemas de información de SAVIA deben estar separadas en segmentos de red lógicos, independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La división de los segmentos lógicos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad.

• Se debe monitorear mediante software de monitorización de redes, los tiempos de respuesta, la capacidad, latencia de red excesiva y seguimiento de la conectividad a modo de garantizar la transmisión de datos entre los terminales de manera rápida y constante de dispositivos de red, tales como canales, servidores y aplicaciones.

9.9. Gestión de incidentes de seguridad de la información

9.9.1. Reporte de eventos de seguridad de la información

Los eventos de seguridad de la información se deben informar a través de la Mesa de ayuda, tan pronto como sea posible. La Jefatura de Tecnologías e Información deberá recopilar, documentar y tipificar los incidentes que reporten los usuarios. Esto debe incluir la violación de claves de acceso, la pérdida de información, el daño físico de archivos, la violación de la confidencialidad, ataques de hacking directos a la infraestructura, internos o externos, o cualquier otro incidente que ponga en riesgo la seguridad de la información.

9.10. Aspectos de seguridad de la información de la gestión de continuidad de negocio

Desde Tecnología e Información se deben crear para las áreas un plan de contingencias informáticas que incluya al menos los siguientes puntos:

- Continuar con la operación del área con procedimientos informáticos alternos.
- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.

- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- Ejecutar pruebas de la funcionalidad del plan.
- Mantener revisiones del plan a fin de efectuar las actualizaciones
- Identificar y documentar los incidentes de seguridad de la información

9.11. Cumplimiento

9.11.1. Derechos de propiedad intelectual

Con el fin de dar cumplimiento a las normas legales sobre propiedad intelectual y derechos de autor, en SAVIA SALUD se deben tener en cuenta los siguientes lineamientos:

- Todos los derechos de propiedad intelectual de los productos, servicios y aplicaciones que hayan sido diseñados, desarrollados o modificados por empleados o personal subcontratado son de propiedad exclusiva de SAVIA SALUD.

- Se debe instalar solo software que esté licenciado por SAVIA SALUD. En caso de tratarse de un software en demostración, es necesario contar con un documento de autorización del fabricante o distribuidor autorizado y la aprobación de la Jefatura de Tecnología e Información.

- No se debe instalar, copiar software o utilizarlo en beneficio propio o de terceros al igual que reproducirlo sin autorización. El software que es licenciado para SAVIA SALUD o es de su propiedad, solo podrá ser instalado en los computadores de la misma.
- Cualquier reproducción a que hubiere lugar solo se hará para uso exclusivo de SAVIA SALUD y únicamente bajo estricto cumplimiento de los acuerdos de uso que se encuentran vigentes con los fabricantes y proveedores de tales programas.

9.11.2. Monitoreo y uso de los sistemas

Se debe establecer los mecanismos adecuados para detectar las actividades que amenacen la seguridad de la información. Para tal fin se deben tener en cuenta los siguientes lineamientos:

- SAVIA SALUD se reserva el derecho de interceptar o vigilar cualquier tráfico de información que pase a través de las redes de comunicaciones y sistemas de información como parte de sus actividades de vigilancia, mantenimiento, investigación, auditoría o seguridad del desempeño del sistema. Todo el personal debe estar consciente de esto cuando use los sistemas de información de SAVIA SALUD.
- Todas las aplicaciones y servicios críticos que hacen parte de la infraestructura de comunicaciones, seguridad y procesamiento de información deben proporcionar logs para permitir el seguimiento de las actividades de los administradores, y usuarios en general.
- Se deben enviar a los empleados alertas por los incumplimientos a las políticas de seguridad de la información cuando es la primera vez que las infringe y llamado de atención con copia al jefe inmediato y a Gestión Humana, cuando el incumplimiento vaya en contra de preservar la confidencialidad de la información y en las situaciones reincidentes.
- La Jefatura de Tecnologías e Información debe contratar, al menos 1 vez por año, los servicios de test de penetración e identificación de vulnerabilidades, así como documentar los hallazgos, realizar las actividades de remediación que le recomienden y hacer seguimiento a los avances en ese aspecto.
-

9.11.3. Cumplimiento de las políticas de seguridad y cumplimiento técnico

Las políticas de seguridad de la información, deben ser cumplidas por todos los integrantes que hacen parte de SAVIA SALUD, por lo tanto, el incumplimiento de las normas aquí estipuladas pueden acarrear acciones disciplinarias y legales.

El oficial de Seguridad de la Información de la entidad o el encargado de cumplir con sus funciones, deberá velar por el cumplimiento de todas las políticas de seguridad y realizar monitoreo permanente a la evolución de la aplicación del Modelo de Seguridad y Privacidad de la Información en la entidad.

10. Indicadores de seguridad de la información.

La Jefatura de Tecnologías de Información deberá contar con indicadores que reflejen la situación en seguridad de la información y el avance de las mejoras que se vayan realizando al respecto. Estos indicadores deberán estar alineados con las herramientas de medición propuestas por Mintic para el diagnóstico y seguimiento en la implementación del Modelo de Seguridad y Privacidad de la Información.

11. Definiciones

Contraseña: Contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen

Seguridad de la información: Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora

Software Malicioso: Es la descripción general de un programa informático que tiene efectos no deseados. A menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría actualmente busca robar información personal que pueda ser utilizada por los atacantes.

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). Se utiliza a menudo para propagar mensajes e infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam.

Virus: Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de computo

12. Registros

CÓDIGO	NOMBRE
N/A	N/A

13. Anexos

N/A

14. Referencias

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC Colombiana 27001:20013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos

ELABORACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Mintic. Versión 1. 11/05/2016.

Control de cambios

<table>
<tr><th>VERSIÓN</th><th>FECHA DE VIGENCIA</th><th>NATURALEZA DEL CAMBIO</th></tr>
<tr><td>01</td><td>30/03/2017</td><td>Creación del documento
<table>
<tr><th>ACTUALIZÓ</th><th>REVISÓ</th><th>APROBÓ</th></tr>
<tr><td>Analista de Seguridad Informática</td><td>Jefe de TI</td><td>Gerente</td></tr>
</table></td></tr>
<tr><td>02</td><td>30/10/2018</td><td>Se profundizan los apartados del manual especialmente lo relacionado con la suite de Google
<table>
<tr><th>ACTUALIZÓ</th><th>REVISÓ</th><th>APROBÓ</th></tr>
<tr><td>Analista de Seguridad Informática</td><td>Jefe de TI</td><td>Gerente</td></tr>
</table></td></tr>
</table>