Red Salud Armenia E.S.E.

PA CUIDAR DE TODOS

Plan de Seguridad y Privacidad de la Información

2023

CONTENIDO

1. INTRODUCCIÓN

Red Salud Armenia E.S.E. dentro de sus lineamientos de Sistemas de Información tiene establecido primordialmente tener la seguridad y la privacidad de la información de los usuarios que de alguna u otra manera interactúan con el Sistema de Información o mediante cualquier tipo de acceso a los datos institucionales desde alguna estación de trabajo o dispositivo.

De acuerdo a lo anotado anteriormente, desde el proceso de Sistemas de Información de Red Salud Armenia E.S.E. se llevan a cabo acciones encaminadas a propender por ejecución y cumplimiento de las políticas corporativas para el uso de los equipos de cómputo, dispositivos y software dentro de toda la red hospitalaria garantizando de esta manera que nuestra institución no presente problemas en cuanto a la seguridad de su información se refiere.

El siguiente modelo está diseñado para tener una guía de las actividades que se realizan desde el proceso de Sistemas de Información de Red Salud Armenia E.S.E. con respecto a la seguridad de los datos de la institución y de acuerdo a esto para que cada usuario del sistema de información tenga un conocimiento de las actividades que se derivan de allí y sus responsabilidades en cuanto a la confidencialidad y protección de sus datos.

2. JUSTIFICACIÓN

La administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

3. OBJETIVO

Establecer los conceptos básicos y metodológicos para una adecuada administración de la seguridad y privacidad de la información en RED SALUD ARMENIA E.S.E.

3.1 OBJETIVOS ESPECÍFICOS

- Establecer las políticas corporativas para el uso de los equipos de cómputo y software dentro de toda la red hospitalaria y garantizar su ejecución y cumplimiento.

- Establecer indicadores para realizar seguimiento y control al proceso de seguridad y confiabilidad de la información en el sistema de información institucional Dinámica Gerencial Hospitalaria .Net.

4. ALCANCE DEL DOCUMENTO

El presente documento pretende determinar la manera en que se llevara a cabo el proceso de protección de acceso a la información institucional de usuarios que de alguna u otra manera interactúan con el Sistema de Información o cualquier tipo de acceso a los datos institucionales desde alguna estación de trabajo o dispositivo, así como también, establecer las políticas corporativas para el uso de los equipos de cómputo y software dentro de toda la red hospitalaria y garantizando su ejecución, cumplimiento y seguimiento y control por medio de indicadores de gestión para estos procesos tan relevantes dentro de la institución.

5. FASE DE DIAGNOSTICO – ESTADO ACTUAL

Actualmente Red Salud Armenia E.S.E. cuenta con un proceso de Sistemas de Información mediante el cual se lideran diferentes lineamientos para administrar todo lo inherente a las Tecnologías de la Información y las Comunicaciones TIC, abarcando dentro de este la Seguridad y la Privacidad de la Información.

En cuanto a la infraestructura se tienen componentes de Servidores, Equipos de cómputo y de comunicaciones con la siguiente distribución:

- ✓ **Servidores**

Tipo	CANTIDAD
Servidor de Bases de datos – HP DL380 G10	1
Servidor de respaldo – HP DL 380 G7	1
TOTAL	**2**

- ✓ **Equipos de Computo**

CENTRO DE SALUD	CANTIDAD
CS CAA DEL SUR	30
CS CORREA GRILLO	10
CS EL CAIMO	4
CS EL PARAISO	10
CS LA CLARITA	13
CS LA MILAGROSA	0
CS PILOTO URIBE	13
CS FUNDADORES	13
HOSPITAL DEL SUR	144
TOTAL	**237**

El Hospital cuenta con un contrato de Outsourcing con la empresa Mundo Salud para el proceso de facturación en la toda la institución, dicha empresa debe proveer a sus colaboradores con sus respectivos equipos de cómputo, de acuerdo a esto

actualmente cuentan con 42 computadores distribuidos en la Unidad Intermedia del sur y los diferentes Centros de salud.

Los equipos de cómputo propios anotados anteriormente presentan el siguiente estado:

CENTRO DE SALUD	OBSOLETO	ACEPTABLE	MALO	ÓPTIMO	TOTAL x CS
CS CAA DEL SUR	21	5		4	30
CS CORREA GRILLO	8	1		1	10
CS EL CAIMO	3	1			4
CS EL PARAISO	8	1		1	10
CS LA CLARITA	9	2		2	13
CS LA MILAGROSA	0	0			0
CS PILOTO URIBE	9	2		3	13
CS FUNDADORES	2	5		6	13
HOSPITAL DEL SUR	91	25	18	10	144
TOTAL x ESTADO	**151**	**42**	**18**	**27**	**237**

En cuanto a software y Sistemas de Información se cuenta con el siguiente inventario en la institución:

Inventario de software de la Entidad					
No	**Nombre**	**Propiedad**	**PERIODO LICENCIA**		**Descripción**
		Propio	**Desde**	**Hasta**	
1	Dinamica Gerencial .Net	X		11/01/2022	Sistema de Información Institucional, se compone por todos los módulos Asistenciales, Administrativos y Financieros de la entidad, se encuentra actualizado a la fecha 11 de enero de 2022.
2	Antivirus Eset Endpoint	X	1/02/2022	09/03/2023	Software de antivirus de la institución, se compone por 330 licencias para estaciones de trabajo y servidores de archivos y consola de administración del Hospital.
3	Software de Backup Xopero	X	1/02/2022	09/03/2022	Licenciamiento ilimitado por un (1) año de software de Backup para servidor y estaciones de trabajo con capacidad de 1 TB en la nube
5	Sistema Operativo Windows 10 Pro	X			Sistema Operativo Equipos de Cómputo del Hospital
9	Office 2016 Pro	X			Software de Ofimática Equipos de Cómputo del Hospital
10	Office 2013 Home and Business	X			Software de Ofimática Equipos de Cómputo del Hospital
11	Office 2010 Standard	X			Software de Ofimática Equipos de Cómputo del Hospital
12	Office 2010 Pro	X			Software de Ofimática Equipos de Cómputo del Hospital

13	Windows Server 2008 R2	X			Sistema Operativo para Servidor del Hospital
14	Windows Server 2012 R2	X			Sistema Operativo para Servidor del Hospital
15	Windows Server 2008 User Cal	X			Licenciamiento para conexión de equipos de cómputo al Servidor del Hospital
16	Windows Server 2012 Device Cal	X			Licenciamiento para conexión de equipos de cómputo al Servidor del Hospital
17	SQL Server 2008 Standard	X			Software de Bases de Datos para el Servidor del Hospital
18	SQL Server 2014 Standard	X			Software de Bases de Datos para el Servidor del Hospital
19	Windows Server Standard Core 2019 OLP 18Lic NL Gov CoreLic	X			Sistema Operativo para Servidor de Bases de Datos del Hospital
20	Windows Server CAL 2019 OLP NL Gov UsrCAL - 250				Licenciamiento para conexión de equipos de cómputo al Servidor Principal del Hospital

Toda la infraestructura de equipos de cómputo y servidores se encuentra protegida mediante un software de antivirus debidamente licenciado y actualizado el cual se denomina **Eset Endpoint Antivirus**.

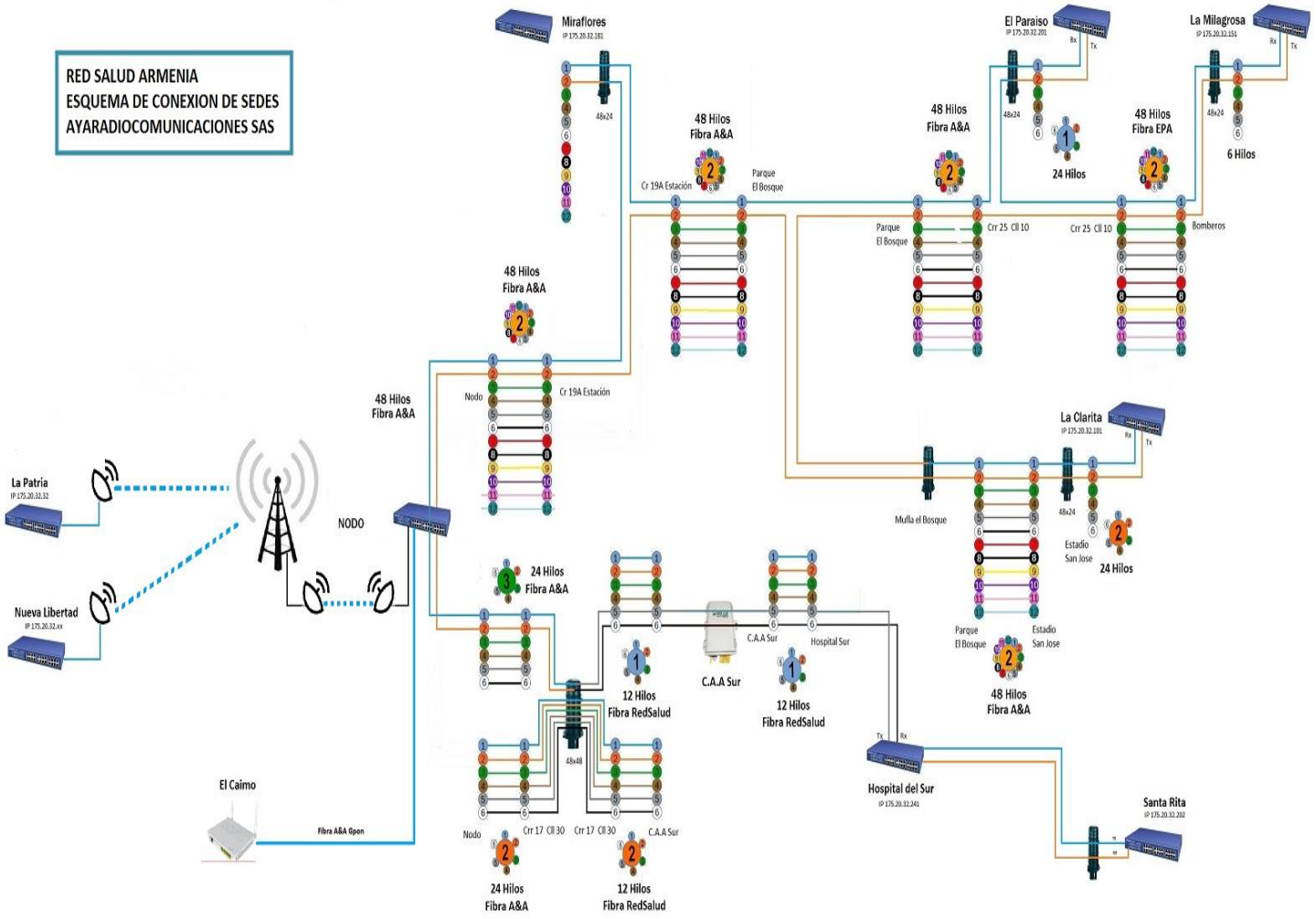
En cuanto a equipos de comunicación se tiene implementado un **UTM – Gestión Unificada de Amenazas** el cual se encuentra estableciendo una barrera perimetral de protección de la red LAN ante cualquier amenaza externa que pueda presentarse en cualquier momento.

Finalmente, se tienen establecidas políticas de seguridad y privacidad de la información mediante el Manual Seguridad y Gestión de Usuarios del Sistema de Información.

Red Salud Armenia E.S.E., actualmente, Red Salud Armenia E.S.E cuenta con una sede principal y nueve centros de salud distribuidos por la ciudad de Armenia, desde el año 2015 ha venido implementado una interconexión en fibra óptica entre su sede principal y tres de sus sedes de mayor tamaño y cercanas a esta como son: Centro de Salud CAA del Sur, Centro de Salud Piloto Uribe y Centro de Salud Correa Grillo, lo cual a la fecha ha mejorado totalmente la transmisión de datos entre estas sedes con la sede principal, la conectividad para la trasmisión de datos de los diez centros de salud restantes con la sede principal a partir del año 2017 se viene realizando por medio de un arrendamiento con un proveedor externo de un hilo de fibra óptica para los Centros de Salud: El Paraíso, La Milagrosa, La Clarita, Nueva Libertad, Santa Rita y El Caimo y mediante enlaces inalámbricos para los Centros de Salud: Los Fundadores.

Para el caso de la red de fibra óptica propia que interconecta nuestra sede principal y tres centros de salud: Centro de Salud CAA del Sur, Centro de Salud Piloto Uribe y Centro de Salud Correa Grillo, tanto para el mantenimiento preventivo como correctivo, debe realizarse un contrato con un proveedor externo especializado en este tipo de redes esto debido a que el hospital no cuenta con personal contratado capacitado para llevar a cabo estas labores.

En el caso de los centros de salud que la red ya sea fibra óptica o radioenlace se encuentra en arrendamiento con un proveedor externo, será este el encargado de garantizar tanto el mantenimiento preventivo como el correctivo para estos, es importante aclarar que de esta manera debe quedar estipulado en las obligaciones contractuales en el contrato celebrado entre el proveedor y Red Salud Armenia E.S.E.



Los equipos de redes presentan en algunos casos obsolescencia debido a que ya han cumplido con su vida útil razón por la cual se debe procurar en la presente vigencia por realizar una actualización de estos equipos.

7. FASE DE PLANIFICACION

POLITICAS DEL ADMINISTRADOR

Las siguientes son las recomendaciones a tener en cuenta en el momento de crear una cuenta de dominio de usuario de red:

- ✓ Si es una cuenta del dominio, esta se crea en el directorio activo con el nombre completo del funcionario y un alias; el estándar de creación del alias es el primer nombre seguido de un punto y el primer apellido. Si existen nombres homónimos, entonces se procede a utilizar el nombre completo seguido del primer apellido.
- ✓ El sistema permite crear una contraseña para este usuario.; con el fin de dar soporte a los equipos de todos los centros se recomienda no cambiarlas, pero si se necesita el usuario puede solicitar el cambio de contraseña.
- ✓ El uso de contraseñas en forma inteligente puede ser muy efectivo para garantizar la seguridad.
- ✓ Para el caso de creación de usuario de las aplicaciones se deben tener en cuenta el rol del usuario (Consulta, inclusión de datos, borrado de datos o control total) dependiendo del área según pertenezca.

- ✓ Toda solicitud de creación de cuenta a los usuarios se debe realizar por escrito con la autorización expresa del jefe de cada Dependencia explicando el motivo de su creación y uso respectivo.

POLITICAS DEL USUARIO

- ✓ Los computadores, periféricos, impresoras, programas, servicios, sistemas de información y comunicación solo deben usarse para el propósito de la empresa.
- ✓ Ningún funcionario está autorizado para instalar, actualizar o remover software o hardware en los equipos de escritorio, portátiles, impresoras o cualquier otro dispositivo informático. (Sin autorización o solicitud por escrito del Área de Sistemas de Información) Solo los funcionarios del Área de Sistemas de Información o contratistas en su representación están autorizados para realizar dichas actividades. Si se detecta algún software (Música, videos, protectores de pantalla etc.) o Hardware (cámaras de video, parlantes etc.,) instalados sin autorización, este puede ser desinstalado sin previo aviso del empleado, informándole de este evento a su jefe inmediato y con copia a los entes o directivas de control de la institución y a las respectivas cooperativas en caso del personal contratista.
- ✓ Los usuarios deben informar rápidamente todas las alertas, advertencias y en general los mensajes de error presentados por los equipos al Área de Sistemas de Información.

- ✓ El mantenimiento preventivo y limpieza de computadores e impresoras sólo puede ser realizado por personal calificado y directamente contratado por la empresa. Esto evita el daño, deterioro y posibles descargas eléctricas por mal manejo y filtración de agua y/o jabones que no son adecuados para este propósito.
- ✓ Cada usuario tiene un equipo de cómputo para sus actividades laborales, por tal motivo es directamente responsable del mismo. Si el equipo sufre daño, perdida, hurto o es trasladado o retirado de la entidad por personal diferente a los funcionarios de sistemas, la persona responsable debe informar al Área de Sistemas de Información en forma Inmediata y por escrito.
- ✓ El Software de la empresa, es para uso exclusivo de los computadores de Red Salud Armenia E.S.E.
- ✓ Cuando sea necesario instalar, mover o reubicar un computador o una impresora debe informarse al Departamento de Bienes y Servicios (Activos Fijos) y al Área de Sistemas de Información y este será el único encargado de autorizar y realizar el movimiento, el cual debe estar justificado por escrito e ingresado al Sistema.
- ✓ Ningún funcionario debe extraer los equipos de las instalaciones de la empresa sin la autorización escrita del Área de Sistemas de Información, excepto aquellos que tienen asignados un equipo portátil para lo cual deberán contar con el visto bueno del Área de Sistemas de Información y deberá reportarse a la empresa de vigilancia al salir y entrar de la institución.
- ✓ De la información consignada en los discos duros de las estaciones de trabajo, es responsabilidad del usuario realizar copias de seguridad y mantenerlas en un lugar seguro. Los respaldos tienen cubrimiento sólo sobre las unidades de red.
- ✓ No se deben consumir alimentos o bebidas mientras se trabaja en un computador de Red Salud Armenia E.S.E ya que puede causar daño a los equipos electrónicos, como teclado, Mouse, monitor etc. Si esto llegare a ocurrir el responsable deberá asumir los costos en que ello incurra los cuales serán reportados al área de Talento Humano para su respectiva gestión en caso del personal de planta y a las cooperativas al personal contratista.
- ✓ Todo usuario deberá proteger la información, evitando ser entregada a usuarios no autorizados. Esta debe ser utilizada únicamente para el propósito pretendido según sus funciones dentro de la empresa, a sí mismo solo la Gerencia autoriza la entrega de información a quien la solicite y deberá ser indicado el propósito para el cual es requerida.
- ✓ Todo usuario de la red debe tener su propia contraseña, esta a su vez no debe ser revelada, ni prestada para ser utilizada por otra persona, se debe cambiar periódicamente o cuando sospeche su uso indebido.
- ✓ Si se encuentra ausente de su puesto de trabajo, los equipos deben estar fuera de la aplicación de trabajo, impidiendo así el uso no autorizado de las mismas. El no tener en cuenta esta precaución se hará responsable de que la información bajo su custodia llegare a manos de otros.

- ✓ Queda prohibido a los usuarios el uso de Internet en los equipos de cómputo con fines diferentes a aquellos para los cuales fueron autorizados como son sus fines labores, si se llegare a encontrar un usuario haciendo uso indebido de Internet se informará al jefe inmediato y será inmediatamente desinstalado y reportado al comité de control interno disciplinario en caso de personal de planta y a las cooperativas al personal contratista. Igualmente se instalará Internet exclusivamente en las coordinaciones y en las áreas que requieran previa autorización de la Gerencia.
- ✓ Cada usuario al final de la jornada será el responsable de dejar el equipo de cómputo debidamente apagado y en completo orden; los computadores e impresoras dejados en funcionamiento serán reportados al coordinador respectivo y los daños causados por este olvido correrían a cargo del usuario responsable.
- ✓ Los correos electrónicos Institucionales deberán ser utilizados para el fin que fueron creados y serán revisados periódicamente por el personal del Área de Sistemas de Información y de la Gerencia. En caso de recibir notificaciones diferentes a lo laboral por este medio deberán darlas a conocer a la Gerencia.
- ✓ Para el uso de la página Web institucional deberá notificarse a la Gerencia y de ser aprobado reportado al Área de Sistemas de Información para ser publicado y así dar un buen uso a este servicio.
- ✓ El uso del mensajero de Intranet por medio de la plataforma Torresoft es para manejo empresarial y totalmente para temas laborales, queda prohibido en envió de fotos, videos, la venta de productos, mensajes personales u otros que no cumplan con las políticas institucionales.

POLITICAS DE PROTECCION EN EL PUESTO DE TRABAJO

- ✓ Establezca una contraseña para proteger el teclado y la pantalla que se active automáticamente cuando la inactividad sea mayor a quince (15) minutos. En su defecto bloquee el teclado pulsando simultáneamente las teclas “Control”, “Alt”, “Supr” y dar clic en “bloquear el equipo”.
- ✓ Cuando el usuario requiera retirarse de su puesto de trabajo por determinado tiempo, este debe cerrar sesión en el sistema de información institucional Dinámica Gerencial .Net, de igual forma al finalizar la jornada laboral, debe salir completamente del sistema de información y proceder a pagar el equipo de cómputo.
- ✓ Es importante recordar que el usuario y contraseña son de carácter personal y no deben ser prestadas en los puestos de trabajo bajo ninguna circunstancia.
- ✓ En las áreas de consulta externa, facturación y urgencias, los monitores deben estar asegurados físicamente con guayas para evitar robos de los mismos.

- ✓ Adicionalmente, todos los equipos de la institución están protegidos contra virus informáticos, malware, spyware y demás ataque informáticos que podamos sufrir en el desarrollo de las actividades propias de la institución.

8. FASE DE IMPLEMENTACION

8.1. COPIAS DE SEGURIDAD

El componente de copias de seguridad y restauración del motor de base de datos SQL Server ofrece una protección esencial para los datos críticos almacenados en las bases de datos de SQL Server. Para minimizar el riesgo de pérdida de datos catastrófica, debe realizar copias de seguridad de las bases de datos para conservar las modificaciones en los datos de forma periódica. Una estrategia de copias de seguridad y restauración correctamente planeada contribuye a la protección de las bases de datos de la pérdida de datos derivada de daños causados por diferentes errores.
Red Salud Armenia E.S.E. dentro de sus lineamientos de Sistemas de Información tiene establecido primordialmente tener asegurados todos sus datos tanto correspondientes a bases de datos del sistema de información institucional como también tener lineamientos claros acerca de la información operativa de cada usuario o que este pueda tener en sus equipos de trabajo, para así ante cualquier eventualidad se puedan tener respaldos que nos generen el mínimo de inconvenientes operativos ante una restauración.

8.1.1 Copias De Seguridad Bases De Datos

La información almacenada en medios magnéticos u ópticos tendrá diversas copias de respaldo en otro medio de que disponga Red Salud Armenia E.S.E., debido a la importancia de los datos para la toma de decisiones, el conocimiento de la contratación, tipos de afiliación, los servicios prestados y la situación de salud de las personas entre otras.

Las copias de respaldo de los datos son esenciales, como principal mecanismo de seguridad de la información, para facilitar las tareas se deben centralizar las copias de seguridad del servidor, mediante unos horarios determinados.

El esquema de copias de seguridad para el Sistema de Información institucional en Red Salud Armenia E.S.E. se realizara de la siguiente manera:

Copias de Seguridad en el Servidor de Backup

Periodo	Fecha	Hora	Observaciones
Diaria	Diario	6:00 a.m.	Copia diaria, copia de seguridad completa de la base de datos de producción.

Periodo	Fecha	Hora	Observaciones
Diaria	Diario	01:00 a.m. 06:00 a.m. 11:00 a.m. 04:00 p.m. 09:00 p.m.	Copias diarias, se realizan copias de seguridad diferenciales cada 5 horas a partir de las 8:00 a.m. hasta las 12:00 a.m., las cuales guardan registro de las modificaciones de la base de datos desde la última copia completa o diferencial.
Semanal	Semanal	6:00 a.m.	Copia Semanal, se guarda una copia semanal de los días 1, 8, 15, 22 y 30 o 31 de cada mes, en la nube de Google Drive.

Las fechas y horas definidas, deben de ser de estricto cumplimiento y reforzarse con otras copias de seguridad cuando sea necesario de presentarse algún cambio o ajuste muy significativo en el sistema de información como por ejemplo un proceso de actualización del mismo o por manejo interno de la oficina de Sistemas de Información.

Red Salud Armenia E.S.E. ubicará mensualmente una de las copias de seguridad completas en una caja fuerte, bien sea de Red Salud Armenia E.S.E., o de Archivo central donde se tenga la custodia de las copias, adicionalmente este proceso también podrá realizarse en la nube, buscando mantener almacenadas por lo menos 3 copias de fecha diferente, esto con el fin de protegerse contra los posibles siniestros que puedan suceder en las Instalaciones de la Empresa.
Se tendrá siempre en cuenta en Red Salud Armenia E.S.E. los siguientes lineamientos:

- ✓ La información debe ser verificada íntegramente, tanto el original como las copias y revisar que la información no esté contaminada con virus informáticos.
- ✓ El disco duro es un medio de almacenamiento temporal de la información, el cual debe ser depurado permanentemente de los archivos que no volverán a ser utilizados en forma inmediata.
- ✓ Sólo el personal encargado de la elaboración y procesamiento del sistema y el usuario responsable del mismo, podrán acceder y usar la información que está almacenada en los medios magnéticos u ópticos.

Toda información almacenada en medios magnéticos u ópticos debe contar con la norma de gestión documental. Donde se identifique.

Carpeta No.
Caja:
Folios No.
Código: 411

Unidad Administradora: SUBGERENCIA PLANIFICACION INSTITUCIONAL
Oficina Productora: SISTEMAS
Serie Documental: COPIAS DE SEGURIDAD
Subserie Documento: COPIAS DINAMICA GERENCIAL HOSPITALARIA

Los medios magnéticos u ópticos (cintas, discos), que contienen a los archivos de información, deben tener etiquetas con su respectivo rótulo donde se especifiquen las características anteriormente detallada, además de la fecha de generación de los mismos.

8.1.2 Copias De Seguridad De La Información, Archivos Y Documentos De Los Usuarios

En Red Salud Armenia E.S.E. los usuarios son los responsables de hacer periódicamente copias de seguridad de su información, archivos y/o documentos, es importante tener en cuenta que estos podrán tener apoyo del área de Sistemas de Información para el proceso de copias de seguridad siempre que lo solicite, tanto para que el usuario pueda guardar registro de sus archivos en medios extraíbles de su propiedad así como también para que el área de Sistemas de Información guarde un respaldo o copia de estos en discos duros externos o en la Nube.

Para el caso de los usuarios de nivel Directivo (Gerente, Subgerentes, Asesores), Lideres de Proceso y Coordinadores, adicional a lo anotado anteriormente, contaran con cuentas corporativas de Gmail, las cuales aparte de ser utilizadas para el servicio de correo electrónico tanto interno como externo, poseen la herramienta Google Drive con una capacidad de mínimo 30 Gigas y la misma se podrá incrementar más cuando el usuario lo requiera que les permitirá a estos usuarios realizar copias de seguridad en la Nube así como también poder acceder a nuestra información almacenada desde cualquier lugar, esto siempre con los niéveles de acceso y seguridad establecidos por Google.

8.2. ALMACENAMIENTO DE LA INFORMACION

8.2.1 Almacenamiento Físico

Los ambientes donde se depositan los medios magnéticos deben contar con adecuadas condiciones de temperatura y no presentar humedad.

Los medios magnéticos en los cuales se almacena la información histórica deben ser completamente nuevos (primer uso), verificándose su buen estado operacional.

Los medios magnéticos donde está grabada la información deben recibir mantenimiento de limpieza cada dos meses como mínimo.

Sólo el personal responsable de la seguridad de los archivos tendrá acceso al ambiente donde se encuentren estos medios magnéticos almacenados.

8.2.2 Acceso a la información.

Para acceder continuamente a los datos del Sistema de Información de Red Salud Armenia E.S.E., se tienen definidos los siguientes lineamientos:

En los Sistemas Informáticos se tienen programas de cómputo, que cuentan con rutinas de control para el acceso de los usuarios.

Las rutinas de control, permiten que los usuarios ingresen al Sistema, previa identificación, mediante una palabra clave (password), la cual será única para cada uno de ellos; negando el acceso a las personas que no han sido definidas como usuarios del Sistema.

Las rutinas de control de acceso identifican a los usuarios autorizados a usar determinados sistemas con su correspondiente nivel de acceso, el cual incluye la lectura o modificación en sus diferentes formas.

Es recomendable que existan 4 niveles de acceso a la información:
a) Nivel de consulta de la información no restringida o reservada.
b) Nivel de mantenimiento de la información no restringida o reservada
c) Nivel de consulta de la información incluyendo la restringida o reservada.
d) Nivel de mantenimiento de la información incluyendo la restringida o reservada

Para garantizar estos niveles cada rol o perfil de usuario tendrá asignada uno de estos niveles de acceso.

Consecuentemente la información que se considere restringida o reservada estará debidamente identificada, así como a los usuarios que la acceden.

Cada área maneja los 4 niveles de acceso a la información, contando para ello con un Administrador de la Información, quien es responsable de la asignación de las palabras claves, de los niveles de acceso y las fechas de expiración.

Para la administración de claves se dispondrá de un procedimiento que posibilite que las palabras claves tengan o se generen bajo un período de tiempo prudencial de vigencia

El jefe de cada área es responsable del acceso a la información y será quien proporcione las directivas adecuadas al Administrador de la Información.

Los operadores de la información restringida o reservada realizarán estrictamente lo indicado en cada procedimiento establecido de procesamiento de la información, para lo cual éstos deberán estar claramente documentados.

Los operadores de la información deben mantener su clave en estricta reserva, ésta sólo debe ser conocida individualmente por cada uno de los usuarios y máximo por otra persona más de apoyo a cada proceso en cada una de las áreas, diferente al Administrador del Sistema de cómputo general.

8.2.3 Protección Especial De La Información

Se recomienda la adquisición de un software que permita encriptar la información con el fin de obtener mayor protección a la información. Garantizando un límite máximo de instalaciones (licencias autorizadas), para uso
La protección especial de la información incluye establecer procedimientos adecuados para el control y distribución de la información impresa, así como para la grabación de los medios magnéticos u ópticos y su respectivo almacenamiento.

8.3. PLAN DE CONTINGENCIA – SISTEMAS DE INFORMACION

8.3.1 Plan de Contingencia

Un porcentaje muy alto de los incumplimientos TI, es debido a la caída de infraestructura Hardware o Software, la cual supone una afectación en el servicio sin previo aviso. De forma proactiva se establecen planes y herramientas que mejoren la capacidad del entorno, pero de forma reactiva, están los llamados Planes de Contingencia para tecnologías de la información (TI).

Un plan de contingencia es un instrumento de gestión para el buen gobierno de las Tecnología de la Información y las comunicaciones en el dominio del soporte y desempeño. Estos planes de contingencia contienen las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de la empresa. Es un caso particular de plan de continuidad de la empresa, pero dada la importancia actual de las tecnologías modernas, el plan de contingencias es el más relevante. El objetivo de este documento es explicar que es un plan de contingencia, el porqué de su importancia y el cómo de su preparación. La mejora de dicho plan se basa principalmente en la automatización de las acciones.

Red Salud Armenia ESE, tiene implementado un Plan de Contingencia para el proceso de Sistemas de Información, el cual se encuentra debidamente documentado (Ver Anexo 1 - Plan de Contingencia - Sistemas de Información)

9. FASE DE EVALUACION DEL DESEMPEÑO

Para realizar seguimiento y control al proceso de seguridad y Privacidad de la información en el sistema de información institucional Dinámica Gerencial Hospitalaria .Net, se tendrán en cuenta los siguientes indicadores:

Número de Copias de Seguridad realizadas en el mes / Número Total de Copias de Seguridad Programadas en el mes

Número de Solicitudes de Creación de Usuarios realizadas en el mes / Número Total de Solicitudes de Creación Tramitadas en el mes.

Número de Solicitudes de Inactivación de Usuarios realizadas en el mes / Número Total de Inactivaciones Realizadas en el mes.

La frecuencia con la que se realizará seguimiento y control a estos indicadores será trimestralmente.

10. FASE DE MEJORA CONTINUA

Esta fase le permitirá a la Entidad, consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el MSPI - Modelo de Seguridad y Privacidad de la información.

11. GLOSARIO DE TÉRMINOS

Administrar: Gobernar, ejercer la autoridad o el mando sobre un territorio y sobre las personas que lo habitan. Dirigir una institución. Ordenar, disponer, organizar, en especial la hacienda o los bienes.
Arquitectura Empresarial o TI: Describe la estructura y las relaciones de todos los elementos de TI de una organización. Se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de servicios tecnológicos. Incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de TI (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos).
Gel: Gobierno en línea es el nombre que recibe la estrategia de gobierno electrónico (e-government) en Colombia, que busca construir un Estado más eficiente, más transparente y más participativo gracias a las TIC.
Gestionar: Hacer diligencias conducentes al logro de un negocio o un objetivo.
Gobierno Corporativo: manera en que las entidades son dirigidas, mejorando su funcionamiento interna y externamente, buscando eficiencia, transparencia e integridad, para responder adecuadamente ante sus grupos de interés, asegurando un comportamiento ético organizacional.
Copia de seguridad: Copia los datos o los registros de una base de datos de SQL Server o del registro de transacciones en un dispositivo de copia de seguridad, como un disco, para crear una copia de seguridad de datos o de registros.
Copia de los datos que se puede usar para restaurar y recuperar los datos después de un error. Las copias de seguridad de una base de datos también se pueden usar para restaurar una copia de la base de datos en una nueva ubicación.
Dispositivo de copia de seguridad: Disco o dispositivo de cinta en el que se escriben las copias de seguridad de SQL Server del que se pueden restaurar.
Copia de seguridad de datos: Copia de seguridad de datos en una base de datos completa (copia de seguridad de base de datos), una base de datos parcial (copia de seguridad parcial) o un conjunto de archivos de datos o grupos de archivos (copia de seguridad de archivos).
Copia de seguridad de base de datos: Las copias de seguridad completas representan la base de datos completa en el momento en que finalizó la copia de seguridad. Las copias de seguridad diferenciales solo contienen los cambios realizados en la base de datos desde la copia de seguridad completa más reciente.
Copia de seguridad diferencial: Copia de seguridad de datos basada en la última copia de seguridad completa de una base de datos completa o parcial o de un conjunto de archivos de datos o grupos de archivos (base diferencial) y que solo incluye los datos que han cambiado desde dicha base.
Recuperar: Devolver una base de datos a un estado estable y coherente.
Restaurar: Proceso de varias fases que copia todos los datos y páginas del registro desde una copia de seguridad de SQL Server especificada a una base de datos especificada y, a continuación, pone al día todas las transacciones registradas en la copia de seguridad mediante la aplicación de los cambios registrados para poner los datos al día.

12. Bibliografía

MINTIC. (30 de junio de 2014). *Marco de Referencia, Guías, Base del conocimiento*. Obtenido de www.mintic.gov.co/arquitecturati/630/w3-article-9253.html

MINTIC. (2015). *Arquitectura TI*. Obtenido de http://www.mintic.gov.co/arquitecturati/630/w3-channel.html

MINTIC. (2015). *Fortalecimiento de la Gestión TI en el Estado*. Obtenido de Modelo de Gestión TI: http://www.mintic.gov.co/gestionti/615/w3-channel.html

MINTIC. (30 de marzo de 2016). G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información - PETI. Bogotá, Colombia.

MINTIC. (s.f.). *Gobierno en Linea*. Obtenido de http://estrategia.gobiernoenlinea.gov.co/623/w3-channel.html

Elaboró: Jhoanny Andrés Montoya Granada	Cargo: Ingeniero de Sistemas Contratista
Aprobó: José Antonio Correa López	Cargo: Gerente