

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 1 DE 12
		FECHA: 19/10/2017

PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E.

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 2 DE 12
		FECHA: 19/10/2017

CONTENIDO

1. INTRODUCCIÓN.....	3
2. JUSTIFICACIÓN.....	3
3. ALCANCE.....	4
4. OBJETIVOS	4
5. MARCO NORMATIVO.....	5
6. VOCABULARIO.....	5
7. DESARROLLO	9
7.1. BENEFICIOS DE LA IMPLEMENTACIÓN DEL SGSI.....	9
7.2. METODOLOGIA PHVA IMPLEMENTACIÓN DEL SGSI	9
7.3. FASES DE IMPLEMENTACION DEL SGSI.....	9
8. SEGUIMIENTO Y MEDICIÓN.....	12
9. BIBLIOGRAFÍA.....	12
ANEXOS.....	12

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 3 DE 12
		FECHA: 19/10/2017

1. INTRODUCCIÓN

En la actual comunidad global, donde gran parte de la información viaja a través del ciberespacio expuesta a una serie de vectores de ataque, que van desde las ciber amenazas hasta el conflicto de intereses e incumplimiento de regulaciones, surge el concepto de SGSI (Sistema de Gestión de Seguridad de la Información) como una fórmula magnífica para la protección de la información. No obstante, ponerla en práctica requiere de acciones y actividades que en gran parte de los casos resultan infructuosos o difíciles de mantener.

No hace más de una o dos décadas que las organizaciones no tenían estas preocupaciones o solo les inquietaban algunos programas maliciosos, hoy en día cuando el nivel de transacciones electrónicas que viajan a través de las redes de datos se mide en el orden de TERA y PETA bytes y que la información contenida es de gran valor, re aparece la piratería, pero esta vez en el ámbito cibernético. Entonces se debe pensar, qué tanto se está expuesto a este grupo delincuencial y si la información que se produce es objeto de un ataque o existe algún tipo de interés para un tercero, creer lo contrario es uno de los errores más comunes en seguridad – “esto no me toca”. Si buscamos en Google “Seguridad de la información” seguramente encontramos más 25 millones de resultados y muchos de estos resultados hacen referencia a equipos, software metodologías, consultorías, normas, etc., que prometen la solución a todos los problemas, no obstante, estas soluciones por si solas logran proteger tan solo una parte de los activos, en tanto que la combinación y su personalización, permitirán obtener buenos resultados en materia de seguridad.

No hay sistema ni organización 100% segura, un firewall no puede detener un atacante interno y una norma o política no detiene un atacante externo, pero si a estos se les une una estricta gestión de riesgos, un buen grado de concienciación y un excelente clima laboral, los resultados serán extraordinarios. Adicionalmente y como lo afirma, J.M San Martin en ¹, la mayoría de los sistemas informáticos implantados en las empresas no son seguros, bien porque no fueron diseñados para ser seguros, bien porque no cuentan con los medios técnicos necesarios.

Finalmente, continua J.M San Martin en ¹, “la Seguridad no se consigue solo con medios técnicos. Para lograr un adecuado nivel de Seguridad en la empresa, es fundamental disponer de una gestión y unos procedimientos adecuados, mediante los cuales se planifiquen los sistemas de protección y control necesarios. En definitiva, se necesita implantar un Sistema de Gestión de Seguridad que abarque y tenga en cuenta a toda la organización, desde sus directivos y empleados, a sus clientes, proveedores, e incluso accionistas, así como sus procesos y recursos productivos.”

2. JUSTIFICACIÓN

Considerando que la Alcaldía Mayor de Bogotá dentro de su Plan de Desarrollo Administrativo, dispuso la estrategia de fortalecer e integrar los sistemas de gestión al interior de las entidades del sector Público Distrital a través del Decreto 652 de 2011, por medio del cual se adopta la Norma Técnica Distrital del Sistema Integrado de Gestión - NTD-SIG 001:2011- para las entidades y organismos Distritales.

En el artículo 1º del Decreto 176 de 2010 de la Alcaldía Mayor de Bogotá, establece que el Sistema Integrado de Gestión se enmarca en el Sistema de Desarrollo Administrativo y está conformado por los siguientes Subsistemas: Gestión de la Calidad (SGC), Gestión Documental y Archivo (SIGA),

¹ [1] J.M San Martin G, “La Seguridad de la Información Nueva ventaja competitiva en la empresa (I/IV)” [Online].

Disponible: <http://dialnet.unirioja.es/servlet/articulo?sessionid=14432189D775360F21145B837ECC2C47.dialnet01?codigo=824400>

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 4 DE 12
		FECHA: 19/10/2017

Gestión de Seguridad de la Información (SGSI), Gestión de Seguridad y Salud Ocupacional (S&SO), Responsabilidad Social (SRS), Gestión Ambiental (SGA), Control Interno (SCI) y para los hospitales del Distrito Capital, el Subsistema Único de Acreditación (SUA), este último enmarca el estándar de gerencia de la Información.

De acuerdo con la anterior normatividad, este plan se enfoca en el desarrollo de los subsistemas de: Gestión de Seguridad de la Información (SGSI), Subsistema Único de Acreditación (SUA) estándares de gerencia de la Información y la normatividad complementaria de los anteriores subsistemas:

SGSI:

NTC-ISO/IEC:27001, 27002, 27003, 27005
Resolución No. 305 de 2008

SUA Acreditación:

Resolución No. 123 de 2012 (Estándares de gerencia de la información)

La Subred Norte ESE reconoce la información como un activo importante para la atención de los pacientes y en el desarrollo de sus procesos internos, por lo tanto, se preocupa por definir lineamientos que permitan mitigar los posibles riesgos para la información.

El manual de seguridad es un documento que contiene los lineamientos que apoyan la gestión y administración de los planes y procedimientos de seguridad de la información dando claridad sobre las prácticas de seguridad aplicadas en la institución.

3. ALCANCE

El presente Plan es aplicable a todos los funcionarios que hacen parte de la **Subred Integrada de Servicios de Salud Norte ESE**, así como a todas aquellas personas naturales o jurídicas, públicas o privadas que desarrollen contratos o convenios con la institución y tengan acceso y/o hagan uso de la infraestructura tecnológica de la Subred Norte ESE. El Plan contempla los lineamientos principales para la seguridad de la información en la Subred Integrada de Servicios de Salud Norte ESE.

4. OBJETIVOS

Diseñar e Implementar el Subsistema de Gestión de Seguridad de la Información (SGSI) para la Subred Integrada de Servicios de Salud Norte ESE, que permita integrar el Plan de Gerencia de la Información y de respuesta a los requerimientos estratégicos, tácticos y operativos de la institución, y así mantener la integridad, disponibilidad y confidencialidad de la información que es recibida, procesada, generada o que reposa en la Subred Norte E.S.E.

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 5 DE 12
		FECHA: 19/10/2017

5. MARCO NORMATIVO

La norma BS 7799/ISO 17799	Para un mejor acercamiento a la seguridad de la información
Norma técnica colombiana NTC-ISO/IEC 17799	Código de buenas prácticas para la gestión de la seguridad de la información, 13 de diciembre de 2004
RESOLUCIÓN No. 305 DE 2008:	Resolución expedida por secretaria general del distrito en la cual se establece políticas públicas para las entidades del distrito capital, en materia de tecnologías de información y comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de datos espaciales y software libre.
Acuerdo 279 de 2007	Establece lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital
Directiva 05 de 2005	Se adoptan las Políticas Generales de Tecnología de Información y comunicaciones aplicables al Distrito Capital.
NTC-ISO/IEC: 27001, 27002, 27003, 27005	Norma técnica Colombiana
Resolución 246 de 2016	Por la cual se dictan disposiciones en relación con el Sistema de Información para la Calidad y se establecen los indicadores para el monitoreo de la calidad en salud.
Resolución no. 123 de 2012	Modifica el artículo 2° de la Resolución 1445 de 2006, sobre los Estándares de Acreditación para instituciones prestadoras de salud IPS. Con el fin de que los entes acreditadores certifiquen el nivel de calidad en la atención en las IPS, las Entidades Administradoras de Planes de Beneficios y las Direcciones Territoriales de Salud.

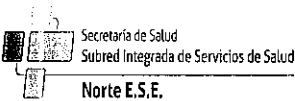
6. VOCABULARIO

ACEPTACIÓN DEL RIESGO: Es la decisión de aceptar el riesgo. (ISO/27001)

ACTIVO: Cualquier bien tangible o intangible que tenga valor para la organización.

ACTIVO DE INFORMACIÓN: Recurso informático que tiene valor importante para la entidad.

AMENAZA: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 6 DE 12
		FECHA: 19/10/2017

ANÁLISIS DE RIESGO: Uso sistemático de la información para identificar fuentes y para estimar el riesgo. (ISO/27001).

BACKUP: Copia de seguridad o respaldo de información considerados lo suficientemente importantes para ser conservados.

EVALUACIÓN DEL RIESGO: Proceso para comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo. (ISO/27001)

EVENTO DE SEGURIDAD DE LA INFORMACION: Es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas o una situación previamente desconocida que puede ser relevante para la seguridad.

GESTIÓN DEL RIEGO: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo. (ISO/27001)

INFORMACION: Es un activo muy importante para la Subred Norte ESE y está formado por un conjunto de datos que al relacionarlos y/o analizarlos produce conocimiento por lo tanto necesita de una adecuada protección.

INCIDENTE DE SEGURIDAD: Es un evento de seguridad de la información no deseado o inesperado que tienen una significativa probabilidad de comprometer las operaciones de la Subred Norte ESE y amenazan la seguridad de la información.

INFORMACIÓN PRIMARIA: Elemento de control conformado por el conjunto de datos de fuentes externas provenientes de las instancias con las cuales la organización está en permanente contacto, así como las variables que no están en relación directa con la entidad pero afectan su desempeño.

INFORMACIÓN SECUNDARIA: Elemento de control conformado por el conjunto de datos que se originan o procesan al interior de la entidad pública proveniente del ejercicio de su función.

MATERIAL NO AUTORIZADO: Material protegido por derechos de autor, marca comercial u otro derecho sobre la propiedad intelectual utilizada sin debida autorización y material que resulte obsceno, difamatorio, con contenido explícito sexual, pornografía o con contenido ilegal de acuerdo con las normas vigentes.

NTC-ISO/IEC: 27001: Para el diseño del plan de seguridad de la información se toma como referencia la norma NTC-ISO/IEC: 27001, la cual nos ofrece un modelo de enfoque para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI), por medio del modelo de proceso (PDCA) Planear, Hacer, Chequear y actual.

NTC-ISO/IEC: 27002: es la guía que nos ofrece las pautas para la implementación del SGSI por medio de buenas prácticas que describe los objetivos de control y controles

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 7 DE 12
		FECHA: 19/10/2017

recomendables para el cumplimiento de la norma. La guía contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

NTC-ISO/IEC: 27003: ofrece una guía estructurada de los aspectos a tener en cuenta para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) teniendo como referencia el modelo PDCA de la ISO / IEC 27001:2005.

La ISO 27003, describe el paso a paso de las especificaciones del SGSI desde el inicio (Alcance) hasta el diseño y elaboración de planes de ejecución.

1. Alcance
2. Referencias Normativas
3. Términos y Definiciones
4. Estructura de esta Norma Internacional
5. Obteniendo la aprobación de la alta dirección para iniciar un SGSI
6. Definir el alcance del SGSI, límites y políticas
7. Evaluación de los requerimientos de seguridad de la información
8. Evaluación de Riesgos y Plan de tratamiento de riesgos
9. Diseño del SGSI

NTC-ISO/IEC: 27005: Esta norma establece las directrices para la gestión del riesgo en la seguridad de la información, está diseñada para ayudar al cumplimiento de las propiedades de la seguridad de la información basada en un enfoque de procesos teniendo en cuenta fase de análisis y gestión de riesgos

PRINCIPIOS DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION.

- ✓ Sensibilización
- ✓ Responsabilidad
- ✓ Respuesta
- ✓ Ética
- ✓ Democracia
- ✓ Valoración del riesgo
- ✓ Concepción y aplicación de la seguridad
- ✓ Gestión de la seguridad
- ✓ Reevaluación.

PROPIEDADES DE SEGURIDAD INFORMATICA:

- ✓ **Confidencialidad:** Protección para que el activo de información sea accesible solamente por aquellas personas autorizadas para ello.
- ✓ **Integridad:** Protección de la exactitud y estado completo de la información y sus métodos de procedimientos.

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 8 DE 12
		FECHA: 19/10/2017

- ✓ **Disponibilidad:** Garantizar que los usuarios autorizados tengan acceso a los activos de información cada vez que lo requiera.
- ✓ **No-Repudio:** No se puede negar un evento o una transacción.
- ✓ **Autenticidad:** Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.

RIESGO RESIDUAL: Es el riesgo realmente existente después del tratamiento del riesgo. (ISO/27001)

RIESGOS TECNOLÓGICOS: Son aquellos que tienen que ver con la capacidad de la entidad y organismo para que la tecnología disponible satisfaga sus necesidades actuales y futuras en aras de garantizar el cumplimiento de su misión y objetivos institucionales

SISTEMA INTEGRADO DE GESTION: Es el conjunto de orientaciones, procesos, políticas, metodologías, instancias e instrumentos enfocados en garantizar un desempeño institucional articulado y armónico que busque de manera constatable la satisfacción de los grupos de interés.

SEGURIDAD DE LA INFORMACIÓN: Es el conjunto de medidas preventivas de los sistemas tecnológicos que permiten resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de la misma, y otras propiedades como autenticidad, responsabilidad, no-repudio y confiabilidad.

SEGURIDAD INFORMÁTICA: Hace referencia a la protección de la infraestructura tecnológica y de comunicación que soportan el funcionamiento adecuado de la Subred Norte ESE (hardware y software).

SERVICIO DE PROCESAMIENTO DE INFORMACIÓN: Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los alberga.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI): Es parte del sistema de integrado de gestión, basado en un enfoque de riesgo que permite: establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

SOFTWARE: Es todo conjunto intangible de datos y programas implementados para un sistema informático.

SOFTWARE MALICIOSO: Software que tiene como objetivo infiltrarse, dañar o controlar el sistema de un computador sin consentimiento de su propietario.

TRATAMIENTO DEL RIESGO: Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo. (ISO/27001).

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 9 DE 12
		FECHA: 19/10/2017

7. DESARROLLO

7.1. BENEFICIOS DE LA IMPLEMENTACIÓN DEL SGSI

La implementación del SGSI, ofrece a la Subred Integrada de Servicios de Salud Norte ESE beneficios económicos, legales y reputaciones como:

- Reducción de los costos vinculados a los incidentes.
- El incremento de los niveles de confianza de clientes.
- Una mejora continua en la gestión de la seguridad.
- Mejora y mantener la imagen de la organización.
- Una garantía de continuidad y disponibilidad de los servicios informáticos.
- Voluntad de cumplir con la legislación vigente de protección de datos de carácter personal, servicios de la sociedad de la información, comercio electrónico, propiedad intelectual
- Análisis de riesgos, identificando amenazas, vulnerabilidades e impactos en la organización.

7.2. METODOLOGÍA PHVA IMPLEMENTACIÓN DEL SGSI

El proceso de implementación del SGSI, adopta el modelo de mejora continua PHVA (Planificar, hacer, verificar y actuar) aplicado a toda la estructura de procesos del SGSI. El modelo PHVA establece que no es suficiente con el diseño e implementación del SGSI, sino que es necesario garantizar la revisión periódica y continua.

Un SGSI debe identificar fundamentalmente, los objetivos, alcance, situación actual del sistema y los procesos de negocio críticos para la organización

7.3. FASES DE IMPLEMENTACION DEL SGSI

Para el diseño del plan de seguridad de la información se toma como base el ciclo de mejora continua para lograr de una forma sistemática y estructurada el desarrollo del sistema teniendo en cuenta los siguientes aspectos:

- 7.3.1. **Planear:** Es la primera fase de desarrollo del sistema, en la cual se tiene como producto principal el diagnóstico del estado actual de la seguridad de la información de la Subred Norte ESE y es necesario identificar los siguientes ítems:
- ✓ Levantamiento de la información relacionada con tecnología de la información y comunicaciones.
 - ✓ Caracterización de las diferentes bases de datos que maneja la Subred Norte ESE.
 - ✓ Análisis de la situación actual.
 - ✓ Definición del alcance de seguridad de la información.
 - ✓ Aprobación y de la política de seguridad de la información.
 - ✓ Compromiso de la alta dirección, de la importancia de la seguridad de la información para Subred Norte ESE.
 - ✓ Identificación del grado de capacidad y madurez de la seguridad de la información.
 - ✓ Definición de metodología a seguir, identificando la normatividad.
 - ✓ Definición de Cronograma de implementación.

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 10 DE 12
		FECHA: 19/10/2017

- ✓ Definición de manuales de uso de activos de información

7.3.2. **Hacer:** Para continuar con el proceso de diseño del plan de seguridad de la información es necesario llevar a cabo el cronograma de trabajo y las acciones planeadas en la fase anterior, de acuerdo a esto y teniendo en cuenta que esta fase corresponde a la formación y educación del personal es necesario realizar:

- ✓ Gestión de los Activos:

El objetivo promueve la protección y tratamiento de los activos de información importantes para la organización; establece responsabilidades sobre ellos y clasifica la información basada en su confidencialidad, es necesario definir: Inventario de los Activos y asignación de propietario/responsable, clasificación de los Activos, según su valor, los aspectos legales o criticidad para la empresa.

- ✓ Gestión de Riesgos:

El objetivo es realizar la evaluación del riesgo, estableciendo como primera medida el contexto, para luego realizar el análisis de riesgos, análisis de vulnerabilidades, la evaluación, el monitoreo y la aceptación del riesgo.

- ✓ Seguridad Ligada a los Recursos Humanos:

La seguridad de la información depende del recurso humano, tanto interno como externo, por lo cual es necesario establecer procedimientos e instructivos para: Escenarios posibles (antes, durante y después de la contratación) y actividades a realizar, definición de roles y perfiles de usuario para cada área de la Subred Norte ESE con respecto a la seguridad, establecer responsabilidades de los roles, Plan de capacitación sobre políticas de seguridad implementadas en la Subred Norte ESE.

- ✓ Seguridad Física y Ambiental:

El objetivo es proteger los recursos de información críticos y sensibles de la Subred Norte ESE, relacionados con la seguridad física, especialmente los accesos no autorizados o interrupciones en las actividades, incluye desde los edificios hasta la seguridad física de los equipos, donde es necesario identificar: Elementos físicos y ambientales a proteger, medidas de protección, roles y responsabilidades que intervienen, elementos a proteger.

- ✓ Gestión de las Comunicaciones y Operaciones:

El objetivo es establecer las responsabilidades y procedimientos para la gestión y operación de todos los recursos de información, como: Actualización de los sistemas, Protección de los sistemas frente a código malicioso o descargable, Seguridad de las redes, Registro de actividades y Copias de seguridad.

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 11 DE 12
		FECHA: 19/10/2017

✓ **Control de Acceso:**

Se refiere a los accesos lógicos a la información de la Subred Norte ESE, se basa en la forma como se puede evitar que personal no autorizado pueda lograr el acceso a la información que se está protegiendo. Para lo cual para el ingreso a los recursos informáticos de la Subred Norte ESE tiene un sistema de autenticación de los usuarios, de forma general a través de usuario y contraseña. Como actividades es necesario trabajar: Definición de los niveles de acceso, Definición de las medidas técnicas a implantar, Definición de los permisos de acceso, Definición y difusión de políticas de acceso, Acceso a nivel de Red, Acceso a nivel de sistema operativo, Acceso a nivel de aplicaciones y datos.

✓ **Adquisición, Desarrollo y Mantenimiento de Sistemas de Información:**

En este procedimiento se refiere a los aspectos relevantes a tener en cuenta para la implementación y mantenimiento de un sistema de información integral: Gestionar la Adquisición de un Sistema de Información Integrado, Implementación del Sistema de Información Integrado, Asegurar que la seguridad sea una parte integral de los sistemas de información, evitar errores, perdida, modificaciones no autorizada o mal uso de la información en las aplicaciones, proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos, garantizar la seguridad de los archivos del sistema.

✓ **Gestión de Incidencias de Seguridad:**

El objetivo de la Gestión de Incidencias es resolver de la manera rápida, eficiente y eficaz, cualquier incidente o no conformidad relacionada con la seguridad de los sistemas.

✓ **Planes de Contingencia:**

El objetivo es garantizar la continuidad de las operaciones de los elementos o procesos informáticos considerados como críticos y que componen el sistema de Información, por medio de acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen el Sistema de Información.

✓ **Acreditación:**

El objetivo es documentar, aprobar y socializar el plan de gerencia de la información, como parte fundamental del proceso de acreditación en salud de la Subred Norte ESE.

- 7.3.3. **Verificar:** Para la tercera fase se realiza seguimiento y evaluación de los factores descritos en la segunda fase, teniendo en cuenta los requisitos legales, reglamentarios y contractuales de seguridad a los que están sujetos los sistemas de información, y garantizar del plan de seguridad de la información cumpliendo con los tiempos y resultados esperados.

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:AP-GI-PL-02-01
		VERSION :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 12 DE 12
		FECHA: 19/10/2017

7.3.4. **Actuar:** En la fase de actuar permite realizar mejora continua de acuerdo a la evaluación, seguimiento y auditorías realizadas en el diseño del plan de seguridad de la información permitiendo la toma de decisiones.

8. SEGUIMIENTO Y MEDICIÓN

El seguimiento del Plan de Gerencia de la Información se realizará a través del Comité de Sistemas y Seguridad de la Información, el cual sesionará de acuerdo con la resolución que lo conforma. No obstante y para efectos de verificar la efectividad del Plan se diseñará y mantendrá un tablero de seguimiento para los proyectos y metas definidos en cada uno de los estándares, el cual tendrá un seguimiento no mayor al semestre y con sus respectivos informes.

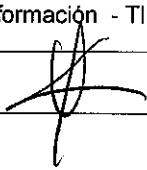
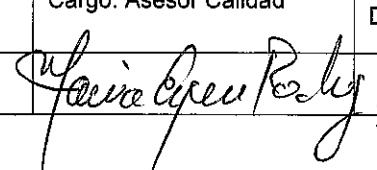
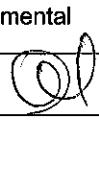
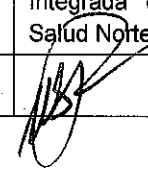
9. BIBLIOGRAFÍA

- Compendio Sistema de Gestión de la Seguridad de la Información (SGSI)
- Modelo de Seguridad y Privacidad de la Información – Seguridad y privacidad de la información – MinTIC.
- J.M San Martin G, “La Seguridad de la Información Nueva ventaja competitiva en la empresa (I/IV)” [Online]. Disponible:
<http://dialnet.unirioja.es/servlet/articulo;jsessionid=14432189D775360F21145B837ECC2C47.dialnet01?codigo=824400>

ANEXOS

- Anexo 1. Instructivo de Administración de Cuentas de Usuario
Anexo 2. Instructivo Generación Copias de Seguridad (BACKUPS)
Anexo 3. Instructivo Uso Recursos Tecnológicos.

CONTROL DEL DOCUMENTO			
Versión	Fecha	Descripción de la modificación	Realizada por
1	19/10/2017	Creación	Nombre: Norberto Ruiz Rodríguez Cargo: Jefe Oficina Sistemas de Información - TIC

Elaboró:	Revisó:	Aval técnico de normalización:	Aprobó:
Nombre: Norberto Ruiz Rodríguez	Nombre: María Eugenia Rodríguez	Nombre: Luisa Fernanda Castillo Rodríguez	Nombre: Yidney Isabel García Rodríguez
Cargo: Jefe Oficina Sistemas de Información - TIC	Cargo: Asesor Calidad	Cargo: Profesional Gestión Documental	Cargo: Gerente Subred Integrada de Servicios de Salud Norte ESE
			

La última versión de cada documento será la única válida para su utilización y estará disponible en el Listado Maestro de Documentos.
No haga copias de este documento porque corre el riesgo de tener una versión desactualizada