PLAN DE TRATAMIENTO DEL RIESGO DE LA INFORMACIÓN

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

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

CONTENIDO

1. INTRODUCCIÓN 3
2. JUSTIFICACIÓN 3
3. ALCANCE 3
4. OBJETIVOS 3
4.1 Objetivos Específicos 4
5. MARCO NORMATIVO 4
5.1 De orden Nacional 4
5.2 De orden Internacional 7
6. VOCABULARIO 7
7. DESARROLLO 11
7.1 Actividades del Plan de tratamiento 11
7.2 Cumplimiento de Implementación 12
7.3 Cronograma 13
8. SEGUIMIENTO Y MEDICIÓN 13
9. BIBLIOGRAFÍA 13

1. INTRODUCCIÓN

La gestión de los riesgos de Seguridad y Privacidad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, lo que permite conocer las debilidades que pueden afectar el ciclo de vida del servicio TI, adicionalmente el incremento en la participación digital de los ciudadanos, trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado; situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo.

2. JUSTIFICACIÓN

La creciente relevancia del entorno digital sobre las actividades socioeconómicas, y su alto dinamismo, ha traído consigo un conjunto de riesgos, amenazas, vulnerabilidades e incidentes de diversos tipos, a los que se encuentran expuestos los individuos y las organizaciones, públicas como la nuestra y las privadas.

Es muy importante que las organizaciones cuenten con un plan de gestión de riesgos para garantizar la continuidad del negocio. Por este motivo, se tiene la necesidad de desarrollar un análisis de riesgo de Seguridad y Privacidad de la información aplicado a la Subred Integrada de Servicios de Salud Norte ESE.

3. ALCANCE

Para iniciar con este plan de gestión se debe realizar el autodiagnóstico del sistema actual de la entidad, donde se conoce la situación actual de la institución y la identificación de los activos de información, para continuar con la medición de riesgos existentes y sugerir las protecciones y controles necesarios que podrían formar parte del plan de gestión de riesgos en la Seguridad y Privacidad de la información en la Subred Integrada de Servicios de Salud Norte ESE.

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos de información mediante el nivel de madurez de la seguridad existente y sobre todo incentivar a todos los funcionarios y / o servidores, contratistas, proveedores y particulares a seguir las respectivas políticas, normas y procedimientos referentes a la Seguridad y Privacidad de la información y recursos.

4. OBJETIVOS

Desarrollar e implementar el Plan de Tratamiento de la gestión de la seguridad y privacidad de la información que permita minimizar los riesgos de pérdida de activos de la información y de la ciberseguridad de la institución.

4.1 Objetivos Específicos

- Plantear reportes para uso en cada incidencia presentada en la Subred Integrada de Servicios de Salud Norte ESE.
- Gestionar los eventos de Seguridad y Privacidad de la información así como de ciberseguridad para detectar y tratar con eficiencia, los incidentes de seguridad .Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Definir los principales activos de Información a proteger en la Subred Integrada de Servicios de Salud Norte ESE.
- Identificar las principales amenazas que afectan a los activos de información.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo de información.

5. MARCO NORMATIVO

5.1 De orden Nacional

NORMA	CONTENIDO
Constitución Nacional	**Art. 15.** Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

NORMA	CONTENIDO
Ley 527 de 1999 (Comercio Electrónico)	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

NORMA	CONTENIDO
Ley 1266 de 2008 (Habeas Data)	Contempla las disposiciones generales en relación al Derecho de Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009 (Delitos Cibernéticos)	En el año 2009 se expide la Ley 1273 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos” – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones”. Se crean los siguientes tipos penales: Capítulo I – “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”, este capítulo tipifica las siguientes conductas penales: Acceso Abusivo a un sistema informático, obstaculización ilegítima de sistema informático o de red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales. Capítulo II – “De los atentados informáticos y otras infracciones”, este capítulo tipifica las siguientes conductas: hurto por medios informáticos y semejantes, transferencia no consentida de activos.
Ley 1453 de 2011 (Estatuto de seguridad ciudadana)	**El Art. 236** Establece que cuando el fiscal tenga motivos razonables, para inferir que el indicado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a la policía la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado. La aprehensión que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados, de ser el caso.

NORMA	CONTENIDO
Ley 1581 de 2012 (Habeas Data)	"Por la cual se dictan disposiciones generales para la protección de datos". Esta Ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios.
Resolución SIC No. 76434 de 2012 (Habeas Data)	Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países.
Resolución CRC 3067 de 2011 "Por la cual se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones"	Está Resolución establece en el artículo 2.3, que los PRST que ofrezcan acceso a internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción e interferencia del mismo. Para lo cual, deben informar en su página web las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls. Filtros antivirus y la prevención del spam, phishing, malware entre otros; no obstante la responsabilidad de los PRST no cubre los equipos del cliente, puesto que los mismos son controlados directamente por el usuario del servicio. Adicionalmente, los PRST que ofrezcan acceso a internet deberán implementar modelos de seguridad, de acuerdos con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, en línea con los marcos de seguridad definidos por la UIT, en lo relativo a las recomendaciones pertenecientes a las series X.800, y en relación con los siguientes aspectos: autenticación (UIT X.805 y UIT X.811), acceso (UIT X.805 y UIT X.812), no repudio (UIT X.805 y UIT X.813), confidencialidad de datos (UIT X.805 y UIT X.814), integridad de datos (UIT X.805 y UIT X.815) y disponibilidad (UIT X.805). Finalmente se establece, los PRST a través de redes móviles, deberán implementar modelos de seguridad que eviten el acceso no autorizado, la interrupción, el repudio o la interferencia deliberada de la comunicación, utilizando modelos de cifrados, firmas digitales y controles de acceso descritos en las recomendaciones UIT X.1121 y X.1122.

5.2 De orden Internacional

NORMA	CONTENIDO
Convenio sobre Ciberdelincuencia del Consejo de Europa	Conocido como el convenio sobre Cibercriminalidad de Budapest, mediante el cual se adopta una legislación que facilita la prevención de las conductas delictivas y contribuye con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas
Resolución AG /RES 2004 (XXXIV-O/04) de la Asamblea General de la OEA	Mediante la cual se establece una estrategia integral para combatir las amenazas a la seguridad cibernética con un enfoque multidimensional y multidisciplinario, para la creación de una cultura de la seguridad cibernética
Decisión 587 de la Comunidad Andina	Por la cual se establecen los lineamientos de la Política de seguridad externa común andina.
Declaración de la Cumbre de Gales de la OTAN en 2014	En donde se resaltan acuerdos para abordar la ciberseguridad en los países de dicha alianza.

6. VOCABULARIO

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

7. DESARROLLO

Para el desarrollo del presente Plan se debe tener en cuenta la metodología establecida por la Subred Norte ESE así como la Política de Administración del Riesgo definida. Este plan de tratamiento del riesgo de la información va enfocado a la Seguridad y Privacidad de la información así como el tratamiento que se le da a la información que maneja la institución.

7.1 Actividades del Plan de tratamiento

- ***Realizar autodiagnóstico***, para esta actividad se tomara la matriz de autodiagnóstico entregada por MINTIC y la de MIPG en relación a Seguridad Digital.
- ***Elaborar el Alcance*** del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
- ***Realizar la Identificación de los Riesgos*** con los líderes del Proceso que manejan información y realizan tratamiento a los diversos datos en los diferentes sistemas de información ya sean manuales o automáticos dentro de la Subred Norte ESE.
- ***Definir el riesgo o los riesgos*** encontrados dentro de la Seguridad y Privacidad de la información y su tratamiento, incluye ciberseguridad y seguridad digital.
- ***Análisis del Riesgo***, En esta etapa se busca el desarrollo y la comprensión del riesgo, tomando como entrada la información obtenida de la identificación del riesgo. Dos aspectos fundamentales se deben definir dentro de este proceso:

  Probabilidad: Posibilidad de ocurrencia del riesgo.
  Impacto: Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

TABLA DE PROBABILIDAD			
DESCRIPTOR	**NIVEL**	**DESCRIPCIÓN**	**FRECUENCIA**
Rara vez	1	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
Improbable	2	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
Posible	3	El evento podría ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
Casi seguro	5	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

TABLA DE IMPACTO		
DESCRIPTOR	NIVEL	DESCRIPCIÓN
Insignificante	1	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
Menor	2	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
Moderado	3	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
Mayor	4	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
Catastrófico	5	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

- ***Evaluación del riesgo***; Permite comparar los resultados de su calificación en términos de probabilidad e impacto, para tener un primer resultado cuantitativo y cualitativo del estado actual del riesgo sin haber tomado acción alguna para su manejo y así posteriormente poder tomar decisiones y definir los controles a ejecutar.
- ***Valoración del riesgo y controles***.

7.2 Cumplimiento de Implementación

De acuerdo a las actividades mencionadas anteriormente, se describe a continuación los dominios que se deben tener en cuenta a la hora de identificar riesgos y establecer los controles o mejoras:

- Revisión y/o Modificación de la actual Política de Seguridad si da lugar.
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

7.3 Cronograma

Se tendrá en cuenta el cronograma establecido por la oficina de desarrollo institucional de la Subred Norte ESE para la Gestión de riesgos.

8. SEGUIMIENTO Y MEDICIÓN

Se realizara acorde a lo definido por la oficina de desarrollo institucional de la Subred Norte ESE para el seguimiento y evaluación de la gestión de riesgos.

9. BIBLIOGRAFÍA

- Guía para la administración del Riesgo del Departamento Administrativo de la Función Pública – DAFP.
- CONPES 3701 de 2011 sobre los lineamientos de políticas para la ciberseguridad y ciberdefensa de la Republica de Colombia.
- Documento de Análisis y consulta de Identificación de posibles acciones regulatorias a implementar en materia de ciberseguridad, de la Comisión de Regulación de Comunicaciones – CRC de Julio de 2015 de la Republica de Colombia.

CONTROL DEL DOCUMENTO			
Versión	**Fecha**	**Descripción de la modificación**	**Realizada por**
1	08/08/2018	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: Martha Ligia Castillo Díaz	Nombre: Yidney Isabel García Rodríguez
Cargo: Jefe Oficina Sistemas de Información - TIC	Cargo: Asesor Calidad	Cargo: Líder Gestión Documental	Cargo: Gerente Subred Integrada de Servicios de Salud Norte ESE
ORIGINAL FIRMADO			