CONTROL DEL DOCUMENTO

Información del Documento

	Información del Documento
Dueño del Documento	Ministerio de Salud y Protección Social
Última Fecha Actualizado	Octubre 2014
Ubicación y Nombre del Archivo	.
Circulación	*Ministerio de Salud Y Protección Social*

Historia del Documento

Versión	Fecha de Elaboración del documento o del Cambio	Resumen General del Contenido del Documento o Descripción General de Cambio al mismo
1.0	*Agosto - 2014*	Política general de seguridad de la información del Ministerio de Salud y Protección Social.

Revisión del Documento

Nombre	Rol	Firmas	Fecha

Aprobación del Documento

Nombre	Rol	Firmas	Fecha

1. Objetivo

Proteger, conservar y asegurar los recursos de información del Ministerio de Salud y Protección Social, y las herramientas tecnológicas utilizadas para su generación, procesamiento y publicación, con el fin de preservar la confidencialidad, integridad y disponibilidad frente amenazas internas o externas, deliberadas o accidentales.

2. Alcance

Esta política estable los criterios y comportamientos que deben seguir todos los miembros de la comunidad del Ministerio de Salud y Protección Social (servidores públicos, contratistas y terceros, entre otros) para preservar la seguridad de la información en el Ministerio.

3. Glosario

Activo de información: cualquier elemento que represente valor para la organización

Activos de información: bases de datos, documentación, manuales, software, hardware, contratos, equipos de comunicación, servicios informáticos y de comunicaciones, utilidades generales (iluminación, energía, aire acondicionado, etc.) y las personas (son quienes generan, transmiten y destruyen información)

Amenaza: Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización [ISO 27000:2014]

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo [ISO 27000:2014].

Comunicación del riesgo: Comunicar o intercambiar la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [ISO/IEC 27000: 2014]

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada [27000: 2014].

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Identificación del riesgo: Proceso para encontrar, numerar y caracterizar los elementos del riesgo.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrado.

Integridad: Propiedad de la información relativa a su exactitud y completitud. [ISO/IEC 27000: 2014]

Probabilidad: Frecuencia o factibilidad de ocurrencia del Riesgo.

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.

Tratamiento del riesgo: Selección e implementación de las opciones o acciones apropiadas para ocuparse del riesgo.

Valor del Impacto: Está determinado por el responsable del activo de información, quién provee el grado de afectación por incidentes o materialización de riesgos de los activos de información que tenga a cargo.

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

4. Introducción

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración del Ministerio de Salud y Protección Social con respecto a la protección de los activos de información (los servidores públicos, la información, los procesos, las tecnologías de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

El Ministerio debe contar con plataformas apropiadas protegiendo los mecanismos de tratamiento, almacenamiento y comunicación donde están contenidos y soportados sus servicios de consulta, registro, validación y realización de trámites del sistema de Seguridad Social de Colombia, contando con personal competente y comprometido con una cultura de seguridad reflejada en la aceptación y aplicación de las directrices establecidas.

Con la implementación de políticas en seguridad de la información el Ministerio busca dar cumplimiento a disposiciones legales y regulatorias emitidas por los diferentes organismos estatales, contar con una metodología de gestión de riesgos como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la continuidad de los procesos del Ministerio.

Las políticas del sistema de gestión de seguridad de la información se definen según su orden de importancia en:

Primer Nivel.
Corresponde a la política del Sistema de Gestión de Seguridad de la información (SGSI), la cual es una directriz global que establece qué y por qué se quiere proteger. Su definición y actualización está alineada con la planeación estratégica de la organización.

Segundo Nivel.
Corresponde a la política General de Seguridad de la información, la cual establece las responsabilidades generales aplicables a todo el Ministerio en lo que respecta al uso adecuado de los activos para la gestión de la información.

Tercer Nivel.
Corresponde a políticas específicas enfocadas a grupos, servicios o actividades particulares. Su definición y actualización debe reflejar cambios de índole organizacional y tecnológica.

5. Política del Sistema de Gestión de Seguridad de la información (SGSI).

Es la directriz global que establece qué se quiere proteger, por qué se requiere la protección y cómo se deben proteger los activos y sistemas informáticos del Ministerio de Salud y Protección Social, la definición y actualización de la política está orientada a los procesos del Ministerio (misionales, apoyo, estratégicos y evaluación).

Los principales objetivos de esta política son:

- Contar con plataformas apropiadas que protejan los mecanismos de tratamiento, almacenamiento y comunicación donde están contenidos y soportados los servicios de consulta, registro, validación y realización de trámites del Ministerio de Salud y protección Social.

- Educar al personal para lograr servidores públicos competentes y comprometidos con una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices de seguridad.

- Implementar una metodología de gestión de riesgos de seguridad de la información como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la continuidad, confidencialidad e integridad de la información Ministerio de Salud y Protección Social.

6. Política General.

La información que se maneja en el Ministerio de Salud y Protección Social, solamente podrá ser utilizada con fines de interés publico de conformidad con la constitución y las leyes.

Las herramientas y servicios informáticos asignados a cada usuario, son para uso limitado a la función institucional.

Todos los servidores públicos, contratistas y terceros que conforman las diferentes áreas del Ministerio deberán clasificar la información que tengan bajo su custodia en alguna de las categorías establecidas.

La información confidencial de terceros que por cualquier circunstancia se conozca por parte del Ministerio, debe ser tratada bajo los mismos lineamientos establecidos para el tratamiento de la información confidencial del Ministerio.

Toda la información catalogada por las áreas como critica debe contar con copias de respaldo para garantizar su seguridad.

Los centros de cómputo y procesamiento de información son áreas de acceso restringido por tal motivo el ingreso y permanencia debe ser controlado y supervisado.

El acceso a los diferentes equipos informáticos y sistemas de información debe hacerse a través de los mecanismos de autenticación establecidos de acuerdo con los niveles de seguridad.

El acceso no autorizado a los sistemas de información y uso indebido de los recursos informáticos de la entidad está prohibido. Se considera que hay uso indebido de la información y de los recursos, cuando la persona incurre en cualquiera de las siguientes conductas:

a. Suministrar información confidencial o que tenga carácter reservado a quien no tenga derecho a conocerla.
b. Usar la información con el fin de obtener beneficio propio o de terceros.

c. Ocultar la información maliciosamente causando cualquier perjuicio.
d. Hacer pública la información sin la debida autorización.
e. Hurtar software del Ministerio (copia o reproducción entre usuarios finales).
f. Realizar copias no autorizadas de software del Ministerio, dentro y fuera de sus instalaciones.
g. Falsificar y duplicar un producto informático de Ministerio.
h. Descargar software, a través de Internet sin la debida autorización.
i. Intentar modificar, reubicar o sustraer equipos de cómputo, software, Información o periféricos sin la debida autorización.
j. Capturar sin autorización la información de los accesos de otros usuarios a los sistemas.
k. Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.
l. Utilizar la infraestructura del Ministerio (computadores, software, información o redes) para acceder a recursos externos con propósitos ilegales o no autorizados.
m. Enviar cualquier comunicación electrónica fraudulenta.
n. Apropiarse los aplicativos, desarrollos o información del Ministerio y publicarla como propio.
o. Adueñarse del trabajo de otros individuos, o de alguna manera apropiarse del trabajo ajeno.
o. Usar cualquier medio para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
p. Lanzar cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil o destructiva.
q. Descargar o publicar material ilegal, o implique la vulneración de derechos de terceros, o material nocivo usando un recurso del Ministerio.
r. Uso personal de cualquier recurso informático del Ministerio para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material prohibido.
s. Acceder sin autorización a información o documentos públicos que tengan carácter reservado por disposición constitucional o legal.
t. Violar cualquier Ley o Regulación Nacional respecto al uso de sistemas de información.

7. Políticas Específicas

Forman parte integral de la Política de Seguridad de la Información, todas aquellas directrices que por su tema particular, requieren un mayor nivel de detalle y especialización para su definición, las cuales son elaboradas y mantenidas por las áreas

de seguridad, según el dinamismo de la misión del Ministerio y las cuales a su vez pueden estar complementadas por estándares y guías,
a continuación se describen algunas de ellas.

Políticas específicas para funcionario y contratistas:

- Política de uso de estaciones de trabajo.
- Política de desarrollo y mantenimiento de aplicaciones.
- Política de contraseñas.
- Política de correo electrónico.
- Política de uso de Internet e Intranet.
- Política de antivirus.
- Política de Acceso aplicaciones.
- Política de asignación y uso de dispositivos de autenticación fuerte.
- Política de seguridad física a los sistemas de información.
- Política de uso VPN y acceso remoto.
- Política de acceso a servidores.
- Política de acceso a Bases de datos
- Política de tratamiento de datos personales

Políticas específicas para usuarios externos:

- Política de uso de Internet.
- Política para estaciones de trabajo de terceros.

8. Cumplimiento

Estas políticas a todo nivel, son mandatarias, por lo tanto deben ser cumplidas por los servidores públicos, contratistas y terceros que interactúen con los Sistemas de Información y demás recursos informáticos del Ministerio.

El Incumplimiento significa toda conducta de cualquier miembro del Ministerio que no respete las políticas. Entre los ejemplos de incumplimiento se incluyen, sin limitarse a ellos:

a. Los servidores públicos que sean negligentes en la aplicación de medidas de seguridad y control dentro de la organización.

b. Una acción o inacción por parte de un servidor público que contribuye a la violación de las normas orientadas al buen uso de la información.

c. Un servidor público que no resuelve o remite inmediatamente a una autoridad superior los problemas de seguridad de la información que sean detectados.

d. Los servidores públicos que no tomen las medidas correspondientes ante una queja o un incidente de seguridad.

Todos los miembros del Ministerio son responsables de implementar las Políticas y procedimientos de seguridad que se contemplan o son referenciados en este documento y sus complementarios.
El incumplimiento de las Políticas y Procedimientos de Seguridad, para los servidores públicos constituye falta disciplinaria conforme a lo señalado en los numerales 4 y 5 del artículo 34 y numerales 16 y 43 del artículo 48 de la ley 734 de 2002.

Artículo 34 Son deberes de todo servidor público:

"… 4. Utilizar los bienes y recursos asignados para el desempeño de su empleo , cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función en forma exclusiva para los fines a que están afectos."

"… 5. Custodiar y cuidar la documentación que por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos."

Articulo 48. Son faltas Gravísimas las siguientes:

"…16. Atentar con cualquier propósito, contra la inviolabilidad de la correspondencia y demás formas de comunicación, u obtener información o recaudar prueba con desconocimiento de los derechos y garantías constitucionales y legales"

"…43. Causar daño a los equipos estatales de informática, alterar, falsificar ,introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos y en los que se almacene o guarde la misma, o permita el acceso a ella a personas no autorizadas."

Los contratistas, consultores y terceros que estén involucrados en incidentes de incumplimiento pueden ver terminado su contrato de acuerdo con las condiciones que en él se han establecido.

Si por alguna razón, estas Políticas no cubren algún caso en concreto, se deberá consultar a la OTIC, quien emitirá su concepto o disposición al respecto previa consulta de las áreas del Ministerio que haya lugar, según sea el caso.

La competencia para realizar la investigación disciplinaria es la Oficina de Control Interno Disciplinario (art.76 Ley 734 de 2002). Las faltas y sanciones son las establecidas en la ley 734 de 2002, conforme al procedimiento constituido para el efecto.

9. Notificación de Incidentes

Toda violación de estas políticas se deberá notificar inmediatamente a la OTIC a través de la cuenta gr.sgsi@minsalud.gov.co.

Se busca asegurar que todos comprendan y respeten las políticas con el fin de reducir al mínimo el riesgo, protegiendo a todas las personas, así como al Ministerio.

Se deberán notificar situaciones tales como:

- Personas ajenas del Ministerio en centros de cómputo sin la debía autorización.
- Correos con virus,
- Reinicio de los equipos de cómputo o enrutadores,
- Mala utilización de recursos,
- Uso ilegal del software,
- Mal uso de información corporativa,
- Alteración de información, etc.

Las políticas de seguridad de la información del Ministerio fueron diseñadas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en las leyes y regulaciones, por lo tanto si algún servidor publico, contratista y/o tercero del Ministerio considera que alguna política de seguridad de información está en conflicto con las leyes y regulaciones existentes, tiene la responsabilidad de reportar en forma inmediata dicha situación a través de la cuenta gr.sgsi@minsalud.gov.co donde será atendida.

10. Roles

Usuario:
Todo servidor publico, contratista, ente regulador, socios de negocios, y terceros entre otros que estén involucrados con información del Ministerio de Salud y Protección Social.

Líder de Seguridad:
Servidor publico responsable de establecer y mantener la estrategia y programa para asegurar los activos de información en el Ministerio de Salud y Protección Social.

11. Normatividad.

CONGRESO DE LA REPUBLICA. LEY 734 DE 2002 .Por la cual se expide el código disciplinario único. Febrero 2002.

CONGRESO DE LA REPUBLICA. LEY 1273. 2009 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, entre otras disposiciones.

CONGRESO DE LA REPUBLICA LEY 1581 DE 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

CONGRESO DE LA REPUBLICA 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.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana NTC-ISO-IEC-27001 Sistemas de Gestión de la Seguridad de la Información (SGSI).

MINISTERIO DE SALUD Y PROTECCION SOCIAL. Resolución 2624 de 2013.
Por la cual se modifica la Resolución No. 2624 del 18 de julio de 2013 Por la que “se crean, conforman y asignan funciones a órganos de asesoría y coordinación del Ministerio de Salud y Protección Social, se establece el Sistema Integrado de Gestión Institucional, se definen sus instancias, y se dictan otras disposiciones”

MINISTERIO DE SALUD Y PROTECCION SOCIAL. Resolución 2126 del 2012. Por la cual se crea el Comité de Gobierno en Línea y Antitrámites en Ministerio de Salud y Protección Social y se dictan otras disposiciones. Agosto 2012.

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Modelo de seguridad de la información de Seguridad de la información para la estrategia de GOBIERNO EN LÍNEA. Diciembre 2008.