E.S.E. HOSPITAL DEL ROSARIO CAMPOALEGRE HUILA

MECI 1000 2014
NTC GP 1000 2009
SOGCS
Decreto 1011 del 2006

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION-2020

ENERO DEL 2020

1. PRESENTACION

El presente plan se elabora con el fin de dar a conocer como se realizará la implementación y socialización del componente de Gobierno en línea en el Eje Temática de la Estrategia en seguridad y privacidad de la información, el cual busca salvaguardar los datos de los usuarios de la E.S.E HOSPITAL DEL ROSARIO, Teniendo en cuenta la importancia que cada uno de estos representa para nuestra institución.

2. DEFINICIONES

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 controle 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)

- Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

- Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

- Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- 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.

- Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

- 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)

- Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (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).

- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

3. OBJETIVO GENERAL

Identificar y controlar los riesgos asociados a los diferentes procesos tecnológicos que se llevan en la E.S.E HOSPITAL DEL ROSARIO. Con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de los usuarios encargados de dichos procesos.

OBJETIVOS ESPECIFICOS.

- Adaptar los procesos de la ESE HOSPITAL DEL ROSARIO con referencia a la norma y políticas en los riesgos de seguridad y privacidad de la información.

- Realizar una validación a los procesos de la ESE HOSPITAL DEL ROSARIO para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.

- Evaluar a cada líder del proceso para identificar el manejo e importancia que le da a la seguridad y privacidad de la información.

4. METODOLOGIA DE IMPLEMENTACION.

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la E.S.E HOSPITAL DEL ROSARIO, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

5. DESCRIPCION DEL CICLO DE OPERACIÓN.

El ciclo de funcionamiento para el modelo de operación de la E.S.E HOSPITAL DEL ROSARIO consta de 5 fases, a través de la descripción detallada de cada una de estas que lo comprenden. Estas, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.

PROCESO TOMADO MINTIC MODELO SEGURIDAD y PRIVACIDAD DE LA INFORMACION

6. FASES DE IMPLEMENTACION.

DIAGNOSTICO: en esta fase se pretende identificar la funcionalidad de cada proceso que se lleva en la E.S.E HOSPITAL DEL ROSARIO y tener un diagnóstico claro en cuanto a los avances que se necesita o si cumple con los parámetros que requiere la norma.

PROCESO TOMADO MINTIC MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

7. TABLA DE DIAGNOSTICO Y ESTADO ACTUAL DEL MSPI.

DIAGNOSTICO		
METAS	**RESULTADOS**	**INSTRUMENTOS MSPI**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	La E.S.E HOSPITAL DELROSARIO actualmente cuenta con un proceso de seguridad y privacidad de la información en cada una de las áreas en donde se presta el servicio en la institución, la información de cada uno de los usuarios que se obtiene cada día es resguardada en sistemas de información y bases de datos bajo estándares de calidad.	**Norma NTCISO/IEC 27001:2013.**
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Actualmente en la E.S.E HOSPITAL DEL ROSARIO cuenta con sistemas de información can capacidad de salvaguardar la información que es obtenida en cada uno de sus procesos, en la identificación de normatividad de cada una de sus áreas se pudo constatar que cada proceso debe ser adaptado a las políticas de seguridad que exige la norma.	**Norma NTCISO/IEC 27001:2013.**
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	En algunos procesos que se lleva en la E.S.E HOSPITAL DEL ROSARIO se pudo identificar que se cumplen los estándares de seguridad y procedimiento, pero se identificó que hay áreas que no tienen la política identificada como lo exige la norma.	**Norma NTCISO/IEC 27001:2013.**

8. FASE DE DIAGNÓSTICO DEL MSPI.

- Se diagnosticó el estado actual de la E.S.E HOSPITAL DEL ROSARIO referente al sistema de gestión de seguridad y privacidad de la información en cada uno de sus procesos.
- Referente al diagnóstico del estado y madurez de cada uno de los procesos se encontró que se deben realizar avances y adaptaciones a los procesos referente a la norma.
- La E.S.E HOSPITAL DEL ROSARIO se debe fijar plazos para la implementación del Modelo de Seguridad y Privacidad de la Información ya que se debe cumplir unos ciclos antes de estar en total funcionamiento.
- La E.S.E HOSPITAL DEL ROSARIO tiene políticas de la ley de protección de datos que se debe adoptar a las nuevas políticas y como lo exige la norma NTCISO/IEC 27001:2013.

- La E.S.E HOSPITAL DEL ROSARIO cuenta con políticas y herramientas al interior de la institución para la protección de los datos de cada uno de sus usuarios y ha establecido políticas institucionales para el buen uso de las herramientas de la información y la comunicación.

9. CRONOGRAMA.

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DIAGNOSTICO PRIMER CICLO ESE HOSPITAL DEL ROSARIO.			
ACTIVIDAD	**DESCRIPCION**	**FECHA**	**RESPONSABLE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	29-02-2020	Área de sistemas.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	06-03-2020	Área de sistemas.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación. Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación. Documento con los hallazgos encontrados en las pruebas de vulnerabilidad	06-03-2020	Área de sistemas.
Adoptar e implementar el Sistema de Gestión de Seguridad de la Información (SGSI) y preparar a la ESE Hospital del Rosario para la Certificación en ISO 27001:2013.	Crear y documentar el Sistema de Gestión de Seguridad de la Información (SGSI) y avanzar en la preparación de la Institución en la Certitifcación ISO 27001:2013.	13-03-2020	Área de sistemas.

10. SEGUIMIENTO y EVALUACION.

- DIAGNOSTICO: el primer ciclo de diagnóstico de la E.S.E HOSPITAL DE ROSARIO se logró identificar el proceso que se realizaba en cada una de las áreas de la institución.

- PLANIFICACION: el ciclo de planificación se encuentra en proceso de identificación y planeación referente a la necesidad de cada proceso.

- IMPLEMENTACION: el ciclo de implementación del plan de tratamiento se debe ejecutar con el diagnóstico y la planificación que se le haga a cada uno de los procesos de la E.S.E HOSPITAL DEL ROSARIO.

- EVALUACION DE DESEMPEÑO: el ciclo de evaluación de desempeño de la E.S.E HOSPITAL DEL ROSARIO se debe implementar en cada proceso cuando ya se encuentre en total funcionamiento el plan de tratamiento de riesgo de seguridad y privacidad de la información.

- MEJORA CONTINUA: el ciclo de mejora continua de la E.S.E HOSPITAL DEL ROSARIO se debe implementar en cada proceso cuando ya se encuentre en total funcionamiento el plan de tratamiento de riesgo de seguridad y privacidad de la información.

Original firmado

Andersson Zabala Toledo
Gerente ESE Hospital del Rosario