HOSPITAL CIVIL DE IPIALES
EMPRESA SOCIAL DEL ESTADO

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2019

Contenido

1. INTRODUCCIÓN

El Hospital Civil de Ipiales en busca de la mejora continua implementa un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados el manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma.

La institución en su quehacer diarioutiliza TICen cuanto a captura, procesamiento y reporte de información tanto internamente como externamente para comunicarse con los diferentes actores del sistema de salud, lo cual implica que la institución sea vulnerable a ataques mal intencionados o mala manipulación de la información lo que acarrea problemas económicos, legales, y administrativos por lo cual este documento busca establecer un línea de trabajo que permita a la entidad sortear los riesgos que lo rodean y lograr que su información este segura.

2. OBJETIVOS

OBJETIVO GENERAL

Desarrollar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información el cual sea una guía para el control y minimización de los de los riesgos y así proteger la privacidad de la información y los datos tanto de los procesos como de las personas vinculadas con la información de la institución.

OBJETIVOS ESPECÍFICOS

- Lograr un diagnóstico real de la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información

- Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y Mintic para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información

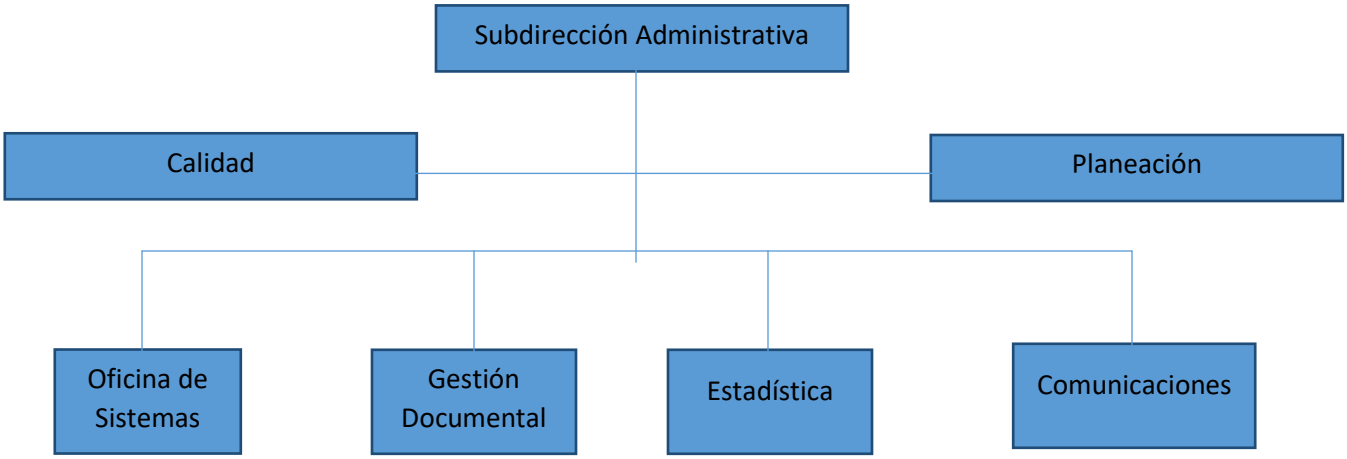
- Optimización de los recursos de la institución en la aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

3. ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

4. RESPONSABLES

La estructura organizacional de los procesos responsables de la realización del plan es la siguiente:



- Subdirector Administrativo
- Profesional Universitarios de Planeación
- Profesional Universitarios de Calidad
- Ingeniero De Sistemas
- Técnico en gestión documental
- Técnico administrativo en estadística
- Comunicadora social

5. MARCO CONCEPTUAL

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).

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.

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).

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

Ciberespacio: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española). ControlLas políticas, los procedimientos, las prácticas y las estructuras organizativasconcebidas para mantener los riesgos de seguridad de la información por debajodel nivel de riesgo asumido. Control es también utilizado como sinónimo desalvaguarda o contramedida. En una definición más simple, es una medida quemodifica el riesgo.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión deSeguridad de la Información – SGSI, de la organización tras el resultado de losprocesos de evaluación y tratamiento de riesgos y su justificación, así como lajustificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC27000).

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

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionaleso 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 dela información inaceptables e implantar los controles necesarios para proteger lamisma. (ISO/IEC 27000).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidadpara causar una pérdida o daño en un activo de información. Suele considerarsecomo 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 lainformación. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados interactuantes (estructuraorganizativa, políticas, planificación de actividades, responsabilidades,procesos, procedimientos y recursos) que utiliza una organización paraestablecer una política y unos objetivos de seguridad de la información yalcanzar dichos objetivos, basándose en un enfoque de gestión y de mejoracontinua. (ISO/IEC 27000).

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

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

Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a símisma como afectada por una decisión o actividad.

6. MARCO NORMATIVO

- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales
- Ley 527 de 1999 - Ley de Comercio Electrónico
- Ley 594 de 2000 - Ley General de Archivos
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información
- Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
- Decreto 2364 de 2012 - Firma electrónica
- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública

- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

- Decreto 1083 de 2015

- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública

- decreto 1008 de 2018[7], en donde se establecen los lineamientos generales de la Política de Gobierno Digital

- Decreto 612 de 2018 donde se consideran las definiciones del Decreto Único Reglamentario del Sector de TIC 1078 de 2015, estableciendo los instrumentos para implementar la "Estrategia de Gobierno en Línea"

7. DESCRIPCIÓN DEL PLAN

Identificación del riesgo:

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas recolectan datos de entrada para esta actividad.

Categorías de riesgos:

ET: Estratégicos: Relacionados a lineamientos, políticas, estrategias o directrices no adecuadas o no convenientes para la Entidad.

OP: Operativo: Relacionado a procesos, conductas o actividades inapropiadas, contrarias al deber ser o que presente una posible brecha frente a la calidad esperada.

FA: Financiero: Relacionado con la asignación, suficiencia o recaudo de recursos económicos que puedan afectar a corto, mediano o largo plazo financieramente a los procesos o la entidad.

TEC: Tecnológico: Relacionado al uso, manejo o disposición de equipos biomédicos, industriales o de cómputo y periféricos.

CL: Clínico: Relacionados a condiciones patológicas de pacientes atendidos en el HCI, considerar la aplicación de la metodología AMFE según lo definido en el MP-0266 MANUAL DE GESTION INTEGRAL DEL RIESGO.

Identificación de riesgos:

Normalmente se identifican los riesgos como eventos o situaciones no deseadas que se pretenden evitar, por tal razón la identificación de riesgos inicia con términos como: Ausencia, No adherencia, Inadecuada, No suficiencia, entre otros.

Una vez se identifique el riesgo, debe complementarse para obtener el contexto del riesgo, ya que éste puede presentarse en un área, en un horario, por parte de un grupo de colaboradores, o en unas circunstancias específicas que ayudarán más adelante a determinar las acciones a tomar. Estos son algunos ejemplos de preposiciones a utilizar: al, durante, en, sobre, con, hacia, de, mediante, entre otros.

Descripción de Causas:

Se describen las causas asociadas al riesgo identificado, pueden ser intrínsecas: atribuidas a personas, métodos, materiales, equipos, instalaciones, directamente involucradas en el proceso o externas: cuando provienen del entorno en el que se desarrolla el proceso.

Consecuencias:

Se describen los efectos asociados a la materialización del riesgo, que incidan sobre el objetivo del proceso o la Entidad. Pueden agruparse en: Daños a pacientes o trabajadores, Perdidas económicas, Perjuicio de la imagen, Sanciones legales, reproceso, Demoras, Insatisfacción, entre otras.

Barreras de Seguridad Existentes:

Se describen los controles implementados o barreras que existen actualmente para evitar la materialización del riesgo, se pueden encontrar en los protocolos o procedimientos documentados, en las guías de reacción inmediata o en los correctos de buenas prácticas de seguridad del paciente.

Valoración del Riesgo:

Se mide en cuanto a probabilidad e impacto para obtener un dato cuantitativo que permita su comparación y priorización, como se muestra en las siguientes escalas de valoración:

RESULTADOS DE LA CALIFICACION DEL RIESGO DE SEGURIDAD DIGITAL						
PROBABILIDAD	PUNTAJE			ZONAS DE RIESGO DE SEGURIDAD DIGITAL		
CASI SEGURO	5					
PROBABLE	4					
POSIBLE	3					
IMPROBABLE	2					
RARA VEZ	1					
IMPACTO		INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTROFICO
PUNTAJE		0	1	5	10	20

Tratamiento y Seguimiento del Riesgo:

Se describen los controles o barreras a ser implementadas que fortalezcan las existes, con lo cual aportar y evitar la materialización del riesgo desde la reducción de la probabilidad y/o del impacto. Las acciones propuestas pueden en algunos casos significar actualización de protocolos o procedimientos documentados, adopción de mejores prácticas a través de referenciaciones realizas, fortalecimiento de buenas prácticas de seguridad del paciente, asesorías con expertos, entre otras.

Un aspecto de gran importancia es la definición de indicadores para determinar el impacto de las acciones realizadas, ya que no es suficiente cumplir las actividades propuestas sino también valorar como estas acciones permiten disminuir la probabilidad de ocurrencia o nivel de impacto del riesgo; es decir, el indicador mide la efectividad de las acciones frente a la mitigación del riesgo.

IDENTIFICACION, VALORACION Y SEGUIMIENTO DE RIESGOS POR PROCESOS

CATEGORIA	Nº	IDENTIFICACION DE RIESGOS	FECHA DE IDENTIFICACION DE RIESGO	ANALISIS DEL RIESGO			VALORACION INICIAL DEL RIESGO		
				CAUSAS	CONSECUENCIAS	BARRERAS DE SEGURIDAD EXISTENTES	VALOR DE PROBABILIDAD	VALOR DE IMPACTO	NIVEL DEL RIESGO
TEC	1	Perdida de información por alretaciones en el sistema ó invonvenientes en equipos de computo ó servidores de datos, fluido electrico, daño en hardware especializado como servidores, swicth principales	1/01/2017	- Daño en hadware y sioftware especializado **redes**: daño en swicth principales como de nucleo, acceso, distribución y routerboard **Servidores:** daño fisico y logico de los principales servidores de produccion del HCI - Intrución Malware (virus informáticos, gusanos, troyanos, spyware, adware, rootkits) - Caidas y variaciones en el fluido electrico - Perdida de documentos del archivo de archivo de gestion, centra, historico e Historia clinica fisica	- Perdida de información administrativa y asistencial fisica ó magnetica - Retrazo de procesos como el registro de información clinica y administrativa - Perdidas economicas -Sancionales Legales	- Proceso de copia de seguridad diaria de la bases de datos de sistemas de información pricipales (SIHOS, Annar, Daruma) En redes: El diseño de la red de datos permite cambiar la forma la forma de como fluye la información por las diferentes redes en caso de daño algun dispositivo principal. - Los Swicth principales distribuidos por el hospital pueden ser configurados como de acceso, distribución ó núcleo en caso de daño se algún dispositivo, además se cuenta con 2 swicth básicos de 24 puertos ubicados en el área de sistema para soportar por un tiempo el daño de algún dispositivo de acceso, además se cuenta con un ruterboard de respaldo debido a criticidad de este tipo de hardware - Plan de contingencia en caso de caida del sistema de informacion principal - El servidor principal del HCI el cual contiene el sistema de información SIHOS trabaja con un motor de bases de datos que permite hacer la replicación de la misma en el caso del HCI se hace una réplica de esta base en una máquina virtual instalada en el mismo servidor de producción y también en otro servidor fisico lo cual garantiza que si ocurre algún daño en la maquina principal se pueda dar levantar las máquinas de respaldo en menos de 10 minutos para dar continuidad al negocio y no exista perdida de información, además la maquina principal tiene configurado un RAID 5 (también llamado distribuido con paridad) lo que limita la perdida datos. -Procesos de custodia de documentos de archivo de gestion, central e historico e Historia clinica fisica - Implementación de un servidor NAS en Raid 5 con 12 TB capacidad de almacenaje de la información principal de los usuarios del sistema de información del HCI. - 400 Licencias de antivirus NOD 32 System para los equipos de los usuarios finales además del administrador remoto que permite verificar el estado actual de los equipos y detectar Malware que ataca a los equipos de cómputo. - Cronograma de mantenimiento preventivo y correctivo de computadores y equipo de redes de datos - Firewall configurado	4	20	80

CATEGORIA	Nº	IDENTIFICACION DE RIESGOS	FECHA DE IDENTIFICACION DE RIESGO	ANALISIS DEL RIESGO			VALORACION INICIAL DEL RIESGO		
				CAUSAS	CONSECUENCIAS	BARRERAS DE SEGURIDAD EXISTENTES	VALOR DE PROBABILIDAD	VALOR DE IMPACTO	NIVEL DEL RIESGO
TEC	2	Vulnerabilidad, adulteración o uso indebido de la información	1/01/2017	- Desconocimiento de política de confidencialidad y seguridad de la información - Desconocimiento de política de Gerencia de la información - Falta de procesos y procedimientos que regule, controle y mejore el acceso a la información	-Perdidas economicas - Daños a pacientes o trabajadores, Perdidas economicas, Perjuicio de la imagen, Sanciones legales	Policitas se seguridad y confidencialidad de la información - Politica de gerencia de la información -Procedimiemientos de creación de usuarios en los sistemas de información --Procesos de custodia de documentos de archivo de gestion, central e historico e Historia clinica fisica	3	5	80

8. BIBLIOGRAFÍA

https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

http://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=62866

http://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83433

http://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=85742

http://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=85742

https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

https://www.mintic.gov.co/portal/604/articles-74903_documento.pdf

Articulado Plan Nacional de Desarrollo. Artículo 147. Transformación Digital Pública:

https://colaboracion.dnp.gov.co/CDT/Prensa/Ley1955-PlanNacionaldeDesarrollo-pacto-por-colombia-pacto-por-la-equidad.pdf

Manual de Gobierno Digital: http://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf

Articulado Plan Nacional de Desarrollo. Artículo 147. Transformación Digital Pública:

https://colaboracion.dnp.gov.co/CDT/Prensa/Ley1955-PlanNacionaldeDesarrollo-pacto-por-colombia-pacto-por-la-equidad.pdf

https://www.mintic.gov.co/portal/604/articles-74903_documento.pdf

https://www.mintic.gov.co/marcodereferencia/

http://www.funcionpublica.gov.co/web/mipg/furag