E.S.E SAN JUAN DE DIOS EL CARMEN DE VIBORAL

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DEL HOSPITAL SAN JUAN DE DIOS EL CARMEN DE VIBORAL

Actualización a enero 2023

CONTENIDO

INTRODUCCION

Según la norma técnica ISO 27001, la seguridad de la información se describe como la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan. Esto conlleva a que las empresas pensemos de manera organizada en mantener un sistema que permita organizar, gestionar, controlar y salvaguardar la información.

La E.S.E Hospital San Juan de Dios de El Carmen de Viboral, es una entidad descentralizada proveedora de gran cantidad de información tanto magnética como física, la cual se encuentra en continuo procesamiento para el reporte de diferentes informes tanto internos como externos, hecho que implica un riesgo a la negligente manipulación de la información o a la perdida de la misma, lo que podría traer problemas económicos, legales y/o administrativos por lo cual este documento busca establecer una línea de trabajo que permita a la entidad sortear los riesgos a la cual está expuesta y lograr que su información este segura, aspectos que hacen que se identifique, controle y proteja cada uno de los mecanismos a través de los cuales se accesa y manipula la información, pues el no contar con una buena gestión de la seguridad de la información, puede traer consecuencias graves, como pérdida fuga o robo de información, alteración de documentos, negación de servicios etc.

GLOSARIO

- Seguridad informática: Se ocupa de la implementación técnica y de la
- operación para la protección de la información.
- Seguridad de la información: Se Ocupa de evaluar el riesgo y las amenazas,
- traza el plan de acción y esquemas normativos. Es la línea estratégica de las
- Seguridad.
- Amenazas: Cualquier evento, persona, situación o fenómeno que pueda causar daño.
- Vulnerabilidades: Falla o debilidad en un sistema que puede ser explotada por quien la conozca.
- Riesgo: Probabilidad de ocurrencia de una amenaza.
- Controles: Conjunto de mecanismos que regulan el funcionamiento de un sistema.
- ISO: Organización Internacional de Normalización es una organización para la creación de estándares internacionales.
- Activo: Bienes, recursos o derechos que tenga valor para una organización.
- Activo de Información: Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.
- Análisis de brechas: es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.
- Análisis de Riesgo: Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.
- Gestión del Riesgo Informáticos: Actividades empleadas para mitigar los riesgos informáticos.
- Incidente de seguridad informática: daño que puede comprometer las operaciones de la alcaldía municipal.
- Evento: Acción que puedo haber causado daño, pero fue controlado.
- Información: Conjunto de datos que tienen un significado.
- Probabilidad: Posibilidad de que una amenaza se materialice
- Impacto: Daño que provoca la materialización de una amenaza.
- SGSI: Sistema de Gestión de seguridad de la Información
- MSPI: Modelo de seguridad y privacidad de la información
- PHVA: Planear, hacer, verificar, actuar
- Seguridad informática: Se ocupa de la implementación técnica y de la operación para la protección de la información.
- Seguridad de la información: Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.
- Amenazas: Cualquier evento, persona, situación o fenómeno que pueda causar daño.

- Vulnerabilidades: Falla o debilidad en un sistema que puede ser explotada por quien la conozca.
- Riesgo: Probabilidad de ocurrencia de una amenaza.
- Controles: Conjunto de mecanismos que regulan el funcionamiento de un sistema.
- ISO: Organización Internacional de Normalización es una organización para la creación de estándares internacionales.
- Activo: Bienes, recursos o derechos que tenga valor para una organización.
- Activo de Información: Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.
- Análisis de brechas: es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.
- Análisis de Riesgo: Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.
- Gestión del Riesgo Informáticos: Actividades empleadas para mitigar los riesgos informáticos.
- Incidente de seguridad informática: daño que puede comprometer las operaciones de la alcaldía municipal.
- Evento: Acción que puedo haber causado daño, pero fue controlado.
- Información: Conjunto de datos que tienen un significado.
- Probabilidad: Posibilidad de que una amenaza se materialice

OBJETIVOS

OBJETIVO GENERAL

Identificar y gestionar los Riesgos de Seguridad y Privacidad de la Información de la E.S.E Hospital San Juan de Dios de El Carmen de Viboral.

OBJETIVOS ESPECÍFICOS

- Identificar la ubicación y propietarios de los activos de información a través del inventario del mismo
- Categorizar y valorar los activos de información.
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.
- Diagnosticar la situación actual de la institución en materia de riesgos de
- seguridad y privacidad de la Información
- Plantear estrategias para el control, minimización y protección contra el
- riesgo de pérdida y/o privacidad de la información de la E.S.E Hospital San Juan de Dios de El Carmen de Viboral
- Mejorar el sistema de Seguridad y Privacidad de la Información con el fin de que las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad
- Proteger los activos informáticos mediante la implementación de acciones de mitigación frente al riesgo.

ALCANCE

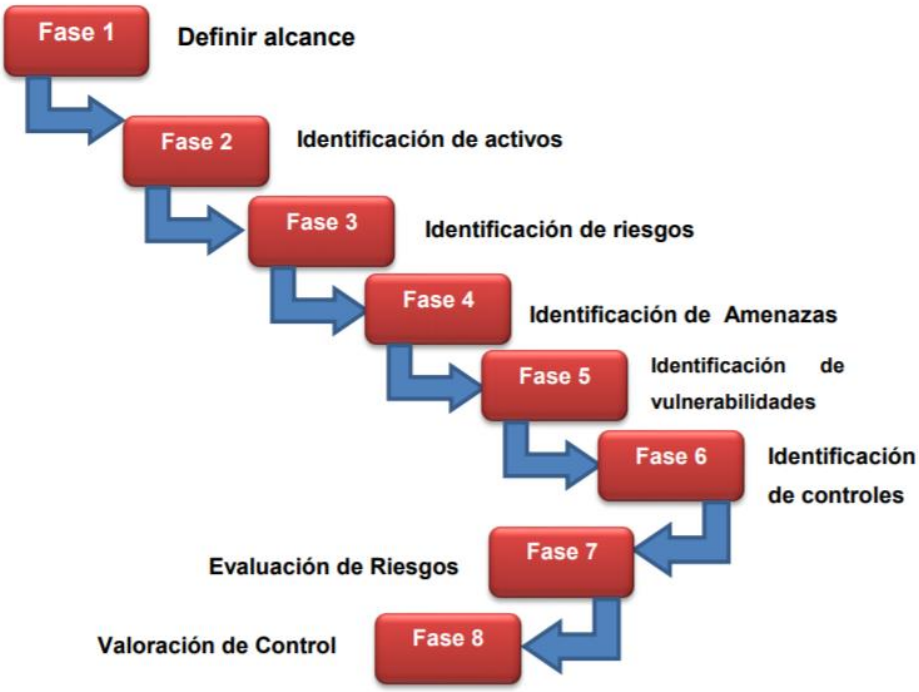
El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos del Hospital, los cuales manejen, procesen o interactúen con información física y magnética de la E.S.E.

NORMATIVIDAD

- Ley Estatutaria 1581 (17 de octubre de 2012): “Por la cual se dictan disposiciones generales para la protección de datos personales.”
- Ley 1266 (31 de diciembre de 2008): “Por la cual se dictan las disposiciones generales del hábeas 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.”
- Resolución 3564 de 2015 (31 de diciembre de 2015): Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
- Decreto 1078 (26 de mayo de 2015): “Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.”
- Ley 1712 (06 de marzo de 2014: Ley de Transparencia y acceso a la información pública nacional.
- Ley 57 (05 de julio de 1985): “Por la cual se ordena la publicidad de los actos y documentos oficiales.”
- Acuerdo 03 (17 de febrero de 2015) del Archivo General de la Nación; “por el cual se establecen lineamientos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la ley 1437 de 2011, se reglamenta el artículo 21 de la ley 594 de 2000 y el capítulo IV del decreto 2669 de 2011”
- Decreto 019 de 2012: "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública".
- Decreto 2364 (22 de noviembre de 2012): Firma electrónica.
- Ley 962 (08 de julio de 2005): “Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.”
- Decreto 1747 (11 de septiembre de 2000): “Por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales”
- Ley 527 (18 de agosto de 1999): Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y Se establecen las entidades de certificación y se dictan otras disposiciones.
- Decreto Ley 2150 de (05 de diciembre de 1995): “Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.”
- Decreto 1078 (26 de mayo de 2015): “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Ley 2052 de de 2020, "Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los

particulares que cumplan funciones públicas y/o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones"

ETAPAS O FASES DEL PLAN



ETAPA1:
Definir el alcance de aplicación del plan. En esta fase se establece los objetivos, justificación del procedimiento que se va a realizar, los funcionarios implicados y el contexto de seguridad informática con el que cuenta el Hospital

ETAPA2:
Inicialmente se hace una breve descripción de los activos informáticos con que cuenta la E.S.E Hospital San Juan de Dios de El Carmen de Viboral, con el fin de reconocer el tipo de información y su clasificación.

Teniendo en cuenta que el principal activo de una organización es la información en sí, la cual puede estar en forma física como documentos impresos o escritos a mano, en medios electrónicos almacenados en Discos Duros Externos, Memorias USB o en forma digital, en los equipos de cómputo o en la Nube. Toda esta información requiere ser analizada para su protección. (Un activo es todo aquello que genera valor para una empresa u organización.)

Se debe realizar un inventario de activos de información que contenga los siguientes campos:

- Nombre del líder del proceso / Nombre del funcionario
- Nombre del activo de información / Nombre correspondiente al activo de información como Base de Datos, Actas, informes, Sistemas de información etc.
- Descripción del activo de información

ETAPA3:
Identificar los riesgos que tienen cada uno de los activos informáticos

ETAPA4:
Para cada una de las amenazas se analiza las vulnerabilidades (debilidades) que se podrían presentar en el proceso.

ETAPA5:
Se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de la información.

ETAPA6:
Finalmente se describen acciones que se deben llevar a cabo para solventar las problemáticas presentadas.

ETAPA7:
Evaluar en qué estado se encuentran cada uno de los riesgos de la información

ETAPA8:
Evaluar cada uno de los controles establecidos, para determinar su efectividad.

CLASIFICACION DE LOS ACTIVOS

Los activos de información se clasifican en dos tipos:

1. Primarios:

- Procesos o subprocesos y actividades de la entidad: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización:
  - información del área de facturación.
  - Información de historias clínicas

- Información: información que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados; información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo:
  - Información del área de tesorería, presupuesto y contabilidad.
  - Información del área de contratación.
  - Información de talento humano.
  - Inventarios del área de farmacia.
  - Inventarios área de almacén.

- Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.
  - Información del área de tesorería.
  - Información del área de contratación.
  - Información de procesos jurídicos de la entidad.

2. De Soporte:

- Hardware: Consta de todos los elementos físicos que dan soporte a los procesos.
- Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos:

  - Software Institucional
  - Programas de apoyo
  - Programas externos

- Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)

  - Red line.
  - Red conmutada con los centros de salud.

- Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

  - Personal a cargo de elementos de cómputo de la institución.

ANALISIS DE RIESGOS

Para iniciar con el análisis de riesgos, primero se identifica los tipos de riesgo y su magnitud con la que pueden afectar a la seguridad y privacidad de la información, apoyados en la guía de administración de riesgos del DAFP.

Después de la identificación, se determinan las causas, las cuales son el fundamento, motivo, origen y principio de algo; con respecto al riesgo estas pueden ser generadas por personas, procesos, equipos, tiempo, entre otras que provocan un mal uso, una inadecuada acción o mal trabajo como origen de un hecho ya sea positivo o negativo.

Una vez se cuente con las causas, se identifican las consecuencias, las cuales son los efectos asociados a la materialización del riesgo, estos pueden ser de diferente índole de acuerdo a la acción realizada y al perjuicio que se presente después de lo acontecido.

Siguiente, se realiza el análisis del riesgo, para ello se utilizará una escala cuantitativa de valoración donde uno (1) es el valor más bajo y cinco (5) más alto, ello con el fin proyectar una comparación y priorización del riesgo de la información tanto en su seguridad como en la privacidad.

El análisis se realiza teniendo en cuenta las siguientes variables:

IMPACTO Y PRIVACIDAD:

IMPACTO: consecuencias que puede ocasionar a la organización la materialización del riesgo, se Clasifican en los siguientes:
IMPACTO O EVENTO MENOR: Sin impacto sobre el ususrio quien puede no notarlo, calificacion 1
IMPACTO O EVENTO MODERADO: Puede corregirse y el impacto sobre el usuario es minimo. Calificacion: 4
IMPACTO O EVENTO MAYOR: Incapacidad temporal o permanente menor con alto grado de inconformidad por parte del usuario. Calificacion: 7
IMPACTO O EVENTO CATASTROFICO: Puede causar la muerte o incapacidad permanente mayor al usuario. Calificacion: 10
PROBABILIDAD: Posibilidad de que ocurra el evento. Tipos:
PROBABILIDAD FRECUENTE: Puede ocurrir dentro de un breve periodo varias veces en un año. Calificacion=4.
PROBABILIDAD OCASIONAL: Puede ocurrir una a dos veces al año, calificacion=3
PROBABILIDAD RARO: Puede ocurrir una vez en 2 a 5 años. Calificacion= 2
PROBABILIDAD REMOTA: Puede ocurrir una vez de 5 a 30 años. Calificación 1
NIVEL DE RIESGO: Resultado de confrontar el impacto y la probabilidad con los controles existentes al interior de los diferentes procesos y procedimientos que se realizan

(Ver mapa de riesgos)

DISPONIBILIDAD DE LA INFORMACION:

Nivel	Descripción Criterio de Disponibilidad
0	Información cuya inaccesibilidad no afecta la operatoria de la Alcaldía.
1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para la Alcaldía o terceros.
2	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la Alcaldía o a terceros.
3	Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas a la Alcaldía o a terceros.

VULNERABILIDADES:

Las vulnerabilidades son las Fallas o debilidades en un sistema, que puede ser explotada por quien la conozca. Cuando la amenaza encuentra la vulnerabilidad es cuando se crea el riesgo. Por eso es necesario conocer la lista de amenazas y el inventario de activos de información

VULNERABILIDADES	DESCRIPCIÓN
Fácil acceso a las dependencias o Secretarías.	No existe un control para el acceso de las personas no autorizadas a las secretarías.
Falta de dispositivos de seguridad biométrica para acceso a las secretarias de alto riesgo.	El dispositivo de seguridad biométrica reduce el riesgo de robo de información o equipos electrónicos por fácil acceso.
Falta de Aplicación de la Política de escritorio Limpio.	La política de escritorio limpio, es implementada para que los funcionarios no dejen expuestos: documentos, equipos electrónicos u objetos de valor, sobre los escritorios, que pueden ser robados fácilmente.

Falta de Capacitación de los funcionarios en temas de seguridad Informática.	El eslabón más débil en términos de seguridad informática en una organización son los funcionarios, dado que no tienen conocimiento sobre las amenazas y riesgos que enfrentan y como poder mitigarlos.

Falta de equipos institucionales.	El no contar con suficientes equipos institucionales, lleva a los funcionarios a traer equipo personal que pueden afectar el funcionamiento de la red o infectarla. Adicionalmente promueve el compartir cuentas de usuarios y calves que pueden afectar al prestador
Equipo clon.	Los equipos clon, no cuentan con software legal que pueden infectar la red o traer problemas legales

TRATAMIENTO DEL RIESGO:

Evaluación del riesgo:

Permite una comparación entre los riesgos que se presenta en la institución con el fin de discernir cuan peligrosos pueden ser, de tal forma que se tomen medidas para mitigar sus consecuencias:

CONCEPTO	DESCRIPCION	DENOMINACIÓN
Zona de riesgo baja	Asumir el riesgo	B
Zona de riesgo moderada	Asumir el riesgo, reducir riesgo	M
Zona de riesgo alta	Reducir riesgo, evitar, compartir.	A
Zona de riesgo extrema	Reducir riesgo, evitar, compartir o transferir	E

Acciones:

Son las medidas que se pueden tomar una vez identificado el resultado de la acción, estas pueden servir para corrección, para mejora, tratamiento enmendadura de los efectos que dejo un riesgo.

Responsables:

Es la persona encargada y responsable de tomar medidas para dar solución a las circunstancias presentadas ya sea en mediano, corto o largo plazo, con el fin de remitir respuesta y dar solución a los eventos presentados.

Controles existentes:

La identificación de los controles existentes permite realizar la evaluación de riesgos. Los controles garantizan que al momento de la materialización de un riesgo se reduzcan o mitiguen los riesgos informáticos y la organización funcionen correctamente. Pero se debe tener en cuenta que nunca se va a estar 100% seguros.

Dada la importancia de los controles, con que cuenta El Hospital, no es adecuado exponerlos en el proyecto, por lo que se pueden crear perfiles de ataque.

VALORACIÓN DE CONTROL		
PARAMETROS	**CRITERIOS**	**PUNTAJE**
HERRAMIENTAS PARA EJERCER EL CONTROL	Posee una herramienta para ejercer el control.	15
	Existen manuales, Instructivos o procedimientos para el manejo de la herramienta.	15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.	30
SEGUIMIENTO AL CONTROL	Están definidos los responsables de la ejecución del control y del seguimiento.	15
	La frecuencia de ejecución del control y seguimiento es adecuada.	25
TOTAL		100

ANALISIS DE RESULTADOS

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, que nos permite discernir como la información generada por la E.S.E Hospital San Juan de Dios de El Carmen de Viboral, se encuentra expuesta a eventos adversos especialmente provocados por prácticas inadecuadas del personal de la entidad y falta de dotación de equipos idóneos para cumplirlas, hecho que ponen en riesgo el cumplimiento de la misión encaminada a satisfacer las necesidades y expectativas de sus clientes bajo los principios de responsabilidad, rentabilidad económica y social, por tanto es conveniente que las partes responsables, en este caso la gerente general encamine medidas para solventar la problemática presentada y disminuir la exposición al riesgo en al que la información se ve expuesta, con medidas correctivas, precautorias y de mejora.

PLAN DE ACCION 2023

ETAPA	ACTIVIDAD	MES
1	Definir el alcance	Enero a feb
2	Identificacion de activos	Febrero a marzo
3	Identificacion de riesgos	Abril a mayo
4	Identificacion de amenazas	Mayo a Junio
5	Identificacion de vulnerabilidades	Junio a Julio
6	Identificacion de controles	Julio a agosto
7	Evaluacion de riesgos	Agosto a sept
8	Evaluacion del control	Sept a nov

BIBLIOGRAFIA

- DAFP (Octubre de 2018). Guía para la administración del riesgo y diseño de controles en entidades públicas. Riesgo de gestión, corrupción y seguridad digital.

- DAFP (Septiembre de 2011). Guía para la administración del riesgo.

- MINITIC. Proyecto de ley para modernizar el sector TIC. Disponible en: https://www.mintic.gov.co