RESOLUCION No. 116.

(22 DE MARZO DE 2024)

POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA E.S.E. HOSPITAL CRISTIAN MORENO PALLARES DEL MUNICIPIO DE CURUMANI – CESAR, VIGENCIA 2024.

La Gerente de la E.S.E. Hospital Cristian MorenoPallares del Municipio de Curumani – Cesar, en uso de sus Facultades legales y Estatutarias, y

CONSIDERANDO:

1. Que la Constitución Política en su artículo 113 señala que los diferentes órganos del Estado tienen funciones separadas, pero colaboran armónicamente para la realización de sus funciones.

2. Que el numeral 8 del artículo 2 de la Ley 1341 de 2009 establece que el Gobierno Nacional fijará los mecanismos y condiciones para garantizar la masificación del Gobierno en Línea (ahora Política de Gobierno Digital), con el fin de lograr la prestación de servicios eficientes a los ciudadanos, así mismo, la citada Ley determino que es función del Estado intervenir en el sector de las Tecnologías de la información y la comunicación (TIC), con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo de dicho sector; así como reglamentar las condiciones en que se garantizará el acceso a la información en línea, de manera abierta, ininterrumpida y actualizada.

3. Que la Ley 1712 de 2014, "por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones", señala que sus sujetos obligados deberán observar lo establecido

por la estrategia de Gobierno en Línea - (ahora Política de Gobierno Digital) en cuanto a la publicación y divulgación de información pública.

4. Que el Decreto 1078 de 2015, Por el cual se expide el Decreto Único Reglamentario del sector Tecnologías de información y las comunicaciones acoge el Decreto 1008 de 2018 subrogando lo indicado en el capítulo 1 del título 9 de la parte 2 del libro 2.

5. Que el Decreto 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado, entre ellos el Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Plan de Seguridad y Privacidad de la Información.

6. Que el Decreto 1008 de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

7. Que el Artículo 2.2.9.1.2.2.del Decreto 1008 de 2018 establece que, para la implementación de la Política de Gobierno Digital, las entidades públicas deberán

Aplicar el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de esta Política de Gobierno Digital, el cual será elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en coordinación con el Departamento Nacional de plantación En mérito de lo antes expuesto, La Gerente de la E.S.E. Hospital Cristian MorenoPallares del Municipio de Curumani – Cesar

RESUELVE:

ARTÍCULO PRIMERO: Adóptese el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la de E.S.E. Hospital Cristian MorenoPallares, vigencia año 2024.

ARTÍCULO SEGUNDO. ALCANCE DE IMPLEMENTACIÓN: El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E se dicta en cumplimiento de las disposiciones legales vigentes y basada en la norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información de la entidad, con el ánimo de gestionar adecuadamente la seguridad de la información en los procesos, en los activos, en sistemas informáticos y lógicos, partes interesada, la infraestructura de red de la organización, instalaciones físicas y el entorno.

Esta política aplica a los procesos y procedimientos de la entidad y está dirigido a todos los usuarios internos, externos, servidores, funcionarios en todas las vinculaciones.

ARTÍCULO TERCERO: Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la de E.S.E. Hospital Cristian MorenoPallares, será actualizado teniendo en cuenta lo establecido en las exigencias normativas y/o cambio en la situación de seguridad y privacidad de la información para la entidad.

ARTÍCULO CUARTO: Articular el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E. con el Plan de Acción de la Entidad.

ARTICULO QUINTO: Ordenar la publicación del presente acto en la página web de la E.S.E. Hospital Cristian MorenoPallares del Municipio de Curumani – Cesar.

ARTICULO SEXTO: La presente resolución rige a partir de la fecha de su Expedición.

COMUNÍQUESE Y CÚMPLASE

Dado en Curumani - Cesar, a los Veintidós (22) días del mes de marzo de 2024

OMAIRA CHAVEZ GUTIERREZ
Gerente

INTRODUCCIÓN

El presente documento aborda el Plan de Tratamiento de Riesgos de Seguridad de la Información diseñado específicamente para la E.S.E. Hospital Cristian Moreno Pallares del Municipio de Curumani – Cesar.

Este plan se fundamenta en la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" emitida por el Departamento Administrativo de la Función Pública.

La gestión de riesgos se concibe como la respuesta primordial para mitigar diversos riesgos, siendo ejecutada por la primera línea de defensa. En este contexto, el enfoque principal de la planificación se centra en el tratamiento de riesgos asociados con la Seguridad y Privacidad de la Información, específicamente en la salvaguarda de los activos informativos bajo la responsabilidad de la Administración de la E.S.E.

La imperante necesidad de adoptar estrategias de seguridad digital se manifiesta en la integración de principios, políticas, procedimientos, guías, manuales, formatos y lineamientos destinados a la gestión efectiva de la seguridad de la información digital. Este enfoque refleja el compromiso de la alta gerencia con la protección y privacidad de la información en su custodia.

OBJETIVO

El objetivo principal de este plan es determinar las acciones específicas para el tratamiento de riesgos relacionados con la seguridad y privacidad de la información en la E.S.E. Esto se logrará a través de la identificación, análisis, valoración y tratamiento de los riesgos asociados con la pérdida de confidencialidad, disponibilidad e integridad de la información. El propósito es prevenir la materialización de estos riesgos y/o reducir los impactos negativos que podrían afectar la gestión institucional.

OBJETIVOS ESPECÍFICOS

1. Preparar a los Colaboradores: Implementar medidas y programas de formación para capacitar a todos los colaboradores, con el fin de que estén preparados para responder de manera efectiva ante incidentes de seguridad que puedan afectar los activos de información de la E.S.E.
2. Mejorar la Confianza Institucional: Implementar acciones destinadas a mejorar la confianza de los diferentes grupos de interés en la capacidad institucional de la E.S.E, para preservar la seguridad de la información.
3. Esto incluirá comunicaciones efectivas, demostración de medidas de seguridad y transparencia en la gestión de la información.

ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad de la Información abarca todos los procesos que se llevan a cabo en la alta gerencia de la E.S.E, incluyendo aquellos relacionados con las áreas Estratégicas, Misionales, de Apoyo y de Evaluación y Seguimiento.

La adopción de este plan, para la vigencia 2024, se centra en dos aspectos principales:

1. Fortalecimiento de la Seguridad: Implementar medidas y controles destinados a fortalecer la seguridad de la información en todos los procesos y áreas de la E.S.E.
2. Generación de Confianza Digital: Desarrollar estrategias que contribuyan a generar confianza digital. Esto implica anticiparse adecuadamente a posibles riesgos, gestionar de manera eficiente los riesgos existentes, brindar una atención oportuna a incidentes y defenderse ante las amenazas presentes

en el entorno digital. Todo ello se llevará a cabo dentro de un marco de gobernanza eficiente, adaptado a las necesidades actuales y en constante evolución, para responder rápidamente a la seguridad digital ante la aparición de nuevas tecnologías.

MARCO NORMATIVO

Constitución Política de Colombia 1991: Enfatiza el derecho de todas las personas a la intimidad personal y familiar, así como al buen nombre. Establece que el Estado debe respetar estos derechos y asegurar su protección. Asimismo, reconoce el derecho de las personas a conocer, actualizar y rectificar la información recogida sobre ellas en bancos de datos y archivos de entidades públicas y privadas.

Ley 1712 de 2014: Crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional. Esta ley busca garantizar el acceso a la información por parte de los ciudadanos y establece disposiciones para promover la transparencia en las entidades públicas.

Decreto 1494 de 2015: Reglamenta parcialmente la Ley 1712 de 2014 y establece disposiciones adicionales para su implementación. Este decreto proporciona directrices sobre cómo las entidades deben gestionar y hacer accesible la información pública.

Decreto 612 de 4 de abril de 2018: Fija directrices para la integración de los planes relacionados con la implementación de la Ley 1712 de 2014. Establece criterios y procedimientos para asegurar la transparencia y el acceso a la información pública.

Decreto 1008 de 14 de junio de 2018: Establece los lineamientos generales de la política de Gobierno Digital. Define las pautas para la implementación de estrategias

digitales en el ámbito gubernamental, lo cual puede tener implicaciones directas en la gestión de la información y la seguridad digital.

Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

ANÁLISIS DE RIESGOS

El análisis del riesgo informático tiene como objetivo determinar la probabilidad de ocurrencia y las consecuencias de un riesgo, permitiendo su evaluación y clasificación. Se consideran dos aspectos principales: probabilidad e impacto.

1. **Probabilidad:**
    - *Definición:* Es la posibilidad de ocurrencia del riesgo.
    - *Medición:* Puede medirse con criterios de frecuencia si el riesgo se ha materializado o de factibilidad, considerando factores internos y externos que podrían propiciar su ocurrencia.

2. **Impacto:**
    - *Definición:* Las consecuencias que puede ocasionar la materialización del riesgo en la entidad.
    - *Medición:* Se mide por la magnitud de las consecuencias en distintas áreas, como estratégica, operativa, financiera, cumplimiento, tecnología e imagen.

Pasos para el análisis de riesgos:

1. **Identificación de riesgos:** Reconocer los posibles riesgos informáticos que podrían afectar a la entidad.
2. **Calificación del riesgo:**
    - *Clasificación del riesgo:* Se realiza según la categoría del riesgo (estratégico, operativo, financiero, cumplimiento, tecnología, imagen).
    - *Magnitud del impacto:* Determinar el nivel en el que se encuentra el riesgo.
3. **Evaluación del riesgo:**
    - *Comparación:* Comparar los resultados de la calificación con criterios definidos para establecer el grado de exposición al riesgo.
    - *Ubicación en la matriz de evaluación:* Definir la zona de ubicación del riesgo inherente (antes de la definición de controles).
4. **Evaluación del riesgo inherente:**
    - *Cálculo:* Utilizar variables cuantitativas y cualitativas para calcular la evaluación del riesgo antes de la implementación de controles.

Este análisis proporciona una visión integral de los riesgos informáticos, permitiendo una toma de decisiones informada en la formulación de estrategias de control y mitigación.

VALORACIÓN DE LOS RIESGOS:

La valoración de riesgos es el resultado de confrontar la evaluación del riesgo con los controles (preventivos o correctivos) implementados en los procesos. Este proceso se lleva a cabo en tres etapas:

1. **Identificación de Controles:**
    - Se identifican los controles (preventivos o correctivos) que pueden reducir la probabilidad de ocurrencia o mitigar el impacto del riesgo.
2. **Evaluación de Controles:**
    - Se evalúan los controles identificados para determinar su eficacia en la gestión del riesgo.
3. **Determinación del Riesgo Residual:**
    - Con base en los resultados de la evaluación de controles, se determina la evaluación del riesgo residual, es decir, el riesgo que persiste después de aplicar los controles.
4. **Opción de Manejo del Riesgo:**
    - Se define la opción de manejo del riesgo considerando la evaluación del riesgo residual. Las opciones pueden incluir transferir, mitigar, evitar o aceptar el riesgo.

TRATAMIENTO DE RIESGOS:

El tratamiento de riesgos tiene como objetivo minimizar la probabilidad de materialización del riesgo. Las opciones de tratamiento son las siguientes:

1. **Transferir:**

    - Procedimientos que eliminan el riesgo mediante la transferencia de responsabilidad a terceros.

2. **Mitigar:**

    - Reducción de la probabilidad de ocurrencia del riesgo o disminución de sus consecuencias mediante controles de gestión, políticas y procedimientos.

3. **Evitar:**

    - Prevención del riesgo no llevando a cabo la actividad que lo implicaría o eligiendo medios alternativos que logren el mismo resultado sin incorporar el riesgo.

4. **Aceptar:**

    - Afrontar el riesgo, ya sea porque no se ha identificado otra estrategia adecuada o porque se trata de un riesgo que la entidad está dispuesta a asumir.

SEGUIMIENTO DE RIESGOS:

La Oficina de Control Interno llevará a cabo el seguimiento del componente de administración de riesgos, verificando aspectos como:

- Cumplimiento de políticas y directrices para la administración del riesgo.
- Funcionamiento de la metodología de Administración del Riesgo.
- Administración de riesgos por proceso e institucionales, incluyendo calificación y evaluación, efectividad de los controles y cumplimiento de acciones.

Los responsables de procesos y sus equipos deben garantizar que la información de los riesgos sea adecuada, coherente, pertinente y actualizada. Cualquier ajuste necesario debe notificarse al oficial de seguridad.

ACTIVIDAD

- Implementación de Controles de Seguridad Informática.
- Análisis, calificación, evaluación, tratamiento a los riesgos de seguridad de información de la E.S.E.
- Generar Indicadores De Gestión.
- Hacer Plan de Revisión y seguimiento.