# FONDO PARA LA CONSOLIDACION DEL PASIVO PENSIONAL CARTAGO

# 2022

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

IMPLEMENTACIÓN ESTRATEGIA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

## 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 del Hospital.

• **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.

## INTRODUCCION

Para toda entidad es de gran importancia contar con un plan de gestión de riesgos con el fin de garantizar la continuidad de la misma. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado FCPACP. El tratamiento de los riesgos de seguridad de la información se basa en procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Para la realización de este plan e FCPACP diagnóstico su situación actual, realizando la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

La realización de este plan del FCPACP permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

La norma ISO 27005:2011 es un estándar internacional diseñado para la gestión del riesgo en la seguridad de la información dentro de un sistema de gestión de seguridad de la información.

Contiene diferentes procedimientos y directrices, que permiten establecer los riesgos que enfrenta una organización y poder mitigarlos de la mejor manera.

Se realiza la identificación, el análisis, la evaluación de los riesgos, las políticas y controles que permiten reaccionar ante una posible materialización del riesgo mediante el plan de tratamiento de riesgos.

El no contar con una buena gestión de la seguridad de la información, para el FCPACP puede traer consecuencias graves, como pérdida fuga o robo de información, alteración de documentos, negación de servicios etc.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad de la entidad tras sufrir alguna pérdida o daño en la información de la misma.

## 1. OBJETIVOS

### 1.1 OBJETIVO GENERAL

• Mitigar los riesgos informáticos del FCPACP, mediante la aplicación de la norma ISO 27005.

### 1.2 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.

• Proyectar el mapa de riesgos informáticos del FCPACP Valle donde se establece el contexto.

## 2. MARCO TEORICO

**2.1 SEGURIDAD INFORMÁTICA** La seguridad Informática y la seguridad de la información son métodos y técnicas físicas y documentales empleadas para mantener siempre la confidencialidad, integridad y disponibilidad de la información.

**2.1 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/IEC27000).

**2.2. 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/IEC27000).

**2.3 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).

**2.4 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/IEC27000).

**2.5 SEGURIDAD DE LA INFORMACIÓN** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

**2.6 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI** Conjunto de elementos interrelacionados 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/IEC27000).

**2.7 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/IEC27000).

**2.8 VULNERABILIDAD** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

## 3 MARCO NORMATIVO

**NORMA ISO 27001** La norma ISO 27001 es un estándar internacional que describe

cómo implementar el Sistema de gestión de seguridad de la información de una empresa. Investiga como salvaguardar la información mediante una serie de estándares, lineamientos y procesos que facilitan la identificación de los riesgos.

**NORMA ISO 27005** La norma ISO 27005 es un soporte a la norma (ISO 27001) la cual proporciona directrices para la gestión de riesgos de seguridad de la información, es aplicable a todos los tipos de organización y no proporciona ni recomienda una metodología específica.

**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

**LEY 1712 DE 2014** - Ley de Transparencia y acceso a la información pública

**LEY 57 DE 1985** -Publicidad de los actos y documentos oficiales

**LEY 594 DE 2000** - Ley General de Archivos

**TÍTULO 9 - DECRETO 1078 DE 2015** - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

**TÍTULO 9 - DECRETO 1078 DE 2015** - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

**LEY ESTATUTARIA 1757 DE 2015** - Promoción y protección del derecho a la participación democrática

**TÍTULO 9 - DECRETO 1078 DE 2015** - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

**LEY ESTATUTARIA 1618 DE 2013** Ejercicio pleno de las personas con discapacidad

**TÍTULO 9 - DECRETO 1078 DE 2015** - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

**LEY 1437 DE 2011** - Código de Procedimiento Administrativo y de lo Contencioso Administrativo

**ACUERDO 03 DE 2015** del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

**TÍTULO 9 - DECRETO 1078 DE 2015** - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

**DECRETO 019 DE 2012** - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública

**DECRETO 2364 DE 2012** - Firma electrónica

**LEY 962 DE 2005** - Racionalización de trámites y procedimientos administrativos procedimientos administrativos

**DECRETO LEY 2150 DE 1995** - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública

**TÍTULO 9 - DECRETO 1078 DE 2015** - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

**LEY ESTATUTARIA 1581 DE 2012** - Protección de datos personales

**LEY 1266 DE 2008** - Disposiciones generales de habeas data y se regula el manejo de la información

## 4. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO DEL PROYECTO.

### 4.1 DEFINIR EL ALCLANCE

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 FCPACP

### 4.2 LIMITACIONES

Crear el rubro del presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en el FCPACP

### 4.3 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACION

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 diseñó un formato de inventario de activos de información que contiene los siguientes campos:

### 4.4 IDENTIFICACIÓN DEL RIESGO.

**RIESGO ESTRATÉGICO:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia. **RIESGOS DE IMAGEN:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

**RIESGOS OPERATIVOS:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias. **RIESGOS FINANCIEROS:** Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes. **RIESGOS DE CUMPLIMIENTO:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso

ante la comunidad, de acuerdo con su misión.
**RIESGOS DE TECNOLOGÍA:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión

**RIESGOS OPERATIVOS:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.
**RIESGOS FINANCIEROS:** Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
**RIESGOS DE CUMPLIMIENTO:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.
**RIESGOS DE TECNOLOGÍA:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

### 4.5 SITUACION NO DESEADA

Hurto de información o de equipos informáticos.

Hurto de información durante el cumplimiento de las funciones laborales, por intromisión Incendio en las instalaciones de la empresa por desastre natural o de manera intencional. Alteración de claves y de información.

Pérdida de información.

Daño de equipos y de información

Atrasos en la entrega de información

Atrasos en asistencia técnica

Fuga de información

Manipulación indebida de información

### 4.6 VULNERABILIDADES

**1.** Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos con switches pequeños según se va presentando la necesidad generando cascadas lo cual afecta la transmisión de los datos.

**2.** No existe una estructura o protocolo fijo y establecido para la infraestructura física del Fondo para la consolidación del pasivo pensional

**3.** Algunos cables de datos están sueltos o no están cerca a los escritorios, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcance a ser guardada.

**4.** En la entidad se presenta incumplimiento del cuidado tanto de los equipos informáticos y como de la información física y digital, algunos de estos son:

Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.

En algunos papeles reutilizables se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.

En algunas oficinas del FCPACP no existen los equipos de cómputo suficientes para el uso de la totalidad de su personal. Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.

La información es llevada en memorias o discos duros portátiles personales, por ende la información sale de la entidad.

No hay control para el uso de memorias portátiles en los equipos del hospital, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.

No existe un área de sistemas con personal encargado de revisar, documentar, diseñar y controlar los procesos propios de un modelo de seguridad de la información para el hospital.

Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a perdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.