1. Introducción

La gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica, le permite al FONVALMED realizar la identificación, análisis y tratamiento a los riesgos que pueden comprometer el cumplimiento de los objetivos en cumplimiento de su objeto misional, contribuyendo en la toma de decisiones con el fin de prevenir la materialización de estos.

La gestión de riesgos de seguridad y privacidad de la información son los procesos por medio de los cuales se busca eliminar las pérdidas de información, facilitando el conocer las fortalezas y debilidades a los que está expuesto el servicio durante todo su ciclo de vida.

De acuerdo con lo mencionado, hemos tomado como referencia la normativa establecida por el estado colombiano, CONPES 3854 de 2016 y 3995 de 2020 Modelo de Seguridad y Privacidad de MinTic y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos establecidos en los estándares ISO 27001:2013 y la Política de administración del riesgo de la Entidad.

2. Objetivo del Plan

Definir y aplicar los lineamientos para tratar de manera los riesgos de Seguridad y Privacidad de la Información.

3. Alcance

El alcance inicia con la identificación de los riesgos relacionados con la seguridad de la información hasta su posterior control.

4. Definiciones

- **Confidencialidad:** es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.

- **Integridad:** es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.

- **Disponibilidad:** es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.

- **Seguridad** de la Información: consiste en asegurar que los recursos del Sistema de Información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.

- **Activos de información** son los elementos que la Seguridad de la Información debe proteger. Por lo que son tres elementos lo que forman los activos:
    - **Información:** es el objeto de mayor valor para la empresa.
    - **Equipos**: suelen ser software, hardware y la propia organización.
    - **Usuarios:** son las personas que usan la tecnología de la organización.

- **Administración/gestión del riesgo:** actividades coordinadas para dirigir y controlar la organización con relación al riesgo.
- **Evento:** ocurrencia o cambio de un conjunto particular de circunstancias.
- **Control:** medida que mantiene y/o modifica un riesgo.
- **Consecuencia/impacto:** resultado de un evento que afecta a los objetivos.
- **Fuente de riesgo:** elemento que, por si solo o en combinación con otros, tiene el potencial de generar riesgo.
- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

- **Matriz de riesgos:** documento con la información resultante de la gestión del riesgo.

5. Marco legal.

- **Decreto 1499 de 2017** “Por medio del cual se establece el MIPG”.

- **Decreto 103 de 2015** “Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”

- **Ley 1712 de 2014** “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.

- **Decreto 1377 de 2013** “Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.

- **ISO 27001 de 2013**. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la Información (SGSI). Requisitos.

- **ISO/IEC 27002:2013**. Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

- **Ley 1581 de 2012** “Por la cual se dictan disposiciones generales para la protección de datos personales.”

- **LEY 1273 de 2009**. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **Resolución 2021-76** Por medio de la cual se adopta la Política de Protección de Datos Personales del ciudadano en el Fondo de Valorización del Municipio de Medellín- FONVALMED.

- Guía vigente de administración del riesgo establecida por la Función Pública año 2021.

6. Gestionar los riesgos

La gestión de riesgo es una actividad que está inmersa en las actividades del modelo de operación por procesos de la Entidad y hacen parte de las responsabilidades de la alta dirección y de las 3 líneas de defensa que establece el MECI.

Para el desarrollo del plan de tratamiento de riesgos, FONVALMED se adhiere a los lineamientos que establece la norma para poder identificar, analizar, tratar, valorar, evaluar y monitorear los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y todos aquellos relacionados en la materia.

6.1. Establecimiento del contexto

Se deben analizar los factores internos (tanto de la entidad como del proceso) y externos que afecten o puedan afectar su operación, dentro de los cuales pueden estar los siguientes:

Factores externos: se podrán considerar factores relacionados con el entorno político, económico, social, cultural, tecnológico, legal, ambiental, entre otros.

Factores internos: dentro de este grupo se podrán considerar variables relacionadas con: disponibilidad de personal, asignación presupuestal, competencias del personal, seguridad y salud en el trabajo, articulación de procesos, estructura organizacional, cultura organizacional, gestión del conocimiento, disponibilidad de datos y sistemas de información, direccionamiento estratégico, aspectos tecnológicos, entre otros.

Se pueden analizar variables tales como: diseño del proceso, articulación, procedimientos asociados, liderazgo al interior, activos de TI del proceso, etc.

Dentro del análisis del contexto interno y de proceso se deberán identificar: las aplicaciones, servicios web, redes, información física o digital, tecnologías de la

información, que se utilizan en el Instituto con las cuales tenga interacción el proceso o aquellas que sean propias del mismo.

6.2. Identificación del Riesgo:

El líder de TI y su equipo realizan la identificación de los riesgos que pueden afectar el cumplimiento del objetivo del proceso, mediante lluvia de ideas, teniendo en cuenta el análisis de contexto realizado previamente.

Debe clasificar el riesgo, teniendo como base las tipologías de riesgo establecidas en Política de Administración del Riesgo de FONVALMED, escogiendo la que se considere se ajusta a la naturaleza del evento que se está analizando. Dentro de las tipologías se tienen:

- Estratégicos: Son los riesgos asociados a la Administración de FONVALMED, se enfoca a asuntos globales relacionados con la Misión y el cumplimiento de los Objetivos Estratégicos, la definición de Políticas, diseño y conceptualización de la entidad por parte de la Dirección.

- De imagen: Relacionado con la percepción y la confianza por parte de nuestros grupos de valor, partes interesadas y comunidad en general, hacia FONVALMED.

- Operativos: Riesgo asociado a la estructuración y ejecución de los proyectos.

- Financieros: Relacionado con el manejo de recursos que incluyen la Ejecución Presupuestal, la elaboración de los Estados Financieros, modelo financiero, los Pagos, y el Manejo sobre los Bienes.

- Cumplimiento y conformidad: Se asocian con la capacidad de FONVALMED para Cumplir con los Requisitos Legales, contractuales, de la política de integridad y transparencia y en general con su compromiso ante la comunidad.

- Tecnológicos: Están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la Misión.

• De información: Se asocia a la calidad, seguridad, oportunidad, pertinencia y confiabilidad de la Información.

• Administrativos: Riesgo asociado a la gestión de los procesos dentro del MOP.

Una vez clasificado el riesgo, se define su descripción, principales causas, los agentes generadores y sus efectos, teniendo en cuenta las siguientes descripciones:

Descripción del riesgo: Es la definición específica de cómo se manifiesta el riesgo, acordado por el respectivo Equipo de Trabajo.

Causa: Son factores generadores del riesgo (debilidades y amenazas). Son los por qué de la ocurrencia del evento riesgoso.

Efecto: Son las consecuencias o el impacto que se genera con la ocurrencia del riesgo.

6.3 Calificación preliminar de los Riesgos

En esta etapa El líder de TI determina la probabilidad y el impacto de los riesgos identificados sin tener en cuenta el efecto de los controles que se estén implementando o se puedan implementar para su tratamiento.

La calificación de la probabilidad e impacto se realiza de acuerdo con las siguientes escalas:

Frecuencia-Probabilidad

Improbable 1
Posible 2
Frecuente 3

Impacto

Menor 1
Moderado 2
Catastrófico 3

6.4. Valoración del riesgo después del control:

El líder de TI analiza y describe los controles existentes relacionados directamente con el riesgo identificado y sus principales causas y los documenta en la columna “acciones para el control” del formato Mapa de Riesgos. Los controles pueden estar definidos en los procedimientos, en la normatividad legal aplicable, o políticas o directrices administrativas, entre otros.

En esta etapa se determina nuevamente la probabilidad y el impacto de los riesgos identificados teniendo en cuenta el efecto de los controles que se estén implementando para mitigar la materialización del riesgo.

Esta valoración determina la calificación del riesgo en una escala de bajo, medio o alto.

6.5 Realizar el tratamiento de los riesgos

Para dar el tratamiento a los riesgos, de acuerdo con la valoración obtenida, el Líder de TI y su equipo de trabajo determina los controles propuestos, considerando lo establecido en la “Matriz de Calificación, evaluación y Respuesta a los Riesgos” y teniendo en cuenta la viabilidad técnica y financiera.

La prioridad para la toma de las acciones depende de la zona de riesgo donde se ubica, considerando lo siguiente:

Zona Roja: Requiere atención inmediata

Zona Amarilla (Zona Moderada): Requiere acciones de control y monitoreo permanente.

Zona Verde: Seguir aplicando los controles existentes y hacer monitoreo periódico.

Teniendo en cuenta la criticidad del riesgo se deja registro en el formato PE-F04 “Acción Correctiva y Preventiva” en el caso de requerir establecer acciones asociadas a los controles propuestos.

6.6 Ejecutar el monitoreo y seguimiento:

El monitoreo a los riesgos se debe realizar de manera permanente y está a cargo del líder de cada proceso quien debe consolidar un seguimiento a la matriz de riesgos y ser enviado a al Líder de Planeación.

Planeación como segunda línea de defensa, consolidará un informe sobre la administración del riesgo a nivel global, utilizando como insumo la información suministrada por cada proceso la resultante de las actividades de acompañamiento desarrolladas. Dicho informe será presentado al Comité Institucional Coordinador de Control Interno.

Para efectos del seguimiento a los riesgos clasificados como de corrupción, se consolidará una matriz propia para la temática, la cual resultará del trabajo de identificación de riesgos a nivel de proceso. También será objeto de auditoría por parte de la Oficina de Control Interno con corte a las siguientes fechas: 30 de abril, 31 de agosto y 31 de diciembre de cada año, tal como lo establece la norma.

7. Anexo

- Matriz de riesgos Proceso de TI

Adoptado por el Comité de Institucional de Gestión y Desempeño
Medellín, 29 de enero de 2024