CAJA DE PREVISION SOCIAL MUNICIPAL DE BUCARAMANGA

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

VIGENCIA 2024

TABLA DE CONTENIDO

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se apoya en la cultura de prevención de la entidad, de esta manera se pueden evidenciar los riesgos, su impacto y las acciones a tomar para reducir el impacto en la entidad.

El presente plan tiene su sustento en el CONPES 3854 de 2016, 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 de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

1. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información permite fortalecer la seguridad de la información de la Caja de Previsión Social Municipal de Bucaramanga.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

- Fortalecer el Sistema de Gestión de Seguridad de la Información de la CPSMB, mediante la identificación de los riesgos y la implementación de herramientas que permitan gestionarlos de forma eficiente

2.2. OBJETIVOS ESPECÍFICOS

• Identificar los principales activos de información de la CPSMB.

• Crear un registro de los principales eventos donde se vea comprometida la seguridad de la información de la CPSMB.

• Identificar las amenazas que puedan comprometer la seguridad de la información en la CPSMB mediante el uso del modelo de privacidad y seguridad de la información propuesto por el MINTIC y la norma ISO27001.

• Avanzar en la implementación de las fases del Modelo de Privacidad y Seguridad de la Información MSPI.

• Implementar soluciones que permitan mitigar los posibles riesgos encontrados

3. METODOLOGIA PARA LA EVALUACIÓN Y TRATAMIENTO DEL RIESGO BASADA EN LA NORMA ISO 27001 y MPSI - IMPLEMENTACIÓN EN SEIS PASOS

La Evaluación del Riesgo (a menudo llamado Análisis de Riesgo) es probablemente la parte más compleja de la implementación ISO 27001; pero a la vez la evaluación (y tratamiento) del riesgo es el paso más importante al comienzo de su proyecto de seguridad de la información – establece las bases para la seguridad de la información en su compañía. La pregunta es – ¿por qué es tan importante? La respuesta es algo simple pero no entendida por muchas personas: la filosofía principal de ISO 27001 es encontrar cuáles incidentes pueden ocurrir (p.e. evaluando los riesgos) y encontrar las maneras más apropiadas para evitar dichos incidentes (p.e. tratamiento de los riesgos). No sólo eso, también tiene que evaluar la importancia de cada riesgo para que pueda enfocarse en los más importantes.

Paso 1. Establecer un marco de gestión de riesgos

Se trata de definir las reglas que regirán la gestión de riesgos. Se determina, entre otras cuestiones, quiénes serán los responsables de las tareas de gestión, los métodos de estimación del impacto y la probabilidad de ocurrencia de los posibles riesgos. En este sentido, una metodología de evaluación de riesgos debe abordar cuatro temas: • Cómo serán los criterios de seguridad. • Qué escala de riesgo se empleará. • Cuál es el apetito de riesgo de la organización. • La evaluación de riesgos basada en activos.

Paso 2. Identificar los riesgos

La identificación de los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información, es la tarea más larga del proceso de evaluación y tratamiento de riesgos en ISO 27001. Se recomienda optar por un proceso de evaluación de riesgos basado en activos. Desarrollar una lista de activos de información es un buen punto de partida. Será más fácil comenzar la labor a partir de una lista existente de copias impresas de información, archivos electrónicos, dispositivos móviles e intangibles, etc.

Paso 3. Analizar los riesgos

En primer lugar, se han de establecer las amenazas y debilidades de cada activo. Por ejemplo, la amenaza puede ser “el robo de un dispositivo móvil” y la debilidad asociada es que “no existe una política establecida con respecto al uso tales dispositivos”. Lo siguiente es asignar un impacto y un valor de probabilidad de acuerdo con los criterios que se hayan establecido en el paso 1.

Paso 4. Evaluar los riesgos Un siguiente paso es la evaluación.

En ella, se deberá medir cada uno de los riesgos frente a sus niveles predeterminados de aceptabilidad. Tras eso, se determinará qué riesgos serán abordados y se priorizará en qué orden.

Paso 5. Seleccionar opciones de tratamiento de riesgo

En este punto, retomamos las cuatro opciones de la gestión de riesgos clásica, utilizada en gestión de la calidad, de la seguridad y salud en el trabajo o del medio ambiente: • Evitar el riesgo eliminándolo por completo. • Modificar el riesgo, poniendo en marcha controles de seguridad. • Compartir el riesgo o trasladarlo a un tercero. • Retener el riesgo, solo si se trata de un nivel aceptable.

Paso 6. Compilar informes de riesgos

La norma ISO 27001 requiere que la organización establezca un conjunto de informes sobre la evaluación de riesgos con fines de auditoría y certificación. Para cumplir con ese punto, dos informes resultan imprescindibles:

- Declaración de aplicabilidad: su propósito es crear una lista de verificación según lo recomendado por el Anexo A de ISO 27001. Además, con ella se pretende obtener documentación sobre si se ha establecido el control, si ha sido implementado o no y una justificación para su inclusión o exclusión.

- Plan de tratamiento de riesgos: describe cómo la organización planea gestionar los riesgos identificados en la evaluación de riesgos. *Metodología de seis pasos tomada del artículo publicado por la escuelaeuropeaexcelencia.com en https://www.escuelaeuropeaexcelencia.com/2019/06/6-pasos-basicos-en-la-evaluacion-y-tratamiento-deriesgos-en-iso-27001/ y del sitio https://advisera.com/27001academy/es/knowledgebase/evaluacion-ytratamiento-del-riesgo-en-iso-27001-6-pasos-basicos/

Elaboró: JOSE DAVID VELÁSQUEZ MAYORGA - Profesional Universitario – Ingeniero de Sistemas –

Revisó: Alejandra Hoyos Carvajal - Subdirectora Administrativa - CPSM.