INFORME DE SEGUIMIENTO A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

OFICINA PRODUCTORA	SUBDIRECTORA ADMINISTRATIVA
FECHA	MARZO 25 DE 2025
PROCESO	SEGUIMIENTO A LA SEGURIDAD Y PRIVACIDAD DE INFORMACION.
PERIODO	DEL 01 DE ENERO AL 28 DE FEBRERO DE 2025

INTRODUCCIÓN:

Este informe tiene como objetivo presentar el seguimiento a las políticas, medidas y controles establecidos para garantizar la seguridad y privacidad de la información en la entidad, el seguimiento se realizó de acuerdo con los lineamientos establecidos en el marco normativo y regulatorio vigente, así como con las mejores prácticas internacionales en cuanto a la protección de datos y seguridad informática.

2. OBJETIVO GENERAL:

Evaluar la correcta identificación, análisis, efectividad de los controles y cumplimiento de las acciones de mitigación en la gestión de Riesgos de Seguridad de la información de la CPSM, con el fin de fortalecer las buenas prácticas de seguridad de la información como son: confidencialidad, integridad y disponibilidad y autenticidad de la información.

2.1 OBJETIVO ESPECIFICO:

Evaluar el estado de la Implementación del Modelo de Seguridad y Privacidad de la información (MSPI)

Establecer el nivel de cumplimiento de las acciones propuestas en los mapas de riesgo de seguridad de la información de la Caja de Previsión Social Municipal.

Identificar las acciones de mejora necesarias para cumplimiento a todas las acciones propuestas y a los estándares exigidos.

3. ALCANCE:

Verificar el cumplimiento de las acciones establecidas por la CPSM para la definición y tratamiento de los riesgos de seguridad de la información del 1 de enero al 28 de febrero de 2025.

4. MARCO NORMATIVO:

Norma	**Contenido**
Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
Ley 1266 de 2008	Conocida como "Ley de Habeas Data", ha sido establecida por el gobierno nacional con el objeto de desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en Banco de Datos.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
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.
Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información

	pública, accesibilidad web, seguridad digital, y datos abiertos
Decreto 1081 de 2015	Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la Republica

5. DESARROLLO DEL SEGUIMIENTO:

Dando cumplimiento a las funciones propias de la Oficina de Control Interno y al Plan Anual de auditorías se efectúo seguimiento a la Seguridad de la Información de la CPSM, el cual incluye el mapa de riesgos de seguridad de la información, a actividades implementadas y a la incorporación de las recomendaciones dadas en el seguimiento realizado en el 2024.

En este sentido, se inicia el seguimiento evaluando los siguientes parámetros:

5.1 Estado Actual de la Seguridad de la Información

En este ítem se evalúa el estado actual de la seguridad de la información de la Caja de Previsión Social Municipal que incluye:

Evaluación de Riesgos

Identifica los riesgos asociados con la gestión de la información y su clasificación, en este sentido la CPSM, cuenta con los siguientes

Fuga de información sensible: hace referencia al incidente de datos confidenciales o privados tales como información personal, financiera o estratégica que se filtran o se exponen sin autorización o control por parte de la persona encargada de sistemas de la entidad, que por errores humanos al configurar el sistema puede dar lugar a accesos indebidos o datos sensibles.

Accesos no autorizados: Se refiere a situaciones en las que personas o sistemas no autorizados logran obtener acceso a datos o recursos que deberían estar protegidos. Este tipo de acceso puede ocurrir en diferentes niveles y contextos dentro de una red y constituye una de las principales amenazas para la privacidad, integridad y disponibilidad de la información, que puede conllevar a Robo o alteración de datos, daños a la reputación e Interrupción del servicio.

Ataques Cibernéticos: hacen referencia a cualquier intento malintencionado de comprometer la confidencialidad, integridad o disponibilidad de la información almacenada, procesada en el sistema. Entre los ataques cibernéticos mas riesgosos se encuentra el Malware, Ransomware, Phishing y ataques de denegación de servicio DOS.

5.2 Riesgos Identificados:

Accesos no autorizados: Existe el riesgo de uso indebido de credenciales, ya sea por parte de terceros externos o de empleados malintencionados dentro de la entidad. No obstante, al momento del seguimiento, no se han evidenciado accesos no autorizados, lo que refleja que las medidas de control implementadas hasta la fecha están funcionando de manera efectiva para proteger los sistemas y la información. Sin embargo, se continuará monitorizando de forma constante para prevenir cualquier intento de acceso no autorizado.

Ataques Cibernéticos: Malware, Ransomware, Phishing y Ataques de Denegación de Servicio (DDoS): Estos tipos de ataques cibernéticos representan una amenaza significativa para la seguridad de la información y la infraestructura tecnológica de la entidad. No obstante, se ha logrado controlar eficazmente este tipo de amenazas mediante la implementación de capacitaciones de seguridad, brindadas de manera regular a los funcionarios. Estas capacitaciones están diseñadas para sensibilizar al personal sobre los riesgos asociados con los ataques cibernéticos y proporcionarles las herramientas necesarias para reconocer y mitigar estos ataques de manera oportuna. De esta manera, la CPSM, ha logrado fortalecer su postura de seguridad frente a este tipo de incidentes.

Fallos en la Infraestructura Tecnológica: Vulnerabilidad derivada de configuraciones inseguras o desactualización del software: Este riesgo se refiere a las posibles fallas en la infraestructura tecnológica ocasionadas por configuraciones incorrectas o por el uso de software desactualizado, lo que podría comprometer la seguridad de los sistemas. Sin embargo, este riesgo no se ha evidenciado en la entidad, ya que el software instalado es licenciado y se actualiza de forma periódica. Estas prácticas garantizan que la infraestructura tecnológica se mantenga segura, minimizando las vulnerabilidades derivadas de configuraciones inseguras o la falta de actualizaciones.

Riesgos en la protección de datos personales: Posibles amenazas y vulnerabilidades que comprometan la privacidad y seguridad de los datos personales: Este riesgo hace referencia a las amenazas que podrían afectar la

confidencialidad, integridad y disponibilidad de los datos personales almacenados, procesados o transmitidos en los sistemas de la entidad. En la Caja de Previsión Social Municipal (CPSM), existe un alto nivel de confiabilidad en cuanto a la capacidad de mantener la seguridad y privacidad de los datos personales, tanto de los funcionarios como de los afiliados adscritos a la entidad. Las políticas y procedimientos implementados garantizan que los datos personales sean protegidos adecuadamente, minimizando cualquier riesgo que pudiera comprometer su seguridad y privacidad.

5.3 Monitoreo realizado por el área de sistemas:

La dependencia de sistemas lleva a cabo un monitoreo continuo utilizando herramientas automatizadas para identificar vulnerabilidades y anomalías en la infraestructura tecnológica de la entidad. Para este propósito, se emplea el software Kaspersky, el cual cuenta con una licencia vigente que se renueva anualmente, asegurando así una protección constante contra amenazas cibernéticas.

Además, el área de sistemas brinda asesoría especializada para reaccionar de manera efectiva ante cualquier incidente relacionado con ataques cibernéticos, en particular aquellos que involucren Phishing, como los correos malintencionados. Se proporciona orientación sobre cómo identificar estos correos y las acciones correctivas necesarias para mitigar los riesgos asociados, garantizando la seguridad de la información y la infraestructura tecnológica de la entidad.

5.4 Controles de Seguridad realizados por la CPSM:

El sitio web de la Caja de Previsión Social cuenta un certificado SSL, el cual garantiza el intercambio seguro de la información transportando los datos de forma encriptada de extremo a extremo es decir que pueda ingresar a la plataforma web teniendo la seguridad de que no se va alterar la información en el proceso.

La Caja de Previsión Social Municipal de Bucaramanga, mediante su política de seguridad digital, establece las condiciones de uso de la infraestructura tecnología para los usuarios internos y externos así:

Las claves de acceso a los sistemas de información, correo electrónico y demás recursos tecnológicos son uso personal e intransferible, por tal razón se prohíbe compartir este tipo de credenciales de acceso.

Restricción de instalación y uso de juegos en los computadores de uso

institucional.

Los computadores y la infraestructura de red de la entidad solo pueden ser utilizada para usos instruccionales de la entidad.

Utilizar los recursos informáticos en forma negligente que ocasiones un daño temporal o permanente en los mismos.

Utilizar cualquier recurso informático de la entidad para propósitos comerciales que no tengan relación con la CPSM, para beneficio personal.

Utilización de los recursos informáticos de la red para guardar o transportar material ilegal pornográfico, que haga alusión al crimen o violencia ofensivo que lesione el buen nombre de los compañeros de trabajo.

Implementación de herramientas basada en antivirus y Firewalls embebido en equipos de cómputo de la entidad, es decir que vienen por defecto incluidos en cada uno de los equipos de la entidad.

Aplicación del principio de menor privilegio para limitar accesos únicamente a personal autorizado, cuentas de correo e inicio de sesión equipos personalizadas, para tal fin la entidad cuenta con diferentes tipos de acceso para que otros usuarios no tengan accesos a los mismos.

Permisos de usuarios para el ingreso de información requerida (administración y usuario).

Cuenta con privilegios dentro de los aplicativos que contienen información en la intranet (super administrador, moderador y usuario).

5.5 Mecanismos utilizados para almacenar la información:

En cuanto a los mecanismos relacionados con la infraestructura tecnológica utilizada para almacenar, procesar y trasmitir la información, la CPSM utiliza los Siguientes:

Almacenamiento: para tal fin hace uso de un servidor de la Alcaldía de Bucaramanga con configuraciones seguras, que se realiza cada dos meses y además discos duros locales para almacenamiento de copias de seguridad, las cuales son realizadas en forma mensual a cada una de las dependencias que conforman la Caja.

Trasmisión: Cifrado de extremo a extremo en todas las comunicaciones internas y externas con túneles seguros (VPN).

Protección de Datos Personales: Es una medida fundamental cuyo propósito es garantizar la privacidad y seguridad de la información personal en línea. Este concepto se centra en asegurar componentes clave de la seguridad de los datos, como la confidencialidad, la integridad y la disponibilidad de la información, tanto pública como privada. La implementación de medidas adecuadas en este ámbito busca proteger los datos de accesos no autorizados, alteraciones o destrucción, y asegurar que la información sea accesible solo por personas o entidades autorizadas para su uso.

En la CPSM, se ha establecido la protección de datos personales mediante la asignación de contraseñas, lo cual garantiza la confiabilidad e integridad de la información. Este sistema asegura que solo personas autorizadas puedan acceder a los datos sensibles.

Es importante señalar que los tipos de datos manejados en la entidad son los siguientes:

Datos Públicos: Son aquellos datos cuya consulta está permitida a cualquier persona sin restricción alguna. Se trata de información pública que se encuentra disponible en la página web de la entidad y en los equipos de las dependencias. Esta categoría abarca la información contenida en publicaciones sobre Transferencia y Acceso a la Información Pública.

Datos Privados: Son datos que, por su naturaleza íntima, solo interesan a los funcionarios autorizados para su manejo. Estos datos están reservados en las historias laborales, tanto en formato físico como digital, y se gestionan con estrictas medidas de seguridad para garantizar su confidencialidad.

Consentimiento Informado: Mecanismos claros y verificables para recolectar y documentar el consentimiento informado de los titulares, en el cual el afiliado autoriza el uso de su información personal, el cual se encuentra publicado en la página web en el apartado Autorización de Tratamiento de Datos Personales De conformidad con lo establecido en la Ley 1581 de 2012 y sus Decretos reglamentarios, y en concordancia con los lineamientos definidos en la Política de Tratamiento de Datos Personales de la Caja de Previsión Social Municipal de Bucaramanga.

5.6 Incidentes de Privacidad de la Información:

Hacen referencia a cualquier evento que ponga en peligro la privacidad de los datos personales, ya sea por acceso no autorizado, filtraciones, errores humanos o ciberataques. Para el caso de la CPSM, de acuerdo a la información reportada por el ingeniero de sistemas del periodo comprendido entre el 1 de enero al 28 de febrero de 2025 se registró 0 incidentes.

5.7 Capacitaciones:

Durante el periodo comprendido entre el 1 de enero y el 28 de febrero de 2025, no se han realizado capacitaciones. No obstante, es importante resaltar que el 19 de noviembre de 2024 se llevó a cabo una capacitación para los funcionarios de la entidad, enfocada en Ciberseguridad y Simulación de Ingeniería Social. Esta capacitación tuvo como objetivo reforzar los conocimientos y habilidades del personal en temas clave para la protección de la información y la seguridad digital.

5.8 Mapa de Riesgos de Gestión, Corrupción y Seguridad en la Información

Considerando el periodo de seguimiento evaluado, comprendido entre el 1 de enero y el 28 de febrero de 2025, se tomó como referencia el análisis realizado durante la vigencia del año 2024, específicamente a los Mapas de Riesgos de Gestión, Corrupción y Seguridad en la Información. A partir de este seguimiento, se obtuvieron los siguientes resultados:

Tipo de Riesgo	Descripción del Riesgo	Acciones Preventivas	Observación
GESTIÓN Y SEGURIDAD DE LA INFORMACION	Perdida de Información Física y Digital.	Solicitud a la oficina TIC acciones preventivas tomadas o a tomar para garantizar la salvaguarda de la información. Actualización de la documentación del proceso.	Durante la vigencia 2024, se evidencia que se realiza una copia de seguridad mensual, garantizando la protección y disponibilidad de la información La Valoración del Riesgo tiene una probabilidad Baja. Durante la vigencia 2024, se actualizaron los documentos relacionados con las TIC, el normograma, el procedimiento de respaldo de copias de seguridad, el procedimiento de seguridad y privacidad de la información, y el protocolo para la gestión, de incidentes de seguridad. Estas actualizaciones aseguran el cumplimiento de las normativas y la mejora continua en la gestión de la seguridad de la información. La Valoración del Riesgo tiene una probabilidad BAJA.

	GESTIÓN Y SEGURIDAD DE LA INFORMACION	Divulgación de información de manera inoportuna-inadecuada y desactualizada.	Documento de control para llevar el control de las publicaciones realizadas en la página web interna (intranet) y externa	Durante la vigencia 2024, se evidencio que existe control en cuanto al proceso de Gestión Tecnología En el periodo evaluado se evidencio que existe control en cuanto al proceso de Gestión Tecnología de Información referente al posible riesgo "Divulgación de información de manera inoportuna-inadecuada y desactualizada", la entidad ha realizado 42 publicaciones de contenidos solicitados por medio de correo electrónico a las diferentes áreas de la institución, el formato utilizado es el F-GTI-001 que reposa en la intranet, asegurando la pertinencia y oportunidad de la información divulgada. La evaluación del Riesgo tiene una Probabilidad BAJA.
	GESTIÓN Y SEGURIDAD DE LA INFORMACION	Utilización de herramientas tecnológicas inadecuadas (software, hardware, acceso a internet) que no permitan informar en las diferentes plataformas y/o frágiles ante la presencia de virus.	Revisión periódica del estado actual del antivirus Mantenimiento general de los equipos	Durante la vigencia del año 2024, se evidenció que, para mitigar el riesgo asociado al uso de los equipos que pueda afectar el software, hardware o el acceso a internet de las diferentes plataformas, la entidad realiza revisiones periódicas del estado actual del antivirus instalado en cada uno de los equipos. Estas revisiones incluyen un análisis detallado del funcionamiento y el estado de cada antivirus, garantizando su eficacia en la protección contra amenazas cibernéticas y asegurando la seguridad de la infraestructura tecnológica de la entidad. Durante la vigencia 2024 se llevaron a cabo 6 mantenimientos de software de seguridad antivirus, con el fin de asegurar la protección continua de los sistemas frente a posibles amenazas y garantizar su funcionamiento eficiente y actualizado. La valoración del riesgo es BAJA
	GESTIÓN Y SEGURIDAD DE LA INFORMACION	Perdida de disponibilidad de los sistemas de información que soporte los procesos de la entidad.	Realizar como mínimo una revisión y posterior mantenimiento a los equipos de la infraestructura tecnológica de la entidad.	Durante la vigencia 2024, Para mitigar el riesgo de pérdida de disponibilidad de los sistemas de información, la entidad realizo un mantenimiento preventivo a equipos de la entidad, teniendo en cuenta que la infraestructura física es adecuada para el funcionamiento de los equipos de la entidad. la probabilidad de riesgo es BAJA.

GESTIÓN Y SEGURIDAD DE LA INFORMACION	Pérdida de Confidencialidad de la información almacenada y gestionada en los sistemas de información de la entidad por parte de los exfuncionarios de la Entidad	Revisar de manera periódica y actualizar (si es necesario) los accesos a aplicativos GD para inhabilitar los accesos a los sistemas y activos de información de la entidad a los funcionarios y/o contratistas que finalicen sus labores contractuales con la entidad.	Durante la vigencia 2024, se revisaron de manera periódica y se actualizaron las accesos a los aplicativos GD, en cuanto al proceso de Gestión y Seguridad de la información, referente al posible riesgo "Pérdida de Confidencialidad de la información almacenada y gestionada en los sistemas de información de la entidad por parte de los exfuncionarios de la Entidad, la CPSM como medida de mitigación realiza la creación de usuarios en el sistema de información y deshabilita funcionarios que ya no laboran en la Caja de Previsión Social Municipal. La valoración del riesgo es BAJA
CORRUPCION	Posibilidad de afectación reputacional por adulterar o hacer mal uso de la información institucional, en beneficio propio o de terceros a través del suministro de información confidencial o protegida	Solicitud a sistemas de acciones preventivas tomadas o a tomar para garantizar la salvaguarda de la información.	En la vigencia 2024, Frente a la posibilidad de recibir o solicitar dádivas, ya sea a nombre propio o de terceros, para alterar la documentación oficial de la entidad, la CPSM mitiga este riesgo mediante la implementación de mecanismos para garantizar la confidencialidad de la información gestionada por el personal encargado de la gestión documental. Además, se controla estrictamente el préstamo de documentos, lo que evidencia que no existe riesgo de corrupción al respecto. En la página web de la entidad se encuentra disponible el "Índice de Información Clasificada y Reservada", el cual detalla las restricciones y condiciones para la consulta de la información producida por la CPSM. Este índice puede consultarse a través del siguiente enlace: https://asufn-my.sharepoint.com/:x:/g/personal/licencia20_asufn_onmicrosoft_com/ETan1rgSLFpGv8W1JV3hULMB9D9K4ZlmPAqSjauPqqsXow?e=xBkKPy La probabilidad de riesgo es baja, según el Tercer Seguimiento Evaluado.

5.9 Seguimiento a Recomendaciones FURAG

Desde la evaluación de los elementos de la Política de Seguridad y Privacidad de la Información, conforme con el último reporte de FURAG, se tomaron en cuenta las recomendaciones suministradas por el Departamento Administrativo de la Función Pública, de la siguiente manera:

Establecer, documentar e implementar un procedimiento para la gestión de incidentes de seguridad digital (Ciberseguridad) que incluya la notificación a las autoridades pertinentes, como el CSIRT Gobierno y COLCERT.

En relación con esta recomendación, la entidad ha implementado un procedimiento integral para la seguridad y privacidad de la información, así como para la gestión de incidentes de seguridad digital. Este procedimiento asegura una respuesta efectiva ante posibles amenazas y vulnerabilidades, mediante la actualización continua de las políticas de ciberseguridad. Además, se ha establecido un protocolo para la notificación oportuna a las autoridades pertinentes en caso de incidentes que lo requieran.

Implementar el Modelo de Seguridad y Privacidad de la Informacion (MSPI).

La entidad tiene implementado el Modelo de Seguridad y Privacidad de la Información (MSPI), asegurando la protección de los datos y la gestión de riesgos de seguridad digital.

Evidencias de implementación:

Política de Seguridad y Privacidad de la Información:

La entidad cuenta con una política formalizada de seguridad y privacidad, la cual establece directrices claras sobre la gestión de la información, clasificación de datos y medidas de protección.

Gestión de Riesgos de Seguridad de la Información:

Se han realizado análisis de riesgos periódicos, identificando amenazas y vulnerabilidades que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Se han implementado controles de seguridad en infraestructura tecnológica, sistemas de información y accesos.

Procedimientos y Planes de Contingencia:

Se cuenta con un procedimiento documentado de gestión de incidentes de seguridad digital, asegurando la notificación a las autoridades pertinentes, como CSIRT-Gobierno o COLCERT.

Se han establecido planes de continuidad del negocio y recuperación ante desastres para garantizar la operatividad de los servicios en caso de incidentes críticos.

Protección de Datos Personales:

Se han adoptado medidas para garantizar el cumplimiento de la Ley 1581 de 2012 sobre protección de datos personales, asegurando que el tratamiento de la información sea seguro y conforme a la normativa vigente.

Capacitaciones en Seguridad Digital:

Se han realizado capacitaciones a funcionarios y contratistas en temas de seguridad y privacidad de la información, incluyendo buenas prácticas de ciberseguridad y normativas aplicables.

Se han aplicado herramientas de monitoreo y control para detectar y mitigar posibles riesgos de seguridad.

Con estas acciones, la entidad asegura la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), fortaleciendo la ciberseguridad y la protección de los datos en todos sus procesos.

Realizar analisis de vulnerabilidades para Portal Web, Sede electronica y Servicios expuestos en internet.

En lo que respecta a esta recomendación se ha realizado el análisis de vulnerabilidades para el Portal Web, la Sede Electrónica y los Servicios expuestos en Internet, con el fin de identificar y mitigar riesgos de seguridad digital. Para ello se presenta el Informe analisis vulnerabilidad de seguridad a los activos de información.

Este análisis fortalece la ciberseguridad de la entidad y contribuye a la protección de los datos y la disponibilidad de los servicios digitales.

Análisis de Vulnerabilidades para Portal Web, Sede Electrónica y Servicios Expuestos en Internet

En lo que respecta a esta recomendación, se ha realizado un análisis exhaustivo de vulnerabilidades para el Portal Web, la Sede Electrónica y los Servicios expuestos en Internet, con el objetivo de identificar y mitigar los riesgos de seguridad digital.

Este análisis refuerza la ciberseguridad de la entidad, contribuyendo significativamente a la protección de los datos y a garantizar la disponibilidad continua de los servicios digitales, minimizando así posibles amenazas que puedan comprometer la seguridad y funcionamiento de los sistemas expuestos en línea.

Realizar pruebas de respaldo a las copias de seguridad de la informacion de los aplicativos misionales, estrategicos, soporte y de mejora de manera programada para aegurar la disponibilidad de los datos en caso de Ransomware, de manera coordinada con los responsables del proceso.

La Caja de Previsión Social Municipal ha llevado a cabo pruebas periódicas de respaldo y restauración de las copias de seguridad de la información de los aplicativos misionales, estratégicos, de soporte y de mejora, de manera programada y en estrecha coordinación con los responsables del proceso. El objetivo de estas pruebas es asegurar la disponibilidad de los datos en caso de un ataque de Ransomware u otros incidentes de seguridad.

Estas copias de seguridad se realizan al final de cada mes o cuando se requiera, garantizando así la integridad y disponibilidad de la información crítica para la entidad en cualquier situación de emergencia.

Separar los equipos que realizan las copias de respaldo de la informacion, del software e imágenes de los sistemas de la red de servidores y computadores.

Los equipos encargados de realizar las copias de respaldo de la información, del software e imágenes de los sistemas de la red de servidores y computadores están completamente separados, garantizando así la seguridad y disponibilidad de los datos en caso de incidentes. Tanto el servidor externo utilizado para almacenar las copias de seguridad, como los discos duros internos de los equipos, están físicamente separados, lo que minimiza el riesgo de pérdida de datos y mejora la protección frente a amenazas externas, como ataques de ransomware u otros incidentes de seguridad.

Tener documentados e implementados procedimientos para copias de respaldo y de restauracion de la informacion, del software e imágenes de los sistemas.

La entidad cuenta con procedimientos debidamente documentados e

implementados para la realización de copias de respaldo y restauración de la información, del software e imágenes de los sistemas, con el fin de garantizar la seguridad, disponibilidad e integridad de los datos en caso de incidentes.

Procedimientos Documentados:

Se dispone de un Plan de Backup y Recuperación de Datos, el cual establece los lineamientos y las mejores prácticas para la ejecución de copias de seguridad y restauración de la información.

Se han definido roles y responsabilidades claras para el personal encargado de gestionar los respaldos, lo que asegura una ejecución eficiente y controlada del proceso.

Tipos de Copias de Respaldo Implementadas:

Respaldo completo: Se realiza una copia integral de toda la información en intervalos periódicos definidos.

Respaldo incremental: Solo se almacenan los cambios realizados desde la última copia de seguridad, optimizando el espacio y reduciendo el tiempo de respaldo.

Respaldo diferencial: Permite recuperar la información en menor tiempo, ya que contiene todos los cambios efectuados desde la última copia completa.

Frecuencia y Almacenamiento de los Respaldos:

Los respaldos se realizan de manera programada, con copias mensuales, adaptándose a la criticidad de cada sistema.

Se almacenan en infraestructura separada, incluyendo discos locales y almacenamiento en la nube, con cifrado y control de acceso para garantizar la seguridad de la información.

Procedimiento de Restauración de la Información:

Se han documentado los pasos detallados para recuperar los datos en caso de incidentes, asegurando una respuesta rápida y efectiva.

Se realizan pruebas de restauración periódicas en entornos controlados para validar la integridad y disponibilidad de los datos, garantizando que el proceso de restauración sea eficiente y confiable en caso de necesidad.

Verificación y Aseguramiento del Cumplimiento de Políticas de Ciberseguridad por Proveedores y Contratistas

La entidad asegura que tanto proveedores como contratistas cumplen con las políticas de ciberseguridad internas mediante la implementación de controles periódicos que garantizan el cumplimiento de los estándares de seguridad establecidos. Estos controles incluyen evaluaciones regulares, revisiones de los protocolos de seguridad y la exigencia de acuerdos contractuales que estipulen claramente los requisitos de ciberseguridad. De esta manera, se minimizan los riesgos asociados con la gestión de proveedores y contratistas, asegurando la protección de la información y la infraestructura de la entidad.

6. CONCLUSIONES Y RECOMENDACIONES

Conclusión:

La Caja de Previsión Social Municipal, ha implementado un conjunto robusto de políticas y procedimientos para garantizar la seguridad y privacidad de la información, adaptándose a los estándares y mejores prácticas del sector.

A lo largo del periodo evaluado, se han tomado medidas significativas para proteger los datos tanto personales como sensibles, incluyendo la implementación de controles de seguridad, la realización de pruebas periódicas de respaldo y restauración, y la gestión de incidentes de ciberseguridad.

Además, se han establecido protocolos claros para asegurar el cumplimiento de las políticas de seguridad por parte de proveedores y contratistas.

El seguimiento constante y la actualización de los procedimientos de seguridad permiten a la entidad fortalecer su infraestructura tecnológica y garantizar la disponibilidad e integridad de la información en todo momento.

NUBIA ESTHER LEON VILLALBA
Jefe de Oficina de Control Interno.